



API Reference

AWS Security Agent



API Version 2025-09-06

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

AWS Security Agent: 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
AddArtifact	4
Request Syntax	4
URI Request Parameters	4
Request Body	4
Response Syntax	5
Response Elements	5
Errors	5
See Also	6
BatchDeletePentests	8
Request Syntax	8
URI Request Parameters	8
Request Body	8
Response Syntax	8
Response Elements	10
Errors	11
See Also	11
BatchGetAgentSpaces	12
Request Syntax	12
URI Request Parameters	12
Request Body	12
Response Syntax	12
Response Elements	13
Errors	14
See Also	14
BatchGetArtifactMetadata	15
Request Syntax	15
URI Request Parameters	15
Request Body	15
Response Syntax	15
Response Elements	16
Errors	16
See Also	17

BatchGetFindings	18
Request Syntax	18
URI Request Parameters	18
Request Body	18
Response Syntax	18
Response Elements	19
Errors	20
See Also	20
BatchGetPentestJobs	21
Request Syntax	21
URI Request Parameters	21
Request Body	21
Response Syntax	21
Response Elements	24
Errors	24
See Also	24
BatchGetPentestJobTasks	26
Request Syntax	26
URI Request Parameters	26
Request Body	26
Response Syntax	26
Response Elements	27
Errors	28
See Also	28
BatchGetPentests	29
Request Syntax	29
URI Request Parameters	29
Request Body	29
Response Syntax	29
Response Elements	31
Errors	32
See Also	32
BatchGetTargetDomains	33
Request Syntax	33
URI Request Parameters	33
Request Body	33

Response Syntax	33
Response Elements	34
Errors	34
See Also	35
CreateAgentSpace	36
Request Syntax	36
URI Request Parameters	36
Request Body	37
Response Syntax	38
Response Elements	39
Errors	40
See Also	40
CreateApplication	41
Request Syntax	41
URI Request Parameters	41
Request Body	41
Response Syntax	42
Response Elements	42
Errors	42
See Also	43
CreateIntegration	44
Request Syntax	44
URI Request Parameters	44
Request Body	44
Response Syntax	45
Response Elements	45
Errors	46
See Also	47
CreateMembership	48
Request Syntax	48
URI Request Parameters	48
Request Body	48
Response Syntax	49
Response Elements	49
Errors	49
See Also	49

CreatePentest	51
Request Syntax	51
URI Request Parameters	52
Request Body	52
Response Syntax	54
Response Elements	56
Errors	57
See Also	57
CreateTargetDomain	59
Request Syntax	59
URI Request Parameters	59
Request Body	59
Response Syntax	60
Response Elements	60
Errors	61
See Also	61
DeleteAgentSpace	63
Request Syntax	63
URI Request Parameters	63
Request Body	63
Response Syntax	63
Response Elements	64
Errors	64
See Also	64
DeleteApplication	65
Request Syntax	65
URI Request Parameters	65
Request Body	65
Response Syntax	65
Response Elements	65
Errors	65
See Also	66
DeleteArtifact	67
Request Syntax	67
URI Request Parameters	67
Request Body	67

Response Syntax	67
Response Elements	68
Errors	68
See Also	68
DeleteIntegration	70
Request Syntax	70
URI Request Parameters	70
Request Body	70
Response Syntax	70
Response Elements	70
Errors	70
See Also	71
DeleteMembership	73
Request Syntax	73
URI Request Parameters	73
Request Body	73
Response Syntax	74
Response Elements	74
Errors	74
See Also	74
DeleteTargetDomain	76
Request Syntax	76
URI Request Parameters	76
Request Body	76
Response Syntax	76
Response Elements	77
Errors	77
See Also	77
GetApplication	78
Request Syntax	78
URI Request Parameters	78
Request Body	78
Response Syntax	78
Response Elements	79
Errors	80
See Also	80

GetArtifact	81
Request Syntax	81
URI Request Parameters	81
Request Body	81
Response Syntax	81
Response Elements	82
Errors	83
See Also	83
GetIntegration	85
Request Syntax	85
URI Request Parameters	85
Request Body	85
Response Syntax	85
Response Elements	86
Errors	87
See Also	87
InitiateProviderRegistration	89
Request Syntax	89
URI Request Parameters	89
Request Body	89
Response Syntax	89
Response Elements	90
Errors	90
See Also	91
ListAgentSpaces	92
Request Syntax	92
URI Request Parameters	92
Request Body	92
Response Syntax	93
Response Elements	93
Errors	93
See Also	94
ListApplications	95
Request Syntax	95
URI Request Parameters	95
Request Body	95

Response Syntax	96
Response Elements	96
Errors	96
See Also	97
ListArtifacts	98
Request Syntax	98
URI Request Parameters	98
Request Body	98
Response Syntax	99
Response Elements	99
Errors	100
See Also	100
ListDiscoveredEndpoints	102
Request Syntax	102
URI Request Parameters	102
Request Body	102
Response Syntax	103
Response Elements	104
Errors	104
See Also	104
ListFindings	106
Request Syntax	106
URI Request Parameters	106
Request Body	106
Response Syntax	108
Response Elements	109
Errors	109
See Also	109
ListIntegratedResources	111
Request Syntax	111
URI Request Parameters	111
Request Body	111
Response Syntax	112
Response Elements	113
Errors	113
See Also	114

ListIntegrations	115
Request Syntax	115
URI Request Parameters	115
Request Body	115
Response Syntax	116
Response Elements	116
Errors	117
See Also	118
ListMemberships	119
Request Syntax	119
URI Request Parameters	119
Request Body	119
Response Syntax	120
Response Elements	121
Errors	121
See Also	121
ListPentestJobsForPentest	123
Request Syntax	123
URI Request Parameters	123
Request Body	123
Response Syntax	124
Response Elements	124
Errors	125
See Also	125
ListPentestJobTasks	126
Request Syntax	126
URI Request Parameters	126
Request Body	126
Response Syntax	127
Response Elements	128
Errors	128
See Also	128
ListPentests	130
Request Syntax	130
URI Request Parameters	130
Request Body	130

Response Syntax	131
Response Elements	131
Errors	132
See Also	132
ListTagsForResource	133
Request Syntax	133
URI Request Parameters	133
Request Body	133
Response Syntax	133
Response Elements	133
Errors	134
See Also	134
ListTargetDomains	135
Request Syntax	135
URI Request Parameters	135
Request Body	135
Response Syntax	136
Response Elements	136
Errors	136
See Also	137
StartCodeRemediation	138
Request Syntax	138
URI Request Parameters	138
Request Body	138
Response Syntax	139
Response Elements	139
Errors	139
See Also	139
StartPentestJob	140
Request Syntax	140
URI Request Parameters	140
Request Body	140
Response Syntax	140
Response Elements	141
Errors	142
See Also	142

StopPentestJob	143
Request Syntax	143
URI Request Parameters	143
Request Body	143
Response Syntax	143
Response Elements	144
Errors	144
See Also	144
TagResource	145
Request Syntax	145
URI Request Parameters	145
Request Body	145
Response Syntax	145
Response Elements	146
Errors	146
See Also	146
UntagResource	147
Request Syntax	147
URI Request Parameters	147
Request Body	147
Response Syntax	147
Response Elements	147
Errors	147
See Also	148
UpdateAgentSpace	149
Request Syntax	149
URI Request Parameters	149
Request Body	149
Response Syntax	151
Response Elements	151
Errors	152
See Also	153
UpdateApplication	154
Request Syntax	154
URI Request Parameters	154
Request Body	154

Response Syntax	155
Response Elements	155
Errors	155
See Also	155
UpdateFinding	157
Request Syntax	157
URI Request Parameters	157
Request Body	157
Response Syntax	158
Response Elements	158
Errors	158
See Also	158
UpdateIntegratedResources	160
Request Syntax	160
URI Request Parameters	160
Request Body	160
Response Syntax	161
Response Elements	161
Errors	161
See Also	162
UpdatePentest	163
Request Syntax	163
URI Request Parameters	164
Request Body	164
Response Syntax	167
Response Elements	168
Errors	169
See Also	170
UpdateTargetDomain	171
Request Syntax	171
URI Request Parameters	171
Request Body	171
Response Syntax	171
Response Elements	172
Errors	173
See Also	173

VerifyTargetDomain	175
Request Syntax	175
URI Request Parameters	175
Request Body	175
Response Syntax	175
Response Elements	176
Errors	177
See Also	177
Data Types	178
Actor	181
Contents	181
See Also	181
AgentSpace	183
Contents	183
See Also	184
AgentSpaceSummary	185
Contents	185
See Also	185
ApplicationSummary	187
Contents	187
See Also	187
Artifact	189
Contents	189
See Also	189
ArtifactMetadataItem	190
Contents	190
See Also	190
ArtifactSummary	192
Contents	192
See Also	192
Assets	193
Contents	193
See Also	194
Authentication	195
Contents	195
See Also	195

AWSResources	196
Contents	196
See Also	197
Category	198
Contents	198
See Also	198
CloudWatchLog	199
Contents	199
See Also	199
CodeRemediationTask	200
Contents	200
See Also	200
CodeRemediationTaskDetails	202
Contents	202
See Also	202
CodeReviewSettings	203
Contents	203
See Also	203
CustomHeader	204
Contents	204
See Also	204
DeletePentestFailure	205
Contents	205
See Also	205
DiscoveredEndpoint	206
Contents	206
See Also	207
DnsVerification	208
Contents	208
See Also	208
DocumentInfo	210
Contents	210
See Also	210
Endpoint	211
Contents	211
See Also	211

ErrorInformation	212
Contents	212
See Also	212
ExecutionContext	213
Contents	213
See Also	213
Finding	215
Contents	215
See Also	218
FindingSummary	219
Contents	219
See Also	221
GitHubIntegrationInput	222
Contents	222
See Also	222
GitHubRepositoryMetadata	223
Contents	223
See Also	223
GitHubRepositoryResource	225
Contents	225
See Also	225
GitHubResourceCapabilities	226
Contents	226
See Also	226
HttpVerification	227
Contents	227
See Also	227
IdCConfiguration	228
Contents	228
See Also	228
IntegratedRepository	229
Contents	229
See Also	229
IntegratedResource	230
Contents	230
See Also	230

IntegratedResourceInputItem	231
Contents	231
See Also	231
IntegratedResourceMetadata	232
Contents	232
See Also	232
IntegratedResourceSummary	233
Contents	233
See Also	233
IntegrationFilter	235
Contents	235
See Also	235
IntegrationSummary	237
Contents	237
See Also	238
LogLocation	239
Contents	239
See Also	239
MemberMetadata	240
Contents	240
See Also	240
MembershipConfig	241
Contents	241
See Also	241
MembershipSummary	242
Contents	242
See Also	244
NetworkTrafficConfig	245
Contents	245
See Also	245
NetworkTrafficRule	246
Contents	246
See Also	246
Pentest	248
Contents	248
See Also	250

PentestJob	251
Contents	251
See Also	255
PentestJobSummary	256
Contents	256
See Also	257
PentestSummary	258
Contents	258
See Also	259
ProviderInput	260
Contents	260
See Also	260
ProviderResourceCapabilities	261
Contents	261
See Also	261
SourceCodeRepository	262
Contents	262
See Also	262
Step	263
Contents	263
See Also	264
TargetDomain	265
Contents	265
See Also	266
TargetDomainSummary	267
Contents	267
See Also	267
Task	268
Contents	268
See Also	270
TaskSummary	271
Contents	271
See Also	273
UserConfig	274
Contents	274
See Also	274

UserMetadata	275
Contents	275
See Also	275
ValidationExceptionField	276
Contents	276
See Also	276
VerificationDetails	277
Contents	277
See Also	277
VpcConfig	279
Contents	279
See Also	279
Common Parameters	280
Common Error Types	283

Welcome

AWS Security Agent is a frontier agent that proactively secures your applications throughout the development lifecycle. It conducts automated security reviews tailored to your organizational requirements and delivers context-aware penetration testing on demand. By continuously validating security from design to deployment, AWS Security Agent helps prevent vulnerabilities early across all your environments. Key capabilities include design security review for architecture documents, code security review for pull requests in connected repositories, and on-demand penetration testing that discovers, validates, and remediates security vulnerabilities through tailored multi-step attack scenarios. For more information, see the [AWS Security Agent User Guide](#).

This document was last published on April 5, 2026.

Actions

The following actions are supported:

- [AddArtifact](#)
- [BatchDeletePentests](#)
- [BatchGetAgentSpaces](#)
- [BatchGetArtifactMetadata](#)
- [BatchGetFindings](#)
- [BatchGetPentestJobs](#)
- [BatchGetPentestJobTasks](#)
- [BatchGetPentests](#)
- [BatchGetTargetDomains](#)
- [CreateAgentSpace](#)
- [CreateApplication](#)
- [CreateIntegration](#)
- [CreateMembership](#)
- [CreatePentest](#)
- [CreateTargetDomain](#)
- [DeleteAgentSpace](#)
- [DeleteApplication](#)
- [DeleteArtifact](#)
- [DeleteIntegration](#)
- [DeleteMembership](#)
- [DeleteTargetDomain](#)
- [GetApplication](#)
- [GetArtifact](#)
- [GetIntegration](#)
- [InitiateProviderRegistration](#)
- [ListAgentSpaces](#)
- [ListApplications](#)

- [ListArtifacts](#)
- [ListDiscoveredEndpoints](#)
- [ListFindings](#)
- [ListIntegratedResources](#)
- [ListIntegrations](#)
- [ListMemberships](#)
- [ListPentestJobsForPentest](#)
- [ListPentestJobTasks](#)
- [ListPentests](#)
- [ListTagsForResource](#)
- [ListTargetDomains](#)
- [StartCodeRemediation](#)
- [StartPentestJob](#)
- [StopPentestJob](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateAgentSpace](#)
- [UpdateApplication](#)
- [UpdateFinding](#)
- [UpdateIntegratedResources](#)
- [UpdatePentest](#)
- [UpdateTargetDomain](#)
- [VerifyTargetDomain](#)

AddArtifact

Uploads an artifact to an agent space. Artifacts provide additional context for security testing, such as architecture diagrams, API specifications, or configuration files.

