aws

API Reference

Amazon GuardDuty



API Version 2017-11-28

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon GuardDuty: API Reference

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Welcome **1**
Actions **2**
AcceptAdministratorInvitation 6
Request Syntax 6
URI Request Parameters 6
Request Body 6
Response Syntax 7
Response Elements 7
Errors 7
See Also 8
AcceptInvitation 9
Request Syntax 9
URI Request Parameters 9
Request Body 9
Response Syntax 10
Response Elements 10
Errors 10
See Also 11
ArchiveFindings 12
Request Syntax 12
URI Request Parameters 12
Request Body 12
Response Syntax 13
Response Elements 13
Errors 13
See Also 14
CreateCustomDetectionRuleAssociation 15
Request Syntax 15
URI Request Parameters 15
Request Body 15
Response Syntax 16
Response Elements 17
Errors 17
See Also 19

CreateCustomDetectionRuleOrgConfiguration ... 20
Request Syntax ... 20
URI Request Parameters ... 20
Request Body ... 20
Response Syntax ... 21
Response Elements ... 22
Errors ... 22
See Also ... 23
CreateDetector ... 25
Request Syntax ... 25
URI Request Parameters ... 26
Request Body ... 26
Response Syntax ... 28
Response Elements ... 28
Errors ... 29
See Also ... 29
CreateFilter ... 31
Request Syntax ... 31
URI Request Parameters ... 32
Request Body ... 32
Response Syntax ... 56
Response Elements ... 56
Errors ... 57
See Also ... 57
CreateInvestigation ... 59
Request Syntax ... 59
URI Request Parameters ... 59
Request Body ... 60
Response Syntax ... 60
Response Elements ... 61
Errors ... 61
See Also ... 62
CreateIPSet ... 63
Request Syntax ... 63
URI Request Parameters ... 63
Request Body ... 64

Response Syntax ... 65
Response Elements ... 66
Errors ... 66
See Also ... 67
CreateMalwareProtectionPlan ... 68
Request Syntax ... 68
URI Request Parameters ... 68
Request Body ... 68
Response Syntax ... 70
Response Elements ... 70
Errors ... 70
See Also ... 71
CreateMembers ... 73
Request Syntax ... 73
URI Request Parameters ... 74
Request Body ... 74
Response Syntax ... 74
Response Elements ... 75
Errors ... 75
See Also ... 76
CreatePublishingDestination ... 77
Request Syntax ... 77
URI Request Parameters ... 77
Request Body ... 77
Response Syntax ... 79
Response Elements ... 79
Errors ... 79
See Also ... 80
CreateSampleFindings ... 81
Request Syntax ... 81
URI Request Parameters ... 81
Request Body ... 81
Response Syntax ... 82
Response Elements ... 82
Errors ... 82
See Also ... 83

CreateThreatEntitySet 84
Request Syntax 84
URI Request Parameters 84
Request Body 85
Response Syntax 87
Response Elements 87
Errors 87
See Also 88
CreateThreatIntelSet 89
Request Syntax 89
URI Request Parameters 89
Request Body 90
Response Syntax 91
Response Elements 92
Errors 92
See Also 93
CreateTrustedEntitySet 94
Request Syntax 94
URI Request Parameters 94
Request Body 95
Response Syntax 97
Response Elements 97
Errors 97
See Also 98
DeclineInvitations 99
Request Syntax 99
URI Request Parameters 99
Request Body 99
Response Syntax 99
Response Elements 100
Errors 100
See Also 101
DeleteCustomDetectionRuleAssociation 102
Request Syntax 102
URI Request Parameters 102
Request Body 102

Response Syntax 102
Response Elements 103
Errors 103
See Also 104
DeleteCustomDetectionRuleOrgConfiguration 105
Request Syntax 105
URI Request Parameters 105
Request Body 105
Response Syntax 105
Response Elements 106
Errors 106
See Also 107
DeleteDetector 109
Request Syntax 109
URI Request Parameters 109
Request Body 109
Response Syntax 109
Response Elements 109
Errors 109
See Also 110
DeleteFilter 112
Request Syntax 112
URI Request Parameters 112
Request Body 112
Response Syntax 112
Response Elements 112
Errors 113
See Also 113
DeleteInvitations 115
Request Syntax 115
URI Request Parameters 115
Request Body 115
Response Syntax 115
Response Elements 116
Errors 116
See Also 117

DeleteIPSet ... 118
Request Syntax ... 118
URI Request Parameters ... 118
Request Body ... 118
Response Syntax ... 118
Response Elements ... 118
Errors ... 119
See Also ... 119
DeleteMalwareProtectionPlan ... 121
Request Syntax ... 121
URI Request Parameters ... 121
Request Body ... 121
Response Syntax ... 121
Response Elements ... 121
Errors ... 121
See Also ... 123
DeleteMembers ... 124
Request Syntax ... 124
URI Request Parameters ... 124
Request Body ... 124
Response Syntax ... 125
Response Elements ... 125
Errors ... 125
See Also ... 126
DeletePublishingDestination ... 127
Request Syntax ... 127
URI Request Parameters ... 127
Request Body ... 127
Response Syntax ... 127
Response Elements ... 127
Errors ... 128
See Also ... 128
DeleteThreatEntitySet ... 130
Request Syntax ... 130
URI Request Parameters ... 130
Request Body ... 130

Response Syntax 130
Response Elements 130
Errors 131
See Also 131
DeleteThreatIntelSet 133
Request Syntax 133
URI Request Parameters 133
Request Body 133
Response Syntax 133
Response Elements 133
Errors 134
See Also 134
DeleteTrustedEntitySet 136
Request Syntax 136
URI Request Parameters 136
Request Body 136
Response Syntax 136
Response Elements 136
Errors 137
See Also 137
DescribeMalwareScans 139
Request Syntax 139
URI Request Parameters 139
Request Body 140
Response Syntax 141
Response Elements 142
Errors 142
See Also 143
DescribeOrganizationConfiguration 144
Request Syntax 144
URI Request Parameters 144
Request Body 145
Response Syntax 145
Response Elements 146
Errors 147
See Also 148

DescribePublishingDestination ... 149
Request Syntax ... 149
URI Request Parameters ... 149
Request Body ... 149
Response Syntax ... 149
Response Elements ... 150
Errors ... 151
See Also ... 152
DisableOrganizationAdminAccount ... 153
Request Syntax ... 153
URI Request Parameters ... 153
Request Body ... 153
Response Syntax ... 153
Response Elements ... 153
Errors ... 154
See Also ... 154
DisassociateFromAdministratorAccount ... 156
Request Syntax ... 156
URI Request Parameters ... 156
Request Body ... 156
Response Syntax ... 156
Response Elements ... 156
Errors ... 157
See Also ... 157
DisassociateFromMasterAccount ... 159
Request Syntax ... 159
URI Request Parameters ... 159
Request Body ... 159
Response Syntax ... 159
Response Elements ... 159
Errors ... 160
See Also ... 160
DisassociateMembers ... 162
Request Syntax ... 162
URI Request Parameters ... 162
Request Body ... 163

Response Syntax ... 163
Response Elements ... 164
Errors ... 164
See Also ... 165
EnableOrganizationAdminAccount ... 166
Request Syntax ... 166
URI Request Parameters ... 166
Request Body ... 166
Response Syntax ... 166
Response Elements ... 166
Errors ... 167
See Also ... 167
GetAdministratorAccount ... 169
Request Syntax ... 169
URI Request Parameters ... 169
Request Body ... 169
Response Syntax ... 169
Response Elements ... 170
Errors ... 170
See Also ... 171
GetCoverageStatistics ... 172
Request Syntax ... 172
URI Request Parameters ... 172
Request Body ... 173
Response Syntax ... 173
Response Elements ... 173
Errors ... 174
See Also ... 174
GetCustomDetectionRule ... 176
Request Syntax ... 176
URI Request Parameters ... 176
Request Body ... 176
Response Syntax ... 176
Response Elements ... 177
Errors ... 177
See Also ... 179

GetCustomDetectionRuleAssociation 180
Request Syntax 180
URI Request Parameters 180
Request Body 180
Response Syntax 180
Response Elements 181
Errors 182
See Also 183
GetCustomDetectionRuleOrgConfiguration 184
Request Syntax 184
URI Request Parameters 184
Request Body 184
Response Syntax 184
Response Elements 185
Errors 185
See Also 186
GetDetector 188
Request Syntax 188
URI Request Parameters 188
Request Body 188
Response Syntax 188
Response Elements 190
Errors 191
See Also 192
GetFilter 193
Request Syntax 193
URI Request Parameters 193
Request Body 193
Response Syntax 193
Response Elements 194
Errors 196
See Also 197
GetFindings 198
Request Syntax 198
URI Request Parameters 198
Request Body 198

Response Syntax 199
Response Elements 224
Errors 224
See Also 225
GetFindingsStatistics 226
Request Syntax 226
URI Request Parameters 227
Request Body 227
Response Syntax 228
Response Elements 229
Errors 230
See Also 231
GetInvestigation 232
Request Syntax 232
URI Request Parameters 232
Request Body 232
Response Syntax 233
Response Elements 233
Errors 234
See Also 235
GetInvitationsCount 236
Request Syntax 236
URI Request Parameters 236
Request Body 236
Response Syntax 236
Response Elements 236
Errors 237
See Also 237
GetIPSet 239
Request Syntax 239
URI Request Parameters 239
Request Body 239
Response Syntax 239
Response Elements 240
Errors 241
See Also 242

GetMalwareProtectionPlan ... 243
Request Syntax ... 243
URI Request Parameters ... 243
Request Body ... 243
Response Syntax ... 243
Response Elements ... 244
Errors ... 245
See Also ... 247
GetMalwareScan ... 248
Request Syntax ... 248
URI Request Parameters ... 248
Request Body ... 248
Response Syntax ... 248
Response Elements ... 250
Errors ... 254
See Also ... 255
GetMalwareScanSettings ... 256
Request Syntax ... 256
URI Request Parameters ... 256
Request Body ... 256
Response Syntax ... 256
Response Elements ... 257
Errors ... 258
See Also ... 258
GetMasterAccount ... 260
Request Syntax ... 260
URI Request Parameters ... 260
Request Body ... 260
Response Syntax ... 260
Response Elements ... 261
Errors ... 261
See Also ... 262
GetMemberDetectors ... 263
Request Syntax ... 263
URI Request Parameters ... 263
Request Body ... 263

Response Syntax ... 264
Response Elements ... 265
Errors ... 266
See Also ... 266
GetMembers ... 268
Request Syntax ... 268
URI Request Parameters ... 268
Request Body ... 268
Response Syntax ... 269
Response Elements ... 269
Errors ... 270
See Also ... 270
GetOrganizationStatistics ... 272
Request Syntax ... 272
URI Request Parameters ... 272
Request Body ... 272
Response Syntax ... 272
Response Elements ... 273
Errors ... 273
See Also ... 274
GetRemainingFreeTrialDays ... 275
Request Syntax ... 275
URI Request Parameters ... 275
Request Body ... 275
Response Syntax ... 276
Response Elements ... 277
Errors ... 277
See Also ... 278
GetThreatEntitySet ... 279
Request Syntax ... 279
URI Request Parameters ... 279
Request Body ... 279
Response Syntax ... 279
Response Elements ... 280
Errors ... 282
See Also ... 282

GetThreatIntelSet ... 284
Request Syntax ... 284
URI Request Parameters ... 284
Request Body ... 284
Response Syntax ... 284
Response Elements ... 285
Errors ... 286
See Also ... 287
GetTrustedEntitySet ... 288
Request Syntax ... 288
URI Request Parameters ... 288
Request Body ... 288
Response Syntax ... 288
Response Elements ... 289
Errors ... 291
See Also ... 291
GetUsageStatistics ... 293
Request Syntax ... 293
URI Request Parameters ... 293
Request Body ... 294
Response Syntax ... 295
Response Elements ... 296
Errors ... 297
See Also ... 297
InviteMembers ... 299
Request Syntax ... 299
URI Request Parameters ... 300
Request Body ... 300
Response Syntax ... 301
Response Elements ... 301
Errors ... 301
See Also ... 302
ListCoverage ... 303
Request Syntax ... 303
URI Request Parameters ... 303
Request Body ... 304

Response Syntax ... 305
Response Elements ... 306
Errors ... 306
See Also ... 307
ListCustomDetectionRuleAssociations ... 308
Request Syntax ... 308
URI Request Parameters ... 308
Request Body ... 308
Response Syntax ... 309
Response Elements ... 309
Errors ... 309
See Also ... 310
ListCustomDetectionRuleOrgConfigurations ... 312
Request Syntax ... 312
URI Request Parameters ... 312
Request Body ... 312
Response Syntax ... 312
Response Elements ... 313
Errors ... 313
See Also ... 314
ListCustomDetectionRules ... 316
Request Syntax ... 316
URI Request Parameters ... 316
Request Body ... 316
Response Syntax ... 317
Response Elements ... 318
Errors ... 318
See Also ... 319
ListDetectors ... 320
Request Syntax ... 320
URI Request Parameters ... 320
Request Body ... 320
Response Syntax ... 320
Response Elements ... 321
Errors ... 321
See Also ... 322

ListFilters ... 323
Request Syntax ... 323
URI Request Parameters ... 323
Request Body ... 323
Response Syntax ... 324
Response Elements ... 324
Errors ... 324
See Also ... 325
ListFindings ... 326
Request Syntax ... 326
URI Request Parameters ... 327
Request Body ... 327
Response Syntax ... 330
Response Elements ... 330
Errors ... 330
See Also ... 331
ListInvestigations ... 332
Request Syntax ... 332
URI Request Parameters ... 332
Request Body ... 333
Response Syntax ... 333
Response Elements ... 334
Errors ... 334
See Also ... 335
ListInvitations ... 337
Request Syntax ... 337
URI Request Parameters ... 337
Request Body ... 337
Response Syntax ... 337
Response Elements ... 338
Errors ... 338
See Also ... 339
ListIPSets ... 340
Request Syntax ... 340
URI Request Parameters ... 340
Request Body ... 340

Response Syntax ... 341
Response Elements ... 341
Errors ... 341
See Also ... 342
ListMalwareProtectionPlans ... 343
Request Syntax ... 343
URI Request Parameters ... 343
Request Body ... 343
Response Syntax ... 343
Response Elements ... 343
Errors ... 344
See Also ... 345
ListMalwareScans ... 346
Request Syntax ... 346
URI Request Parameters ... 346
Request Body ... 347
Response Syntax ... 347
Response Elements ... 348
Errors ... 348
See Also ... 349
ListMembers ... 350
Request Syntax ... 350
URI Request Parameters ... 350
Request Body ... 351
Response Syntax ... 351
Response Elements ... 351
Errors ... 352
See Also ... 352
ListOrganizationAdminAccounts ... 354
Request Syntax ... 354
URI Request Parameters ... 354
Request Body ... 354
Response Syntax ... 354
Response Elements ... 355
Errors ... 355
See Also ... 356

ListPublishingDestinations ... 357
Request Syntax ... 357
URI Request Parameters ... 357
Request Body ... 357
Response Syntax ... 357
Response Elements ... 358
Errors ... 358
See Also ... 359
ListTagsForResource ... 360
Request Syntax ... 360
URI Request Parameters ... 360
Request Body ... 360
Response Syntax ... 360
Response Elements ... 361
Errors ... 361
See Also ... 362
ListThreatEntitySets ... 363
Request Syntax ... 363
URI Request Parameters ... 363
Request Body ... 363
Response Syntax ... 364
Response Elements ... 364
Errors ... 364
See Also ... 365
ListThreatIntelSets ... 366
Request Syntax ... 366
URI Request Parameters ... 366
Request Body ... 366
Response Syntax ... 367
Response Elements ... 367
Errors ... 367
See Also ... 368
ListTrustedEntitySets ... 369
Request Syntax ... 369
URI Request Parameters ... 369
Request Body ... 369

Response Syntax ... 370
Response Elements ... 370
Errors ... 370
See Also ... 371
SendObjectMalwareScan ... 372
Request Syntax ... 372
URI Request Parameters ... 372
Request Body ... 372
Response Syntax ... 373
Response Elements ... 373
Errors ... 373
See Also ... 374
StartMalwareScan ... 375
Request Syntax ... 375
URI Request Parameters ... 375
Request Body ... 375
Response Syntax ... 376
Response Elements ... 376
Errors ... 377
See Also ... 378
StartMonitoringMembers ... 379
Request Syntax ... 379
URI Request Parameters ... 379
Request Body ... 379
Response Syntax ... 380
Response Elements ... 380
Errors ... 380
See Also ... 381
StopMonitoringMembers ... 382
Request Syntax ... 382
URI Request Parameters ... 382
Request Body ... 382
Response Syntax ... 383
Response Elements ... 383
Errors ... 383
See Also ... 384

TagResource ... 386
Request Syntax ... 386
URI Request Parameters ... 386
Request Body ... 386
Response Syntax ... 387
Response Elements ... 387
Errors ... 387
See Also ... 388
UnarchiveFindings ... 389
Request Syntax ... 389
URI Request Parameters ... 389
Request Body ... 389
Response Syntax ... 390
Response Elements ... 390
Errors ... 390
See Also ... 391
UntagResource ... 392
Request Syntax ... 392
URI Request Parameters ... 392
Request Body ... 392
Response Syntax ... 392
Response Elements ... 393
Errors ... 393
See Also ... 394
UpdateCustomDetectionRuleAssociation ... 395
Request Syntax ... 395
URI Request Parameters ... 395
Request Body ... 395
Response Syntax ... 396
Response Elements ... 396
Errors ... 396
See Also ... 398
UpdateCustomDetectionRuleOrgConfiguration ... 399
Request Syntax ... 399
URI Request Parameters ... 399
Request Body ... 399

Response Syntax ... 400
Response Elements ... 400
Errors ... 400
See Also ... 402
UpdateDetector ... 403
Request Syntax ... 403
URI Request Parameters ... 404
Request Body ... 404
Response Syntax ... 405
Response Elements ... 405
Errors ... 405
See Also ... 406
UpdateFilter ... 407
Request Syntax ... 407
URI Request Parameters ... 407
Request Body ... 408
Response Syntax ... 431
Response Elements ... 431
Errors ... 432
See Also ... 432
UpdateFindingsFeedback ... 434
Request Syntax ... 434
URI Request Parameters ... 434
Request Body ... 434
Response Syntax ... 435
Response Elements ... 435
Errors ... 435
See Also ... 436
UpdateIPSet ... 437
Request Syntax ... 437
URI Request Parameters ... 437
Request Body ... 437
Response Syntax ... 438
Response Elements ... 439
Errors ... 439
See Also ... 440

UpdateMalwareProtectionPlan ... 441
Request Syntax ... 441
URI Request Parameters ... 441
Request Body ... 441
Response Syntax ... 442
Response Elements ... 442
Errors ... 442
See Also ... 444
UpdateMalwareScanSettings ... 445
Request Syntax ... 445
URI Request Parameters ... 445
Request Body ... 446
Response Syntax ... 446
Response Elements ... 446
Errors ... 447
See Also ... 447
UpdateMemberDetectors ... 449
Request Syntax ... 449
URI Request Parameters ... 450
Request Body ... 450
Response Syntax ... 451
Response Elements ... 451
Errors ... 452
See Also ... 452
UpdateOrganizationConfiguration ... 454
Request Syntax ... 454
URI Request Parameters ... 455
Request Body ... 455
Response Syntax ... 457
Response Elements ... 457
Errors ... 457
See Also ... 458
UpdatePublishingDestination ... 459
Request Syntax ... 459
URI Request Parameters ... 459
Request Body ... 459

Response Syntax ... 460
Response Elements ... 460
Errors ... 460
See Also ... 461
UpdateThreatEntitySet ... 462
Request Syntax ... 462
URI Request Parameters ... 462
Request Body ... 462
Response Syntax ... 464
Response Elements ... 464
Errors ... 464
See Also ... 464
UpdateThreatIntelSet ... 466
Request Syntax ... 466
URI Request Parameters ... 466
Request Body ... 466
Response Syntax ... 467
Response Elements ... 468
Errors ... 468
See Also ... 469
UpdateTrustedEntitySet ... 470
Request Syntax ... 470
URI Request Parameters ... 470
Request Body ... 470
Response Syntax ... 472
Response Elements ... 472
Errors ... 472
See Also ... 472
Data Types ... 474
AccessControlList ... 484
Contents ... 484
See Also ... 484
AccessKey ... 485
Contents ... 485
See Also ... 485
AccessKeyDetails ... 486

Contents ... 486
See Also ... 486
Account ... 488
Contents ... 488
See Also ... 488
AccountDetail ... 489
Contents ... 489
See Also ... 490
AccountFreeTrialInfo ... 491
Contents ... 491
See Also ... 491
AccountLevelPermissions ... 492
Contents ... 492
See Also ... 492
AccountStatistics ... 493
Contents ... 493
See Also ... 493
Action ... 494
Contents ... 494
See Also ... 495
Activity ... 497
Contents ... 497
See Also ... 497
Actor ... 498
Contents ... 498
See Also ... 498
ActorProcess ... 500
Contents ... 500
See Also ... 500
AdditionalInfo ... 502
Contents ... 502
See Also ... 502
AddonDetails ... 503
Contents ... 503
See Also ... 503
AdminAccount ... 504

Contents 504
See Also 504
Administrator 505
Contents 505
See Also 505
AgentDetails 507
Contents 507
See Also 507
Anomaly 508
Contents 508
See Also 508
AnomalyObject 509
Contents 509
See Also 509
AnomalyUnusual 511
Contents 511
See Also 511
ApiCall 512
Contents 512
See Also 513
AssociationDetail 514
Contents 514
See Also 515
AssociationSummary 517
Contents 517
See Also 518
AutonomousSystem 519
Contents 519
See Also 519
AutoscalingAutoScalingGroup 520
Contents 520
See Also 520
AwsApiCallAction 521
Contents 521
See Also 522
BedrockGuardrail 523

Contents ... 523
See Also ... 523
BedrockGuardrailDetails ... 524
Contents ... 524
See Also ... 525
BedrockGuardrailResource ... 526
Contents ... 526
See Also ... 526
BlockPublicAccess ... 528
Contents ... 528
See Also ... 528
BucketLevelPermissions ... 530
Contents ... 530
See Also ... 530
BucketPolicy ... 531
Contents ... 531
See Also ... 531
City ... 532
Contents ... 532
See Also ... 532
CloudDetails ... 533
Contents ... 533
See Also ... 533
CloudformationStack ... 535
Contents ... 535
See Also ... 535
CloudTrailConfigurationResult ... 536
Contents ... 536
See Also ... 536
Condition ... 537
Contents ... 537
See Also ... 540
Container ... 541
Contents ... 541
See Also ... 542
ContainerFindingResource ... 543

Contents ... 543
See Also ... 543
ContainerInstanceDetails ... 544
Contents ... 544
See Also ... 544
ContentPolicyFilter ... 545
Contents ... 545
See Also ... 545
ContinuousScanDetails ... 547
Contents ... 547
See Also ... 547
Country ... 548
Contents ... 548
See Also ... 548
CoverageEc2InstanceDetails ... 549
Contents ... 549
See Also ... 550
CoverageEcsClusterDetails ... 551
Contents ... 551
See Also ... 551
CoverageEksClusterDetails ... 552
Contents ... 552
See Also ... 553
CoverageFilterCondition ... 554
Contents ... 554
See Also ... 554
CoverageFilterCriteria ... 555
Contents ... 555
See Also ... 555
CoverageFilterCriterion ... 556
Contents ... 556
See Also ... 556
CoverageResource ... 558
Contents ... 558
See Also ... 559
CoverageResourceDetails ... 560

Contents ... 560
See Also ... 560
CoverageSortCriteria ... 562
Contents ... 562
See Also ... 562
CoverageStatistics ... 564
Contents ... 564
See Also ... 564
CreateProtectedResource ... 565
Contents ... 565
See Also ... 565
CreateS3BucketResource ... 566
Contents ... 566
See Also ... 566
DataSourceConfigurations ... 567
Contents ... 567
See Also ... 567
DataSourceConfigurationsResult ... 568
Contents ... 568
See Also ... 569
DataSourceFreeTrial ... 570
Contents ... 570
See Also ... 570
DataSourcesFreeTrial ... 571
Contents ... 571
See Also ... 572
DateStatistics ... 573
Contents ... 573
See Also ... 573
DefaultServerSideEncryption ... 575
Contents ... 575
See Also ... 575
Destination ... 576
Contents ... 576
See Also ... 576
DestinationProperties ... 578

Contents 578
See Also 578
Detection 579
Contents 579
See Also 579
DetectionRuleEc2Requirements 580
Contents 580
See Also 580
DetectionRuleEcsFargateRequirements 581
Contents 581
See Also 581
DetectionRuleEksRequirements 582
Contents 582
See Also 582
DetectionRuleFilter 583
Contents 583
See Also 583
DetectionRuleOrgConfiguration 585
Contents 585
See Also 587
DetectionRuleOrgConfigurationSummary 588
Contents 588
See Also 589
DetectionRuleRuntimeMonitoringDetails 590
Contents 590
See Also 590
DetectionRuleRuntimePlatforms 591
Contents 591
See Also 591
DetectorAdditionalConfiguration 593
Contents 593
See Also 593
DetectorAdditionalConfigurationResult 594
Contents 594
See Also 595
DetectorFeatureConfiguration 596

Contents ... 596
See Also ... 597
DetectorFeatureConfigurationResult ... 598
Contents ... 598
See Also ... 599
DNSLogsConfigurationResult ... 600
Contents ... 600
See Also ... 600
DnsRequestAction ... 601
Contents ... 601
See Also ... 602
DomainDetails ... 603
Contents ... 603
See Also ... 603
EbsSnapshot ... 604
Contents ... 604
See Also ... 604
EbsSnapshotDetails ... 605
Contents ... 605
See Also ... 605
EbsVolumeDetails ... 606
Contents ... 606
See Also ... 606
EbsVolumeScanDetails ... 607
Contents ... 607
See Also ... 608
EbsVolumesResult ... 609
Contents ... 609
See Also ... 609
Ec2Image ... 610
Contents ... 610
See Also ... 610
Ec2ImageDetails ... 611
Contents ... 611
See Also ... 611
Ec2Instance ... 612

Contents ... 612
See Also ... 613
Ec2LaunchTemplate ... 615
Contents ... 615
See Also ... 615
Ec2NetworkInterface ... 616
Contents ... 616
See Also ... 617
Ec2Vpc ... 618
Contents ... 618
See Also ... 618
EcsCluster ... 619
Contents ... 619
See Also ... 619
EcsClusterDetails ... 620
Contents ... 620
See Also ... 621
EcsTask ... 622
Contents ... 622
See Also ... 623
EcsTaskDetails ... 624
Contents ... 624
See Also ... 626
EksCluster ... 627
Contents ... 627
See Also ... 628
EksClusterDetails ... 629
Contents ... 629
See Also ... 630
Evidence ... 631
Contents ... 631
See Also ... 631
FargateDetails ... 632
Contents ... 632
See Also ... 632
FilterCondition ... 634

Contents 634
See Also 634
FilterCriteria 636
Contents 636
See Also 636
FilterCriterion 637
Contents 637
See Also 637
Finding 638
Contents 638
See Also 641
FindingCriteria 642
Contents 642
See Also 642
FindingStatistics 643
Contents 643
See Also 644
FindingTypeStatistics 645
Contents 645
See Also 645
FlowLogsConfigurationResult 646
Contents 646
See Also 646
FreeTrialFeatureConfigurationResult 647
Contents 647
See Also 647
GeoLocation 648
Contents 648
See Also 648
GetMalwareScanResultDetails 649
Contents 649
See Also 650
HighestSeverityThreatDetails 652
Contents 652
See Also 652
HostPath 653

Contents ... 653
See Also ... 653
IamInstanceProfile ... 654
Contents ... 654
See Also ... 654
IamInstanceProfileV2 ... 655
Contents ... 655
See Also ... 655
ImpersonatedUser ... 656
Contents ... 656
See Also ... 656
IncrementalScanDetails ... 657
Contents ... 657
See Also ... 657
Indicator ... 658
Contents ... 658
See Also ... 659
InstanceDetails ... 660
Contents ... 660
See Also ... 662
Investigation ... 663
Contents ... 663
See Also ... 666
InvestigationMetadata ... 667
Contents ... 667
See Also ... 667
InvestigationSortCriteria ... 668
Contents ... 668
See Also ... 668
InvestigationSummary ... 669
Contents ... 669
See Also ... 671
Invitation ... 672
Contents ... 672
See Also ... 672
ItemDetails ... 674

Contents 674
See Also 674
ItemPath 676
Contents 676
See Also 676
KubernetesApiCallAction 677
Contents 677
See Also 679
KubernetesAuditLogsConfiguration 680
Contents 680
See Also 680
KubernetesAuditLogsConfigurationResult 681
Contents 681
See Also 681
KubernetesConfiguration 682
Contents 682
See Also 682
KubernetesConfigurationResult 683
Contents 683
See Also 683
KubernetesDataSourceFreeTrial 684
Contents 684
See Also 684
KubernetesDetails 685
Contents 685
See Also 685
KubernetesPermissionCheckedDetails 686
Contents 686
See Also 686
KubernetesRoleBindingDetails 688
Contents 688
See Also 689
KubernetesRoleDetails 690
Contents 690
See Also 690
KubernetesUserDetails 691

Contents ... 691
See Also ... 692
KubernetesWorkload ... 693
Contents ... 693
See Also ... 693
KubernetesWorkloadDetails ... 695
Contents ... 695
See Also ... 696
LambdaDetails ... 698
Contents ... 698
See Also ... 699
LineageObject ... 700
Contents ... 700
See Also ... 701
ListMalwareScansFilterCriteria ... 702
Contents ... 702
See Also ... 702
ListMalwareScansFilterCriterion ... 703
Contents ... 703
See Also ... 703
LocalIpDetails ... 704
Contents ... 704
See Also ... 704
LocalPortDetails ... 705
Contents ... 705
See Also ... 705
LoginAttribute ... 706
Contents ... 706
See Also ... 706
MalwareProtectionConfiguration ... 708
Contents ... 708
See Also ... 708
MalwareProtectionConfigurationResult ... 709
Contents ... 709
See Also ... 709
MalwareProtectionDataSourceFreeTrial ... 710

Contents 710
See Also 710
MalwareProtectionFindingsScanConfiguration 711
Contents 711
See Also 711
MalwareProtectionPlanActions 712
Contents 712
See Also 712
MalwareProtectionPlanStatusReason 713
Contents 713
See Also 713
MalwareProtectionPlanSummary 714
Contents 714
See Also 714
MalwareProtectionPlanTaggingAction 715
Contents 715
See Also 715
MalwareScan 716
Contents 716
See Also 717
MalwareScanDetails 719
Contents 719
See Also 720
Master 721
Contents 721
See Also 721
Member 723
Contents 723
See Also 724
MemberAdditionalConfiguration 725
Contents 725
See Also 725
MemberAdditionalConfigurationResult 726
Contents 726
See Also 727
MemberDataSourceConfiguration 728

Contents ... 728
See Also ... 728
MemberFeaturesConfiguration ... 730
Contents ... 730
See Also ... 730
MemberFeaturesConfigurationResult ... 732
Contents ... 732
See Also ... 733
ModelDetail ... 734
Contents ... 734
See Also ... 734
NetworkConnection ... 735
Contents ... 735
See Also ... 735
NetworkConnectionAction ... 736
Contents ... 736
See Also ... 737
NetworkEndpoint ... 738
Contents ... 738
See Also ... 739
NetworkGeoLocation ... 740
Contents ... 740
See Also ... 740
NetworkInterface ... 742
Contents ... 742
See Also ... 743
Observations ... 745
Contents ... 745
See Also ... 745
Organization ... 746
Contents ... 746
See Also ... 746
OrganizationAdditionalConfiguration ... 748
Contents ... 748
See Also ... 749
OrganizationAdditionalConfigurationResult ... 750

Contents ... 750
See Also ... 751
OrganizationDataSourceConfigurations ... 752
Contents ... 752
See Also ... 752
OrganizationDataSourceConfigurationsResult ... 753
Contents ... 753
See Also ... 753
OrganizationDetails ... 754
Contents ... 754
See Also ... 754
OrganizationEbsVolumes ... 755
Contents ... 755
See Also ... 755
OrganizationEbsVolumesResult ... 756
Contents ... 756
See Also ... 756
OrganizationFeatureConfiguration ... 757
Contents ... 757
See Also ... 758
OrganizationFeatureConfigurationResult ... 759
Contents ... 759
See Also ... 760
OrganizationFeatureStatistics ... 761
Contents ... 761
See Also ... 761
OrganizationFeatureStatisticsAdditionalConfiguration ... 763
Contents ... 763
See Also ... 763
OrganizationKubernetesAuditLogsConfiguration ... 764
Contents ... 764
See Also ... 764
OrganizationKubernetesAuditLogsConfigurationResult ... 765
Contents ... 765
See Also ... 765
OrganizationKubernetesConfiguration ... 766

Contents ... 766
See Also ... 766
OrganizationKubernetesConfigurationResult ... 767
Contents ... 767
See Also ... 767
OrganizationMalwareProtectionConfiguration ... 768
Contents ... 768
See Also ... 768
OrganizationMalwareProtectionConfigurationResult ... 769
Contents ... 769
See Also ... 769
OrganizationS3LogsConfiguration ... 770
Contents ... 770
See Also ... 770
OrganizationS3LogsConfigurationResult ... 771
Contents ... 771
See Also ... 771
OrganizationScanEc2InstanceWithFindings ... 772
Contents ... 772
See Also ... 772
OrganizationScanEc2InstanceWithFindingsResult ... 773
Contents ... 773
See Also ... 773
OrganizationStatistics ... 774
Contents ... 774
See Also ... 775
Owner ... 776
Contents ... 776
See Also ... 776
PermissionConfiguration ... 777
Contents ... 777
See Also ... 777
PortProbeAction ... 778
Contents ... 778
See Also ... 778
PortProbeDetail ... 779

Contents ... 779
See Also ... 779
PrivateIpAddressDetails ... 780
Contents ... 780
See Also ... 780
ProcessDetails ... 781
Contents ... 781
See Also ... 783
Product ... 784
Contents ... 784
See Also ... 784
ProductCode ... 785
Contents ... 785
See Also ... 785
PublicAccess ... 786
Contents ... 786
See Also ... 786
PublicAccessConfiguration ... 787
Contents ... 787
See Also ... 788
RdsDbInstanceDetails ... 789
Contents ... 789
See Also ... 790
RdsDbUserDetails ... 791
Contents ... 791
See Also ... 792
RdsLimitlessDbDetails ... 793
Contents ... 793
See Also ... 794
RdsLoginAttemptAction ... 795
Contents ... 795
See Also ... 795
RecoveryPoint ... 796
Contents ... 796
See Also ... 796
RecoveryPointDetails ... 797

Contents ... 797
See Also ... 797
RemoteAccountDetails ... 798
Contents ... 798
See Also ... 798
RemoteIpDetails ... 800
Contents ... 800
See Also ... 801
RemotePortDetails ... 802
Contents ... 802
See Also ... 802
Resource ... 803
Contents ... 803
See Also ... 806
ResourceData ... 807
Contents ... 807
See Also ... 810
ResourceDetails ... 811
Contents ... 811
See Also ... 811
ResourceStatistics ... 812
Contents ... 812
See Also ... 813
ResourceV2 ... 814
Contents ... 814
See Also ... 816
RuleDefinition ... 817
Contents ... 817
See Also ... 817
RuleDetail ... 818
Contents ... 818
See Also ... 821
RuleSummary ... 822
Contents ... 822
See Also ... 824
RuntimeContext ... 826

Contents ... 826
See Also ... 831
RuntimeDetails ... 832
Contents ... 832
See Also ... 832
S3Bucket ... 833
Contents ... 833
See Also ... 835
S3BucketDetail ... 836
Contents ... 836
See Also ... 837
S3LogsConfiguration ... 838
Contents ... 838
See Also ... 838
S3LogsConfigurationResult ... 839
Contents ... 839
See Also ... 839
S3Object ... 840
Contents ... 840
See Also ... 840
S3ObjectDetail ... 841
Contents ... 841
See Also ... 842
S3ObjectForSendObjectMalwareScan ... 843
Contents ... 843
See Also ... 843
Scan ... 845
Contents ... 845
See Also ... 848
ScanCondition ... 849
Contents ... 849
See Also ... 849
ScanConditionPair ... 850
Contents ... 850
See Also ... 850
ScanConfiguration ... 851

Contents 851
See Also 851
ScanConfigurationContinuousScanDetails 853
Contents 853
See Also 853
ScanConfigurationRecoveryPoint 854
Contents 854
See Also 854
ScanDetections 855
Contents 855
See Also 855
ScanEc2InstanceWithFindings 857
Contents 857
See Also 857
ScanEc2InstanceWithFindingsResult 858
Contents 858
See Also 858
ScanFilePath 859
Contents 859
See Also 859
ScannedItemCount 861
Contents 861
See Also 861
ScannedResource 862
Contents 862
See Also 863
ScannedResourceDetails 864
Contents 864
See Also 864
ScanResourceCriteria 865
Contents 865
See Also 865
ScanResultDetails 866
Contents 866
See Also 866
ScanResultThreat 867

Contents ... 867
See Also ... 868
ScanThreatName ... 869
Contents ... 869
See Also ... 869
SecurityContext ... 871
Contents ... 871
See Also ... 871
SecurityGroup ... 872
Contents ... 872
See Also ... 872
Sequence ... 873
Contents ... 873
See Also ... 874
Service ... 876
Contents ... 876
See Also ... 878
ServiceAdditionalInfo ... 880
Contents ... 880
See Also ... 880
Session ... 881
Contents ... 881
See Also ... 882
SeverityStatistics ... 883
Contents ... 883
See Also ... 883
Signal ... 884
Contents ... 884
See Also ... 887
SortCriteria ... 888
Contents ... 888
See Also ... 888
StartMalwareScanConfiguration ... 889
Contents ... 889
See Also ... 889
Tag ... 891

Contents ... 891
See Also ... 891
Threat ... 892
Contents ... 892
See Also ... 893
ThreatDetectedByName ... 894
Contents ... 894
See Also ... 894
ThreatIntelligenceDetail ... 896
Contents ... 896
See Also ... 896
ThreatsDetectedItemCount ... 897
Contents ... 897
See Also ... 897
Total ... 898
Contents ... 898
See Also ... 898
TriggerDetails ... 899
Contents ... 899
See Also ... 899
UnprocessedAccount ... 901
Contents ... 901
See Also ... 901
UnprocessedDataSourcesResult ... 902
Contents ... 902
See Also ... 902
UpdateProtectedResource ... 903
Contents ... 903
See Also ... 903
UpdateS3BucketResource ... 904
Contents ... 904
See Also ... 904
UsageAccountResult ... 905
Contents ... 905
See Also ... 905
UsageCriteria ... 906

Contents ... 906
See Also ... 907
UsageDataSourceResult ... 908
Contents ... 908
See Also ... 908
UsageFeatureResult ... 909
Contents ... 909
See Also ... 909
UsageResourceResult ... 910
Contents ... 910
See Also ... 910
UsageStatistics ... 911
Contents ... 911
See Also ... 912
UsageTopAccountResult ... 913
Contents ... 913
See Also ... 913
UsageTopAccountsResult ... 914
Contents ... 914
See Also ... 914
User ... 916
Contents ... 916
See Also ... 917
Volume ... 918
Contents ... 918
See Also ... 918
VolumeDetail ... 919
Contents ... 919
See Also ... 920
VolumeMount ... 921
Contents ... 921
See Also ... 921
VpcConfig ... 922
Contents ... 922
See Also ... 922
Common Parameters ... 923

Common Error Types 926

Welcome

Amazon GuardDuty is a continuous security monitoring service that analyzes and processes the following foundational data sources - VPC flow logs, AWS CloudTrail management event logs, CloudTrail S3 data event logs, EKS audit logs, DNS logs, Amazon EBS volume data, runtime activity belonging to container workloads, such as Amazon EKS, Amazon ECS (including AWS Fargate), and Amazon EC2 instances. It uses threat intelligence feeds, such as lists of malicious IPs and domains, and machine learning to identify unexpected, potentially unauthorized, and malicious activity within your AWS environment. This can include issues like escalations of privileges, uses of exposed credentials, or communication with malicious IPs, domains, or presence of malware on your Amazon EC2 instances and container workloads. For example, GuardDuty can detect compromised EC2 instances and container workloads serving malware, or mining bitcoin.

GuardDuty also monitors AWS account access behavior for signs of compromise, such as unauthorized infrastructure deployments like EC2 instances deployed in a Region that has never been used, or unusual API calls like a password policy change to reduce password strength.

GuardDuty informs you about the status of your AWS environment by producing security findings that you can view in the GuardDuty console or through Amazon EventBridge. For more information, see the *Amazon GuardDuty User Guide* .

This document was last published on October 30, 2026.

Actions

The following actions are supported:

- AcceptAdministratorInvitation
- AcceptInvitation
- ArchiveFindings
- CreateCustomDetectionRuleAssociation
- CreateCustomDetectionRuleOrgConfiguration
- CreateDetector
- CreateFilter
- CreateInvestigation
- CreateIPSet
- CreateMalwareProtectionPlan
- CreateMembers
- CreatePublishingDestination
- CreateSampleFindings
- CreateThreatEntitySet
- CreateThreatIntelSet
- CreateTrustedEntitySet
- DeclineInvitations
- DeleteCustomDetectionRuleAssociation
- DeleteCustomDetectionRuleOrgConfiguration
- DeleteDetector
- DeleteFilter
- DeleteInvitations
- DeleteIPSet
- DeleteMalwareProtectionPlan
- DeleteMembers
- DeletePublishingDestination
- DeleteThreatEntitySet

- DeleteThreatIntelSet
- DeleteTrustedEntitySet
- DescribeMalwareScans
- DescribeOrganizationConfiguration
- DescribePublishingDestination
- DisableOrganizationAdminAccount
- DisassociateFromAdministratorAccount
- DisassociateFromMasterAccount
- DisassociateMembers
- EnableOrganizationAdminAccount
- GetAdministratorAccount
- GetCoverageStatistics
- GetCustomDetectionRule
- GetCustomDetectionRuleAssociation
- GetCustomDetectionRuleOrgConfiguration
- GetDetector
- GetFilter
- GetFindings
- GetFindingsStatistics
- GetInvestigation
- GetInvitationsCount
- GetIPSet
- GetMalwareProtectionPlan
- GetMalwareScan
- GetMalwareScanSettings
- GetMasterAccount
- GetMemberDetectors
- GetMembers
- GetOrganizationStatistics
- GetRemainingFreeTrialDays

- GetThreatEntitySet
- GetThreatIntelSet
- GetTrustedEntitySet
- GetUsageStatistics
- InviteMembers
- ListCoverage
- ListCustomDetectionRuleAssociations
- ListCustomDetectionRuleOrgConfigurations
- ListCustomDetectionRules
- ListDetectors
- ListFilters
- ListFindings
- ListInvestigations
- ListInvitations
- ListIPSets
- ListMalwareProtectionPlans
- ListMalwareScans
- ListMembers
- ListOrganizationAdminAccounts
- ListPublishingDestinations
- ListTagsForResource
- ListThreatEntitySets
- ListThreatIntelSets
- ListTrustedEntitySets
- SendObjectMalwareScan
- StartMalwareScan
- StartMonitoringMembers
- StopMonitoringMembers
- TagResource
- UnarchiveFindings

- UntagResource
- UpdateCustomDetectionRuleAssociation
- UpdateCustomDetectionRuleOrgConfiguration
- UpdateDetector
- UpdateFilter
- UpdateFindingsFeedback
- UpdateIPSet
- UpdateMalwareProtectionPlan
- UpdateMalwareScanSettings
- UpdateMemberDetectors
- UpdateOrganizationConfiguration
- UpdatePublishingDestination
- UpdateThreatEntitySet
- UpdateThreatIntelSet
- UpdateTrustedEntitySet

AcceptAdministratorInvitation

Accepts the invitation to be a member account and get monitored by a GuardDuty administrator account that sent the invitation.

Request Syntax

```
POST /detector/DetectorId/administrator HTTP/1.1
Content-type: application/json

{
   "administratorId": "string",
   "invitationId": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty member account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

administratorId

The account ID of the GuardDuty administrator account whose invitation you're accepting.

Type: String

Required: Yes

invitationId

The value that is used to validate the administrator account to the member account.

Type: String

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

AcceptInvitation

This action has been deprecated.

Accepts the invitation to be monitored by a GuardDuty administrator account.

Request Syntax

```
POST /detector/DetectorId/master HTTP/1.1
Content-type: application/json

{
   "invitationId": "string",
   "masterId": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty member account.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

invitationId

The value that is used to validate the administrator account to the member account.

Type: String

Required: Yes

masterId

The account ID of the GuardDuty administrator account whose invitation you're accepting.

Type: String

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ArchiveFindings

Archives GuardDuty findings that are specified by the list of finding IDs.

> **Note**
>
> Only the administrator account can archive findings. Member accounts don't have permission to archive findings from their accounts.

Request Syntax

```
POST /detector/DetectorId/findings/archive HTTP/1.1
Content-type: application/json

{
   "findingIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The ID of the detector that specifies the GuardDuty service whose findings you want to archive.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

findingIds

The IDs of the findings that you want to archive.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateCustomDetectionRuleAssociation

Enables a custom detection rule for your account by creating an association. You specify the rule and the mode in which it operates.

Request Syntax

```
POST /custom-detection-rule/association HTTP/1.1
Content-type: application/json

{
   "clientToken": "string",
   "mode": "string",
   "ruleId": "string",
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

clientToken

A unique, case-sensitive identifier to ensure that the operation completes no more than one time. Maximum 64 characters.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

mode

The rule execution mode. Valid values: `LIVE` | `DRY_RUN`.

Type: String

Valid Values: `LIVE | DRY_RUN`

Required: Yes

ruleId

The unique identifier for the custom detection rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Required: Yes

tags

The tags to be added to the new custom detection rule association resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "ruleAssociation": {
      "accountId": "string",
      "arn": "string",
      "associationId": "string",
```

```
      "createdAt": number,
      "expiresAt": number,
      "mode": "string",
      "ruleId": "string",
      "updatedAt": number
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

ruleAssociation

The details of the newly created custom detection rule association.

Type: AssociationDetail object

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

ConflictException

A request conflict exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 409

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

ResourceNotFoundException

The requested resource can't be found.

Message

The error message.

Type

The error type.

HTTP Status Code: 404

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateCustomDetectionRuleOrgConfiguration

Creates an organization-level configuration that enables a custom detection rule across your organization. This operation is available only to the delegated administrator account.

Request Syntax

```
POST /custom-detection-rule/org-configuration HTTP/1.1
Content-type: application/json

{
   "clientToken": "string",
   "excludeAccountIds": [ "string" ],
   "includeAccountIds": [ "string" ],
   "mode": "string",
   "ruleId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

clientToken

A unique, case-sensitive identifier to ensure that the operation completes no more than one time.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

excludeAccountIds

The account IDs to exclude from the organization configuration. Mutually exclusive with `IncludeAccountIds`.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50000 items.

Length Constraints: Fixed length of 12.

Required: No

includeAccountIds

The account IDs to include in the organization configuration. Mutually exclusive with `ExcludeAccountIds`.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50000 items.

Length Constraints: Fixed length of 12.

Required: No

mode

The execution mode of the organization configuration. Valid values: `LIVE` | `DRY_RUN`.

Type: String

Valid Values: `LIVE | DRY_RUN`

Required: Yes

ruleId

The unique identifier for the custom detection rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

ConflictException

A request conflict exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 409

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

ResourceNotFoundException

The requested resource can't be found.

Message

The error message.

Type

The error type.

HTTP Status Code: 404

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3

- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateDetector

Creates a single GuardDuty detector. A detector is a resource that represents the GuardDuty service. To start using GuardDuty, you must create a detector in each Region where you enable the service. You can have only one detector per account per Region. All data sources are enabled in a new detector by default.

- When you don't specify any `features`, with an exception to `RUNTIME_MONITORING`, all the optional features are enabled by default.
- When you specify some of the `features`, any feature that is not specified in the API call gets enabled by default, with an exception to `RUNTIME_MONITORING`.

Specifying both EKS Runtime Monitoring (`EKS_RUNTIME_MONITORING`) and Runtime Monitoring (`RUNTIME_MONITORING`) will cause an error. You can add only one of these two features because Runtime Monitoring already includes the threat detection for Amazon EKS resources. For more information, see Runtime Monitoring.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see Regions and endpoints.

Request Syntax

```
POST /detector HTTP/1.1
Content-type: application/json

{
   "clientToken": "string",
   "dataSources": {
      "kubernetes": {
         "auditLogs": {
            "enable": boolean
         }
      },
      "malwareProtection": {
         "scanEc2InstanceWithFindings": {
            "ebsVolumes": boolean
         }
      },
      "s3Logs": {
```

```
         "enable": boolean
      }
   },
   "enable": boolean,
   "features": [
      {
         "additionalConfiguration": [
            {
               "name": "string",
               "status": "string"
            }
         ],
         "name": "string",
         "status": "string"
      }
   ],
   "findingPublishingFrequency": "string",
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

clientToken

The idempotency token for the create request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

dataSources

This parameter has been deprecated.

Describes which data sources will be enabled for the detector.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see Regions and endpoints.

Type: DataSourceConfigurations object

Required: No

enable

A Boolean value that specifies whether the detector is to be enabled.

Type: Boolean

Required: Yes

features

A list of features that will be configured for the detector.

Type: Array of DetectorFeatureConfiguration objects

Required: No

findingPublishingFrequency

A value that specifies how frequently updated findings are exported.

Type: String

Valid Values: `FIFTEEN_MINUTES | ONE_HOUR | SIX_HOURS`

Required: No

tags

The tags to be added to a new detector resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "detectorId": "string",
   "unprocessedDataSources": {
      "malwareProtection": {
         "scanEc2InstanceWithFindings": {
            "ebsVolumes": {
               "reason": "string",
               "status": "string"
            }
         },
         "serviceRole": "string"
      }
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

detectorId

The unique ID of the created detector.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

unprocessedDataSources

Specifies the data sources that couldn't be enabled when GuardDuty was enabled for the first time.

Type: UnprocessedDataSourcesResult object

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateFilter

Creates a filter using the specified finding criteria. The maximum number of saved filters per AWS account per Region is 100. For more information, see Quotas for GuardDuty.

