aws

API Reference

Amazon Detective

API Version 2018-10-26

Amazon Detective: API Reference

Table of Contents

Welcome

Detective uses machine learning and purpose-built visualizations to help you to analyze and investigate security issues across your Amazon Web Services (AWS) workloads. Detective automatically extracts time-based events such as login attempts, API calls, and network traffic from AWS CloudTrail and Amazon Virtual Private Cloud (Amazon VPC) flow logs. It also extracts findings detected by Amazon GuardDuty.

The Detective API primarily supports the creation and management of behavior graphs. A behavior graph contains the extracted data from a set of member accounts, and is created and managed by an administrator account.

To add a member account to the behavior graph, the administrator account sends an invitation to the account. When the account accepts the invitation, it becomes a member account in the behavior graph.

Detective is also integrated with Organizations. The organization management account designates the Detective administrator account for the organization. That account becomes the administrator account for the organization behavior graph. The Detective administrator account is also the delegated administrator account for Detective in Organizations.

The Detective administrator account can enable any organization account as a member account in the organization behavior graph. The organization accounts do not receive invitations. The Detective administrator account can also invite other accounts to the organization behavior graph.

Every behavior graph is specific to a Region. You can only use the API to manage behavior graphs that belong to the Region that is associated with the currently selected endpoint.

The administrator account for a behavior graph can use the Detective API to do the following:

- Enable and disable Detective. Enabling Detective creates a new behavior graph.
- View the list of member accounts in a behavior graph.
- Add member accounts to a behavior graph.
- Remove member accounts from a behavior graph.
- Apply tags to a behavior graph.

The organization management account can use the Detective API to select the delegated administrator for Detective.

The Detective administrator account for an organization can use the Detective API to do the following:

- Perform all of the functions of an administrator account.
- Determine whether to automatically enable new organization accounts as member accounts in the organization behavior graph.

An invited member account can use the Detective API to do the following:

- View the list of behavior graphs that they are invited to.
- Accept an invitation to contribute to a behavior graph.
- Decline an invitation to contribute to a behavior graph.
- Remove their account from a behavior graph.

All API actions are logged as CloudTrail events. See Logging Detective API Calls with CloudTrail.

Note

We replaced the term "master account" with the term "administrator account". An administrator account is used to centrally manage multiple accounts. In the case of Detective, the administrator account manages the accounts in their behavior graph.

This document was last published on July 2, 2024.

Actions

The following actions are supported:

- AcceptInvitation
- BatchGetGraphMemberDatasources
- BatchGetMembershipDatasources
- CreateGraph
- CreateMembers
- DeleteGraph
- DeleteMembers
- DescribeOrganizationConfiguration
- DisableOrganizationAdminAccount
- DisassociateMembership
- EnableOrganizationAdminAccount
- GetInvestigation
- GetMembers
- ListDatasourcePackages
- ListGraphs
- ListIndicators
- ListInvestigations
- ListInvitations
- ListMembers
- ListOrganizationAdminAccounts
- ListTagsForResource
- RejectInvitation
- StartInvestigation
- StartMonitoringMember
- TagResource
- UntagResource
- UpdateDatasourcePackages

- UpdateInvestigationState
- UpdateOrganizationConfiguration

AcceptInvitation

Accepts an invitation for the member account to contribute data to a behavior graph. This operation can only be called by an invited member account.

The request provides the ARN of behavior graph.

The member account status in the graph must be `INVITED`.

Request Syntax

```
PUT /invitation HTTP/1.1
Content-type: application/json

{
   "GraphArn": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

GraphArn

The ARN of the behavior graph that the member account is accepting the invitation for.

The member account status in the behavior graph must be `INVITED`.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

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 Errors.

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

ConflictException

The request attempted an invalid action.

HTTP Status Code: 409

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of AcceptInvitation.

Sample Request

```
PUT /invitation HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 94
Authorization: AUTHPARAMS
X-Amz-Date: 20200124T163018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
 "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
}
```

Example

This example illustrates one usage of AcceptInvitation.

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 0
Date: Fri, 24 Jan 2020 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive
```

See Also

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

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

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

BatchGetGraphMemberDatasources

Gets data source package information for the behavior graph.

Request Syntax

```
POST /graph/datasources/get HTTP/1.1
Content-type: application/json

{
   "AccountIds": [ "string" ],
   "GraphArn": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

AccountIds

The list of AWS accounts to get data source package information on.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Length Constraints: Fixed length of 12.

Pattern: `^[0-9]+$`

Required: Yes

GraphArn

The ARN of the behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: Yes

Response Syntax

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

{
   "MemberDatasources": [
      {
         "AccountId": "string",
         "DatasourcePackageIngestHistory": {
            "string" : {
               "string" : {
                  "Timestamp": "string"
               }
            }
         },
         "GraphArn": "string"
      }
   ],
   "UnprocessedAccounts": [
      {
         "AccountId": "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.

MemberDatasources

Details on the status of data source packages for members of the behavior graph.

Type: Array of MembershipDatasources objects

UnprocessedAccounts

Accounts that data source package information could not be retrieved for.

Type: Array of UnprocessedAccount objects

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of BatchGetGraphMemberDatasources.

Sample Request

```
GET /graph/datasources/get HTTP/1.1
```

```
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: gzip, deflate, br
Content-Length: 94
Authorization: AUTHPARAMS
X-Amz-Date: 20220511T171741Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
  "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:1a8ef4ba50e74440b4b3c0d4a32ef48b",
  "AccountIds": ["379346275224"]
}
```

Example

This example illustrates one usage of BatchGetGraphMemberDatasources.

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 596
Date: Wed, 11 May 2022 17:17:41 GMT
x-amzn-RequestId: ddce670a-02cf-4993-9bb7-72e05c2d08f1
Connection: Keep-alive

{
  "MemberDatasources": [
    {
      "AccountId": "379346275224",
      "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:1a8ef4ba50e74440b4b3c0d4a32ef48b",
      "DatasourcePackageIngestHistory": {
        "DETECTIVE_CORE": {
          "STOPPED": null,
          "STARTED": {
            "Timestamp": "2022-05-05T18:56:33.656Z"
          }
        },
        "EKS_AUDIT": {
          "STOPPED": {
            "Timestamp": "2022-05-05T19:00:12.621Z"
          },
```

```
          "STARTED": {
            "Timestamp": "2022-05-05T18:56:33.656Z"
          }
        },
         "ASFF_SECURITYHUB_FINDING": {
          "STOPPED":{
            "Timestamp":"2023-05-15T12:47:23.975Z"
          },
          "STARTED":{
            "Timestamp":"2023-05-15T12:46:11.488Z"
          }
        }
      }
    }
  ],
  "UnprocessedAccounts": []
}
```

See Also

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

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

BatchGetMembershipDatasources

Gets information on the data source package history for an account.

Request Syntax

```
POST /membership/datasources/get HTTP/1.1
Content-type: application/json

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

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

GraphArns

The ARN of the behavior graph.

Type: Array of strings

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

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: Yes

Response Syntax

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

```
{
   "MembershipDatasources": [
      {
         "AccountId": "string",
         "DatasourcePackageIngestHistory": {
            "string" : {
               "string" : {
                  "Timestamp": "string"
               }
            }
         },
         "GraphArn": "string"
      }
   ],
   "UnprocessedGraphs": [
      {
         "GraphArn": "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.

MembershipDatasources

Details on the data source package history for an member of the behavior graph.

Type: Array of MembershipDatasources objects

UnprocessedGraphs

Graphs that data source package information could not be retrieved for.

Type: Array of UnprocessedGraph objects

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of BatchGetMembershipDatasources.

Sample Request

```
GET /membership/datasources/get HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: gzip, deflate, br
Content-Length: 94
Authorization: AUTHPARAMS
X-Amz-Date: 20220511T171741Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
  "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:1a8ef4ba50e74440b4b3c0d4a32ef48b"
}
```

Example

This example illustrates one usage of BatchGetMembershipDatasources.

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 681
Date: Wed, 11 May 2022 17:17:41 GMT
x-amzn-RequestId: ddce670a-02cf-4993-9bb7-72e05c2d08f1
Connection: Keep-alive

{
   "MembershipDatasources":[
      {
         "AccountId":"379346275224",
         "GraphArn":"arn:aws:detective:us-
east-1:111122223333:graph:1a8ef4ba50e74440b4b3c0d4a32ef48b",
         "DatasourcePackageIngestHistory":{
            "DETECTIVE_CORE":{
               "STOPPED":null,
               "STARTED":{
                  "Timestamp":"2022-05-05T18:56:33.656Z"
               }
            },
            "EKS_AUDIT":{
               "STOPPED":{
                  "Timestamp":"2022-05-05T19:00:12.621Z"
               },
               "STARTED":{
                  "Timestamp":"2022-05-05T18:56:33.656Z"
               }
            },
            "ASFF_SECURITYHUB_FINDING":{
               "STOPPED":{
                  "Timestamp":"2023-05-15T12:47:23.975Z"
               },
               "STARTED":{
                  "Timestamp":"2023-05-15T12:46:11.488Z"
               }
            }
         }
      }
```