Request Syntax

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

{
  "agentSpaceId": "string",
  "artifactContent": blob,
  "artifactType": "string",
  "fileName": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space to add the artifact to.

Type: String

Required: Yes

artifactContent

The binary content of the artifact to upload.

Type: Base64-encoded binary data object

Required: Yes

artifactType

The file type of the artifact. Valid values include TXT, PNG, JPEG, MD, PDF, DOCX, DOC, JSON, and YAML.

Type: String

Valid Values: TXT | PNG | JPEG | MD | PDF | DOCX | DOC | JSON | YAML

Required: Yes

fileName

The file name of the artifact.

Type: String

Required: Yes

Response Syntax

```
HTTP/1.1 201
Content-type: application/json

{
  "artifactId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

artifactId

The unique identifier assigned to the uploaded artifact.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

An unexpected error occurred during the processing of your request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource was not found. Verify that the resource identifier is correct and that the resource exists in the specified agent space or account.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The input fails to satisfy the constraints specified by the service.

HTTP Status Code: 400

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](#)
- [AWS SDK for Ruby V3](#)

BatchDeletePentests

Deletes one or more pentests from an agent space.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "pentestIds": [ "string" ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space that contains the pentests to delete.

Type: String

Required: Yes

pentestIds

The list of pentest identifiers to delete.

Type: Array of strings

Required: Yes

Response Syntax

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

```
{
  "deleted": [
    {
      "agentSpaceId": "string",
      "assets": {
        "actors": [
          {
            "authentication": {
              "providerType": "string",
              "value": "string"
            },
            "description": "string",
            "identifier": "string",
            "uris": [ "string " ]
          }
        ],
        "documents": [
          {
            "artifactId": "string",
            "s3Location": "string"
          }
        ],
        "endpoints": [
          {
            "uri": "string"
          }
        ],
        "integratedRepositories": [
          {
            "integrationId": "string",
            "providerResourceId": "string"
          }
        ],
        "sourceCode": [
          {
            "s3Location": "string"
          }
        ]
      },
      "codeRemediationStrategy": "string",
      "createdAt": "string",
      "excludeRiskTypes": [ "string " ],
      "logConfig": {
```

```
    "logGroup": "string",
    "logStream": "string"
  },
  "networkTrafficConfig": {
    "customHeaders": [
      {
        "name": "string",
        "value": "string"
      }
    ],
    "rules": [
      {
        "effect": "string",
        "networkTrafficRuleType": "string",
        "pattern": "string"
      }
    ]
  },
  "pentestId": "string",
  "serviceRole": "string",
  "title": "string",
  "updatedAt": "string",
  "vpcConfig": {
    "securityGroupArns": [ "string" ],
    "subnetArns": [ "string" ],
    "vpcArn": "string"
  }
},
"failed": [
  {
    "pentestId": "string",
    "reason": "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.

deleted

The list of pentests that were successfully deleted.

Type: Array of [Pentest](#) objects

failed

The list of pentests that failed to delete, including the reason for each failure.

Type: Array of [DeletePentestFailure](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

BatchGetAgentSpaces

Retrieves information about one or more agent spaces.

Request Syntax

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

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

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceIds

The list of agent space identifiers to retrieve.

Type: Array of strings

Required: Yes

Response Syntax

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

```
{
  "agentSpaces": [
    {
      "agentSpaceId": "string",
      "awsResources": {
        "iamRoles": [ "string" ],

```

```
    "lambdaFunctionArns": [ "string" ],
    "logGroups": [ "string" ],
    "s3Buckets": [ "string" ],
    "secretArns": [ "string" ],
    "vpcs": [
      {
        "securityGroupArns": [ "string" ],
        "subnetArns": [ "string" ],
        "vpcArn": "string"
      }
    ],
  },
  "codeReviewSettings": {
    "controlsScanning": boolean,
    "generalPurposeScanning": boolean
  },
  "createdAt": "string",
  "description": "string",
  "kmsKeyId": "string",
  "name": "string",
  "targetDomainIds": [ "string" ],
  "updatedAt": "string"
}
],
"notFound": [ "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.

agentSpaces

The list of agent spaces that were found.

Type: Array of [AgentSpace](#) objects

notFound

The list of agent space identifiers that were not found.

Type: Array of strings

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

BatchGetArtifactMetadata

Retrieves metadata for one or more artifacts in an agent space.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "artifactIds": [ "string" ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space that contains the artifacts.

Type: String

Required: Yes

artifactIds

The list of artifact identifiers to retrieve metadata for.

Type: Array of strings

Required: Yes

Response Syntax

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

```
{
  "artifactMetadataList": [
    {
      "agentSpaceId": "string",
      "artifactId": "string",
      "fileName": "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.

artifactMetadataList

The list of artifact metadata items that were found.

Type: Array of [ArtifactMetadataItem](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

An unexpected error occurred during the processing of your request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource was not found. Verify that the resource identifier is correct and that the resource exists in the specified agent space or account.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The input fails to satisfy the constraints specified by the service.

HTTP Status Code: 400

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](#)
- [AWS SDK for Ruby V3](#)

BatchGetFindings

Retrieves information about one or more security findings in an agent space.

Request Syntax

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

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

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space that contains the findings.

Type: String

Required: Yes

findingIds

The list of finding identifiers to retrieve.

Type: Array of strings

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Content-type: application/json

```
{
  "findings": [
    {
      "agentSpaceId": "string",
      "attackScript": "string",
      "codeRemediationTask": {
        "status": "string",
        "statusReason": "string",
        "taskDetails": [
          {
            "codeDiffLink": "string",
            "pullRequestLink": "string",
            "repoName": "string"
          }
        ]
      },
      "confidence": "string",
      "createdAt": "string",
      "description": "string",
      "findingId": "string",
      "lastUpdatedBy": "string",
      "name": "string",
      "pentestId": "string",
      "pentestJobId": "string",
      "reasoning": "string",
      "riskLevel": "string",
      "riskScore": "string",
      "riskType": "string",
      "status": "string",
      "taskId": "string",
      "updatedAt": "string"
    }
  ],
  "notFound": [ "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

The list of findings that were found.

Type: Array of [Finding](#) objects

notFound

The list of finding identifiers that were not found.

Type: Array of strings

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

BatchGetPentestJobs

Retrieves information about one or more pentest jobs in an agent space.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "pentestJobIds": [ "string" ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space that contains the pentest jobs.

Type: String

Required: Yes

pentestJobIds

The list of pentest job identifiers to retrieve.

Type: Array of strings

Required: Yes

Response Syntax

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

```
{
  "notFound": [ "string" ],
  "pentestJobs": [
    {
      "actors": [
        {
          "authentication": {
            "providerType": "string",
            "value": "string"
          },
          "description": "string",
          "identifier": "string",
          "uris": [ "string" ]
        }
      ],
      "allowedDomains": [
        {
          "uri": "string"
        }
      ],
      "codeRemediationStrategy": "string",
      "createdAt": "string",
      "documents": [
        {
          "artifactId": "string",
          "s3Location": "string"
        }
      ],
      "endpoints": [
        {
          "uri": "string"
        }
      ],
      "errorInformation": {
        "code": "string",
        "message": "string"
      },
      "excludePaths": [
        {
          "uri": "string"
        }
      ],
      "excludeRiskTypes": [ "string" ],

```

```
"executionContext": [
  {
    "context": "string",
    "contextType": "string",
    "timestamp": "string"
  }
],
"integratedRepositories": [
  {
    "integrationId": "string",
    "providerResourceId": "string"
  }
],
"logConfig": {
  "logGroup": "string",
  "logStream": "string"
},
"networkTrafficConfig": {
  "customHeaders": [
    {
      "name": "string",
      "value": "string"
    }
  ],
  "rules": [
    {
      "effect": "string",
      "networkTrafficRuleType": "string",
      "pattern": "string"
    }
  ]
},
"overview": "string",
"pentestId": "string",
"pentestJobId": "string",
"serviceRole": "string",
"sourceCode": [
  {
    "s3Location": "string"
  }
],
"status": "string",
"steps": [
  {
```

```
        "createdAt": "string",
        "name": "string",
        "status": "string",
        "updatedAt": "string"
    }
],
"title": "string",
"updatedAt": "string",
"vpcConfig": {
    "securityGroupArns": [ "string" ],
    "subnetArns": [ "string" ],
    "vpcArn": "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.

notFound

The list of pentest job identifiers that were not found.

Type: Array of strings

pentestJobs

The list of pentest jobs that were found.

Type: Array of [PentestJob](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

BatchGetPentestJobTasks

Retrieves information about one or more tasks within a pentest job.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "taskIds": [ "string" ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space that contains the tasks.

Type: String

Required: Yes

taskIds

The list of task identifiers to retrieve.

Type: Array of strings

Required: Yes

Response Syntax

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

```
{
  "notFound": [ "string" ],
  "tasks": [
    {
      "agentSpaceId": "string",
      "categories": [
        {
          "isPrimary": boolean,
          "name": "string"
        }
      ],
      "createdAt": "string",
      "description": "string",
      "executionStatus": "string",
      "logsLocation": {
        "cloudWatchLog": {
          "logGroup": "string",
          "logStream": "string"
        },
        "logType": "string"
      },
      "pentestId": "string",
      "pentestJobId": "string",
      "riskType": "string",
      "targetEndpoint": {
        "uri": "string"
      },
      "taskId": "string",
      "title": "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.

notFound

The list of task identifiers that were not found.

Type: Array of strings

tasks

The list of tasks that were found.

Type: Array of [Task](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

BatchGetPentests

Retrieves information about one or more pentests in an agent space.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "pentestIds": [ "string" ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

[agentSpaceId](#)

The unique identifier of the agent space that contains the pentests.

Type: String

Required: Yes

[pentestIds](#)

The list of pentest identifiers to retrieve.

Type: Array of strings

Required: Yes

Response Syntax

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

```
{
  "notFound": [ "string" ],
  "pentests": [
    {
      "agentSpaceId": "string",
      "assets": {
        "actors": [
          {
            "authentication": {
              "providerType": "string",
              "value": "string"
            },
            "description": "string",
            "identifier": "string",
            "uris": [ "string" ]
          }
        ],
        "documents": [
          {
            "artifactId": "string",
            "s3Location": "string"
          }
        ],
        "endpoints": [
          {
            "uri": "string"
          }
        ],
        "integratedRepositories": [
          {
            "integrationId": "string",
            "providerResourceId": "string"
          }
        ],
        "sourceCode": [
          {
            "s3Location": "string"
          }
        ]
      },
      "codeRemediationStrategy": "string",
      "createdAt": "string",
      "excludeRiskTypes": [ "string" ],

```

```
"logConfig": {
  "logGroup": "string",
  "logStream": "string"
},
"networkTrafficConfig": {
  "customHeaders": [
    {
      "name": "string",
      "value": "string"
    }
  ],
  "rules": [
    {
      "effect": "string",
      "networkTrafficRuleType": "string",
      "pattern": "string"
    }
  ]
},
"pentestId": "string",
"serviceRole": "string",
"title": "string",
"updatedAt": "string",
"vpcConfig": {
  "securityGroupArns": [ "string" ],
  "subnetArns": [ "string" ],
  "vpcArn": "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.

notFound

The list of pentest identifiers that were not found.

Type: Array of strings

[pentests](#)

The list of pentests that were found.

Type: Array of [Pentest](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

BatchGetTargetDomains

Retrieves information about one or more target domains.

Request Syntax

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

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

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

targetDomainIds

The list of target domain identifiers to retrieve.

Type: Array of strings

Required: Yes

Response Syntax

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

{
  "notFound": [ "string" ],
  "targetDomains": [
    {
      "createdAt": "string",
```

```
    "domainName": "string",
    "targetDomainId": "string",
    "verificationDetails": {
      "dnsTxt": {
        "dnsRecordName": "string",
        "dnsRecordType": "string",
        "token": "string"
      },
      "httpRoute": {
        "routePath": "string",
        "token": "string"
      },
      "method": "string"
    },
    "verificationStatus": "string",
    "verifiedAt": "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.

notFound

The list of target domain identifiers that were not found.

Type: Array of strings

targetDomains

The list of target domains that were found.

Type: Array of [TargetDomain](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

CreateAgentSpace

Creates a new agent space. An agent space is a dedicated workspace for securing a specific application.