Request Syntax

```
POST /detector/DetectorId/filter HTTP/1.1
Content-type: application/json

{
   "action": "string",
   "clientToken": "string",
   "description": "string",
   "findingCriteria": {
      "criterion": {
         "string" : {
            "eq": [ "string" ],
            "equals": [ "string" ],
            "greaterThan": number,
            "greaterThanOrEqual": number,
            "gt": number,
            "gte": number,
            "lessThan": number,
            "lessThanOrEqual": number,
            "lt": number,
            "lte": number,
            "matches": [ "string" ],
            "neq": [ "string" ],
            "notEquals": [ "string" ],
            "notMatches": [ "string" ]
         }
      }
   },
   "name": "string",
   "rank": number,
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The detector ID associated with the GuardDuty account for which you want to create a filter.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

action

Specifies the action that is to be applied to the findings that match the filter.

Default: NOOP

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `NOOP | ARCHIVE`

Required: No

clientToken

The idempotency token for the create request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

description

The description of the filter. Valid characters include alphanumeric characters, and special characters such as hyphen, period, colon, underscore, parentheses ({ }, [ ], and ( )), forward slash, horizontal tab, vertical tab, newline, form feed, return, and whitespace.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 512.

Required: No

findingCriteria

Represents the criteria to be used in the filter for querying findings. The following fields are available for filtering:

- accountId
- arn
- associatedAttackSequenceArn
- confidence
- createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- id
- partition
- region
- resource.accessKeyDetails.accessKeyId
- resource.accessKeyDetails.principalId
- resource.accessKeyDetails.userIdentity.accessKeyId
- resource.accessKeyDetails.userIdentity.accountId
- resource.accessKeyDetails.userIdentity.arn
- resource.accessKeyDetails.userIdentity.principalId
- resource.accessKeyDetails.userIdentity.sessionContext.attributes.mfaAuthenticated
- resource.accessKeyDetails.userIdentity.sessionContext.ec2RoleDelivery
- resource.accessKeyDetails.userIdentity.sessionContext.invokedBy

- resource.accessKeyDetails.userIdentity.sessionContext.sessionIssuer.accountId
- resource.accessKeyDetails.userIdentity.sessionContext.sessionIssuer.arn
- resource.accessKeyDetails.userIdentity.sessionContext.sessionIssuer.principalId
- resource.accessKeyDetails.userIdentity.sessionContext.sessionIssuer.type
- resource.accessKeyDetails.userIdentity.sessionContext.sessionIssuer.userName
- resource.accessKeyDetails.userIdentity.sessionContext.sourceIdentity
- resource.accessKeyDetails.userIdentity.sessionContext.webIdFederationData.attributes
- resource.accessKeyDetails.userIdentity.sessionContext.webIdFederationData.federatedProvider
- resource.accessKeyDetails.userIdentity.type
- resource.accessKeyDetails.userIdentity.userName
- resource.accessKeyDetails.userName
- resource.accessKeyDetails.userType
- resource.bedrockGuardrailDetails.guardrailArn
- resource.bedrockGuardrailDetails.guardrailVersion
- resource.containerDetails.containerRuntime
- resource.containerDetails.id
- resource.containerDetails.image
- resource.containerDetails.imagePrefix
- resource.containerDetails.name
- resource.containerDetails.securityContext.allowPrivilegeEscalation
- resource.containerDetails.securityContext.privileged
- resource.containerDetails.volumeMounts.mountPath
- resource.containerDetails.volumeMounts.name
- resource.ebsSnapshotDetails.snapshotArn
- resource.ebsVolumeDetails.scannedVolumeDetails.deviceName
- resource.ebsVolumeDetails.scannedVolumeDetails.encryptionType
- resource.ebsVolumeDetails.scannedVolumeDetails.kmsKeyArn
- resource.ebsVolumeDetails.scannedVolumeDetails.snapshotArn
- resource.ebsVolumeDetails.scannedVolumeDetails.volumeArn
- resource.ebsVolumeDetails.scannedVolumeDetails.volumeSizeInGB

- resource.ebsVolumeDetails.scannedVolumeDetails.volumeType
- resource.ebsVolumeDetails.skippedVolumeDetails.deviceName
- resource.ebsVolumeDetails.skippedVolumeDetails.encryptionType
- resource.ebsVolumeDetails.skippedVolumeDetails.kmsKeyArn
- resource.ebsVolumeDetails.skippedVolumeDetails.snapshotArn
- resource.ebsVolumeDetails.skippedVolumeDetails.volumeArn
- resource.ebsVolumeDetails.skippedVolumeDetails.volumeSizeInGB
- resource.ebsVolumeDetails.skippedVolumeDetails.volumeType
- resource.ec2ImageDetails.imageArn
- resource.ecsClusterDetails.activeServicesCount
- resource.ecsClusterDetails.arn
- resource.ecsClusterDetails.name
- resource.ecsClusterDetails.registeredContainerInstancesCount
- resource.ecsClusterDetails.runningTasksCount
- resource.ecsClusterDetails.status
- resource.ecsClusterDetails.tags.key
- resource.ecsClusterDetails.tags.value
- resource.ecsClusterDetails.taskDetails.arn
- resource.ecsClusterDetails.taskDetails.containers.containerRuntime
- resource.ecsClusterDetails.taskDetails.containers.id
- resource.ecsClusterDetails.taskDetails.containers.image
- resource.ecsClusterDetails.taskDetails.containers.imagePrefix
- resource.ecsClusterDetails.taskDetails.containers.name
- resource.ecsClusterDetails.taskDetails.containers.securityContext.allowPrivilegeEscalation
- resource.ecsClusterDetails.taskDetails.containers.securityContext.privileged
- resource.ecsClusterDetails.taskDetails.containers.volumeMounts.mountPath
- resource.ecsClusterDetails.taskDetails.containers.volumeMounts.name
- resource.ecsClusterDetails.taskDetails.createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- resource.ecsClusterDetails.taskDetails.definitionArn

- resource.ecsClusterDetails.taskDetails.group
- resource.ecsClusterDetails.taskDetails.launchType
- resource.ecsClusterDetails.taskDetails.startedAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- resource.ecsClusterDetails.taskDetails.startedBy
- resource.ecsClusterDetails.taskDetails.tags.key
- resource.ecsClusterDetails.taskDetails.tags.value
- resource.ecsClusterDetails.taskDetails.version
- resource.ecsClusterDetails.taskDetails.volumes.hostPath.path
- resource.ecsClusterDetails.taskDetails.volumes.name
- resource.eksClusterDetails.arn
- resource.eksClusterDetails.createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- resource.eksClusterDetails.name
- resource.eksClusterDetails.status
- resource.eksClusterDetails.tags.key
- resource.eksClusterDetails.tags.value
- resource.eksClusterDetails.vpcId
- resource.instanceDetails.availabilityZone
- resource.instanceDetails.iamInstanceProfile.arn
- resource.instanceDetails.iamInstanceProfile.id
- resource.instanceDetails.imageDescription
- resource.instanceDetails.imageId
- resource.instanceDetails.instanceId
- resource.instanceDetails.instanceState
- resource.instanceDetails.instanceType
- resource.instanceDetails.launchTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- resource.instanceDetails.networkInterfaces.ipv6Addresses

- resource.instanceDetails.networkInterfaces.networkInterfaceId
- resource.instanceDetails.networkInterfaces.privateDnsName
- resource.instanceDetails.networkInterfaces.privateIpAddress
- resource.instanceDetails.networkInterfaces.privateIpAddresses.privateDnsName
- resource.instanceDetails.networkInterfaces.privateIpAddresses.privateIpAddress
- resource.instanceDetails.networkInterfaces.publicDnsName
- resource.instanceDetails.networkInterfaces.publicIp
- resource.instanceDetails.networkInterfaces.securityGroups.groupId
- resource.instanceDetails.networkInterfaces.securityGroups.groupName
- resource.instanceDetails.networkInterfaces.subnetId
- resource.instanceDetails.networkInterfaces.vpcId
- resource.instanceDetails.outpostArn
- resource.instanceDetails.platform
- resource.instanceDetails.productCodes.productCodeId
- resource.instanceDetails.productCodes.productCodeType
- resource.instanceDetails.tags.key
- resource.instanceDetails.tags.value
- resource.kubernetesDetails.kubernetesUserDetails.groups
- resource.kubernetesDetails.kubernetesUserDetails.impersonatedUser.groups
- resource.kubernetesDetails.kubernetesUserDetails.impersonatedUser.username
- resource.kubernetesDetails.kubernetesUserDetails.sessionName
- resource.kubernetesDetails.kubernetesUserDetails.uid
- resource.kubernetesDetails.kubernetesUserDetails.username
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.containerRuntime
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.id
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.imagePrefix
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.name
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.allowPrivilegeEsca
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.privileged

- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.volumeMounts.mountPath
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.volumeMounts.name
- resource.kubernetesDetails.kubernetesWorkloadDetails.hostIpc
- resource.kubernetesDetails.kubernetesWorkloadDetails.hostNetwork
- resource.kubernetesDetails.kubernetesWorkloadDetails.hostPid
- resource.kubernetesDetails.kubernetesWorkloadDetails.name
- resource.kubernetesDetails.kubernetesWorkloadDetails.namespace
- resource.kubernetesDetails.kubernetesWorkloadDetails.serviceAccountName
- resource.kubernetesDetails.kubernetesWorkloadDetails.type
- resource.kubernetesDetails.kubernetesWorkloadDetails.uid
- resource.kubernetesDetails.kubernetesWorkloadDetails.volumes.hostPath.path
- resource.kubernetesDetails.kubernetesWorkloadDetails.volumes.name
- resource.lambdaDetails.description
- resource.lambdaDetails.functionArn
- resource.lambdaDetails.functionName
- resource.lambdaDetails.functionVersion
- resource.lambdaDetails.lastModifiedAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- resource.lambdaDetails.revisionId
- resource.lambdaDetails.role
- resource.lambdaDetails.tags.key
- resource.lambdaDetails.tags.value
- resource.lambdaDetails.vpcConfig.securityGroups.groupId
- resource.lambdaDetails.vpcConfig.securityGroups.groupName
- resource.lambdaDetails.vpcConfig.subnetIds
- resource.lambdaDetails.vpcConfig.vpcId
- resource.rdsDbInstanceDetails.dbClusterIdentifier
- resource.rdsDbInstanceDetails.dbInstanceArn
- resource.rdsDbInstanceDetails.dbInstanceIdentifier
- resource.rdsDbInstanceDetails.dbSecurityGroups.name

- resource.rdsDbInstanceDetails.dbSecurityGroups.status
- resource.rdsDbInstanceDetails.dbiResourceId
- resource.rdsDbInstanceDetails.engine
- resource.rdsDbInstanceDetails.engineVersion
- resource.rdsDbInstanceDetails.iamDatabaseAuthenticationEnabled
- resource.rdsDbInstanceDetails.publiclyAccessible
- resource.rdsDbInstanceDetails.vpcId
- resource.rdsDbInstanceDetails.vpcSecurityGroups.status
- resource.rdsDbInstanceDetails.vpcSecurityGroups.vpcSecurityGroupId
- resource.rdsDbUserDetails.application
- resource.rdsDbUserDetails.authMethod
- resource.rdsDbUserDetails.database
- resource.rdsDbUserDetails.ssl
- resource.rdsDbUserDetails.user
- resource.rdsLimitlessDbDetails.dbClusterIdentifier
- resource.rdsLimitlessDbDetails.dbShardGroupArn
- resource.rdsLimitlessDbDetails.dbShardGroupIdentifier
- resource.rdsLimitlessDbDetails.dbShardGroupResourceId
- resource.rdsLimitlessDbDetails.engine
- resource.rdsLimitlessDbDetails.engineVersion
- resource.rdsLimitlessDbDetails.tags.key
- resource.rdsLimitlessDbDetails.tags.value
- resource.recoveryPointDetails.backupVaultName
- resource.recoveryPointDetails.recoveryPointArn
- resource.resourceType
- resource.s3BucketDetails.arn
- resource.s3BucketDetails.createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- resource.s3BucketDetails.defaultServerSideEncryption.encryptionType
- resource.s3BucketDetails.defaultServerSideEncryption.kmsMasterKeyArn

- resource.s3BucketDetails.name
- resource.s3BucketDetails.owner.id
- resource.s3BucketDetails.publicAccess.effectivePermission
- resource.s3BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublic
- resource.s3BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublic
- resource.s3BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublic
- resource.s3BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublic
- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.accessContro
- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.accessContro
- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicA
- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicA
- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicA
- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicA
- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.bucketPolicy
- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.bucketPolicy
- resource.s3BucketDetails.s3ObjectDetails.eTag
- resource.s3BucketDetails.s3ObjectDetails.hash
- resource.s3BucketDetails.s3ObjectDetails.key
- resource.s3BucketDetails.s3ObjectDetails.objectArn
- resource.s3BucketDetails.s3ObjectDetails.versionId
- resource.s3BucketDetails.tags.key
- resource.s3BucketDetails.tags.value
- resource.s3BucketDetails.type
- schemaVersion
- service.action.actionType
- service.action.awsApiCallAction.api
- service.action.awsApiCallAction.callerType
- service.action.awsApiCallAction.domainDetails.domain
- service.action.awsApiCallAction.errorCode
- service.action.awsApiCallAction.remoteAccountDetails.accountId

- service.action.awsApiCallAction.remoteAccountDetails.affiliated
- service.action.awsApiCallAction.remoteAccountDetails.awsServiceName
- service.action.awsApiCallAction.remoteIpDetails.city.cityName
- service.action.awsApiCallAction.remoteIpDetails.country.countryCode
- service.action.awsApiCallAction.remoteIpDetails.country.countryName
- service.action.awsApiCallAction.remoteIpDetails.geoLocation.lat
- service.action.awsApiCallAction.remoteIpDetails.geoLocation.lon
- service.action.awsApiCallAction.remoteIpDetails.ipAddressV4
- service.action.awsApiCallAction.remoteIpDetails.ipAddressV6
- service.action.awsApiCallAction.remoteIpDetails.organization.asn
- service.action.awsApiCallAction.remoteIpDetails.organization.asnOrg
- service.action.awsApiCallAction.remoteIpDetails.organization.isp
- service.action.awsApiCallAction.remoteIpDetails.organization.org
- service.action.awsApiCallAction.serviceName
- service.action.awsApiCallAction.userAgent
- service.action.dnsRequestAction.blocked
- service.action.dnsRequestAction.domain
- service.action.dnsRequestAction.domainWithSuffix
- service.action.dnsRequestAction.protocol
- service.action.dnsRequestAction.vpcOwnerAccountId
- service.action.kubernetesApiCallAction.namespace
- service.action.kubernetesApiCallAction.parameters
- service.action.kubernetesApiCallAction.remoteIpDetails.city.cityName
- service.action.kubernetesApiCallAction.remoteIpDetails.country.countryCode
- service.action.kubernetesApiCallAction.remoteIpDetails.country.countryName
- service.action.kubernetesApiCallAction.remoteIpDetails.geoLocation.lat
- service.action.kubernetesApiCallAction.remoteIpDetails.geoLocation.lon
- service.action.kubernetesApiCallAction.remoteIpDetails.ipAddressV4
- service.action.kubernetesApiCallAction.remoteIpDetails.ipAddressV6
- service.action.kubernetesApiCallAction.remoteIpDetails.organization.asn

- service.action.kubernetesApiCallAction.remoteIpDetails.organization.asnOrg
- service.action.kubernetesApiCallAction.remoteIpDetails.organization.isp
- service.action.kubernetesApiCallAction.remoteIpDetails.organization.org
- service.action.kubernetesApiCallAction.requestUri
- service.action.kubernetesApiCallAction.resource
- service.action.kubernetesApiCallAction.resourceName
- service.action.kubernetesApiCallAction.sourceIPs
- service.action.kubernetesApiCallAction.statusCode
- service.action.kubernetesApiCallAction.subresource
- service.action.kubernetesApiCallAction.userAgent
- service.action.kubernetesApiCallAction.verb
- service.action.kubernetesPermissionCheckedDetails.allowed
- service.action.kubernetesPermissionCheckedDetails.namespace
- service.action.kubernetesPermissionCheckedDetails.resource
- service.action.kubernetesPermissionCheckedDetails.verb
- service.action.kubernetesRoleBindingDetails.kind
- service.action.kubernetesRoleBindingDetails.name
- service.action.kubernetesRoleBindingDetails.roleRefKind
- service.action.kubernetesRoleBindingDetails.roleRefName
- service.action.kubernetesRoleBindingDetails.uid
- service.action.kubernetesRoleDetails.kind
- service.action.kubernetesRoleDetails.name
- service.action.kubernetesRoleDetails.uid
- service.action.networkConnectionAction.blocked
- service.action.networkConnectionAction.connectionDirection
- service.action.networkConnectionAction.localIpDetails.ipAddressV4
- service.action.networkConnectionAction.localIpDetails.ipAddressV6
- service.action.networkConnectionAction.localNetworkInterface
- service.action.networkConnectionAction.localPortDetails.port
- service.action.networkConnectionAction.localPortDetails.portName

- service.action.networkConnectionAction.protocol
- service.action.networkConnectionAction.remoteIpDetails.city.cityName
- service.action.networkConnectionAction.remoteIpDetails.country.countryCode
- service.action.networkConnectionAction.remoteIpDetails.country.countryName
- service.action.networkConnectionAction.remoteIpDetails.geoLocation.lat
- service.action.networkConnectionAction.remoteIpDetails.geoLocation.lon
- service.action.networkConnectionAction.remoteIpDetails.ipAddressV4
- service.action.networkConnectionAction.remoteIpDetails.ipAddressV6
- service.action.networkConnectionAction.remoteIpDetails.organization.asn
- service.action.networkConnectionAction.remoteIpDetails.organization.asnOrg
- service.action.networkConnectionAction.remoteIpDetails.organization.isp
- service.action.networkConnectionAction.remoteIpDetails.organization.org
- service.action.networkConnectionAction.remotePortDetails.port
- service.action.networkConnectionAction.remotePortDetails.portName
- service.action.portProbeAction.blocked
- service.action.portProbeAction.portProbeDetails.localIpDetails.ipAddressV4
- service.action.portProbeAction.portProbeDetails.localIpDetails.ipAddressV6
- service.action.portProbeAction.portProbeDetails.localPortDetails.port
- service.action.portProbeAction.portProbeDetails.localPortDetails.portName
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.city.cityName
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.country.countryCode
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.country.countryName
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.geoLocation.lat
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.geoLocation.lon
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.ipAddressV4
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.ipAddressV6
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.organization.asn
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.organization.asnOrg
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.organization.isp
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.organization.org

- service.action.rdsLoginAttemptAction.loginAttributes.application
- service.action.rdsLoginAttemptAction.loginAttributes.failedLoginAttempts
- service.action.rdsLoginAttemptAction.loginAttributes.successfulLoginAttempts
- service.action.rdsLoginAttemptAction.loginAttributes.user
- service.action.rdsLoginAttemptAction.remoteIpDetails.city.cityName
- service.action.rdsLoginAttemptAction.remoteIpDetails.country.countryCode
- service.action.rdsLoginAttemptAction.remoteIpDetails.country.countryName
- service.action.rdsLoginAttemptAction.remoteIpDetails.geoLocation.lat
- service.action.rdsLoginAttemptAction.remoteIpDetails.geoLocation.lon
- service.action.rdsLoginAttemptAction.remoteIpDetails.ipAddressV4
- service.action.rdsLoginAttemptAction.remoteIpDetails.ipAddressV6
- service.action.rdsLoginAttemptAction.remoteIpDetails.organization.asn
- service.action.rdsLoginAttemptAction.remoteIpDetails.organization.asnOrg
- service.action.rdsLoginAttemptAction.remoteIpDetails.organization.isp
- service.action.rdsLoginAttemptAction.remoteIpDetails.organization.org
- service.additionalInfo.agentDetails.agentId
- service.additionalInfo.agentDetails.agentVersion
- service.additionalInfo.anomalies.anomalousAPIs
- service.additionalInfo.authenticationMethod
- service.additionalInfo.averagePacketSizeIn
- service.additionalInfo.averagePacketSizeOut
- service.additionalInfo.context
- service.additionalInfo.domain
- service.additionalInfo.inBytes
- service.additionalInfo.localNetworkInterfaceOwner
- service.additionalInfo.localPort
- service.additionalInfo.outBytes
- service.additionalInfo.packetsIn
- service.additionalInfo.packetsOut
- service.additionalInfo.policyArn

- service.additionalInfo.policyName
- service.additionalInfo.remotePort
- service.additionalInfo.sample
- service.additionalInfo.scannedPort
- service.additionalInfo.threatFileSha256
- service.additionalInfo.threatListName
- service.additionalInfo.threatName
- service.additionalInfo.totalBytesIn
- service.additionalInfo.totalBytesOut
- service.additionalInfo.type
- service.additionalInfo.unusual.asnOrg
- service.additionalInfo.unusual.port
- service.additionalInfo.unusualProtocol
- service.additionalInfo.userAgent.fullUserAgent
- service.additionalInfo.userAgent.userAgentCategory
- service.additionalInfo.value
- service.additionalInfo.vpcOwnerAccountId
- service.archived
- service.count
- service.detection.sequence.actors.id
- service.detection.sequence.actors.process.name
- service.detection.sequence.actors.process.path
- service.detection.sequence.actors.process.sha256
- service.detection.sequence.actors.session.createdTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.detection.sequence.actors.session.issuer
- service.detection.sequence.actors.session.mfaStatus
- service.detection.sequence.actors.session.uid
- service.detection.sequence.actors.user.account.account
- service.detection.sequence.actors.user.account.uid

- service.detection.sequence.actors.user.credentialUid
- service.detection.sequence.actors.user.name
- service.detection.sequence.actors.user.type
- service.detection.sequence.actors.user.uid
- service.detection.sequence.additionalSequenceTypes
- service.detection.sequence.description
- service.detection.sequence.endpoints.autonomousSystem.name
- service.detection.sequence.endpoints.autonomousSystem.number
- service.detection.sequence.endpoints.connection.direction
- service.detection.sequence.endpoints.domain
- service.detection.sequence.endpoints.id
- service.detection.sequence.endpoints.ip
- service.detection.sequence.endpoints.location.city
- service.detection.sequence.endpoints.location.country
- service.detection.sequence.endpoints.location.lat
- service.detection.sequence.endpoints.location.lon
- service.detection.sequence.endpoints.port
- service.detection.sequence.resources.accountId
- service.detection.sequence.resources.cloudPartition
- service.detection.sequence.resources.data.accessKey.principalId
- service.detection.sequence.resources.data.accessKey.userName
- service.detection.sequence.resources.data.accessKey.userType
- service.detection.sequence.resources.data.autoscalingAutoScalingGroup.ec2InstanceUids
- service.detection.sequence.resources.data.cloudformationStack.ec2InstanceUids
- service.detection.sequence.resources.data.container.image
- service.detection.sequence.resources.data.container.imageUid
- service.detection.sequence.resources.data.ec2Image.ec2InstanceUids
- service.detection.sequence.resources.data.ec2Instance.availabilityZone
- service.detection.sequence.resources.data.ec2Instance.ec2NetworkInterfaceUids
- service.detection.sequence.resources.data.ec2Instance.iamInstanceProfile.arn

- service.detection.sequence.resources.data.ec2Instance.iamInstanceProfile.id
- service.detection.sequence.resources.data.ec2Instance.imageDescription
- service.detection.sequence.resources.data.ec2Instance.instanceState
- service.detection.sequence.resources.data.ec2Instance.instanceType
- service.detection.sequence.resources.data.ec2Instance.outpostArn
- service.detection.sequence.resources.data.ec2Instance.platform
- service.detection.sequence.resources.data.ec2Instance.productCodes.productCodeId
- service.detection.sequence.resources.data.ec2Instance.productCodes.productCodeType
- service.detection.sequence.resources.data.ec2LaunchTemplate.ec2InstanceUids
- service.detection.sequence.resources.data.ec2LaunchTemplate.version
- service.detection.sequence.resources.data.ec2NetworkInterface.ipv6Addresses
- service.detection.sequence.resources.data.ec2NetworkInterface.privateIpAddresses.privateDnsName
- service.detection.sequence.resources.data.ec2NetworkInterface.privateIpAddresses.privateIpAddress
- service.detection.sequence.resources.data.ec2NetworkInterface.publicIp
- service.detection.sequence.resources.data.ec2NetworkInterface.securityGroups.groupId
- service.detection.sequence.resources.data.ec2NetworkInterface.securityGroups.groupName
- service.detection.sequence.resources.data.ec2NetworkInterface.subNetId
- service.detection.sequence.resources.data.ec2NetworkInterface.vpcId
- service.detection.sequence.resources.data.ec2Vpc.ec2InstanceUids
- service.detection.sequence.resources.data.ecsCluster.ec2InstanceUids
- service.detection.sequence.resources.data.ecsCluster.status
- service.detection.sequence.resources.data.ecsTask.containerUids
- service.detection.sequence.resources.data.ecsTask.createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.detection.sequence.resources.data.ecsTask.launchType
- service.detection.sequence.resources.data.ecsTask.taskDefinitionArn
- service.detection.sequence.resources.data.eksCluster.arn
- service.detection.sequence.resources.data.eksCluster.createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000

- service.detection.sequence.resources.data.eksCluster.ec2InstanceUids
- service.detection.sequence.resources.data.eksCluster.status
- service.detection.sequence.resources.data.eksCluster.vpcId
- service.detection.sequence.resources.data.iamInstanceProfile.ec2InstanceUids
- service.detection.sequence.resources.data.iamInstanceProfile.id
- service.detection.sequence.resources.data.kubernetesWorkload.containerUids
- service.detection.sequence.resources.data.kubernetesWorkload.namespace
- service.detection.sequence.resources.data.kubernetesWorkload.type
- service.detection.sequence.resources.data.s3Bucket.accountPublicAccess.publicAclAccess
- service.detection.sequence.resources.data.s3Bucket.accountPublicAccess.publicAclIgnoreBehavior
- service.detection.sequence.resources.data.s3Bucket.accountPublicAccess.publicBucketRestrictBehavio
- service.detection.sequence.resources.data.s3Bucket.accountPublicAccess.publicPolicyAccess
- service.detection.sequence.resources.data.s3Bucket.bucketPublicAccess.publicAclAccess
- service.detection.sequence.resources.data.s3Bucket.bucketPublicAccess.publicAclIgnoreBehavior
- service.detection.sequence.resources.data.s3Bucket.bucketPublicAccess.publicBucketRestrictBehavior
- service.detection.sequence.resources.data.s3Bucket.bucketPublicAccess.publicPolicyAccess
- service.detection.sequence.resources.data.s3Bucket.createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.detection.sequence.resources.data.s3Bucket.effectivePermission
- service.detection.sequence.resources.data.s3Bucket.encryptionKeyArn
- service.detection.sequence.resources.data.s3Bucket.encryptionType
- service.detection.sequence.resources.data.s3Bucket.ownerId
- service.detection.sequence.resources.data.s3Bucket.publicReadAccess
- service.detection.sequence.resources.data.s3Bucket.publicWriteAccess
- service.detection.sequence.resources.data.s3Bucket.s3ObjectUids
- service.detection.sequence.resources.data.s3Object.eTag
- service.detection.sequence.resources.data.s3Object.key
- service.detection.sequence.resources.data.s3Object.versionId
- service.detection.sequence.resources.name
- service.detection.sequence.resources.region

- service.detection.sequence.resources.resourceType
- service.detection.sequence.resources.service
- service.detection.sequence.resources.tags.key
- service.detection.sequence.resources.tags.value
- service.detection.sequence.resources.uid
- service.detection.sequence.sequenceIndicators.key
- service.detection.sequence.sequenceIndicators.title
- service.detection.sequence.sequenceIndicators.values
- service.detection.sequence.signals.actorIds
- service.detection.sequence.signals.count
- service.detection.sequence.signals.createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.detection.sequence.signals.description
- service.detection.sequence.signals.endpointIds
- service.detection.sequence.signals.firstSeenAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.detection.sequence.signals.lastSeenAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.detection.sequence.signals.name
- service.detection.sequence.signals.resourceUids
- service.detection.sequence.signals.severity
- service.detection.sequence.signals.signalIndicators.key
- service.detection.sequence.signals.signalIndicators.title
- service.detection.sequence.signals.signalIndicators.values
- service.detection.sequence.signals.type
- service.detection.sequence.signals.uid
- service.detection.sequence.signals.updatedAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.detection.sequence.uid

- service.detectorId
- service.ebsVolumeScanDetails.scanCompletedAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.ebsVolumeScanDetails.scanDetections.highestSeverityThreatDetails.count
- service.ebsVolumeScanDetails.scanDetections.highestSeverityThreatDetails.severity
- service.ebsVolumeScanDetails.scanDetections.highestSeverityThreatDetails.threatName
- service.ebsVolumeScanDetails.scanDetections.scannedItemCount.files
- service.ebsVolumeScanDetails.scanDetections.scannedItemCount.totalGb
- service.ebsVolumeScanDetails.scanDetections.scannedItemCount.volumes
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.itemCount
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.shortened
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.fileNam
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.filePath
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.hash
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.volume
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.itemCount
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.name
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.severity
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.uniqueThreatNameCount
- service.ebsVolumeScanDetails.scanDetections.threatsDetectedItemCount.files
- service.ebsVolumeScanDetails.scanId
- service.ebsVolumeScanDetails.scanStartedAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.ebsVolumeScanDetails.scanType
- service.ebsVolumeScanDetails.sources
- service.ebsVolumeScanDetails.triggerFindingId
- service.eventFirstSeen

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.eventLastSeen

Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000

- service.evidence.threatIntelligenceDetails.threatFileSha256
- service.evidence.threatIntelligenceDetails.threatListName
- service.evidence.threatIntelligenceDetails.threatNames
- service.featureName
- service.malwareScanDetails.scanCategory
- service.malwareScanDetails.scanConfiguration.incrementalScanDetails.baselineResourceArn
- service.malwareScanDetails.scanConfiguration.triggerType
- service.malwareScanDetails.scanId
- service.malwareScanDetails.scanType
- service.malwareScanDetails.threats.count
- service.malwareScanDetails.threats.hash
- service.malwareScanDetails.threats.itemDetails.additionalInfo.deviceName
- service.malwareScanDetails.threats.itemDetails.additionalInfo.versionId
- service.malwareScanDetails.threats.itemDetails.hash
- service.malwareScanDetails.threats.itemDetails.itemPath
- service.malwareScanDetails.threats.itemDetails.resourceArn
- service.malwareScanDetails.threats.itemPaths.hash
- service.malwareScanDetails.threats.itemPaths.nestedItemPath
- service.malwareScanDetails.threats.name
- service.malwareScanDetails.threats.source
- service.malwareScanDetails.uniqueThreatCount
- service.resourceRole
- service.runtimeDetails.context.addressFamily
- service.runtimeDetails.context.commandLineExample
- service.runtimeDetails.context.fileOperation
- service.runtimeDetails.context.filePath
- service.runtimeDetails.context.fileSystemType
- service.runtimeDetails.context.flags

- service.runtimeDetails.context.ianaProtocolNumber
- service.runtimeDetails.context.ldPreloadValue
- service.runtimeDetails.context.libraryPath
- service.runtimeDetails.context.memoryRegions
- service.runtimeDetails.context.modifiedAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.runtimeDetails.context.modifyingProcess.euid
- service.runtimeDetails.context.modifyingProcess.executablePath
- service.runtimeDetails.context.modifyingProcess.executableSha256
- service.runtimeDetails.context.modifyingProcess.lineage.euid
- service.runtimeDetails.context.modifyingProcess.lineage.executablePath
- service.runtimeDetails.context.modifyingProcess.lineage.name
- service.runtimeDetails.context.modifyingProcess.lineage.namespacePid
- service.runtimeDetails.context.modifyingProcess.lineage.parentUuid
- service.runtimeDetails.context.modifyingProcess.lineage.pid
- service.runtimeDetails.context.modifyingProcess.lineage.startTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.runtimeDetails.context.modifyingProcess.lineage.userId
- service.runtimeDetails.context.modifyingProcess.lineage.uuid
- service.runtimeDetails.context.modifyingProcess.name
- service.runtimeDetails.context.modifyingProcess.namespacePid
- service.runtimeDetails.context.modifyingProcess.parentUuid
- service.runtimeDetails.context.modifyingProcess.pid
- service.runtimeDetails.context.modifyingProcess.pwd
- service.runtimeDetails.context.modifyingProcess.startTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.runtimeDetails.context.modifyingProcess.user
- service.runtimeDetails.context.modifyingProcess.userId
- service.runtimeDetails.context.modifyingProcess.uuid

- service.runtimeDetails.context.moduleFilePath
- service.runtimeDetails.context.moduleName
- service.runtimeDetails.context.moduleSha256
- service.runtimeDetails.context.mountSource
- service.runtimeDetails.context.mountTarget
- service.runtimeDetails.context.relatedFilePaths
- service.runtimeDetails.context.releaseAgentPath
- service.runtimeDetails.context.runcBinaryPath
- service.runtimeDetails.context.scriptPath
- service.runtimeDetails.context.serviceName
- service.runtimeDetails.context.shellHistoryFilePath
- service.runtimeDetails.context.socketPath
- service.runtimeDetails.context.targetProcess.euid
- service.runtimeDetails.context.targetProcess.executablePath
- service.runtimeDetails.context.targetProcess.executableSha256
- service.runtimeDetails.context.targetProcess.lineage.euid
- service.runtimeDetails.context.targetProcess.lineage.executablePath
- service.runtimeDetails.context.targetProcess.lineage.name
- service.runtimeDetails.context.targetProcess.lineage.namespacePid
- service.runtimeDetails.context.targetProcess.lineage.parentUuid
- service.runtimeDetails.context.targetProcess.lineage.pid
- service.runtimeDetails.context.targetProcess.lineage.startTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.runtimeDetails.context.targetProcess.lineage.userId
- service.runtimeDetails.context.targetProcess.lineage.uuid
- service.runtimeDetails.context.targetProcess.name
- service.runtimeDetails.context.targetProcess.namespacePid
- service.runtimeDetails.context.targetProcess.parentUuid
- service.runtimeDetails.context.targetProcess.pid

- service.runtimeDetails.context.targetProcess.pwd
- service.runtimeDetails.context.targetProcess.startTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.runtimeDetails.context.targetProcess.user
- service.runtimeDetails.context.targetProcess.userId
- service.runtimeDetails.context.targetProcess.uuid
- service.runtimeDetails.context.threatFilePath
- service.runtimeDetails.context.toolCategory
- service.runtimeDetails.context.toolName
- service.runtimeDetails.process.euid
- service.runtimeDetails.process.executablePath
- service.runtimeDetails.process.executableSha256
- service.runtimeDetails.process.lineage.euid
- service.runtimeDetails.process.lineage.executablePath
- service.runtimeDetails.process.lineage.name
- service.runtimeDetails.process.lineage.namespacePid
- service.runtimeDetails.process.lineage.parentUuid
- service.runtimeDetails.process.lineage.pid
- service.runtimeDetails.process.lineage.startTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.runtimeDetails.process.lineage.userId
- service.runtimeDetails.process.lineage.uuid
- service.runtimeDetails.process.name
- service.runtimeDetails.process.namespacePid
- service.runtimeDetails.process.parentUuid
- service.runtimeDetails.process.pid
- service.runtimeDetails.process.pwd
- service.runtimeDetails.process.startTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000

- service.runtimeDetails.process.user
- service.runtimeDetails.process.userId
- service.runtimeDetails.process.uuid
- service.serviceName
- service.userFeedback
- severity

  To configure severity based filters, use the following for the FindingCriteria condition:

  - **Low**: `["1", "2", "3"]`
  - **Medium**: `["4", "5", "6"]`
  - **High**: `["7", "8"]`
  - **Critical**: `["9", "10"]`

  For more information, see Findings severity levels in the *Amazon GuardDuty User Guide*.
- type
- updatedAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000

Type: FindingCriteria object

Required: Yes

name

The name of the filter. Valid characters include period (.), underscore (_), dash (-), and alphanumeric characters. A whitespace is considered to be an invalid character.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 64.

Required: Yes

rank

Specifies the position of the filter in the list of current filters. Also specifies the order in which this filter is applied to the findings.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

tags

The tags to be added to a new filter resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "name": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

name

The name of the successfully created filter.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 64.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateInvestigation

This API is currently available as a preview. During the preview, you can initiate up to 10 investigations per account per day, with a total limit of 100 investigations per account. This feature is available in the following AWS Regions: US East (N. Virginia), US East (Ohio), US West (Oregon), Canada (Central), Europe (Frankfurt), Europe (Ireland), Europe (London), Europe (Paris), Europe (Stockholm), and Asia Pacific (Tokyo).

Initiates a GuardDuty investigation that automatically analyzes security findings, correlates related activity, performs account-level analysis, and produces a structured investigation summary with recommended next steps.

Only the administrator account can create an investigation. Member accounts don't have permission to create investigations from their accounts.

To use this operation, the `AI_ANALYST` feature must be enabled on your detector.

This feature uses Amazon Bedrock models that leverage Cross-Region Inference (CRIS), which automatically selects the optimal AWS Region within your geography to process the investigation analysis and generate the investigation report. This maximizes available compute resources, model availability, and delivers the best customer experience. Your data remains stored only in the Region where the investigation request originates, however, investigation data and summary results may be processed outside that Region. All data is transmitted encrypted across Amazon's secure network. For more information, see GuardDuty Investigation.

Request Syntax

```
POST /detector/DetectorId/investigation HTTP/1.1
Content-type: application/json

{
   "clientToken": "string",
   "triggerPrompt": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the GuardDuty detector for the account in which the investigation is created.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

clientToken

The idempotency token for the create request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

triggerPrompt

A natural-language description of what to investigate. For example:

- `"Investigate finding 1ab2c3d4e5f6a7b8c9d0e1f2a3b4c5d6 in account 123456789012"`
- `"Analyze findings in account with id 123456789012"`
- `"Analyze findings in my organization"`

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

Response Syntax

```
HTTP/1.1 202
```

```
Content-type: application/json

{
   "investigationId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 202 response.

The following data is returned in JSON format by the service.

investigationId

The unique identifier of the newly created investigation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-fA-F0-9\-]+`

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateIPSet

Creates a new IPSet, which is called a trusted IP list in the console user interface. An IPSet is a list of IP addresses that are trusted for secure communication with AWS infrastructure and applications. GuardDuty doesn't generate findings for IP addresses that are included in IPSets. Only users from the administrator account can use this operation.

Request Syntax

```
POST /detector/DetectorId/ipset HTTP/1.1
Content-type: application/json

{
   "activate": boolean,
   "clientToken": "string",
   "expectedBucketOwner": "string",
   "format": "string",
   "location": "string",
   "name": "string",
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty account for which you want to create an IPSet.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

activate

A Boolean value that indicates whether GuardDuty is to start using the uploaded IPSet.

Type: Boolean

Required: Yes

clientToken

The idempotency token for the create request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

expectedBucketOwner

The AWS account ID that owns the Amazon S3 bucket specified in the **location** parameter.

Type: String

Length Constraints: Fixed length of 12.

Required: No

format

The format of the file that contains the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `TXT | STIX | OTX_CSV | ALIEN_VAULT | PROOF_POINT | FIRE_EYE`

Required: Yes

location

The URI of the file that contains the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

name

The user-friendly name to identify the IPSet.

Allowed characters are alphanumeric, whitespace, dash (-), and underscores (_).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

tags

The tags to be added to a new IP set resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "ipSetId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

ipSetId

The ID of the IPSet resource.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateMalwareProtectionPlan

Creates a new Malware Protection plan for the protected resource.

When you create a Malware Protection plan, the AWS service terms for GuardDuty Malware Protection apply. For more information, see AWS service terms for GuardDuty Malware Protection.

Request Syntax

```
POST /malware-protection-plan HTTP/1.1
Content-type: application/json

{
   "actions": {
      "tagging": {
         "status": "string"
      }
   },
   "clientToken": "string",
   "protectedResource": {
      "s3Bucket": {
         "bucketName": "string",
         "objectPrefixes": [ "string" ]
      }
   },
   "role": "string",
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

actions

Information about whether the tags will be added to the S3 object after scanning.

Type: MalwareProtectionPlanActions object

Required: No

clientToken

The idempotency token for the create request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

protectedResource

Information about the protected resource that is associated with the created Malware Protection plan. Presently, `S3Bucket` is the only supported protected resource.

Type: CreateProtectedResource object

Required: Yes

role

Amazon Resource Name (ARN) of the IAM role that has the permissions to scan and add tags to the associated protected resource.

Type: String

Required: Yes

tags

Tags added to the Malware Protection plan resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "malwareProtectionPlanId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

malwareProtectionPlanId

A unique identifier associated with the Malware Protection plan resource.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

ConflictException

A request conflict exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 409

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateMembers

Creates member accounts of the current AWS account by specifying a list of AWS account IDs. This step is a prerequisite for managing the associated member accounts either by invitation or through an organization.

As a delegated administrator, using `CreateMembers` will enable GuardDuty in the added member accounts, with the exception of the organization delegated administrator account. A delegated administrator must enable GuardDuty prior to being added as a member.

When you use CreateMembers as an AWS Organizations delegated administrator, GuardDuty applies your organization's auto-enable settings to the member accounts in this request, irrespective of the accounts being new or existing members. For more information about the existing auto-enable settings for your organization, see DescribeOrganizationConfiguration.

If you disassociate a member account that was added by invitation, the member account details obtained from this API, including the associated email addresses, will be retained. This is done so that the delegated administrator can invoke the InviteMembers API without the need to invoke the CreateMembers API again. To remove the details associated with a member account, the delegated administrator must invoke the DeleteMembers API.

When the member accounts added through AWS Organizations are later disassociated, you (administrator) can't invite them by calling the InviteMembers API. You can create an association with these member accounts again only by calling the CreateMembers API.

Request Syntax

```
POST /detector/DetectorId/member HTTP/1.1
Content-type: application/json

{
   "accountDetails": [
      {
         "accountId": "string",
         "email": "string"
      }
   ]
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty account for which you want to associate member accounts.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountDetails

A list of account ID and email address pairs of the accounts that you want to associate with the GuardDuty administrator account.

Type: Array of AccountDetail objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "string"
```

```
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

unprocessedAccounts

A list of objects that include the `accountIds` of the unprocessed accounts and a result string that explains why each was unprocessed.

Type: Array of UnprocessedAccount objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreatePublishingDestination

Creates a publishing destination where you can export your GuardDuty findings. Before you start exporting the findings, the destination resource must exist.

Request Syntax

```
POST /detector/DetectorId/publishingDestination HTTP/1.1
Content-type: application/json

{
   "clientToken": "string",
   "destinationProperties": {
      "destinationArn": "string",
      "kmsKeyArn": "string"
   },
   "destinationType": "string",
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The ID of the GuardDuty detector associated with the publishing destination.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

clientToken

The idempotency token for the request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

destinationProperties

The properties of the publishing destination, including the ARNs for the destination and the KMS key used for encryption.

Type: DestinationProperties object

Required: Yes

destinationType

The type of resource for the publishing destination. Currently only Amazon S3 buckets are supported.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: S3

Required: Yes

tags

The tags to be added to a new publishing destination resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "destinationId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

destinationId

The ID of the publishing destination that is created.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateSampleFindings

Generates sample findings of types specified by the list of finding types. If 'NULL' is specified for `findingTypes`, the API generates sample findings of all supported finding types.

Request Syntax

```
POST /detector/DetectorId/findings/create HTTP/1.1
Content-type: application/json

{
   "findingTypes": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The ID of the detector for which you need to create sample findings.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

findingTypes

The types of sample findings to generate.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 100.

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateThreatEntitySet

Creates a new threat entity set. In a threat entity set, you can provide known malicious threat entities for your AWS environment. GuardDuty generates findings based on the entries in the threat entity sets. Only users of the administrator account can manage entity sets, which automatically apply to member accounts.

Request Syntax

```
POST /detector/DetectorId/threatentityset HTTP/1.1
Content-type: application/json

{
   "activate": boolean,
   "clientToken": "string",
   "expectedBucketOwner": "string",
   "format": "string",
   "location": "string",
   "name": "string",
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty account for which you want to create a threat entity set.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

activate

A boolean value that indicates whether GuardDuty should start using the uploaded threat entity set to generate findings.

Type: Boolean

Required: Yes

clientToken

The idempotency token for the create request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

expectedBucketOwner

The AWS account ID that owns the Amazon S3 bucket specified in the **location** parameter.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `[0-9]+`

Required: No

format

The format of the file that contains the threat entity set.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `TXT | STIX | OTX_CSV | ALIEN_VAULT | PROOF_POINT | FIRE_EYE`

Required: Yes

location

The URI of the file that contains the threat entity set. The format of the `Location` URL must be a valid Amazon S3 URL format. Invalid URL formats will result in an error, regardless of whether you activate the entity set or not. For more information about format of the location URLs, see Format of location URL under Step 2: Adding trusted or threat intelligence data in the *Amazon GuardDuty User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

name

A user-friendly name to identify the threat entity set.

The name of your list can include lowercase letters, uppercase letters, numbers, dash (-), and underscore (_).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

tags

The tags to be added to a new threat entity set resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "threatEntitySetId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

threatEntitySetId

The ID returned by GuardDuty after creation of the threat entity set resource.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateThreatIntelSet

Creates a new ThreatIntelSet. ThreatIntelSets consist of known malicious IP addresses. GuardDuty generates findings based on ThreatIntelSets. Only users of the administrator account can use this operation.

Request Syntax

```
POST /detector/DetectorId/threatintelset HTTP/1.1
Content-type: application/json

{
   "activate": boolean,
   "clientToken": "string",
   "expectedBucketOwner": "string",
   "format": "string",
   "location": "string",
   "name": "string",
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty account for which you want to create a `threatIntelSet`.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

activate

A Boolean value that indicates whether GuardDuty is to start using the uploaded ThreatIntelSet.

Type: Boolean

Required: Yes

clientToken

The idempotency token for the create request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

expectedBucketOwner

The AWS account ID that owns the Amazon S3 bucket specified in the **location** parameter.

Type: String

Length Constraints: Fixed length of 12.

Required: No

format

The format of the file that contains the ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `TXT | STIX | OTX_CSV | ALIEN_VAULT | PROOF_POINT | FIRE_EYE`

Required: Yes

location

The URI of the file that contains the ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

name

A user-friendly ThreatIntelSet name displayed in all findings that are generated by activity that involves IP addresses included in this ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

tags

The tags to be added to a new threat list resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "threatIntelSetId": "string"
```

```
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

threatIntelSetId

The ID of the ThreatIntelSet resource.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateTrustedEntitySet

Creates a new trusted entity set. In the trusted entity set, you can provide IP addresses and domains that you believe are secure for communication in your AWS environment. GuardDuty will not generate findings for the entries that are specified in a trusted entity set. At any given time, you can have only one trusted entity set.

Only users of the administrator account can manage the entity sets, which automatically apply to member accounts.

Request Syntax

```
POST /detector/DetectorId/trustedentityset HTTP/1.1
Content-type: application/json

{
   "activate": boolean,
   "clientToken": "string",
   "expectedBucketOwner": "string",
   "format": "string",
   "location": "string",
   "name": "string",
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty account for which you want to create a trusted entity set.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

activate

A boolean value that indicates whether GuardDuty is to start using the uploaded trusted entity set.

Type: Boolean

Required: Yes

clientToken

The idempotency token for the create request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

expectedBucketOwner

The AWS account ID that owns the Amazon S3 bucket specified in the **location** parameter.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `[0-9]+`

Required: No

format

The format of the file that contains the trusted entity set.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `TXT | STIX | OTX_CSV | ALIEN_VAULT | PROOF_POINT | FIRE_EYE`

Required: Yes

location

The URI of the file that contains the threat entity set. The format of the `Location` URL must be a valid Amazon S3 URL format. Invalid URL formats will result in an error, regardless of whether you activate the entity set or not. For more information about format of the location URLs, see Format of location URL under Step 2: Adding trusted or threat intelligence data in the *Amazon GuardDuty User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

name

A user-friendly name to identify the trusted entity set.

The name of your list can include lowercase letters, uppercase letters, numbers, dash (-), and underscore (_).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

tags

The tags to be added to a new trusted entity set resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "trustedEntitySetId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

trustedEntitySetId

The ID returned by GuardDuty after creation of the trusted entity set resource.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeclineInvitations

Declines invitations sent to the current member account by AWS accounts specified by their account IDs.

Request Syntax

```
POST /invitation/decline HTTP/1.1
Content-type: application/json

{
   "accountIds": [ "string" ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

accountIds

A list of account IDs of the AWS accounts that sent invitations to the current member account that you want to decline invitations from.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

unprocessedAccounts

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of UnprocessedAccount objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteCustomDetectionRuleAssociation

Disables a custom detection rule by deleting its association. This operation is idempotent.

Request Syntax

```
DELETE /custom-detection-rule/rule/RuleId/association/AssociationId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

AssociationId

The unique identifier for the association to delete.

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-zA-Z0-9_-]{1,64}`

Required: Yes

RuleId

The unique identifier for the custom detection rule.

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

ResourceNotFoundException

The requested resource can't be found.

Message

The error message.

Type

The error type.

HTTP Status Code: 404

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteCustomDetectionRuleOrgConfiguration

Deletes the organization-level configuration for a custom detection rule. This operation is available only to the delegated administrator account.

Request Syntax

```
DELETE /custom-detection-rule/org-configuration/RuleId?mode=Mode HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

Mode

The execution mode of the organization configuration to delete. Valid values: `LIVE` | `DRY_RUN`.

Valid Values: `LIVE | DRY_RUN`

Required: Yes

RuleId

The unique identifier for the custom detection rule.

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

ConflictException

A request conflict exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 409

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

ResourceNotFoundException

The requested resource can't be found.

Message

The error message.

Type

The error type.

HTTP Status Code: 404

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3

- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteDetector

Deletes an Amazon GuardDuty detector that is specified by the detector ID.

Request Syntax

```
DELETE /detector/DetectorId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector that you want to delete.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)

- AWS SDK for Ruby V3

DeleteFilter

Deletes the filter specified by the filter name.

Request Syntax

```
DELETE /detector/DetectorId/filter/FilterName HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector that is associated with the filter.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

FilterName

The name of the filter that you want to delete.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteInvitations

Deletes invitations sent to the current member account by AWS accounts specified by their account IDs.

Request Syntax

```
POST /invitation/delete HTTP/1.1
Content-type: application/json

{
   "accountIds": [ "string" ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

accountIds

A list of account IDs of the AWS accounts that sent invitations to the current member account that you want to delete invitations from.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

unprocessedAccounts

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of UnprocessedAccount objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteIPSet

Deletes the IPSet specified by the `ipSetId`. IPSets are called trusted IP lists in the console user interface.

Request Syntax

```
DELETE /detector/DetectorId/ipset/IpSetId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector associated with the IPSet.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

IpSetId

The unique ID of the IPSet to delete.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteMalwareProtectionPlan

Deletes the Malware Protection plan ID associated with the Malware Protection plan resource. Use this API only when you no longer want to protect the resource associated with this Malware Protection plan ID.