```
    ],
    "UnprocessedGraphs":[

    ]
}
```

See Also

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

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

CreateGraph

Creates a new behavior graph for the calling account, and sets that account as the administrator account. This operation is called by the account that is enabling Detective.

The operation also enables Detective for the calling account in the currently selected Region. It returns the ARN of the new behavior graph.

`CreateGraph` triggers a process to create the corresponding data tables for the new behavior graph.

An account can only be the administrator account for one behavior graph within a Region. If the same account calls `CreateGraph` with the same administrator account, it always returns the same behavior graph ARN. It does not create a new behavior graph.

Request Syntax

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

{
   "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.

Tags

The tags to assign to the new behavior graph. You can add up to 50 tags. For each tag, you provide the tag key and the tag value. Each tag key can contain up to 128 characters. Each tag value can contain up to 256 characters.

Type: String to string map

Map Entries: Maximum number of 50 items.

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

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

Value Length Constraints: Maximum length of 256.

Required: No

Response Syntax

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

{
   "GraphArn": "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.

GraphArn

The ARN of the new behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

ConflictException

The request attempted an invalid action.

HTTP Status Code: 409

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ServiceQuotaExceededException

This request cannot be completed for one of the following reasons.

- This request cannot be completed if it would cause the number of member accounts in the behavior graph to exceed the maximum allowed. A behavior graph cannot have more than 1,200 member accounts.
- This request cannot be completed if the current volume ingested is above the limit of 10 TB per day. Detective will not allow you to add additional member accounts.

HTTP Status Code: 402

Examples

Example

This example illustrates one usage of CreateGraph.

Sample Request

```
POST /graph HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 50
Authorization: AUTHPARAMS
X-Amz-Date: 20200122T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
   "Tags": {
```

```
      "Department" : "Finance"
   }
}
```

Example

This example illustrates one usage of CreateGraph.

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 94
Date: Wed, 22 Jan 2020 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive

{
 "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
}
```

See Also

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

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

CreateMembers

`CreateMembers` is used to send invitations to accounts. For the organization behavior graph, the Detective administrator account uses `CreateMembers` to enable organization accounts as member accounts.

For invited accounts, `CreateMembers` sends a request to invite the specified AWS accounts to be member accounts in the behavior graph. This operation can only be called by the administrator account for a behavior graph.

`CreateMembers` verifies the accounts and then invites the verified accounts. The administrator can optionally specify to not send invitation emails to the member accounts. This would be used when the administrator manages their member accounts centrally.

For organization accounts in the organization behavior graph, `CreateMembers` attempts to enable the accounts. The organization accounts do not receive invitations.

The request provides the behavior graph ARN and the list of accounts to invite or to enable.

The response separates the requested accounts into two lists:

- The accounts that `CreateMembers` was able to process. For invited accounts, includes member accounts that are being verified, that have passed verification and are to be invited, and that have failed verification. For organization accounts in the organization behavior graph, includes accounts that can be enabled and that cannot be enabled.
- The accounts that `CreateMembers` was unable to process. This list includes accounts that were already invited to be member accounts in the behavior graph.

Request Syntax

```
POST /graph/members HTTP/1.1
Content-type: application/json

{
   "Accounts": [
      {
         "AccountId": "string",
         "EmailAddress": "string"
      }
```

```
    ],
    "DisableEmailNotification": boolean,
    "GraphArn": "string",
    "Message": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

Accounts

The list of AWS accounts to invite or to enable. You can invite or enable up to 50 accounts at a time. For each invited account, the account list contains the account identifier and the AWS account root user email address. For organization accounts in the organization behavior graph, the email address is not required.

Type: Array of Account objects

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

Required: Yes

DisableEmailNotification

if set to `true`, then the invited accounts do not receive email notifications. By default, this is set to `false`, and the invited accounts receive email notifications.

Organization accounts in the organization behavior graph do not receive email notifications.

Type: Boolean

Required: No

GraphArn

The ARN of the behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: Yes

Message

Customized message text to include in the invitation email message to the invited member accounts.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1000.

Required: No

Response Syntax

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

{
   "Members": [
      {
         "AccountId": "string",
         "AdministratorId": "string",
         "DatasourcePackageIngestStates": {
            "string" : "string"
         },
         "DisabledReason": "string",
         "EmailAddress": "string",
         "GraphArn": "string",
         "InvitationType": "string",
         "InvitedTime": "string",
         "MasterId": "string",
         "PercentOfGraphUtilization": number,
         "PercentOfGraphUtilizationUpdatedTime": "string",
         "Status": "string",
         "UpdatedTime": "string",
         "VolumeUsageByDatasourcePackage": {
            "string" : {
               "VolumeUsageInBytes": number,
               "VolumeUsageUpdateTime": "string"
```

```
            }
         },
         "VolumeUsageInBytes": number,
         "VolumeUsageUpdatedTime": "string"
      }
   ],
   "UnprocessedAccounts": [
      {
         "AccountId": "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.

Members

The set of member account invitation or enablement requests that Detective was able to process. This includes accounts that are being verified, that failed verification, and that passed verification and are being sent an invitation or are being enabled.

Type: Array of MemberDetail objects

UnprocessedAccounts

The list of accounts for which Detective was unable to process the invitation or enablement request. For each account, the list provides the reason why the request could not be processed. The list includes accounts that are already member accounts in the behavior graph.

Type: Array of UnprocessedAccount objects

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ServiceQuotaExceededException

This request cannot be completed for one of the following reasons.

- This request cannot be completed if it would cause the number of member accounts in the behavior graph to exceed the maximum allowed. A behavior graph cannot have more than 1,200 member accounts.
- This request cannot be completed if the current volume ingested is above the limit of 10 TB per day. Detective will not allow you to add additional member accounts.

HTTP Status Code: 402

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of CreateMembers.

Sample Request

```
PUT /graph/members HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 442
```

```
Authorization: AUTHPARAMS
X-Amz-Date: 20200123T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
 "Accounts": [
 {
  "AccountId": "444455556666",
  "EmailAddress": "mmajor@example.com"
 },
 {
  "AccountId": "123456789012",
  "EmailAddress": "jstiles@example.com"
 }
 ],
 "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
 "Message": "This is Paul Santos. I need to add your account to the data we use
 for security investigation in Detective. If you have any questions, contact me at
 psantos@example.com."
}
```

Example

This example illustrates one usage of CreateMembers.

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 625
Date: Thu, 23 Jan 2020 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive

{
 "Members": [
 {
  "AccountId": "444455556666",
  "AdministratorId": "111122223333",
  "EmailAddress": "mmajor@example.com",
  "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
  "InvitedTime": "2020-01-24T12:35:0.1587Z",
```

```
  "MasterId": "111122223333",
  "Status": "INVITED",
  "UpdatedTime": "2020-01-24T12:35:0.1587Z"
 },
 {
  "AccountId": "123456789012",
  "AdministratorId": "111122223333",
  "EmailAddress": "jstiles@example.com",
  "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
  "InvitedTime": "2020-01-24T12:35:0.1587Z",
  "MasterId": "111122223333",
  "Status": "VERIFICATION_IN_PROGRESS",
  "UpdatedTime": "2020-01-24T12:35:0.1587Z"
 }
 ],
 "UnprocessedAccounts": [ ]
}
```


See Also

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

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

DeleteGraph

Disables the specified behavior graph and queues it to be deleted. This operation removes the behavior graph from each member account's list of behavior graphs.

`DeleteGraph` can only be called by the administrator account for a behavior graph.

Request Syntax

```
POST /graph/removal HTTP/1.1
Content-type: application/json

{
   "GraphArn": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

GraphArn

The ARN of the behavior graph to disable.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

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 Errors.

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of DeleteGraph.

Sample Request

```
POST /graph/removal HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
```

```
Content-Length: 94
Authorization: AUTHPARAMS
X-Amz-Date: 20200221T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
 "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
}
```

Example

This example illustrates one usage of DeleteGraph.

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 0
Date: Fri, 21 Feb 2020 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive
```

See Also

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

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

DeleteMembers

Removes the specified member accounts from the behavior graph. The removed accounts no longer contribute data to the behavior graph. This operation can only be called by the administrator account for the behavior graph.

For invited accounts, the removed accounts are deleted from the list of accounts in the behavior graph. To restore the account, the administrator account must send another invitation.

For organization accounts in the organization behavior graph, the Detective administrator account can always enable the organization account again. Organization accounts that are not enabled as member accounts are not included in the `ListMembers` results for the organization behavior graph.

An administrator account cannot use `DeleteMembers` to remove their own account from the behavior graph. To disable a behavior graph, the administrator account uses the `DeleteGraph` API method.

Request Syntax

```
POST /graph/members/removal HTTP/1.1
Content-type: application/json

{
   "AccountIds": [ "string" ],
   "GraphArn": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

AccountIds

The list of AWS account identifiers for the member accounts to remove from the behavior graph. You can remove up to 50 member accounts at a time.

Type: Array of strings

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

Length Constraints: Fixed length of 12.

Pattern: `^[0-9]+$`

Required: Yes

GraphArn

The ARN of the behavior graph to remove members from.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: Yes

Response Syntax

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

{
   "AccountIds": [ "string" ],
   "UnprocessedAccounts": [
      {
         "AccountId": "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.

AccountIds

The list of AWS account identifiers for the member accounts that Detective successfully removed from the behavior graph.

Type: Array of strings

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

Length Constraints: Fixed length of 12.

Pattern: `^[0-9]+$`

UnprocessedAccounts

The list of member accounts that Detective was not able to remove from the behavior graph. For each member account, provides the reason that the deletion could not be processed.

Type: Array of UnprocessedAccount objects

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

ConflictException

The request attempted an invalid action.

HTTP Status Code: 409

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of DeleteMembers.

Sample Request

```
POST /graph/members/removal HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 128
Authorization: AUTHPARAMS
X-Amz-Date: 20200220T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
 "AccountIds": [ "444455556666" ],
 "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
}
```

Example

This example illustrates one usage of DeleteMembers.

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 63
Date: Thu, 20 Feb 2020 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572

{
```

```
  "AccountIds": [ "444455556666" ],
  "UnprocessedAccounts": [ ]
}
```

See Also

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

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

DescribeOrganizationConfiguration

Returns information about the configuration for the organization behavior graph. Currently indicates whether to automatically enable new organization accounts as member accounts.