Request Syntax

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

{
  "awsResources": {
    "iamRoles": [ "string" ],
    "lambdaFunctionArns": [ "string" ],
    "logGroups": [ "string" ],
    "s3Buckets": [ "string" ],
    "secretArns": [ "string" ],
    "vpcs": [
      {
        "securityGroupArns": [ "string" ],
        "subnetArns": [ "string" ],
        "vpcArn": "string"
      }
    ]
  },
  "codeReviewSettings": {
    "controlsScanning": boolean,
    "generalPurposeScanning": boolean
  },
  "description": "string",
  "kmsKeyId": "string",
  "name": "string",
  "tags": {
    "string" : "string"
  },
  "targetDomainIds": [ "string" ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

awsResources

The AWS resources to associate with the agent space.

Type: [AWSResources](#) object

Required: No

codeReviewSettings

The code review settings for the agent space.

Type: [CodeReviewSettings](#) object

Required: No

description

A description of the agent space.

Type: String

Required: No

kmsKeyId

The identifier of the AWS KMS key to use for encrypting data in the agent space.

Type: String

Required: No

name

The name of the agent space.

Type: String

Required: Yes

tags

The tags to associate with the agent space.

Type: String to string map

Required: No

targetDomainIds

The list of target domain identifiers to associate with the agent space.

Type: Array of strings

Required: No

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json
```

```
{
  "agentSpaceId": "string",
  "awsResources": {
    "iamRoles": [ "string" ],
    "lambdaFunctionArns": [ "string" ],
    "logGroups": [ "string" ],
    "s3Buckets": [ "string" ],
    "secretArns": [ "string" ],
    "vpcs": [
      {
        "securityGroupArns": [ "string" ],
        "subnetArns": [ "string" ],
        "vpcArn": "string"
      }
    ]
  },
  "codeReviewSettings": {
    "controlsScanning": boolean,
    "generalPurposeScanning": boolean
  },
  "createdAt": "string",
  "description": "string",
  "kmsKeyId": "string",
  "name": "string",
  "targetDomainIds": [ "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.

[agentSpaceId](#)

The unique identifier of the created agent space.

Type: String

[awsResources](#)

The AWS resources associated with the agent space.

Type: [AWSResources](#) object

[codeReviewSettings](#)

The code review settings for the agent space.

Type: [CodeReviewSettings](#) object

[createdAt](#)

The date and time the agent space was created, in UTC format.

Type: Timestamp

[description](#)

The description of the agent space.

Type: String

[kmsKeyId](#)

The identifier of the AWS KMS key used to encrypt data in the agent space.

Type: String

[name](#)

The name of the agent space.

Type: String

targetDomainIds

The list of target domain identifiers associated with the agent space.

Type: Array of strings

updatedAt

The date and time the agent space was last updated, in UTC format.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

CreateApplication

Creates a new application. An application is the top-level organizational unit that supports IAM Identity Center integration.

Request Syntax

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

```
{
  "defaultKmsKeyId": "string",
  "idcInstanceArn": "string",
  "roleArn": "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.

defaultKmsKeyId

The identifier of the default AWS KMS key to use for encrypting data in the application.

Type: String

Required: No

idcInstanceArn

The Amazon Resource Name (ARN) of the IAM Identity Center instance to associate with the application.

Type: String

Required: No

[roleArn](#)

The Amazon Resource Name (ARN) of the IAM role to associate with the application.

Type: String

Required: No

[tags](#)

The tags to associate with the application.

Type: String to string map

Required: No

Response Syntax

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

{
  "applicationId": "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.

[applicationId](#)

The unique identifier of the created application.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

CreateIntegration

Creates a new integration with a third-party provider, such as GitHub, for code review and remediation.

Request Syntax

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

{
  "input": { ... },
  "integrationDisplayName": "string",
  "kmsKeyId": "string",
  "provider": "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.

input

The provider-specific input required to create the integration.

Type: [ProviderInput](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

integrationDisplayName

The display name for the integration.

Type: String

Required: Yes

kmsKeyId

The identifier of the AWS KMS key to use for encrypting data associated with the integration.

Type: String

Required: No

provider

The integration provider. Currently, only GITHUB is supported.

Type: String

Valid Values: GITHUB

Required: Yes

tags

The tags to associate with the integration.

Type: String to string map

Required: No

Response Syntax

```
HTTP/1.1 201
Content-type: application/json

{
  "integrationId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

integrationId

The unique identifier of the created integration.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ConflictException

The request could not be completed due to a conflict with the current state of the resource.

HTTP Status Code: 409

InternalServerErrorException

An unexpected error occurred during the processing of your request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource was not found. Verify that the resource identifier is correct and that the resource exists in the specified agent space or account.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The input fails to satisfy the constraints specified by the service.

HTTP Status Code: 400

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](#)
- [AWS SDK for Ruby V3](#)

CreateMembership

Creates a new membership, granting a user access to an agent space within an application.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "applicationId": "string",
  "config": { ... },
  "membershipId": "string",
  "memberType": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space to grant access to.

Type: String

Required: Yes

applicationId

The unique identifier of the application that contains the agent space.

Type: String

Required: Yes

config

The configuration for the membership, such as the user role.

Type: [MembershipConfig](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: No

[membershipId](#)

The unique identifier for the membership.

Type: String

Required: Yes

[memberType](#)

The type of member. Currently, only USER is supported.

Type: String

Valid Values: USER

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](#).

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](#)
- [AWS SDK for Ruby V3](#)

CreatePentest

Creates a new pentest configuration in an agent space. A pentest defines the security test parameters, including target assets, risk type exclusions, and logging configuration.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "assets": {
    "actors": [
      {
        "authentication": {
          "providerType": "string",
          "value": "string"
        },
        "description": "string",
        "identifier": "string",
        "uris": [ "string" ]
      }
    ],
    "documents": [
      {
        "artifactId": "string",
        "s3Location": "string"
      }
    ],
    "endpoints": [
      {
        "uri": "string"
      }
    ],
    "integratedRepositories": [
      {
        "integrationId": "string",
        "providerResourceId": "string"
      }
    ],
    "sourceCode": [
      {
```

```
        "s3Location": "string"
      }
    ]
  },
  "codeRemediationStrategy": "string",
  "excludeRiskTypes": [ "string" ],
  "logConfig": {
    "logGroup": "string",
    "logStream": "string"
  },
  "networkTrafficConfig": {
    "customHeaders": [
      {
        "name": "string",
        "value": "string"
      }
    ],
    "rules": [
      {
        "effect": "string",
        "networkTrafficRuleType": "string",
        "pattern": "string"
      }
    ]
  },
  "serviceRole": "string",
  "title": "string",
  "vpcConfig": {
    "securityGroupArns": [ "string" ],
    "subnetArns": [ "string" ],
    "vpcArn": "string"
  }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space to create the pentest in.

Type: String

Required: Yes

assets

The assets to include in the pentest, such as endpoints, actors, documents, and source code.

Type: [Assets](#) object

Required: No

codeRemediationStrategy

The code remediation strategy for the pentest. Valid values are AUTOMATIC and DISABLED.

Type: String

Valid Values: AUTOMATIC | DISABLED

Required: No

excludeRiskTypes

The list of risk types to exclude from the pentest.

Type: Array of strings

Valid Values: CROSS_SITE_SCRIPTING | DEFAULT_CREDENTIALS | INSECURE_DIRECT_OBJECT_REFERENCE | PRIVILEGE_ESCALATION | SERVER_SIDE_TEMPLATE_INJECTION | COMMAND_INJECTION | CODE_INJECTION | SQL_INJECTION | ARBITRARY_FILE_UPLOAD | INSECURE_DESERIALIZATION | LOCAL_FILE_INCLUSION | INFORMATION_DISCLOSURE | PATH_TRAVERSAL | SERVER_SIDE_REQUEST_FORGERY | JSON_WEB_TOKEN_VULNERABILITIES | XML_EXTERNAL_ENTITY | FILE_DELETION | OTHER | GRAPHQL_VULNERABILITIES | BUSINESS_LOGIC_VULNERABILITIES | CRYPTOGRAPHIC_VULNERABILITIES | DENIAL_OF_SERVICE | FILE_ACCESS | FILE_CREATION | DATABASE_MODIFICATION | DATABASE_ACCESS | OUTBOUND_SERVICE_REQUEST | UNKNOWN

Required: No

logConfig

The CloudWatch Logs configuration for the pentest.

Type: [CloudWatchLog](#) object

Required: No

networkTrafficConfig

The network traffic configuration for the pentest, including custom headers and traffic rules.

Type: [NetworkTrafficConfig](#) object

Required: No

serviceRole

The IAM service role to use for the pentest.

Type: String

Required: No

title

The title of the pentest.

Type: String

Required: Yes

vpcConfig

The VPC configuration for the pentest.

Type: [VpcConfig](#) object

Required: No

Response Syntax

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

{
  "agentSpaceId": "string",
```

```
"assets": {
  "actors": [
    {
      "authentication": {
        "providerType": "string",
        "value": "string"
      },
      "description": "string",
      "identifier": "string",
      "uris": [ "string" ]
    }
  ],
  "documents": [
    {
      "artifactId": "string",
      "s3Location": "string"
    }
  ],
  "endpoints": [
    {
      "uri": "string"
    }
  ],
  "integratedRepositories": [
    {
      "integrationId": "string",
      "providerResourceId": "string"
    }
  ],
  "sourceCode": [
    {
      "s3Location": "string"
    }
  ]
},
"createdAt": "string",
"excludeRiskTypes": [ "string" ],
"logConfig": {
  "logGroup": "string",
  "logStream": "string"
},
"pentestId": "string",
"serviceRole": "string",
"title": "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.

[agentSpaceId](#)

The unique identifier of the agent space that contains the pentest.

Type: String

[assets](#)

The assets included in the pentest.

Type: [Assets](#) object

[createdAt](#)

The date and time the pentest was created, in UTC format.

Type: Timestamp

[excludeRiskTypes](#)

The list of risk types excluded from the pentest.

Type: Array of strings

Valid Values: CROSS_SITE_SCRIPTING | DEFAULT_CREDENTIALS | INSECURE_DIRECT_OBJECT_REFERENCE | PRIVILEGE_ESCALATION | SERVER_SIDE_TEMPLATE_INJECTION | COMMAND_INJECTION | CODE_INJECTION | SQL_INJECTION | ARBITRARY_FILE_UPLOAD | INSECURE_DESERIALIZATION | LOCAL_FILE_INCLUSION | INFORMATION_DISCLOSURE | PATH_TRAVERSAL | SERVER_SIDE_REQUEST_FORGERY | JSON_WEB_TOKEN_VULNERABILITIES | XML_EXTERNAL_ENTITY | FILE_DELETION | OTHER | GRAPHQL_VULNERABILITIES | BUSINESS_LOGIC_VULNERABILITIES | CRYPTOGRAPHIC_VULNERABILITIES | DENIAL_OF_SERVICE | FILE_ACCESS | FILE_CREATION | DATABASE_MODIFICATION | DATABASE_ACCESS | OUTBOUND_SERVICE_REQUEST | UNKNOWN

[logConfig](#)

The CloudWatch Logs configuration for the pentest.

Type: [CloudWatchLog](#) object

[pentestId](#)

The unique identifier of the created pentest.

Type: String

[serviceRole](#)

The IAM service role used for the pentest.

Type: String

[title](#)

The title of the pentest.

Type: String

[updatedAt](#)

The date and time the pentest was last updated, in UTC format.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

CreateTargetDomain

Creates a new target domain for penetration testing. A target domain is a web domain that must be registered and verified before it can be tested.

Request Syntax

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

```
{
  "tags": {
    "string" : "string"
  },
  "targetDomainName": "string",
  "verificationMethod": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

tags

The tags to associate with the target domain.

Type: String to string map

Required: No

targetDomainName

The domain name to register as a target domain.

Type: String

Required: Yes

verificationMethod

The method to use for verifying domain ownership. Valid values are DNS_TXT and HTTP_ROUTE.

Type: String

Valid Values: DNS_TXT | HTTP_ROUTE

Required: Yes

Response Syntax

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

{
  "createdAt": "string",
  "domainName": "string",
  "targetDomainId": "string",
  "verificationDetails": {
    "dnsTxt": {
      "dnsRecordName": "string",
      "dnsRecordType": "string",
      "token": "string"
    },
    "httpRoute": {
      "routePath": "string",
      "token": "string"
    },
    "method": "string"
  },
  "verificationStatus": "string",
  "verifiedAt": "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 date and time the target domain was created, in UTC format.

Type: Timestamp

domainName

The domain name of the target domain.

Type: String

targetDomainId

The unique identifier of the created target domain.

Type: String

verificationDetails

The verification details for the target domain, including the verification token and instructions.

Type: [VerificationDetails](#) object

verificationStatus

The current verification status of the target domain.

Type: String

Valid Values: PENDING | VERIFIED | FAILED | UNREACHABLE

verifiedAt

The date and time the target domain was verified, in UTC format.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

DeleteAgentSpace

Deletes an agent space and all of its associated resources, including pentests, findings, and artifacts.

Request Syntax

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

```
{
  "agentSpaceId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

[agentSpaceId](#)

The unique identifier of the agent space to delete.

Type: String

Required: Yes

Response Syntax

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

```
{
  "agentSpaceId": "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.

agentSpaceId

The unique identifier of the deleted agent space.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

DeleteApplication

Deletes an application and its associated configuration, including IAM Identity Center settings.

Request Syntax

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

```
{
  "applicationId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

applicationId

The unique identifier of the application to delete.

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](#).

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](#)
- [AWS SDK for Ruby V3](#)

DeleteArtifact

Deletes an artifact from an agent space.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "artifactId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

[agentSpaceId](#)

The unique identifier of the agent space that contains the artifact.