Request Syntax

```
DELETE /malware-protection-plan/MalwareProtectionPlanId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

MalwareProtectionPlanId

A unique identifier associated with Malware Protection plan resource.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

ResourceNotFoundException

The requested resource can't be found.

Message

The error message.

Type

The error type.

HTTP Status Code: 404

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteMembers

Deletes GuardDuty member accounts (to the current GuardDuty administrator account) specified by the account IDs.

With `autoEnableOrganizationMembers` configuration for your organization set to `ALL`, you'll receive an error if you attempt to disable GuardDuty for a member account in your organization.

Request Syntax

```
POST /detector/DetectorId/member/delete HTTP/1.1
Content-type: application/json

{
   "accountIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty account whose members you want to delete.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds

A list of account IDs of the GuardDuty member accounts that you want to delete.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

unprocessedAccounts

The accounts that could not be processed.

Type: Array of UnprocessedAccount objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeletePublishingDestination

Deletes the publishing definition with the specified `destinationId`.

Request Syntax

```
DELETE /detector/DetectorId/publishingDestination/DestinationId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DestinationId

The ID of the publishing destination to delete.

Required: Yes

DetectorId

The unique ID of the detector associated with the publishing destination to delete.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteThreatEntitySet

Deletes the threat entity set that is associated with the specified `threatEntitySetId`.

Request Syntax

```
DELETE /detector/DetectorId/threatentityset/ThreatEntitySetId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector associated with the threat entity set resource.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

ThreatEntitySetId

The unique ID that helps GuardDuty identify which threat entity set needs to be deleted.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteThreatIntelSet

Deletes the ThreatIntelSet specified by the ThreatIntelSet ID.

Request Syntax

```
DELETE /detector/DetectorId/threatintelset/ThreatIntelSetId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector that is associated with the threatIntelSet.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

ThreatIntelSetId

The unique ID of the threatIntelSet that you want to delete.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteTrustedEntitySet

Deletes the trusted entity set that is associated with the specified `trustedEntitySetId`.

Request Syntax

```
DELETE /detector/DetectorId/trustedentityset/TrustedEntitySetId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector associated with the trusted entity set resource.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

TrustedEntitySetId

The unique ID that helps GuardDuty identify which trusted entity set needs to be deleted.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeMalwareScans

Returns a list of malware scans. Each member account can view the malware scans for their own accounts. An administrator can view the malware scans for all the member accounts.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see Regions and endpoints.

Request Syntax

```
POST /detector/DetectorId/malware-scans HTTP/1.1
Content-type: application/json

{
   "filterCriteria": {
      "filterCriterion": [
         {
            "criterionKey": "string",
            "filterCondition": {
               "equalsValue": "string",
               "greaterThan": number,
               "lessThan": number
            }
         }
      ]
   },
   "maxResults": number,
   "nextToken": "string",
   "sortCriteria": {
      "attributeName": "string",
      "orderBy": "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector that the request is associated with.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

filterCriteria

Represents the criteria to be used in the filter for describing scan entries.

Type: FilterCriteria object

Required: No

maxResults

You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 50.

Required: No

nextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Type: String

Required: No

sortCriteria

Represents the criteria used for sorting scan entries. The `attributeName` is required and it must be `scanStartTime`.

Type: SortCriteria object

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "nextToken": "string",
   "scans": [
      {
         "accountId": "string",
         "adminDetectorId": "string",
         "attachedVolumes": [
            {
               "deviceName": "string",
               "encryptionType": "string",
               "kmsKeyArn": "string",
               "snapshotArn": "string",
               "volumeArn": "string",
               "volumeSizeInGB": number,
               "volumeType": "string"
            }
         ],
         "detectorId": "string",
         "failureReason": "string",
         "fileCount": number,
         "resourceDetails": {
            "instanceArn": "string"
         },
         "scanEndTime": number,
         "scanId": "string",
         "scanResultDetails": {
            "scanResult": "string"
         },
         "scanStartTime": number,
         "scanStatus": "string",
         "scanType": "string",
         "totalBytes": number,
         "triggerDetails": {
            "description": "string",
```

```
            "guardDutyFindingId": "string",
            "triggerType": "string"
         }
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

scans

Contains information about malware scans associated with GuardDuty Malware Protection for EC2.

Type: Array of Scan objects

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeOrganizationConfiguration

Returns information about the account selected as the delegated administrator for GuardDuty.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see Regions and endpoints.

Request Syntax

```
GET /detector/DetectorId/admin?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The detector ID of the delegated administrator for which you need to retrieve the information.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

MaxResults

You can use this parameter to indicate the maximum number of items that you want in the response.

Valid Range: Minimum value of 1. Maximum value of 50.

NextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill `nextToken` in the request with the value of `NextToken` from the previous response to continue listing data.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "autoEnable": boolean,
   "autoEnableOrganizationMembers": "string",
   "dataSources": {
      "kubernetes": {
         "auditLogs": {
            "autoEnable": boolean
         }
      },
      "malwareProtection": {
         "scanEc2InstanceWithFindings": {
            "ebsVolumes": {
               "autoEnable": boolean
            }
         }
      },
      "s3Logs": {
         "autoEnable": boolean
      }
   },
   "features": [
      {
         "additionalConfiguration": [
            {
               "autoEnable": "string",
               "name": "string"
            }
         ],
         "autoEnable": "string",
         "name": "string"
      }
   ],
   "memberAccountLimitReached": boolean,
   "nextToken": "string"
```

```
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

autoEnable

This parameter has been deprecated.

Indicates whether GuardDuty is automatically enabled for accounts added to the organization.

Even though this is still supported, we recommend using `AutoEnableOrganizationMembers` to achieve the similar results.

Type: Boolean

autoEnableOrganizationMembers

Indicates the auto-enablement configuration of GuardDuty or any of the corresponding protection plans for the member accounts in the organization.

- `NEW`: Indicates that when a new account joins the organization, they will have GuardDuty or any of the corresponding protection plans enabled automatically.
- `ALL`: Indicates that all accounts in the organization have GuardDuty and any of the corresponding protection plans enabled automatically. This includes `NEW` accounts that join the organization and accounts that may have been suspended or removed from the organization in GuardDuty.
- `NONE`: Indicates that GuardDuty or any of the corresponding protection plans will not be automatically enabled for any account in the organization. The administrator must manage GuardDuty for each account in the organization individually.

  When you update the auto-enable setting from `ALL` or `NEW` to `NONE`, this action doesn't disable the corresponding option for your existing accounts. This configuration will apply to the new accounts that join the organization. After you update the auto-enable settings, no new account will have the corresponding option as enabled.

Type: String

Valid Values: `NEW | ALL | NONE`

dataSources

This parameter has been deprecated.

Describes which data sources are enabled automatically for member accounts.

Type: OrganizationDataSourceConfigurationsResult object

features

A list of features that are configured for this organization.

Type: Array of OrganizationFeatureConfigurationResult objects

memberAccountLimitReached

Indicates whether the maximum number of allowed member accounts are already associated with the delegated administrator account for your organization.

Type: Boolean

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribePublishingDestination

Returns information about the publishing destination specified by the provided `destinationId`.

Request Syntax

```
GET /detector/DetectorId/publishingDestination/DestinationId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DestinationId

The ID of the publishing destination to retrieve.

Required: Yes

DetectorId

The unique ID of the detector associated with the publishing destination to retrieve.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "destinationId": "string",
```

```
   "destinationProperties": {
      "destinationArn": "string",
      "kmsKeyArn": "string"
   },
   "destinationType": "string",
   "publishingFailureStartTimestamp": number,
   "status": "string",
   "tags": {
      "string" : "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

destinationId

The ID of the publishing destination.

Type: String

destinationProperties

A `DestinationProperties` object that includes the `DestinationArn` and `KmsKeyArn` of the publishing destination.

Type: DestinationProperties object

destinationType

The type of publishing destination. Currently, only Amazon S3 buckets are supported.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: S3

publishingFailureStartTimestamp

The time, in epoch millisecond format, at which GuardDuty was first unable to publish findings to the destination.

Type: Long

status

The status of the publishing destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `PENDING_VERIFICATION | PUBLISHING | UNABLE_TO_PUBLISH_FIX_DESTINATION_PROPERTY | STOPPED`

tags

The tags of the publishing destination resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DisableOrganizationAdminAccount

Removes the existing GuardDuty delegated administrator of the organization. Only the organization's management account can run this API operation.

Request Syntax

```
POST /admin/disable HTTP/1.1
Content-type: application/json

{
   "adminAccountId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

adminAccountId

The AWS Account ID for the organizations account to be disabled as a GuardDuty delegated administrator.

Type: String

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DisassociateFromAdministratorAccount

Disassociates the current GuardDuty member account from its administrator account.

When you disassociate an invited member from a GuardDuty delegated administrator, the member account details obtained from the CreateMembers API, including the associated email addresses, are retained. This is done so that the delegated administrator can invoke the InviteMembers API without the need to invoke the CreateMembers API again. To remove the details associated with a member account, the delegated administrator must invoke the DeleteMembers API.

With `autoEnableOrganizationMembers` configuration for your organization set to `ALL`, you'll receive an error if you attempt to disable GuardDuty in a member account.

Request Syntax

```
POST /detector/DetectorId/administrator/disassociate HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty member account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DisassociateFromMasterAccount

This action has been deprecated.

Disassociates the current GuardDuty member account from its administrator account.

When you disassociate an invited member from a GuardDuty delegated administrator, the member account details obtained from the CreateMembers API, including the associated email addresses, are retained. This is done so that the delegated administrator can invoke the InviteMembers API without the need to invoke the CreateMembers API again. To remove the details associated with a member account, the delegated administrator must invoke the DeleteMembers API.

Request Syntax

```
POST /detector/DetectorId/master/disassociate HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty member account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DisassociateMembers

Disassociates GuardDuty member accounts (from the current administrator account) specified by the account IDs.

When you disassociate an invited member from a GuardDuty delegated administrator, the member account details obtained from the CreateMembers API, including the associated email addresses, are retained. This is done so that the delegated administrator can invoke the InviteMembers API without the need to invoke the CreateMembers API again. To remove the details associated with a member account, the delegated administrator must invoke the DeleteMembers API.

With `autoEnableOrganizationMembers` configuration for your organization set to `ALL`, you'll receive an error if you attempt to disassociate a member account before removing them from your organization.

If you disassociate a member account that was added by invitation, the member account details obtained from this API, including the associated email addresses, will be retained. This is done so that the delegated administrator can invoke the InviteMembers API without the need to invoke the CreateMembers API again. To remove the details associated with a member account, the delegated administrator must invoke the DeleteMembers API.

When the member accounts added through AWS Organizations are later disassociated, you (administrator) can't invite them by calling the InviteMembers API. You can create an association with these member accounts again only by calling the CreateMembers API.

Request Syntax

```
POST /detector/DetectorId/member/disassociate HTTP/1.1
Content-type: application/json

{
   "accountIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty account whose members you want to disassociate from the administrator account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds

A list of account IDs of the GuardDuty member accounts that you want to disassociate from the administrator account.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

unprocessedAccounts

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of UnprocessedAccount objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

EnableOrganizationAdminAccount

Designates an AWS account within the organization as your GuardDuty delegated administrator. Only the organization's management account can run this API operation.

Request Syntax

```
POST /admin/enable HTTP/1.1
Content-type: application/json

{
   "adminAccountId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

adminAccountId

The AWS account ID for the organization account to be enabled as a GuardDuty delegated administrator.

Type: String

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetAdministratorAccount

Provides the details of the GuardDuty administrator account associated with the current GuardDuty member account.

Based on the type of account that runs this API, the following list shows how the API behavior varies:

- When the GuardDuty administrator account runs this API, it will return success (`HTTP 200`) but no content.
- When a member account runs this API, it will return the details of the GuardDuty administrator account that is associated with this calling member account.
- When an individual account (not associated with an organization) runs this API, it will return success (`HTTP 200`) but no content.

Request Syntax

```
GET /detector/DetectorId/administrator HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty member account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "administrator": {
      "accountId": "string",
      "invitationId": "string",
      "invitedAt": "string",
      "relationshipStatus": "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

administrator

The administrator account details.

Type: Administrator object

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetCoverageStatistics

Retrieves aggregated statistics for your account. If you are a GuardDuty administrator, you can retrieve the statistics for all the resources associated with the active member accounts in your organization who have enabled Runtime Monitoring and have the GuardDuty security agent running on their resources.

Request Syntax

```
POST /detector/DetectorId/coverage/statistics HTTP/1.1
Content-type: application/json

{
   "filterCriteria": {
      "filterCriterion": [
         {
            "criterionKey": "string",
            "filterCondition": {
               "equals": [ "string" ],
               "notEquals": [ "string" ]
            }
         }
      ]
   },
   "statisticsType": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the GuardDuty detector.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

filterCriteria

Represents the criteria used to filter the coverage statistics.

Type: CoverageFilterCriteria object

Required: No

statisticsType

Represents the statistics type used to aggregate the coverage details.

Type: Array of strings

Valid Values: `COUNT_BY_RESOURCE_TYPE | COUNT_BY_COVERAGE_STATUS`

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "coverageStatistics": {
      "countByCoverageStatus": {
         "string" : number
      },
      "countByResourceType": {
         "string" : number
      }
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

coverageStatistics

Represents the count aggregated by the `statusCode` and `resourceType`.

Type: CoverageStatistics object

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetCustomDetectionRule

Returns details for a custom detection rule in GuardDuty, including its detection logic.

Request Syntax

```
GET /custom-detection-rule/rule/RuleId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

RuleId

The unique identifier for the custom detection rule.

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "rule": {
      "arn": "string",
      "createdAt": number,
      "dataSource": "string",
      "definition": {
         "expression": "string"
      },
      "description": "string",
      "language": "string",
```

```
      "name": "string",
      "ruleId": "string",
      "runtimeMonitoringDetails": {
         "platforms": {
            "ec2": {
               "minAgentVersion": "string"
            },
            "ecsFargate": {
               "minAgentVersion": "string"
            },
            "eks": {
               "minAgentVersion": "string"
            }
         }
      },
      "schema": "string",
      "service": "string",
      "severity": "string",
      "tactic": "string",
      "technique": "string",
      "updatedAt": number
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

rule

The details of the custom detection rule.

Type: RuleDetail object

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

ResourceNotFoundException

The requested resource can't be found.

Message

The error message.

Type

The error type.

HTTP Status Code: 404

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetCustomDetectionRuleAssociation

Returns details for a custom detection rule association.

Request Syntax

```
GET /custom-detection-rule/rule/RuleId/association/AssociationId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

AssociationId

The unique identifier for the association.

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-zA-Z0-9_-]{1,64}`

Required: Yes

RuleId

The unique identifier for the custom detection rule.

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "ruleAssociation": {
      "accountId": "string",
      "arn": "string",
      "associationId": "string",
      "createdAt": number,
      "expiresAt": number,
      "mode": "string",
      "ruleId": "string",
      "updatedAt": number
   },
   "tags": {
      "string" : "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

ruleAssociation

The details of the custom detection rule association.

Type: AssociationDetail object

tags

The tags associated with the custom detection rule association resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

ResourceNotFoundException

The requested resource can't be found.

Message

The error message.

Type

The error type.

HTTP Status Code: 404

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetCustomDetectionRuleOrgConfiguration

Returns the organization-level configuration for a custom detection rule.

Request Syntax

```
GET /custom-detection-rule/org-configuration/RuleId?mode=Mode HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

Mode

The execution mode of the organization configuration to retrieve. Valid values: `LIVE` | `DRY_RUN`.

Valid Values: `LIVE | DRY_RUN`

Required: Yes

RuleId

The unique identifier for the custom detection rule.

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "configuration": {
      "createdAt": number,
```

```
      "excludeAccountIds": [ "string" ],
      "expiresAt": number,
      "includeAccountIds": [ "string" ],
      "mode": "string",
      "ruleId": "string",
      "status": "string",
      "statusReason": "string",
      "updatedAt": number
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

configuration

The details of the organization configuration.

Type: DetectionRuleOrgConfiguration object

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

ResourceNotFoundException

The requested resource can't be found.

Message

The error message.

Type

The error type.

HTTP Status Code: 404

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetDetector

Retrieves a GuardDuty detector specified by the detectorId.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see Regions and endpoints.

Request Syntax

```
GET /detector/DetectorId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector that you want to get.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "createdAt": "string",
   "dataSources": {
      "cloudTrail": {
         "status": "string"
```

```
      },
      "dnsLogs": {
         "status": "string"
      },
      "flowLogs": {
         "status": "string"
      },
      "kubernetes": {
         "auditLogs": {
            "status": "string"
         }
      },
      "malwareProtection": {
         "scanEc2InstanceWithFindings": {
            "ebsVolumes": {
               "reason": "string",
               "status": "string"
            }
         },
         "serviceRole": "string"
      },
      "s3Logs": {
         "status": "string"
      }
   },
   "features": [
      {
         "additionalConfiguration": [
            {
               "managedBy": "string",
               "name": "string",
               "status": "string",
               "updatedAt": number
            }
         ],
         "managedBy": "string",
         "name": "string",
         "status": "string",
         "updatedAt": number
      }
   ],
   "findingPublishingFrequency": "string",
   "serviceRole": "string",
   "status": "string",
```

```
   "tags": {
      "string" : "string"
   },
   "updatedAt": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

createdAt

The timestamp of when the detector was created.

Type: String

dataSources

This parameter has been deprecated.

Describes which data sources are enabled for the detector.

Type: DataSourceConfigurationsResult object

features

Describes the features that have been enabled for the detector.

Type: Array of DetectorFeatureConfigurationResult objects

findingPublishingFrequency

The publishing frequency of the finding.

Type: String

Valid Values: `FIFTEEN_MINUTES | ONE_HOUR | SIX_HOURS`

serviceRole

The GuardDuty service role.

Type: String

status

The detector status.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `ENABLED | DISABLED`

tags

The tags of the detector resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

updatedAt

The last-updated timestamp for the detector.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetFilter

Returns the details of the filter specified by the filter name.

Request Syntax

```
GET /detector/DetectorId/filter/FilterName HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector that is associated with this filter.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

FilterName

The name of the filter you want to get.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "action": "string",
   "createdAt": number,
```

```
   "description": "string",
   "findingCriteria": {
      "criterion": {
         "string" : {
            "eq": [ "string" ],
            "equals": [ "string" ],
            "greaterThan": number,
            "greaterThanOrEqual": number,
            "gt": number,
            "gte": number,
            "lessThan": number,
            "lessThanOrEqual": number,
            "lt": number,
            "lte": number,
            "matches": [ "string" ],
            "neq": [ "string" ],
            "notEquals": [ "string" ],
            "notMatches": [ "string" ]
         }
      }
   },
   "name": "string",
   "rank": number,
   "tags": {
      "string" : "string"
   },
   "updatedAt": number,
   "version": number
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

action

Specifies the action that is to be applied to the findings that match the filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `NOOP | ARCHIVE`

createdAt

The timestamp when the filter was created. This field is not available for filters that were created before the lifecycle metadata feature was enabled (legacy filters).

Type: Timestamp

description

The description of the filter.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 512.

findingCriteria

Represents the criteria to be used in the filter for querying findings.

Type: FindingCriteria object

name

The name of the filter.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 64.

rank

Specifies the position of the filter in the list of current filters. Also specifies the order in which this filter is applied to the findings.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

tags

The tags of the filter resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

updatedAt

The timestamp when the filter was last updated. For legacy filters, this field is present only after the filter has been updated at least once since the lifecycle metadata feature was enabled.

Type: Timestamp

version

The version of the filter. Every time the filter is updated, the version increments by 1. This field is not available for legacy filters that were created before the lifecycle metadata feature was enabled.

Type: Long

Valid Range: Minimum value of 1.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetFindings

Describes Amazon GuardDuty findings specified by finding IDs.

Request Syntax

```
POST /detector/DetectorId/findings/get HTTP/1.1
Content-type: application/json

{
   "findingIds": [ "string" ],
   "sortCriteria": {
      "attributeName": "string",
      "orderBy": "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The ID of the detector that specifies the GuardDuty service whose findings you want to retrieve.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

findingIds

The IDs of the findings that you want to retrieve.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

sortCriteria

Represents the criteria used for sorting findings.

Type: SortCriteria object

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "findings": [
      {
         "accountId": "string",
         "arn": "string",
         "associatedAttackSequenceArn": "string",
         "confidence": number,
         "createdAt": "string",
         "customDetectionRuleName": "string",
         "description": "string",
         "id": "string",
         "partition": "string",
         "region": "string",
         "resource": {
            "accessKeyDetails": {
               "accessKeyId": "string",
               "principalId": "string",
               "userName": "string",
               "userType": "string"
            },
            "bedrockGuardrailDetails": {
               "contentPolicyFilters": [
                  {
                     "action": "string",
                     "confidence": "string",
```

```
                    "type": "string"
                }
            ],
            "guardrailAction": "string",
            "guardrailArn": "string",
            "guardrails": [
                {
                    "arn": "string",
                    "version": "string"
                }
            ],
            "guardrailSource": "string",
            "guardrailVersion": "string"
        },
        "containerDetails": {
            "containerRuntime": "string",
            "id": "string",
            "image": "string",
            "imagePrefix": "string",
            "name": "string",
            "securityContext": {
                "allowPrivilegeEscalation": boolean,
                "privileged": boolean
            },
            "volumeMounts": [
                {
                    "mountPath": "string",
                    "name": "string"
                }
            ]
        },
        "ebsSnapshotDetails": {
            "snapshotArn": "string"
        },
        "ebsVolumeDetails": {
            "scannedVolumeDetails": [
                {
                    "deviceName": "string",
                    "encryptionType": "string",
                    "kmsKeyArn": "string",
                    "snapshotArn": "string",
                    "volumeArn": "string",
                    "volumeSizeInGB": number,
                    "volumeType": "string"
```

```
            }
         ],
         "skippedVolumeDetails": [
            {
               "deviceName": "string",
               "encryptionType": "string",
               "kmsKeyArn": "string",
               "snapshotArn": "string",
               "volumeArn": "string",
               "volumeSizeInGB": number,
               "volumeType": "string"
            }
         ]
      },
      "ec2ImageDetails": {
         "imageArn": "string"
      },
      "ecsClusterDetails": {
         "activeServicesCount": number,
         "arn": "string",
         "name": "string",
         "registeredContainerInstancesCount": number,
         "runningTasksCount": number,
         "status": "string",
         "tags": [
            {
               "key": "string",
               "value": "string"
            }
         ],
         "taskDetails": {
            "arn": "string",
            "containers": [
               {
                  "containerRuntime": "string",
                  "id": "string",
                  "image": "string",
                  "imagePrefix": "string",
                  "name": "string",
                  "securityContext": {
                     "allowPrivilegeEscalation": boolean,
                     "privileged": boolean
                  },
                  "volumeMounts": [
```

```
                        {
                           "mountPath": "string",
                           "name": "string"
                        }
                     ]
                  }
               ],
               "definitionArn": "string",
               "group": "string",
               "launchType": "string",
               "startedAt": number,
               "startedBy": "string",
               "tags": [
                  {
                     "key": "string",
                     "value": "string"
                  }
               ],
               "createdAt": number,
               "version": "string",
               "volumes": [
                  {
                     "hostPath": {
                        "path": "string"
                     },
                     "name": "string"
                  }
               ]
            }
         },
         "eksClusterDetails": {
            "arn": "string",
            "createdAt": number,
            "name": "string",
            "status": "string",
            "tags": [
               {
                  "key": "string",
                  "value": "string"
               }
            ],
            "vpcId": "string"
         },
         "instanceDetails": {
```

```
            "availabilityZone": "string",
            "iamInstanceProfile": {
               "arn": "string",
               "id": "string"
            },
            "imageDescription": "string",
            "imageId": "string",
            "instanceId": "string",
            "instanceState": "string",
            "instanceType": "string",
            "launchTime": "string",
            "networkInterfaces": [
               {
                  "ipv6Addresses": [ "string" ],
                  "networkInterfaceId": "string",
                  "privateDnsName": "string",
                  "privateIpAddress": "string",
                  "privateIpAddresses": [
                     {
                        "privateDnsName": "string",
                        "privateIpAddress": "string"
                     }
                  ],
                  "publicDnsName": "string",
                  "publicIp": "string",
                  "securityGroups": [
                     {
                        "groupId": "string",
                        "groupName": "string"
                     }
                  ],
                  "subnetId": "string",
                  "vpcId": "string"
               }
            ],
            "outpostArn": "string",
            "platform": "string",
            "productCodes": [
               {
                  "productCodeId": "string",
                  "productCodeType": "string"
               }
            ],
            "tags": [
```

```
                {
                   "key": "string",
                   "value": "string"
                }
             ]
          },
          "kubernetesDetails": {
             "kubernetesUserDetails": {
                "groups": [ "string" ],
                "impersonatedUser": {
                   "groups": [ "string" ],
                   "username": "string"
                },
                "sessionName": [ "string" ],
                "uid": "string",
                "username": "string"
             },
             "kubernetesWorkloadDetails": {
                "containers": [
                   {
                      "containerRuntime": "string",
                      "id": "string",
                      "image": "string",
                      "imagePrefix": "string",
                      "name": "string",
                      "securityContext": {
                         "allowPrivilegeEscalation": boolean,
                         "privileged": boolean
                      },
                      "volumeMounts": [
                         {
                            "mountPath": "string",
                            "name": "string"
                         }
                      ]
                   }
                ],
                "hostIPC": boolean,
                "hostNetwork": boolean,
                "hostPID": boolean,
                "name": "string",
                "namespace": "string",
                "serviceAccountName": "string",
                "type": "string",
```

```
            "uid": "string",
            "volumes": [
               {
                  "hostPath": {
                     "path": "string"
                  },
                  "name": "string"
               }
            ]
         }
      },
      "lambdaDetails": {
         "description": "string",
         "functionArn": "string",
         "functionName": "string",
         "functionVersion": "string",
         "lastModifiedAt": number,
         "revisionId": "string",
         "role": "string",
         "tags": [
            {
               "key": "string",
               "value": "string"
            }
         ],
         "vpcConfig": {
            "securityGroups": [
               {
                  "groupId": "string",
                  "groupName": "string"
               }
            ],
            "subnetIds": [ "string" ],
            "vpcId": "string"
         }
      },
      "modelDetails": [
         {
            "modelId": "string"
         }
      ],
      "rdsDbInstanceDetails": {
         "dbClusterIdentifier": "string",
         "dbInstanceArn": "string",
```

```
            "dbInstanceIdentifier": "string",
            "dbiResourceId": "string",
            "engine": "string",
            "engineVersion": "string",
            "tags": [
               {
                  "key": "string",
                  "value": "string"
               }
            ]
         },
         "rdsDbUserDetails": {
            "application": "string",
            "authMethod": "string",
            "database": "string",
            "ssl": "string",
            "user": "string"
         },
         "rdsLimitlessDbDetails": {
            "dbClusterIdentifier": "string",
            "dbShardGroupArn": "string",
            "dbShardGroupIdentifier": "string",
            "dbShardGroupResourceId": "string",
            "engine": "string",
            "engineVersion": "string",
            "tags": [
               {
                  "key": "string",
                  "value": "string"
               }
            ]
         },
         "recoveryPointDetails": {
            "backupVaultName": "string",
            "continuousScanDetails": {
               "endTime": number,
               "startTime": number
            },
            "recoveryPointArn": "string"
         },
         "resourceType": "string",
         "s3BucketDetails": [
            {
               "arn": "string",
```

```
            "createdAt": number,
            "defaultServerSideEncryption": {
               "encryptionType": "string",
               "kmsMasterKeyArn": "string"
            },
            "name": "string",
            "owner": {
               "id": "string"
            },
            "publicAccess": {
               "effectivePermission": "string",
               "permissionConfiguration": {
                  "accountLevelPermissions": {
                     "blockPublicAccess": {
                        "blockPublicAcls": boolean,
                        "blockPublicPolicy": boolean,
                        "ignorePublicAcls": boolean,
                        "restrictPublicBuckets": boolean
                     }
                  },
                  "bucketLevelPermissions": {
                     "accessControlList": {
                        "allowsPublicReadAccess": boolean,
                        "allowsPublicWriteAccess": boolean
                     },
                     "blockPublicAccess": {
                        "blockPublicAcls": boolean,
                        "blockPublicPolicy": boolean,
                        "ignorePublicAcls": boolean,
                        "restrictPublicBuckets": boolean
                     },
                     "bucketPolicy": {
                        "allowsPublicReadAccess": boolean,
                        "allowsPublicWriteAccess": boolean
                     }
                  }
               }
            },
            "s3ObjectDetails": [
               {
                  "eTag": "string",
                  "hash": "string",
                  "key": "string",
                  "objectArn": "string",
```

```
                        "versionId": "string"
                     }
                  ],
                  "tags": [
                     {
                        "key": "string",
                        "value": "string"
                     }
                  ],
                  "type": "string"
               }
            ]
         },
         "schemaVersion": "string",
         "service": {
            "action": {
               "actionType": "string",
               "awsApiCallAction": {
                  "affectedResources": {
                     "string" : "string"
                  },
                  "api": "string",
                  "callerType": "string",
                  "domainDetails": {
                     "domain": "string"
                  },
                  "errorCode": "string",
                  "remoteAccountDetails": {
                     "accountId": "string",
                     "affiliated": boolean,
                     "awsServiceName": "string"
                  },
                  "remoteIpDetails": {
                     "city": {
                        "cityName": "string"
                     },
                     "country": {
                        "countryCode": "string",
                        "countryName": "string"
                     },
                     "geoLocation": {
                        "lat": number,
                        "lon": number
                     },
```

```
                  "ipAddressV4": "string",
                  "ipAddressV6": "string",
                  "organization": {
                     "asn": "string",
                     "asnOrg": "string",
                     "isp": "string",
                     "org": "string"
                  }
               },
               "serviceName": "string",
               "userAgent": "string"
            },
            "dnsRequestAction": {
               "blocked": boolean,
               "domain": "string",
               "domainWithSuffix": "string",
               "protocol": "string",
               "vpcOwnerAccountId": "string"
            },
            "kubernetesApiCallAction": {
               "namespace": "string",
               "parameters": "string",
               "remoteIpDetails": {
                  "city": {
                     "cityName": "string"
                  },
                  "country": {
                     "countryCode": "string",
                     "countryName": "string"
                  },
                  "geoLocation": {
                     "lat": number,
                     "lon": number
                  },
                  "ipAddressV4": "string",
                  "ipAddressV6": "string",
                  "organization": {
                     "asn": "string",
                     "asnOrg": "string",
                     "isp": "string",
                     "org": "string"
                  }
               },
               "requestUri": "string",
```

```
            "resource": "string",
            "resourceName": "string",
            "sourceIPs": [ "string" ],
            "statusCode": number,
            "subresource": "string",
            "userAgent": "string",
            "verb": "string"
         },
         "kubernetesPermissionCheckedDetails": {
            "allowed": boolean,
            "namespace": "string",
            "resource": "string",
            "verb": "string"
         },
         "kubernetesRoleBindingDetails": {
            "kind": "string",
            "name": "string",
            "roleRefKind": "string",
            "roleRefName": "string",
            "uid": "string"
         },
         "kubernetesRoleDetails": {
            "kind": "string",
            "name": "string",
            "uid": "string"
         },
         "networkConnectionAction": {
            "blocked": boolean,
            "connectionDirection": "string",
            "localIpDetails": {
               "ipAddressV4": "string",
               "ipAddressV6": "string"
            },
            "localNetworkInterface": "string",
            "localPortDetails": {
               "port": number,
               "portName": "string"
            },
            "protocol": "string",
            "remoteIpDetails": {
               "city": {
                  "cityName": "string"
               },
               "country": {
```

```
                        "countryCode": "string",
                        "countryName": "string"
                     },
                     "geoLocation": {
                        "lat": number,
                        "lon": number
                     },
                     "ipAddressV4": "string",
                     "ipAddressV6": "string",
                     "organization": {
                        "asn": "string",
                        "asnOrg": "string",
                        "isp": "string",
                        "org": "string"
                     }
                  },
                  "remotePortDetails": {
                     "port": number,
                     "portName": "string"
                  }
               },
               "portProbeAction": {
                  "blocked": boolean,
                  "portProbeDetails": [
                     {
                        "localIpDetails": {
                           "ipAddressV4": "string",
                           "ipAddressV6": "string"
                        },
                        "localPortDetails": {
                           "port": number,
                           "portName": "string"
                        },
                        "remoteIpDetails": {
                           "city": {
                              "cityName": "string"
                           },
                           "country": {
                              "countryCode": "string",
                              "countryName": "string"
                           },
                           "geoLocation": {
                              "lat": number,
                              "lon": number
```

```
                        },
                        "ipAddressV4": "string",
                        "ipAddressV6": "string",
                        "organization": {
                           "asn": "string",
                           "asnOrg": "string",
                           "isp": "string",
                           "org": "string"
                        }
                     }
                  }
               ]
            },
            "rdsLoginAttemptAction": {
               "LoginAttributes": [
                  {
                     "application": "string",
                     "failedLoginAttempts": number,
                     "successfulLoginAttempts": number,
                     "user": "string"
                  }
               ],
               "remoteIpDetails": {
                  "city": {
                     "cityName": "string"
                  },
                  "country": {
                     "countryCode": "string",
                     "countryName": "string"
                  },
                  "geoLocation": {
                     "lat": number,
                     "lon": number
                  },
                  "ipAddressV4": "string",
                  "ipAddressV6": "string",
                  "organization": {
                     "asn": "string",
                     "asnOrg": "string",
                     "isp": "string",
                     "org": "string"
                  }
               }
            }
```

```
            },
            "additionalInfo": {
               "type": "string",
               "value": "string"
            },
            "archived": boolean,
            "count": number,
            "detection": {
               "anomaly": {
                  "profiles": {
                     "string" : {
                        "string" : [
                           {
                              "observations": {
                                 "number": [ number ],
                                 "text": [ "string" ]
                              },
                              "profileSubtype": "string",
                              "profileType": "string"
                           }
                        ]
                     }
                  },
                  "unusual": {
                     "behavior": {
                        "string" : {
                           "string" : {
                              "observations": {
                                 "number": [ number ],
                                 "text": [ "string" ]
                              },
                              "profileSubtype": "string",
                              "profileType": "string"
                           }
                        }
                     }
                  }
               },
               "sequence": {
                  "actors": [
                     {
                        "id": "string",
                        "process": {
                           "name": "string",
```

```
                  "path": "string",
                  "sha256": "string"
               },
               "session": {
                  "createdTime": number,
                  "issuer": "string",
                  "mfaStatus": "string",
                  "uid": "string"
               },
               "user": {
                  "account": {
                     "account": "string",
                     "uid": "string"
                  },
                  "credentialUid": "string",
                  "name": "string",
                  "type": "string",
                  "uid": "string"
               }
            }
         ],
         "additionalSequenceTypes": [ "string" ],
         "description": "string",
         "endpoints": [
            {
               "autonomousSystem": {
                  "name": "string",
                  "number": number
               },
               "connection": {
                  "direction": "string"
               },
               "domain": "string",
               "id": "string",
               "ip": "string",
               "location": {
                  "city": "string",
                  "country": "string",
                  "lat": number,
                  "lon": number
               },
               "port": number
            }
         ],
```

```
"resources": [
   {
      "accountId": "string",
      "cloudPartition": "string",
      "data": {
         "accessKey": {
            "principalId": "string",
            "userName": "string",
            "userType": "string"
         },
         "autoscalingAutoScalingGroup": {
            "ec2InstanceUids": [ "string" ]
         },
         "bedrockGuardrail": {
            "guardrailAction": "string",
            "guardrailSource": "string",
            "version": "string"
         },
         "cloudformationStack": {
            "ec2InstanceUids": [ "string" ]
         },
         "container": {
            "image": "string",
            "imageUid": "string"
         },
         "ec2Image": {
            "ec2InstanceUids": [ "string" ]
         },
         "ec2Instance": {
            "availabilityZone": "string",
            "ec2NetworkInterfaceUids": [ "string" ],
            "IamInstanceProfile": {
               "arn": "string",
               "id": "string"
            },
            "imageDescription": "string",
            "instanceState": "string",
            "instanceType": "string",
            "outpostArn": "string",
            "platform": "string",
            "productCodes": [
               {
                  "productCodeId": "string",
                  "productCodeType": "string"
```

```
            }
         ]
      },
      "ec2LaunchTemplate": {
         "ec2InstanceUids": [ "string" ],
         "version": "string"
      },
      "ec2NetworkInterface": {
         "ipv6Addresses": [ "string" ],
         "privateIpAddresses": [
            {
               "privateDnsName": "string",
               "privateIpAddress": "string"
            }
         ],
         "publicIp": "string",
         "securityGroups": [
            {
               "groupId": "string",
               "groupName": "string"
            }
         ],
         "subNetId": "string",
         "vpcId": "string"
      },
      "ec2Vpc": {
         "ec2InstanceUids": [ "string" ]
      },
      "ecsCluster": {
         "ec2InstanceUids": [ "string" ],
         "status": "string"
      },
      "ecsTask": {
         "containerUids": [ "string" ],
         "createdAt": number,
         "launchType": "string",
         "taskDefinitionArn": "string"
      },
      "eksCluster": {
         "arn": "string",
         "createdAt": number,
         "ec2InstanceUids": [ "string" ],
         "status": "string",
         "vpcId": "string"
```

```
            },
            "iamInstanceProfile": {
               "ec2InstanceUids": [ "string" ]
            },
            "kubernetesWorkload": {
               "containerUids": [ "string" ],
               "type": "string",
               "namespace": "string"
            },
            "s3Bucket": {
               "accountPublicAccess": {
                  "publicAclAccess": "string",
                  "publicAclIgnoreBehavior": "string",
                  "publicBucketRestrictBehavior": "string",
                  "publicPolicyAccess": "string"
               },
               "bucketPublicAccess": {
                  "publicAclAccess": "string",
                  "publicAclIgnoreBehavior": "string",
                  "publicBucketRestrictBehavior": "string",
                  "publicPolicyAccess": "string"
               },
               "createdAt": number,
               "effectivePermission": "string",
               "encryptionKeyArn": "string",
               "encryptionType": "string",
               "ownerId": "string",
               "publicReadAccess": "string",
               "publicWriteAccess": "string",
               "s3ObjectUids": [ "string" ]
            },
            "s3Object": {
               "eTag": "string",
               "key": "string",
               "versionId": "string"
            }
         },
         "name": "string",
         "region": "string",
         "resourceType": "string",
         "service": "string",
         "tags": [
            {
               "key": "string",
```

```
                        "value": "string"
                     }
                  ],
                  "uid": "string"
               }
            ],
            "sequenceIndicators": [
               {
                  "key": "string",
                  "title": "string",
                  "values": [ "string" ]
               }
            ],
            "signals": [
               {
                  "activities": [
                     {
                        "api": {
                           "error": "string",
                           "operation": "string",
                           "service": "string",
                           "userAgent": "string"
                        },
                        "type": "string"
                     }
                  ],
                  "actorIds": [ "string" ],
                  "count": number,
                  "createdAt": number,
                  "description": "string",
                  "endpointIds": [ "string" ],
                  "firstSeenAt": number,
                  "lastSeenAt": number,
                  "name": "string",
                  "resourceUids": [ "string" ],
                  "severity": number,
                  "signalIndicators": [
                     {
                        "key": "string",
                        "title": "string",
                        "values": [ "string" ]
                     }
                  ],
                  "type": "string",
```

```
                        "uid": "string",
                        "updatedAt": number
                     }
                  ],
                  "uid": "string"
               }
            },
            "detectorId": "string",
            "ebsVolumeScanDetails": {
               "scanCompletedAt": number,
               "scanDetections": {
                  "highestSeverityThreatDetails": {
                     "count": number,
                     "severity": "string",
                     "threatName": "string"
                  },
                  "scannedItemCount": {
                     "files": number,
                     "totalGb": number,
                     "volumes": number
                  },
                  "threatDetectedByName": {
                     "itemCount": number,
                     "shortened": boolean,
                     "threatNames": [
                        {
                           "filePaths": [
                              {
                                 "fileName": "string",
                                 "filePath": "string",
                                 "hash": "string",
                                 "volumeArn": "string"
                              }
                           ],
                           "itemCount": number,
                           "name": "string",
                           "severity": "string"
                        }
                     ],
                     "uniqueThreatNameCount": number
                  },
                  "threatsDetectedItemCount": {
                     "files": number
                  }
```

```
            },
            "scanId": "string",
            "scanStartedAt": number,
            "scanType": "string",
            "sources": [ "string" ],
            "triggerFindingId": "string"
         },
         "eventFirstSeen": "string",
         "eventLastSeen": "string",
         "evidence": {
            "threatIntelligenceDetails": [
               {
                  "threatFileSha256": "string",
                  "threatListName": "string",
                  "threatNames": [ "string" ]
               }
            ]
         },
         "featureName": "string",
         "malwareScanDetails": {
            "scanCategory": "string",
            "scanConfiguration": {
               "incrementalScanDetails": {
                  "baselineResourceArn": "string"
               },
               "triggerType": "string"
            },
            "scanId": "string",
            "scanType": "string",
            "threats": [
               {
                  "count": number,
                  "hash": "string",
                  "itemDetails": [
                     {
                        "additionalInfo": {
                           "deviceName": "string",
                           "versionId": "string"
                        },
                        "hash": "string",
                        "itemPath": "string",
                        "resourceArn": "string"
                     }
                  ],
```

```
                  "itemPaths": [
                     {
                        "hash": "string",
                        "nestedItemPath": "string"
                     }
                  ],
                  "name": "string",
                  "source": "string"
               }
            ],
            "uniqueThreatCount": number
         },
         "resourceRole": "string",
         "runtimeDetails": {
            "context": {
               "addressFamily": "string",
               "commandLineExample": "string",
               "fileOperation": "string",
               "filePath": "string",
               "fileSystemType": "string",
               "flags": [ "string" ],
               "ianaProtocolNumber": number,
               "ldPreloadValue": "string",
               "libraryPath": "string",
               "memoryRegions": [ "string" ],
               "modifiedAt": number,
               "modifyingProcess": {
                  "euid": number,
                  "executablePath": "string",
                  "executableSha256": "string",
                  "lineage": [
                     {
                        "euid": number,
                        "executablePath": "string",
                        "name": "string",
                        "namespacePid": number,
                        "parentUuid": "string",
                        "pid": number,
                        "startTime": number,
                        "userId": number,
                        "uuid": "string"
                     }
                  ],
                  "name": "string",
```

```
            "namespacePid": number,
            "parentUuid": "string",
            "pid": number,
            "pwd": "string",
            "startTime": number,
            "user": "string",
            "userId": number,
            "uuid": "string"
         },
         "moduleFilePath": "string",
         "moduleName": "string",
         "moduleSha256": "string",
         "mountSource": "string",
         "mountTarget": "string",
         "relatedFilePaths": [ "string" ],
         "releaseAgentPath": "string",
         "runcBinaryPath": "string",
         "scriptPath": "string",
         "serviceName": "string",
         "shellHistoryFilePath": "string",
         "socketPath": "string",
         "targetProcess": {
            "euid": number,
            "executablePath": "string",
            "executableSha256": "string",
            "lineage": [
               {
                  "euid": number,
                  "executablePath": "string",
                  "name": "string",
                  "namespacePid": number,
                  "parentUuid": "string",
                  "pid": number,
                  "startTime": number,
                  "userId": number,
                  "uuid": "string"
               }
            ],
            "name": "string",
            "namespacePid": number,
            "parentUuid": "string",
            "pid": number,
            "pwd": "string",
            "startTime": number,
```

```
                    "user": "string",
                    "userId": number,
                    "uuid": "string"
                 },
                 "threatFilePath": "string",
                 "toolCategory": "string",
                 "toolName": "string"
              },
              "process": {
                 "euid": number,
                 "executablePath": "string",
                 "executableSha256": "string",
                 "lineage": [
                    {
                       "euid": number,
                       "executablePath": "string",
                       "name": "string",
                       "namespacePid": number,
                       "parentUuid": "string",
                       "pid": number,
                       "startTime": number,
                       "userId": number,
                       "uuid": "string"
                    }
                 ],
                 "name": "string",
                 "namespacePid": number,
                 "parentUuid": "string",
                 "pid": number,
                 "pwd": "string",
                 "startTime": number,
                 "user": "string",
                 "userId": number,
                 "uuid": "string"
              }
           },
           "serviceName": "string",
           "userFeedback": "string"
        },
        "severity": number,
        "title": "string",
        "type": "string",
        "updatedAt": "string"
     }
```

```
    ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

findings

A list of findings.

Type: Array of Finding objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetFindingsStatistics

Lists GuardDuty findings statistics for the specified detector ID.

You must provide either `findingStatisticTypes` or `groupBy` parameter, and not both. You can use the `maxResults` and `orderBy` parameters only when using `groupBy`.

There might be regional differences because some flags might not be available in all the Regions where GuardDuty is currently supported. For more information, see Regions and endpoints.

Request Syntax

```
POST /detector/DetectorId/findings/statistics HTTP/1.1
Content-type: application/json

{
   "findingCriteria": {
      "criterion": {
         "string" : {
            "eq": [ "string" ],
            "equals": [ "string" ],
            "greaterThan": number,
            "greaterThanOrEqual": number,
            "gt": number,
            "gte": number,
            "lessThan": number,
            "lessThanOrEqual": number,
            "lt": number,
            "lte": number,
            "matches": [ "string" ],
            "neq": [ "string" ],
            "notEquals": [ "string" ],
            "notMatches": [ "string" ]
         }
      }
   },
   "findingStatisticTypes": [ "string" ],
   "groupBy": "string",
   "maxResults": number,
   "orderBy": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The ID of the detector whose findings statistics you want to retrieve.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

findingCriteria

Represents the criteria that is used for querying findings.

Type: FindingCriteria object

Required: No

findingStatisticTypes

This parameter has been deprecated.

The types of finding statistics to retrieve.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 10 items.

Valid Values: `COUNT_BY_SEVERITY`

Required: No

groupBy

Displays the findings statistics grouped by one of the listed valid values.

Type: String

Valid Values: `ACCOUNT | DATE | FINDING_TYPE | RESOURCE | SEVERITY`

Required: No

maxResults

The maximum number of results to be returned in the response. The default value is 25.

You can use this parameter only with the `groupBy` parameter.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

orderBy

Displays the sorted findings in the requested order. The default value of `orderBy` is `DESC`.

You can use this parameter only with the `groupBy` parameter.

Type: String

Valid Values: `ASC | DESC`

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "findingStatistics": {
      "countBySeverity": {
         "string" : number
      },
      "groupedByAccount": [
         {
            "accountId": "string",
            "lastGeneratedAt": number,
```

```
            "totalFindings": number
         }
      ],
      "groupedByDate": [
         {
            "date": number,
            "lastGeneratedAt": number,
            "severity": number,
            "totalFindings": number
         }
      ],
      "groupedByFindingType": [
         {
            "findingType": "string",
            "lastGeneratedAt": number,
            "totalFindings": number
         }
      ],
      "groupedByResource": [
         {
            "accountId": "string",
            "lastGeneratedAt": number,
            "resourceId": "string",
            "resourceType": "string",
            "totalFindings": number
         }
      ],
      "groupedBySeverity": [
         {
            "lastGeneratedAt": number,
            "severity": number,
            "totalFindings": number
         }
      ]
   },
   "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

findingStatistics

The finding statistics object.

Type: FindingStatistics object

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

This parameter is currently not supported.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetInvestigation

This API is currently available as a preview. This feature is available in the following AWS Regions: US East (N. Virginia), US East (Ohio), US West (Oregon), Canada (Central), Europe (Frankfurt), Europe (Ireland), Europe (London), Europe (Paris), Europe (Stockholm), and Asia Pacific (Tokyo).

Retrieves the results and status of a specific GuardDuty investigation.

An administrator account can retrieve any investigation within the organization. Member accounts can only retrieve investigations that belong to them.

Request Syntax

```
GET /detector/DetectorId/investigation/InvestigationId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the GuardDuty detector associated with the investigation.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

InvestigationId

The unique identifier of the investigation to retrieve.

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-fA-F0-9\-]+`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "investigation": {
      "cloud": {
         "account": "string",
         "provider": "string",
         "region": "string"
      },
      "confidence": "string",
      "endTime": number,
      "error": "string",
      "investigationId": "string",
      "metadata": {
         "product": {
            "feature": "string",
            "name": "string"
         },
         "version": "string"
      },
      "risk": "string",
      "riskLevel": "string",
      "startTime": number,
      "status": "string",
      "summary": "string",
      "triggeredBy": "string",
      "triggerPrompt": "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

investigation

The details and results of the requested investigation.

Type: Investigation object

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

ResourceNotFoundException

The requested resource can't be found.

Message

The error message.

Type

The error type.

HTTP Status Code: 404

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetInvitationsCount

Returns the count of all GuardDuty membership invitations that were sent to the current member account except the currently accepted invitation.

Request Syntax

```
GET /invitation/count HTTP/1.1
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "invitationsCount": number
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

invitationsCount

The number of received invitations.

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetIPSet

Retrieves the IPSet specified by the `ipSetId`.

Request Syntax

```
GET /detector/DetectorId/ipset/IpSetId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector that is associated with the IPSet.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

IpSetId

The unique ID of the IPSet to retrieve.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "expectedBucketOwner": "string",
```

```
   "format": "string",
   "location": "string",
   "name": "string",
   "status": "string",
   "tags": {
      "string" : "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

expectedBucketOwner

The AWS account ID that owns the Amazon S3 bucket specified in the **location** parameter. This field appears in the response only if it was provided during IPSet creation or update.

Type: String

Length Constraints: Fixed length of 12.

format

The format of the file that contains the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `TXT | STIX | OTX_CSV | ALIEN_VAULT | PROOF_POINT | FIRE_EYE`

location

The URI of the file that contains the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

name

The user-friendly name for the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

status

The status of IPSet file that was uploaded.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `INACTIVE | ACTIVATING | ACTIVE | DEACTIVATING | ERROR | DELETE_PENDING | DELETED`

tags

The tags of the IPSet resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetMalwareProtectionPlan

Retrieves the Malware Protection plan details associated with a Malware Protection plan ID.