Can only be called by the Detective administrator account for the organization.

Request Syntax

```
POST /orgs/describeOrganizationConfiguration HTTP/1.1
Content-type: application/json

{
   "GraphArn": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

GraphArn

The ARN of the organization behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: Yes

Response Syntax

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

{
```

```
   "AutoEnable": boolean
}
```

Response Elements

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

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

AutoEnable

Indicates whether to automatically enable new organization accounts as member accounts in the organization behavior graph.

Type: Boolean

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

TooManyRequestsException

The request cannot be completed because too many other requests are occurring at the same time.

HTTP Status Code: 429

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of DescribeOrganizationConfiguration.

Sample Request

```
POST /orgs/describeOrganizationConfiguration HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 94
Authorization: AUTHPARAMS
X-Amz-Date: 20210923T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
 "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
}
```

Example

This example illustrates one usage of DescribeOrganizationConfiguration.

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 19
Date: Thu, 23 Sep 2021 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive

{
   "AutoEnable": true
}
```

See Also

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

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

DisableOrganizationAdminAccount

Removes the Detective administrator account in the current Region. Deletes the organization behavior graph.

Can only be called by the organization management account.

Removing the Detective administrator account does not affect the delegated administrator account for Detective in Organizations.

To remove the delegated administrator account in Organizations, use the Organizations API. Removing the delegated administrator account also removes the Detective administrator account in all Regions, except for Regions where the Detective administrator account is the organization management account.

Request Syntax

```
POST /orgs/disableAdminAccount HTTP/1.1
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

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 Errors.

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

TooManyRequestsException

The request cannot be completed because too many other requests are occurring at the same time.

HTTP Status Code: 429

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of DisableOrganizationAdminAccount.

Sample Request

```
POST /orgs/disableAdminAccount HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 0
Authorization: AUTHPARAMS
X-Amz-Date: 20210923T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33
```

Example

This example illustrates one usage of DisableOrganizationAdminAccount.

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 0
Date: Thu, 23 Sep 2021 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive
```

See Also

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

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

DisassociateMembership

Removes the member account from the specified behavior graph. This operation can only be called by an invited member account that has the ENABLED status.

`DisassociateMembership` cannot be called by an organization account in the organization behavior graph. For the organization behavior graph, the Detective administrator account determines which organization accounts to enable or disable as member accounts.

Request Syntax

```
POST /membership/removal HTTP/1.1
Content-type: application/json

{
   "GraphArn": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

GraphArn

The ARN of the behavior graph to remove the member account from.

The member account's member status in the behavior graph must be ENABLED.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

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 Errors.

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

ConflictException

The request attempted an invalid action.

HTTP Status Code: 409

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of DisassociateMembership.

Sample Request

```
POST /membership/removal HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 94
Authorization: AUTHPARAMS
X-Amz-Date: 20200221T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
 "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
}
```

Example

This example illustrates one usage of DisassociateMembership.

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 0
Date: Thu, 21 Feb 2020 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive
```

See Also

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

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

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

EnableOrganizationAdminAccount

Designates the Detective administrator account for the organization in the current Region.

If the account does not have Detective enabled, then enables Detective for that account and creates a new behavior graph.

Can only be called by the organization management account.

If the organization has a delegated administrator account in Organizations, then the Detective administrator account must be either the delegated administrator account or the organization management account.

If the organization does not have a delegated administrator account in Organizations, then you can choose any account in the organization. If you choose an account other than the organization management account, Detective calls Organizations to make that account the delegated administrator account for Detective. The organization management account cannot be the delegated administrator account.

Request Syntax

```
POST /orgs/enableAdminAccount HTTP/1.1
Content-type: application/json

{
   "AccountId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

AccountId

The AWS account identifier of the account to designate as the Detective administrator account for the organization.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `^[0-9]+$`

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

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

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

TooManyRequestsException

The request cannot be completed because too many other requests are occurring at the same time.

HTTP Status Code: 429

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of EnableOrganizationAdminAccount.

Sample Request

```
POST /orgs/enableAdminAccount HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 28
Authorization: AUTHPARAMS
X-Amz-Date: 20210923T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
   "AccountId": "111122223333"
}
```

Example

This example illustrates one usage of EnableOrganizationAdminAccount.

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 0
Date: Thu, 23 Sep 2021 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive
```

See Also

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

- AWS Command Line Interface

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetInvestigation

Detective investigations lets you investigate IAM users and IAM roles using indicators of compromise. An indicator of compromise (IOC) is an artifact observed in or on a network, system, or environment that can (with a high level of confidence) identify malicious activity or a security incident. `GetInvestigation` returns the investigation results of an investigation for a behavior graph.

Request Syntax

```
POST /investigations/getInvestigation HTTP/1.1
Content-type: application/json

{
   "GraphArn": "string",
   "InvestigationId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

GraphArn

The Amazon Resource Name (ARN) of the behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: Yes

InvestigationId

The investigation ID of the investigation report.

Type: String

Length Constraints: Fixed length of 21.

Pattern: ^[0-9]+$

Required: Yes

Response Syntax

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

{
   "CreatedTime": "string",
   "EntityArn": "string",
   "EntityType": "string",
   "GraphArn": "string",
   "InvestigationId": "string",
   "ScopeEndTime": "string",
   "ScopeStartTime": "string",
   "Severity": "string",
   "State": "string",
   "Status": "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.

CreatedTime

The creation time of the investigation report in UTC time stamp format.

Type: Timestamp

EntityArn

The unique Amazon Resource Name (ARN). Detective supports IAM user ARNs and IAM role ARNs.

Type: String

Pattern: `^arn:.*`

EntityType

Type of entity. For example, AWS accounts, such as an IAM user and/or IAM role.

Type: String

Valid Values: `IAM_ROLE | IAM_USER`

GraphArn

The Amazon Resource Name (ARN) of the behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

InvestigationId

The investigation ID of the investigation report.

Type: String

Length Constraints: Fixed length of 21.

Pattern: `^[0-9]+$`

ScopeEndTime

The data and time when the investigation began. The value is an UTC ISO8601 formatted string. For example, `2021-08-18T16:35:56.284Z`.

Type: Timestamp

ScopeStartTime

The start date and time used to set the scope time within which you want to generate the investigation report. The value is an UTC ISO8601 formatted string. For example, `2021-08-18T16:35:56.284Z`.

Type: Timestamp

Severity

The severity assigned is based on the likelihood and impact of the indicators of compromise discovered in the investigation.

Type: String

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

State

The current state of the investigation. An archived investigation indicates that you have completed reviewing the investigation.

Type: String

Valid Values: `ACTIVE | ARCHIVED`

Status

The status based on the completion status of the investigation.

Type: String

Valid Values: `RUNNING | FAILED | SUCCESSFUL`

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

TooManyRequestsException

The request cannot be completed because too many other requests are occurring at the same time.

HTTP Status Code: 429

ValidationException

The request parameters are invalid.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetMembers

Returns the membership details for specified member accounts for a behavior graph.

Request Syntax

```
POST /graph/members/get HTTP/1.1
Content-type: application/json

{
   "AccountIds": [ "string" ],
   "GraphArn": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

AccountIds

The list of AWS account identifiers for the member account for which to return member details. You can request details for up to 50 member accounts at a time.

You cannot use `GetMembers` to retrieve information about member accounts that were removed from the behavior graph.

Type: Array of strings

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

Length Constraints: Fixed length of 12.

Pattern: `^[0-9]+$`

Required: Yes

GraphArn

The ARN of the behavior graph for which to request the member details.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: Yes

Response Syntax

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

{
   "MemberDetails": [
      {
         "AccountId": "string",
         "AdministratorId": "string",
         "DatasourcePackageIngestStates": {
            "string" : "string"
         },
         "DisabledReason": "string",
         "EmailAddress": "string",
         "GraphArn": "string",
         "InvitationType": "string",
         "InvitedTime": "string",
         "MasterId": "string",
         "PercentOfGraphUtilization": number,
         "PercentOfGraphUtilizationUpdatedTime": "string",
         "Status": "string",
         "UpdatedTime": "string",
         "VolumeUsageByDatasourcePackage": {
            "string" : {
               "VolumeUsageInBytes": number,
               "VolumeUsageUpdateTime": "string"
            }
         },
         "VolumeUsageInBytes": number,
         "VolumeUsageUpdatedTime": "string"
      }
```

```
    ],
    "UnprocessedAccounts": [
       {
          "AccountId": "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.

MemberDetails

The member account details that Detective is returning in response to the request.

Type: Array of MemberDetail objects

UnprocessedAccounts

The requested member accounts for which Detective was unable to return member details.

For each account, provides the reason why the request could not be processed.

Type: Array of UnprocessedAccount objects

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of GetMembers.

Sample Request

```
POST /graph/members/get HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 128
Authorization: AUTHPARAMS
X-Amz-Date: 20200127T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
 "AccountIds": [ "444455556666" ],
 "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
}
```

Example

This example illustrates one usage of GetMembers.

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json
```

```
Content-Length: 332
Date: Mon, 27 Jan 2020 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive

{
 "MemberDetails": [
 {
  "AccountId": "444455556666",
  "AdministratorId": "111122223333",
  "EmailAddress": "mmajor@example.com",
  "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
  "InvitedTime": "2020-01-24T12:35:0.1587Z",
  "MasterId": "111122223333",
  "Status": "INVITED",
  "UpdatedTime": "2020-01-24T12:35:0.1587Z"
 }
 ],
 "UnprocessedAccounts": [ ]
}
```

See Also

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

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

ListDatasourcePackages

Lists data source packages in the behavior graph.