Type: String

Required: Yes

[artifactId](#)

The unique identifier of the artifact to delete.

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](#).

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred during the processing of your request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource was not found. Verify that the resource identifier is correct and that the resource exists in the specified agent space or account.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The input fails to satisfy the constraints specified by the service.

HTTP Status Code: 400

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](#)
- [AWS SDK for Ruby V3](#)

DeleteIntegration

Deletes an integration with a third-party provider.

Request Syntax

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

```
{
  "integrationId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

integrationId

The unique identifier of the integration to delete.

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](#).

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ConflictException

The request could not be completed due to a conflict with the current state of the resource.

HTTP Status Code: 409

InternalServerErrorException

An unexpected error occurred during the processing of your request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource was not found. Verify that the resource identifier is correct and that the resource exists in the specified agent space or account.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The input fails to satisfy the constraints specified by the service.

HTTP Status Code: 400

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](#)
- [AWS SDK for Ruby V3](#)

DeleteMembership

Deletes a membership, revoking a user's access to an agent space.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "applicationId": "string",
  "membershipId": "string",
  "memberType": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space to revoke access from.

Type: String

Required: Yes

applicationId

The unique identifier of the application that contains the agent space.

Type: String

Required: Yes

membershipId

The unique identifier of the membership to delete.

Type: String

Required: Yes

memberType

The type of member to remove.

Type: String

Valid Values: USER

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](#).

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](#)
- [AWS SDK for Ruby V3](#)

DeleteTargetDomain

Deletes a target domain registration. After deletion, the domain can no longer be used for penetration testing.

Request Syntax

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

{
  "targetDomainId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

targetDomainId

The unique identifier of the target domain to delete.

Type: String

Required: Yes

Response Syntax

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

{
  "targetDomainId": "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.

targetDomainId

The unique identifier of the deleted target domain.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

GetApplication

Retrieves information about an application.

Request Syntax

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

{
  "applicationId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

[applicationId](#)

The unique identifier of the application to retrieve.

Type: String

Required: Yes

Response Syntax

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

{
  "applicationId": "string",
  "applicationName": "string",
  "defaultKmsKeyId": "string",
  "domain": "string",
  "idcConfiguration": {
```

```
    "idcApplicationArn": "string",  
    "idcInstanceArn": "string"  
  },  
  "roleArn": "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.

applicationId

The unique identifier of the application.

Type: String

applicationName

The name of the application.

Type: String

defaultKmsKeyId

The identifier of the default AWS KMS key used to encrypt data for the application.

Type: String

domain

The domain associated with the application.

Type: String

idcConfiguration

The IAM Identity Center configuration for the application.

Type: [IdCConfiguration](#) object

roleArn

The Amazon Resource Name (ARN) of the IAM role associated with the application.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

GetArtifact

Retrieves an artifact from an agent space.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "artifactId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space that contains the artifact.

Type: String

Required: Yes

artifactId

The unique identifier of the artifact to retrieve.

Type: String

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json
```

```
{
  "agentSpaceId": "string",
  "artifact": {
    "contents": "string",
    "type": "string"
  },
  "artifactId": "string",
  "fileName": "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.

agentSpaceId

The unique identifier of the agent space that contains the artifact.

Type: String

artifact

The artifact content and type.

Type: [Artifact](#) object

artifactId

The unique identifier of the artifact.

Type: String

fileName

The file name of the artifact.

Type: String

updatedAt

The date and time the artifact was last updated, in UTC format.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

An unexpected error occurred during the processing of your request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource was not found. Verify that the resource identifier is correct and that the resource exists in the specified agent space or account.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The input fails to satisfy the constraints specified by the service.

HTTP Status Code: 400

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](#)
- [AWS SDK for Ruby V3](#)

GetIntegration

Retrieves information about an integration.

Request Syntax

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

{
  "integrationId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

[integrationId](#)

The unique identifier of the integration to retrieve.

Type: String

Required: Yes

Response Syntax

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

{
  "displayName": "string",
  "installationId": "string",
  "integrationId": "string",
  "kmsKeyId": "string",
  "provider": "string",
}
```

```
"providerType": "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.

[displayName](#)

The display name of the integration.

Type: String

[installationId](#)

The installation identifier from the integration provider.

Type: String

[integrationId](#)

The unique identifier of the integration.

Type: String

[kmsKeyId](#)

The identifier of the AWS KMS key used to encrypt data associated with the integration.

Type: String

[provider](#)

The integration provider.

Type: String

Valid Values: GITHUB

[providerType](#)

The type of the integration provider.

Type: String

Valid Values: SOURCE_CODE | DOCUMENTATION

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

An unexpected error occurred during the processing of your request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource was not found. Verify that the resource identifier is correct and that the resource exists in the specified agent space or account.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The input fails to satisfy the constraints specified by the service.

HTTP Status Code: 400

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](#)
- [AWS SDK for Ruby V3](#)

InitiateProviderRegistration

Initiates the OAuth registration flow with a third-party provider. Returns a redirect URL and CSRF state token for completing the authorization.

Request Syntax

```
POST /oauth2/provider/register HTTP/1.1
Content-type: application/json
```

```
{
  "provider": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

provider

The provider to initiate registration with. Currently, only GITHUB is supported.

Type: String

Valid Values: GITHUB

Required: Yes

Response Syntax

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

```
{
  "csrfState": "string",
}
```

```
"redirectTo": "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.

csrfState

The CSRF state token to use when completing the OAuth flow.

Type: String

redirectTo

The URL to redirect the user to for completing the OAuth authorization.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ConflictException

The request could not be completed due to a conflict with the current state of the resource.

HTTP Status Code: 409

InternalServerError

An unexpected error occurred during the processing of your request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource was not found. Verify that the resource identifier is correct and that the resource exists in the specified agent space or account.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The input fails to satisfy the constraints specified by the service.

HTTP Status Code: 400

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](#)
- [AWS SDK for Ruby V3](#)

ListAgentSpaces

Returns a paginated list of agent space summaries in your account.

Request Syntax

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

```
{
  "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.

maxResults

The maximum number of results to return in a single call.

Type: Integer

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Required: No

Response Syntax

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

{
  "agentSpaceSummaries": [
    {
      "agentSpaceId": "string",
      "createdAt": "string",
      "name": "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.

agentSpaceSummaries

The list of agent space summaries.

Type: Array of [AgentSpaceSummary](#) 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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

ListApplications

Returns a paginated list of application summaries in your account.

Request Syntax

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

```
{
  "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.

maxResults

The maximum number of results to return in a single call.

Type: Integer

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Required: No

Response Syntax

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

{
  "applicationSummaries": [
    {
      "applicationId": "string",
      "applicationName": "string",
      "defaultKmsKeyId": "string",
      "domain": "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.

applicationSummaries

The list of application summaries.

Type: Array of [ApplicationSummary](#) 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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

ListArtifacts

Returns a paginated list of artifact summaries for the specified agent space.

Request Syntax

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

```
{
  "agentSpaceId": "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.

agentSpaceId

The unique identifier of the agent space to list artifacts for.

Type: String

Required: Yes

maxResults

The maximum number of results to return in a single call.

Type: Integer

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Required: No

Response Syntax

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

{
  "artifactSummaries": [
    {
      "artifactId": "string",
      "artifactType": "string",
      "fileName": "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.

[artifactSummaries](#)

The list of artifact summaries.

Type: Array of [ArtifactSummary](#) 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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

An unexpected error occurred during the processing of your request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource was not found. Verify that the resource identifier is correct and that the resource exists in the specified agent space or account.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The input fails to satisfy the constraints specified by the service.

HTTP Status Code: 400

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](#)
- [AWS SDK for Ruby V3](#)

ListDiscoveredEndpoints

Returns a paginated list of endpoints discovered during a pentest job execution.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "maxResults": number,
  "nextToken": "string",
  "pentestJobId": "string",
  "prefix": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space.

Type: String

Required: Yes

maxResults

The maximum number of results to return in a single call.

Type: Integer

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Required: No

pentestJobId

The unique identifier of the pentest job to list discovered endpoints for.

Type: String

Required: Yes

prefix

A prefix to filter discovered endpoints by URI.

Type: String

Required: No

Response Syntax

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

{
  "discoveredEndpoints": [
    {
      "agentSpaceId": "string",
      "description": "string",
      "evidence": "string",
      "operation": "string",
      "pentestJobId": "string",
      "taskId": "string",
      "uri": "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.

discoveredEndpoints

The list of discovered endpoints.

Type: Array of [DiscoveredEndpoint](#) 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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

ListFindings

Lists the security findings for a pentest job.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "confidence": "string",
  "maxResults": number,
  "name": "string",
  "nextToken": "string",
  "pentestJobId": "string",
  "riskLevel": "string",
  "riskType": "string",
  "status": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space.

Type: String

Required: Yes

confidence

Filter findings by confidence level.

Type: String

Valid Values: FALSE_POSITIVE | UNCONFIRMED | LOW | MEDIUM | HIGH

Required: No

maxResults

The maximum number of results to return in a single call.

Type: Integer

Required: No

name

Filter findings by name.

Type: String

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Required: No

pentestJobId

The unique identifier of the pentest job to list findings for.

Type: String

Required: Yes

riskLevel

Filter findings by risk level.

Type: String

Valid Values: UNKNOWN | INFORMATIONAL | LOW | MEDIUM | HIGH | CRITICAL

Required: No

riskType

Filter findings by risk type.

Type: String

Required: No

status

Filter findings by status.

Type: String

Valid Values: ACTIVE | RESOLVED | ACCEPTED | FALSE_POSITIVE

Required: No

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json
```

```
{
  "findingsSummaries": [
    {
      "agentSpaceId": "string",
      "confidence": "string",
      "createdAt": "string",
      "findingId": "string",
      "name": "string",
      "pentestId": "string",
      "pentestJobId": "string",
      "riskLevel": "string",
      "riskType": "string",
      "status": "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.

[findingsSummaries](#)

The list of finding summaries.

Type: Array of [FindingSummary](#) 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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)

- [AWS SDK for Ruby V3](#)

ListIntegratedResources

Lists the integrated resources for an agent space, optionally filtered by integration or resource type.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "integrationId": "string",
  "maxResults": number,
  "nextToken": "string",
  "resourceType": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space to list integrated resources for.

Type: String

Required: Yes

integrationId

The unique identifier of the integration to filter by.

Type: String

Required: No

maxResults

The maximum number of results to return in a single call.

Type: Integer

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Required: No

resourceType

The type of resource to filter by.

Type: String

Valid Values: CODE_REPOSITORY

Required: No

Response Syntax

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

{
  "integratedResourceSummaries": [
    {
      "capabilities": { ... },
      "integrationId": "string",
      "resource": { ... }
    }
  ],
  "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.

[integratedResourceSummaries](#)

The list of integrated resource summaries.

Type: Array of [IntegratedResourceSummary](#) 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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

An unexpected error occurred during the processing of your request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource was not found. Verify that the resource identifier is correct and that the resource exists in the specified agent space or account.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The input fails to satisfy the constraints specified by the service.

HTTP Status Code: 400

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](#)
- [AWS SDK for Ruby V3](#)

ListIntegrations

Lists the integrations in your account, optionally filtered by provider or provider type.