Request Syntax

```
GET /malware-protection-plan/MalwareProtectionPlanId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

MalwareProtectionPlanId

A unique identifier associated with Malware Protection plan resource.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "actions": {
      "tagging": {
         "status": "string"
      }
   },
   "arn": "string",
   "createdAt": number,
   "protectedResource": {
      "s3Bucket": {
         "bucketName": "string",
         "objectPrefixes": [ "string" ]
      }
```

```
   },
   "role": "string",
   "status": "string",
   "statusReasons": [
      {
         "code": "string",
         "message": "string"
      }
   ],
   "tags": {
      "string" : "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

actions

Information about whether the tags will be added to the S3 object after scanning.

Type: MalwareProtectionPlanActions object

arn

Amazon Resource Name (ARN) of the protected resource.

Type: String

createdAt

The timestamp when the Malware Protection plan resource was created.

Type: Timestamp

protectedResource

Information about the protected resource that is associated with the created Malware Protection plan. Presently, `S3Bucket` is the only supported protected resource.

Type: CreateProtectedResource object

role

Amazon Resource Name (ARN) of the IAM role that includes the permissions to scan and add tags to the associated protected resource.

Type: String

status

Malware Protection plan status.

Type: String

Valid Values: `ACTIVE | WARNING | ERROR`

statusReasons

Information about the issue code and message associated to the status of your Malware Protection plan.

Type: Array of MalwareProtectionPlanStatusReason objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

tags

Tags added to the Malware Protection plan resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

ResourceNotFoundException

The requested resource can't be found.

Message

The error message.

Type

The error type.

HTTP Status Code: 404

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetMalwareScan

Retrieves the detailed information for a specific malware scan. Each member account can view the malware scan details for their own account. An administrator can view malware scan details for all accounts in the organization.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see Regions and endpoints.

Request Syntax

```
GET /malware-scan/ScanId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ScanId

A unique identifier that gets generated when you invoke the API without any error. Each malware scan has a corresponding scan ID. Using this scan ID, you can monitor the status of your malware scan.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "adminDetectorId": "string",
   "detectorId": "string",
   "failedResourcesCount": number,
   "resourceArn": "string",
```

```
   "resourceType": "string",
   "scanCategory": "string",
   "scanCompletedAt": number,
   "scanConfiguration": {
      "incrementalScanDetails": {
         "baselineResourceArn": "string"
      },
      "recoveryPoint": {
         "backupVaultName": "string",
         "continuousScanDetails": {
            "endTime": number,
            "startTime": number
         }
      },
      "role": "string",
      "triggerDetails": {
         "description": "string",
         "guardDutyFindingId": "string",
         "triggerType": "string"
      }
   },
   "scanId": "string",
   "scannedResources": [
      {
         "resourceDetails": {
            "ebsSnapshot": {
               "deviceName": "string"
            },
            "ebsVolume": {
               "deviceName": "string",
               "encryptionType": "string",
               "kmsKeyArn": "string",
               "snapshotArn": "string",
               "volumeArn": "string",
               "volumeSizeInGB": number,
               "volumeType": "string"
            }
         },
         "scannedResourceArn": "string",
         "scannedResourceStatus": "string",
         "scannedResourceType": "string",
         "scanStatusReason": "string"
      }
   ],
```

```
   "scannedResourcesCount": number,
   "scanResultDetails": {
      "failedFileCount": number,
      "scanResultStatus": "string",
      "skippedFileCount": number,
      "threatFoundFileCount": number,
      "threats": [
         {
            "count": number,
            "hash": "string",
            "itemDetails": [
               {
                  "additionalInfo": {
                     "deviceName": "string",
                     "versionId": "string"
                  },
                  "hash": "string",
                  "itemPath": "string",
                  "resourceArn": "string"
               }
            ],
            "name": "string",
            "source": "string"
         }
      ],
      "totalBytes": number,
      "totalFileCount": number,
      "uniqueThreatCount": number
   },
   "scanStartedAt": number,
   "scanStatus": "string",
   "scanStatusReason": "string",
   "scanType": "string",
   "skippedResourcesCount": number
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

adminDetectorId

The unique detector ID of the administrator account that the request is associated with. If the account is an administrator, the `AdminDetectorId` will be the same as the one used for `DetectorId. If the customer is not a GuardDuty customer, this field will not be present..`

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

detectorId

The unique ID of the detector that is associated with the request, if it belongs to an account which is a GuardDuty customer.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

failedResourcesCount

The total number of resources that failed to be scanned.

Type: Integer

Valid Range: Minimum value of 0.

resourceArn

Amazon Resource Name (ARN) of the resource on which a malware scan was invoked.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

resourceType

The type of resource that was scanned for malware.

Type: String

Valid Values: `EBS_RECOVERY_POINT | EBS_SNAPSHOT | EBS_VOLUME | EC2_AMI | EC2_INSTANCE | EC2_RECOVERY_POINT | S3_RECOVERY_POINT | S3_BUCKET | S3_POINT_IN_TIME_RECOVERY`

scanCategory

The category of the malware scan, indicating the type of scan performed.

Type: String

Valid Values: `FULL_SCAN | INCREMENTAL_SCAN`

scanCompletedAt

The timestamp representing when the malware scan was completed.

Type: Timestamp

scanConfiguration

Information about the scan configuration used for the malware scan.

Type: ScanConfiguration object

scanId

A unique identifier associated with the malware scan. Each malware scan has a corresponding scan ID. Using this scan ID, you can monitor the status of your malware scan.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

scannedResources

A list of resources along with their metadata that were scanned as part of the malware scan operation.

Type: Array of ScannedResource objects

scannedResourcesCount

The total number of resources that were successfully scanned. This is dependent on the resource type.

Type: Integer

Valid Range: Minimum value of 0.

scanResultDetails

Detailed information about the results of the malware scan, if the scan completed.

Type: GetMalwareScanResultDetails object

scanStartedAt

The timestamp representing when the malware scan was started.

Type: Timestamp

scanStatus

A value representing the current status of the malware scan.

Type: String

Valid Values: `RUNNING | COMPLETED | COMPLETED_WITH_ISSUES | FAILED | SKIPPED`

scanStatusReason

Represents the reason for the current scan status, if applicable.

Type: String

Valid Values: `ACCESS_DENIED | RESOURCE_NOT_FOUND | SNAPSHOT_SIZE_LIMIT_EXCEEDED | RESOURCE_UNAVAILABLE | INCONSISTENT_SOURCE | INCREMENTAL_NO_DIFFERENCE | NO_EBS_VOLUMES_FOUND | UNSUPPORTED_PRODUCT_CODE_TYPE | AMI_SNAPSHOT_LIMIT_EXCEEDED | UNRELATED_RESOURCES | BASE_RESOURCE_NOT_SCANNED | BASE_CREATED_AFTER_TARGET | UNSUPPORTED_FOR_INCREMENTAL | UNSUPPORTED_AMI | UNSUPPORTED_SNAPSHOT | UNSUPPORTED_COMPOSITE_RECOVERY_POINT | ALL_FILES_SKIPPED_OR_FAILED`

scanType

A value representing the initiator of the scan.

Type: String

Valid Values: `BACKUP_INITIATED | ON_DEMAND | GUARDDUTY_INITIATED`

skippedResourcesCount

The total number of resources that were skipped during the scan.

Type: Integer

Valid Range: Minimum value of 0.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

ResourceNotFoundException

The requested resource can't be found.

Message

The error message.

Type

The error type.

HTTP Status Code: 404

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetMalwareScanSettings

Returns the details of the malware scan settings.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see Regions and endpoints.

Request Syntax

```
GET /detector/DetectorId/malware-scan-settings HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector that is associated with this scan.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "ebsSnapshotPreservation": "string",
```

```
   "scanResourceCriteria": {
      "exclude": {
         "string" : {
            "mapEquals": [
               {
                  "key": "string",
                  "value": "string"
               }
            ]
         }
      },
      "include": {
         "string" : {
            "mapEquals": [
               {
                  "key": "string",
                  "value": "string"
               }
            ]
         }
      }
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

ebsSnapshotPreservation

An enum value representing possible snapshot preservation settings.

Type: String

Valid Values: `NO_RETENTION | RETENTION_WITH_FINDING`

scanResourceCriteria

Represents the criteria to be used in the filter for scanning resources.

Type: ScanResourceCriteria object

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetMasterAccount

This action has been deprecated.

Provides the details for the GuardDuty administrator account associated with the current GuardDuty member account.

Request Syntax

```
GET /detector/DetectorId/master HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty member account.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "master": {
      "accountId": "string",
      "invitationId": "string",
      "invitedAt": "string",
```

```
      "relationshipStatus": "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

master

The administrator account details.

Type: Master object

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetMemberDetectors

Describes which data sources are enabled for the member account's detector.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see Regions and endpoints.

Request Syntax

```
POST /detector/DetectorId/member/detector/get HTTP/1.1
Content-type: application/json

{
   "accountIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The detector ID for the administrator account.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds

A list of member account IDs.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "members": [
      {
         "accountId": "string",
         "dataSources": {
            "cloudTrail": {
               "status": "string"
            },
            "dnsLogs": {
               "status": "string"
            },
            "flowLogs": {
               "status": "string"
            },
            "kubernetes": {
               "auditLogs": {
                  "status": "string"
               }
            },
            "malwareProtection": {
               "scanEc2InstanceWithFindings": {
                  "ebsVolumes": {
                     "reason": "string",
                     "status": "string"
                  }
               },
               "serviceRole": "string"
            },
            "s3Logs": {
               "status": "string"
            }
         },
```

```
         "features": [
            {
               "additionalConfiguration": [
                  {
                     "managedBy": "string",
                     "name": "string",
                     "status": "string",
                     "updatedAt": number
                  }
               ],
               "managedBy": "string",
               "name": "string",
               "status": "string",
               "updatedAt": number
            }
         ]
      }
   ],
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

members

An object that describes which data sources are enabled for a member account.

Type: Array of MemberDataSourceConfiguration objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

unprocessedAccounts

A list of member account IDs that were unable to be processed along with an explanation for why they were not processed.

Type: Array of UnprocessedAccount objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetMembers

Retrieves GuardDuty member accounts (of the current GuardDuty administrator account) specified by the account IDs.

Request Syntax

```
POST /detector/DetectorId/member/get HTTP/1.1
Content-type: application/json

{
   "accountIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty account whose members you want to retrieve.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds

A list of account IDs of the GuardDuty member accounts that you want to describe.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "members": [
      {
         "accountId": "string",
         "administratorId": "string",
         "detectorId": "string",
         "email": "string",
         "invitedAt": "string",
         "masterId": "string",
         "relationshipStatus": "string",
         "updatedAt": "string"
      }
   ],
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

members

A list of members.

Type: Array of Member objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

unprocessedAccounts

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of UnprocessedAccount objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetOrganizationStatistics

Retrieves how many active member accounts have each feature enabled within GuardDuty. Only a delegated GuardDuty administrator of an organization can run this API.

When you create a new organization, it might take up to 24 hours to generate the statistics for the entire organization.

Request Syntax

```
GET /organization/statistics HTTP/1.1
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "organizationDetails": {
      "organizationStatistics": {
         "activeAccountsCount": number,
         "countByFeature": [
            {
               "additionalConfiguration": [
                  {
                     "enabledAccountsCount": number,
                     "name": "string"
                  }
               ],
               "enabledAccountsCount": number,
               "name": "string"
            }
         ],
```

```
            "enabledAccountsCount": number,
            "memberAccountsCount": number,
            "totalAccountsCount": number
        },
        "updatedAt": number
    }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

organizationDetails

Information about the statistics report for your organization.

Type: OrganizationDetails object

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetRemainingFreeTrialDays

Provides the number of days left for each data source used in the free trial period.

Request Syntax

```
POST /detector/DetectorId/freeTrial/daysRemaining HTTP/1.1
Content-type: application/json

{
   "accountIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty member account.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds

A list of account identifiers of the GuardDuty member account.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "accounts": [
      {
         "accountId": "string",
         "dataSources": {
            "cloudTrail": {
               "freeTrialDaysRemaining": number
            },
            "dnsLogs": {
               "freeTrialDaysRemaining": number
            },
            "flowLogs": {
               "freeTrialDaysRemaining": number
            },
            "kubernetes": {
               "auditLogs": {
                  "freeTrialDaysRemaining": number
               }
            },
            "malwareProtection": {
               "scanEc2InstanceWithFindings": {
                  "freeTrialDaysRemaining": number
               }
            },
            "s3Logs": {
               "freeTrialDaysRemaining": number
            }
         },
         "features": [
            {
               "freeTrialDaysRemaining": number,
               "name": "string"
            }
         ]
```

```
      }
   ],
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

accounts

The member accounts which were included in a request and were processed successfully.

Type: Array of AccountFreeTrialInfo objects

unprocessedAccounts

The member account that was included in a request but for which the request could not be processed.

Type: Array of UnprocessedAccount objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetThreatEntitySet

Retrieves the threat entity set associated with the specified `threatEntitySetId`.

Request Syntax

```
GET /detector/DetectorId/threatentityset/ThreatEntitySetId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector associated with the threat entity set resource.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

ThreatEntitySetId

The unique ID that helps GuardDuty identify the threat entity set.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "createdAt": number,
   "errorDetails": "string",
```

```
   "expectedBucketOwner": "string",
   "format": "string",
   "location": "string",
   "name": "string",
   "status": "string",
   "tags": {
      "string" : "string"
   },
   "updatedAt": number
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

createdAt

The timestamp when the associated threat entity set was created.

Type: Timestamp

errorDetails

The error details when the status is shown as ERROR.

Type: String

expectedBucketOwner

The AWS account ID that owns the Amazon S3 bucket specified in the **location** parameter.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `[0-9]+`

format

The format of the file that contains the threat entity set.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `TXT | STIX | OTX_CSV | ALIEN_VAULT | PROOF_POINT | FIRE_EYE`

location

The URI of the file that contains the threat entity set.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

name

The name of the threat entity set associated with the specified `threatEntitySetId`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

status

The status of the associated threat entity set.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `INACTIVE | ACTIVATING | ACTIVE | DEACTIVATING | ERROR | DELETE_PENDING | DELETED`

tags

The tags associated with the threat entity set resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

updatedAt

The timestamp when the associated threat entity set was updated.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetThreatIntelSet

Retrieves the ThreatIntelSet that is specified by the ThreatIntelSet ID.

Request Syntax

```
GET /detector/DetectorId/threatintelset/ThreatIntelSetId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector that is associated with the threatIntelSet.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

ThreatIntelSetId

The unique ID of the threatIntelSet that you want to get.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "expectedBucketOwner": "string",
   "format": "string",
```

```
   "location": "string",
   "name": "string",
   "status": "string",
   "tags": {
      "string" : "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

expectedBucketOwner

The AWS account ID that owns the Amazon S3 bucket specified in the **location** parameter. This field appears in the response only if it was provided during ThreatIntelSet creation or update.

Type: String

Length Constraints: Fixed length of 12.

format

The format of the threatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `TXT | STIX | OTX_CSV | ALIEN_VAULT | PROOF_POINT | FIRE_EYE`

location

The URI of the file that contains the ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

name

A user-friendly ThreatIntelSet name displayed in all findings that are generated by activity that involves IP addresses included in this ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

status

The status of threatIntelSet file uploaded.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `INACTIVE | ACTIVATING | ACTIVE | DEACTIVATING | ERROR | DELETE_PENDING | DELETED`

tags

The tags of the threat list resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetTrustedEntitySet

Retrieves the trusted entity set associated with the specified `trustedEntitySetId`.

Request Syntax

```
GET /detector/DetectorId/trustedentityset/TrustedEntitySetId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the GuardDuty detector associated with this trusted entity set.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

TrustedEntitySetId

The unique ID that helps GuardDuty identify the trusted entity set.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "createdAt": number,
   "errorDetails": "string",
   "expectedBucketOwner": "string",
   "format": "string",
   "location": "string",
```

```
   "name": "string",
   "status": "string",
   "tags": {
      "string" : "string"
   },
   "updatedAt": number
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

createdAt

The timestamp when the associated trusted entity set was created.

Type: Timestamp

errorDetails

The error details when the status is shown as ERROR.

Type: String

expectedBucketOwner

The AWS account ID that owns the Amazon S3 bucket specified in the **location** parameter.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `[0-9]+`

format

The format of the file that contains the trusted entity set.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `TXT | STIX | OTX_CSV | ALIEN_VAULT | PROOF_POINT | FIRE_EYE`

location

The URI of the file that contains the trusted entity set.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

name

The name of the threat entity set associated with the specified `trustedEntitySetId`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

status

The status of the associated trusted entity set.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `INACTIVE | ACTIVATING | ACTIVE | DEACTIVATING | ERROR | DELETE_PENDING | DELETED`

tags

The tags associated with trusted entity set resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

updatedAt

The timestamp when the associated trusted entity set was updated.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetUsageStatistics

Lists Amazon GuardDuty usage statistics over the last 30 days for the specified detector ID. For newly enabled detectors or data sources, the cost returned will include only the usage so far under 30 days. This may differ from the cost metrics in the console, which project usage over 30 days to provide a monthly cost estimate. For more information, see Understanding How Usage Costs are Calculated.

Request Syntax

```
POST /detector/DetectorId/usage/statistics HTTP/1.1
Content-type: application/json

{
   "maxResults": number,
   "nextToken": "string",
   "unit": "string",
   "usageCriteria": {
      "accountIds": [ "string" ],
      "dataSources": [ "string" ],
      "features": [ "string" ],
      "resources": [ "string" ]
   },
   "usageStatisticsType": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The ID of the detector that specifies the GuardDuty service whose usage statistics you want to retrieve.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

maxResults

The maximum number of results to return in the response.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 50.

Required: No

nextToken

A token to use for paginating results that are returned in the response. Set the value of this parameter to null for the first request to a list action. For subsequent calls, use the NextToken value returned from the previous request to continue listing results after the first page.

Type: String

Required: No

unit

The currency unit you would like to view your usage statistics in. Current valid values are USD.

Type: String

Required: No

usageCriteria

Represents the criteria used for querying usage.

Type: UsageCriteria object

Required: Yes

usageStatisticsType

The type of usage statistics to retrieve.

Type: String

Valid Values: SUM_BY_ACCOUNT | SUM_BY_DATA_SOURCE | SUM_BY_RESOURCE | TOP_RESOURCES | SUM_BY_FEATURES | TOP_ACCOUNTS_BY_FEATURE

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "nextToken": "string",
   "usageStatistics": {
      "sumByAccount": [
         {
            "accountId": "string",
            "total": {
               "amount": "string",
               "unit": "string"
            }
         }
      ],
      "sumByDataSource": [
         {
            "dataSource": "string",
            "total": {
               "amount": "string",
               "unit": "string"
            }
         }
      ],
      "sumByFeature": [
         {
            "feature": "string",
            "total": {
               "amount": "string",
               "unit": "string"
            }
         }
      ],
```

```
      "sumByResource": [
         {
            "resource": "string",
            "total": {
               "amount": "string",
               "unit": "string"
            }
         }
      ],
      "topAccountsByFeature": [
         {
            "accounts": [
               {
                  "accountId": "string",
                  "total": {
                     "amount": "string",
                     "unit": "string"
                  }
               }
            ],
            "feature": "string"
         }
      ],
      "topResources": [
         {
            "resource": "string",
            "total": {
               "amount": "string",
               "unit": "string"
            }
         }
      ]
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

usageStatistics

The usage statistics object. If a UsageStatisticType was provided, the objects representing other types will be null.

Type: UsageStatistics object

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

InviteMembers

Invites AWS accounts to become members of an organization administered by the AWS account that invokes this API. If you are using AWS Organizations to manage your GuardDuty environment, this step is not needed. For more information, see Managing accounts with organizations.

To invite AWS accounts, the first step is to ensure that GuardDuty has been enabled in the potential member accounts. You can now invoke this API to add accounts by invitation. The invited accounts can either accept or decline the invitation from their GuardDuty accounts. Each invited AWS account can choose to accept the invitation from only one AWS account. For more information, see Managing GuardDuty accounts by invitation.

After the invite has been accepted and you choose to disassociate a member account (by using DisassociateMembers) from your account, the details of the member account obtained by invoking CreateMembers, including the associated email addresses, will be retained. This is done so that you can invoke InviteMembers without the need to invoke CreateMembers again. To remove the details associated with a member account, you must also invoke DeleteMembers.

If you disassociate a member account that was added by invitation, the member account details obtained from this API, including the associated email addresses, will be retained. This is done so that the delegated administrator can invoke the InviteMembers API without the need to invoke the CreateMembers API again. To remove the details associated with a member account, the delegated administrator must invoke the DeleteMembers API.

When the member accounts added through AWS Organizations are later disassociated, you (administrator) can't invite them by calling the InviteMembers API. You can create an association with these member accounts again only by calling the CreateMembers API.

Request Syntax

```
POST /detector/DetectorId/member/invite HTTP/1.1
Content-type: application/json

{
   "accountIds": [ "string" ],
   "disableEmailNotification": boolean,
   "message": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty account with which you want to invite members.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds

A list of account IDs of the accounts that you want to invite to GuardDuty as members.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

disableEmailNotification

A Boolean value that specifies whether you want to disable email notification to the accounts that you are inviting to GuardDuty as members.

Type: Boolean

Required: No

message

The invitation message that you want to send to the accounts that you're inviting to GuardDuty as members.

Type: String

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

unprocessedAccounts

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of UnprocessedAccount objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListCoverage

Lists coverage details for your GuardDuty account. If you're a GuardDuty administrator, you can retrieve all resources associated with the active member accounts in your organization.

Make sure the accounts have Runtime Monitoring enabled and GuardDuty agent running on their resources.

Request Syntax

```
POST /detector/DetectorId/coverage HTTP/1.1
Content-type: application/json

{
   "filterCriteria": {
      "filterCriterion": [
         {
            "criterionKey": "string",
            "filterCondition": {
               "equals": [ "string" ],
               "notEquals": [ "string" ]
            }
         }
      ]
   },
   "maxResults": number,
   "nextToken": "string",
   "sortCriteria": {
      "attributeName": "string",
      "orderBy": "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector whose coverage details you want to retrieve.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

filterCriteria

Represents the criteria used to filter the coverage details.

Type: CoverageFilterCriteria object

Required: No

maxResults

The maximum number of results to return in the response.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 50.

Required: No

nextToken

A token to use for paginating results that are returned in the response. Set the value of this parameter to null for the first request to a list action. For subsequent calls, use the NextToken value returned from the previous request to continue listing results after the first page.

Type: String

Required: No

sortCriteria

Represents the criteria used to sort the coverage details.

Type: CoverageSortCriteria object

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "nextToken": "string",
   "resources": [
      {
         "accountId": "string",
         "coverageStatus": "string",
         "detectorId": "string",
         "issue": "string",
         "resourceDetails": {
            "ec2InstanceDetails": {
               "agentDetails": {
                  "version": "string"
               },
               "clusterArn": "string",
               "instanceId": "string",
               "instanceType": "string",
               "managementType": "string"
            },
            "ecsClusterDetails": {
               "clusterName": "string",
               "containerInstanceDetails": {
                  "compatibleContainerInstances": number,
                  "coveredContainerInstances": number
               },
               "fargateDetails": {
                  "issues": [ "string" ],
                  "managementType": "string"
               }
            },
            "eksClusterDetails": {
               "addonDetails": {
                  "addonStatus": "string",
                  "addonVersion": "string"
               },
```

```
                "clusterName": "string",
                "compatibleNodes": number,
                "coveredNodes": number,
                "managementType": "string"
            },
            "resourceType": "string"
        },
        "resourceId": "string",
        "updatedAt": number
    }
  ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

resources

A list of resources and their attributes providing cluster details.

Type: Array of CoverageResource objects

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListCustomDetectionRuleAssociations

Returns all custom detection rule associations for your account. You can filter by rule ID and mode.

Request Syntax

```
GET /custom-detection-rule/association?
maxResults=MaxResults&mode=Mode&nextToken=NextToken&ruleId=RuleId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

MaxResults

The maximum number of results to return in a single page. Minimum value of 1, maximum value of 100.

Valid Range: Minimum value of 1. Maximum value of 100.

Mode

The rule execution mode to filter associations by.

Valid Values: `LIVE | DRY_RUN`

NextToken

A pagination token from a previous response. Use this token to retrieve the next page of results.

RuleId

The unique identifier for the custom detection rule to filter associations by.

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "nextToken": "string",
   "ruleAssociations": [
      {
         "arn": "string",
         "associationId": "string",
         "createdAt": number,
         "expiresAt": number,
         "mode": "string",
         "ruleId": "string",
         "updatedAt": number
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

nextToken

A pagination token to retrieve the next page of results. If this field is empty, there are no additional results.

Type: String

ruleAssociations

A list of custom detection rule association summaries.

Type: Array of AssociationSummary objects

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2

- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListCustomDetectionRuleOrgConfigurations

Returns all organization-level configurations for custom detection rules. You can filter the results by status.

Request Syntax

```
GET /custom-detection-rule/org-configuration?
maxResults=MaxResults&nextToken=NextToken&status=Status HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

MaxResults

The maximum number of results to return in a single page. Minimum value of 1, maximum value of 100.

Valid Range: Minimum value of 1. Maximum value of 100.

NextToken

A pagination token from a previous response. Use this token to retrieve the next page of results.

Status

The configuration status to filter by.

Valid Values: `ACTIVE | PROCESSING | FAILED`

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "configurations": [
      {
         "createdAt": number,
         "expiresAt": number,
         "mode": "string",
         "ruleId": "string",
         "status": "string",
         "statusReason": "string",
         "updatedAt": number
      }
   ],
   "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

configurations

A list of organization configurations for custom detection rules.

Type: Array of DetectionRuleOrgConfigurationSummary objects

nextToken

A pagination token to retrieve the next page of results. If this field is empty, there are no additional results.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListCustomDetectionRules

Returns all available custom detection rules in GuardDuty. You can filter the results by data source, severity, tactic, technique, and service.

Request Syntax

```
POST /custom-detection-rule/rule HTTP/1.1
Content-type: application/json

{
   "filters": [
      {
         "condition": "string",
         "name": "string",
         "values": [ "string" ]
      }
   ],
   "maxResults": number,
   "nextToken": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

filters

A list of filter criteria to apply when listing custom detection rules.

Type: Array of DetectionRuleFilter objects

Array Members: Minimum number of 0 items. Maximum number of 100 items.

Required: No

maxResults

The maximum number of results to return in a single page. Minimum value of 1, maximum value of 100.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

nextToken

A pagination token from a previous response. Use this token to retrieve the next page of results.

Type: String

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "nextToken": "string",
   "rules": [
      {
         "arn": "string",
         "createdAt": number,
         "dataSource": "string",
         "description": "string",
         "language": "string",
         "name": "string",
         "ruleId": "string",
         "schema": "string",
         "service": "string",
         "severity": "string",
         "tactic": "string",
         "technique": "string",
         "updatedAt": number
      }
   ]
```

```
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

nextToken

A pagination token to retrieve the next page of results. If this field is empty, there are no additional results.

Type: String

rules

A list of custom detection rule summaries.

Type: Array of RuleSummary objects

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListDetectors

Lists detectorIds of all the existing Amazon GuardDuty detector resources.

Request Syntax

```
GET /detector?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

MaxResults

You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.

Valid Range: Minimum value of 1. Maximum value of 50.

NextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "detectorIds": [ "string" ],
   "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

detectorIds

A list of detector IDs.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 300.

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListFilters

Returns a paginated list of the current filters.

Request Syntax

```
GET /detector/DetectorId/filter?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector that is associated with the filter.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

MaxResults

You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.

Valid Range: Minimum value of 1. Maximum value of 50.

NextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "filterNames": [ "string" ],
   "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

filterNames

A list of filter names.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 3. Maximum length of 64.

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListFindings

Lists GuardDuty findings for the specified detector ID.

There might be regional differences because some flags might not be available in all the Regions where GuardDuty is currently supported. For more information, see Regions and endpoints.

Request Syntax

```
POST /detector/DetectorId/findings HTTP/1.1
Content-type: application/json

{
   "findingCriteria": {
      "criterion": {
         "string" : {
            "eq": [ "string" ],
            "equals": [ "string" ],
            "greaterThan": number,
            "greaterThanOrEqual": number,
            "gt": number,
            "gte": number,
            "lessThan": number,
            "lessThanOrEqual": number,
            "lt": number,
            "lte": number,
            "matches": [ "string" ],
            "neq": [ "string" ],
            "notEquals": [ "string" ],
            "notMatches": [ "string" ]
         }
      }
   },
   "maxResults": number,
   "nextToken": "string",
   "sortCriteria": {
      "attributeName": "string",
      "orderBy": "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The ID of the detector that specifies the GuardDuty service whose findings you want to list.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

findingCriteria

Represents the criteria used for querying findings. Valid values include:

- JSON field name
- accountId
- region
- confidence
- id
- resource.accessKeyDetails.accessKeyId
- resource.accessKeyDetails.principalId
- resource.accessKeyDetails.userName
- resource.accessKeyDetails.userType
- resource.instanceDetails.iamInstanceProfile.id
- resource.instanceDetails.imageId
- resource.instanceDetails.instanceId
- resource.instanceDetails.networkInterfaces.ipv6Addresses
- resource.instanceDetails.networkInterfaces.privateIpAddresses.privateIpAddress

- resource.instanceDetails.networkInterfaces.publicDnsName
- resource.instanceDetails.networkInterfaces.publicIp
- resource.instanceDetails.networkInterfaces.securityGroups.groupId
- resource.instanceDetails.networkInterfaces.securityGroups.groupName
- resource.instanceDetails.networkInterfaces.subnetId
- resource.instanceDetails.networkInterfaces.vpcId
- resource.instanceDetails.tags.key
- resource.instanceDetails.tags.value
- resource.resourceType
- service.action.actionType
- service.action.awsApiCallAction.api
- service.action.awsApiCallAction.callerType
- service.action.awsApiCallAction.remoteIpDetails.city.cityName
- service.action.awsApiCallAction.remoteIpDetails.country.countryName
- service.action.awsApiCallAction.remoteIpDetails.ipAddressV4
- service.action.awsApiCallAction.remoteIpDetails.organization.asn
- service.action.awsApiCallAction.remoteIpDetails.organization.asnOrg
- service.action.awsApiCallAction.serviceName
- service.action.dnsRequestAction.domain
- service.action.dnsRequestAction.domainWithSuffix
- service.action.networkConnectionAction.blocked
- service.action.networkConnectionAction.connectionDirection
- service.action.networkConnectionAction.localPortDetails.port
- service.action.networkConnectionAction.protocol
- service.action.networkConnectionAction.remoteIpDetails.country.countryName
- service.action.networkConnectionAction.remoteIpDetails.ipAddressV4
- service.action.networkConnectionAction.remoteIpDetails.organization.asn
- service.action.networkConnectionAction.remoteIpDetails.organization.asnOrg
- service.action.networkConnectionAction.remotePortDetails.port
- service.additionalInfo.threatListName

- service.archived

  When this attribute is set to 'true', only archived findings are listed. When it's set to 'false', only unarchived findings are listed. When this attribute is not set, all existing findings are listed.
- service.ebsVolumeScanDetails.scanId
- service.resourceRole
- severity
- type
- updatedAt

  Type: Timestamp in Unix Epoch millisecond format: 1486685375000

Type: FindingCriteria object

Required: No

maxResults

You can use this parameter to indicate the maximum number of items you want in the response. The default value is 50. The maximum value is 50.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 50.

Required: No

nextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Type: String

Required: No

sortCriteria

Represents the criteria used for sorting findings.

Type: SortCriteria object

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "findingIds": [ "string" ],
   "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

findingIds

The IDs of the findings that you're listing.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 300.

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListInvestigations

This API is currently available as a preview. This feature is available in the following AWS Regions: US East (N. Virginia), US East (Ohio), US West (Oregon), Canada (Central), Europe (Frankfurt), Europe (Ireland), Europe (London), Europe (Paris), Europe (Stockholm), and Asia Pacific (Tokyo).

Returns a list of investigations associated with the specified GuardDuty detector.

An administrator account sees all investigations across the organization. Member accounts see only the investigations that belong to them.

Request Syntax

```
POST /detector/DetectorId/investigation/list HTTP/1.1
Content-type: application/json

{
   "maxResults": number,
   "nextToken": "string",
   "sortCriteria": {
      "attributeName": "string",
      "orderBy": "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the GuardDuty detector whose investigations you want to list.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

maxResults

You can use this parameter to indicate the maximum number of items you want in the response. The default value is 50.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 50.

Required: No

nextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `[a-zA-Z0-9+/=_\-]+`

Required: No

sortCriteria

Represents the criteria used for sorting investigations.

Type: InvestigationSortCriteria object

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "investigations": [
      {
         "accountId": "string",
         "confidence": "string",
         "endTime": number,
         "investigationId": "string",
         "riskLevel": "string",
         "startTime": number,
         "status": "string",
         "title": "string",
         "triggerPrompt": "string"
      }
   ],
   "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

investigations

A list of investigation summaries associated with the specified detector.

Type: Array of InvestigationSummary objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `[a-zA-Z0-9+/=_\-]+`

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2

- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListInvitations

Lists all GuardDuty membership invitations that were sent to the current AWS account.

Request Syntax

```
GET /invitation?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

MaxResults

You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.

Valid Range: Minimum value of 1. Maximum value of 50.

NextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "invitations": [
      {
         "accountId": "string",
         "invitationId": "string",
         "invitedAt": "string",
```

```
            "relationshipStatus": "string"
        }
    ],
    "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

invitations

A list of invitation descriptions.

Type: Array of Invitation objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListIPSets

Lists the IPSets of the GuardDuty service specified by the detector ID. If you use this operation from a member account, the IPSets returned are the IPSets from the associated administrator account.

Request Syntax

```
GET /detector/DetectorId/ipset?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector that is associated with IPSet.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

MaxResults

You can use this parameter to indicate the maximum number of items you want in the response. The default value is 50. The maximum value is 50.

Valid Range: Minimum value of 1. Maximum value of 50.

NextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "ipSetIds": [ "string" ],
   "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

ipSetIds

The IDs of the IPSet resources.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListMalwareProtectionPlans

Lists the Malware Protection plan IDs associated with the protected resources in your AWS account.

Request Syntax

```
GET /malware-protection-plan?nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

NextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of `NextToken` from the previous response to continue listing data. The default page size is 100 plans.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "malwareProtectionPlans": [
      {
         "malwareProtectionPlanId": "string"
      }
   ],
   "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

malwareProtectionPlans

A list of unique identifiers associated with each Malware Protection plan.

Type: Array of MalwareProtectionPlanSummary objects

nextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of `NextToken` from the previous response to continue listing data.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListMalwareScans

Returns a list of malware scans. Each member account can view the malware scans for their own accounts. An administrator can view the malware scans for all of its members' accounts.

Request Syntax

```
POST /malware-scan?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
Content-type: application/json

{
   "filterCriteria": {
      "filterCriterion": [
         {
            "filterCondition": {
               "equalsValue": "string",
               "greaterThan": number,
               "lessThan": number
            },
            "criterionKey": "string"
         }
      ]
   },
   "sortCriteria": {
      "attributeName": "string",
      "orderBy": "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

MaxResults

You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.

Valid Range: Minimum value of 1. Maximum value of 50.

NextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing results.

Request Body

The request accepts the following data in JSON format.

filterCriteria

Represents the criteria used to filter the malware scan entries.

Type: ListMalwareScansFilterCriteria object

Required: No

sortCriteria

Represents the criteria used for sorting malware scan entries.

Type: SortCriteria object

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "nextToken": "string",
   "scans": [
      {
         "resourceArn": "string",
         "resourceType": "string",
         "scanCompletedAt": number,
         "scanId": "string",
         "scanResultStatus": "string",
         "scanStartedAt": number,
         "scanStatus": "string",
```

```
            "scanType": "string"
        }
    ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

nextToken

The pagination parameter to be used on the next list operation to retrieve more scans.

Type: String

scans

The list of malware scans associated with the provided input parameters.

Type: Array of MalwareScan objects

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListMembers

Lists details about all member accounts for the current GuardDuty administrator account.

Request Syntax

```
GET /detector/DetectorId/member?
maxResults=MaxResults&nextToken=NextToken&onlyAssociated=OnlyAssociated HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector that is associated with the member.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

MaxResults

You can use this parameter to indicate the maximum number of items you want in the response. The default value is 50. The maximum value is 50.

Valid Range: Minimum value of 1. Maximum value of 50.

NextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

OnlyAssociated

Specifies whether to only return associated members or to return all members (including members who haven't been invited yet or have been disassociated). Member accounts must have been previously associated with the GuardDuty administrator account using `CreateMembers`.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "members": [
      {
         "accountId": "string",
         "administratorId": "string",
         "detectorId": "string",
         "email": "string",
         "invitedAt": "string",
         "masterId": "string",
         "relationshipStatus": "string",
         "updatedAt": "string"
      }
   ],
   "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

members

A list of members.

> **Note**
>
> The values for `email` and `invitedAt` are available only if the member accounts are added by invitation.

Type: Array of Member objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListOrganizationAdminAccounts

Lists the accounts designated as GuardDuty delegated administrators. Only the organization's management account can run this API operation.

Request Syntax

```
GET /admin?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

MaxResults

The maximum number of results to return in the response.

Valid Range: Minimum value of 1. Maximum value of 50.

NextToken

A token to use for paginating results that are returned in the response. Set the value of this parameter to null for the first request to a list action. For subsequent calls, use the `NextToken` value returned from the previous request to continue listing results after the first page.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "adminAccounts": [
      {
         "adminAccountId": "string",
         "adminStatus": "string"
      }
```

```
    ],
    "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

adminAccounts

A list of accounts configured as GuardDuty delegated administrators.

Type: Array of AdminAccount objects

Array Members: Minimum number of 0 items. Maximum number of 1 item.

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListPublishingDestinations

Returns a list of publishing destinations associated with the specified `detectorId`.

Request Syntax

```
GET /detector/DetectorId/publishingDestination?
maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The detector ID for which you want to retrieve the publishing destination.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

MaxResults

The maximum number of results to return in the response.

Valid Range: Minimum value of 1. Maximum value of 50.

NextToken

A token to use for paginating results that are returned in the response. Set the value of this parameter to null for the first request to a list action. For subsequent calls, use the `NextToken` value returned from the previous request to continue listing results after the first page.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "destinations": [
      {
         "destinationId": "string",
         "destinationType": "string",
         "status": "string"
      }
   ],
   "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

destinations

A `Destinations` object that includes information about each publishing destination returned.

Type: Array of Destination objects

nextToken

A token to use for paginating results that are returned in the response. Set the value of this parameter to null for the first request to a list action. For subsequent calls, use the `NextToken` value returned from the previous request to continue listing results after the first page.

Type: String

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListTagsForResource

Lists tags for a resource. Tagging is currently supported for detectors, finding filters, IP sets, threat intel sets, and publishing destination, with a limit of 50 tags per resource. When invoked, this operation returns all assigned tags for a given resource.

Request Syntax

```
GET /tags/ResourceArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ResourceArn

The Amazon Resource Name (ARN) for the given GuardDuty resource.

Pattern: `arn:[A-Za-z_.-]{1,20}:guardduty:[A-Za-z0-9_/.-]{0,63}:\d+:detector/[A-Za-z0-9_/.-]{32,264}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "tags": {
      "string" : "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

tags

The tags associated with the resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListThreatEntitySets

Lists the threat entity sets associated with the specified GuardDuty detector ID. If you use this operation from a member account, the threat entity sets that are returned as a response, belong to the administrator account.

Request Syntax

```
GET /detector/DetectorId/threatentityset?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the GuardDuty detector that is associated with this threat entity set.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

MaxResults

You can use this parameter to indicate the maximum number of items you want in the response. The default value is 50.

Valid Range: Minimum value of 1. Maximum value of 50.

NextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "nextToken": "string",
   "threatEntitySetIds": [ "string" ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

threatEntitySetIds

The IDs of the threat entity set resources.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListThreatIntelSets

Lists the ThreatIntelSets of the GuardDuty service specified by the detector ID. If you use this operation from a member account, the ThreatIntelSets associated with the administrator account are returned.

Request Syntax

```
GET /detector/DetectorId/threatintelset?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector that is associated with the threatIntelSet.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

MaxResults

You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.

Valid Range: Minimum value of 1. Maximum value of 50.

NextToken

You can use this parameter to paginate results in the response. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "nextToken": "string",
   "threatIntelSetIds": [ "string" ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

threatIntelSetIds

The IDs of the ThreatIntelSet resources.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListTrustedEntitySets

Lists the trusted entity sets associated with the specified GuardDuty detector ID. If you use this operation from a member account, the trusted entity sets that are returned as a response, belong to the administrator account.

Request Syntax

```
GET /detector/DetectorId/trustedentityset?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the GuardDuty detector that is associated with this threat entity set.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

MaxResults

You can use this parameter to indicate the maximum number of items you want in the response. The default value is 50.

Valid Range: Minimum value of 1. Maximum value of 50.

NextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "nextToken": "string",
   "trustedEntitySetIds": [ "string" ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

trustedEntitySetIds

The IDs of the trusted entity set resources.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

SendObjectMalwareScan

Initiates a malware scan for a specific S3 object. This API allows you to perform on-demand malware scanning of individual objects in S3 buckets that have Malware Protection for S3 enabled.

When you use this API, the AWS service terms for GuardDuty Malware Protection apply. For more information, see AWS service terms for GuardDuty Malware Protection.

Request Syntax

```
POST /object-malware-scan/send HTTP/1.1
Content-type: application/json

{
   "s3Object": {
      "bucket": "string",
      "key": "string",
      "versionId": "string"
   }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

s3Object

The S3 object information for the object you want to scan. The bucket must have a Malware Protection plan configured to use this API.

Type: S3ObjectForSendObjectMalwareScan object

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

StartMalwareScan

Initiates the malware scan. Invoking this API will automatically create the Service-linked role in the corresponding account if the resourceArn belongs to an EC2 instance.

When the malware scan starts, you can use the associated scan ID to track the status of the scan. For more information, see ListMalwareScans and GetMalwareScan.

When you use this API, the AWS service terms for GuardDuty Malware Protection apply. For more information, see AWS service terms for GuardDuty Malware Protection.

Request Syntax

```
POST /malware-scan/start HTTP/1.1
Content-type: application/json

{
   "clientToken": "string",
   "resourceArn": "string",
   "scanConfiguration": {
      "incrementalScanDetails": {
         "baselineResourceArn": "string"
      },
      "recoveryPoint": {
         "backupVaultName": "string",
         "continuousScanDetails": {
            "endTime": number,
            "startTime": number
         }
      },
      "role": "string"
   }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

clientToken

The idempotency token for the create request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

resourceArn

Amazon Resource Name (ARN) of the resource for which you invoked the API.

Type: String

Pattern: `arn:[A-Za-z-]+:[A-Za-z0-9]+:[A-Za-z0-9-]+:\d+:(([A-Za-z0-9-]+)[:\/])?[A-Za-z0-9:-]*`

Required: Yes

scanConfiguration

Contains information about the configuration to be used for the malware scan.

Type: StartMalwareScanConfiguration object

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "scanId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

scanId

A unique identifier that gets generated when you invoke the API without any error. Each malware scan has a corresponding scan ID. Using this scan ID, you can monitor the status of your malware scan.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

ConflictException

A request conflict exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 409

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

StartMonitoringMembers

Turns on GuardDuty monitoring of the specified member accounts. Use this operation to restart monitoring of accounts that you stopped monitoring with the StopMonitoringMembers operation.

Request Syntax

```
POST /detector/DetectorId/member/start HTTP/1.1
Content-type: application/json

{
   "accountIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector of the GuardDuty administrator account associated with the member accounts to monitor.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds

A list of account IDs of the GuardDuty member accounts to start monitoring.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

unprocessedAccounts

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of UnprocessedAccount objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

StopMonitoringMembers

Stops GuardDuty monitoring for the specified member accounts. Use the `StartMonitoringMembers` operation to restart monitoring for those accounts.

With `autoEnableOrganizationMembers` configuration for your organization set to `ALL`, you'll receive an error if you attempt to stop monitoring the member accounts in your organization.

Request Syntax

```
POST /detector/DetectorId/member/stop HTTP/1.1
Content-type: application/json

{
   "accountIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector associated with the GuardDuty administrator account that is monitoring member accounts.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds

A list of account IDs for the member accounts to stop monitoring.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

unprocessedAccounts

A list of objects that contain an accountId for each account that could not be processed, and a result string that indicates why the account was not processed.

Type: Array of UnprocessedAccount objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)

- AWS SDK for Ruby V3

TagResource

Adds tags to a resource.

Request Syntax

```
POST /tags/ResourceArn HTTP/1.1
Content-type: application/json

{
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

ResourceArn

The Amazon Resource Name (ARN) for the GuardDuty resource to apply a tag to.

Pattern: `arn:[A-Za-z_.-]{1,20}:guardduty:[A-Za-z0-9_/.-]{0,63}:\d+:detector/[A-Za-z0-9_/.-]{32,264}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

tags

The tags to be added to a resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Value Length Constraints: Minimum length of 0. Maximum length of 256.

Required: Yes

Response Syntax

```
HTTP/1.1 204
```

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UnarchiveFindings

Unarchives GuardDuty findings specified by the `findingIds`.

Request Syntax

```
POST /detector/DetectorId/findings/unarchive HTTP/1.1
Content-type: application/json

{
   "findingIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The ID of the detector associated with the findings to unarchive.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

findingIds

The IDs of the findings to unarchive.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UntagResource

Removes tags from a resource.

Request Syntax

```
DELETE /tags/ResourceArn?tagKeys=TagKeys HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ResourceArn

The Amazon Resource Name (ARN) for the resource to remove tags from.

Pattern: `arn:[A-Za-z_.-]{1,20}:guardduty:[A-Za-z0-9_/.-]{0,63}:\d+:detector/[A-Za-z0-9_/.-]{32,264}`

Required: Yes

TagKeys

The tag keys to remove from the resource.

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 204
```

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateCustomDetectionRuleAssociation

Updates the mode of an existing custom detection rule association.

Request Syntax

```
PUT /custom-detection-rule/rule/RuleId/association/AssociationId HTTP/1.1
Content-type: application/json

{
   "mode": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

AssociationId

The unique identifier for the association to update.

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-zA-Z0-9_-]{1,64}`

Required: Yes

RuleId

The unique identifier for the custom detection rule.

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Required: Yes

Request Body

The request accepts the following data in JSON format.

mode

The rule execution mode. Valid values: `LIVE` | `DRY_RUN`.

Type: String

Valid Values: `LIVE` | `DRY_RUN`

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

ConflictException

A request conflict exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 409

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

ResourceNotFoundException

The requested resource can't be found.

Message

The error message.

Type

The error type.

HTTP Status Code: 404

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateCustomDetectionRuleOrgConfiguration

Updates the organization-level configuration for a custom detection rule, including the mode and include/exclude account lists.

Request Syntax

```
PUT /custom-detection-rule/org-configuration/RuleId HTTP/1.1
Content-type: application/json

{
   "excludeAccountIds": [ "string" ],
   "includeAccountIds": [ "string" ],
   "mode": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

RuleId

The unique identifier for the custom detection rule.

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Required: Yes

Request Body

The request accepts the following data in JSON format.

excludeAccountIds

The account IDs to exclude from the organization configuration. Mutually exclusive with `IncludeAccountIds`.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50000 items.

Length Constraints: Fixed length of 12.

Required: No

includeAccountIds

The account IDs to include in the organization configuration. Mutually exclusive with `ExcludeAccountIds`.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50000 items.

Length Constraints: Fixed length of 12.

Required: No

mode

The execution mode of the organization configuration. Valid values: `LIVE` | `DRY_RUN`.

Type: String

Valid Values: `LIVE | DRY_RUN`

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

ConflictException

A request conflict exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 409

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

ResourceNotFoundException

The requested resource can't be found.

Message

The error message.

Type

The error type.

HTTP Status Code: 404

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateDetector

Updates the GuardDuty detector specified by the detector ID.

Specifying both EKS Runtime Monitoring (`EKS_RUNTIME_MONITORING`) and Runtime Monitoring (`RUNTIME_MONITORING`) will cause an error. You can add only one of these two features because Runtime Monitoring already includes the threat detection for Amazon EKS resources. For more information, see Runtime Monitoring.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see Regions and endpoints.

Request Syntax

```
POST /detector/DetectorId HTTP/1.1
Content-type: application/json

{
   "dataSources": {
      "kubernetes": {
         "auditLogs": {
            "enable": boolean
         }
      },
      "malwareProtection": {
         "scanEc2InstanceWithFindings": {
            "ebsVolumes": boolean
         }
      },
      "s3Logs": {
         "enable": boolean
      }
   },
   "enable": boolean,
   "features": [
      {
         "additionalConfiguration": [
            {
               "name": "string",
               "status": "string"
            }
```

```
            ],
            "name": "string",
            "status": "string"
        }
    ],
    "findingPublishingFrequency": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector to update.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

dataSources

This parameter has been deprecated.

Describes which data sources will be updated.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see Regions and endpoints.

Type: DataSourceConfigurations object

Required: No

enable

Specifies whether the detector is enabled or not enabled.

Type: Boolean

Required: No

features

Provides the features that will be updated for the detector.

Type: Array of DetectorFeatureConfiguration objects

Required: No

findingPublishingFrequency

An enum value that specifies how frequently findings are exported, such as to CloudWatch Events.

Type: String

Valid Values: `FIFTEEN_MINUTES | ONE_HOUR | SIX_HOURS`

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateFilter

Updates the filter specified by the filter name.

Request Syntax

```
POST /detector/DetectorId/filter/FilterName HTTP/1.1
Content-type: application/json

{
   "action": "string",
   "description": "string",
   "findingCriteria": {
      "criterion": {
         "string" : {
            "eq": [ "string" ],
            "equals": [ "string" ],
            "greaterThan": number,
            "greaterThanOrEqual": number,
            "gt": number,
            "gte": number,
            "lessThan": number,
            "lessThanOrEqual": number,
            "lt": number,
            "lte": number,
            "matches": [ "string" ],
            "neq": [ "string" ],
            "notEquals": [ "string" ],
            "notMatches": [ "string" ]
         }
      }
   },
   "rank": number
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector that specifies the GuardDuty service where you want to update a filter.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

FilterName

The name of the filter.

Required: Yes

Request Body

The request accepts the following data in JSON format.

action

Specifies the action that is to be applied to the findings that match the filter.

Default: NOOP

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `NOOP | ARCHIVE`

Required: No

description

The description of the filter. Valid characters include alphanumeric characters, and special characters such as hyphen, period, colon, underscore, parentheses ({ }, [ ], and ( )), forward slash, horizontal tab, vertical tab, newline, form feed, return, and whitespace.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 512.