Request Syntax

```
POST /graph/datasources/list HTTP/1.1
Content-type: application/json

{
   "GraphArn": "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.

GraphArn

The ARN of the behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: Yes

MaxResults

The maximum number of results to return.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 200.

Required: No

NextToken

For requests to get the next page of results, the pagination token that was returned with the previous set of results. The initial request does not include a pagination token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

Response Syntax

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

{
   "DatasourcePackages": {
      "string" : {
         "DatasourcePackageIngestState": "string",
         "LastIngestStateChange": {
            "string" : {
               "Timestamp": "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.

DatasourcePackages

Details on the data source packages active in the behavior graph.

Type: String to DatasourcePackageIngestDetail object map

Valid Keys: `DETECTIVE_CORE | EKS_AUDIT | ASFF_SECURITYHUB_FINDING`

NextToken

For requests to get the next page of results, the pagination token that was returned with the previous set of results. The initial request does not include a pagination token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of ListDatasourcePackages.

Sample Request

```
POST /graph/datasources/list HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: gzip, deflate, br
Content-Length: 94
Authorization: AUTHPARAMS
X-Amz-Date: 20220511T171741Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
  "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:1a8ef4ba50e74440b4b3c0d4a32ef48b"
}
```

Example

This example illustrates one usage of ListDatasourcePackages.

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 759
Date: Wed, 11 May 2022 17:17:41 GMT
x-amzn-RequestId: ddce670a-02cf-4993-9bb7-72e05c2d08f1
Connection: Keep-alive

{
   "DatasourcePackages":{
      "DETECTIVE_CORE":{
         "DatasourcePackageIngestState":"STARTED",
         "LastIngestStateChange":{
            "DISABLED":null,
            "STOPPED":null,
            "STARTED":{
               "Timestamp":"2022-01-03T15:25:39.865Z"
            }
         }
      },
      "EKS_AUDIT":{
         "DatasourcePackageIngestState":"STARTED",
         "LastIngestStateChange":{
```

```
            "DISABLED":null,
            "STOPPED":{
               "Timestamp":"2022-05-05T14:38:13.959Z"
            },
            "STARTED":{
               "Timestamp":"2022-05-05T14:38:47.379Z"
            }
         },
       "ASFF_SECURITYHUB_FINDING":{
         "DatasourcePackageIngestState":"STARTED",
         "LastIngestStateChange":{
            "DISABLED":null,
            "STOPPED":{
               "Timestamp":"2023-05-15T09:22:10.331Z"
            },
            "STARTED":{
               "Timestamp":"2022-05-15T09:22:55.020Z"
            }
         }
      }
   }
}
```


See Also

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

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

ListGraphs

Returns the list of behavior graphs that the calling account is an administrator account of. This operation can only be called by an administrator account.

Because an account can currently only be the administrator of one behavior graph within a Region, the results always contain a single behavior graph.

Request Syntax

```
POST /graphs/list 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 graphs to return at a time. The total must be less than the overall limit on the number of results to return, which is currently 200.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 200.

Required: No

NextToken

For requests to get the next page of results, the pagination token that was returned with the previous set of results. The initial request does not include a pagination token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

Response Syntax

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

{
   "GraphList": [
      {
         "Arn": "string",
         "CreatedTime": "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.

GraphList

A list of behavior graphs that the account is an administrator account for.

Type: Array of Graph objects

NextToken

If there are more behavior graphs remaining in the results, then this is the pagination token to use to request the next page of behavior graphs.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of ListGraphs.

Sample Request

```
POST /graphs/list HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 0
Authorization: AUTHPARAMS
X-Amz-Date: 20200123T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33
```

Example

This example illustrates one usage of ListGraphs.

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 144
Date: Thu, 23 Jan 2020 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive

{
 "GraphList": [
 {
  "Arn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
  "CreatedTime": "2020-01-22T11:35:11.372Z"
 }
 ]
}
```

See Also

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

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

ListIndicators

Gets the indicators from an investigation. You can use the information from the indicators to determine if an IAM user and/or IAM role is involved in an unusual activity that could indicate malicious behavior and its impact.

Request Syntax

```
POST /investigations/listIndicators HTTP/1.1
Content-type: application/json

{
   "GraphArn": "string",
   "IndicatorType": "string",
   "InvestigationId": "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.

GraphArn

The Amazon Resource Name (ARN) of the behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: Yes

IndicatorType

For the list of indicators of compromise that are generated by Detective investigations, see Detective investigations.

Type: String

Valid Values: `TTP_OBSERVED | IMPOSSIBLE_TRAVEL | FLAGGED_IP_ADDRESS | NEW_GEOLOCATION | NEW_ASO | NEW_USER_AGENT | RELATED_FINDING | RELATED_FINDING_GROUP`

Required: No

InvestigationId

The investigation ID of the investigation report.

Type: String

Length Constraints: Fixed length of 21.

Pattern: `^[0-9]+$`

Required: Yes

MaxResults

Lists the maximum number of indicators in a page.

Type: Integer

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

Required: No

NextToken

Lists if there are more results available. The value of nextToken is a unique pagination token for each page. Repeat the call using the returned token to retrieve the next page. Keep all other arguments unchanged.

Each pagination token expires after 24 hours. Using an expired pagination token will return a Validation Exception error.

Type: String

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

Required: No

Response Syntax

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

{
   "GraphArn": "string",
   "Indicators": [
      {
         "IndicatorDetail": {
            "FlaggedIpAddressDetail": {
               "IpAddress": "string",
               "Reason": "string"
            },
            "ImpossibleTravelDetail": {
               "EndingIpAddress": "string",
               "EndingLocation": "string",
               "HourlyTimeDelta": number,
               "StartingIpAddress": "string",
               "StartingLocation": "string"
            },
            "NewAsoDetail": {
               "Aso": "string",
               "IsNewForEntireAccount": boolean
            },
            "NewGeolocationDetail": {
               "IpAddress": "string",
               "IsNewForEntireAccount": boolean,
               "Location": "string"
            },
            "NewUserAgentDetail": {
               "IsNewForEntireAccount": boolean,
               "UserAgent": "string"
            },
            "RelatedFindingDetail": {
               "Arn": "string",
               "IpAddress": "string",
               "Type": "string"
            },
            "RelatedFindingGroupDetail": {
               "Id": "string"
            },
            "TTPsObservedDetail": {
```

```
                "APIFailureCount": number,
                "APIName": "string",
                "APISuccessCount": number,
                "IpAddress": "string",
                "Procedure": "string",
                "Tactic": "string",
                "Technique": "string"
            }
        },
        "IndicatorType": "string"
    }
  ],
  "InvestigationId": "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.

GraphArn

The Amazon Resource Name (ARN) of the behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Indicators

Lists the indicators of compromise.

Type: Array of Indicator objects

InvestigationId

The investigation ID of the investigation report.

Type: String

Length Constraints: Fixed length of 21.

Pattern: ^[0-9]+$

NextToken

Lists if there are more results available. The value of nextToken is a unique pagination token for each page. Repeat the call using the returned token to retrieve the next page. Keep all other arguments unchanged.

Each pagination token expires after 24 hours. Using an expired pagination token will return a Validation Exception error.

Type: String

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

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

TooManyRequestsException

The request cannot be completed because too many other requests are occurring at the same time.

HTTP Status Code: 429

ValidationException

The request parameters are invalid.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListInvestigations

Detective investigations lets you investigate IAM users and IAM roles using indicators of compromise. An indicator of compromise (IOC) is an artifact observed in or on a network, system, or environment that can (with a high level of confidence) identify malicious activity or a security incident. `ListInvestigations` lists all active Detective investigations.

Request Syntax

```
POST /investigations/listInvestigations HTTP/1.1
Content-type: application/json

{
   "FilterCriteria": {
      "CreatedTime": {
         "EndInclusive": "string",
         "StartInclusive": "string"
      },
      "EntityArn": {
         "Value": "string"
      },
      "Severity": {
         "Value": "string"
      },
      "State": {
         "Value": "string"
      },
      "Status": {
         "Value": "string"
      }
   },
   "GraphArn": "string",
   "MaxResults": number,
   "NextToken": "string",
   "SortCriteria": {
      "Field": "string",
      "SortOrder": "string"
   }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

FilterCriteria

Filters the investigation results based on a criteria.

Type: FilterCriteria object

Required: No

GraphArn

The Amazon Resource Name (ARN) of the behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: Yes

MaxResults

Lists the maximum number of investigations in a page.

Type: Integer

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

Required: No

NextToken

Lists if there are more results available. The value of nextToken is a unique pagination token for each page. Repeat the call using the returned token to retrieve the next page. Keep all other arguments unchanged.