Request Syntax

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

```
{
  "filter": { ... },
  "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.

filter

A filter to apply to the list of integrations.

Type: [IntegrationFilter](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: No

maxResults

The maximum number of results to return in a single call.

Type: Integer

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Required: No

Response Syntax

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

{
  "integrationSummaries": [
    {
      "displayName": "string",
      "installationId": "string",
      "integrationId": "string",
      "provider": "string",
      "providerType": "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.

integrationSummaries

The list of integration summaries.

Type: Array of [IntegrationSummary](#) 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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

An unexpected error occurred during the processing of your request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource was not found. Verify that the resource identifier is correct and that the resource exists in the specified agent space or account.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The input fails to satisfy the constraints specified by the service.

HTTP Status Code: 400

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](#)
- [AWS SDK for Ruby V3](#)

ListMemberships

Returns a paginated list of membership summaries for the specified agent space within an application.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "applicationId": "string",
  "maxResults": number,
  "memberType": "string",
  "nextToken": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space to list memberships for.

Type: String

Required: Yes

applicationId

The unique identifier of the application that contains the agent space.

Type: String

Required: Yes

maxResults

The maximum number of results to return in a single call.

Type: Integer

Required: No

memberType

Filter memberships by member type.

Type: String

Valid Values: USER | ALL

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Required: No

Response Syntax

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

{
  "membershipSummaries": [
    {
      "agentSpaceId": "string",
      "applicationId": "string",
      "config": { ... },
      "createdAt": "string",
      "createdBy": "string",
      "membershipId": "string",
      "memberType": "string",
      "metadata": { ... },
```

```
    "updatedAt": "string",  
    "updatedBy": "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.

membershipSummaries

The list of membership summaries.

Type: Array of [MembershipSummary](#) 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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

ListPentestJobsForPentest

Returns a paginated list of pentest job summaries for the specified pentest configuration.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "maxResults": number,
  "nextToken": "string",
  "pentestId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

[agentSpaceId](#)

The unique identifier of the agent space.

Type: String

Required: Yes

[maxResults](#)

The maximum number of results to return in a single call.

Type: Integer

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Required: No

pentestId

The unique identifier of the pentest to list jobs for.

Type: String

Required: Yes

Response Syntax

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

{
  "nextToken": "string",
  "pentestJobSummaries": [
    {
      "createdAt": "string",
      "pentestId": "string",
      "pentestJobId": "string",
      "status": "string",
      "title": "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.

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

pentestJobSummaries

The list of pentest job summaries.

Type: Array of [PentestJobSummary](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

ListPentestJobTasks

Returns a paginated list of task summaries for the specified pentest job, optionally filtered by step name or category.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "categoryName": "string",
  "maxResults": number,
  "nextToken": "string",
  "pentestJobId": "string",
  "stepName": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space.

Type: String

Required: Yes

categoryName

Filter tasks by category name.

Type: String

Required: No

maxResults

The maximum number of results to return in a single call.

Type: Integer

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Required: No

pentestJobId

The unique identifier of the pentest job to list tasks for.

Type: String

Required: No

stepName

Filter tasks by step name. Valid values include PREFLIGHT, STATIC_ANALYSIS, PENTEST, and FINALIZING.

Type: String

Valid Values: PREFLIGHT | STATIC_ANALYSIS | PENTEST | FINALIZING

Required: No

Response Syntax

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

{
  "nextToken": "string",
  "taskSummaries": [
```

```
{
  "agentSpaceId": "string",
  "createdAt": "string",
  "executionStatus": "string",
  "pentestId": "string",
  "pentestJobId": "string",
  "riskType": "string",
  "taskId": "string",
  "title": "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.

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

taskSummaries

The list of task summaries.

Type: Array of [TaskSummary](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

ListPentests

Returns a paginated list of pentest summaries for the specified agent space.

Request Syntax

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

{
  "agentSpaceId": "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.

agentSpaceId

The unique identifier of the agent space to list pentests for.

Type: String

Required: Yes

maxResults

The maximum number of results to return in a single call.

Type: Integer

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Required: No

Response Syntax

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

{
  "nextToken": "string",
  "pentestSummaries": [
    {
      "agentSpaceId": "string",
      "createdAt": "string",
      "pentestId": "string",
      "title": "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.

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

pentestSummaries

The list of pentest summaries.

Type: Array of PentestSummary objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

ListTagsForResource

Returns the tags associated with the specified 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) of the resource to list tags for.

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

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

ListTargetDomains

Returns a paginated list of target domain summaries in your account.

Request Syntax

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

```
{
  "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.

maxResults

The maximum number of results to return in a single call.

Type: Integer

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

Required: No

Response Syntax

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

{
  "nextToken": "string",
  "targetDomainSummaries": [
    {
      "domainName": "string",
      "targetDomainId": "string",
      "verificationStatus": "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

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. For subsequent calls, use the nextToken value returned from the previous request.

Type: String

targetDomainSummaries

The list of target domain summaries.

Type: Array of [TargetDomainSummary](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

StartCodeRemediation

Initiates code remediation for one or more security findings. This creates pull requests in integrated repositories to fix the identified vulnerabilities.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "findingIds": [ "string" ],
  "pentestJobId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space.

Type: String

Required: Yes

findingIds

The list of finding identifiers to initiate code remediation for.

Type: Array of strings

Required: Yes

pentestJobId

The unique identifier of the pentest job that produced the findings.

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](#).

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](#)
- [AWS SDK for Ruby V3](#)

StartPentestJob

Starts a new pentest job for a pentest configuration. The job executes the security tests defined in the pentest.

Request Syntax

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

{
  "agentSpaceId": "string",
  "pentestId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space.

Type: String

Required: Yes

pentestId

The unique identifier of the pentest to start a job for.

Type: String

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json
```

```
{
  "agentSpaceId": "string",
  "createdAt": "string",
  "pentestId": "string",
  "pentestJobId": "string",
  "status": "string",
  "title": "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.

[agentSpaceId](#)

The unique identifier of the agent space.

Type: String

[createdAt](#)

The date and time the pentest job was created, in UTC format.

Type: Timestamp

[pentestId](#)

The unique identifier of the pentest.

Type: String

[pentestJobId](#)

The unique identifier of the started pentest job.

Type: String

[status](#)

The current status of the pentest job.

Type: String

Valid Values: IN_PROGRESS | STOPPING | STOPPED | FAILED | COMPLETED

title

The title of the pentest job.

Type: String

updatedAt

The date and time the pentest job was last updated, in UTC format.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

StopPentestJob

Stops a running pentest job. The job transitions to a stopping state and then to stopped after cleanup completes.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "pentestJobId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space.

Type: String

Required: Yes

pentestJobId

The unique identifier of the pentest job to stop.

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](#).

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](#)
- [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) of the resource to tag.

Required: Yes

Request Body

The request accepts the following data in JSON format.

tags

The tags to add to the resource.

Type: String to string map

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](#).

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](#)
- [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) of the resource to remove tags from.

Required: Yes

tagKeys

The list of tag keys to remove from the resource.

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](#).

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](#)
- [AWS SDK for Ruby V3](#)

UpdateAgentSpace

Updates the configuration of an existing agent space, including its name, description, AWS resources, target domains, and code review settings.

Request Syntax

```
POST /UpdateAgentSpace HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "agentSpaceId": "string",
  "awsResources": {
    "iamRoles": [ "string" ],
    "lambdaFunctionArns": [ "string" ],
    "logGroups": [ "string" ],
    "s3Buckets": [ "string" ],
    "secretArns": [ "string" ],
    "vpcs": [
      {
        "securityGroupArns": [ "string" ],
        "subnetArns": [ "string" ],
        "vpcArn": "string"
      }
    ]
  },
  "codeReviewSettings": {
    "controlsScanning": boolean,
    "generalPurposeScanning": boolean
  },
  "description": "string",
  "name": "string",
  "targetDomainIds": [ "string" ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space to update.

Type: String

Required: Yes

awsResources

The updated AWS resources to associate with the agent space.

Type: [AWSResources](#) object

Required: No

codeReviewSettings

The updated code review settings for the agent space.

Type: [CodeReviewSettings](#) object

Required: No

description

The updated description of the agent space.

Type: String

Required: No

name

The updated name of the agent space.

Type: String

Required: No

targetDomainIds

The updated list of target domain identifiers to associate with the agent space.

Type: Array of strings

Required: No

Response Syntax

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

{
  "agentSpaceId": "string",
  "awsResources": {
    "iamRoles": [ "string" ],
    "lambdaFunctionArns": [ "string" ],
    "logGroups": [ "string" ],
    "s3Buckets": [ "string" ],
    "secretArns": [ "string" ],
    "vpcs": [
      {
        "securityGroupArns": [ "string" ],
        "subnetArns": [ "string" ],
        "vpcArn": "string"
      }
    ]
  },
  "codeReviewSettings": {
    "controlsScanning": boolean,
    "generalPurposeScanning": boolean
  },
  "createdAt": "string",
  "description": "string",
  "name": "string",
  "targetDomainIds": [ "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.

agentSpaceId

The unique identifier of the updated agent space.

Type: String

awsResources

The AWS resources associated with the agent space.

Type: [AWSResources](#) object

codeReviewSettings

The code review settings for the agent space.

Type: [CodeReviewSettings](#) object

createdAt

The date and time the agent space was created, in UTC format.

Type: Timestamp

description

The description of the agent space.

Type: String

name

The name of the agent space.

Type: String

targetDomainIds

The list of target domain identifiers associated with the agent space.

Type: Array of strings

updatedAt

The date and time the agent space was last updated, in UTC format.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

UpdateApplication

Updates the configuration of an existing application, including the IAM role and default KMS key.

Request Syntax

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

{
  "applicationId": "string",
  "defaultKmsKeyId": "string",
  "roleArn": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

applicationId

The unique identifier of the application to update.

Type: String

Required: Yes

defaultKmsKeyId

The updated identifier of the default AWS KMS key for the application.

Type: String

Required: No

roleArn

The updated Amazon Resource Name (ARN) of the IAM role for the application.

Type: String

Required: No

Response Syntax

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

{
  "applicationId": "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.

applicationId

The unique identifier of the updated application.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

UpdateFinding

Updates the status or risk level of a security finding.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "findingId": "string",
  "riskLevel": "string",
  "status": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space that contains the finding.

Type: String

Required: Yes

findingId

The unique identifier of the finding to update.

Type: String

Required: Yes

riskLevel

The updated risk level for the finding.

Type: String

Valid Values: UNKNOWN | INFORMATIONAL | LOW | MEDIUM | HIGH | CRITICAL

Required: No

status

The updated status for the finding.

Type: String

Valid Values: ACTIVE | RESOLVED | ACCEPTED | FALSE_POSITIVE

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](#).

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](#)
- [AWS SDK for Ruby V3](#)

UpdateIntegratedResources

Updates the integrated resources for an agent space, including their capabilities.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "integrationId": "string",
  "items": [
    {
      "capabilities": { ... },
      "resource": { ... }
    }
  ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space.

Type: String

Required: Yes

integrationId

The unique identifier of the integration.

Type: String

Required: Yes

items

The list of integrated resource items to update.

Type: Array of [IntegratedResourceInputItem](#) objects

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

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ConflictException

The request could not be completed due to a conflict with the current state of the resource.

HTTP Status Code: 409

InternalServerErrorException

An unexpected error occurred during the processing of your request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource was not found. Verify that the resource identifier is correct and that the resource exists in the specified agent space or account.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The input fails to satisfy the constraints specified by the service.

HTTP Status Code: 400

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](#)
- [AWS SDK for Ruby V3](#)

UpdatePentest

Updates an existing pentest configuration.

Request Syntax

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

```
{
  "agentSpaceId": "string",
  "assets": {
    "actors": [
      {
        "authentication": {
          "providerType": "string",
          "value": "string"
        },
        "description": "string",
        "identifier": "string",
        "uris": [ "string" ]
      }
    ],
    "documents": [
      {
        "artifactId": "string",
        "s3Location": "string"
      }
    ],
    "endpoints": [
      {
        "uri": "string"
      }
    ],
    "integratedRepositories": [
      {
        "integrationId": "string",
        "providerResourceId": "string"
      }
    ],
    "sourceCode": [
      {
        "s3Location": "string"
      }
    ]
  }
}
```

```
    }
  ]
},
"codeRemediationStrategy": "string",
"excludeRiskTypes": [ "string" ],
"logConfig": {
  "logGroup": "string",
  "logStream": "string"
},
"networkTrafficConfig": {
  "customHeaders": [
    {
      "name": "string",
      "value": "string"
    }
  ],
  "rules": [
    {
      "effect": "string",
      "networkTrafficRuleType": "string",
      "pattern": "string"
    }
  ]
},
"pentestId": "string",
"serviceRole": "string",
"title": "string",
"vpcConfig": {
  "securityGroupArns": [ "string" ],
  "subnetArns": [ "string" ],
  "vpcArn": "string"
}
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

agentSpaceId

The unique identifier of the agent space that contains the pentest.

Type: String

Required: Yes

assets

The updated assets for the pentest.

Type: [Assets](#) object

Required: No

codeRemediationStrategy

The updated code remediation strategy for the pentest.

Type: String

Valid Values: AUTOMATIC | DISABLED

Required: No

excludeRiskTypes

The updated list of risk types to exclude from the pentest.

Type: Array of strings

Valid Values: CROSS_SITE_SCRIPTING | DEFAULT_CREDENTIALS | INSECURE_DIRECT_OBJECT_REFERENCE | PRIVILEGE_ESCALATION | SERVER_SIDE_TEMPLATE_INJECTION | COMMAND_INJECTION | CODE_INJECTION | SQL_INJECTION | ARBITRARY_FILE_UPLOAD | INSECURE_DESERIALIZATION | LOCAL_FILE_INCLUSION | INFORMATION_DISCLOSURE | PATH_TRAVERSAL | SERVER_SIDE_REQUEST_FORGERY | JSON_WEB_TOKEN_VULNERABILITIES | XML_EXTERNAL_ENTITY | FILE_DELETION | OTHER | GRAPHQL_VULNERABILITIES | BUSINESS_LOGIC_VULNERABILITIES | CRYPTOGRAPHIC_VULNERABILITIES | DENIAL_OF_SERVICE | FILE_ACCESS | FILE_CREATION | DATABASE_MODIFICATION | DATABASE_ACCESS | OUTBOUND_SERVICE_REQUEST | UNKNOWN

Required: No

logConfig

The updated CloudWatch Logs configuration for the pentest.

Type: [CloudWatchLog](#) object

Required: No

networkTrafficConfig

The updated network traffic configuration for the pentest.

Type: [NetworkTrafficConfig](#) object

Required: No

pentestId

The unique identifier of the pentest to update.

Type: String

Required: Yes

serviceRole

The updated IAM service role for the pentest.

Type: String

Required: No

title

The updated title of the pentest.

Type: String

Required: No

vpcConfig

The updated VPC configuration for the pentest.