Required: No

findingCriteria

Represents the criteria to be used in the filter for querying findings. The following fields are available for filtering:

- accountId
- arn
- associatedAttackSequenceArn
- confidence
- createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- id
- partition
- region
- resource.accessKeyDetails.accessKeyId
- resource.accessKeyDetails.principalId
- resource.accessKeyDetails.userIdentity.accessKeyId
- resource.accessKeyDetails.userIdentity.accountId
- resource.accessKeyDetails.userIdentity.arn
- resource.accessKeyDetails.userIdentity.principalId
- resource.accessKeyDetails.userIdentity.sessionContext.attributes.mfaAuthenticated
- resource.accessKeyDetails.userIdentity.sessionContext.ec2RoleDelivery
- resource.accessKeyDetails.userIdentity.sessionContext.invokedBy
- resource.accessKeyDetails.userIdentity.sessionContext.sessionIssuer.accountId
- resource.accessKeyDetails.userIdentity.sessionContext.sessionIssuer.arn
- resource.accessKeyDetails.userIdentity.sessionContext.sessionIssuer.principalId
- resource.accessKeyDetails.userIdentity.sessionContext.sessionIssuer.type
- resource.accessKeyDetails.userIdentity.sessionContext.sessionIssuer.userName
- resource.accessKeyDetails.userIdentity.sessionContext.sourceIdentity
- resource.accessKeyDetails.userIdentity.sessionContext.webIdFederationData.attributes

- resource.accessKeyDetails.userIdentity.sessionContext.webIdFederationData.federatedProvider
- resource.accessKeyDetails.userIdentity.type
- resource.accessKeyDetails.userIdentity.userName
- resource.accessKeyDetails.userName
- resource.accessKeyDetails.userType
- resource.bedrockGuardrailDetails.guardrailArn
- resource.bedrockGuardrailDetails.guardrailVersion
- resource.containerDetails.containerRuntime
- resource.containerDetails.id
- resource.containerDetails.image
- resource.containerDetails.imagePrefix
- resource.containerDetails.name
- resource.containerDetails.securityContext.allowPrivilegeEscalation
- resource.containerDetails.securityContext.privileged
- resource.containerDetails.volumeMounts.mountPath
- resource.containerDetails.volumeMounts.name
- resource.ebsSnapshotDetails.snapshotArn
- resource.ebsVolumeDetails.scannedVolumeDetails.deviceName
- resource.ebsVolumeDetails.scannedVolumeDetails.encryptionType
- resource.ebsVolumeDetails.scannedVolumeDetails.kmsKeyArn
- resource.ebsVolumeDetails.scannedVolumeDetails.snapshotArn
- resource.ebsVolumeDetails.scannedVolumeDetails.volumeArn
- resource.ebsVolumeDetails.scannedVolumeDetails.volumeSizeInGB
- resource.ebsVolumeDetails.scannedVolumeDetails.volumeType
- resource.ebsVolumeDetails.skippedVolumeDetails.deviceName
- resource.ebsVolumeDetails.skippedVolumeDetails.encryptionType
- resource.ebsVolumeDetails.skippedVolumeDetails.kmsKeyArn
- resource.ebsVolumeDetails.skippedVolumeDetails.snapshotArn
- resource.ebsVolumeDetails.skippedVolumeDetails.volumeArn
- resource.ebsVolumeDetails.skippedVolumeDetails.volumeSizeInGB

- resource.ebsVolumeDetails.skippedVolumeDetails.volumeType
- resource.ec2ImageDetails.imageArn
- resource.ecsClusterDetails.activeServicesCount
- resource.ecsClusterDetails.arn
- resource.ecsClusterDetails.name
- resource.ecsClusterDetails.registeredContainerInstancesCount
- resource.ecsClusterDetails.runningTasksCount
- resource.ecsClusterDetails.status
- resource.ecsClusterDetails.tags.key
- resource.ecsClusterDetails.tags.value
- resource.ecsClusterDetails.taskDetails.arn
- resource.ecsClusterDetails.taskDetails.containers.containerRuntime
- resource.ecsClusterDetails.taskDetails.containers.id
- resource.ecsClusterDetails.taskDetails.containers.image
- resource.ecsClusterDetails.taskDetails.containers.imagePrefix
- resource.ecsClusterDetails.taskDetails.containers.name
- resource.ecsClusterDetails.taskDetails.containers.securityContext.allowPrivilegeEscalation
- resource.ecsClusterDetails.taskDetails.containers.securityContext.privileged
- resource.ecsClusterDetails.taskDetails.containers.volumeMounts.mountPath
- resource.ecsClusterDetails.taskDetails.containers.volumeMounts.name
- resource.ecsClusterDetails.taskDetails.createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- resource.ecsClusterDetails.taskDetails.definitionArn
- resource.ecsClusterDetails.taskDetails.group
- resource.ecsClusterDetails.taskDetails.launchType
- resource.ecsClusterDetails.taskDetails.startedAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- resource.ecsClusterDetails.taskDetails.startedBy
- resource.ecsClusterDetails.taskDetails.tags.key
- resource.ecsClusterDetails.taskDetails.tags.value

- resource.ecsClusterDetails.taskDetails.version
- resource.ecsClusterDetails.taskDetails.volumes.hostPath.path
- resource.ecsClusterDetails.taskDetails.volumes.name
- resource.eksClusterDetails.arn
- resource.eksClusterDetails.createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- resource.eksClusterDetails.name
- resource.eksClusterDetails.status
- resource.eksClusterDetails.tags.key
- resource.eksClusterDetails.tags.value
- resource.eksClusterDetails.vpcId
- resource.instanceDetails.availabilityZone
- resource.instanceDetails.iamInstanceProfile.arn
- resource.instanceDetails.iamInstanceProfile.id
- resource.instanceDetails.imageDescription
- resource.instanceDetails.imageId
- resource.instanceDetails.instanceId
- resource.instanceDetails.instanceState
- resource.instanceDetails.instanceType
- resource.instanceDetails.launchTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- resource.instanceDetails.networkInterfaces.ipv6Addresses
- resource.instanceDetails.networkInterfaces.networkInterfaceId
- resource.instanceDetails.networkInterfaces.privateDnsName
- resource.instanceDetails.networkInterfaces.privateIpAddress
- resource.instanceDetails.networkInterfaces.privateIpAddresses.privateDnsName
- resource.instanceDetails.networkInterfaces.privateIpAddresses.privateIpAddress
- resource.instanceDetails.networkInterfaces.publicDnsName
- resource.instanceDetails.networkInterfaces.publicIp
- resource.instanceDetails.networkInterfaces.securityGroups.groupId

- resource.instanceDetails.networkInterfaces.securityGroups.groupName
- resource.instanceDetails.networkInterfaces.subnetId
- resource.instanceDetails.networkInterfaces.vpcId
- resource.instanceDetails.outpostArn
- resource.instanceDetails.platform
- resource.instanceDetails.productCodes.productCodeId
- resource.instanceDetails.productCodes.productCodeType
- resource.instanceDetails.tags.key
- resource.instanceDetails.tags.value
- resource.kubernetesDetails.kubernetesUserDetails.groups
- resource.kubernetesDetails.kubernetesUserDetails.impersonatedUser.groups
- resource.kubernetesDetails.kubernetesUserDetails.impersonatedUser.username
- resource.kubernetesDetails.kubernetesUserDetails.sessionName
- resource.kubernetesDetails.kubernetesUserDetails.uid
- resource.kubernetesDetails.kubernetesUserDetails.username
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.containerRuntime
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.id
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.imagePrefix
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.name
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.allowPrivilegeEsca
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.privileged
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.volumeMounts.mountPath
- resource.kubernetesDetails.kubernetesWorkloadDetails.containers.volumeMounts.name
- resource.kubernetesDetails.kubernetesWorkloadDetails.hostIpc
- resource.kubernetesDetails.kubernetesWorkloadDetails.hostNetwork
- resource.kubernetesDetails.kubernetesWorkloadDetails.hostPid
- resource.kubernetesDetails.kubernetesWorkloadDetails.name
- resource.kubernetesDetails.kubernetesWorkloadDetails.namespace
- resource.kubernetesDetails.kubernetesWorkloadDetails.serviceAccountName

- resource.kubernetesDetails.kubernetesWorkloadDetails.type
- resource.kubernetesDetails.kubernetesWorkloadDetails.uid
- resource.kubernetesDetails.kubernetesWorkloadDetails.volumes.hostPath.path
- resource.kubernetesDetails.kubernetesWorkloadDetails.volumes.name
- resource.lambdaDetails.description
- resource.lambdaDetails.functionArn
- resource.lambdaDetails.functionName
- resource.lambdaDetails.functionVersion
- resource.lambdaDetails.lastModifiedAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- resource.lambdaDetails.revisionId
- resource.lambdaDetails.role
- resource.lambdaDetails.tags.key
- resource.lambdaDetails.tags.value
- resource.lambdaDetails.vpcConfig.securityGroups.groupId
- resource.lambdaDetails.vpcConfig.securityGroups.groupName
- resource.lambdaDetails.vpcConfig.subnetIds
- resource.lambdaDetails.vpcConfig.vpcId
- resource.rdsDbInstanceDetails.dbClusterIdentifier
- resource.rdsDbInstanceDetails.dbInstanceArn
- resource.rdsDbInstanceDetails.dbInstanceIdentifier
- resource.rdsDbInstanceDetails.dbSecurityGroups.name
- resource.rdsDbInstanceDetails.dbSecurityGroups.status
- resource.rdsDbInstanceDetails.dbiResourceId
- resource.rdsDbInstanceDetails.engine
- resource.rdsDbInstanceDetails.engineVersion
- resource.rdsDbInstanceDetails.iamDatabaseAuthenticationEnabled
- resource.rdsDbInstanceDetails.publiclyAccessible
- resource.rdsDbInstanceDetails.vpcId
- resource.rdsDbInstanceDetails.vpcSecurityGroups.status

- resource.rdsDbInstanceDetails.vpcSecurityGroups.vpcSecurityGroupId
- resource.rdsDbUserDetails.application
- resource.rdsDbUserDetails.authMethod
- resource.rdsDbUserDetails.database
- resource.rdsDbUserDetails.ssl
- resource.rdsDbUserDetails.user
- resource.rdsLimitlessDbDetails.dbClusterIdentifier
- resource.rdsLimitlessDbDetails.dbShardGroupArn
- resource.rdsLimitlessDbDetails.dbShardGroupIdentifier
- resource.rdsLimitlessDbDetails.dbShardGroupResourceId
- resource.rdsLimitlessDbDetails.engine
- resource.rdsLimitlessDbDetails.engineVersion
- resource.rdsLimitlessDbDetails.tags.key
- resource.rdsLimitlessDbDetails.tags.value
- resource.recoveryPointDetails.backupVaultName
- resource.recoveryPointDetails.recoveryPointArn
- resource.resourceType
- resource.s3BucketDetails.arn
- resource.s3BucketDetails.createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- resource.s3BucketDetails.defaultServerSideEncryption.encryptionType
- resource.s3BucketDetails.defaultServerSideEncryption.kmsMasterKeyArn
- resource.s3BucketDetails.name
- resource.s3BucketDetails.owner.id
- resource.s3BucketDetails.publicAccess.effectivePermission
- resource.s3BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublic
- resource.s3BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublic
- resource.s3BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublic
- resource.s3BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublic
- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.accessContro

- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.accessContro
- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicA
- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicA
- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicA
- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicA
- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.bucketPolicy
- resource.s3BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.bucketPolicy
- resource.s3BucketDetails.s3ObjectDetails.eTag
- resource.s3BucketDetails.s3ObjectDetails.hash
- resource.s3BucketDetails.s3ObjectDetails.key
- resource.s3BucketDetails.s3ObjectDetails.objectArn
- resource.s3BucketDetails.s3ObjectDetails.versionId
- resource.s3BucketDetails.tags.key
- resource.s3BucketDetails.tags.value
- resource.s3BucketDetails.type
- schemaVersion
- service.action.actionType
- service.action.awsApiCallAction.api
- service.action.awsApiCallAction.callerType
- service.action.awsApiCallAction.domainDetails.domain
- service.action.awsApiCallAction.errorCode
- service.action.awsApiCallAction.remoteAccountDetails.accountId
- service.action.awsApiCallAction.remoteAccountDetails.affiliated
- service.action.awsApiCallAction.remoteAccountDetails.awsServiceName
- service.action.awsApiCallAction.remoteIpDetails.city.cityName
- service.action.awsApiCallAction.remoteIpDetails.country.countryCode
- service.action.awsApiCallAction.remoteIpDetails.country.countryName
- service.action.awsApiCallAction.remoteIpDetails.geoLocation.lat
- service.action.awsApiCallAction.remoteIpDetails.geoLocation.lon
- service.action.awsApiCallAction.remoteIpDetails.ipAddressV4

- service.action.awsApiCallAction.remoteIpDetails.ipAddressV6
- service.action.awsApiCallAction.remoteIpDetails.organization.asn
- service.action.awsApiCallAction.remoteIpDetails.organization.asnOrg
- service.action.awsApiCallAction.remoteIpDetails.organization.isp
- service.action.awsApiCallAction.remoteIpDetails.organization.org
- service.action.awsApiCallAction.serviceName
- service.action.awsApiCallAction.userAgent
- service.action.dnsRequestAction.blocked
- service.action.dnsRequestAction.domain
- service.action.dnsRequestAction.domainWithSuffix
- service.action.dnsRequestAction.protocol
- service.action.dnsRequestAction.vpcOwnerAccountId
- service.action.kubernetesApiCallAction.namespace
- service.action.kubernetesApiCallAction.parameters
- service.action.kubernetesApiCallAction.remoteIpDetails.city.cityName
- service.action.kubernetesApiCallAction.remoteIpDetails.country.countryCode
- service.action.kubernetesApiCallAction.remoteIpDetails.country.countryName
- service.action.kubernetesApiCallAction.remoteIpDetails.geoLocation.lat
- service.action.kubernetesApiCallAction.remoteIpDetails.geoLocation.lon
- service.action.kubernetesApiCallAction.remoteIpDetails.ipAddressV4
- service.action.kubernetesApiCallAction.remoteIpDetails.ipAddressV6
- service.action.kubernetesApiCallAction.remoteIpDetails.organization.asn
- service.action.kubernetesApiCallAction.remoteIpDetails.organization.asnOrg
- service.action.kubernetesApiCallAction.remoteIpDetails.organization.isp
- service.action.kubernetesApiCallAction.remoteIpDetails.organization.org
- service.action.kubernetesApiCallAction.requestUri
- service.action.kubernetesApiCallAction.resource
- service.action.kubernetesApiCallAction.resourceName
- service.action.kubernetesApiCallAction.sourceIPs
- service.action.kubernetesApiCallAction.statusCode

- service.action.kubernetesApiCallAction.subresource
- service.action.kubernetesApiCallAction.userAgent
- service.action.kubernetesApiCallAction.verb
- service.action.kubernetesPermissionCheckedDetails.allowed
- service.action.kubernetesPermissionCheckedDetails.namespace
- service.action.kubernetesPermissionCheckedDetails.resource
- service.action.kubernetesPermissionCheckedDetails.verb
- service.action.kubernetesRoleBindingDetails.kind
- service.action.kubernetesRoleBindingDetails.name
- service.action.kubernetesRoleBindingDetails.roleRefKind
- service.action.kubernetesRoleBindingDetails.roleRefName
- service.action.kubernetesRoleBindingDetails.uid
- service.action.kubernetesRoleDetails.kind
- service.action.kubernetesRoleDetails.name
- service.action.kubernetesRoleDetails.uid
- service.action.networkConnectionAction.blocked
- service.action.networkConnectionAction.connectionDirection
- service.action.networkConnectionAction.localIpDetails.ipAddressV4
- service.action.networkConnectionAction.localIpDetails.ipAddressV6
- service.action.networkConnectionAction.localNetworkInterface
- service.action.networkConnectionAction.localPortDetails.port
- service.action.networkConnectionAction.localPortDetails.portName
- service.action.networkConnectionAction.protocol
- service.action.networkConnectionAction.remoteIpDetails.city.cityName
- service.action.networkConnectionAction.remoteIpDetails.country.countryCode
- service.action.networkConnectionAction.remoteIpDetails.country.countryName
- service.action.networkConnectionAction.remoteIpDetails.geoLocation.lat
- service.action.networkConnectionAction.remoteIpDetails.geoLocation.lon
- service.action.networkConnectionAction.remoteIpDetails.ipAddressV4
- service.action.networkConnectionAction.remoteIpDetails.ipAddressV6

- service.action.networkConnectionAction.remoteIpDetails.organization.asn
- service.action.networkConnectionAction.remoteIpDetails.organization.asnOrg
- service.action.networkConnectionAction.remoteIpDetails.organization.isp
- service.action.networkConnectionAction.remoteIpDetails.organization.org
- service.action.networkConnectionAction.remotePortDetails.port
- service.action.networkConnectionAction.remotePortDetails.portName
- service.action.portProbeAction.blocked
- service.action.portProbeAction.portProbeDetails.localIpDetails.ipAddressV4
- service.action.portProbeAction.portProbeDetails.localIpDetails.ipAddressV6
- service.action.portProbeAction.portProbeDetails.localPortDetails.port
- service.action.portProbeAction.portProbeDetails.localPortDetails.portName
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.city.cityName
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.country.countryCode
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.country.countryName
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.geoLocation.lat
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.geoLocation.lon
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.ipAddressV4
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.ipAddressV6
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.organization.asn
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.organization.asnOrg
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.organization.isp
- service.action.portProbeAction.portProbeDetails.remoteIpDetails.organization.org
- service.action.rdsLoginAttemptAction.loginAttributes.application
- service.action.rdsLoginAttemptAction.loginAttributes.failedLoginAttempts
- service.action.rdsLoginAttemptAction.loginAttributes.successfulLoginAttempts
- service.action.rdsLoginAttemptAction.loginAttributes.user
- service.action.rdsLoginAttemptAction.remoteIpDetails.city.cityName
- service.action.rdsLoginAttemptAction.remoteIpDetails.country.countryCode
- service.action.rdsLoginAttemptAction.remoteIpDetails.country.countryName
- service.action.rdsLoginAttemptAction.remoteIpDetails.geoLocation.lat

- service.action.rdsLoginAttemptAction.remoteIpDetails.geoLocation.lon
- service.action.rdsLoginAttemptAction.remoteIpDetails.ipAddressV4
- service.action.rdsLoginAttemptAction.remoteIpDetails.ipAddressV6
- service.action.rdsLoginAttemptAction.remoteIpDetails.organization.asn
- service.action.rdsLoginAttemptAction.remoteIpDetails.organization.asnOrg
- service.action.rdsLoginAttemptAction.remoteIpDetails.organization.isp
- service.action.rdsLoginAttemptAction.remoteIpDetails.organization.org
- service.additionalInfo.agentDetails.agentId
- service.additionalInfo.agentDetails.agentVersion
- service.additionalInfo.anomalies.anomalousAPIs
- service.additionalInfo.authenticationMethod
- service.additionalInfo.averagePacketSizeIn
- service.additionalInfo.averagePacketSizeOut
- service.additionalInfo.context
- service.additionalInfo.domain
- service.additionalInfo.inBytes
- service.additionalInfo.localNetworkInterfaceOwner
- service.additionalInfo.localPort
- service.additionalInfo.outBytes
- service.additionalInfo.packetsIn
- service.additionalInfo.packetsOut
- service.additionalInfo.policyArn
- service.additionalInfo.policyName
- service.additionalInfo.remotePort
- service.additionalInfo.sample
- service.additionalInfo.scannedPort
- service.additionalInfo.threatFileSha256
- service.additionalInfo.threatListName
- service.additionalInfo.threatName
- service.additionalInfo.totalBytesIn

- service.additionalInfo.totalBytesOut
- service.additionalInfo.type
- service.additionalInfo.unusual.asnOrg
- service.additionalInfo.unusual.port
- service.additionalInfo.unusualProtocol
- service.additionalInfo.userAgent.fullUserAgent
- service.additionalInfo.userAgent.userAgentCategory
- service.additionalInfo.value
- service.additionalInfo.vpcOwnerAccountId
- service.archived
- service.count
- service.detection.sequence.actors.id
- service.detection.sequence.actors.process.name
- service.detection.sequence.actors.process.path
- service.detection.sequence.actors.process.sha256
- service.detection.sequence.actors.session.createdTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.detection.sequence.actors.session.issuer
- service.detection.sequence.actors.session.mfaStatus
- service.detection.sequence.actors.session.uid
- service.detection.sequence.actors.user.account.account
- service.detection.sequence.actors.user.account.uid
- service.detection.sequence.actors.user.credentialUid
- service.detection.sequence.actors.user.name
- service.detection.sequence.actors.user.type
- service.detection.sequence.actors.user.uid
- service.detection.sequence.additionalSequenceTypes
- service.detection.sequence.description
- service.detection.sequence.endpoints.autonomousSystem.name
- service.detection.sequence.endpoints.autonomousSystem.number

- service.detection.sequence.endpoints.connection.direction
- service.detection.sequence.endpoints.domain
- service.detection.sequence.endpoints.id
- service.detection.sequence.endpoints.ip
- service.detection.sequence.endpoints.location.city
- service.detection.sequence.endpoints.location.country
- service.detection.sequence.endpoints.location.lat
- service.detection.sequence.endpoints.location.lon
- service.detection.sequence.endpoints.port
- service.detection.sequence.resources.accountId
- service.detection.sequence.resources.cloudPartition
- service.detection.sequence.resources.data.accessKey.principalId
- service.detection.sequence.resources.data.accessKey.userName
- service.detection.sequence.resources.data.accessKey.userType
- service.detection.sequence.resources.data.autoscalingAutoScalingGroup.ec2InstanceUids
- service.detection.sequence.resources.data.cloudformationStack.ec2InstanceUids
- service.detection.sequence.resources.data.container.image
- service.detection.sequence.resources.data.container.imageUid
- service.detection.sequence.resources.data.ec2Image.ec2InstanceUids
- service.detection.sequence.resources.data.ec2Instance.availabilityZone
- service.detection.sequence.resources.data.ec2Instance.ec2NetworkInterfaceUids
- service.detection.sequence.resources.data.ec2Instance.iamInstanceProfile.arn
- service.detection.sequence.resources.data.ec2Instance.iamInstanceProfile.id
- service.detection.sequence.resources.data.ec2Instance.imageDescription
- service.detection.sequence.resources.data.ec2Instance.instanceState
- service.detection.sequence.resources.data.ec2Instance.instanceType
- service.detection.sequence.resources.data.ec2Instance.outpostArn
- service.detection.sequence.resources.data.ec2Instance.platform
- service.detection.sequence.resources.data.ec2Instance.productCodes.productCodeId
- service.detection.sequence.resources.data.ec2Instance.productCodes.productCodeType

- service.detection.sequence.resources.data.ec2LaunchTemplate.ec2InstanceUids
- service.detection.sequence.resources.data.ec2LaunchTemplate.version
- service.detection.sequence.resources.data.ec2NetworkInterface.ipv6Addresses
- service.detection.sequence.resources.data.ec2NetworkInterface.privateIpAddresses.privateDnsName
- service.detection.sequence.resources.data.ec2NetworkInterface.privateIpAddresses.privateIpAddress
- service.detection.sequence.resources.data.ec2NetworkInterface.publicIp
- service.detection.sequence.resources.data.ec2NetworkInterface.securityGroups.groupId
- service.detection.sequence.resources.data.ec2NetworkInterface.securityGroups.groupName
- service.detection.sequence.resources.data.ec2NetworkInterface.subNetId
- service.detection.sequence.resources.data.ec2NetworkInterface.vpcId
- service.detection.sequence.resources.data.ec2Vpc.ec2InstanceUids
- service.detection.sequence.resources.data.ecsCluster.ec2InstanceUids
- service.detection.sequence.resources.data.ecsCluster.status
- service.detection.sequence.resources.data.ecsTask.containerUids
- service.detection.sequence.resources.data.ecsTask.createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.detection.sequence.resources.data.ecsTask.launchType
- service.detection.sequence.resources.data.ecsTask.taskDefinitionArn
- service.detection.sequence.resources.data.eksCluster.arn
- service.detection.sequence.resources.data.eksCluster.createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.detection.sequence.resources.data.eksCluster.ec2InstanceUids
- service.detection.sequence.resources.data.eksCluster.status
- service.detection.sequence.resources.data.eksCluster.vpcId
- service.detection.sequence.resources.data.iamInstanceProfile.ec2InstanceUids
- service.detection.sequence.resources.data.iamInstanceProfile.id
- service.detection.sequence.resources.data.kubernetesWorkload.containerUids
- service.detection.sequence.resources.data.kubernetesWorkload.namespace
- service.detection.sequence.resources.data.kubernetesWorkload.type
- service.detection.sequence.resources.data.s3Bucket.accountPublicAccess.publicAclAccess

- service.detection.sequence.resources.data.s3Bucket.accountPublicAccess.publicAclIgnoreBehavior
- service.detection.sequence.resources.data.s3Bucket.accountPublicAccess.publicBucketRestrictBehavio
- service.detection.sequence.resources.data.s3Bucket.accountPublicAccess.publicPolicyAccess
- service.detection.sequence.resources.data.s3Bucket.bucketPublicAccess.publicAclAccess
- service.detection.sequence.resources.data.s3Bucket.bucketPublicAccess.publicAclIgnoreBehavior
- service.detection.sequence.resources.data.s3Bucket.bucketPublicAccess.publicBucketRestrictBehavior
- service.detection.sequence.resources.data.s3Bucket.bucketPublicAccess.publicPolicyAccess
- service.detection.sequence.resources.data.s3Bucket.createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.detection.sequence.resources.data.s3Bucket.effectivePermission
- service.detection.sequence.resources.data.s3Bucket.encryptionKeyArn
- service.detection.sequence.resources.data.s3Bucket.encryptionType
- service.detection.sequence.resources.data.s3Bucket.ownerId
- service.detection.sequence.resources.data.s3Bucket.publicReadAccess
- service.detection.sequence.resources.data.s3Bucket.publicWriteAccess
- service.detection.sequence.resources.data.s3Bucket.s3ObjectUids
- service.detection.sequence.resources.data.s3Object.eTag
- service.detection.sequence.resources.data.s3Object.key
- service.detection.sequence.resources.data.s3Object.versionId
- service.detection.sequence.resources.name
- service.detection.sequence.resources.region
- service.detection.sequence.resources.resourceType
- service.detection.sequence.resources.service
- service.detection.sequence.resources.tags.key
- service.detection.sequence.resources.tags.value
- service.detection.sequence.resources.uid
- service.detection.sequence.sequenceIndicators.key
- service.detection.sequence.sequenceIndicators.title
- service.detection.sequence.sequenceIndicators.values
- service.detection.sequence.signals.actorIds

- service.detection.sequence.signals.count
- service.detection.sequence.signals.createdAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.detection.sequence.signals.description
- service.detection.sequence.signals.endpointIds
- service.detection.sequence.signals.firstSeenAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.detection.sequence.signals.lastSeenAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.detection.sequence.signals.name
- service.detection.sequence.signals.resourceUids
- service.detection.sequence.signals.severity
- service.detection.sequence.signals.signalIndicators.key
- service.detection.sequence.signals.signalIndicators.title
- service.detection.sequence.signals.signalIndicators.values
- service.detection.sequence.signals.type
- service.detection.sequence.signals.uid
- service.detection.sequence.signals.updatedAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.detection.sequence.uid
- service.detectorId
- service.ebsVolumeScanDetails.scanCompletedAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.ebsVolumeScanDetails.scanDetections.highestSeverityThreatDetails.count
- service.ebsVolumeScanDetails.scanDetections.highestSeverityThreatDetails.severity
- service.ebsVolumeScanDetails.scanDetections.highestSeverityThreatDetails.threatName
- service.ebsVolumeScanDetails.scanDetections.scannedItemCount.files
- service.ebsVolumeScanDetails.scanDetections.scannedItemCount.totalGb
- service.ebsVolumeScanDetails.scanDetections.scannedItemCount.volumes

- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.itemCount
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.shortened
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.fileNam
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.filePath
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.hash
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.volume
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.itemCount
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.name
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.severity
- service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.uniqueThreatNameCount
- service.ebsVolumeScanDetails.scanDetections.threatsDetectedItemCount.files
- service.ebsVolumeScanDetails.scanId
- service.ebsVolumeScanDetails.scanStartedAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.ebsVolumeScanDetails.scanType
- service.ebsVolumeScanDetails.sources
- service.ebsVolumeScanDetails.triggerFindingId
- service.eventFirstSeen

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.eventLastSeen

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.evidence.threatIntelligenceDetails.threatFileSha256
- service.evidence.threatIntelligenceDetails.threatListName
- service.evidence.threatIntelligenceDetails.threatNames
- service.featureName
- service.malwareScanDetails.scanCategory
- service.malwareScanDetails.scanConfiguration.incrementalScanDetails.baselineResourceArn
- service.malwareScanDetails.scanConfiguration.triggerType
- service.malwareScanDetails.scanId

- service.malwareScanDetails.scanType
- service.malwareScanDetails.threats.count
- service.malwareScanDetails.threats.hash
- service.malwareScanDetails.threats.itemDetails.additionalInfo.deviceName
- service.malwareScanDetails.threats.itemDetails.additionalInfo.versionId
- service.malwareScanDetails.threats.itemDetails.hash
- service.malwareScanDetails.threats.itemDetails.itemPath
- service.malwareScanDetails.threats.itemDetails.resourceArn
- service.malwareScanDetails.threats.itemPaths.hash
- service.malwareScanDetails.threats.itemPaths.nestedItemPath
- service.malwareScanDetails.threats.name
- service.malwareScanDetails.threats.source
- service.malwareScanDetails.uniqueThreatCount
- service.resourceRole
- service.runtimeDetails.context.addressFamily
- service.runtimeDetails.context.commandLineExample
- service.runtimeDetails.context.fileOperation
- service.runtimeDetails.context.filePath
- service.runtimeDetails.context.fileSystemType
- service.runtimeDetails.context.flags
- service.runtimeDetails.context.ianaProtocolNumber
- service.runtimeDetails.context.ldPreloadValue
- service.runtimeDetails.context.libraryPath
- service.runtimeDetails.context.memoryRegions
- service.runtimeDetails.context.modifiedAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.runtimeDetails.context.modifyingProcess.euid
- service.runtimeDetails.context.modifyingProcess.executablePath
- service.runtimeDetails.context.modifyingProcess.executableSha256
- service.runtimeDetails.context.modifyingProcess.lineage.euid

- service.runtimeDetails.context.modifyingProcess.lineage.executablePath
- service.runtimeDetails.context.modifyingProcess.lineage.name
- service.runtimeDetails.context.modifyingProcess.lineage.namespacePid
- service.runtimeDetails.context.modifyingProcess.lineage.parentUuid
- service.runtimeDetails.context.modifyingProcess.lineage.pid
- service.runtimeDetails.context.modifyingProcess.lineage.startTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.runtimeDetails.context.modifyingProcess.lineage.userId
- service.runtimeDetails.context.modifyingProcess.lineage.uuid
- service.runtimeDetails.context.modifyingProcess.name
- service.runtimeDetails.context.modifyingProcess.namespacePid
- service.runtimeDetails.context.modifyingProcess.parentUuid
- service.runtimeDetails.context.modifyingProcess.pid
- service.runtimeDetails.context.modifyingProcess.pwd
- service.runtimeDetails.context.modifyingProcess.startTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.runtimeDetails.context.modifyingProcess.user
- service.runtimeDetails.context.modifyingProcess.userId
- service.runtimeDetails.context.modifyingProcess.uuid
- service.runtimeDetails.context.moduleFilePath
- service.runtimeDetails.context.moduleName
- service.runtimeDetails.context.moduleSha256
- service.runtimeDetails.context.mountSource
- service.runtimeDetails.context.mountTarget
- service.runtimeDetails.context.relatedFilePaths
- service.runtimeDetails.context.releaseAgentPath
- service.runtimeDetails.context.runcBinaryPath
- service.runtimeDetails.context.scriptPath
- service.runtimeDetails.context.serviceName
- service.runtimeDetails.context.shellHistoryFilePath

- service.runtimeDetails.context.socketPath
- service.runtimeDetails.context.targetProcess.euid
- service.runtimeDetails.context.targetProcess.executablePath
- service.runtimeDetails.context.targetProcess.executableSha256
- service.runtimeDetails.context.targetProcess.lineage.euid
- service.runtimeDetails.context.targetProcess.lineage.executablePath
- service.runtimeDetails.context.targetProcess.lineage.name
- service.runtimeDetails.context.targetProcess.lineage.namespacePid
- service.runtimeDetails.context.targetProcess.lineage.parentUuid
- service.runtimeDetails.context.targetProcess.lineage.pid
- service.runtimeDetails.context.targetProcess.lineage.startTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.runtimeDetails.context.targetProcess.lineage.userId
- service.runtimeDetails.context.targetProcess.lineage.uuid
- service.runtimeDetails.context.targetProcess.name
- service.runtimeDetails.context.targetProcess.namespacePid
- service.runtimeDetails.context.targetProcess.parentUuid
- service.runtimeDetails.context.targetProcess.pid
- service.runtimeDetails.context.targetProcess.pwd
- service.runtimeDetails.context.targetProcess.startTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.runtimeDetails.context.targetProcess.user
- service.runtimeDetails.context.targetProcess.userId
- service.runtimeDetails.context.targetProcess.uuid
- service.runtimeDetails.context.threatFilePath
- service.runtimeDetails.context.toolCategory
- service.runtimeDetails.context.toolName
- service.runtimeDetails.process.euid
- service.runtimeDetails.process.executablePath
- service.runtimeDetails.process.executableSha256

- service.runtimeDetails.process.lineage.euid
- service.runtimeDetails.process.lineage.executablePath
- service.runtimeDetails.process.lineage.name
- service.runtimeDetails.process.lineage.namespacePid
- service.runtimeDetails.process.lineage.parentUuid
- service.runtimeDetails.process.lineage.pid
- service.runtimeDetails.process.lineage.startTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.runtimeDetails.process.lineage.userId
- service.runtimeDetails.process.lineage.uuid
- service.runtimeDetails.process.name
- service.runtimeDetails.process.namespacePid
- service.runtimeDetails.process.parentUuid
- service.runtimeDetails.process.pid
- service.runtimeDetails.process.pwd
- service.runtimeDetails.process.startTime

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000
- service.runtimeDetails.process.user
- service.runtimeDetails.process.userId
- service.runtimeDetails.process.uuid
- service.serviceName
- service.userFeedback
- severity

  To configure severity based filters, use the following for the FindingCriteria condition:

  - **Low**: `["1", "2", "3"]`
  - **Medium**: `["4", "5", "6"]`
  - **High**: `["7", "8"]`
  - **Critical**: `["9", "10"]`

  For more information, see Findings severity levels in the *Amazon GuardDuty User Guide*.

- type
- updatedAt

  Type: Timestamp in Unix Epoch millisecond format. Ex: 1486685375000

Type: FindingCriteria object

Required: No

rank

Specifies the position of the filter in the list of current filters. Also specifies the order in which this filter is applied to the findings.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "name": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

name

The name of the filter.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 64.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateFindingsFeedback

Marks the specified GuardDuty findings as useful or not useful.

Request Syntax

```
POST /detector/DetectorId/findings/feedback HTTP/1.1
Content-type: application/json

{
   "comments": "string",
   "feedback": "string",
   "findingIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The ID of the detector that is associated with the findings for which you want to update the feedback.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

comments

Additional feedback about the GuardDuty findings.

Type: String

Required: No

feedback

The feedback for the finding.

Type: String

Valid Values: `USEFUL | NOT_USEFUL`

Required: Yes

findingIds

The IDs of the findings that you want to mark as useful or not useful.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateIPSet

Updates the IPSet specified by the IPSet ID.

Request Syntax

```
POST /detector/DetectorId/ipset/IpSetId HTTP/1.1
Content-type: application/json

{
   "activate": boolean,
   "expectedBucketOwner": "string",
   "location": "string",
   "name": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The detectorID that specifies the GuardDuty service whose IPSet you want to update.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

IpSetId

The unique ID that specifies the IPSet that you want to update.

Required: Yes

Request Body

The request accepts the following data in JSON format.

activate

The updated Boolean value that specifies whether the IPSet is active or not.

Type: Boolean

Required: No

expectedBucketOwner

The AWS account ID that owns the Amazon S3 bucket specified in the **location** parameter.

Type: String

Length Constraints: Fixed length of 12.

Required: No

location

The updated URI of the file that contains the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

name

The unique ID that specifies the IPSet that you want to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateMalwareProtectionPlan

Updates an existing Malware Protection plan resource.

Request Syntax

```
PATCH /malware-protection-plan/MalwareProtectionPlanId HTTP/1.1
Content-type: application/json

{
   "actions": {
      "tagging": {
         "status": "string"
      }
   },
   "protectedResource": {
      "s3Bucket": {
         "objectPrefixes": [ "string" ]
      }
   },
   "role": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

MalwareProtectionPlanId

A unique identifier associated with the Malware Protection plan.

Required: Yes

Request Body

The request accepts the following data in JSON format.

actions

Information about whether the tags will be added to the S3 object after scanning.

Type: MalwareProtectionPlanActions object

Required: No

protectedResource

Information about the protected resource that is associated with the created Malware Protection plan. Presently, `S3Bucket` is the only supported protected resource.

Type: UpdateProtectedResource object

Required: No

role

Amazon Resource Name (ARN) of the IAM role with permissions to scan and add tags to the associated protected resource.

Type: String

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

ResourceNotFoundException

The requested resource can't be found.

Message

The error message.

Type

The error type.

HTTP Status Code: 404

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateMalwareScanSettings

Updates the malware scan settings.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see Regions and endpoints.

Request Syntax

```
POST /detector/DetectorId/malware-scan-settings HTTP/1.1
Content-type: application/json

{
   "ebsSnapshotPreservation": "string",
   "scanResourceCriteria": {
      "exclude": {
         "string" : {
            "mapEquals": [
               {
                  "key": "string",
                  "value": "string"
               }
            ]
         }
      },
      "include": {
         "string" : {
            "mapEquals": [
               {
                  "key": "string",
                  "value": "string"
               }
            ]
         }
      }
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the detector that specifies the GuardDuty service where you want to update scan settings.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

ebsSnapshotPreservation

An enum value representing possible snapshot preservation settings.

Type: String

Valid Values: `NO_RETENTION | RETENTION_WITH_FINDING`

Required: No

scanResourceCriteria

Represents the criteria to be used in the filter for selecting resources to scan.

Type: ScanResourceCriteria object

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateMemberDetectors

Contains information on member accounts to be updated.

Specifying both EKS Runtime Monitoring (`EKS_RUNTIME_MONITORING`) and Runtime Monitoring (`RUNTIME_MONITORING`) will cause an error. You can add only one of these two features because Runtime Monitoring already includes the threat detection for Amazon EKS resources. For more information, see Runtime Monitoring.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see Regions and endpoints.

Request Syntax

```
POST /detector/DetectorId/member/detector/update HTTP/1.1
Content-type: application/json

{
   "accountIds": [ "string" ],
   "dataSources": {
      "kubernetes": {
         "auditLogs": {
            "enable": boolean
         }
      },
      "malwareProtection": {
         "scanEc2InstanceWithFindings": {
            "ebsVolumes": boolean
         }
      },
      "s3Logs": {
         "enable": boolean
      }
   },
   "features": [
      {
         "additionalConfiguration": [
            {
               "name": "string",
               "status": "string"
            }
```

```
            ],
            "name": "string",
            "status": "string"
        }
    ]
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The detector ID of the administrator account.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds

A list of member account IDs to be updated.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

dataSources

This parameter has been deprecated.

Describes which data sources will be updated.

Type: DataSourceConfigurations object

Required: No

features

A list of features that will be updated for the specified member accounts.

Type: Array of MemberFeaturesConfiguration objects

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

unprocessedAccounts

A list of member account IDs that were unable to be processed along with an explanation for why they were not processed.

Type: Array of UnprocessedAccount objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateOrganizationConfiguration

Configures the delegated administrator account with the provided values. You must provide a value for either `autoEnableOrganizationMembers` or `autoEnable`, but not both.

Specifying both EKS Runtime Monitoring (`EKS_RUNTIME_MONITORING`) and Runtime Monitoring (`RUNTIME_MONITORING`) will cause an error. You can add only one of these two features because Runtime Monitoring already includes the threat detection for Amazon EKS resources. For more information, see Runtime Monitoring.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see Regions and endpoints.

Request Syntax

```
POST /detector/DetectorId/admin HTTP/1.1
Content-type: application/json

{
   "autoEnable": boolean,
   "autoEnableOrganizationMembers": "string",
   "dataSources": {
      "kubernetes": {
         "auditLogs": {
            "autoEnable": boolean
         }
      },
      "malwareProtection": {
         "scanEc2InstanceWithFindings": {
            "ebsVolumes": {
               "autoEnable": boolean
            }
         }
      },
      "s3Logs": {
         "autoEnable": boolean
      }
   },
   "features": [
      {
         "additionalConfiguration": [
```

```
            {
               "autoEnable": "string",
               "name": "string"
            }
         ],
         "autoEnable": "string",
         "name": "string"
      }
   ]
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The ID of the detector that configures the delegated administrator.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

autoEnable

This parameter has been deprecated.

Represents whether to automatically enable member accounts in the organization. This applies to only new member accounts, not the existing member accounts. When a new account joins the organization, the chosen features will be enabled for them by default.

Even though this is still supported, we recommend using `AutoEnableOrganizationMembers` to achieve the similar results. You must provide a value for either `autoEnableOrganizationMembers` or `autoEnable`.

Type: Boolean

Required: No

autoEnableOrganizationMembers

Indicates the auto-enablement configuration of GuardDuty for the member accounts in the organization. You must provide a value for either `autoEnableOrganizationMembers` or `autoEnable`.

Use one of the following configuration values for `autoEnableOrganizationMembers`:

- `NEW`: Indicates that when a new account joins the organization, they will have GuardDuty enabled automatically.
- `ALL`: Indicates that all accounts in the organization have GuardDuty enabled automatically. This includes `NEW` accounts that join the organization and accounts that may have been suspended or removed from the organization in GuardDuty.

  It may take up to 24 hours to update the configuration for all the member accounts.
- `NONE`: Indicates that GuardDuty will not be automatically enabled for any account in the organization. The administrator must manage GuardDuty for each account in the organization individually.

  When you update the auto-enable setting from `ALL` or `NEW` to `NONE`, this action doesn't disable the corresponding option for your existing accounts. This configuration will apply to the new accounts that join the organization. After you update the auto-enable settings, no new account will have the corresponding option as enabled.

Type: String

Valid Values: `NEW | ALL | NONE`

Required: No

dataSources

This parameter has been deprecated.

Describes which data sources will be updated.

Type: OrganizationDataSourceConfigurations object

Required: No

features

A list of features that will be configured for the organization.

Type: Array of OrganizationFeatureConfiguration objects

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdatePublishingDestination

Updates information about the publishing destination specified by the `destinationId`.

Request Syntax

```
POST /detector/DetectorId/publishingDestination/DestinationId HTTP/1.1
Content-type: application/json

{
   "destinationProperties": {
      "destinationArn": "string",
      "kmsKeyArn": "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

DestinationId

The ID of the publishing destination to update.

Required: Yes

DetectorId

The ID of the detector associated with the publishing destinations to update.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

destinationProperties

A `DestinationProperties` object that includes the `DestinationArn` and `KmsKeyArn` of the publishing destination.

Type: DestinationProperties object

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateThreatEntitySet

Updates the threat entity set associated with the specified `threatEntitySetId`.

Request Syntax

```
POST /detector/DetectorId/threatentityset/ThreatEntitySetId HTTP/1.1
Content-type: application/json

{
   "activate": boolean,
   "expectedBucketOwner": "string",
   "location": "string",
   "name": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the GuardDuty detector associated with the threat entity set that you want to update.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

ThreatEntitySetId

The ID returned by GuardDuty after updating the threat entity set resource.

Required: Yes

Request Body

The request accepts the following data in JSON format.

activate

A boolean value that indicates whether GuardDuty is to start using this updated threat entity set. After you update an entity set, you will need to activate it again. It might take up to 15 minutes for the updated entity set to be effective.

Type: Boolean

Required: No

expectedBucketOwner

The AWS account ID that owns the Amazon S3 bucket specified in the **location** parameter.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `[0-9]+`

Required: No

location

The URI of the file that contains the trusted entity set.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

name

A user-friendly name to identify the trusted entity set.

The name of your list can include lowercase letters, uppercase letters, numbers, dash (-), and underscore (_).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateThreatIntelSet

Updates the ThreatIntelSet specified by the ThreatIntelSet ID.

Request Syntax

```
POST /detector/DetectorId/threatintelset/ThreatIntelSetId HTTP/1.1
Content-type: application/json

{
   "activate": boolean,
   "expectedBucketOwner": "string",
   "location": "string",
   "name": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The detectorID that specifies the GuardDuty service whose ThreatIntelSet you want to update.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

ThreatIntelSetId

The unique ID that specifies the ThreatIntelSet that you want to update.

Required: Yes

Request Body

The request accepts the following data in JSON format.

activate

The updated Boolean value that specifies whether the ThreateIntelSet is active or not.

Type: Boolean

Required: No

expectedBucketOwner

The AWS account ID that owns the Amazon S3 bucket specified in the **location** parameter.

Type: String

Length Constraints: Fixed length of 12.

Required: No

location

The updated URI of the file that contains the ThreateIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

name

The unique ID that specifies the ThreatIntelSet that you want to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

An access denied exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 403

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateTrustedEntitySet

Updates the trusted entity set associated with the specified `trustedEntitySetId`.

Request Syntax

```
POST /detector/DetectorId/trustedentityset/TrustedEntitySetId HTTP/1.1
Content-type: application/json

{
   "activate": boolean,
   "expectedBucketOwner": "string",
   "location": "string",
   "name": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

DetectorId

The unique ID of the GuardDuty detector associated with the threat entity set that you want to update.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

TrustedEntitySetId

The ID returned by GuardDuty after updating the trusted entity set resource.

Required: Yes

Request Body

The request accepts the following data in JSON format.

activate

A boolean value that indicates whether GuardDuty is to start using this updated trusted entity set. After you update an entity set, you will need to activate it again. It might take up to 15 minutes for the updated entity set to be effective.

Type: Boolean

Required: No

expectedBucketOwner

The AWS account ID that owns the Amazon S3 bucket specified in the **location** parameter.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `[0-9]+`

Required: No

location

The URI of the file that contains the trusted entity set.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

name

A user-friendly name to identify the trusted entity set.

The name of your list can include lowercase letters, uppercase letters, numbers, dash (-), and underscore (_).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

BadRequestException

A bad request exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

Message

The error message.

Type

The error type.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

Data Types

The Amazon GuardDuty API contains several data types that various actions use. This section describes each data type in detail.

> **Note**
>
> The order of each element in a data type structure is not guaranteed. Applications should not assume a particular order.

The following data types are supported:

- AccessControlList
- AccessKey
- AccessKeyDetails
- Account
- AccountDetail
- AccountFreeTrialInfo
- AccountLevelPermissions
- AccountStatistics
- Action
- Activity
- Actor
- ActorProcess
- AdditionalInfo
- AddonDetails
- AdminAccount
- Administrator
- AgentDetails
- Anomaly
- AnomalyObject
- AnomalyUnusual

- ApiCall
- AssociationDetail
- AssociationSummary
- AutonomousSystem
- AutoscalingAutoScalingGroup
- AwsApiCallAction
- BedrockGuardrail
- BedrockGuardrailDetails
- BedrockGuardrailResource
- BlockPublicAccess
- BucketLevelPermissions
- BucketPolicy
- City
- CloudDetails
- CloudformationStack
- CloudTrailConfigurationResult
- Condition
- Container
- ContainerFindingResource
- ContainerInstanceDetails
- ContentPolicyFilter
- ContinuousScanDetails
- Country
- CoverageEc2InstanceDetails
- CoverageEcsClusterDetails
- CoverageEksClusterDetails
- CoverageFilterCondition
- CoverageFilterCriteria
- CoverageFilterCriterion
- CoverageResource

- CoverageResourceDetails
- CoverageSortCriteria
- CoverageStatistics
- CreateProtectedResource
- CreateS3BucketResource
- DataSourceConfigurations
- DataSourceConfigurationsResult
- DataSourceFreeTrial
- DataSourcesFreeTrial
- DateStatistics
- DefaultServerSideEncryption
- Destination
- DestinationProperties
- Detection
- DetectionRuleEc2Requirements
- DetectionRuleEcsFargateRequirements
- DetectionRuleEksRequirements
- DetectionRuleFilter
- DetectionRuleOrgConfiguration
- DetectionRuleOrgConfigurationSummary
- DetectionRuleRuntimeMonitoringDetails
- DetectionRuleRuntimePlatforms
- DetectorAdditionalConfiguration
- DetectorAdditionalConfigurationResult
- DetectorFeatureConfiguration
- DetectorFeatureConfigurationResult
- DNSLogsConfigurationResult
- DnsRequestAction
- DomainDetails
- EbsSnapshot

- EbsSnapshotDetails
- EbsVolumeDetails
- EbsVolumeScanDetails
- EbsVolumesResult
- Ec2Image
- Ec2ImageDetails
- Ec2Instance
- Ec2LaunchTemplate
- Ec2NetworkInterface
- Ec2Vpc
- EcsCluster
- EcsClusterDetails
- EcsTask
- EcsTaskDetails
- EksCluster
- EksClusterDetails
- Evidence
- FargateDetails
- FilterCondition
- FilterCriteria
- FilterCriterion
- Finding
- FindingCriteria
- FindingStatistics
- FindingTypeStatistics
- FlowLogsConfigurationResult
- FreeTrialFeatureConfigurationResult
- GeoLocation
- GetMalwareScanResultDetails
- HighestSeverityThreatDetails

- HostPath
- IamInstanceProfile
- IamInstanceProfileV2
- ImpersonatedUser
- IncrementalScanDetails
- Indicator
- InstanceDetails
- Investigation
- InvestigationMetadata
- InvestigationSortCriteria
- InvestigationSummary
- Invitation
- ItemDetails
- ItemPath
- KubernetesApiCallAction
- KubernetesAuditLogsConfiguration
- KubernetesAuditLogsConfigurationResult
- KubernetesConfiguration
- KubernetesConfigurationResult
- KubernetesDataSourceFreeTrial
- KubernetesDetails
- KubernetesPermissionCheckedDetails
- KubernetesRoleBindingDetails
- KubernetesRoleDetails
- KubernetesUserDetails
- KubernetesWorkload
- KubernetesWorkloadDetails
- LambdaDetails
- LineageObject
- ListMalwareScansFilterCriteria

- ListMalwareScansFilterCriterion
- LocalIpDetails
- LocalPortDetails
- LoginAttribute
- MalwareProtectionConfiguration
- MalwareProtectionConfigurationResult
- MalwareProtectionDataSourceFreeTrial
- MalwareProtectionFindingsScanConfiguration
- MalwareProtectionPlanActions
- MalwareProtectionPlanStatusReason
- MalwareProtectionPlanSummary
- MalwareProtectionPlanTaggingAction
- MalwareScan
- MalwareScanDetails
- Master
- Member
- MemberAdditionalConfiguration
- MemberAdditionalConfigurationResult
- MemberDataSourceConfiguration
- MemberFeaturesConfiguration
- MemberFeaturesConfigurationResult
- ModelDetail
- NetworkConnection
- NetworkConnectionAction
- NetworkEndpoint
- NetworkGeoLocation
- NetworkInterface
- Observations
- Organization
- OrganizationAdditionalConfiguration

- OrganizationAdditionalConfigurationResult
- OrganizationDataSourceConfigurations
- OrganizationDataSourceConfigurationsResult
- OrganizationDetails
- OrganizationEbsVolumes
- OrganizationEbsVolumesResult
- OrganizationFeatureConfiguration
- OrganizationFeatureConfigurationResult
- OrganizationFeatureStatistics
- OrganizationFeatureStatisticsAdditionalConfiguration
- OrganizationKubernetesAuditLogsConfiguration
- OrganizationKubernetesAuditLogsConfigurationResult
- OrganizationKubernetesConfiguration
- OrganizationKubernetesConfigurationResult
- OrganizationMalwareProtectionConfiguration
- OrganizationMalwareProtectionConfigurationResult
- OrganizationS3LogsConfiguration
- OrganizationS3LogsConfigurationResult
- OrganizationScanEc2InstanceWithFindings
- OrganizationScanEc2InstanceWithFindingsResult
- OrganizationStatistics
- Owner
- PermissionConfiguration
- PortProbeAction
- PortProbeDetail
- PrivateIpAddressDetails
- ProcessDetails
- Product
- ProductCode
- PublicAccess

- PublicAccessConfiguration
- RdsDbInstanceDetails
- RdsDbUserDetails
- RdsLimitlessDbDetails
- RdsLoginAttemptAction
- RecoveryPoint
- RecoveryPointDetails
- RemoteAccountDetails
- RemoteIpDetails
- RemotePortDetails
- Resource
- ResourceData
- ResourceDetails
- ResourceStatistics
- ResourceV2
- RuleDefinition
- RuleDetail
- RuleSummary
- RuntimeContext
- RuntimeDetails
- S3Bucket
- S3BucketDetail
- S3LogsConfiguration
- S3LogsConfigurationResult
- S3Object
- S3ObjectDetail
- S3ObjectForSendObjectMalwareScan
- Scan
- ScanCondition
- ScanConditionPair

- ScanConfiguration
- ScanConfigurationContinuousScanDetails
- ScanConfigurationRecoveryPoint
- ScanDetections
- ScanEc2InstanceWithFindings
- ScanEc2InstanceWithFindingsResult
- ScanFilePath
- ScannedItemCount
- ScannedResource
- ScannedResourceDetails
- ScanResourceCriteria
- ScanResultDetails
- ScanResultThreat
- ScanThreatName
- SecurityContext
- SecurityGroup
- Sequence
- Service
- ServiceAdditionalInfo
- Session
- SeverityStatistics
- Signal
- SortCriteria
- StartMalwareScanConfiguration
- Tag
- Threat
- ThreatDetectedByName
- ThreatIntelligenceDetail
- ThreatsDetectedItemCount
- Total

- TriggerDetails
- UnprocessedAccount
- UnprocessedDataSourcesResult
- UpdateProtectedResource
- UpdateS3BucketResource
- UsageAccountResult
- UsageCriteria
- UsageDataSourceResult
- UsageFeatureResult
- UsageResourceResult
- UsageStatistics
- UsageTopAccountResult
- UsageTopAccountsResult
- User
- Volume
- VolumeDetail
- VolumeMount
- VpcConfig

AccessControlList

Contains information on the current access control policies for the bucket.