Each pagination token expires after 24 hours. Using an expired pagination token will return a Validation Exception error.

Type: String

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

Required: No

SortCriteria

Sorts the investigation results based on a criteria.

Type: SortCriteria object

Required: No

Response Syntax

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

{
   "InvestigationDetails": [
      {
         "CreatedTime": "string",
         "EntityArn": "string",
         "EntityType": "string",
         "InvestigationId": "string",
         "Severity": "string",
         "State": "string",
         "Status": "string"
      }
   ],
   "NextToken": "string"
}
```

Response Elements

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

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

InvestigationDetails

Lists the summary of uncommon behavior or malicious activity which indicates a compromise.

Type: Array of InvestigationDetail objects

NextToken

Lists if there are more results available. The value of nextToken is a unique pagination token for each page. Repeat the call using the returned token to retrieve the next page. Keep all other arguments unchanged.

Each pagination token expires after 24 hours.

Type: String

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

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

TooManyRequestsException

The request cannot be completed because too many other requests are occurring at the same time.

HTTP Status Code: 429

ValidationException

The request parameters are invalid.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListInvitations

Retrieves the list of open and accepted behavior graph invitations for the member account. This operation can only be called by an invited member account.

Open invitations are invitations that the member account has not responded to.

The results do not include behavior graphs for which the member account declined the invitation. The results also do not include behavior graphs that the member account resigned from or was removed from.

Request Syntax

```
POST /invitations/list 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 behavior graph invitations to return in the response. The total must be less than the overall limit on the number of results to return, which is currently 200.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 200.

Required: No

NextToken

For requests to retrieve the next page of results, the pagination token that was returned with the previous page of results. The initial request does not include a pagination token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

Response Syntax

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

{
   "Invitations": [
      {
         "AccountId": "string",
         "AdministratorId": "string",
         "DatasourcePackageIngestStates": {
            "string" : "string"
         },
         "DisabledReason": "string",
         "EmailAddress": "string",
         "GraphArn": "string",
         "InvitationType": "string",
         "InvitedTime": "string",
         "MasterId": "string",
         "PercentOfGraphUtilization": number,
         "PercentOfGraphUtilizationUpdatedTime": "string",
         "Status": "string",
         "UpdatedTime": "string",
         "VolumeUsageByDatasourcePackage": {
            "string" : {
               "VolumeUsageInBytes": number,
               "VolumeUsageUpdateTime": "string"
            }
         },
         "VolumeUsageInBytes": number,
         "VolumeUsageUpdatedTime": "string"
      }
```

```
    ],
    "NextToken": "string"
}
```

Response Elements

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

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

Invitations

The list of behavior graphs for which the member account has open or accepted invitations.

Type: Array of MemberDetail objects

NextToken

If there are more behavior graphs remaining in the results, then this is the pagination token to use to request the next page of behavior graphs.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of ListInvitations.

Sample Request

```
POST /invitations/list HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 0
Authorization: AUTHPARAMS
X-Amz-Date: 20200124T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33
```

Example

This example illustrates one usage of ListInvitations.

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 302
Date: Fri, 24 Jan 2020 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive

{
 "Invitations": [
 {
  "AccountId": "444455556666",
  "AdministratorId": "111122223333",
  "EmailAddress": "mmajor@example.com",
  "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
  "InvitedTime": "2020-01-24T12:35:0.1587Z",
  "MasterId": "111122223333",
  "Status": "INVITED",
```

```
   "UpdatedTime": "2020-01-24T12:35:0.1587Z"
  }
  ]
}
```

See Also

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

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

ListMembers

Retrieves the list of member accounts for a behavior graph.

For invited accounts, the results do not include member accounts that were removed from the behavior graph.

For the organization behavior graph, the results do not include organization accounts that the Detective administrator account has not enabled as member accounts.

Request Syntax

```
POST /graph/members/list HTTP/1.1
Content-type: application/json

{
   "GraphArn": "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.

GraphArn

The ARN of the behavior graph for which to retrieve the list of member accounts.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: Yes

MaxResults

The maximum number of member accounts to include in the response. The total must be less than the overall limit on the number of results to return, which is currently 200.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 200.

Required: No

NextToken

For requests to retrieve the next page of member account results, the pagination token that was returned with the previous page of results. The initial request does not include a pagination token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

Response Syntax

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

{
   "MemberDetails": [
      {
         "AccountId": "string",
         "AdministratorId": "string",
         "DatasourcePackageIngestStates": {
            "string" : "string"
         },
         "DisabledReason": "string",
         "EmailAddress": "string",
         "GraphArn": "string",
         "InvitationType": "string",
         "InvitedTime": "string",
         "MasterId": "string",
         "PercentOfGraphUtilization": number,
```

```
            "PercentOfGraphUtilizationUpdatedTime": "string",
            "Status": "string",
            "UpdatedTime": "string",
            "VolumeUsageByDatasourcePackage": {
               "string" : {
                  "VolumeUsageInBytes": number,
                  "VolumeUsageUpdateTime": "string"
               }
            },
            "VolumeUsageInBytes": number,
            "VolumeUsageUpdatedTime": "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.

MemberDetails

The list of member accounts in the behavior graph.

For invited accounts, the results include member accounts that did not pass verification and member accounts that have not yet accepted the invitation to the behavior graph. The results do not include member accounts that were removed from the behavior graph.

For the organization behavior graph, the results do not include organization accounts that the Detective administrator account has not enabled as member accounts.

Type: Array of MemberDetail objects

NextToken

If there are more member accounts remaining in the results, then use this pagination token to request the next page of member accounts.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of ListMembers.

Sample Request

```
POST /graph/members/list HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 94
Authorization: AUTHPARAMS
X-Amz-Date: 20200124T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33
```

```
{
 "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
}
```

Example

This example illustrates one usage of ListMembers.

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 586
Date: Fri, 24 Jan 2020 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive

{
 "MemberDetails": [
 {
  "AccountId": "444455556666",
  "AdministratorId": "111122223333",
  "EmailAddress": "mmajor@example.com",
  "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
  "InvitedTime": "2020-01-24T12:35:0.1587Z",
  "MasterId": "111122223333",
  "PercentOfGraphUtilization": 5,
  "PercentOfGraphUtilizationUpdatedTime": 1586287843,
  "Status": "INVITED",
  "UpdatedTime": "2020-01-24T12:35:0.1587Z",
  "VolumeUsageInBytes": 500,
  "VolumeUsageUpdatedTime": "2020-01-26T11:15:24.129Z"
 },
 {
  "AccountId": "123456789012",
  "AdministratorId": "111122223333",
  "EmailAddress": "jstiles@example.com",
  "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
  "InvitedTime": "2020-01-24T12:35:0.1587Z",
  "MasterId": "111122223333",
```

```
  "PercentOfGraphUtilization": 2,
  "PercentOfGraphUtilizationUpdatedTime": 1586287843,
  "Status": "ENABLED",
  "UpdatedTime": "2020-01-25T05:35:11.623Z",
  "VolumeUsageInBytes": 200,
  "VolumeUsageUpdatedTime": "2020-01-26T11:14:26.427Z"
 }
 ]
}
```

See Also

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

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

ListOrganizationAdminAccounts

Returns information about the Detective administrator account for an organization. Can only be called by the organization management account.

Request Syntax

```
POST /orgs/adminAccountslist 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.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 200.

Required: No

NextToken

For requests to get the next page of results, the pagination token that was returned with the previous set of results. The initial request does not include a pagination token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

Response Syntax

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

{
   "Administrators": [
      {
         "AccountId": "string",
         "DelegationTime": "string",
         "GraphArn": "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.

Administrators

The list of Detective administrator accounts.

Type: Array of Administrator objects

NextToken

If there are more accounts remaining in the results, then this is the pagination token to use to request the next page of accounts.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

TooManyRequestsException

The request cannot be completed because too many other requests are occurring at the same time.

HTTP Status Code: 429

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of ListOrganizationAdminAccounts.

Sample Request

```
POST /orgs/adminAccountslist HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 0
Authorization: AUTHPARAMS
X-Amz-Date: 20210923T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33
```

Example

This example illustrates one usage of ListOrganizationAdminAccounts.

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 173
Date: Thu, 23 Sep 2021 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive

{
   "Administrators": [
      {
         "AccountId": "111122223333",
         "DelegationTime": "2021-09-23T:14:17:40.812Z",
         "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
      }
   ]
}
```

See Also

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

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

ListTagsForResource

Returns the tag values that are assigned to a behavior graph.

Request Syntax

```
GET /tags/ResourceArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ResourceArn

The ARN of the behavior graph for which to retrieve the tag values.

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

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 tag values that are assigned to the behavior graph. The request returns up to 50 tag values.

Type: String to string map

Map Entries: Maximum number of 50 items.

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

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

Value Length Constraints: Maximum length of 256.

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of ListTagsForResource.

Sample Request

```
GET /tags/resourceArn HTTP/1.1
Content-Type: application/json
Content-Length: 94
Date: Fri, 24 Jan 2020 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive

{
 "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
}
```

Example

This example illustrates one usage of ListTagsForResource.

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 33
Date: Fri, 24 Jan 2020 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive

{
   "Tags": {
      "Department" : "Finance"
   }
}
```

See Also

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

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

RejectInvitation

Rejects an invitation to contribute the account data to a behavior graph. This operation must be called by an invited member account that has the `INVITED` status.