Type: [VpcConfig](#) object

Required: No

Response Syntax

HTTP/1.1 200

Content-type: application/json

```
{
  "agentSpaceId": "string",
  "assets": {
    "actors": [
      {
        "authentication": {
          "providerType": "string",
          "value": "string"
        },
        "description": "string",
        "identifier": "string",
        "uris": [ "string" ]
      }
    ],
    "documents": [
      {
        "artifactId": "string",
        "s3Location": "string"
      }
    ],
    "endpoints": [
      {
        "uri": "string"
      }
    ],
    "integratedRepositories": [
      {
        "integrationId": "string",
        "providerResourceId": "string"
      }
    ],
    "sourceCode": [
      {
        "s3Location": "string"
      }
    ]
  }
}
```

```
    }
  ]
},
"createdAt": "string",
"excludeRiskTypes": [ "string " ],
"logConfig": {
  "logGroup": "string",
  "logStream": "string"
},
"pentestId": "string",
"serviceRole": "string",
"title": "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.

agentSpaceId

The unique identifier of the agent space that contains the pentest.

Type: String

assets

The assets included in the pentest.

Type: [Assets](#) object

createdAt

The date and time the pentest was created, in UTC format.

Type: Timestamp

excludeRiskTypes

The list of risk types excluded from the pentest.

Type: Array of strings

Valid Values: CROSS_SITE_SCRIPTING | DEFAULT_CREDENTIALS | INSECURE_DIRECT_OBJECT_REFERENCE | PRIVILEGE_ESCALATION | SERVER_SIDE_TEMPLATE_INJECTION | COMMAND_INJECTION | CODE_INJECTION | SQL_INJECTION | ARBITRARY_FILE_UPLOAD | INSECURE_DESERIALIZATION | LOCAL_FILE_INCLUSION | INFORMATION_DISCLOSURE | PATH_TRAVERSAL | SERVER_SIDE_REQUEST_FORGERY | JSON_WEB_TOKEN_VULNERABILITIES | XML_EXTERNAL_ENTITY | FILE_DELETION | OTHER | GRAPHQL_VULNERABILITIES | BUSINESS_LOGIC_VULNERABILITIES | CRYPTOGRAPHIC_VULNERABILITIES | DENIAL_OF_SERVICE | FILE_ACCESS | FILE_CREATION | DATABASE_MODIFICATION | DATABASE_ACCESS | OUTBOUND_SERVICE_REQUEST | UNKNOWN

logConfig

The CloudWatch Logs configuration for the pentest.

Type: [CloudWatchLog](#) object

pentestId

The unique identifier of the pentest.

Type: String

serviceRole

The IAM service role used for the pentest.

Type: String

title

The title of the pentest.

Type: String

updatedAt

The date and time the pentest was last updated, in UTC format.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

UpdateTargetDomain

Updates the verification method for a target domain.

Request Syntax

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

{
  "targetDomainId": "string",
  "verificationMethod": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

targetDomainId

The unique identifier of the target domain to update.

Type: String

Required: Yes

verificationMethod

The updated verification method for the target domain.

Type: String

Valid Values: DNS_TXT | HTTP_ROUTE

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
  "createdAt": "string",
  "domainName": "string",
  "targetDomainId": "string",
  "verificationDetails": {
    "dnsTxt": {
      "dnsRecordName": "string",
      "dnsRecordType": "string",
      "token": "string"
    },
    "httpRoute": {
      "routePath": "string",
      "token": "string"
    },
    "method": "string"
  },
  "verificationStatus": "string",
  "verifiedAt": "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 date and time the target domain was created, in UTC format.

Type: Timestamp

domainName

The domain name of the target domain.

Type: String

targetDomainId

The unique identifier of the target domain.

Type: String

verificationDetails

The updated verification details for the target domain.

Type: [VerificationDetails](#) object

verificationStatus

The current verification status of the target domain.

Type: String

Valid Values: PENDING | VERIFIED | FAILED | UNREACHABLE

verifiedAt

The date and time the target domain was verified, in UTC format.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

VerifyTargetDomain

Initiates verification of a target domain. This checks whether the domain ownership verification token has been properly configured.

Request Syntax

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

{
  "targetDomainId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

targetDomainId

The unique identifier of the target domain to verify.

Type: String

Required: Yes

Response Syntax

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

{
  "createdAt": "string",
  "domainName": "string",
  "status": "string",
  "targetDomainId": "string",
}
```

```
"updatedAt": "string",  
"verifiedAt": "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 date and time the target domain was created, in UTC format.

Type: Timestamp

[domainName](#)

The domain name of the target domain.

Type: String

[status](#)

The verification status of the target domain.

Type: String

Valid Values: PENDING | VERIFIED | FAILED | UNREACHABLE

[targetDomainId](#)

The unique identifier of the target domain.

Type: String

[updatedAt](#)

The date and time the target domain was last updated, in UTC format.

Type: Timestamp

[verifiedAt](#)

The date and time the target domain was verified, in UTC format.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

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](#)
- [AWS SDK for Ruby V3](#)

Data Types

The AWS Security Agent 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:

- [Actor](#)
- [AgentSpace](#)
- [AgentSpaceSummary](#)
- [ApplicationSummary](#)
- [Artifact](#)
- [ArtifactMetadataItem](#)
- [ArtifactSummary](#)
- [Assets](#)
- [Authentication](#)
- [AWSResources](#)
- [Category](#)
- [CloudWatchLog](#)
- [CodeRemediationTask](#)
- [CodeRemediationTaskDetails](#)
- [CodeReviewSettings](#)
- [CustomHeader](#)
- [DeletePentestFailure](#)
- [DiscoveredEndpoint](#)
- [DnsVerification](#)
- [DocumentInfo](#)

- [Endpoint](#)
- [ErrorInformation](#)
- [ExecutionContext](#)
- [Finding](#)
- [FindingSummary](#)
- [GitHubIntegrationInput](#)
- [GitHubRepositoryMetadata](#)
- [GitHubRepositoryResource](#)
- [GitHubResourceCapabilities](#)
- [HttpVerification](#)
- [IdCConfiguration](#)
- [IntegratedRepository](#)
- [IntegratedResource](#)
- [IntegratedResourceInputItem](#)
- [IntegratedResourceMetadata](#)
- [IntegratedResourceSummary](#)
- [IntegrationFilter](#)
- [IntegrationSummary](#)
- [LogLocation](#)
- [MemberMetadata](#)
- [MembershipConfig](#)
- [MembershipSummary](#)
- [NetworkTrafficConfig](#)
- [NetworkTrafficRule](#)
- [Pentest](#)
- [PentestJob](#)
- [PentestJobSummary](#)
- [PentestSummary](#)
- [ProviderInput](#)
- [ProviderResourceCapabilities](#)

- [SourceCodeRepository](#)
- [Step](#)
- [TargetDomain](#)
- [TargetDomainSummary](#)
- [Task](#)
- [TaskSummary](#)
- [UserConfig](#)
- [UserMetadata](#)
- [ValidationExceptionField](#)
- [VerificationDetails](#)
- [VpcConfig](#)

Actor

Represents an actor used during penetration testing. An actor defines a user or entity that interacts with the target application, including authentication credentials and target URIs.

Contents

authentication

The authentication configuration for the actor.

Type: [Authentication](#) object

Required: No

description

A description of the actor.

Type: String

Required: No

identifier

The unique identifier for the actor.

Type: String

Required: No

uris

The list of URIs that the actor targets during testing.

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](#)

AgentSpace

Represents an agent space, which is a dedicated workspace for securing a specific application. An agent space contains the configuration, resources, and settings needed for security testing.

Contents

agentSpaceId

The unique identifier of the agent space.

Type: String

Required: Yes

name

The name of the agent space.

Type: String

Required: Yes

awsResources

The AWS resources associated with the agent space.

Type: [AWSResources](#) object

Required: No

codeReviewSettings

The code review settings for the agent space.

Type: [CodeReviewSettings](#) object

Required: No

createdAt

The date and time the agent space was created, in UTC format.

Type: Timestamp

Required: No

description

A description of the agent space.

Type: String

Required: No

kmsKeyId

The identifier of the AWS KMS key used to encrypt data in the agent space.

Type: String

Required: No

targetDomainIds

The list of target domain identifiers associated with the agent space.

Type: Array of strings

Required: No

updatedAt

The date and time the agent space was last updated, 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](#)

AgentSpaceSummary

Contains summary information about an agent space.

Contents

agentSpaceId

The unique identifier of the agent space.

Type: String

Required: Yes

name

The name of the agent space.

Type: String

Required: Yes

createdAt

The date and time the agent space was created, in UTC format.

Type: Timestamp

Required: No

updatedAt

The date and time the agent space was last updated, 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](#)

ApplicationSummary

Contains summary information about an application.

Contents

applicationId

The unique identifier of the application.

Type: String

Required: Yes

applicationName

The name of the application.

Type: String

Required: Yes

domain

The domain associated with the application.

Type: String

Required: Yes

defaultKmsKeyId

The identifier of the default AWS KMS key used to encrypt data for the application.

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](#)

Artifact

Represents an artifact that provides context for security testing, such as documentation, diagrams, or configuration files.

Contents

contents

The content of the artifact.

Type: String

Required: Yes

type

The file type of the artifact.

Type: String

Valid Values: TXT | PNG | JPEG | MD | PDF | DOCX | DOC | JSON | YAML

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](#)

ArtifactMetadataItem

Contains metadata about an artifact.

Contents

agentSpaceId

The unique identifier of the agent space that contains the artifact.

Type: String

Required: Yes

artifactId

The unique identifier of the artifact.

Type: String

Required: Yes

fileName

The file name of the artifact.

Type: String

Required: Yes

updatedAt

The date and time the artifact was last updated, in UTC format.

Type: Timestamp

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](#)

ArtifactSummary

Contains summary information about an artifact.

Contents

artifactId

The unique identifier of the artifact.

Type: String

Required: Yes

artifactType

The file type of the artifact.

Type: String

Valid Values: TXT | PNG | JPEG | MD | PDF | DOCX | DOC | JSON | YAML

Required: Yes

fileName

The file name of the artifact.

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](#)

Assets

The collection of assets used in a pentest configuration, including endpoints, actors, documents, source code repositories, and integrated repositories.

Contents

actors

The list of actors used during penetration testing.

Type: Array of [Actor](#) objects

Required: No

documents

The list of documents that provide context for the pentest.

Type: Array of [DocumentInfo](#) objects

Required: No

endpoints

The list of endpoints to test during the pentest.

Type: Array of [Endpoint](#) objects

Required: No

integratedRepositories

The list of integrated repositories associated with the pentest.

Type: Array of [IntegratedRepository](#) objects

Required: No

sourceCode

The list of source code repositories to analyze during the pentest.

Type: Array of [SourceCodeRepository](#) 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](#)

Authentication

The authentication configuration for an actor, specifying the provider type and credentials.

Contents

providerType

The type of authentication provider. Valid values include `SECRETS_MANAGER`, `AWS_LAMBDA`, `AWS_IAM_ROLE`, and `AWS_INTERNAL`.

Type: String

Valid Values: `SECRETS_MANAGER` | `AWS_LAMBDA` | `AWS_IAM_ROLE` | `AWS_INTERNAL`

Required: No

value

The authentication value, such as a secret ARN, Lambda function ARN, or IAM role ARN, depending on the provider 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](#)

AWSResources

The AWS resources associated with an agent space, including VPCs, log groups, S3 buckets, secrets, Lambda functions, and IAM roles.

Contents

iamRoles

The IAM roles associated with the agent space.

Type: Array of strings

Required: No

lambdaFunctionArns

The Amazon Resource Names (ARNs) of the Lambda functions associated with the agent space.

Type: Array of strings

Required: No

logGroups

The Amazon Resource Names (ARNs) of the CloudWatch log groups associated with the agent space.

Type: Array of strings

Required: No

s3Buckets

The Amazon Resource Names (ARNs) of the S3 buckets associated with the agent space.

Type: Array of strings

Required: No

secretArns

The Amazon Resource Names (ARNs) of the Secrets Manager secrets associated with the agent space.

Type: Array of strings

Required: No

vpcs

The VPC configurations associated with the agent space.

Type: Array of [VpcConfig](#) 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](#)

Category

Represents a category assigned to a security testing task.

Contents

isPrimary

Indicates whether this is the primary category for the task.

Type: Boolean

Required: No

name

The name of the category.

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](#)

CloudWatchLog

The Amazon CloudWatch Logs configuration for pentest job logging.

Contents

logGroup

The name of the CloudWatch log group.

Type: String

Required: No

logStream

The name of the CloudWatch log stream.

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](#)

CodeRemediationTask

Represents a code remediation task that was initiated to fix a security finding.

Contents

status

The current status of the code remediation task.

Type: String

Valid Values: IN_PROGRESS | COMPLETED | FAILED

Required: Yes

statusReason

The reason for the current status of the code remediation task.

Type: String

Required: No

taskDetails

The list of details for the code remediation task, including repository name, code diff link, and pull request link.

Type: Array of [CodeRemediationTaskDetails](#) 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](#)

CodeRemediationTaskDetails

Contains details about a code remediation task, including links to the code diff and pull request.

Contents

codeDiffLink

The link to the code diff for the remediation.

Type: String

Required: No

pullRequestLink

The link to the pull request created for the remediation.

Type: String

Required: No

repoName

The name of the repository where the remediation was applied.

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](#)

CodeReviewSettings

The code review settings for an agent space, controlling which types of scanning are enabled.

Contents

controlsScanning

Indicates whether controls scanning is enabled for code reviews.

Type: Boolean

Required: Yes

generalPurposeScanning

Indicates whether general-purpose scanning is enabled for code reviews.

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](#)

CustomHeader

A custom HTTP header to include in network traffic during penetration testing.

Contents

name

The name of the custom header.

Type: String

Required: No

value