Contents

allowsPublicReadAccess

A value that indicates whether public read access for the bucket is enabled through an Access Control List (ACL).

Type: Boolean

Required: No

allowsPublicWriteAccess

A value that indicates whether public write access for the bucket is enabled through an Access Control List (ACL).

Type: Boolean

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AccessKey

Contains information about the access keys.

Contents

principalId

Principal ID of the user.

Type: String

Required: No

userName

Name of the user.

Type: String

Required: No

userType

Type of the user.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AccessKeyDetails

Contains information about the access keys.

Contents

accessKeyId

The access key ID of the user.

Type: String

Required: No

principalId

The principal ID of the user.

Type: String

Required: No

userName

The name of the user.

Type: String

Required: No

userType

The type of the user.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

Account

Contains information about the AWS account within which the activity took place.

Contents

uid

The AWS account ID within which the activity took place. This may differ from the account that owns the user identity.

Type: String

Required: Yes

account

Name of the member's AWS account.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AccountDetail

Contains information about the account.

Contents

accountId

The member account ID.

Type: String

Length Constraints: Fixed length of 12.

Required: Yes

email

The email address of the member account. The following list includes the rules for a valid email address:

- The email address must be a minimum of 6 and a maximum of 64 characters long.
- All characters must be 7-bit ASCII characters.
- There must be one and only one @ symbol, which separates the local name from the domain name.
- The local name can't contain any of the following characters:

  whitespace, " ' ( ) < > [ ] : ' , \ | % &
- The local name can't begin with a dot (.).
- The domain name can consist of only the characters [a-z], [A-Z], [0-9], hyphen (-), or dot (.).
- The domain name can't begin or end with a dot (.) or hyphen (-).
- The domain name must contain at least one dot.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AccountFreeTrialInfo

Provides details of the GuardDuty member account that uses a free trial service.

Contents

accountId

The account identifier of the GuardDuty member account.

Type: String

Required: No

dataSources

This member has been deprecated.

Describes the data source enabled for the GuardDuty member account.

Type: DataSourcesFreeTrial object

Required: No

features

A list of features enabled for the GuardDuty account.

Type: Array of FreeTrialFeatureConfigurationResult objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AccountLevelPermissions

Contains information about the account level permissions on the S3 bucket.

Contents

blockPublicAccess

Describes the S3 Block Public Access settings of the bucket's parent account.

Type: BlockPublicAccess object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AccountStatistics

Represents a list of map of accounts with the number of findings associated with each account.

Contents

accountId

The ID of the AWS account.

Type: String

Required: No

lastGeneratedAt

The timestamp at which the finding for this account was last generated.

Type: Timestamp

Required: No

totalFindings

The total number of findings associated with an account.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Action

Contains information about actions.

Contents

actionType

The GuardDuty finding activity type.

Type: String

Required: No

awsApiCallAction

Information about the AWS_API_CALL action described in this finding.

Type: AwsApiCallAction object

Required: No

dnsRequestAction

Information about the DNS_REQUEST action described in this finding.

Type: DnsRequestAction object

Required: No

kubernetesApiCallAction

Information about the Kubernetes API call action described in this finding.

Type: KubernetesApiCallAction object

Required: No

kubernetesPermissionCheckedDetails

Information whether the user has the permission to use a specific Kubernetes API.

Type: KubernetesPermissionCheckedDetails object

Required: No

kubernetesRoleBindingDetails

Information about the role binding that grants the permission defined in a Kubernetes role.

Type: KubernetesRoleBindingDetails object

Required: No

kubernetesRoleDetails

Information about the Kubernetes role name and role type.

Type: KubernetesRoleDetails object

Required: No

networkConnectionAction

Information about the NETWORK_CONNECTION action described in this finding.

Type: NetworkConnectionAction object

Required: No

portProbeAction

Information about the PORT_PROBE action described in this finding.

Type: PortProbeAction object

Required: No

rdsLoginAttemptAction

Information about `RDS_LOGIN_ATTEMPT` action described in this finding.

Type: RdsLoginAttemptAction object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Activity

Contains information about an activity, such as an API call, that was observed for a signal.

Contents

type

The type of the observed activity.

Type: String

Valid Values: `API_CALL`

Required: Yes

api

Contains information about the API call that was observed, when the activity type is `API_CALL`.

Type: ApiCall object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Actor

Information about the actors involved in an attack sequence.

Contents

id

ID of the threat actor.

Type: String

Required: Yes

process

Contains information about the process associated with the threat actor. This includes details such as process name, path, execution time, and unique identifiers that help track the actor's activities within the system.

Type: ActorProcess object

Required: No

session

Contains information about the user session where the activity initiated.

Type: Session object

Required: No

user

Contains information about the user credentials used by the threat actor.

Type: User object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ActorProcess

Contains information about a process involved in a GuardDuty finding, including process identification, execution details, and file information.

Contents

name

The name of the process as it appears in the system.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 4096.

Required: Yes

path

The full file path to the process executable on the system.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 4096.

Required: Yes

sha256

The SHA256 hash of the process executable file, which can be used for identification and verification purposes.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AdditionalInfo

Contains additional information about the detected threat.

Contents

deviceName

The device name of the EBS volume, if applicable.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

versionId

The version ID of the S3 object, if applicable.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AddonDetails

Information about the installed EKS add-on (GuardDuty security agent).

Contents

addonStatus

Status of the installed EKS add-on.

Type: String

Required: No

addonVersion

Version of the installed EKS add-on.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AdminAccount

The account within the organization specified as the GuardDuty delegated administrator.

Contents

adminAccountId

The AWS account ID for the account.

Type: String

Required: No

adminStatus

Indicates whether the account is enabled as the delegated administrator.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `ENABLED | DISABLE_IN_PROGRESS`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Administrator

Contains information about the administrator account and invitation.

Contents

accountId

The ID of the account used as the administrator account.

Type: String

Length Constraints: Fixed length of 12.

Required: No

invitationId

The value that is used to validate the administrator account to the member account.

Type: String

Required: No

invitedAt

The timestamp when the invitation was sent.

Type: String

Required: No

relationshipStatus

The status of the relationship between the administrator and member accounts.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AgentDetails

Information about the installed GuardDuty security agent.

Contents

version

Version of the installed GuardDuty security agent.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Anomaly

Contains information about the anomalies.

Contents

profiles

Information about the types of profiles.

Type: String to string to array of AnomalyObject objects map map

Required: No

unusual

Information about the behavior of the anomalies.

Type: AnomalyUnusual object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AnomalyObject

Contains information about the unusual anomalies.

Contents

observations

The recorded value.

Type: Observations object

Required: No

profileSubtype

The frequency of the anomaly.

Type: String

Valid Values: `FREQUENT | INFREQUENT | UNSEEN | RARE | COUNT | AVERAGE`

Required: No

profileType

The type of behavior of the profile.

Type: String

Valid Values: `FREQUENCY | VOLUME`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AnomalyUnusual

Contains information about the behavior of the anomaly that is new to GuardDuty.

Contents

behavior

The behavior of the anomalous activity that caused GuardDuty to generate the finding.

Type: String to string to AnomalyObject object map map

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ApiCall

Contains information about an API call that was observed as part of an activity.

Contents

error

The error code that was returned, if the API call failed.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 512.

Required: No

operation

The name of the API operation that was invoked.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 512.

Required: No

service

The service that the API operation was invoked against.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 512.

Required: No

userAgent

User agent in the request to the API operation

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AssociationDetail

Contains the full details of a custom detection rule association.

Contents

accountId

The AWS account ID associated with this rule association.

Type: String

Length Constraints: Fixed length of 12.

Required: Yes

arn

The Amazon Resource Name (ARN) of the association.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `arn:[a-zA-Z0-9\-]+:[a-zA-Z0-9\-]+:[a-zA-Z0-9\-]*:([0-9]*|aws):.+`

Required: Yes

associationId

The unique identifier for the association.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-zA-Z0-9_-]{1,64}`

Required: Yes

createdAt

The timestamp when the association was created.

Type: Timestamp

Required: Yes

mode

The rule execution mode. Valid values: `LIVE` | `DRY_RUN`.

Type: String

Valid Values: `LIVE | DRY_RUN`

Required: Yes

ruleId

The unique identifier for the custom detection rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Required: Yes

updatedAt

The timestamp when the association was last updated.

Type: Timestamp

Required: Yes

expiresAt

The timestamp when the association expires.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AssociationSummary

Contains summary information about a custom detection rule association.

Contents

arn

The Amazon Resource Name (ARN) of the association.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `arn:[a-zA-Z0-9\-]+:[a-zA-Z0-9\-]+:[a-zA-Z0-9\-]*:([0-9]*|aws):.+`

Required: Yes

associationId

The unique identifier for the association.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-zA-Z0-9_-]{1,64}`

Required: Yes

createdAt

The timestamp when the association was created.

Type: Timestamp

Required: Yes

mode

The rule execution mode. Valid values: `LIVE` | `DRY_RUN`.

Type: String

Valid Values: `LIVE | DRY_RUN`

Required: Yes

ruleId

The unique identifier for the custom detection rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Required: Yes

updatedAt

The timestamp when the association was last updated.

Type: Timestamp

Required: Yes

expiresAt

The timestamp when the association expires.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AutonomousSystem

Contains information about the Autonomous System (AS) associated with the network endpoints involved in an attack sequence.

Contents

name

Name associated with the Autonomous System (AS).

Type: String

Required: Yes

number

The unique number that identifies the Autonomous System (AS).

Type: Integer

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AutoscalingAutoScalingGroup

Contains information about the Auto Scaling Group involved in a GuardDuty finding, including unique identifiers of the Amazon EC2 instances.

Contents

ec2InstanceUids

A list of unique identifiers for the compromised Amazon EC2 instances that are part of the same Auto Scaling Group.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 25 items.

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AwsApiCallAction

Contains information about the API action.

Contents

affectedResources

The details of the AWS account that made the API call. This field identifies the resources that were affected by this API call.

Type: String to string map

Required: No

api

The AWS API name.

Type: String

Required: No

callerType

The AWS API caller type.

Type: String

Required: No

domainDetails

The domain information for the AWS API call.

Type: DomainDetails object

Required: No

errorCode

The error code of the failed AWS API action.

Type: String

Required: No

remoteAccountDetails

The details of the AWS account that made the API call. This field appears if the call was made from outside your account.

Type: RemoteAccountDetails object

Required: No

remoteIpDetails

The remote IP information of the connection that initiated the AWS API call.

Type: RemoteIpDetails object

Required: No

serviceName

The AWS service name whose API was invoked.

Type: String

Required: No

userAgent

The agent through which the API request was made.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BedrockGuardrail

Contains information about a Bedrock guardrail associated with a finding.

Contents

arn

The ARN of the Bedrock guardrail.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

Pattern: `arn:aws(-[^:]+)?:bedrock:[a-z0-9-]{1,20}:[0-9]{12}:guardrail/[a-z0-9]+`

Required: No

version

The version of the Bedrock guardrail.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 8.

Pattern: `(([1-9][0-9]{0,7})|(DRAFT)|(ENFORCED))`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BedrockGuardrailDetails

Contains information about the Bedrock guardrail that was involved in a finding.

Contents

contentPolicyFilters

The list of content policy filters that matched during the guardrail evaluation.

Type: Array of ContentPolicyFilter objects

Array Members: Minimum number of 0 items. Maximum number of 10 items.

Required: No

guardrailAction

Indicates whether the guardrail intervened or not.

Type: String

Valid Values: `GUARDRAIL_INTERVENED | NONE`

Required: No

guardrailArn

The ARN of the Bedrock guardrail. This field is deprecated. Use the `guardrails` list instead.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

Pattern: `arn:aws(-[^:]+)?:bedrock:[a-z0-9-]{1,20}:[0-9]{12}:guardrail/[a-z0-9]+`

Required: No

guardrails

The list of Bedrock guardrails associated with the finding.

Type: Array of BedrockGuardrail objects

Array Members: Minimum number of 0 items. Maximum number of 10 items.

Required: No

guardrailSource

Indicates whether the guardrail was applied on the input or output of the model invocation.

Type: String

Valid Values: `INPUT | OUTPUT`

Required: No

guardrailVersion

The version of the Bedrock guardrail. This field is deprecated. Use the `guardrails` list instead.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 8.

Pattern: `(([1-9][0-9]{0,7})|(DRAFT))`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BedrockGuardrailResource

Contains details about an Amazon Bedrock guardrail evaluated during a model invocation.

Contents

guardrailAction

Indicates whether the guardrail intervened during the model invocation.

Type: String

Valid Values: `GUARDRAIL_INTERVENED | NONE`

Required: No

guardrailSource

Indicates whether the guardrail was applied on the input or output of the model invocation.

Type: String

Valid Values: `INPUT | OUTPUT`

Required: No

version

The version of the Amazon Bedrock guardrail. Valid values are a numeric version, `DRAFT`, or `ENFORCED`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 8.

Pattern: `(([1-9][0-9]{0,7})|(DRAFT)|(ENFORCED))`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BlockPublicAccess

Contains information on how the bucker owner's S3 Block Public Access settings are being applied to the S3 bucket. See S3 Block Public Access for more information.

Contents

blockPublicAcls

Indicates if S3 Block Public Access is set to `BlockPublicAcls`.

Type: Boolean

Required: No

blockPublicPolicy

Indicates if S3 Block Public Access is set to `BlockPublicPolicy`.

Type: Boolean

Required: No

ignorePublicAcls

Indicates if S3 Block Public Access is set to `IgnorePublicAcls`.

Type: Boolean

Required: No

restrictPublicBuckets

Indicates if S3 Block Public Access is set to `RestrictPublicBuckets`.

Type: Boolean

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BucketLevelPermissions

Contains information about the bucket level permissions for the S3 bucket.

Contents

accessControlList

Contains information on how Access Control Policies are applied to the bucket.

Type: AccessControlList object

Required: No

blockPublicAccess

Contains information on which account level S3 Block Public Access settings are applied to the S3 bucket.

Type: BlockPublicAccess object

Required: No

bucketPolicy

Contains information on the bucket policies for the S3 bucket.

Type: BucketPolicy object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BucketPolicy

Contains information on the current bucket policies for the S3 bucket.

Contents

allowsPublicReadAccess

A value that indicates whether public read access for the bucket is enabled through a bucket policy.

Type: Boolean

Required: No

allowsPublicWriteAccess

A value that indicates whether public write access for the bucket is enabled through a bucket policy.

Type: Boolean

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

City

Contains information about the city associated with the IP address.

Contents

cityName

The city name of the remote IP address.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CloudDetails

Contains details about the cloud environment associated with an investigation.

Contents

account

The AWS account ID of the investigated resource.

Type: String

Required: Yes

provider

The cloud provider. Currently, only `AWS` is supported.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 50.

Valid Values: `AWS`

Required: Yes

region

The AWS Region in which the investigated resource resides.

Type: String

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CloudformationStack

Contains information about the CloudFormation stack involved in a GuardDuty finding, including unique identifiers of the Amazon EC2 instances.

Contents

ec2InstanceUids

A list of unique identifiers for the compromised Amazon EC2 instances that were created as part of the same CloudFormation stack.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 25 items.

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CloudTrailConfigurationResult

Contains information on the status of CloudTrail as a data source for the detector.

Contents

status

Describes whether CloudTrail is enabled as a data source for the detector.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `ENABLED | DISABLED`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Condition

Contains information about the condition.

Contents

eq

This member has been deprecated.

Represents the *equal* condition to be applied to a single field when querying for findings.

Max values: 50

Type: Array of strings

Required: No

equals

Represents an *equal* condition to be applied to a single field when querying for findings.

Max values: 50

Type: Array of strings

Required: No

greaterThan

Represents a *greater than* condition to be applied to a single field when querying for findings.

Type: Long

Required: No

greaterThanOrEqual

Represents a *greater than or equal* condition to be applied to a single field when querying for findings.

Type: Long

Required: No

gt

This member has been deprecated.

Represents a *greater than* condition to be applied to a single field when querying for findings.

Type: Integer

Required: No

gte

This member has been deprecated.

Represents a *greater than or equal* condition to be applied to a single field when querying for findings.

Type: Integer

Required: No

lessThan

Represents a *less than* condition to be applied to a single field when querying for findings.

Type: Long

Required: No

lessThanOrEqual

Represents a *less than or equal* condition to be applied to a single field when querying for findings.

Type: Long

Required: No

lt

This member has been deprecated.

Represents a *less than* condition to be applied to a single field when querying for findings.

Type: Integer

Required: No

lte

This member has been deprecated.

Represents a *less than or equal* condition to be applied to a single field when querying for findings.

Type: Integer

Required: No

matches

Represents the *match* condition to be applied to a single field when querying for findings.

> **Note**
>
> The *matches* condition is available only for create-filter and update-filter APIs.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 5 items.

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: No

neq

This member has been deprecated.

Represents the *not equal* condition to be applied to a single field when querying for findings.

Max values: 50

Type: Array of strings

Required: No

notEquals

Represents a *not equal* condition to be applied to a single field when querying for findings.

Max values: 50

Type: Array of strings

Required: No

notMatches

Represents the *not match* condition to be applied to a single field when querying for findings.

> **Note**
>
> The *not-matches* condition is available only for create-filter and update-filter APIs.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 5 items.

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Container

Details of a container.

Contents

containerRuntime

The container runtime (such as, Docker or containerd) used to run the container.

Type: String

Required: No

id

Container ID.

Type: String

Required: No

image

Container image.

Type: String

Required: No

imagePrefix

Part of the image name before the last slash. For example, imagePrefix for public.ecr.aws/amazonlinux/amazonlinux:latest would be public.ecr.aws/amazonlinux. If the image name is relative and does not have a slash, this field is empty.

Type: String

Required: No

name

Container name.

Type: String

Required: No

securityContext

Container security context.

Type: SecurityContext object

Required: No

volumeMounts

Container volume mounts.

Type: Array of VolumeMount objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ContainerFindingResource

Contains information about container resources involved in a GuardDuty finding. This structure provides details about containers that were identified as part of suspicious or malicious activity.

Contents

image

The container image information, including the image name and tag used to run the container that was involved in the finding.

Type: String

Required: Yes

imageUid

The unique ID associated with the container image.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ContainerInstanceDetails

Contains information about the Amazon EC2 instance that is running the Amazon ECS container.

Contents

compatibleContainerInstances

Represents total number of nodes in the Amazon ECS cluster.

Type: Long

Required: No

coveredContainerInstances

Represents the nodes in the Amazon ECS cluster that has a HEALTHY coverage status.

Type: Long

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ContentPolicyFilter

Contains information about a content policy filter that matched during a guardrail evaluation.

Contents

action

The action taken by the guardrail filter.

Type: String

Valid Values: `BLOCKED | NONE`

Required: No

confidence

The confidence level that the content matched the filter.

Type: String

Valid Values: `HIGH | MEDIUM | LOW | NONE`

Required: No

type

The type of content that was filtered by the guardrail.

Type: String

Valid Values: `PROMPT_ATTACK | JAILBREAK | HATE | INSULTS | SEXUAL | VIOLENCE | MISCONDUCT`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

ContinuousScanDetails

Contains information about the time range within the continuous backup in AWS Backup to scan for a point-in-time recovery resource.

Contents

endTime

The timestamp representing the end of the time range to scan.

Type: Timestamp

Required: Yes

startTime

The timestamp representing the start of the time range to scan. Reserved for internal use.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Country

Contains information about the country where the remote IP address is located.

Contents

countryCode

The country code of the remote IP address.

Type: String

Required: No

countryName

The country name of the remote IP address.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CoverageEc2InstanceDetails

Contains information about the Amazon EC2 instance runtime coverage details.

Contents

agentDetails

Information about the installed security agent.

Type: AgentDetails object

Required: No

clusterArn

The cluster ARN of the Amazon ECS cluster running on the Amazon EC2 instance.

Type: String

Required: No

instanceId

The Amazon EC2 instance ID.

Type: String

Required: No

instanceType

The instance type of the Amazon EC2 instance.

Type: String

Required: No

managementType

Indicates how the GuardDuty security agent is managed for this resource.

- `AUTO_MANAGED` indicates that GuardDuty deploys and manages updates for this resource.
- `MANUAL` indicates that you are responsible to deploy, update, and manage the GuardDuty security agent updates for this resource.

> **Note**
>
> The `DISABLED` status doesn't apply to Amazon EC2 instances and Amazon EKS clusters.

Type: String

Valid Values: `AUTO_MANAGED | MANUAL | DISABLED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CoverageEcsClusterDetails

Contains information about Amazon ECS cluster runtime coverage details.

Contents

clusterName

The name of the Amazon ECS cluster.

Type: String

Required: No

containerInstanceDetails

Information about the Amazon ECS container running on Amazon EC2 instance.

Type: ContainerInstanceDetails object

Required: No

fargateDetails

Information about the Fargate details associated with the Amazon ECS cluster.

Type: FargateDetails object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CoverageEksClusterDetails

Information about the EKS cluster that has a coverage status.

Contents

addonDetails

Information about the installed EKS add-on.

Type: AddonDetails object

Required: No

clusterName

Name of the EKS cluster.

Type: String

Required: No

compatibleNodes

Represents all the nodes within the EKS cluster in your account.

Type: Long

Required: No

coveredNodes

Represents the nodes within the EKS cluster that have a `HEALTHY` coverage status.

Type: Long

Required: No

managementType

Indicates how the Amazon EKS add-on GuardDuty agent is managed for this EKS cluster.

`AUTO_MANAGED` indicates GuardDuty deploys and manages updates for this resource.

`MANUAL` indicates that you are responsible to deploy, update, and manage the Amazon EKS add-on GuardDuty agent for this resource.

Type: String

Valid Values: `AUTO_MANAGED | MANUAL | DISABLED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CoverageFilterCondition

Represents a condition that when matched will be added to the response of the operation.

Contents

equals

Represents an equal condition that is applied to a single field while retrieving the coverage details.

Type: Array of strings

Required: No

notEquals

Represents a not equal condition that is applied to a single field while retrieving the coverage details.

Type: Array of strings

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CoverageFilterCriteria

Represents the criteria used in the filter.

Contents

filterCriterion

Represents a condition that when matched will be added to the response of the operation.

Type: Array of CoverageFilterCriterion objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CoverageFilterCriterion

Represents a condition that when matched will be added to the response of the operation.

Contents

criterionKey

An enum value representing possible filter fields.

> **Note**
>
> Replace the enum value `CLUSTER_NAME` with `EKS_CLUSTER_NAME`. `CLUSTER_NAME` has been deprecated.

Type: String

Valid Values: `ACCOUNT_ID | RESOURCE_TYPE | COVERAGE_STATUS | ADDON_VERSION | CLUSTER_NAME | ECS_CLUSTER_NAME | MANAGEMENT_TYPE | EKS_CLUSTER_NAME | AGENT_VERSION | INSTANCE_ID | CLUSTER_ARN`

Required: No

filterCondition

Contains information about the condition.

Type: CoverageFilterCondition object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CoverageResource

Information about the resource of the GuardDuty account.

Contents

accountId

The unique ID of the AWS account.

Type: String

Length Constraints: Fixed length of 12.

Required: No

coverageStatus

Represents the status of the EKS cluster coverage.

Type: String

Valid Values: `HEALTHY | UNHEALTHY`

Required: No

detectorId

The unique ID of the GuardDuty detector associated with the resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

issue

Represents the reason why a coverage status was `UNHEALTHY` for the EKS cluster.

Type: String

Required: No

resourceDetails

Information about the resource for which the coverage statistics are retrieved.

Type: CoverageResourceDetails object

Required: No

resourceId

The unique ID of the resource.

Type: String

Required: No

updatedAt

The timestamp at which the coverage details for the resource were last updated. This is in UTC format.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CoverageResourceDetails

Information about the resource for each individual EKS cluster.

Contents

ec2InstanceDetails

Information about the Amazon EC2 instance assessed for runtime coverage.

Type: CoverageEc2InstanceDetails object

Required: No

ecsClusterDetails

Information about the Amazon ECS cluster that is assessed for runtime coverage.

Type: CoverageEcsClusterDetails object

Required: No

eksClusterDetails

EKS cluster details involved in the coverage statistics.

Type: CoverageEksClusterDetails object

Required: No

resourceType

The type of AWS resource.

Type: String

Valid Values: `EKS | ECS | EC2`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CoverageSortCriteria

Information about the sorting criteria used in the coverage statistics.

Contents

attributeName

Represents the field name used to sort the coverage details.

> **Note**
>
> Replace the enum value `CLUSTER_NAME` with `EKS_CLUSTER_NAME`. `CLUSTER_NAME` has been deprecated.

Type: String

Valid Values: `ACCOUNT_ID | COVERAGE_STATUS | ISSUE | ADDON_VERSION | UPDATED_AT | CLUSTER_NAME | EKS_CLUSTER_NAME | ECS_CLUSTER_NAME | INSTANCE_ID`

Required: No

orderBy

The order in which the sorted findings are to be displayed.

Type: String

Valid Values: `ASC | DESC`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

CoverageStatistics

Information about the coverage statistics for a resource.

Contents

countByCoverageStatus

Represents coverage statistics for EKS clusters aggregated by coverage status.

Type: String to long map

Valid Keys: `HEALTHY` | `UNHEALTHY`

Required: No

countByResourceType

Represents coverage statistics for EKS clusters aggregated by resource type.

Type: String to long map

Valid Keys: `EKS` | `ECS` | `EC2`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CreateProtectedResource

Information about the protected resource that is associated with the created Malware Protection plan. Presently, `S3Bucket` is the only supported protected resource.

Contents

s3Bucket

Information about the protected S3 bucket resource.

Type: CreateS3BucketResource object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CreateS3BucketResource

Information about the protected S3 bucket resource.

Contents

bucketName

Name of the S3 bucket.

Type: String

Required: No

objectPrefixes

Information about the specified object prefixes. The S3 object will be scanned only if it belongs to any of the specified object prefixes.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 5 items.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DataSourceConfigurations

Contains information about which data sources are enabled.

Contents

kubernetes

Describes whether any Kubernetes logs are enabled as data sources.

Type: KubernetesConfiguration object

Required: No

malwareProtection

Describes whether Malware Protection is enabled as a data source.

Type: MalwareProtectionConfiguration object

Required: No

s3Logs

Describes whether S3 data event logs are enabled as a data source.

Type: S3LogsConfiguration object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DataSourceConfigurationsResult

Contains information on the status of data sources for the detector.

Contents

cloudTrail

An object that contains information on the status of CloudTrail as a data source.

Type: CloudTrailConfigurationResult object

Required: Yes

dnsLogs

An object that contains information on the status of DNS logs as a data source.

Type: DNSLogsConfigurationResult object

Required: Yes

flowLogs

An object that contains information on the status of VPC flow logs as a data source.

Type: FlowLogsConfigurationResult object

Required: Yes

s3Logs

An object that contains information on the status of S3 Data event logs as a data source.

Type: S3LogsConfigurationResult object

Required: Yes

kubernetes

An object that contains information on the status of all Kubernetes data sources.

Type: KubernetesConfigurationResult object

Required: No

malwareProtection

Describes the configuration of Malware Protection data sources.

Type: MalwareProtectionConfigurationResult object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DataSourceFreeTrial

Contains information about which data sources are enabled for the GuardDuty member account.

Contents

freeTrialDaysRemaining

A value that specifies the number of days left to use each enabled data source.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DataSourcesFreeTrial

Contains information about which data sources are enabled for the GuardDuty member account.

Contents

cloudTrail

Describes whether any AWS CloudTrail management event logs are enabled as data sources.

Type: DataSourceFreeTrial object

Required: No

dnsLogs

Describes whether any DNS logs are enabled as data sources.

Type: DataSourceFreeTrial object

Required: No

flowLogs

Describes whether any VPC Flow logs are enabled as data sources.

Type: DataSourceFreeTrial object

Required: No

kubernetes

Describes whether any Kubernetes logs are enabled as data sources.

Type: KubernetesDataSourceFreeTrial object

Required: No

malwareProtection

Describes whether Malware Protection is enabled as a data source.

Type: MalwareProtectionDataSourceFreeTrial object

Required: No

s3Logs

Describes whether any S3 data event logs are enabled as data sources.

Type: DataSourceFreeTrial object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DateStatistics

Represents list a map of dates with a count of total findings generated on each date.

Contents

date

The timestamp when the total findings count is observed.

For example, `Date` would look like `"2024-09-05T17:00:00-07:00"` whereas `LastGeneratedAt` would look like 2024-09-05T17:12:29-07:00".

Type: Timestamp

Required: No

lastGeneratedAt

The timestamp at which the last finding in the findings count, was generated.

Type: Timestamp

Required: No

severity

The severity of the findings generated on each date.

Type: Double

Required: No

totalFindings

The total number of findings that were generated per severity level on each date.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DefaultServerSideEncryption

Contains information on the server side encryption method used in the S3 bucket. See S3 Server-Side Encryption for more information.

Contents

encryptionType

The type of encryption used for objects within the S3 bucket.

Type: String

Required: No

kmsMasterKeyArn

The Amazon Resource Name (ARN) of the KMS encryption key. Only available if the bucket `EncryptionType` is `aws:kms`.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Destination

Contains information about the publishing destination, including the ID, type, and status.

Contents

destinationId

The unique ID of the publishing destination.

Type: String

Required: Yes

destinationType

The type of resource used for the publishing destination. Currently, only Amazon S3 buckets are supported.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: S3

Required: Yes

status

The status of the publishing destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `PENDING_VERIFICATION | PUBLISHING | UNABLE_TO_PUBLISH_FIX_DESTINATION_PROPERTY | STOPPED`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DestinationProperties

Contains the Amazon Resource Name (ARN) of the resource to publish to, such as an S3 bucket, and the ARN of the KMS key to use to encrypt published findings.

Contents

destinationArn

The ARN of the resource to publish to.

To specify an S3 bucket folder use the following format: `arn:aws:s3:::DOC-EXAMPLE-BUCKET/myFolder/`

Type: String

Required: No

kmsKeyArn

The ARN of the KMS key to use for encryption.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Detection

Contains information about the detected behavior.

Contents

anomaly

The details about the anomalous activity that caused GuardDuty to generate the finding.

Type: Anomaly object

Required: No

sequence

The details about the attack sequence.

Type: Sequence object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DetectionRuleEc2Requirements

The requirements for running a Runtime Monitoring custom detection rule on Amazon EC2.

Contents

minAgentVersion

The minimum GuardDuty agent version required to run the rule on Amazon EC2.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[0-9]+(\.[0-9]+){1,3}`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DetectionRuleEcsFargateRequirements

The requirements for running a Runtime Monitoring custom detection rule on Amazon ECS with the Fargate launch type.

Contents

minAgentVersion

The minimum GuardDuty agent version required to run the rule on Amazon ECS with the Fargate launch type.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[0-9]+(\.[0-9]+){1,3}`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DetectionRuleEksRequirements

The requirements for running a Runtime Monitoring custom detection rule on Amazon EKS.

Contents

minAgentVersion

The minimum GuardDuty agent version required to run the rule on Amazon EKS.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[0-9]+(\.[0-9]+){1,3}`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DetectionRuleFilter

Contains filter criteria for listing custom detection rules or associations.

Contents

name

The name of the field to filter by.

Type: String

Valid Values: `name | description | dataSource | severity | tactic | technique | service`

Required: Yes

values

The values to match against the specified filter name.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: `[a-zA-Z0-9 _.\-:/]+`

Required: Yes

condition

The condition to apply to the filter. For example, `EQUALS` or `CONTAINS`.

Type: String

Valid Values: `EQUALS | CONTAINS`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DetectionRuleOrgConfiguration

Contains the organization-level configuration for a custom detection rule.

Contents

createdAt

The timestamp when the organization configuration was created.

Type: Timestamp

Required: Yes

excludeAccountIds

A list of member account IDs excluded from the organization configuration. Mutually exclusive with `IncludeAccountIds`.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50000 items.

Length Constraints: Fixed length of 12.

Required: Yes

includeAccountIds

A list of member account IDs included in the organization configuration. Mutually exclusive with `ExcludeAccountIds`.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50000 items.

Length Constraints: Fixed length of 12.

Required: Yes

mode

The execution mode of the organization configuration. Valid values: `LIVE` | `DRY_RUN`.

Type: String

Valid Values: `LIVE | DRY_RUN`

Required: Yes

ruleId

The unique identifier for the custom detection rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Required: Yes

status

The configuration status. Valid values: `ACTIVE` | `PROCESSING` | `FAILED`.

Type: String

Valid Values: `ACTIVE | PROCESSING | FAILED`

Required: Yes

updatedAt

The timestamp when the organization configuration was last updated.

Type: Timestamp

Required: Yes

expiresAt

The timestamp when the organization configuration expires.

Type: Timestamp

Required: No

statusReason

The reason for the current configuration status.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DetectionRuleOrgConfigurationSummary

Contains summary information about an organization-level configuration for a custom detection rule.

Contents

createdAt

The timestamp when the organization configuration was created.

Type: Timestamp

Required: Yes

mode

The rule execution mode.

Type: String

Valid Values: `LIVE | DRY_RUN`

Required: Yes

ruleId

The unique identifier for the custom detection rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Required: Yes

status

The configuration status.

Type: String

Valid Values: `ACTIVE | PROCESSING | FAILED`

Required: Yes

updatedAt

The timestamp when the organization configuration was last updated.

Type: Timestamp

Required: Yes

expiresAt

The timestamp when the organization configuration expires.

Type: Timestamp

Required: No

statusReason

The reason for the current configuration status.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DetectionRuleRuntimeMonitoringDetails

Contains Runtime Monitoring-specific details for a custom detection rule.

Contents

platforms

The platforms on which the rule can run. The presence of a platform member indicates that the rule is supported on that platform; the absence of a member indicates that the rule cannot run on that platform at any agent version.

Type: DetectionRuleRuntimePlatforms object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DetectionRuleRuntimePlatforms

The platforms on which a Runtime Monitoring custom detection rule can run. A member's presence is the support statement: when present, the rule runs on that platform and `minAgentVersion` is the minimum GuardDuty agent version required there. When absent, the rule cannot run on that platform at any agent version.

Contents

ec2

The requirements for running the rule on Amazon EC2.

Type: DetectionRuleEc2Requirements object

Required: No

ecsFargate

The requirements for running the rule on Amazon ECS with the Fargate launch type.

Type: DetectionRuleEcsFargateRequirements object

Required: No

eks

The requirements for running the rule on Amazon EKS.

Type: DetectionRuleEksRequirements object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DetectorAdditionalConfiguration

Information about the additional configuration for a feature in your GuardDuty account.

Contents

name

Name of the additional configuration.

Type: String

Valid Values: `EKS_ADDON_MANAGEMENT | ECS_FARGATE_AGENT_MANAGEMENT | EC2_AGENT_MANAGEMENT | RDS_DATA_RISK`

Required: No

status

Status of the additional configuration.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DetectorAdditionalConfigurationResult

Information about the additional configuration.

Contents

managedBy

Indicates what manages the additional configuration. A value of `GUARDDUTY_POLICY` means a GuardDuty policy manages the additional configuration.

Type: String

Valid Values: `GUARDDUTY_POLICY`

Required: No

name

Name of the additional configuration.

Type: String

Valid Values: `EKS_ADDON_MANAGEMENT | ECS_FARGATE_AGENT_MANAGEMENT | EC2_AGENT_MANAGEMENT | RDS_DATA_RISK`

Required: No

status

Status of the additional configuration.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

updatedAt

The timestamp at which the additional configuration was last updated. This is in UTC format.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DetectorFeatureConfiguration

Contains information about a GuardDuty feature.

Specifying both EKS Runtime Monitoring (`EKS_RUNTIME_MONITORING`) and Runtime Monitoring (`RUNTIME_MONITORING`) will cause an error. You can add only one of these two features because Runtime Monitoring already includes the threat detection for Amazon EKS resources. For more information, see Runtime Monitoring.

Contents

additionalConfiguration

Additional configuration for a resource.

Type: Array of DetectorAdditionalConfiguration objects

Required: No

name

The name of the feature.

Type: String

Valid Values: `S3_DATA_EVENTS | EKS_AUDIT_LOGS | EBS_MALWARE_PROTECTION | RDS_LOGIN_EVENTS | LAMBDA_NETWORK_LOGS | EKS_RUNTIME_MONITORING | RUNTIME_MONITORING | AI_PROTECTION | AI_ANALYST`

Required: No

status

The status of the feature.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DetectorFeatureConfigurationResult

Contains information about a GuardDuty feature.

Specifying both EKS Runtime Monitoring (`EKS_RUNTIME_MONITORING`) and Runtime Monitoring (`RUNTIME_MONITORING`) will cause an error. You can add only one of these two features because Runtime Monitoring already includes the threat detection for Amazon EKS resources. For more information, see Runtime Monitoring.

Contents

additionalConfiguration

Additional configuration for a resource.

Type: Array of DetectorAdditionalConfigurationResult objects

Required: No

managedBy

Indicates what manages the feature. A value of `GUARDDUTY_POLICY` means a GuardDuty policy manages the feature.

Type: String

Valid Values: `GUARDDUTY_POLICY`

Required: No

name

Indicates the name of the feature that can be enabled for the detector.

Type: String

Valid Values: `FLOW_LOGS | CLOUD_TRAIL | DNS_LOGS | S3_DATA_EVENTS | EKS_AUDIT_LOGS | EBS_MALWARE_PROTECTION | RDS_LOGIN_EVENTS | LAMBDA_NETWORK_LOGS | EKS_RUNTIME_MONITORING | RUNTIME_MONITORING | AI_PROTECTION | AI_ANALYST`

Required: No

status

Indicates the status of the feature that is enabled for the detector.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

updatedAt

The timestamp at which the feature object was updated.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DNSLogsConfigurationResult

Contains information on the status of DNS logs as a data source.

Contents

status

Denotes whether DNS logs is enabled as a data source.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `ENABLED | DISABLED`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DnsRequestAction

Contains information about the DNS_REQUEST action described in this finding.

Contents

blocked

Indicates whether the targeted port is blocked.

Type: Boolean

Required: No

domain

The domain information for the DNS query.

Type: String

Required: No

domainWithSuffix

The second and top level domain involved in the activity that potentially prompted GuardDuty to generate this finding. For a list of top-level and second-level domains, see public suffix list.

Type: String

Required: No

protocol

The network connection protocol observed in the activity that prompted GuardDuty to generate the finding.

Type: String

Required: No

vpcOwnerAccountId

The AWS account ID that owns the VPC through which the DNS request was made.

Type: String

Length Constraints: Fixed length of 12.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DomainDetails

Contains information about the domain.

Contents

domain

The domain information for the AWS API call.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EbsSnapshot

Contains information about an EBS snapshot that was scanned for malware.

Contents

deviceName

The device name of the EBS snapshot that was scanned.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EbsSnapshotDetails

Contains details about the EBS snapshot that was scanned for malware.

Contents

snapshotArn

The Amazon Resource Name (ARN) of the EBS snapshot.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EbsVolumeDetails

Contains list of scanned and skipped EBS volumes with details.

Contents

scannedVolumeDetails

List of EBS volumes that were scanned.

Type: Array of VolumeDetail objects

Required: No

skippedVolumeDetails

List of EBS volumes that were skipped from the malware scan.

Type: Array of VolumeDetail objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EbsVolumeScanDetails

Contains details from the malware scan that created a finding.

Contents

scanCompletedAt

Returns the completion date and time of the malware scan.

Type: Timestamp

Required: No

scanDetections

Contains a complete view providing malware scan result details.

Type: ScanDetections object

Required: No

scanId

Unique Id of the malware scan that generated the finding.

Type: String

Required: No

scanStartedAt

Returns the start date and time of the malware scan.

Type: Timestamp

Required: No

scanType

Specifies the scan type that invoked the malware scan.

Type: String

Valid Values: `GUARDDUTY_INITIATED | ON_DEMAND`

Required: No

sources

Contains list of threat intelligence sources used to detect threats.

Type: Array of strings

Required: No

triggerFindingId

GuardDuty finding ID that triggered a malware scan.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EbsVolumesResult

Describes the configuration of scanning EBS volumes as a data source.

Contents

reason

Specifies the reason why scanning EBS volumes (Malware Protection) was not enabled as a data source.

Type: String

Required: No

status

Describes whether scanning EBS volumes is enabled as a data source.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `ENABLED | DISABLED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Ec2Image

Contains information about the Amazon EC2 Image involved in a GuardDuty finding, including unique identifiers of the Amazon EC2 instances.

Contents

ec2InstanceUids

A list of unique identifiers for the compromised Amazon EC2 instances that were launched with the same Amazon Machine Image (AMI).

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 25 items.

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Ec2ImageDetails

Contains details about the EC2 AMI that was scanned.

Contents

imageArn

The Amazon Resource Name (ARN) of the EC2 AMI.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Ec2Instance

Details about the potentially impacted Amazon EC2 instance resource.

Contents

availabilityZone

The availability zone of the Amazon EC2 instance. For more information, see Availability zones in the *Amazon EC2 User Guide*.

Type: String

Required: No

ec2NetworkInterfaceUids

The ID of the network interface.

Type: Array of strings

Required: No

IamInstanceProfile

Contains information about the EC2 instance profile.

Type: IamInstanceProfile object

Required: No

imageDescription

The image description of the Amazon EC2 instance.

Type: String

Required: No

instanceState

The state of the Amazon EC2 instance. For more information, see Amazon EC2 instance state changes in the *Amazon EC2 User Guide*.

Type: String

Required: No

instanceType

Type of the Amazon EC2 instance.

Type: String

Required: No

outpostArn

The Amazon Resource Name (ARN) of the AWS Outpost. This shows applicable AWS Outposts instances.

Type: String

Required: No

platform

The platform of the Amazon EC2 instance.

Type: String

Required: No

productCodes

The product code of the Amazon EC2 instance.

Type: Array of ProductCode objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Ec2LaunchTemplate

Contains information about the Amazon EC2 launch template involved in a GuardDuty finding, including unique identifiers of the Amazon EC2 instances.

Contents

ec2InstanceUids

A list of unique identifiers for the compromised Amazon EC2 instances that share the same Amazon EC2 launch template.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 25 items.

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

version

Version of the EC2 launch template.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Ec2NetworkInterface

Contains information about the elastic network interface of the Amazon EC2 instance.

Contents

ipv6Addresses

A list of IPv6 addresses for the Amazon EC2 instance.

Type: Array of strings

Required: No

privateIpAddresses

Other private IP address information of the Amazon EC2 instance.

Type: Array of PrivateIpAddressDetails objects

Required: No

publicIp

The public IP address of the Amazon EC2 instance.

Type: String

Required: No

securityGroups

The security groups associated with the Amazon EC2 instance.

Type: Array of SecurityGroup objects

Required: No

subNetId

The subnet ID of the Amazon EC2 instance.

Type: String

Required: No

vpcId

The VPC ID of the Amazon EC2 instance.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Ec2Vpc

Contains information about the Amazon EC2 VPC involved in a GuardDuty finding, including unique identifiers of the Amazon EC2 instances.

Contents

ec2InstanceUids

A list of unique identifiers for the compromised Amazon EC2 instances that were launched within the same Virtual Private Cloud (VPC).

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 25 items.

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EcsCluster

Contains information about the Amazon ECS cluster involved in a GuardDuty finding, including cluster identification and status.

Contents

ec2InstanceUids

A list of unique identifiers for the Amazon EC2 instances that serve as container instances in the Amazon ECS cluster.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 25 items.

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

status

The current status of the Amazon ECS cluster.

Type: String

Valid Values: `ACTIVE | PROVISIONING | DEPROVISIONING | FAILED | INACTIVE`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EcsClusterDetails

Contains information about the details of the ECS Cluster.

Contents

activeServicesCount

The number of services that are running on the cluster in an ACTIVE state.

Type: Integer

Required: No

arn

The Amazon Resource Name (ARN) that identifies the cluster.

Type: String

Required: No

name

The name of the ECS Cluster.

Type: String

Required: No

registeredContainerInstancesCount

The number of container instances registered into the cluster.

Type: Integer

Required: No

runningTasksCount

The number of tasks in the cluster that are in the RUNNING state.

Type: Integer

Required: No

status

The status of the ECS cluster.

Type: String

Required: No

tags

The tags of the ECS Cluster.

Type: Array of Tag objects

Required: No

taskDetails

Contains information about the details of the ECS Task.

Type: EcsTaskDetails object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EcsTask

Contains information about Amazon ECS task involved in a GuardDuty finding, including task definition and container identifiers.

Contents

containerUids

A list of unique identifiers for the containers associated with the Amazon ECS task.

Type: Array of strings

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

createdAt

The timestamp indicating when the Amazon ECS task was created, in UTC format.

Type: Timestamp

Required: No

launchType

The infrastructure type on which the Amazon ECS task runs.

Type: String

Valid Values: `FARGATE | EC2`

Required: No

taskDefinitionArn

The ARN of task definition which describes the container and volume definitions of the Amazon ECS task.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EcsTaskDetails

Contains information about the task in an ECS cluster.

Contents

arn

The Amazon Resource Name (ARN) of the task.

Type: String

Required: No

containers

The containers that's associated with the task.

Type: Array of Container objects

Required: No

definitionArn

The ARN of the task definition that creates the task.

Type: String

Required: No

group

The name of the task group that's associated with the task.

Type: String

Required: No

launchType

A capacity on which the task is running. For example, `Fargate` and `EC2`.

Type: String

Required: No

startedAt

The Unix timestamp for the time when the task started.

Type: Timestamp

Required: No

startedBy

Contains the tag specified when a task is started.

Type: String

Required: No

tags

The tags of the ECS Task.

Type: Array of Tag objects

Required: No

createdAt

The Unix timestamp for the time when the task was created.

Type: Timestamp

Required: No

version

The version counter for the task.

Type: String

Required: No

volumes

The list of data volume definitions for the task.

Type: Array of Volume objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EksCluster

Contains information about the Amazon EKS cluster involved in a GuardDuty finding, including cluster identification, status, and network configuration.

Contents

arn

The Amazon Resource Name (ARN) that uniquely identifies the Amazon EKS cluster involved in the finding.

Type: String

Required: No

createdAt

The timestamp indicating when the Amazon EKS cluster was created, in UTC format.

Type: Timestamp

Required: No

ec2InstanceUids

A list of unique identifiers for the Amazon EC2 instances that serve as worker nodes in the Amazon EKS cluster.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 25 items.

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

status

The current status of the Amazon EKS cluster.

Type: String

Valid Values: `CREATING | ACTIVE | DELETING | FAILED | UPDATING | PENDING`

Required: No

vpcId

The ID of the Amazon Virtual Private Cloud (Amazon VPC) associated with the Amazon EKS cluster.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EksClusterDetails

Details about the EKS cluster involved in a Kubernetes finding.

Contents

arn

EKS cluster ARN.

Type: String

Required: No

createdAt

The timestamp when the EKS cluster was created.

Type: Timestamp

Required: No

name

EKS cluster name.

Type: String

Required: No

status

The EKS cluster status.