`RejectInvitation` cannot be called by an organization account in the organization behavior graph. In the organization behavior graph, organization accounts do not receive an invitation.

Request Syntax

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

{
   "GraphArn": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

GraphArn

The ARN of the behavior graph to reject the invitation to.

The member account's current member status in the behavior graph must be `INVITED`.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

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 Errors.

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

ConflictException

The request attempted an invalid action.

HTTP Status Code: 409

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of RejectInvitation.

Sample Request

```
POST /invitation/removal HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 94
Authorization: AUTHPARAMS
X-Amz-Date: 20200124T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
 "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
}
```

Example

This example illustrates one usage of RejectInvitation.

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 0
Date: Fri, 24 Jan 2020 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive
```

See Also

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

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

- AWS SDK for Python
- AWS SDK for Ruby V3

StartInvestigation

Detective investigations lets you investigate IAM users and IAM roles using indicators of compromise. An indicator of compromise (IOC) is an artifact observed in or on a network, system, or environment that can (with a high level of confidence) identify malicious activity or a security incident. `StartInvestigation` initiates an investigation on an entity in a behavior graph.

Request Syntax

```
POST /investigations/startInvestigation HTTP/1.1
Content-type: application/json

{
   "EntityArn": "string",
   "GraphArn": "string",
   "ScopeEndTime": "string",
   "ScopeStartTime": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

EntityArn

The unique Amazon Resource Name (ARN) of the IAM user and IAM role.

Type: String

Pattern: `^arn:.*`

Required: Yes

GraphArn

The Amazon Resource Name (ARN) of the behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: Yes

ScopeEndTime

The data and time when the investigation ended. The value is an UTC ISO8601 formatted string. For example, `2021-08-18T16:35:56.284Z`.

Type: Timestamp

Required: Yes

ScopeStartTime

The data and time when the investigation began. The value is an UTC ISO8601 formatted string. For example, `2021-08-18T16:35:56.284Z`.

Type: Timestamp

Required: Yes

Response Syntax

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

{
   "InvestigationId": "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.

InvestigationId

The investigation ID of the investigation report.

Type: String

Length Constraints: Fixed length of 21.

Pattern: `^[0-9]+$`

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

TooManyRequestsException

The request cannot be completed because too many other requests are occurring at the same time.

HTTP Status Code: 429

ValidationException

The request parameters are invalid.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartMonitoringMember

Sends a request to enable data ingest for a member account that has a status of ACCEPTED_BUT_DISABLED.

For valid member accounts, the status is updated as follows.

- If Detective enabled the member account, then the new status is ENABLED.
- If Detective cannot enable the member account, the status remains ACCEPTED_BUT_DISABLED.

Request Syntax

```
POST /graph/member/monitoringstate HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "GraphArn": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

AccountId

The account ID of the member account to try to enable.

The account must be an invited member account with a status of ACCEPTED_BUT_DISABLED.

Type: String

Length Constraints: Fixed length of 12.

Pattern: ^[0-9]+$

Required: Yes

GraphArn

The ARN of the behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

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 Errors.

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

ConflictException

The request attempted an invalid action.

HTTP Status Code: 409

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ServiceQuotaExceededException

This request cannot be completed for one of the following reasons.

- This request cannot be completed if it would cause the number of member accounts in the behavior graph to exceed the maximum allowed. A behavior graph cannot have more than 1,200 member accounts.
- This request cannot be completed if the current volume ingested is above the limit of 10 TB per day. Detective will not allow you to add additional member accounts.

HTTP Status Code: 402

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of StartMonitoringMember.

Sample Request

```
POST /graph/member/monitoringstate HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 127
Authorization: AUTHPARAMS
X-Amz-Date: 20200127T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
 "AccountId": "444455556666",
 "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
```

```
}
```

Example

This example illustrates one usage of StartMonitoringMember.

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 0
Date: Thu, 21 Feb 2020 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive
```

See Also

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

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

TagResource

Applies tag values to a behavior graph.

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 ARN of the behavior graph to assign the tags to.

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: Yes

Request Body

The request accepts the following data in JSON format.

Tags

The tags to assign to the behavior graph. You can add up to 50 tags. For each tag, you provide the tag key and the tag value. Each tag key can contain up to 128 characters. Each tag value can contain up to 256 characters.

Type: String to string map

Map Entries: Maximum number of 50 items.

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

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

Value Length Constraints: Maximum length of 256.

Required: Yes

Response Syntax

```
HTTP/1.1 204
```

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of TagResource.

Sample Request

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 126
Authorization: AUTHPARAMS
X-Amz-Date: 20200127T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
   "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
   "Tags": {
      "Department" : "Finance"
   }
}
```

Example

This example illustrates one usage of TagResource.

Sample Response

```
HTTP/1.1 204 OK
Content-Length: 0
Date: Thu, 25 Feb 2021 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive
```

See Also

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

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

UntagResource

Removes tags from a behavior graph.

Request Syntax

```
DELETE /tags/ResourceArn?tagKeys=TagKeys HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ResourceArn

The ARN of the behavior graph to remove the tags from.

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: Yes

TagKeys

The tag keys of the tags to remove from the behavior graph. You can remove up to 50 tags at a time.

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

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

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

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 204
```

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

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

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of UntagResource.

Sample Request

```
DELETE /tags/resourceArn?tagKeys=TagKeys HTTP/1.1
Content-type: application/json
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
```

```
Content-Length: 126
Authorization: AUTHPARAMS
X-Amz-Date: 20200127T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
   "ResourceArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
   "TagKeys": ["Department"]
}
```

Example

This example illustrates one usage of UntagResource.

Sample Response

```
HTTP/1.1 204 OK
Content-Length: 0
Date: Thu, 21 Feb 2020 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive
```

See Also

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

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

UpdateDatasourcePackages

Starts a data source package for the Detective behavior graph.

Request Syntax

```
POST /graph/datasources/update HTTP/1.1
Content-type: application/json

{
   "DatasourcePackages": [ "string" ],
   "GraphArn": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

DatasourcePackages

The data source package to start for the behavior graph.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 25 items.

Valid Values: `DETECTIVE_CORE | EKS_AUDIT | ASFF_SECURITYHUB_FINDING`

Required: Yes

GraphArn

The ARN of the behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

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 Errors.

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

ServiceQuotaExceededException

This request cannot be completed for one of the following reasons.

- This request cannot be completed if it would cause the number of member accounts in the behavior graph to exceed the maximum allowed. A behavior graph cannot have more than 1,200 member accounts.
- This request cannot be completed if the current volume ingested is above the limit of 10 TB per day. Detective will not allow you to add additional member accounts.

HTTP Status Code: 402

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of UpdateDatasourcePackages.

Sample Request

```
POST /graph/datasources/set HTTP/1.1
Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: gzip, deflate, br
Content-Length: 167
Authorization: AUTHPARAMS
X-Amz-Date: 20220511T171741Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
   "GraphArn":"arn:aws:detective:us-
east-1:111122223333:graph:1a8ef4ba50e74440b4b3c0d4a32ef48b",
   "DatasourcePackages":[
      "DETECTIVE_CORE",
      "EKS_AUDIT",
      "ASFF_SECURITYHUB_FINDING"
   ]
}
```

Example

This example illustrates one usage of UpdateDatasourcePackages.

Sample Response

```
Sample Response
HTTP/1.1 200 OK
Content-Length: 0
Date: Wed, 11 May 2022 17:17:41 GMT
```

```
x-amzn-RequestId: ddce670a-02cf-4993-9bb7-72e05c2d08f1
Connection: Keep-alive
```

See Also

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

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

UpdateInvestigationState

Updates the state of an investigation.

Request Syntax

```
POST /investigations/updateInvestigationState HTTP/1.1
Content-type: application/json

{
   "GraphArn": "string",
   "InvestigationId": "string",
   "State": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

GraphArn

The Amazon Resource Name (ARN) of the behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: Yes

InvestigationId

The investigation ID of the investigation report.

Type: String

Length Constraints: Fixed length of 21.

Pattern: `^[0-9]+$`

Required: Yes

State

The current state of the investigation. An archived investigation indicates you have completed reviewing the investigation.

Type: String

Valid Values: `ACTIVE | ARCHIVED`

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 Errors.

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

ResourceNotFoundException

The request refers to a nonexistent resource.

HTTP Status Code: 404

TooManyRequestsException

The request cannot be completed because too many other requests are occurring at the same time.

HTTP Status Code: 429

ValidationException

The request parameters are invalid.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateOrganizationConfiguration

Updates the configuration for the Organizations integration in the current Region. Can only be called by the Detective administrator account for the organization.

Request Syntax

```
POST /orgs/updateOrganizationConfiguration HTTP/1.1
Content-type: application/json

{
   "AutoEnable": boolean,
   "GraphArn": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

AutoEnable

Indicates whether to automatically enable new organization accounts as member accounts in the organization behavior graph.

Type: Boolean

Required: No

GraphArn

The ARN of the organization behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

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 Errors.

AccessDeniedException

The request issuer does not have permission to access this resource or perform this operation.

HTTP Status Code: 403

InternalServerException

The request was valid but failed because of a problem with the service.

HTTP Status Code: 500

TooManyRequestsException

The request cannot be completed because too many other requests are occurring at the same time.

HTTP Status Code: 429

ValidationException

The request parameters are invalid.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of UpdateOrganizationConfiguration.