The value of the custom header.

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](#)

DeletePentestFailure

Contains information about a pentest that failed to delete.

Contents

pentestId

The unique identifier of the pentest that failed to delete.

Type: String

Required: No

reason

The reason the pentest failed to delete.

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](#)

DiscoveredEndpoint

Represents an endpoint discovered during a pentest job.

Contents

agentSpaceId

The unique identifier of the agent space associated with the discovered endpoint.

Type: String

Required: Yes

pentestJobId

The unique identifier of the pentest job that discovered the endpoint.

Type: String

Required: Yes

taskId

The unique identifier of the task that discovered the endpoint.

Type: String

Required: Yes

uri

The URI of the discovered endpoint.

Type: String

Required: Yes

description

A description of the discovered endpoint.

Type: String

Required: No

evidence

The evidence that led to the discovery of the endpoint.

Type: String

Required: No

operation

The HTTP operation associated with the discovered endpoint.

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](#)

DnsVerification

Contains DNS verification details for a target domain, including the DNS record to create for domain ownership verification.

Contents

dnsRecordName

The name of the DNS record to create for verification.

Type: String

Required: No

dnsRecordType

The type of DNS record to create. Currently, only TXT is supported.

Type: String

Valid Values: TXT

Required: No

token

The verification token to include in the DNS record value.

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](#)

DocumentInfo

Represents a document that provides context for security testing.

Contents

artifactId

The unique identifier of the artifact associated with the document.

Type: String

Required: No

s3Location

The Amazon S3 location of the document.

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](#)

Endpoint

Represents a target endpoint for penetration testing.

Contents

uri

The URI of the endpoint.

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](#)

ErrorInformation

Contains error information for a pentest job that encountered an error.

Contents

code

The error code. Valid values include CLIENT_ERROR, INTERNAL_ERROR, and STOPPED_BY_USER.

Type: String

Valid Values: CLIENT_ERROR | INTERNAL_ERROR | STOPPED_BY_USER

Required: No

message

A message describing the error.

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](#)

ExecutionContext

Contains contextual information about the execution of a pentest job, such as errors, warnings, or informational messages.

Contents

context

The context message.

Type: String

Required: No

contextType

The type of context. Valid values include ERROR, CLIENT_ERROR, WARNING, and INFO.

Type: String

Valid Values: ERROR | CLIENT_ERROR | WARNING | INFO

Required: No

timestamp

The date and time the context was recorded, 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](#)

Finding

Represents a security finding discovered during a pentest job. A finding contains details about a vulnerability, including its risk level, confidence, and remediation status.

Contents

agentSpaceId

The unique identifier of the agent space associated with the finding.

Type: String

Required: Yes

findingId

The unique identifier of the finding.

Type: String

Required: Yes

attackScript

The attack script used to reproduce the finding.

Type: String

Required: No

codeRemediationTask

The code remediation task associated with the finding, if code remediation was initiated.

Type: [CodeRemediationTask](#) object

Required: No

confidence

The confidence level of the finding. Valid values include FALSE_POSITIVE, UNCONFIRMED, LOW, MEDIUM, and HIGH.

Type: String

Valid Values: FALSE_POSITIVE | UNCONFIRMED | LOW | MEDIUM | HIGH

Required: No

createdAt

The date and time the finding was created, in UTC format.

Type: Timestamp

Required: No

description

A description of the finding.

Type: String

Required: No

lastUpdatedBy

The identifier of the entity that last updated the finding.

Type: String

Required: No

name

The name of the finding.

Type: String

Required: No

pentestId

The unique identifier of the pentest associated with the finding.

Type: String

Required: No

pentestJobId

The unique identifier of the pentest job that produced the finding.

Type: String

Required: No

reasoning

The reasoning behind the finding, explaining why it was identified as a vulnerability.

Type: String

Required: No

riskLevel

The risk level of the finding. Valid values include UNKNOWN, INFORMATIONAL, LOW, MEDIUM, HIGH, and CRITICAL.

Type: String

Valid Values: UNKNOWN | INFORMATIONAL | LOW | MEDIUM | HIGH | CRITICAL

Required: No

riskScore

The numerical risk score of the finding.

Type: String

Required: No

riskType

The type of security risk identified by the finding.

Type: String

Required: No

status

The current status of the finding. Valid values include ACTIVE, RESOLVED, ACCEPTED, and FALSE_POSITIVE.

Type: String

Valid Values: ACTIVE | RESOLVED | ACCEPTED | FALSE_POSITIVE

Required: No

taskId

The unique identifier of the task that produced the finding.

Type: String

Required: No

updatedAt

The date and time the finding was last updated, 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](#)

FindingSummary

Contains summary information about a security finding.

Contents

agentSpaceId

The unique identifier of the agent space associated with the finding.

Type: String

Required: Yes

findingId

The unique identifier of the finding.

Type: String

Required: Yes

confidence

The confidence level of the finding.

Type: String

Valid Values: FALSE_POSITIVE | UNCONFIRMED | LOW | MEDIUM | HIGH

Required: No

createdAt

The date and time the finding was created, in UTC format.

Type: Timestamp

Required: No

name

The name of the finding.

Type: String

Required: No

pentestId

The unique identifier of the pentest associated with the finding.

Type: String

Required: No

pentestJobId

The unique identifier of the pentest job that produced the finding.

Type: String

Required: No

riskLevel

The risk level of the finding.

Type: String

Valid Values: UNKNOWN | INFORMATIONAL | LOW | MEDIUM | HIGH | CRITICAL

Required: No

riskType

The type of security risk identified by the finding.

Type: String

Required: No

status

The current status of the finding.

Type: String

Valid Values: ACTIVE | RESOLVED | ACCEPTED | FALSE_POSITIVE

Required: No

updatedAt

The date and time the finding was last updated, 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](#)

GitHubIntegrationInput

The input required to create a GitHub integration, including the OAuth authorization code and CSRF state.

Contents

code

The OAuth authorization code received from GitHub.

Type: String

Required: Yes

state

The CSRF state token for validating the OAuth flow.

Type: String

Required: Yes

organizationName

The name of the GitHub organization to integrate with.

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](#)

GitHubRepositoryMetadata

Contains metadata about a GitHub repository that is integrated with the service.

Contents

name

The name of the GitHub repository.

Type: String

Required: Yes

owner

The owner of the GitHub repository.

Type: String

Required: Yes

providerResourceId

The provider-specific resource identifier for the GitHub repository.

Type: String

Required: Yes

accessType

The access type of the GitHub repository. Valid values are PRIVATE and PUBLIC.

Type: String

Valid Values: PRIVATE | PUBLIC

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](#)

GitHubRepositoryResource

Represents a GitHub repository resource used in an integration.

Contents

name

The name of the GitHub repository.

Type: String

Required: Yes

owner

The owner of the GitHub repository.

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](#)

GitHubResourceCapabilities

The capabilities enabled for a GitHub resource integration.

Contents

leaveComments

Indicates whether the integration can leave comments on pull requests.

Type: Boolean

Required: No

remediateCode

Indicates whether the integration can create code remediation pull requests.

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](#)

HttpVerification

Contains HTTP route verification details for a target domain, including the route path and token to serve for domain ownership verification.

Contents

routePath

The HTTP route path where the verification token must be served.

Type: String

Required: No

token

The verification token to serve at the specified route path.

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](#)

IdCConfiguration

The IAM Identity Center configuration for an application.

Contents

idcApplicationArn

The Amazon Resource Name (ARN) of the IAM Identity Center application.

Type: String

Required: No

idcInstanceArn

The Amazon Resource Name (ARN) of the IAM Identity Center 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](#)

IntegratedRepository

Represents a code repository that is integrated with the service through a third-party provider.

Contents

integrationId

The unique identifier of the integration that provides access to the repository.

Type: String

Required: Yes

providerResourceId

The provider-specific resource identifier for the repository.

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](#)

IntegratedResource

Represents an integrated resource from a third-party provider. This is a union type that contains provider-specific resource information.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

githubRepository

The GitHub repository resource information.

Type: [GitHubRepositoryResource](#) 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](#)

IntegratedResourceInputItem

Represents an input item for updating integrated resources, including the resource and its capabilities.

Contents

resource

The integrated resource to update.

Type: [IntegratedResource](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

capabilities

The capabilities to enable for the integrated resource.

Type: [ProviderResourceCapabilities](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

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](#)

IntegratedResourceMetadata

Contains metadata about an integrated resource. This is a union type that contains provider-specific metadata.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

githubRepository

The GitHub repository metadata.

Type: [GitHubRepositoryMetadata](#) 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](#)

IntegratedResourceSummary

Contains summary information about an integrated resource.

Contents

integrationId

The unique identifier of the integration that provides access to the resource.

Type: String

Required: Yes

resource

The metadata for the integrated resource.

Type: [IntegratedResourceMetadata](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

capabilities

The capabilities enabled for the integrated resource.

Type: [ProviderResourceCapabilities](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

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](#)

IntegrationFilter

A filter for listing integrations. This is a union type where you can filter by provider or provider type.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

provider

Filter integrations by provider.

Type: String

Valid Values: GITHUB

Required: No

providerType

Filter integrations by provider type.

Type: String

Valid Values: SOURCE_CODE | DOCUMENTATION

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](#)

IntegrationSummary

Contains summary information about an integration.

Contents

displayName

The display name of the integration.

Type: String

Required: Yes

installationId

The installation identifier from the integration provider.

Type: String

Required: Yes

integrationId

The unique identifier of the integration.

Type: String

Required: Yes

provider

The integration provider.

Type: String

Valid Values: GITHUB

Required: Yes

providerType

The type of the integration provider.

Type: String

Valid Values: SOURCE_CODE | DOCUMENTATION

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](#)

LogLocation

The log location for a task, specifying where task execution logs are stored.

Contents

cloudWatchLog

The CloudWatch Logs location for the task logs.

Type: [CloudWatchLog](#) object

Required: No

logType

The type of log storage. Currently, only CLOUDWATCH is supported.

Type: String

Valid Values: CLOUDWATCH

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](#)

MemberMetadata

Contains metadata about a member. This is a union type that contains member-type-specific metadata.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

user

The user metadata for the member.

Type: [UserMetadata](#) 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](#)

MembershipConfig

The configuration for a membership. This is a union type that contains member-type-specific configuration.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

user

The user configuration for the membership.

Type: [UserConfig](#) 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](#)

MembershipSummary

Contains summary information about a membership.

Contents

agentSpaceId

The unique identifier of the agent space.

Type: String

Required: Yes

applicationId

The unique identifier of the application.

Type: String

Required: Yes

createdAt

The date and time the membership was created, in UTC format.

Type: Timestamp

Required: Yes

createdBy

The identifier of the entity that created the membership.

Type: String

Required: Yes

membershipId

The unique identifier of the membership.

Type: String

Required: Yes

memberType

The type of member.

Type: String

Valid Values: USER

Required: Yes

updatedAt

The date and time the membership was last updated, in UTC format.

Type: Timestamp

Required: Yes

updatedBy

The identifier of the entity that last updated the membership.

Type: String

Required: Yes

config

The configuration for the membership.

Type: [MembershipConfig](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: No

metadata

The metadata for the member.

Type: [MemberMetadata](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

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](#)

NetworkTrafficConfig

The network traffic configuration for a pentest, including custom headers and traffic rules.

Contents

customHeaders

The list of custom HTTP headers to include in network traffic during testing.

Type: Array of [CustomHeader](#) objects

Required: No

rules

The list of network traffic rules that control which URLs are allowed or denied during testing.

Type: Array of [NetworkTrafficRule](#) 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](#)

NetworkTrafficRule

A rule that controls network traffic during penetration testing by allowing or denying traffic to specific URL patterns.

Contents

effect

The effect of the rule. Valid values are ALLOW and DENY.

Type: String

Valid Values: ALLOW | DENY

Required: No

networkTrafficRuleType

The type of the network traffic rule. Currently, only URL is supported.

Type: String

Valid Values: URL

Required: No

pattern

The URL pattern to match for the rule.