Type: String

Required: No

tags

The EKS cluster tags.

Type: Array of Tag objects

Required: No

vpcId

The VPC ID to which the EKS cluster is attached.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Evidence

Contains information about the reason that the finding was generated.

Contents

threatIntelligenceDetails

A list of threat intelligence details related to the evidence.

Type: Array of ThreatIntelligenceDetail objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FargateDetails

Contains information about AWS Fargate details associated with an Amazon ECS cluster.

Contents

issues

Runtime coverage issues identified for the resource running on AWS Fargate.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Required: No

managementType

Indicates how the GuardDuty security agent is managed for this resource.

- `AUTO_MANAGED` indicates that GuardDuty deploys and manages updates for this resource.
- `DISABLED` indicates that the deployment of the GuardDuty security agent is disabled for this resource.

> **Note**
>
> The `MANUAL` status doesn't apply to the AWS Fargate (Amazon ECS only) woprkloads.

Type: String

Valid Values: `AUTO_MANAGED | MANUAL | DISABLED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

FilterCondition

Contains information about the condition.

Contents

equalsValue

Represents an *equal* condition to be applied to a single field when querying for scan entries.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

greaterThan

Represents a *greater than* condition to be applied to a single field when querying for scan entries.

Type: Long

Required: No

lessThan

Represents a *less than* condition to be applied to a single field when querying for scan entries.

Type: Long

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FilterCriteria

Represents the criteria to be used in the filter for describing scan entries.

Contents

filterCriterion

Represents a condition that when matched will be added to the response of the operation.

Type: Array of FilterCriterion objects

Array Members: Minimum number of 0 items. Maximum number of 1 item.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FilterCriterion

Represents a condition that when matched will be added to the response of the operation. Irrespective of using any filter criteria, an administrator account can view the scan entries for all of its member accounts. However, each member account can view the scan entries only for their own account.

Contents

criterionKey

An enum value representing possible scan properties to match with given scan entries.

Type: String

Valid Values: `EC2_INSTANCE_ARN | SCAN_ID | ACCOUNT_ID | GUARDDUTY_FINDING_ID | SCAN_START_TIME | SCAN_STATUS | SCAN_TYPE`

Required: No

filterCondition

Contains information about the condition.

Type: FilterCondition object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Finding

Contains information about the finding that is generated when abnormal or suspicious activity is detected.

Contents

accountId

The ID of the account in which the finding was generated.

Type: String

Required: Yes

arn

The ARN of the finding.

Type: String

Required: Yes

createdAt

The time and date when the finding was created.

Type: String

Required: Yes

id

The ID of the finding.

Type: String

Required: Yes

region

The Region where the finding was generated. For findings generated from Global Service Events, the Region value in the finding might differ from the Region where GuardDuty identifies the potential threat. For more information, see How GuardDuty handles AWS CloudTrail global events in the *Amazon GuardDuty User Guide*.

Type: String

Required: Yes

resource

Contains information about the AWS resource associated with the activity that prompted GuardDuty to generate a finding.

Type: Resource object

Required: Yes

schemaVersion

The version of the schema used for the finding.

Type: String

Required: Yes

severity

The severity of the finding.

Type: Double

Required: Yes

type

The type of finding.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Required: Yes

updatedAt

The time and date when the finding was last updated.

Type: String

Required: Yes

associatedAttackSequenceArn

Amazon Resource Name (ARN) associated with the attack sequence finding.

Type: String

Required: No

confidence

The confidence score for the finding.

Type: Double

Required: No

customDetectionRuleName

The name of the custom detection rule that generated this finding.

Type: String

Required: No

description

The description of the finding.

Type: String

Required: No

partition

The partition associated with the finding.

Type: String

Required: No

service

Contains additional information about the generated finding.

Type: Service object

Required: No

title

The title of the finding.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FindingCriteria

Contains information about the criteria used for querying findings.

Contents

criterion

Represents a map of finding properties that match specified conditions and values when querying findings.

Type: String to Condition object map

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FindingStatistics

Contains information about finding statistics.

Contents

countBySeverity

This member has been deprecated.

Represents a list of map of severity to count statistics for a set of findings.

Type: String to integer map

Required: No

groupedByAccount

Represents a list of map of accounts with a findings count associated with each account.

Type: Array of AccountStatistics objects

Required: No

groupedByDate

Represents a list of map of dates with a count of total findings generated on each date per severity level.

Type: Array of DateStatistics objects

Required: No

groupedByFindingType

Represents a list of map of finding types with a count of total findings generated for each type.

Based on the `orderBy` parameter, this request returns either the most occurring finding types or the least occurring finding types. If the `orderBy` parameter is ASC, this will represent the least occurring finding types in your account; otherwise, this will represent the most occurring finding types. The default value of `orderBy` is DESC.

Type: Array of FindingTypeStatistics objects

Required: No

groupedByResource

Represents a list of map of top resources with a count of total findings.

Type: Array of ResourceStatistics objects

Required: No

groupedBySeverity

Represents a list of map of total findings for each severity level.

Type: Array of SeverityStatistics objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FindingTypeStatistics

Information about each finding type associated with the `groupedByFindingType` statistics.

Contents

findingType

Name of the finding type.

Type: String

Required: No

lastGeneratedAt

The timestamp at which this finding type was last generated in your environment.

Type: Timestamp

Required: No

totalFindings

The total number of findings associated with generated for each distinct finding type.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FlowLogsConfigurationResult

Contains information on the status of VPC flow logs as a data source.

Contents

status

Denotes whether VPC flow logs is enabled as a data source.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `ENABLED | DISABLED`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FreeTrialFeatureConfigurationResult

Contains information about the free trial period for a feature.

Contents

freeTrialDaysRemaining

The number of the remaining free trial days for the feature.

Type: Integer

Required: No

name

The name of the feature for which the free trial is configured.

Type: String

Valid Values: `FLOW_LOGS | CLOUD_TRAIL | DNS_LOGS | S3_DATA_EVENTS | EKS_AUDIT_LOGS | EBS_MALWARE_PROTECTION | RDS_LOGIN_EVENTS | LAMBDA_NETWORK_LOGS | EKS_RUNTIME_MONITORING | EC2_RUNTIME_MONITORING | FARGATE_RUNTIME_MONITORING | AI_PROTECTION`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

GeoLocation

Contains information about the location of the remote IP address. By default, GuardDuty returns `Geolocation` with `Lat` and `Lon` as `0.0`.

Contents

lat

The latitude information of the remote IP address.

Type: Double

Required: No

lon

The longitude information of the remote IP address.

Type: Double

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

GetMalwareScanResultDetails

Contains information about the results of the malware scan.

Contents

failedFileCount

The total number of files that failed to be scanned.

Type: Long

Valid Range: Minimum value of 0.

Required: No

scanResultStatus

Status indicating whether threats were found for a completed scan.

Type: String

Valid Values: `NO_THREATS_FOUND | THREATS_FOUND`

Required: No

skippedFileCount

The total number of files that were skipped during the scan.

Type: Long

Valid Range: Minimum value of 0.

Required: No

threatFoundFileCount

The total number of files in which threats were detected.

Type: Long

Valid Range: Minimum value of 0.

Required: No

threats

The threats that were detected during the malware scan.

Type: Array of ScanResultThreat objects

Required: No

totalBytes

The total number of bytes that were scanned.

Type: Long

Valid Range: Minimum value of 0.

Required: No

totalFileCount

The total number of files that were processed during the scan.

Type: Long

Valid Range: Minimum value of 0.

Required: No

uniqueThreatCount

The total number of unique threats that were detected during the scan.

Type: Long

Valid Range: Minimum value of 0.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

HighestSeverityThreatDetails

Contains details of the highest severity threat detected during scan and number of infected files.

Contents

count

Total number of infected files with the highest severity threat detected.

Type: Integer

Required: No

severity

Severity level of the highest severity threat detected.

Type: String

Required: No

threatName

Threat name of the highest severity threat detected as part of the malware scan.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

HostPath

Represents a pre-existing file or directory on the host machine that the volume maps to.

Contents

path

Path of the file or directory on the host that the volume maps to.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

IamInstanceProfile

Contains information about the EC2 instance profile.

Contents

arn

The profile ARN of the EC2 instance.

Type: String

Required: No

id

The profile ID of the EC2 instance.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

IamInstanceProfileV2

Contains information about the IAM instance profile involved in a GuardDuty finding, including unique identifiers of the Amazon EC2 instances.

Contents

ec2InstanceUids

A list of unique identifiers for the compromised Amazon EC2 instances that share the same IAM instance profile.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 25 items.

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ImpersonatedUser

Contains information about the impersonated user.

Contents

groups

The `group` to which the user name belongs.

Type: Array of strings

Required: No

username

Information about the `username` that was being impersonated.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

IncrementalScanDetails

Contains information about the incremental scan configuration.

Contents

baselineResourceArn

Amazon Resource Name (ARN) of the baseline resource used for incremental scanning. The scan will only process changes since this baseline resource was created.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Indicator

Contains information about the indicators that include a set of signals observed in an attack sequence.

Contents

key

Specific indicator keys observed in the attack sequence. For description of the valid values for key, see Attack sequence finding details in the *Amazon GuardDuty User Guide*.

Type: String

Valid Values: `SUSPICIOUS_USER_AGENT | SUSPICIOUS_NETWORK | MALICIOUS_IP | TOR_IP | ATTACK_TACTIC | HIGH_RISK_API | ATTACK_TECHNIQUE | UNUSUAL_API_FOR_ACCOUNT | UNUSUAL_ASN_FOR_ACCOUNT | UNUSUAL_ASN_FOR_USER | SUSPICIOUS_PROCESS | MALICIOUS_DOMAIN | MALICIOUS_PROCESS | CRYPTOMINING_IP | CRYPTOMINING_DOMAIN | CRYPTOMINING_PROCESS | MALICIOUS_FILE | VULNERABILITY | MALICIOUS_PACKAGE | MISCONFIGURATION | REACHABILITY | SENSITIVE_DATA`

Required: Yes

title

Title describing the indicator.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: No

values

Values associated with each indicator key. For example, if the indicator key is `SUSPICIOUS_NETWORK`, then the value will be the name of the network. If the indicator key is `ATTACK_TACTIC`, then the value will be one of the MITRE tactics.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 400 items.

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

InstanceDetails

Contains information about the details of an instance.

Contents

availabilityZone

The Availability Zone of the EC2 instance.

Type: String

Required: No

iamInstanceProfile

The profile information of the EC2 instance.

Type: IamInstanceProfile object

Required: No

imageDescription

The image description of the EC2 instance.

Type: String

Required: No

imageId

The image ID of the EC2 instance.

Type: String

Required: No

instanceId

The ID of the EC2 instance.

Type: String

Required: No

instanceState

The state of the EC2 instance.

Type: String

Required: No

instanceType

The type of the EC2 instance.

Type: String

Required: No

launchTime

The launch time of the EC2 instance.

Type: String

Required: No

networkInterfaces

The elastic network interface information of the EC2 instance.

Type: Array of NetworkInterface objects

Required: No

outpostArn

The Amazon Resource Name (ARN) of the AWS Outpost. Only applicable to AWS Outposts instances.

Type: String

Required: No

platform

The platform of the EC2 instance.

Type: String

Required: No

productCodes

The product code of the EC2 instance.

Type: Array of ProductCode objects

Required: No

tags

The tags of the EC2 instance.

Type: Array of Tag objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Investigation

Contains the details and results of a GuardDuty investigation.

Contents

investigationId

The unique identifier of the investigation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-fA-F0-9\-]+`

Required: Yes

status

The current status of the investigation. Possible values are `RUNNING`, `COMPLETED`, and `FAILED`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `RUNNING | COMPLETED | FAILED`

Required: Yes

triggeredBy

The account that initiated the investigation.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: Yes

triggerPrompt

The natural-language prompt that initiated this investigation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

cloud

Details about the cloud environment in which the investigation was performed, including the provider, region, and account.

Type: CloudDetails object

Required: No

confidence

The confidence level of the investigation's assessment. Possible values are `Unknown`, `Low`, `Medium`, and `High`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 50.

Valid Values: `Unknown | Low | Medium | High`

Required: No

endTime

The timestamp at which the investigation completed.

Type: Timestamp

Required: No

error

Details about the error if the investigation status is `FAILED`.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

Required: No

metadata

Metadata about the product and version that produced the investigation.

Type: InvestigationMetadata object

Required: No

risk

A human-readable description of the assessed risk.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

riskLevel

The assessed risk level of the investigated threat. Possible values are `Info`, `Low`, `Medium`, `High`, and `Critical`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `Info | Low | Medium | High | Critical`

Required: No

startTime

The timestamp at which the investigation started.

Type: Timestamp

Required: No

summary

A structured summary of the investigation findings, including affected resources, threat assessment, and recommended remediation steps.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

InvestigationMetadata

Contains metadata about the product and version that produced an investigation.

Contents

product

Information about the product that produced the investigation.

Type: Product object

Required: Yes

version

The version of the investigation engine that produced the results.

Type: String

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

InvestigationSortCriteria

Contains information about the criteria used for sorting investigations.

Contents

attributeName

The attribute by which to sort investigations.

Type: String

Valid Values: `START_TIME | END_TIME | STATUS | RISK_LEVEL | CONFIDENCE`

Required: No

orderBy

The order in which the sorted results are to be displayed.

Type: String

Valid Values: `ASC | DESC`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

InvestigationSummary

Contains summary information about a GuardDuty investigation.

Contents

accountId

The AWS account ID associated with the investigation.

Type: String

Required: No

confidence

The confidence level of the investigation's assessment.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 50.

Valid Values: `Unknown | Low | Medium | High`

Required: No

endTime

The timestamp at which the investigation completed.

Type: Timestamp

Required: No

investigationId

The unique identifier of the investigation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-fA-F0-9\-]+`

Required: No

riskLevel

The assessed risk level of the investigated threat.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `Info | Low | Medium | High | Critical`

Required: No

startTime

The timestamp at which the investigation started.

Type: Timestamp

Required: No

status

The current status of the investigation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `RUNNING | COMPLETED | FAILED`

Required: No

title

A short title summarizing the investigation.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

triggerPrompt

The natural-language prompt that initiated this investigation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Invitation

Contains information about the invitation to become a member account.

Contents

accountId

The ID of the account that the invitation was sent from.

Type: String

Length Constraints: Fixed length of 12.

Required: No

invitationId

The ID of the invitation. This value is used to validate the inviter account to the member account.

Type: String

Required: No

invitedAt

The timestamp when the invitation was sent.

Type: String

Required: No

relationshipStatus

The status of the relationship between the inviter and invitee accounts.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ItemDetails

Contains detailed information about where a threat was detected.

Contents

additionalInfo

Additional information about the detected threat item.

Type: AdditionalInfo object

Required: No

hash

The hash value of the infected item.

Type: String

Required: No

itemPath

The path where the threat was detected.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

resourceArn

Amazon Resource Name (ARN) of the resource where the threat was detected.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ItemPath

Information about the nested item path and hash of the protected resource.

Contents

hash

The hash value of the infected resource.

Type: String

Required: No

nestedItemPath

The nested item path where the infected file was found.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

KubernetesApiCallAction

Information about the Kubernetes API call action described in this finding.

Contents

namespace

The name of the namespace where the Kubernetes API call action takes place.

Type: String

Required: No

parameters

Parameters related to the Kubernetes API call action.

Type: String

Required: No

remoteIpDetails

Contains information about the remote IP address of the connection.

Type: RemoteIpDetails object

Required: No

requestUri

The Kubernetes API request URI.

Type: String

Required: No

resource

The resource component in the Kubernetes API call action.

Type: String

Required: No

resourceName

The name of the resource in the Kubernetes API call action.

Type: String

Required: No

sourceIPs

The IP of the Kubernetes API caller and the IPs of any proxies or load balancers between the caller and the API endpoint.

Type: Array of strings

Required: No

statusCode

The resulting HTTP response code of the Kubernetes API call action.

Type: Integer

Required: No

subresource

The name of the sub-resource in the Kubernetes API call action.

Type: String

Required: No

userAgent

The user agent of the caller of the Kubernetes API.

Type: String

Required: No

verb

The Kubernetes API request HTTP verb.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

KubernetesAuditLogsConfiguration

Describes whether Kubernetes audit logs are enabled as a data source.

Contents

enable

The status of Kubernetes audit logs as a data source.

Type: Boolean

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

KubernetesAuditLogsConfigurationResult

Describes whether Kubernetes audit logs are enabled as a data source.

Contents

status

A value that describes whether Kubernetes audit logs are enabled as a data source.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `ENABLED | DISABLED`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

KubernetesConfiguration

Describes whether any Kubernetes data sources are enabled.

Contents

auditLogs

The status of Kubernetes audit logs as a data source.

Type: KubernetesAuditLogsConfiguration object

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

KubernetesConfigurationResult

Describes whether any Kubernetes logs will be enabled as a data source.

Contents

auditLogs

Describes whether Kubernetes audit logs are enabled as a data source.

Type: KubernetesAuditLogsConfigurationResult object

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

KubernetesDataSourceFreeTrial

Provides details about the Kubernetes resources when it is enabled as a data source.

Contents

auditLogs

Describes whether Kubernetes audit logs are enabled as a data source.

Type: DataSourceFreeTrial object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

KubernetesDetails

Details about Kubernetes resources such as a Kubernetes user or workload resource involved in a Kubernetes finding.

Contents

kubernetesUserDetails

Details about the Kubernetes user involved in a Kubernetes finding.

Type: KubernetesUserDetails object

Required: No

kubernetesWorkloadDetails

Details about the Kubernetes workload involved in a Kubernetes finding.

Type: KubernetesWorkloadDetails object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

KubernetesPermissionCheckedDetails

Information about the Kubernetes API for which you check if you have permission to call.

Contents

allowed

Information whether the user has the permission to call the Kubernetes API.

Type: Boolean

Required: No

namespace

The namespace where the Kubernetes API action will take place.

Type: String

Required: No

resource

The Kubernetes resource with which your Kubernetes API call will interact.

Type: String

Required: No

verb

The verb component of the Kubernetes API call. For example, when you check whether or not you have the permission to call the `CreatePod` API, the verb component will be `Create`.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

KubernetesRoleBindingDetails

Contains information about the role binding that grants the permission defined in a Kubernetes role.

Contents

kind

The kind of the role. For role binding, this value will be `RoleBinding`.

Type: String

Required: No

name

The name of the `RoleBinding`.

Type: String

Required: No

roleRefKind

The type of the role being referenced. This could be either `Role` or `ClusterRole`.

Type: String

Required: No

roleRefName

The name of the role being referenced. This must match the name of the `Role` or `ClusterRole` that you want to bind to.

Type: String

Required: No

uid

The unique identifier of the role binding.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

KubernetesRoleDetails

Information about the Kubernetes role name and role type.

Contents

kind

The kind of role. For this API, the value of `kind` will be `Role`.

Type: String

Required: No

name

The name of the Kubernetes role.

Type: String

Required: No

uid

The unique identifier of the Kubernetes role name.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

KubernetesUserDetails

Details about the Kubernetes user involved in a Kubernetes finding.

Contents

groups

The groups that include the user who called the Kubernetes API.

Type: Array of strings

Required: No

impersonatedUser

Information about the impersonated user.

Type: ImpersonatedUser object

Required: No

sessionName

Entity that assumes the IAM role when Kubernetes RBAC permissions are assigned to that role.

Type: Array of strings

Required: No

uid

The user ID of the user who called the Kubernetes API.

Type: String

Required: No

username

The username of the user who called the Kubernetes API.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

KubernetesWorkload

Contains information about Kubernetes workloads involved in a GuardDuty finding, including pods, deployments, and other Kubernetes resources.

Contents

containerUids

A list of unique identifiers for the containers that are part of the Kubernetes workload.

Type: Array of strings

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

type

The types of Kubernetes resources involved in the workload.

Type: String

Valid Values: `PODS | JOBS | CRONJOBS | DEPLOYMENTS | DAEMONSETS | STATEFULSETS | REPLICASETS | REPLICATIONCONTROLLERS`

Required: No

namespace

The Kubernetes namespace in which the workload is running, providing logical isolation within the cluster.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

KubernetesWorkloadDetails

Details about the Kubernetes workload involved in a Kubernetes finding.

Contents

containers

Containers running as part of the Kubernetes workload.

Type: Array of Container objects

Required: No

hostIPC

Whether the host IPC flag is enabled for the pods in the workload.

Type: Boolean

Required: No

hostNetwork

Whether the hostNetwork flag is enabled for the pods included in the workload.

Type: Boolean

Required: No

hostPID

Whether the host PID flag is enabled for the pods in the workload.

Type: Boolean

Required: No

name

Kubernetes workload name.

Type: String

Required: No

namespace

Kubernetes namespace that the workload is part of.

Type: String

Required: No

serviceAccountName

The service account name that is associated with a Kubernetes workload.

Type: String

Required: No

type

Kubernetes workload type (e.g. Pod, Deployment, etc.).

Type: String

Required: No

uid

Kubernetes workload ID.

Type: String

Required: No

volumes

Volumes used by the Kubernetes workload.

Type: Array of Volume objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LambdaDetails

Information about the Lambda function involved in the finding.

Contents

description

Description of the Lambda function.

Type: String

Required: No

functionArn

Amazon Resource Name (ARN) of the Lambda function.

Type: String

Required: No

functionName

Name of the Lambda function.

Type: String

Required: No

functionVersion

The version of the Lambda function.

Type: String

Required: No

lastModifiedAt

The timestamp when the Lambda function was last modified. This field is in the UTC date string format (`2023-03-22T19:37:20.168Z`).

Type: Timestamp

Required: No

revisionId

The revision ID of the Lambda function version.

Type: String

Required: No

role

The execution role of the Lambda function.

Type: String

Required: No

tags

A list of tags attached to this resource, listed in the format of `key:value` pair.

Type: Array of Tag objects

Required: No

vpcConfig

Amazon Virtual Private Cloud configuration details associated with your Lambda function.

Type: VpcConfig object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LineageObject

Information about the runtime process details.

Contents

euid

The effective user ID that was used to execute the process.

Type: Integer

Required: No

executablePath

The absolute path of the process executable file.

Type: String

Required: No

name

The name of the process.

Type: String

Required: No

namespacePid

The process ID of the child process.

Type: Integer

Required: No

parentUuid

The unique ID of the parent process. This ID is assigned to the parent process by GuardDuty.

Type: String

Required: No

pid

The ID of the process.

Type: Integer

Required: No

startTime

The time when the process started. This is in UTC format.

Type: Timestamp

Required: No

userId

The user ID of the user that executed the process.

Type: Integer

Required: No

uuid

The unique ID assigned to the process by GuardDuty.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ListMalwareScansFilterCriteria

Represents the criteria used to filter the malware scan entries.

Contents

filterCriterion

Represents a condition that when matched will be added to the response of the operation.

Type: Array of ListMalwareScansFilterCriterion objects

Array Members: Minimum number of 0 items. Maximum number of 1 item.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ListMalwareScansFilterCriterion

Represents a condition that when matched will be added to the response of the operation. Irrespective of using any filter criteria, an administrator account can view the scan entries for all of its member accounts. However, each member account can view the scan entries only for their own account.

Contents

filterCondition

Contains information about the condition.

Type: FilterCondition object

Required: No

criterionKey

An enum value representing possible scan properties to match with given scan entries.

Type: String

Valid Values: `RESOURCE_ARN | SCAN_ID | ACCOUNT_ID | GUARDDUTY_FINDING_ID | RESOURCE_TYPE | SCAN_START_TIME | SCAN_STATUS | SCAN_TYPE`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LocalIpDetails

Contains information about the local IP address of the connection.

Contents

ipAddressV4

The IPv4 local address of the connection.

Type: String

Required: No

ipAddressV6

The IPv6 local address of the connection.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LocalPortDetails

Contains information about the port for the local connection.

Contents

port

The port number of the local connection.

Type: Integer

Required: No

portName

The port name of the local connection.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LoginAttribute

Information about the login attempts.

Contents

application

Indicates the application name used to attempt log in.

Type: String

Required: No

failedLoginAttempts

Represents the sum of failed (unsuccessful) login attempts made to establish a connection to the database instance.

Type: Integer

Required: No

successfulLoginAttempts

Represents the sum of successful connections (a correct combination of login attributes) made to the database instance by the actor.

Type: Integer

Required: No

user

Indicates the user name which attempted to log in.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MalwareProtectionConfiguration

Describes whether Malware Protection will be enabled as a data source.

Contents

scanEc2InstanceWithFindings

Describes the configuration of Malware Protection for EC2 instances with findings.

Type: ScanEc2InstanceWithFindings object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MalwareProtectionConfigurationResult

An object that contains information on the status of all Malware Protection data sources.

Contents

scanEc2InstanceWithFindings

Describes the configuration of Malware Protection for EC2 instances with findings.

Type: ScanEc2InstanceWithFindingsResult object

Required: No

serviceRole

The GuardDuty Malware Protection service role.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MalwareProtectionDataSourceFreeTrial

Provides details about Malware Protection when it is enabled as a data source.

Contents

scanEc2InstanceWithFindings

Describes whether Malware Protection for EC2 instances with findings is enabled as a data source.

Type: DataSourceFreeTrial object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MalwareProtectionFindingsScanConfiguration

Contains finding configuration details about the malware scan.

Contents

incrementalScanDetails

Contains information about the incremental scan configuration.

Type: IncrementalScanDetails object

Required: No

triggerType

The event that triggered the malware scan.

Type: String

Valid Values: `BACKUP | GUARDDUTY`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MalwareProtectionPlanActions

Information about whether the tags will be added to the S3 object after scanning.

Contents

tagging

Indicates whether the scanned S3 object will have tags about the scan result.

Type: MalwareProtectionPlanTaggingAction object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MalwareProtectionPlanStatusReason

Information about the issue code and message associated to the status of your Malware Protection plan.

Contents

code

Issue code.

Type: String

Required: No

message

Issue message that specifies the reason. For information about potential troubleshooting steps, see Troubleshooting Malware Protection for S3 status issues in the *Amazon GuardDuty User Guide*.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MalwareProtectionPlanSummary

Information about the Malware Protection plan resource.

Contents

malwareProtectionPlanId

A unique identifier associated with Malware Protection plan.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MalwareProtectionPlanTaggingAction

Information about adding tags to the scanned S3 object after the scan result.

Contents

status

Indicates whether or not the tags will added.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MalwareScan

Contains information about a particular malware scan.

Contents

resourceArn

Amazon Resource Name (ARN) of the resource for the given malware scan.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

resourceType

The type of resource that was scanned for malware.

Type: String

Valid Values: `EBS_RECOVERY_POINT | EBS_SNAPSHOT | EBS_VOLUME | EC2_AMI | EC2_INSTANCE | EC2_RECOVERY_POINT | S3_RECOVERY_POINT | S3_BUCKET | S3_POINT_IN_TIME_RECOVERY`

Required: No

scanCompletedAt

The timestamp representing when the malware scan was completed.

Type: Timestamp

Required: No

scanId

A unique identifier that gets generated when you invoke the API without any error. Each malware scan has a corresponding scan ID. Using this scan ID, you can monitor the status of your malware scan.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

scanResultStatus

An enum value representing the result of the malware scan.

Type: String

Valid Values: `NO_THREATS_FOUND | THREATS_FOUND`

Required: No

scanStartedAt

The timestamp representing when the malware scan was started.

Type: Timestamp

Required: No

scanStatus

An enum value representing the current status of the malware scan.

Type: String

Valid Values: `RUNNING | COMPLETED | COMPLETED_WITH_ISSUES | FAILED | SKIPPED`

Required: No

scanType

An enum value representing the type of scan that was initiated.

Type: String

Valid Values: `BACKUP_INITIATED | ON_DEMAND | GUARDDUTY_INITIATED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MalwareScanDetails

Information about the malware scan that generated a GuardDuty finding.

Contents

scanCategory

The category of the malware scan.

Type: String

Valid Values: `FULL_SCAN | INCREMENTAL_SCAN`

Required: No

scanConfiguration

The configuration settings used for the malware scan.

Type: MalwareProtectionFindingsScanConfiguration object

Required: No

scanId

The unique identifier for the malware scan.

Type: String

Required: No

scanType

The type of malware scan performed.

Type: String

Valid Values: `BACKUP_INITIATED | ON_DEMAND | GUARDDUTY_INITIATED`

Required: No

threats

Information about the detected threats associated with the generated GuardDuty finding.

Type: Array of Threat objects

Required: No

uniqueThreatCount

The number of unique malware threats detected during the scan.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Master

Contains information about the administrator account and invitation.

Contents

accountId

The ID of the account used as the administrator account.

Type: String

Length Constraints: Fixed length of 12.

Required: No

invitationId

The value used to validate the administrator account to the member account.

Type: String

Required: No

invitedAt

The timestamp when the invitation was sent.

Type: String

Required: No

relationshipStatus

The status of the relationship between the administrator and member accounts.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Member

Contains information about the member account.

Contents

accountId

The ID of the member account.

Type: String

Length Constraints: Fixed length of 12.

Required: Yes

email

The email address of the member account.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Required: Yes

masterId

The administrator account ID.

Type: String

Required: Yes

relationshipStatus

The status of the relationship between the member and the administrator.

Type: String

Required: Yes

updatedAt

The last-updated timestamp of the member.

Type: String

Required: Yes

administratorId

The administrator account ID.

Type: String

Required: No

detectorId

The detector ID of the member account.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

invitedAt

The timestamp when the invitation was sent.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MemberAdditionalConfiguration

Information about the additional configuration for the member account.

Contents

name

Name of the additional configuration.

Type: String

Valid Values: `EKS_ADDON_MANAGEMENT | ECS_FARGATE_AGENT_MANAGEMENT | EC2_AGENT_MANAGEMENT | RDS_DATA_RISK`

Required: No

status

Status of the additional configuration.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MemberAdditionalConfigurationResult

Information about the additional configuration for the member account.

Contents

managedBy

Indicates what manages the additional configuration. A value of `GUARDDUTY_POLICY` means a GuardDuty policy manages the additional configuration.

Type: String

Valid Values: `GUARDDUTY_POLICY`

Required: No

name

Indicates the name of the additional configuration that is set for the member account.

Type: String

Valid Values: `EKS_ADDON_MANAGEMENT | ECS_FARGATE_AGENT_MANAGEMENT | EC2_AGENT_MANAGEMENT | RDS_DATA_RISK`

Required: No

status

Indicates the status of the additional configuration that is set for the member account.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

updatedAt

The timestamp at which the additional configuration was set for the member account. This is in UTC format.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MemberDataSourceConfiguration

Contains information on which data sources are enabled for a member account.

Contents

accountId

The account ID for the member account.

Type: String

Length Constraints: Fixed length of 12.

Required: Yes

dataSources

This member has been deprecated.

Contains information on the status of data sources for the account.

Type: DataSourceConfigurationsResult object

Required: Yes

features

Contains information about the status of the features for the member account.

Type: Array of MemberFeaturesConfigurationResult objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MemberFeaturesConfiguration

Contains information about the features for the member account.

Contents

additionalConfiguration

Additional configuration of the feature for the member account.

Type: Array of MemberAdditionalConfiguration objects

Required: No

name

The name of the feature.

Type: String

Valid Values: `S3_DATA_EVENTS | EKS_AUDIT_LOGS | EBS_MALWARE_PROTECTION | RDS_LOGIN_EVENTS | LAMBDA_NETWORK_LOGS | EKS_RUNTIME_MONITORING | RUNTIME_MONITORING | AI_PROTECTION`

Required: No

status

The status of the feature.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

MemberFeaturesConfigurationResult

Contains information about the features for the member account.

Contents

additionalConfiguration

Indicates the additional configuration of the feature that is configured for the member account.

Type: Array of MemberAdditionalConfigurationResult objects

Required: No

managedBy

Indicates what manages the feature. A value of `GUARDDUTY_POLICY` means a GuardDuty policy manages the feature.

Type: String

Valid Values: `GUARDDUTY_POLICY`

Required: No

name

Indicates the name of the feature that is enabled for the detector.

Type: String

Valid Values: `S3_DATA_EVENTS | EKS_AUDIT_LOGS | EBS_MALWARE_PROTECTION | RDS_LOGIN_EVENTS | LAMBDA_NETWORK_LOGS | EKS_RUNTIME_MONITORING | RUNTIME_MONITORING | AI_PROTECTION`

Required: No

status

Indicates the status of the feature that is enabled for the detector.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

updatedAt

The timestamp at which the feature object was updated.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ModelDetail

Contains information about the AI model involved in a finding.

Contents

modelId

The identifier of the AI model.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkConnection

Contains information about the network connection.

Contents

direction

The direction in which the network traffic is flowing.

Type: String

Valid Values: `INBOUND | OUTBOUND`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkConnectionAction

Contains information about the NETWORK_CONNECTION action described in the finding.

Contents

blocked

Indicates whether EC2 blocked the network connection to your instance.

Type: Boolean

Required: No

connectionDirection

The network connection direction.

Type: String

Required: No

localIpDetails

The local IP information of the connection.

Type: LocalIpDetails object

Required: No

localNetworkInterface

The EC2 instance's local elastic network interface utilized for the connection.

Type: String

Required: No

localPortDetails

The local port information of the connection.

Type: LocalPortDetails object

Required: No

protocol

The network connection protocol.

Type: String

Required: No

remoteIpDetails

The remote IP information of the connection.

Type: RemoteIpDetails object

Required: No

remotePortDetails

The remote port information of the connection.

Type: RemotePortDetails object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkEndpoint

Contains information about network endpoints that were observed in the attack sequence.

Contents

id

The ID of the network endpoint.

Type: String

Required: Yes

autonomousSystem

The Autonomous System (AS) of the network endpoint.

Type: AutonomousSystem object

Required: No

connection

Information about the network connection.

Type: NetworkConnection object

Required: No

domain

The domain information for the network endpoint.

Type: String

Required: No

ip

The IP address associated with the network endpoint.

Type: String

Required: No

location

Information about the location of the network endpoint.

Type: NetworkGeoLocation object

Required: No

port

The port number associated with the network endpoint.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkGeoLocation

Contains information about network endpoint location.

Contents

city

The name of the city.

Type: String

Required: Yes

country

The name of the country.

Type: String

Required: Yes

lat

The latitude information of the endpoint location.

Type: Double

Required: Yes

lon

The longitude information of the endpoint location.

Type: Double

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkInterface

Contains information about the elastic network interface of the EC2 instance.

Contents

ipv6Addresses

A list of IPv6 addresses for the EC2 instance.

Type: Array of strings

Required: No

networkInterfaceId

The ID of the network interface.

Type: String

Required: No

privateDnsName

The private DNS name of the EC2 instance.

Type: String

Required: No

privateIpAddress

The private IP address of the EC2 instance.

Type: String

Required: No

privateIpAddresses

Other private IP address information of the EC2 instance.

Type: Array of PrivateIpAddressDetails objects

Required: No

publicDnsName

The public DNS name of the EC2 instance.

Type: String

Required: No

publicIp

The public IP address of the EC2 instance.

Type: String

Required: No

securityGroups

The security groups associated with the EC2 instance.

Type: Array of SecurityGroup objects

Required: No

subnetId

The subnet ID of the EC2 instance.

Type: String

Required: No

vpcId

The VPC ID of the EC2 instance.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Observations

Contains information about the observed behavior.

Contents

number

The numeric values that were unusual.

Type: Array of longs

Required: No

text

The text that was unusual.

Type: Array of strings

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Organization

Contains information about the ISP organization of the remote IP address.

Contents

asn

The Autonomous System Number (ASN) of the internet provider of the remote IP address.

Type: String

Required: No

asnOrg

The organization that registered this ASN.

Type: String

Required: No

isp

The ISP information for the internet provider.

Type: String

Required: No

org

The name of the internet provider.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationAdditionalConfiguration

A list of additional configurations which will be configured for the organization.

Additional configuration applies to only GuardDuty Runtime Monitoring protection plan.

Contents

autoEnable

The status of the additional configuration that will be configured for the organization. Use one of the following values to configure the feature status for the entire organization:

- `NEW`: Indicates that when a new account joins the organization, they will have the additional configuration enabled automatically.
- `ALL`: Indicates that all accounts in the organization have the additional configuration enabled automatically. This includes `NEW` accounts that join the organization and accounts that may have been suspended or removed from the organization in GuardDuty.

  It may take up to 24 hours to update the configuration for all the member accounts.
- `NONE`: Indicates that the additional configuration will not be automatically enabled for any account in the organization. The administrator must manage the additional configuration for each account individually.

Type: String

Valid Values: `NEW | NONE | ALL`

Required: No

name

The name of the additional configuration that will be configured for the organization. These values are applicable to only Runtime Monitoring protection plan.

Type: String

Valid Values: `EKS_ADDON_MANAGEMENT | ECS_FARGATE_AGENT_MANAGEMENT | EC2_AGENT_MANAGEMENT | RDS_DATA_RISK`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationAdditionalConfigurationResult

A list of additional configuration which will be configured for the organization.

Contents

autoEnable

Describes the status of the additional configuration that is configured for the member accounts within the organization. One of the following values is the status for the entire organization:

- `NEW`: Indicates that when a new account joins the organization, they will have the additional configuration enabled automatically.
- `ALL`: Indicates that all accounts in the organization have the additional configuration enabled automatically. This includes `NEW` accounts that join the organization and accounts that may have been suspended or removed from the organization in GuardDuty.

  It may take up to 24 hours to update the configuration for all the member accounts.
- `NONE`: Indicates that the additional configuration will not be automatically enabled for any account in the organization. The administrator must manage the additional configuration for each account individually.

Type: String

Valid Values: `NEW | NONE | ALL`

Required: No

name

The name of the additional configuration that is configured for the member accounts within the organization. These values are applicable to only Runtime Monitoring protection plan.

Type: String

Valid Values: `EKS_ADDON_MANAGEMENT | ECS_FARGATE_AGENT_MANAGEMENT | EC2_AGENT_MANAGEMENT | RDS_DATA_RISK`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationDataSourceConfigurations

An object that contains information on which data sources will be configured to be automatically enabled for new members within the organization.

Contents

kubernetes

Describes the configuration of Kubernetes data sources for new members of the organization.

Type: OrganizationKubernetesConfiguration object

Required: No

malwareProtection

Describes the configuration of Malware Protection for new members of the organization.

Type: OrganizationMalwareProtectionConfiguration object

Required: No

s3Logs

Describes whether S3 data event logs are enabled for new members of the organization.

Type: OrganizationS3LogsConfiguration object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationDataSourceConfigurationsResult

An object that contains information on which data sources are automatically enabled for new members within the organization.

Contents

s3Logs

Describes whether S3 data event logs are enabled as a data source.

Type: OrganizationS3LogsConfigurationResult object

Required: Yes

kubernetes

Describes the configuration of Kubernetes data sources.

Type: OrganizationKubernetesConfigurationResult object

Required: No

malwareProtection

Describes the configuration of Malware Protection data source for an organization.

Type: OrganizationMalwareProtectionConfigurationResult object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationDetails

Information about GuardDuty coverage statistics for members in your AWS organization.

Contents

organizationStatistics

Information about the GuardDuty coverage statistics for members in your AWS organization.

Type: OrganizationStatistics object

Required: No

updatedAt

The timestamp at which the organization statistics was last updated. This is in UTC format.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationEbsVolumes

Organization-wide EBS volumes scan configuration.

Contents

autoEnable

Whether scanning EBS volumes should be auto-enabled for new members joining the organization.

Type: Boolean

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationEbsVolumesResult

An object that contains information on the status of whether EBS volumes scanning will be enabled as a data source for an organization.

Contents

autoEnable

An object that contains the status of whether scanning EBS volumes should be auto-enabled for new members joining the organization.

Type: Boolean

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationFeatureConfiguration

A list of features which will be configured for the organization.

Contents

additionalConfiguration

The additional information that will be configured for the organization.

Type: Array of OrganizationAdditionalConfiguration objects

Required: No

autoEnable

Describes the status of the feature that is configured for the member accounts within the organization. One of the following values is the status for the entire organization:

- `NEW`: Indicates that when a new account joins the organization, they will have the feature enabled automatically.
- `ALL`: Indicates that all accounts in the organization have the feature enabled automatically. This includes `NEW` accounts that join the organization and accounts that may have been suspended or removed from the organization in GuardDuty.

  It may take up to 24 hours to update the configuration for all the member accounts.
- `NONE`: Indicates that the feature will not be automatically enabled for any account in the organization. The administrator must manage the feature for each account individually.

Type: String

Valid Values: `NEW | NONE | ALL`

Required: No

name

The name of the feature that will be configured for the organization.

Type: String

Valid Values: `S3_DATA_EVENTS | EKS_AUDIT_LOGS | EBS_MALWARE_PROTECTION | RDS_LOGIN_EVENTS | LAMBDA_NETWORK_LOGS | EKS_RUNTIME_MONITORING | RUNTIME_MONITORING | AI_PROTECTION`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationFeatureConfigurationResult

A list of features which will be configured for the organization.

Contents

additionalConfiguration

The additional configuration that is configured for the member accounts within the organization.

Type: Array of OrganizationAdditionalConfigurationResult objects

Required: No

autoEnable

Describes the status of the feature that is configured for the member accounts within the organization.

- `NEW`: Indicates that when a new account joins the organization, they will have the feature enabled automatically.
- `ALL`: Indicates that all accounts in the organization have the feature enabled automatically. This includes `NEW` accounts that join the organization and accounts that may have been suspended or removed from the organization in GuardDuty.
- `NONE`: Indicates that the feature will not be automatically enabled for any account in the organization. In this case, each account will be managed individually by the administrator.

Type: String

Valid Values: `NEW | NONE | ALL`

Required: No

name

The name of the feature that is configured for the member accounts within the organization.

Type: String

Valid Values: `S3_DATA_EVENTS | EKS_AUDIT_LOGS | EBS_MALWARE_PROTECTION | RDS_LOGIN_EVENTS | LAMBDA_NETWORK_LOGS | EKS_RUNTIME_MONITORING | RUNTIME_MONITORING | AI_PROTECTION`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationFeatureStatistics

Information about the number of accounts that have enabled a specific feature.

Contents

additionalConfiguration

Name of the additional configuration.

Type: Array of OrganizationFeatureStatisticsAdditionalConfiguration objects

Required: No

enabledAccountsCount

Total number of accounts that have enabled a specific feature.

Type: Integer

Required: No

name

Name of the feature.

Type: String

Valid Values: `S3_DATA_EVENTS | EKS_AUDIT_LOGS | EBS_MALWARE_PROTECTION | RDS_LOGIN_EVENTS | LAMBDA_NETWORK_LOGS | EKS_RUNTIME_MONITORING | RUNTIME_MONITORING | AI_PROTECTION`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationFeatureStatisticsAdditionalConfiguration

Information about the coverage statistic for the additional configuration of the feature.

Contents

enabledAccountsCount

Total number of accounts that have enabled the additional configuration.

Type: Integer

Required: No

name

Name of the additional configuration within a feature.

Type: String

Valid Values: `EKS_ADDON_MANAGEMENT | ECS_FARGATE_AGENT_MANAGEMENT | EC2_AGENT_MANAGEMENT | RDS_DATA_RISK`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationKubernetesAuditLogsConfiguration

Organization-wide Kubernetes audit logs configuration.

Contents

autoEnable

A value that contains information on whether Kubernetes audit logs should be enabled automatically as a data source for the organization.

Type: Boolean

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationKubernetesAuditLogsConfigurationResult

The current configuration of Kubernetes audit logs as a data source for the organization.

Contents

autoEnable

Whether Kubernetes audit logs data source should be auto-enabled for new members joining the organization.

Type: Boolean

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationKubernetesConfiguration

Organization-wide Kubernetes data sources configurations.

Contents

auditLogs

Whether Kubernetes audit logs data source should be auto-enabled for new members joining the organization.

Type: OrganizationKubernetesAuditLogsConfiguration object

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationKubernetesConfigurationResult

The current configuration of all Kubernetes data sources for the organization.

Contents

auditLogs

The current configuration of Kubernetes audit logs as a data source for the organization.

Type: OrganizationKubernetesAuditLogsConfigurationResult object

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationMalwareProtectionConfiguration

Organization-wide Malware Protection configurations.

Contents

scanEc2InstanceWithFindings

Whether Malware Protection for EC2 instances with findings should be auto-enabled for new members joining the organization.

Type: OrganizationScanEc2InstanceWithFindings object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationMalwareProtectionConfigurationResult

An object that contains information on the status of all Malware Protection data source for an organization.

Contents

scanEc2InstanceWithFindings

Describes the configuration for scanning EC2 instances with findings for an organization.

Type: OrganizationScanEc2InstanceWithFindingsResult object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationS3LogsConfiguration

Describes whether S3 data event logs will be automatically enabled for new members of the organization.

Contents

autoEnable

A value that contains information on whether S3 data event logs will be enabled automatically as a data source for the organization.

Type: Boolean

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationS3LogsConfigurationResult

The current configuration of S3 data event logs as a data source for the organization.

Contents

autoEnable

A value that describes whether S3 data event logs are automatically enabled for new members of the organization.

Type: Boolean

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationScanEc2InstanceWithFindings

Organization-wide EC2 instances with findings scan configuration.

Contents

ebsVolumes

Whether scanning EBS volumes should be auto-enabled for new members joining the organization.

Type: OrganizationEbsVolumes object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationScanEc2InstanceWithFindingsResult

An object that contains information on the status of scanning EC2 instances with findings for an organization.

Contents

ebsVolumes

Describes the configuration for scanning EBS volumes for an organization.

Type: OrganizationEbsVolumesResult object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationStatistics

Information about the coverage statistics of the features for the entire AWS organization.

When you create a new AWS organization, it might take up to 24 hours to generate the statistics summary for this organization.

Contents

activeAccountsCount

Total number of active accounts in your AWS organization that are associated with GuardDuty.

Type: Integer

Required: No

countByFeature

Retrieves the coverage statistics for each feature.

Type: Array of OrganizationFeatureStatistics objects

Required: No

enabledAccountsCount

Total number of accounts that have enabled GuardDuty.

Type: Integer

Required: No

memberAccountsCount

Total number of accounts in your AWS organization that are associated with GuardDuty.

Type: Integer

Required: No

totalAccountsCount

Total number of accounts in your AWS organization.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Owner

Contains information on the owner of the bucket.

Contents

id

The canonical user ID of the bucket owner. For information about locating your canonical user ID see Finding Your Account Canonical User ID.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PermissionConfiguration

Contains information about how permissions are configured for the S3 bucket.

Contents

accountLevelPermissions

Contains information about the account level permissions on the S3 bucket.

Type: AccountLevelPermissions object

Required: No

bucketLevelPermissions

Contains information about the bucket level permissions for the S3 bucket.

Type: BucketLevelPermissions object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PortProbeAction

Contains information about the PORT_PROBE action described in the finding.

Contents

blocked

Indicates whether EC2 blocked the port probe to the instance, such as with an ACL.

Type: Boolean

Required: No

portProbeDetails

A list of objects related to port probe details.

Type: Array of PortProbeDetail objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PortProbeDetail

Contains information about the port probe details.

Contents

localIpDetails

The local IP information of the connection.

Type: LocalIpDetails object

Required: No

localPortDetails

The local port information of the connection.

Type: LocalPortDetails object

Required: No

remoteIpDetails

The remote IP information of the connection.

Type: RemoteIpDetails object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PrivateIpAddressDetails

Contains other private IP address information of the EC2 instance.

Contents

privateDnsName

The private DNS name of the EC2 instance.

Type: String

Required: No

privateIpAddress

The private IP address of the EC2 instance.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ProcessDetails

Information about the observed process.

Contents

euid

The effective user ID of the user that executed the process.

Type: Integer

Required: No

executablePath

The absolute path of the process executable file.

Type: String

Required: No

executableSha256

The SHA256 hash of the process executable.

Type: String

Required: No

lineage

Information about the process's lineage.

Type: Array of LineageObject objects

Required: No

name

The name of the process.

Type: String

Required: No

namespacePid

The ID of the child process.

Type: Integer

Required: No

parentUuid

The unique ID of the parent process. This ID is assigned to the parent process by GuardDuty.

Type: String

Required: No

pid

The ID of the process.

Type: Integer

Required: No

pwd

The present working directory of the process.

Type: String

Required: No

startTime

The time when the process started. This is in UTC format.

Type: Timestamp

Required: No

user

The user that executed the process.

Type: String

Required: No

userId

The unique ID of the user that executed the process.

Type: Integer

Required: No

uuid

The unique ID assigned to the process by GuardDuty.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Product

Contains information about the product that produced an investigation.

Contents

name

The name of the product.

Type: String

Required: Yes

feature

The specific feature within the product that produced the investigation.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ProductCode

Contains information about the product code for the EC2 instance.

Contents

productCodeId

The product code information.

Type: String

Required: No

productCodeType

The product code type.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PublicAccess

Describes the public access policies that apply to the S3 bucket.

Contents

effectivePermission

Describes the effective permission on this bucket after factoring all attached policies.

Type: String

Required: No

permissionConfiguration

Contains information about how permissions are configured for the S3 bucket.

Type: PermissionConfiguration object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PublicAccessConfiguration

Describes public access policies that apply to the Amazon S3 bucket.

For information about each of the following settings, see Blocking public access to your Amazon S3 storage in the *Amazon S3 User Guide*.

Contents

publicAclAccess

Indicates whether or not there is a setting that allows public access to the Amazon S3 buckets through access control lists (ACLs).

Type: String

Valid Values: `BLOCKED | ALLOWED`

Required: No

publicAclIgnoreBehavior

Indicates whether or not there is a setting that ignores all public access control lists (ACLs) on the Amazon S3 bucket and the objects that it contains.

Type: String

Valid Values: `IGNORED | NOT_IGNORED`

Required: No

publicBucketRestrictBehavior

Indicates whether or not there is a setting that restricts access to the bucket with specified policies.

Type: String

Valid Values: `RESTRICTED | NOT_RESTRICTED`

Required: No

publicPolicyAccess

Indicates whether or not there is a setting that allows public access to the Amazon S3 bucket policy.

Type: String

Valid Values: `BLOCKED | ALLOWED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RdsDbInstanceDetails

Contains information about the resource type `RDSDBInstance` involved in a GuardDuty finding.

Contents

dbClusterIdentifier

The identifier of the database cluster that contains the database instance ID involved in the finding.

Type: String

Required: No

dbInstanceArn

The Amazon Resource Name (ARN) that identifies the database instance involved in the finding.

Type: String

Required: No

dbInstanceIdentifier

The identifier associated to the database instance that was involved in the finding.

Type: String

Required: No

dbiResourceId

The unique ID of the database resource involved in the activity that prompted GuardDuty to generate the finding.

Type: String

Required: No

engine

The database engine of the database instance involved in the finding.