Sample Request

```
POST /orgs/updateOrganizationConfiguration HTTP/1.1

Host: api.detective.us-west-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 112
Authorization: AUTHPARAMS
X-Amz-Date: 20210923T193018Z
User-Agent: aws-cli/1.14.29 Python/2.7.9 Windows/8 botocore/1.8.33

{
   "AutoEnable": true,
   "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
}
```

Example

This example illustrates one usage of UpdateOrganizationConfiguration.

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 0
Date: Thu, 23 Sep 2021 23:07:46 GMT
x-amzn-RequestId: 397d0549-0092-11e8-a0ee-a7f9aa6e7572
Connection: Keep-alive
```

See Also

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

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

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Data Types

The Amazon Detective 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:

- Account
- Administrator
- DatasourcePackageIngestDetail
- DatasourcePackageUsageInfo
- DateFilter
- FilterCriteria
- FlaggedIpAddressDetail
- Graph
- ImpossibleTravelDetail
- Indicator
- IndicatorDetail
- InvestigationDetail
- MemberDetail
- MembershipDatasources
- NewAsoDetail
- NewGeolocationDetail
- NewUserAgentDetail
- RelatedFindingDetail
- RelatedFindingGroupDetail
- SortCriteria

- StringFilter
- TimestampForCollection
- TTPsObservedDetail
- UnprocessedAccount
- UnprocessedGraph

Account

An AWS account that is the administrator account of or a member of a behavior graph.

Contents

AccountId

The account identifier of the AWS account.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `^[0-9]+$`

Required: Yes

EmailAddress

The AWS account root user email address for the AWS account.

Type: String

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

Pattern: `^.+@(?:(?:(?!-)[A-Za-z0-9-]{1,62})?[A-Za-z0-9]{1}\.)+[A-Za-z]{2,63}$`

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

Administrator

Information about the Detective administrator account for an organization.

Contents

AccountId

The AWS account identifier of the Detective administrator account for the organization.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `^[0-9]+$`

Required: No

DelegationTime

The date and time when the Detective administrator account was enabled. The value is an ISO8601 formatted string. For example, `2021-08-18T16:35:56.284Z`.

Type: Timestamp

Required: No

GraphArn

The ARN of the organization behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DatasourcePackageIngestDetail

Details about the data source packages ingested by your behavior graph.

Contents

DatasourcePackageIngestState

Details on which data source packages are ingested for a member account.

Type: String

Valid Values: `STARTED | STOPPED | DISABLED`

Required: No

LastIngestStateChange

The date a data source package was enabled for this account

Type: String to TimestampForCollection object map

Valid Keys: `STARTED | STOPPED | DISABLED`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DatasourcePackageUsageInfo

Information on the usage of a data source package in the behavior graph.

Contents

VolumeUsageInBytes

Total volume of data in bytes per day ingested for a given data source package.

Type: Long

Required: No

VolumeUsageUpdateTime

The data and time when the member account data volume was last updated. The value is an ISO8601 formatted string. For example, `2021-08-18T16:35:56.284Z`.

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

DateFilter

Contains details on the time range used to filter data.

Contents

EndInclusive

A timestamp representing the end date of the time period until when data is filtered, including the end date.

Type: Timestamp

Required: Yes

StartInclusive

A timestamp representing the start of the time period from when data is filtered, including the start date.

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

FilterCriteria

Details on the criteria used to define the filter for investigation results.

Contents

CreatedTime

Filter the investigation results based on when the investigation was created.

Type: DateFilter object

Required: No

EntityArn

Filter the investigation results based on the Amazon Resource Name (ARN) of the entity.

Type: StringFilter object

Required: No

Severity

Filter the investigation results based on the severity.

Type: StringFilter object

Required: No

State

Filter the investigation results based on the state.

Type: StringFilter object

Required: No

Status

Filter the investigation results based on the status.

Type: StringFilter 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

FlaggedIpAddressDetail

Contains information on suspicious IP addresses identified as indicators of compromise. This indicator is derived from AWS threat intelligence.

Contents

IpAddress

IP address of the suspicious entity.

Type: String

Required: No

Reason

Details the reason the IP address was flagged as suspicious.

Type: String

Valid Values: `AWS_THREAT_INTELLIGENCE`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Graph

A behavior graph in Detective.

Contents

Arn

The ARN of the behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: No

CreatedTime

The date and time that the behavior graph was created. The value is an ISO8601 formatted string. For example, `2021-08-18T16:35:56.284Z`.

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

ImpossibleTravelDetail

Contains information on unusual and impossible travel in an account.

Contents

EndingIpAddress

IP address where the resource was last used in the impossible travel.

Type: String

Required: No

EndingLocation

Location where the resource was last used in the impossible travel.

Type: String

Required: No

HourlyTimeDelta

Returns the time difference between the first and last timestamp the resource was used.

Type: Integer

Required: No

StartingIpAddress

IP address where the resource was first used in the impossible travel.

Type: String

Required: No

StartingLocation

Location where the resource was first used in the impossible travel.

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

Indicator

Detective investigations triages indicators of compromises such as a finding and surfaces only the most critical and suspicious issues, so you can focus on high-level investigations. An `Indicator` lets you determine if an AWS resource is involved in unusual activity that could indicate malicious behavior and its impact.

Contents

IndicatorDetail

Details about the indicators of compromise that are used to determine if a resource is involved in a security incident. An indicator of compromise (IOC) is an artifact observed in or on a network, system, or environment that can (with a high level of confidence) identify malicious activity or a security incident.

Type: IndicatorDetail object

Required: No

IndicatorType

The type of indicator.

Type: String

Valid Values: `TTP_OBSERVED | IMPOSSIBLE_TRAVEL | FLAGGED_IP_ADDRESS | NEW_GEOLOCATION | NEW_ASO | NEW_USER_AGENT | RELATED_FINDING | RELATED_FINDING_GROUP`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

IndicatorDetail

Details about the indicators of compromise which are used to determine if a resource is involved in a security incident. An indicator of compromise (IOC) is an artifact observed in or on a network, system, or environment that can (with a high level of confidence) identify malicious activity or a security incident. For the list of indicators of compromise that are generated by Detective investigations, see Detective investigations.

Contents

FlaggedIpAddressDetail

Suspicious IP addresses that are flagged, which indicates critical or severe threats based on threat intelligence by Detective. This indicator is derived from AWS threat intelligence.

Type: FlaggedIpAddressDetail object

Required: No

ImpossibleTravelDetail

Identifies unusual and impossible user activity for an account.

Type: ImpossibleTravelDetail object

Required: No

NewAsoDetail

Contains details about the new Autonomous System Organization (ASO).

Type: NewAsoDetail object

Required: No

NewGeolocationDetail

Contains details about the new geographic location.

Type: NewGeolocationDetail object

Required: No

NewUserAgentDetail

Contains details about the new user agent.

Type: NewUserAgentDetail object

Required: No

RelatedFindingDetail

Contains details about related findings.

Type: RelatedFindingDetail object

Required: No

RelatedFindingGroupDetail

Contains details about related finding groups.

Type: RelatedFindingGroupDetail object

Required: No

TTPsObservedDetail

Details about the indicator of compromise.

Type: TTPsObservedDetail 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

InvestigationDetail

Details about the investigation related to a potential security event identified by Detective.

Contents

CreatedTime

The time stamp of the creation time of the investigation report. The value is an UTC ISO8601 formatted string. For example, `2021-08-18T16:35:56.284Z`.

Type: Timestamp

Required: No

EntityArn

The unique Amazon Resource Name (ARN) of the IAM user and IAM role.

Type: String

Pattern: `^arn:.*`

Required: No

EntityType

Type of entity. For example, AWS accounts, such as IAM user and role.

Type: String

Valid Values: `IAM_ROLE | IAM_USER`

Required: No

InvestigationId

The investigation ID of the investigation report.

Type: String

Length Constraints: Fixed length of 21.

Pattern: `^[0-9]+$`

Required: No

Severity

Severity based on the likelihood and impact of the indicators of compromise discovered in the investigation.

Type: String

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

Required: No

State

The current state of the investigation. An archived investigation indicates you have completed reviewing the investigation.

Type: String

Valid Values: `ACTIVE | ARCHIVED`

Required: No

Status

Status based on the completion status of the investigation.

Type: String

Valid Values: `RUNNING | FAILED | SUCCESSFUL`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MemberDetail

Details about a member account in a behavior graph.

Contents

AccountId

The AWS account identifier for the member account.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `^[0-9]+$`

Required: No

AdministratorId

The AWS account identifier of the administrator account for the behavior graph.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `^[0-9]+$`

Required: No

DatasourcePackageIngestStates

The state of a data source package for the behavior graph.

Type: String to string map

Valid Keys: `DETECTIVE_CORE | EKS_AUDIT | ASFF_SECURITYHUB_FINDING`

Valid Values: `STARTED | STOPPED | DISABLED`

Required: No

DisabledReason

For member accounts with a status of `ACCEPTED_BUT_DISABLED`, the reason that the member account is not enabled.

The reason can have one of the following values:

- VOLUME_TOO_HIGH - Indicates that adding the member account would cause the data volume for the behavior graph to be too high.
- VOLUME_UNKNOWN - Indicates that Detective is unable to verify the data volume for the member account. This is usually because the member account is not enrolled in Amazon GuardDuty.

Type: String

Valid Values: VOLUME_TOO_HIGH | VOLUME_UNKNOWN

Required: No

EmailAddress

The AWS account root user email address for the member account.

Type: String

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

Pattern: ^.+@(?:(?:(?!-)[A-Za-z0-9-]{1,62})?[A-Za-z0-9]{1}\.)+[A-Za-z]{2,63}$

Required: No

GraphArn

The ARN of the behavior graph.

Type: String

Pattern: ^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$

Required: No

InvitationType

The type of behavior graph membership.