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](#)

Pentest

Represents a pentest configuration that defines the parameters for security testing, including target assets, risk type exclusions, and infrastructure settings.

Contents

agentSpaceId

The unique identifier of the agent space that contains the pentest.

Type: String

Required: Yes

assets

The assets included in the pentest.

Type: [Assets](#) object

Required: Yes

pentestId

The unique identifier of the pentest.

Type: String

Required: Yes

title

The title of the pentest.

Type: String

Required: Yes

codeRemediationStrategy

The code remediation strategy for the pentest.

Type: String

Valid Values: AUTOMATIC | DISABLED

Required: No

createdAt

The date and time the pentest was created, in UTC format.

Type: Timestamp

Required: No

excludeRiskTypes

The list of risk types excluded from the pentest.

Type: Array of strings

Valid Values: CROSS_SITE_SCRIPTING | DEFAULT_CREDENTIALS | INSECURE_DIRECT_OBJECT_REFERENCE | PRIVILEGE_ESCALATION | SERVER_SIDE_TEMPLATE_INJECTION | COMMAND_INJECTION | CODE_INJECTION | SQL_INJECTION | ARBITRARY_FILE_UPLOAD | INSECURE_DESERIALIZATION | LOCAL_FILE_INCLUSION | INFORMATION_DISCLOSURE | PATH_TRAVERSAL | SERVER_SIDE_REQUEST_FORGERY | JSON_WEB_TOKEN_VULNERABILITIES | XML_EXTERNAL_ENTITY | FILE_DELETION | OTHER | GRAPHQL_VULNERABILITIES | BUSINESS_LOGIC_VULNERABILITIES | CRYPTOGRAPHIC_VULNERABILITIES | DENIAL_OF_SERVICE | FILE_ACCESS | FILE_CREATION | DATABASE_MODIFICATION | DATABASE_ACCESS | OUTBOUND_SERVICE_REQUEST | UNKNOWN

Required: No

logConfig

The CloudWatch Logs configuration for the pentest.

Type: [CloudWatchLog](#) object

Required: No

networkTrafficConfig

The network traffic configuration for the pentest.

Type: [NetworkTrafficConfig](#) object

Required: No

serviceRole

The IAM service role used for the pentest.

Type: String

Required: No

updatedAt

The date and time the pentest was last updated, in UTC format.

Type: Timestamp

Required: No

vpcConfig

The VPC configuration for the pentest.

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](#)

PentestJob

Represents a pentest job, which is an execution instance of a pentest. A pentest job progresses through preflight, static analysis, pentest, and finalizing steps.

Contents

actors

The list of actors used during the pentest job.

Type: Array of [Actor](#) objects

Required: No

allowedDomains

The list of domains allowed during the pentest job.

Type: Array of [Endpoint](#) objects

Required: No

codeRemediationStrategy

The code remediation strategy for the pentest job.

Type: String

Valid Values: AUTOMATIC | DISABLED

Required: No

createdAt

The date and time the pentest job was created, in UTC format.

Type: Timestamp

Required: No

documents

The list of documents providing context for the pentest job.

Type: Array of [DocumentInfo](#) objects

Required: No

endpoints

The list of endpoints being tested in the pentest job.

Type: Array of [Endpoint](#) objects

Required: No

errorInformation

Error information if the pentest job encountered an error.

Type: [ErrorInformation](#) object

Required: No

excludePaths

The list of paths excluded from the pentest job.

Type: Array of [Endpoint](#) objects

Required: No

excludeRiskTypes

The list of risk types excluded from the pentest job.

Type: Array of strings

Valid Values: CROSS_SITE_SCRIPTING | DEFAULT_CREDENTIALS | INSECURE_DIRECT_OBJECT_REFERENCE | PRIVILEGE_ESCALATION | SERVER_SIDE_TEMPLATE_INJECTION | COMMAND_INJECTION | CODE_INJECTION | SQL_INJECTION | ARBITRARY_FILE_UPLOAD | INSECURE_DESERIALIZATION | LOCAL_FILE_INCLUSION | INFORMATION_DISCLOSURE | PATH_TRAVERSAL | SERVER_SIDE_REQUEST_FORGERY | JSON_WEB_TOKEN_VULNERABILITIES | XML_EXTERNAL_ENTITY | FILE_DELETION | OTHER | GRAPHQL_VULNERABILITIES | BUSINESS_LOGIC_VULNERABILITIES | CRYPTOGRAPHIC_VULNERABILITIES | DENIAL_OF_SERVICE | FILE_ACCESS | FILE_CREATION | DATABASE_MODIFICATION | DATABASE_ACCESS | OUTBOUND_SERVICE_REQUEST | UNKNOWN

Required: No

executionContext

The execution context messages for the pentest job.

Type: Array of [ExecutionContext](#) objects

Required: No

integratedRepositories

The list of integrated repositories associated with the pentest job.

Type: Array of [IntegratedRepository](#) objects

Required: No

logConfig

The CloudWatch Logs configuration for the pentest job.

Type: [CloudWatchLog](#) object

Required: No

networkTrafficConfig

The network traffic configuration for the pentest job.

Type: [NetworkTrafficConfig](#) object

Required: No

overview

An overview of the pentest job results.

Type: String

Required: No

pentestId

The unique identifier of the pentest associated with the job.

Type: String

Required: No

pentestJobId

The unique identifier of the pentest job.

Type: String

Required: No

serviceRole

The IAM service role used for the pentest job.

Type: String

Required: No

sourceCode

The list of source code repositories analyzed during the pentest job.

Type: Array of [SourceCodeRepository](#) objects

Required: No

status

The current status of the pentest job.

Type: String

Valid Values: IN_PROGRESS | STOPPING | STOPPED | FAILED | COMPLETED

Required: No

steps

The list of steps in the pentest job execution.

Type: Array of [Step](#) objects

Required: No

title

The title of the pentest job.

Type: String

Required: No

updatedAt

The date and time the pentest job was last updated, in UTC format.

Type: Timestamp

Required: No

vpcConfig

The VPC configuration for the pentest job.

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](#)

PentestJobSummary

Contains summary information about a pentest job.

Contents

pentestId

The unique identifier of the pentest associated with the job.

Type: String

Required: Yes

pentestJobId

The unique identifier of the pentest job.

Type: String

Required: Yes

createdAt

The date and time the pentest job was created, in UTC format.

Type: Timestamp

Required: No

status

The current status of the pentest job.

Type: String

Valid Values: IN_PROGRESS | STOPPING | STOPPED | FAILED | COMPLETED

Required: No

title

The title of the pentest job.

Type: String

Required: No

updatedAt

The date and time the pentest job was last updated, 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](#)

PentestSummary

Contains summary information about a pentest.

Contents

agentSpaceId

The unique identifier of the agent space that contains the pentest.

Type: String

Required: Yes

pentestId

The unique identifier of the pentest.

Type: String

Required: Yes

title

The title of the pentest.

Type: String

Required: Yes

createdAt

The date and time the pentest was created, in UTC format.

Type: Timestamp

Required: No

updatedAt

The date and time the pentest was last updated, 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](#)

ProviderInput

The provider-specific input for creating an integration. This is a union type that contains provider-specific configuration.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

github

The GitHub-specific input for creating an integration.

Type: [GitHubIntegrationInput](#) 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](#)

ProviderResourceCapabilities

The capabilities for an integrated resource from a third-party provider. This is a union type that contains provider-specific capabilities.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

github

The GitHub-specific resource capabilities.

Type: [GitHubResourceCapabilities](#) 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](#)

SourceCodeRepository

Represents a source code repository used for security analysis during a pentest.

Contents

s3Location

The Amazon S3 location of the source code repository archive.

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](#)

Step

Represents a step in the pentest job execution pipeline. Steps include preflight, static analysis, pentest, and finalizing.

Contents

createdAt

The date and time the step was created, in UTC format.

Type: Timestamp

Required: No

name

The name of the step. Valid values include PREFLIGHT, STATIC_ANALYSIS, PENTEST, and FINALIZING.

Type: String

Valid Values: PREFLIGHT | STATIC_ANALYSIS | PENTEST | FINALIZING

Required: No

status

The current status of the step.

Type: String

Valid Values: NOT_STARTED | IN_PROGRESS | COMPLETED | FAILED | STOPPED

Required: No

updatedAt

The date and time the step was last updated, 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](#)

TargetDomain

Represents a target domain registered for penetration testing. A target domain must be verified through DNS TXT or HTTP route verification before it can be used in pentests.

Contents

domainName

The domain name of the target domain.

Type: String

Required: Yes

targetDomainId

The unique identifier of the target domain.

Type: String

Required: Yes

createdAt

The date and time the target domain was created, in UTC format.

Type: Timestamp

Required: No

verificationDetails

The verification details for the target domain.

Type: [VerificationDetails](#) object

Required: No

verificationStatus

The current verification status of the target domain.

Type: String

Valid Values: PENDING | VERIFIED | FAILED | UNREACHABLE

Required: No

verifiedAt

The date and time the target domain was verified, 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](#)

TargetDomainSummary

Contains summary information about a target domain.

Contents

domainName

The domain name of the target domain.

Type: String

Required: Yes

targetDomainId

The unique identifier of the target domain.

Type: String

Required: Yes

verificationStatus

The current verification status of the target domain.

Type: String

Valid Values: PENDING | VERIFIED | FAILED | UNREACHABLE

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](#)

Task

Represents an individual security test task within a pentest job. Each task targets a specific risk type or endpoint and executes independently.

Contents

taskId

The unique identifier of the task.

Type: String

Required: Yes

agentSpaceId

The unique identifier of the agent space.

Type: String

Required: No

categories

The list of categories assigned to the task.

Type: Array of [Category](#) objects

Required: No

createdAt

The date and time the task was created, in UTC format.

Type: Timestamp

Required: No

description

A description of the task.

Type: String

Required: No

executionStatus

The current execution status of the task.

Type: String

Valid Values: IN_PROGRESS | ABORTED | COMPLETED | INTERNAL_ERROR | FAILED

Required: No

logsLocation

The location of the task execution logs.

Type: [LogLocation](#) object

Required: No

pentestId

The unique identifier of the pentest associated with the task.

Type: String

Required: No

pentestJobId

The unique identifier of the pentest job that contains the task.

Type: String

Required: No

riskType

The type of security risk the task is testing for.

Type: String

Valid Values: CROSS_SITE_SCRIPTING | DEFAULT_CREDENTIALS | INSECURE_DIRECT_OBJECT_REFERENCE | PRIVILEGE_ESCALATION | SERVER_SIDE_TEMPLATE_INJECTION | COMMAND_INJECTION | CODE_INJECTION | SQL_INJECTION | ARBITRARY_FILE_UPLOAD | INSECURE_DESERIALIZATION | LOCAL_FILE_INCLUSION | INFORMATION_DISCLOSURE | PATH_TRAVERSAL

| SERVER_SIDE_REQUEST_FORGERY | JSON_WEB_TOKEN_VULNERABILITIES |
XML_EXTERNAL_ENTITY | FILE_DELETION | OTHER | GRAPHQL_VULNERABILITIES
| BUSINESS_LOGIC_VULNERABILITIES | CRYPTOGRAPHIC_VULNERABILITIES |
DENIAL_OF_SERVICE | FILE_ACCESS | FILE_CREATION | DATABASE_MODIFICATION
| DATABASE_ACCESS | OUTBOUND_SERVICE_REQUEST | UNKNOWN

Required: No

targetEndpoint

The target endpoint being tested by the task.

Type: [Endpoint](#) object

Required: No

title

The title of the task.

Type: String

Required: No

updatedAt

The date and time the task was last updated, 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](#)

TaskSummary

Contains summary information about a task.

Contents

taskId

The unique identifier of the task.

Type: String

Required: Yes

agentSpaceId

The unique identifier of the agent space.

Type: String

Required: No

createdAt

The date and time the task was created, in UTC format.

Type: Timestamp

Required: No

executionStatus

The current execution status of the task.

Type: String

Valid Values: IN_PROGRESS | ABORTED | COMPLETED | INTERNAL_ERROR | FAILED

Required: No

pentestId

The unique identifier of the pentest associated with the task.

Type: String

Required: No

pentestJobId

The unique identifier of the pentest job that contains the task.

Type: String

Required: No

riskType

The type of security risk the task is testing for.

Type: String

Valid Values: CROSS_SITE_SCRIPTING | DEFAULT_CREDENTIALS | INSECURE_DIRECT_OBJECT_REFERENCE | PRIVILEGE_ESCALATION | SERVER_SIDE_TEMPLATE_INJECTION | COMMAND_INJECTION | CODE_INJECTION | SQL_INJECTION | ARBITRARY_FILE_UPLOAD | INSECURE_DESERIALIZATION | LOCAL_FILE_INCLUSION | INFORMATION_DISCLOSURE | PATH_TRAVERSAL | SERVER_SIDE_REQUEST_FORGERY | JSON_WEB_TOKEN_VULNERABILITIES | XML_EXTERNAL_ENTITY | FILE_DELETION | OTHER | GRAPHQL_VULNERABILITIES | BUSINESS_LOGIC_VULNERABILITIES | CRYPTOGRAPHIC_VULNERABILITIES | DENIAL_OF_SERVICE | FILE_ACCESS | FILE_CREATION | DATABASE_MODIFICATION | DATABASE_ACCESS | OUTBOUND_SERVICE_REQUEST | UNKNOWN

Required: No

title

The title of the task.

Type: String

Required: No

updatedAt

The date and time the task was last updated, 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](#)

UserConfig

The configuration for a user membership, including the role assigned to the user within the agent space.

Contents

role

The role assigned to the user. Currently, only MEMBER is supported.

Type: String

Valid Values: MEMBER

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](#)

UserMetadata

Contains metadata about a user member, including the username and email address.

Contents

email

The email address of the user.

Type: String

Required: Yes

username

The username of the user.

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](#)

ValidationExceptionField

Describes one specific validation failure for an input member.

Contents

message

A detailed description of the validation failure.

Type: String

Required: Yes

path

A JSONPointer expression to the structure member whose value failed to satisfy the modeled constraint.

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](#)

VerificationDetails

Contains the verification details for a target domain, including the verification method and provider-specific details.

Contents

dnsTxt

The DNS TXT verification details.

Type: [DnsVerification](#) object

Required: No

httpRoute

The HTTP route verification details.

Type: [HttpVerification](#) object

Required: No

method

The verification method used for the target domain.

Type: String

Valid Values: DNS_TXT | HTTP_ROUTE

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

The VPC configuration for a pentest, specifying the VPC, security groups, and subnets to use during testing.

Contents

securityGroupArns

The Amazon Resource Names (ARNs) of the security groups for the VPC configuration.

Type: Array of strings

Required: No

subnetArns

The Amazon Resource Names (ARNs) of the subnets for the VPC configuration.

Type: Array of strings

Required: No

vpcArn

The Amazon Resource Name (ARN) of the VPC.

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