Type: String

Required: No

engineVersion

The version of the database engine that was involved in the finding.

Type: String

Required: No

tags

Information about the tag key-value pairs.

Type: Array of Tag objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RdsDbUserDetails

Contains information about the user and authentication details for a database instance involved in the finding.

Contents

application

The application name used in the anomalous login attempt.

Type: String

Required: No

authMethod

The authentication method used by the user involved in the finding.

Type: String

Required: No

database

The name of the database instance involved in the anomalous login attempt.

Type: String

Required: No

ssl

The version of the Secure Socket Layer (SSL) used for the network.

Type: String

Required: No

user

The user name used in the anomalous login attempt.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RdsLimitlessDbDetails

Contains information about the resource type `RDSLimitlessDB` that is involved in a GuardDuty finding.

Contents

dbClusterIdentifier

The name of the database cluster that is a part of the Limitless Database.

Type: String

Required: No

dbShardGroupArn

The Amazon Resource Name (ARN) that identifies the DB shard group.

Type: String

Required: No

dbShardGroupIdentifier

The name associated with the Limitless DB shard group.

Type: String

Required: No

dbShardGroupResourceId

The resource identifier of the DB shard group within the Limitless Database.

Type: String

Required: No

engine

The database engine of the database instance involved in the finding.

Type: String

Required: No

engineVersion

The version of the database engine.

Type: String

Required: No

tags

Information about the tag key-value pair.

Type: Array of Tag objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RdsLoginAttemptAction

Indicates that a login attempt was made to the potentially compromised database from a remote IP address.

Contents

LoginAttributes

Indicates the login attributes used in the login attempt.

Type: Array of LoginAttribute objects

Required: No

remoteIpDetails

Contains information about the remote IP address of the connection.

Type: RemoteIpDetails object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPoint

Contains information about the recovery point configuration for scanning backup data from AWS Backup.

Contents

backupVaultName

The name of the AWS Backup vault that contains the name of the recovery point to be scanned.

Type: String

Required: Yes

continuousScanDetails

Contains information about the time range within the continuous backup in AWS Backup to scan.

Type: ContinuousScanDetails object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointDetails

Contains details about the backup recovery point.

Contents

backupVaultName

The name of the backup vault containing the recovery point.

Type: String

Required: No

continuousScanDetails

Contains information about the time range within the continuous backup in AWS Backup that was scanned for a point-in-time recovery resource.

Type: ScanConfigurationContinuousScanDetails object

Required: No

recoveryPointArn

The Amazon Resource Name (ARN) of the recovery point.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RemoteAccountDetails

Contains details about the remote AWS account that made the API call.

Contents

accountId

The AWS account ID of the remote API caller.

Type: String

Required: No

affiliated

Details on whether the AWS account of the remote API caller is related to your GuardDuty environment. If this value is `True` the API caller is affiliated to your account in some way. If it is `False` the API caller is from outside your environment.

Type: Boolean

Required: No

awsServiceName

If the remote account belongs to an AWS service, this field indicates which service the remote account belongs to.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RemoteIpDetails

Contains information about the remote IP address of the connection.

Contents

city

The city information of the remote IP address.

Type: City object

Required: No

country

The country code of the remote IP address.

Type: Country object

Required: No

geoLocation

The location information of the remote IP address.

Type: GeoLocation object

Required: No

ipAddressV4

The IPv4 remote address of the connection.

Type: String

Required: No

ipAddressV6

The IPv6 remote address of the connection.

Type: String

Required: No

organization

The ISP organization information of the remote IP address.

Type: Organization object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RemotePortDetails

Contains information about the remote port.

Contents

port

The port number of the remote connection.

Type: Integer

Required: No

portName

The port name of the remote connection.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Resource

Contains information about the AWS resource associated with the activity that prompted GuardDuty to generate a finding.

Contents

accessKeyDetails

The IAM access key details (user information) of a user that engaged in the activity that prompted GuardDuty to generate a finding.

Type: AccessKeyDetails object

Required: No

bedrockGuardrailDetails

Contains information about the Bedrock guardrail that was involved in a finding.

Type: BedrockGuardrailDetails object

Required: No

containerDetails

Details of a container.

Type: Container object

Required: No

ebsSnapshotDetails

Contains details about the EBS snapshot that was scanned.

Type: EbsSnapshotDetails object

Required: No

ebsVolumeDetails

Contains list of scanned and skipped EBS volumes with details.

Type: EbsVolumeDetails object

Required: No

ec2ImageDetails

Contains details about the EC2 image that was scanned.

Type: Ec2ImageDetails object

Required: No

ecsClusterDetails

Contains information about the details of the ECS Cluster.

Type: EcsClusterDetails object

Required: No

eksClusterDetails

Details about the EKS cluster involved in a Kubernetes finding.

Type: EksClusterDetails object

Required: No

instanceDetails

The information about the EC2 instance associated with the activity that prompted GuardDuty to generate a finding.

Type: InstanceDetails object

Required: No

kubernetesDetails

Details about the Kubernetes user and workload involved in a Kubernetes finding.

Type: KubernetesDetails object

Required: No

lambdaDetails

Contains information about the Lambda function that was involved in a finding.

Type: LambdaDetails object

Required: No

modelDetails

Contains information about the AI models involved in a finding.

Type: Array of ModelDetail objects

Required: No

rdsDbInstanceDetails

Contains information about the database instance to which an anomalous login attempt was made.

Type: RdsDbInstanceDetails object

Required: No

rdsDbUserDetails

Contains information about the user details through which anomalous login attempt was made.

Type: RdsDbUserDetails object

Required: No

rdsLimitlessDbDetails

Contains information about the RDS Limitless database that was involved in a GuardDuty finding.

Type: RdsLimitlessDbDetails object

Required: No

recoveryPointDetails

Contains details about the backup recovery point that was scanned.

Type: RecoveryPointDetails object

Required: No

resourceType

The type of AWS resource.

Type: String

Required: No

s3BucketDetails

Contains information on the S3 bucket.

Type: Array of S3BucketDetail objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ResourceData

Contains information about the AWS resource that is associated with the activity that prompted GuardDuty to generate a finding.

Contents

accessKey

Contains information about the IAM access key details of a user that involved in the GuardDuty finding.

Type: AccessKey object

Required: No

autoscalingAutoScalingGroup

Contains detailed information about the Auto Scaling Group associated with the activity that prompted GuardDuty to generate a finding.

Type: AutoscalingAutoScalingGroup object

Required: No

bedrockGuardrail

Contains detailed information about the Amazon Bedrock guardrail associated with the activity that prompted GuardDuty to generate a finding.

Type: BedrockGuardrailResource object

Required: No

cloudformationStack

Contains detailed information about the CloudFormation stack associated with the activity that prompted GuardDuty to generate a finding.

Type: CloudformationStack object

Required: No

container

Contains detailed information about the container associated with the activity that prompted GuardDuty to generate a finding.

Type: ContainerFindingResource object

Required: No

ec2Image

Contains detailed information about the EC2 Image associated with the activity that prompted GuardDuty to generate a finding.

Type: Ec2Image object

Required: No

ec2Instance

Contains information about the Amazon EC2 instance.

Type: Ec2Instance object

Required: No

ec2LaunchTemplate

Contains detailed information about the EC2 launch template associated with the activity that prompted GuardDuty to generate a finding.

Type: Ec2LaunchTemplate object

Required: No

ec2NetworkInterface

Contains information about the elastic network interface of the Amazon EC2 instance.

Type: Ec2NetworkInterface object

Required: No

ec2Vpc

Contains detailed information about the EC2 VPC associated with the activity that prompted GuardDuty to generate a finding.

Type: Ec2Vpc object

Required: No

ecsCluster

Contains detailed information about the Amazon ECS cluster associated with the activity that prompted GuardDuty to generate a finding.

Type: EcsCluster object

Required: No

ecsTask

Contains detailed information about the Amazon ECS task associated with the activity that prompted GuardDuty to generate a finding.

Type: EcsTask object

Required: No

eksCluster

Contains detailed information about the Amazon EKS cluster associated with the activity that prompted GuardDuty to generate a finding.

Type: EksCluster object

Required: No

iamInstanceProfile

Contains detailed information about the IAM instance profile associated with the activity that prompted GuardDuty to generate a finding.

Type: IamInstanceProfileV2 object

Required: No

kubernetesWorkload

Contains detailed information about the Kubernetes workload associated with the activity that prompted GuardDuty to generate a finding.

Type: KubernetesWorkload object

Required: No

s3Bucket

Contains information about the Amazon S3 bucket.

Type: S3Bucket object

Required: No

s3Object

Contains information about the Amazon S3 object.

Type: S3Object object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ResourceDetails

Represents the resources that were scanned in the scan entry.

Contents

instanceArn

Instance ARN that was scanned in the scan entry.

Type: String

Pattern: `arn:(aws|aws-cn|aws-us-gov):[a-z]+:[a-z]+(-[0-9]+|-[a-z]+)+:([0-9]{12}):[a-z\-]+\/[a-zA-Z0-9]*`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ResourceStatistics

Information about each resource type associated with the `groupedByResource` statistics.

Contents

accountId

The ID of the AWS account.

Type: String

Required: No

lastGeneratedAt

The timestamp at which the statistics for this resource was last generated.

Type: Timestamp

Required: No

resourceId

ID associated with each resource. The following list provides the mapping of the resource type and resource ID.

Mapping of resource and resource ID

- AccessKey - `resource.accessKeyDetails.accessKeyId`
- Container - `resource.containerDetails.id`
- ECSCluster - `resource.ecsClusterDetails.name`
- EKSCluster - `resource.eksClusterDetails.name`
- Instance - `resource.instanceDetails.instanceId`
- KubernetesCluster - `resource.kubernetesDetails.kubernetesWorkloadDetails.name`
- Lambda - `resource.lambdaDetails.functionName`
- RDSDBInstance - `resource.rdsDbInstanceDetails.dbInstanceIdentifier`
- S3Bucket - `resource.s3BucketDetails.name`
- S3Object - `resource.s3BucketDetails.name`

Type: String

Required: No

resourceType

The type of resource.

Type: String

Required: No

totalFindings

The total number of findings associated with this resource.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ResourceV2

Contains information about the AWS resource that is associated with the GuardDuty finding.

Contents

resourceType

The type of the AWS resource.

Type: String

Valid Values: `EC2_INSTANCE | EC2_NETWORK_INTERFACE | S3_BUCKET | S3_OBJECT | ACCESS_KEY | EKS_CLUSTER | KUBERNETES_WORKLOAD | CONTAINER | ECS_CLUSTER | ECS_TASK | AUTOSCALING_AUTO_SCALING_GROUP | IAM_INSTANCE_PROFILE | CLOUDFORMATION_STACK | EC2_LAUNCH_TEMPLATE | EC2_VPC | EC2_IMAGE | BEDROCK_CUSTOM_MODEL | BEDROCK_IMPORTED_MODEL | BEDROCK_PROVISIONED_MODEL | BEDROCK_CUSTOM_MODEL_DEPLOYMENT | BEDROCK_INFERENCE_PROFILE | BEDROCK_APPLICATION_INFERENCE_PROFILE | BEDROCK_PROMPT | BEDROCK_PROMPT_ROUTER | BEDROCK_GUARDRAIL | SAGEMAKER_ENDPOINT`

Required: Yes

uid

The unique identifier of the resource.

Type: String

Required: Yes

accountId

The AWS account ID to which the resource belongs.

Type: String

Required: No

cloudPartition

The cloud partition within the AWS Region to which the resource belongs.

Type: String

Required: No

data

Contains information about the AWS resource associated with the activity that prompted GuardDuty to generate a finding.

Type: ResourceData object

Required: No

name

The name of the resource.

Type: String

Required: No

region

The AWS Region where the resource belongs.

Type: String

Required: No

service

The AWS service of the resource.

Type: String

Required: No

tags

Contains information about the tags associated with the resource.

Type: Array of Tag objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleDefinition

Contains the detection logic for a custom detection rule.

Contents

expression

The detection logic expression for the rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleDetail

Contains the full details of a custom detection rule, including its detection logic.

Contents

arn

The Amazon Resource Name (ARN) of the rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `arn:[a-zA-Z0-9\-]+:[a-zA-Z0-9\-]+:[a-zA-Z0-9\-]*:([0-9]*|aws):.+`

Required: Yes

createdAt

The timestamp when the rule was created.

Type: Timestamp

Required: Yes

dataSource

The data source that the rule analyzes.

Type: String

Valid Values: `CloudTrailManagementEvent | RuntimeMonitoring`

Required: Yes

definition

The detection logic definition for the rule.

Type: RuleDefinition object

Required: Yes

description

A description of what the rule detects.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: Yes

name

The display name of the rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: Yes

ruleId

The unique identifier for the rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Required: Yes

service

The AWS service associated with the rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: Yes

severity

The severity level assigned to findings generated by this rule.

Type: String

Valid Values: `CRITICAL | HIGH | MEDIUM | LOW`

Required: Yes

tactic

The MITRE ATT&CK tactic associated with the rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: Yes

technique

The MITRE ATT&CK technique associated with the rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: Yes

language

The language used for the detection logic expression.

Type: String

Valid Values: SQL

Required: No

runtimeMonitoringDetails

Runtime Monitoring-specific details for the rule, including the platforms on which the rule can run and the minimum GuardDuty agent version required on each.

Type: DetectionRuleRuntimeMonitoringDetails object

Required: No

schema

The schema version used by the rule definition.

Type: String

Valid Values: `CloudTrail`

Required: No

updatedAt

The timestamp when the rule was last updated.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleSummary

Contains summary information about a custom detection rule.

Contents

arn

The Amazon Resource Name (ARN) of the rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `arn:[a-zA-Z0-9\-]+:[a-zA-Z0-9\-]+:[a-zA-Z0-9\-]*:([0-9]*|aws):.+`

Required: Yes

createdAt

The timestamp when the rule was created.

Type: Timestamp

Required: Yes

dataSource

The data source that the rule analyzes.

Type: String

Valid Values: `CloudTrailManagementEvent | RuntimeMonitoring`

Required: Yes

description

A description of what the rule detects.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: Yes

name

The display name of the rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: Yes

ruleId

The unique identifier for the rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `[a-z0-9]+(-[a-z0-9]+)*`

Required: Yes

service

The AWS service associated with the rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: Yes

severity

The severity level assigned to findings generated by this rule.

Type: String

Valid Values: `CRITICAL | HIGH | MEDIUM | LOW`

Required: Yes

tactic

The MITRE ATT&CK tactic associated with the rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: Yes

technique

The MITRE ATT&CK technique associated with the rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: Yes

language

The language used for the detection logic expression.

Type: String

Valid Values: SQL

Required: No

schema

The schema version used by the rule definition.

Type: String

Valid Values: `CloudTrail`

Required: No

updatedAt

The timestamp when the rule was last updated.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuntimeContext

Additional information about the suspicious activity.

Contents

addressFamily

Represents the communication protocol associated with the address. For example, the address family `AF_INET` is used for IP version of 4 protocol.

Type: String

Required: No

commandLineExample

Example of the command line involved in the suspicious activity.

Type: String

Required: No

fileOperation

Represents the type of file operation that triggered the finding, such as Write, Delete, Rename, Link, or Symlink.

Type: String

Required: No

filePath

The path of the sensitive file that was modified. Modification includes write, delete, rename, link, or symlink operations. This field is indexed for filtering.

Type: String

Required: No

fileSystemType

Represents the type of mounted fileSystem.

Type: String

Required: No

flags

Represents options that control the behavior of a runtime operation or action. For example, a filesystem mount operation may contain a read-only flag.

Type: Array of strings

Required: No

ianaProtocolNumber

Specifies a particular protocol within the address family. Usually there is a single protocol in address families. For example, the address family `AF_INET` only has the IP protocol.

Type: Integer

Required: No

ldPreloadValue

The value of the LD_PRELOAD environment variable.

Type: String

Required: No

libraryPath

The path to the new library that was loaded.

Type: String

Required: No

memoryRegions

Specifies the Region of a process's address space such as stack and heap.

Type: Array of strings

Required: No

modifiedAt

The timestamp at which the process modified the current process. The timestamp is in UTC date string format.

Type: Timestamp

Required: No

modifyingProcess

Information about the process that modified the current process. This is available for multiple finding types.

Type: ProcessDetails object

Required: No

moduleFilePath

The path to the module loaded into the kernel.

Type: String

Required: No

moduleName

The name of the module loaded into the kernel.

Type: String

Required: No

moduleSha256

The SHA256 hash of the module.

Type: String

Required: No

mountSource

The path on the host that is mounted by the container.

Type: String

Required: No

mountTarget

The path in the container that is mapped to the host directory.

Type: String

Required: No

relatedFilePaths

All file paths modified by the same process that triggered the finding, up to a maximum of 25 paths.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 25 items.

Required: No

releaseAgentPath

The path in the container that modified the release agent file.

Type: String

Required: No

runcBinaryPath

The path to the leveraged `runc` implementation.

Type: String

Required: No

scriptPath

The path to the script that was executed.

Type: String

Required: No

serviceName

Name of the security service that has been potentially disabled.

Type: String

Required: No

shellHistoryFilePath

The path to the modified shell history file.

Type: String

Required: No

socketPath

The path to the docket socket that was accessed.

Type: String

Required: No

targetProcess

Information about the process that had its memory overwritten by the current process.

Type: ProcessDetails object

Required: No

threatFilePath

The suspicious file path for which the threat intelligence details were found.

Type: String

Required: No

toolCategory

Category that the tool belongs to. Some of the examples are Backdoor Tool, Pentest Tool, Network Scanner, and Network Sniffer.

Type: String

Required: No

toolName

Name of the potentially suspicious tool.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuntimeDetails

Information about the process and any required context values for a specific finding.

Contents

context

Additional information about the suspicious activity.

Type: RuntimeContext object

Required: No

process

Information about the observed process.

Type: ProcessDetails object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

S3Bucket

Contains information about the Amazon S3 bucket policies and encryption.

Contents

accountPublicAccess

Contains information about the public access policies that apply to the Amazon S3 bucket at the account level.

Type: PublicAccessConfiguration object

Required: No

bucketPublicAccess

Contains information about public access policies that apply to the Amazon S3 bucket.

Type: PublicAccessConfiguration object

Required: No

createdAt

The timestamp at which the Amazon S3 bucket was created.

Type: Timestamp

Required: No

effectivePermission

Describes the effective permissions on this S3 bucket, after factoring all the attached policies.

Type: String

Required: No

encryptionKeyArn

The Amazon Resource Name (ARN) of the encryption key that is used to encrypt the Amazon S3 bucket and its objects.

Type: String

Required: No

encryptionType

The type of encryption used for the Amazon S3 buckets and its objects. For more information, see Protecting data with server-side encryption in the *Amazon S3 User Guide*.

Type: String

Required: No

ownerId

The owner ID of the associated S3Amazon S3bucket.

Type: String

Required: No

publicReadAccess

Indicates whether or not the public read access is allowed for an Amazon S3 bucket.

Type: String

Valid Values: `BLOCKED | ALLOWED`

Required: No

publicWriteAccess

Indicates whether or not the public write access is allowed for an Amazon S3 bucket.

Type: String

Valid Values: `BLOCKED | ALLOWED`

Required: No

s3ObjectUids

Represents a list of Amazon S3 object identifiers.

Type: Array of strings

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

S3BucketDetail

Contains information on the S3 bucket.

Contents

arn

The Amazon Resource Name (ARN) of the S3 bucket.

Type: String

Required: No

createdAt

The date and time the bucket was created at.

Type: Timestamp

Required: No

defaultServerSideEncryption

Describes the server side encryption method used in the S3 bucket.

Type: DefaultServerSideEncryption object

Required: No

name

The name of the S3 bucket.

Type: String

Required: No

owner

The owner of the S3 bucket.

Type: Owner object

Required: No

publicAccess

Describes the public access policies that apply to the S3 bucket.

Type: PublicAccess object

Required: No

s3ObjectDetails

Information about the S3 object that was scanned.

Type: Array of S3ObjectDetail objects

Required: No

tags

All tags attached to the S3 bucket

Type: Array of Tag objects

Required: No

type

Describes whether the bucket is a source or destination bucket.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

S3LogsConfiguration

Describes whether S3 data event logs will be enabled as a data source.

Contents

enable

The status of S3 data event logs as a data source.

Type: Boolean

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

S3LogsConfigurationResult

Describes whether S3 data event logs will be enabled as a data source.

Contents

status

A value that describes whether S3 data event logs are automatically enabled for new members of the organization.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `ENABLED | DISABLED`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

S3Object

Contains information about the Amazon S3 object.

Contents

eTag

The entity tag is a hash of the Amazon S3 object. The ETag reflects changes only to the contents of an object, and not its metadata.

Type: String

Required: No

key

The key of the Amazon S3 object.

Type: String

Required: No

versionId

The version Id of the Amazon S3 object.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

S3ObjectDetail

Information about the S3 object that was scanned

Contents

eTag

The entity tag is a hash of the S3 object. The ETag reflects changes only to the contents of an object, and not its metadata.

Type: String

Required: No

hash

Hash of the threat detected in this finding.

Type: String

Required: No

key

Key of the S3 object.

Type: String

Required: No

objectArn

Amazon Resource Name (ARN) of the S3 object.

Type: String

Required: No

versionId

Version ID of the object.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

S3ObjectForSendObjectMalwareScan

The S3 object path to initiate a scan, including bucket name, object key, and optional version ID.

Contents

bucket

The name of the S3 bucket containing the object to scan. The bucket must have GuardDuty Malware Protection enabled.

Type: String

Required: No

key

The key (name) of the S3 object to scan for malware. This must be the full key path of the object within the bucket.

Type: String

Required: No

versionId

The version ID of the S3 object to scan. If not specified, the latest version of the object is scanned.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Scan

Contains information about malware scans associated with GuardDuty Malware Protection for EC2.

Contents

accountId

The ID for the account that belongs to the scan.

Type: String

Length Constraints: Fixed length of 12.

Required: No

adminDetectorId

The unique detector ID of the administrator account that the request is associated with. If the account is an administrator, the `AdminDetectorId` will be the same as the one used for `DetectorId`.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

attachedVolumes

List of volumes that were attached to the original instance to be scanned.

Type: Array of VolumeDetail objects

Required: No

detectorId

The unique ID of the detector that is associated with the request.

To find the `detectorId` in the current Region, see the Settings page in the GuardDuty console, or run the ListDetectors API.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

failureReason

Represents the reason for `FAILED` scan status.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

fileCount

Represents the number of files that were scanned.

Type: Long

Valid Range: Minimum value of 0.

Required: No

resourceDetails

Represents the resources that were scanned in the scan entry.

Type: ResourceDetails object

Required: No

scanEndTime

The timestamp of when the scan was finished.

Type: Timestamp

Required: No

scanId

The unique scan ID associated with a scan entry.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

scanResultDetails

Represents the result of the scan.

Type: ScanResultDetails object

Required: No

scanStartTime

The timestamp of when the scan was triggered.

Type: Timestamp

Required: No

scanStatus

An enum value representing possible scan statuses.

Type: String

Valid Values: `RUNNING | COMPLETED | FAILED | SKIPPED`

Required: No

scanType

Specifies the scan type that invoked the malware scan.

Type: String

Valid Values: `GUARDDUTY_INITIATED | ON_DEMAND`

Required: No

totalBytes

Represents total bytes that were scanned.

Type: Long

Valid Range: Minimum value of 0.

Required: No

triggerDetails

Specifies the reason why the scan was initiated.

Type: TriggerDetails object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScanCondition

Contains information about the condition.

Contents

mapEquals

Represents an *mapEqual* condition to be applied to a single field when triggering for malware scan.

Type: Array of ScanConditionPair objects

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScanConditionPair

Represents the `key:value` pair to be matched against given resource property.

Contents

key

Represents the **key** in the map condition.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `(?!aws:)[a-zA-Z+-=._:/]+`

Required: Yes

value

Represents optional **value** in the map condition. If not specified, only the **key** will be matched.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScanConfiguration

Contains information about the configuration used for the malware scan.

Contents

incrementalScanDetails

Information about the incremental scan configuration, if applicable.

Type: IncrementalScanDetails object

Required: No

recoveryPoint

Information about the recovery point configuration used for the scan, if applicable.

Type: ScanConfigurationRecoveryPoint object

Required: No

role

Amazon Resource Name (ARN) of the IAM role that should contain the required permissions for the scan.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

triggerDetails

Information about the entity that triggered the malware scan.

Type: TriggerDetails object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScanConfigurationContinuousScanDetails

Contains information about the time range within the continuous backup in AWS Backup that was scanned for a point-in-time recovery resource.

Contents

endTime

The timestamp representing the end of the time range that was scanned.

Type: Timestamp

Required: Yes

startTime

The timestamp representing the start of the time range that was scanned.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScanConfigurationRecoveryPoint

Contains information about the recovery point configuration used in the scan.

Contents

backupVaultName

The name of the AWS Backup vault that contains the recovery point for the scanned.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

continuousScanDetails

The time range within the continuous backup in AWS Backup that was scanned for a point-in-time recovery resource.

Type: ScanConfigurationContinuousScanDetails object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScanDetections

Contains a complete view providing malware scan result details.

Contents

highestSeverityThreatDetails

Details of the highest severity threat detected during malware scan and number of infected files.

Type: HighestSeverityThreatDetails object

Required: No

scannedItemCount

Total number of scanned files.

Type: ScannedItemCount object

Required: No

threatDetectedByName

Contains details about identified threats organized by threat name.

Type: ThreatDetectedByName object

Required: No

threatsDetectedItemCount

Total number of infected files.

Type: ThreatsDetectedItemCount object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScanEc2InstanceWithFindings

Describes whether Malware Protection for EC2 instances with findings will be enabled as a data source.

Contents

ebsVolumes

Describes the configuration for scanning EBS volumes as data source.

Type: Boolean

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScanEc2InstanceWithFindingsResult

An object that contains information on the status of whether Malware Protection for EC2 instances with findings will be enabled as a data source.

Contents

ebsVolumes

Describes the configuration of scanning EBS volumes as a data source.

Type: EbsVolumesResult object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScanFilePath

Contains details of infected file including name, file path and hash.

Contents

fileName

File name of the infected file.

Type: String

Required: No

filePath

The file path of the infected file.

Type: String

Required: No

hash

The hash value of the infected file.

Type: String

Required: No

volumeArn

EBS volume ARN details of the infected file.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScannedItemCount

Total number of scanned files.

Contents

files

Number of files scanned.

Type: Integer

Required: No

totalGb

Total GB of files scanned for malware.

Type: Integer

Required: No

volumes

Total number of scanned volumes.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScannedResource

Contains information about a resource that was scanned as part of the malware scan operation.

Contents

resourceDetails

Information about the scanned resource.

Type: ScannedResourceDetails object

Required: No

scannedResourceArn

Amazon Resource Name (ARN) of the scanned resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

scannedResourceStatus

The status of the scanned resource.

Type: String

Valid Values: `RUNNING | COMPLETED | COMPLETED_WITH_ISSUES | FAILED | SKIPPED`

Required: No

scannedResourceType

The resource type of the scanned resource.

Type: String

Valid Values: `EBS_RECOVERY_POINT | EBS_SNAPSHOT | EBS_VOLUME | EC2_AMI | EC2_INSTANCE | EC2_RECOVERY_POINT | S3_RECOVERY_POINT | S3_BUCKET | S3_POINT_IN_TIME_RECOVERY`

Required: No

scanStatusReason

The reason for the scan status of this particular resource, if applicable.

Type: String

Valid Values: `ACCESS_DENIED | RESOURCE_NOT_FOUND | SNAPSHOT_SIZE_LIMIT_EXCEEDED | RESOURCE_UNAVAILABLE | INCONSISTENT_SOURCE | INCREMENTAL_NO_DIFFERENCE | NO_EBS_VOLUMES_FOUND | UNSUPPORTED_PRODUCT_CODE_TYPE | AMI_SNAPSHOT_LIMIT_EXCEEDED | UNRELATED_RESOURCES | BASE_RESOURCE_NOT_SCANNED | BASE_CREATED_AFTER_TARGET | UNSUPPORTED_FOR_INCREMENTAL | UNSUPPORTED_AMI | UNSUPPORTED_SNAPSHOT | UNSUPPORTED_COMPOSITE_RECOVERY_POINT | ALL_FILES_SKIPPED_OR_FAILED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScannedResourceDetails

Contains additional information about a resource that was scanned.

Contents

ebsSnapshot

Contains information about the EBS snapshot that was scanned.

Type: EbsSnapshot object

Required: No

ebsVolume

Contains information about the EBS volume that was scanned.

Type: VolumeDetail object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScanResourceCriteria

Contains information about criteria used to filter resources before triggering malware scan.

Contents

exclude

Represents condition that when matched will prevent a malware scan for a certain resource.

Type: String to ScanCondition object map

Valid Keys: `EC2_INSTANCE_TAG`

Required: No

include

Represents condition that when matched will allow a malware scan for a certain resource.

Type: String to ScanCondition object map

Valid Keys: `EC2_INSTANCE_TAG`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScanResultDetails

Represents the result of the scan.

Contents

scanResult

An enum value representing possible scan results.

Type: String

Valid Values: `CLEAN | INFECTED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScanResultThreat

Contains information about a specific threat that was detected during the malware scan.

Contents

count

The number of instances of this threat that were detected.

Type: Long

Valid Range: Minimum value of 0.

Required: No

hash

The hash value associated with the detected threat.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

itemDetails

Additional information about where this threat was detected.

Type: Array of ItemDetails objects

Required: No

name

The name of the detected threat.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

source

The source that detected this threat.

Type: String

Valid Values: `AMAZON | BITDEFENDER`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ScanThreatName

Contains files infected with the given threat providing details of malware name and severity.

Contents

filePaths

List of infected files in EBS volume with details.

Type: Array of ScanFilePath objects

Required: No

itemCount

Total number of files infected with given threat.

Type: Integer

Required: No

name

The name of the identified threat.

Type: String

Required: No

severity

Severity of threat identified as part of the malware scan.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

SecurityContext

Container security context.

Contents

allowPrivilegeEscalation

Whether or not a container or a Kubernetes pod is allowed to gain more privileges than its parent process.

Type: Boolean

Required: No

privileged

Whether the container is privileged.

Type: Boolean

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SecurityGroup

Contains information about the security groups associated with the EC2 instance.

Contents

groupId

The security group ID of the EC2 instance.

Type: String

Required: No

groupName

The security group name of the EC2 instance.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Sequence

Contains information about the GuardDuty attack sequence finding.

Contents

description

Description of the attack sequence.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 4096.

Required: Yes

signals

Contains information about the signals involved in the attack sequence.

Type: Array of Signal objects

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Required: Yes

uid

Unique identifier of the attack sequence.

Type: String

Required: Yes

actors

Contains information about the actors involved in the attack sequence.

Type: Array of Actor objects

Array Members: Minimum number of 0 items. Maximum number of 400 items.

Required: No

additionalSequenceTypes

Additional types of sequences that may be associated with the attack sequence finding, providing further context about the nature of the detected threat.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 100.

Required: No

endpoints

Contains information about the network endpoints that were used in the attack sequence.

Type: Array of NetworkEndpoint objects

Array Members: Minimum number of 0 items. Maximum number of 400 items.

Required: No

resources

Contains information about the resources involved in the attack sequence.

Type: Array of ResourceV2 objects

Array Members: Minimum number of 0 items. Maximum number of 400 items.

Required: No

sequenceIndicators

Contains information about the indicators observed in the attack sequence.

Type: Array of Indicator objects

Array Members: Minimum number of 0 items. Maximum number of 400 items.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Service

Contains additional information about the generated finding.

Contents

action

Information about the activity that is described in a finding.

Type: Action object

Required: No

additionalInfo

Contains additional information about the generated finding.

Type: ServiceAdditionalInfo object

Required: No

archived

Indicates whether this finding is archived.

Type: Boolean

Required: No

count

The total count of the occurrences of this finding type.

Type: Integer

Required: No

detection

Contains information about the detected unusual behavior.

Type: Detection object

Required: No

detectorId

The detector ID for the GuardDuty service.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

ebsVolumeScanDetails

Returns details from the malware scan that created a finding.

Type: EbsVolumeScanDetails object

Required: No

eventFirstSeen

The first-seen timestamp of the activity that prompted GuardDuty to generate this finding.

Type: String

Required: No

eventLastSeen

The last-seen timestamp of the activity that prompted GuardDuty to generate this finding.

Type: String

Required: No

evidence

An evidence object associated with the service.

Type: Evidence object

Required: No

featureName

The name of the feature that generated a finding.

Type: String

Required: No

malwareScanDetails

Returns details from the malware scan that generated a GuardDuty finding.

Type: MalwareScanDetails object

Required: No

resourceRole

The resource role information for this finding.

Type: String

Required: No

runtimeDetails

Information about the process and any required context values for a specific finding

Type: RuntimeDetails object

Required: No

serviceName

The name of the AWS service (GuardDuty) that generated a finding.

Type: String

Required: No

userFeedback

Feedback that was submitted about the finding.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ServiceAdditionalInfo

Additional information about the generated finding.

Contents

type

Describes the type of the additional information.

Type: String

Required: No

value

This field specifies the value of the additional information.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Session

Contains information about the authenticated session.

Contents

createdTime

The timestamp for when the session was created.

In AWS CloudTrail, you can find this value as `userIdentity.sessionContext.attributes.creationDate`.

Type: Timestamp

Required: No

issuer

Identifier of the session issuer.

In AWS CloudTrail, you can find this value as `userIdentity.sessionContext.sessionIssuer.arn`.

Type: String

Required: No

mfaStatus

Indicates whether or not multi-factor authencation (MFA) was used during authentication.

In AWS CloudTrail, you can find this value as `userIdentity.sessionContext.attributes.mfaAuthenticated`.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

uid

The unique identifier of the session.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SeverityStatistics

Information about severity level for each finding type.

Contents

lastGeneratedAt

The timestamp at which a finding type for a specific severity was last generated.

Type: Timestamp

Required: No

severity

The severity level associated with each finding type.

Type: Double

Required: No

totalFindings

The total number of findings associated with this severity.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Signal

Contains information about the signals involved in the attack sequence.

Contents

count

The number of times this signal was observed.

Type: Integer

Required: Yes

createdAt

The timestamp when the first finding or activity related to this signal was observed.

Type: Timestamp

Required: Yes

firstSeenAt

The timestamp when the first finding or activity related to this signal was observed.

Type: Timestamp

Required: Yes

lastSeenAt

The timestamp when the last finding or activity related to this signal was observed.

Type: Timestamp

Required: Yes

name

The name of the signal. For example, when signal type is `FINDING`, the signal name is the name of the finding.

Type: String

Required: Yes

type

The type of the signal used to identify an attack sequence.

Signals can be GuardDuty findings or activities observed in data sources that GuardDuty monitors. For more information, see Foundational data sources in the *Amazon GuardDuty User Guide*.

A signal type can be one of the valid values listed in this API. Here are the related descriptions:

- `FINDING` - Individually generated GuardDuty finding.
- `CLOUD_TRAIL` - Activity observed from CloudTrail logs
- `S3_DATA_EVENTS` - Activity observed from CloudTrail data events for S3. Activities associated with this type will show up only when you have enabled GuardDuty S3 Protection feature in your account. For more information about S3 Protection and steps to enable it, see S3 Protection in the *Amazon GuardDuty User Guide*.

Type: String

Valid Values: `FINDING | CLOUD_TRAIL | S3_DATA_EVENTS | EKS_AUDIT_LOGS | FLOW_LOGS | DNS_LOGS | RUNTIME_MONITORING`

Required: Yes

uid

The unique identifier of the signal.

Type: String

Required: Yes

updatedAt

The timestamp when this signal was last observed.

Type: Timestamp

Required: Yes

activities

Contains information about the activities, such as API calls, that were observed for this signal.

Type: Array of Activity objects

Array Members: Minimum number of 0 items. Maximum number of 100 items.

Required: No

actorIds

Information about the IDs of the threat actors involved in the signal.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 400 items.

Required: No

description

The description of the signal.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2000.

Required: No

endpointIds

Information about the endpoint IDs associated with this signal.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 400 items.

Required: No

resourceUids

Information about the unique identifiers of the resources involved in the signal.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 400 items.

Required: No

severity

The severity associated with the signal. For more information about severity, see Findings severity levels in the *Amazon GuardDuty User Guide*.

Type: Double

Required: No

signalIndicators

Contains information about the indicators associated with the signals.

Type: Array of Indicator objects

Array Members: Minimum number of 0 items. Maximum number of 400 items.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SortCriteria

Contains information about the criteria used for sorting findings.

Contents

attributeName

Represents the finding attribute, such as `accountId`, that sorts the findings.

Type: String

Required: No

orderBy

The order by which the sorted findings are to be displayed.

Type: String

Valid Values: `ASC | DESC`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StartMalwareScanConfiguration

Contains information about the configuration to be used for the malware scan.

Contents

role

Amazon Resource Name (ARN) of the IAM role that is used for scanning the resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: Yes

incrementalScanDetails

Contains information about the incremental scan configuration. When specified, the scan will only process changes since the baseline resource.

Type: IncrementalScanDetails object

Required: No

recoveryPoint

Contains information about the recovery point configuration for the requested scan.

Type: RecoveryPoint object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Tag

Contains information about a tag key-value pair.

Contents

key

Describes the key associated with the tag.

Type: String

Required: No

value

Describes the value associated with the tag key.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Threat

Information about the detected threats associated with the generated finding.

Contents

count

The number of occurrences of this specific threat detected during the scan.

Type: Long

Required: No

hash

The hash identifier of the detected malware threat.

Type: String

Required: No

itemDetails

Detailed information about the detected malware threat.

Type: Array of ItemDetails objects

Required: No

itemPaths

Information about the nested item path and hash of the protected resource.

Type: Array of ItemPath objects

Required: No

name

Name of the detected threat that caused GuardDuty to generate this finding.

Type: String

Required: No

source

Source of the threat that generated this finding.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ThreatDetectedByName

Contains details about identified threats organized by threat name.

Contents

itemCount

Total number of infected files identified.

Type: Integer

Required: No

shortened

Flag to determine if the finding contains every single infected file-path and/or every threat.

Type: Boolean

Required: No

threatNames

List of identified threats with details, organized by threat name.

Type: Array of ScanThreatName objects

Required: No

uniqueThreatNameCount

Total number of unique threats by name identified, as part of the malware scan.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

ThreatIntelligenceDetail

An instance of a threat intelligence detail that constitutes evidence for the finding.

Contents

threatFileSha256

SHA256 of the file that generated the finding.

Type: String

Required: No

threatListName

The name of the threat intelligence list that triggered the finding.

Type: String

Required: No

threatNames

A list of names of the threats in the threat intelligence list that triggered the finding.

Type: Array of strings

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ThreatsDetectedItemCount

Contains total number of infected files.

Contents

files

Total number of infected files.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Total

Contains the total usage with the corresponding currency unit for that value.

Contents

amount

The total usage.

Type: String

Required: No

unit

The currency unit that the amount is given in.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

TriggerDetails

Represents the reason the scan was triggered.

Contents

description

The description of the scan trigger.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

guardDutyFindingId

The ID of the GuardDuty finding that triggered the malware scan.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

triggerType

Specifies the trigger type that started the malware scan.

Type: String

Valid Values: `BACKUP | GUARDDUTY`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

UnprocessedAccount

Contains information about the accounts that weren't processed.

Contents

accountId

The AWS account ID.

Type: String

Length Constraints: Fixed length of 12.

Required: Yes

result

A reason why the account hasn't been processed.

Type: String

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

UnprocessedDataSourcesResult

Specifies the names of the data sources that couldn't be enabled.

Contents

malwareProtection

An object that contains information on the status of all Malware Protection data sources.

Type: MalwareProtectionConfigurationResult object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

UpdateProtectedResource

Information about the protected resource that is associated with the created Malware Protection plan. Presently, `S3Bucket` is the only supported protected resource.

Contents

s3Bucket

Information about the protected S3 bucket resource.

Type: UpdateS3BucketResource object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

UpdateS3BucketResource

Information about the protected S3 bucket resource.

Contents

objectPrefixes

Information about the specified object prefixes. The S3 object will be scanned only if it belongs to any of the specified object prefixes.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 5 items.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

UsageAccountResult

Contains information on the total of usage based on account IDs.

Contents

accountId

The Account ID that generated usage.

Type: String

Length Constraints: Fixed length of 12.

Required: No

total

Represents the total of usage for the Account ID.

Type: Total object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

UsageCriteria

Contains information about the criteria used to query usage statistics.

Contents

accountIds

The account IDs to aggregate usage statistics from.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: No

dataSources

This member has been deprecated.

The data sources to aggregate usage statistics from.

Type: Array of strings

Valid Values: `FLOW_LOGS | CLOUD_TRAIL | DNS_LOGS | S3_LOGS | KUBERNETES_AUDIT_LOGS | EC2_MALWARE_SCAN`

Required: No

features

The features to aggregate usage statistics from.

Type: Array of strings

Valid Values: `FLOW_LOGS | CLOUD_TRAIL | DNS_LOGS | S3_DATA_EVENTS | EKS_AUDIT_LOGS | EBS_MALWARE_PROTECTION | RDS_LOGIN_EVENTS | LAMBDA_NETWORK_LOGS | EKS_RUNTIME_MONITORING | EC2_RUNTIME_MONITORING | FARGATE_RUNTIME_MONITORING | RDS_DBI_PROTECTION_PROVISIONED | RDS_DBI_PROTECTION_SERVERLESS | RDS_DBI_PROTECTION_LIMITLESS | RDS_DATA_ACTIVITY_DBI_PROTECTION_PROVISIONED`

```
| RDS_DATA_ACTIVITY_DBI_PROTECTION_SERVERLESS |
RDS_DATA_ACTIVITY_DBI_PROTECTION_LIMITLESS | AI_PROTECTION
```

Required: No

resources

The resources to aggregate usage statistics from. Only accepts exact resource names.

Type: Array of strings

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

UsageDataSourceResult

Contains information on the result of usage based on data source type.

Contents

dataSource

The data source type that generated usage.

Type: String

Valid Values: `FLOW_LOGS | CLOUD_TRAIL | DNS_LOGS | S3_LOGS | KUBERNETES_AUDIT_LOGS | EC2_MALWARE_SCAN`

Required: No

total

Represents the total of usage for the specified data source.

Type: Total object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

UsageFeatureResult

Contains information about the result of the total usage based on the feature.

Contents

feature

The feature that generated the usage cost.

Type: String

Valid Values: `FLOW_LOGS | CLOUD_TRAIL | DNS_LOGS | S3_DATA_EVENTS | EKS_AUDIT_LOGS | EBS_MALWARE_PROTECTION | RDS_LOGIN_EVENTS | LAMBDA_NETWORK_LOGS | EKS_RUNTIME_MONITORING | EC2_RUNTIME_MONITORING | FARGATE_RUNTIME_MONITORING | RDS_DBI_PROTECTION_PROVISIONED | RDS_DBI_PROTECTION_SERVERLESS | RDS_DBI_PROTECTION_LIMITLESS | RDS_DATA_ACTIVITY_DBI_PROTECTION_PROVISIONED | RDS_DATA_ACTIVITY_DBI_PROTECTION_SERVERLESS | RDS_DATA_ACTIVITY_DBI_PROTECTION_LIMITLESS | AI_PROTECTION`

Required: No

total

Contains the total usage with the corresponding currency unit for that value.

Type: Total object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

UsageResourceResult

Contains information on the sum of usage based on an AWS resource.

Contents

resource

The AWS resource that generated usage.

Type: String

Required: No

total

Represents the sum total of usage for the specified resource type.

Type: Total object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

UsageStatistics

Contains the result of GuardDuty usage. If a UsageStatisticType is provided the result for other types will be null.

Contents

sumByAccount

The usage statistic sum organized by account ID.

Type: Array of UsageAccountResult objects

Required: No

sumByDataSource

The usage statistic sum organized by on data source.

Type: Array of UsageDataSourceResult objects

Required: No

sumByFeature

The usage statistic sum organized by feature.

Type: Array of UsageFeatureResult objects

Required: No

sumByResource

The usage statistic sum organized by resource.

Type: Array of UsageResourceResult objects

Required: No

topAccountsByFeature

Lists the top 50 accounts by feature that have generated the most GuardDuty usage, in the order from most to least expensive.

Currently, this doesn't support `RDS_LOGIN_EVENTS`.

Type: Array of UsageTopAccountsResult objects

Required: No

topResources

Lists the top 50 resources that have generated the most GuardDuty usage, in order from most to least expensive.

Type: Array of UsageResourceResult objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

UsageTopAccountResult

Contains information on the total of usage based on the topmost 50 account IDs.

Contents

accountId

The unique account ID.

Type: String

Length Constraints: Fixed length of 12.

Required: No

total

Contains the total usage with the corresponding currency unit for that value.

Type: Total object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

UsageTopAccountsResult

Information about the usage statistics, calculated by top accounts by feature.

Contents

accounts

The accounts that contributed to the total usage cost.

Type: Array of UsageTopAccountResult objects

Required: No

feature

Features by which you can generate the usage statistics.

`RDS_LOGIN_EVENTS` is currently not supported with `topAccountsByFeature`.

Type: String

Valid Values: `FLOW_LOGS | CLOUD_TRAIL | DNS_LOGS | S3_DATA_EVENTS | EKS_AUDIT_LOGS | EBS_MALWARE_PROTECTION | RDS_LOGIN_EVENTS | LAMBDA_NETWORK_LOGS | EKS_RUNTIME_MONITORING | EC2_RUNTIME_MONITORING | FARGATE_RUNTIME_MONITORING | RDS_DBI_PROTECTION_PROVISIONED | RDS_DBI_PROTECTION_SERVERLESS | RDS_DBI_PROTECTION_LIMITLESS | RDS_DATA_ACTIVITY_DBI_PROTECTION_PROVISIONED | RDS_DATA_ACTIVITY_DBI_PROTECTION_SERVERLESS | RDS_DATA_ACTIVITY_DBI_PROTECTION_LIMITLESS | AI_PROTECTION`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

User

Contains information about the user involved in the attack sequence.

Contents

name

The name of the user.

Type: String

Required: Yes

type

The type of the user.

Type: String

Required: Yes

uid

The unique identifier of the user.

Type: String

Required: Yes

account

Contains information about the AWS account within which the activity took place. This is not necessarily the account that owns the user identity.

Type: Account object

Required: No

credentialUid

The credentials of the user ID.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Volume

Volume used by the Kubernetes workload.

Contents

hostPath

Represents a pre-existing file or directory on the host machine that the volume maps to.

Type: HostPath object

Required: No

name

Volume name.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

VolumeDetail

Contains EBS volume details.

Contents

deviceName

The device name for the EBS volume.

Type: String

Required: No

encryptionType

EBS volume encryption type.

Type: String

Required: No

kmsKeyArn

KMS key ARN used to encrypt the EBS volume.

Type: String

Required: No

snapshotArn

Snapshot ARN of the EBS volume.

Type: String

Required: No

volumeArn

EBS volume ARN information.

Type: String

Required: No

volumeSizeInGB

EBS volume size in GB.

Type: Integer

Required: No

volumeType

The EBS volume type.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

VolumeMount

Container volume mount.

Contents

mountPath

Volume mount path.

Type: String

Required: No

name

Volume mount name.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

VpcConfig

Amazon Virtual Private Cloud configuration details associated with your Lambda function.

Contents

securityGroups

The identifier of the security group attached to the Lambda function.

Type: Array of SecurityGroup objects

Required: No

subnetIds

The identifiers of the subnets that are associated with your Lambda function.

Type: Array of strings

Required: No

vpcId

The identifier of the Amazon Virtual Private Cloud.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see Signing AWS API requests in the *IAM User Guide*.

X-Amz-Algorithm

The hash algorithm that you used to create the request signature.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: *access_key*/*YYYYMMDD*/*region*/*service*/aws4_request.

For more information, see Create a signed AWS API request in the *IAM User Guide*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-Date

The date that is used to create the signature. The format must be ISO 8601 basic format (YYYYMMDD'T'HHMMSS'Z'). For example, the following date time is a valid X-Amz-Date value: `20120325T120000Z`.

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Elements of an AWS API request signature in the *IAM User Guide*.

Type: string

Required: Conditional

X-Amz-Security-Token

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS STS, see AWS services that work with IAM in the *IAM User Guide*.

Condition: If you're using temporary security credentials from AWS STS, you must include the security token.

Type: string

Required: Conditional

X-Amz-Signature

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-SignedHeaders

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see Create a signed AWS API request in the *IAM User Guide*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

Common Error Types

This section lists common error types that this AWS service may return. Not all services return all error types listed here. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You don't have permission to perform this action. Verify that your IAM policy includes the required permissions.

HTTP Status Code: 403

ExpiredTokenException

The security token included in the request has expired. Request a new security token and try again.

HTTP Status Code: 403

IncompleteSignature

The request signature doesn't conform to AWS standards. Verify that you're using valid AWS credentials and that your request is properly formatted. If you're using an SDK, ensure it's up to date.

HTTP Status Code: 403

InternalFailure

The request can't be processed right now because of an internal server issue. Try again later. If the problem persists, contact AWS Support.

HTTP Status Code: 500

MalformedHttpRequestException

The request body can't be processed. This typically happens when the request body can't be decompressed using the specified content encoding algorithm. Verify that the content encoding header matches the compression format used.

HTTP Status Code: 400

NotAuthorized

You don't have permissions to perform this action. Verify that your IAM policy includes the required permissions.

HTTP Status Code: 401

OptInRequired

Your AWS account needs a subscription for this service. Verify that you've enabled the service in your account.

HTTP Status Code: 403

RequestAbortedException

The request was aborted before a response could be returned. This typically happens when the client closes the connection.

HTTP Status Code: 400

RequestEntityTooLargeException

The request entity is too large. Reduce the size of the request body and try again.

HTTP Status Code: 413

RequestTimeoutException

The request timed out. The server didn't receive the complete request within the expected time frame. Try again.

HTTP Status Code: 408

ServiceUnavailable

The service is temporarily unavailable. Try again later.

HTTP Status Code: 503

ThrottlingException

Your request rate is too high. The AWS SDKs automatically retry requests that receive this exception. Reduce the frequency of requests.

HTTP Status Code: 400

UnknownOperationException

The action or operation isn't recognized. Verify that the action name is spelled correctly and that it's supported by the API version you're using.

HTTP Status Code: 404

UnrecognizedClientException

The X.509 certificate or AWS access key ID you provided doesn't exist in our records. Verify that you're using valid credentials and that they haven't expired.

HTTP Status Code: 403

ValidationError

The input doesn't meet the required format or constraints. Check that all required parameters are included and that values are valid.

HTTP Status Code: 400