For an organization account in the organization behavior graph, the type is ORGANIZATION.

For an account that was invited to a behavior graph, the type is INVITATION.

Type: String

Valid Values: `INVITATION | ORGANIZATION`

Required: No

InvitedTime

For invited accounts, the date and time that Detective sent the invitation to the account. The value is an ISO8601 formatted string. For example, `2021-08-18T16:35:56.284Z`.

Type: Timestamp

Required: No

MasterId

This member has been deprecated.

The AWS account identifier of the administrator account for the behavior graph.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `^[0-9]+$`

Required: No

PercentOfGraphUtilization

This member has been deprecated.

The member account data volume as a percentage of the maximum allowed data volume. 0 indicates 0 percent, and 100 indicates 100 percent.

Note that this is not the percentage of the behavior graph data volume.

For example, the data volume for the behavior graph is 80 GB per day. The maximum data volume is 160 GB per day. If the data volume for the member account is 40 GB per day, then `PercentOfGraphUtilization` is 25. It represents 25% of the maximum allowed data volume.

Type: Double

Required: No

PercentOfGraphUtilizationUpdatedTime

This member has been deprecated.

The date and time when the graph utilization percentage was last updated. The value is an ISO8601 formatted string. For example, `2021-08-18T16:35:56.284Z`.

Type: Timestamp

Required: No

Status

The current membership status of the member account. The status can have one of the following values:

- `INVITED` - For invited accounts only. Indicates that the member was sent an invitation but has not yet responded.
- `VERIFICATION_IN_PROGRESS` - For invited accounts only, indicates that Detective is verifying that the account identifier and email address provided for the member account match. If they do match, then Detective sends the invitation. If the email address and account identifier don't match, then the member cannot be added to the behavior graph.

  For organization accounts in the organization behavior graph, indicates that Detective is verifying that the account belongs to the organization.
- `VERIFICATION_FAILED` - For invited accounts only. Indicates that the account and email address provided for the member account do not match, and Detective did not send an invitation to the account.
- `ENABLED` - Indicates that the member account currently contributes data to the behavior graph. For invited accounts, the member account accepted the invitation. For organization accounts in the organization behavior graph, the Detective administrator account enabled the organization account as a member account.
- `ACCEPTED_BUT_DISABLED` - The account accepted the invitation, or was enabled by the Detective administrator account, but is prevented from contributing data to the behavior graph. `DisabledReason` provides the reason why the member account is not enabled.

Invited accounts that declined an invitation or that were removed from the behavior graph are not included. In the organization behavior graph, organization accounts that the Detective administrator account did not enable are not included.

Type: String

Valid Values: `INVITED | VERIFICATION_IN_PROGRESS | VERIFICATION_FAILED | ENABLED | ACCEPTED_BUT_DISABLED`

Required: No

UpdatedTime

The date and time that the member account was last updated. The value is an ISO8601 formatted string. For example, `2021-08-18T16:35:56.284Z`.

Type: Timestamp

Required: No

VolumeUsageByDatasourcePackage

Details on the volume of usage for each data source package in a behavior graph.

Type: String to DatasourcePackageUsageInfo object map

Valid Keys: `DETECTIVE_CORE | EKS_AUDIT | ASFF_SECURITYHUB_FINDING`

Required: No

VolumeUsageInBytes

This member has been deprecated.

The data volume in bytes per day for the member account.

Type: Long

Required: No

VolumeUsageUpdatedTime

This member has been deprecated.

The data and time when the member account data volume was last updated. The value is an ISO8601 formatted string. For example, `2021-08-18T16:35:56.284Z`.

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

MembershipDatasources

Details on data source packages for members of the behavior graph.

Contents

AccountId

The account identifier of the AWS account.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `^[0-9]+$`

Required: No

DatasourcePackageIngestHistory

Details on when a data source package was added to a behavior graph.

Type: String to string to TimestampForCollection object map map

Valid Keys: `DETECTIVE_CORE | EKS_AUDIT | ASFF_SECURITYHUB_FINDING`

Valid Keys: `STARTED | STOPPED | DISABLED`

Required: No

GraphArn

The ARN of the organization behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NewAsoDetail

Details new Autonomous System Organizations (ASOs) used either at the resource or account level.

Contents

Aso

Details about the new Autonomous System Organization (ASO).

Type: String

Required: No

IsNewForEntireAccount

Checks if the Autonomous System Organization (ASO) is new for the entire account.

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

NewGeolocationDetail

Details new geolocations used either at the resource or account level. For example, lists an observed geolocation that is an infrequent or unused location based on previous user activity.

Contents

IpAddress

IP address using which the resource was accessed.

Type: String

Required: No

IsNewForEntireAccount

Checks if the geolocation is new for the entire account.

Type: Boolean

Required: No

Location

Location where the resource was accessed.

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

NewUserAgentDetail

Details new user agents used either at the resource or account level.

Contents

IsNewForEntireAccount

Checks if the user agent is new for the entire account.

Type: Boolean

Required: No

UserAgent

New user agent which accessed the resource.

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

RelatedFindingDetail

Details related activities associated with a potential security event. Lists all distinct categories of evidence that are connected to the resource or the finding group.

Contents

Arn

The Amazon Resource Name (ARN) of the related finding.

Type: String

Pattern: `^arn:.*`

Required: No

IpAddress

The IP address of the finding.

Type: String

Required: No

Type

The type of finding.

Type: String

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RelatedFindingGroupDetail

Details multiple activities as they related to a potential security event. Detective uses graph analysis technique that infers relationships between findings and entities, and groups them together as a finding group.

Contents

Id

The unique identifier for the finding group.

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

SortCriteria

Details about the criteria used for sorting investigations.

Contents

Field

Represents the `Field` attribute to sort investigations.

Type: String

Valid Values: `SEVERITY | STATUS | CREATED_TIME`

Required: No

SortOrder

The order by which the sorted findings are displayed.

Type: String

Valid Values: `ASC | DESC`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StringFilter

A string for filtering Detective investigations.

Contents

Value

The string filter value.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 500.

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

TimestampForCollection

Details on when data collection began for a source package.

Contents

Timestamp

The data and time when data collection began for a source package. The value is an ISO8601 formatted string. For example, `2021-08-18T16:35:56.284Z`.

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

TTPsObservedDetail

Details tactics, techniques, and procedures (TTPs) used in a potential security event. Tactics are based on MITRE ATT&CK Matrix for Enterprise.

Contents

APIFailureCount

The total number of failed API requests.

Type: Long

Required: No

APIName

The name of the API where the tactics, techniques, and procedure (TTP) was observed.

Type: String

Required: No

APISuccessCount

The total number of successful API requests.

Type: Long

Required: No

IpAddress

The IP address where the tactics, techniques, and procedure (TTP) was observed.

Type: String

Required: No

Procedure

The procedure used, identified by the investigation.

Type: String

Required: No

Tactic

The tactic used, identified by the investigation.

Type: String

Required: No

Technique

The technique used, identified by the investigation.

Type: String

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

UnprocessedAccount

A member account that was included in a request but for which the request could not be processed.

Contents

AccountId

The AWS account identifier of the member account that was not processed.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `^[0-9]+$`

Required: No

Reason

The reason that the member account request could not be processed.

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

UnprocessedGraph

Behavior graphs that could not be processed in the request.

Contents

GraphArn

The ARN of the organization behavior graph.

Type: String

Pattern: `^arn:aws[-\w]{0,10}?:detective:[-\w]{2,20}?:\d{12}?:graph:[abcdef\d]{32}?$`

Required: No

Reason

The reason data source package information could not be processed for a behavior graph.

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*.

Action

The action to be performed.

Type: string

Required: Yes

Version

The API version that the request is written for, expressed in the format YYYY-MM-DD.

Type: string

Required: Yes

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 Errors

This section lists the errors common to the API actions of all AWS services. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ExpiredTokenException

The security token included in the request is expired

HTTP Status Code: 403

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 403

InternalFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

MalformedHttpRequestException

Problems with the request at the HTTP level, e.g. we can't decompress the body according to the decompression algorithm specified by the content-encoding.

HTTP Status Code: 400

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 401

OptInRequired

The AWS access key ID needs a subscription for the service.

HTTP Status Code: 403

RequestAbortedException

Convenient exception that can be used when a request is aborted before a reply is sent back (e.g. client closed connection).

HTTP Status Code: 400

RequestEntityTooLargeException

Problems with the request at the HTTP level. The request entity is too large.

HTTP Status Code: 413

RequestExpired

The request reached the service more than 15 minutes after the date stamp on the request or more than 15 minutes after the request expiration date (such as for pre-signed URLs), or the date stamp on the request is more than 15 minutes in the future.

HTTP Status Code: 400

RequestTimeoutException

Problems with the request at the HTTP level. Reading the Request timed out.

HTTP Status Code: 408

ServiceUnavailable

The request has failed due to a temporary failure of the server.

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

UnrecognizedClientException

The X.509 certificate or AWS access key ID provided does not exist in our records.

HTTP Status Code: 403

UnknownOperationException

The action or operation requested is invalid. Verify that the action is typed correctly.

HTTP Status Code: 404

ValidationError

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

HTTP Status Code: 400