

Google Cloud

Documentation

>

Search

English

Console

Sign in

Google Security Operations

Guides

Reference

Resources

Contact Us

Start free

Filter

Google SecOps SIEM reference

Google SecOps permissions in IAM

Quotas and limits

Backstory API

Ingestion API

Migrate CBN alerts to YARA-L alerts

Migrate from CrowdStrike Detects API to Alerts API

YARA-L

SOAR data in dashboards

Reference lists

UDM field list

Key UDM fields for parsers

UDM usage guide

Supported data sets and default parsers

Parser syntax reference

Ingestion metrics table

Ingestion metrics reference for Looker and BigQuery

Events table in BigQuery

Chronicle API

Google SecOps SOAR reference

TIPCommon 2.1.0 library

Google SecOps Response integrations

Google SecOps SDK

Case Manipulation

Custom lists

Integration configuration and script parameters

SiemplifyAction module

SiemplifyConnectors module

SiemplifyDataModel module

SiemplifyJobs module

Siemplify module

ScriptResult module

REST API

<

Security > Google Security Operations > Reference

On this page

class SiemplifyAction.SiemplifyAction

add_alert_entities_to_custom_list

add_attachment

add_comment

add_entity_insight

add_entity_to_case

add_tag

any_alert_entities_in_custom_list

...

Send feedback

SiemplifyAction module

class SiemplifyAction.SiemplifyAction

SiemplifyAction.SiemplifyAction(mock_stdin=None, get_source_file=Fa

Bases: Siemplify

add_alert_entities_to_custom_list

add_alert_entities_to_custom_list(category_name)

Add the alert's entities to the custom list record with the given category.

Parameters

Param name	Param type	Definition	Possible values	Comments
category_name	{string}	Custom list category	"CustomList"	N/A

Returns

{[CustomList]} list of the added objects.

Example

Input: Explicitly, category_name. Implicitly, entities using scope. Running add_alert_entities_to_custom_list will result in a list of "CustomList" objects and a configuration change in the settings.

from SiemplifyAction import SiemplifyAction
siemplify = SiemplifyAction()
result = siemplify.add_alert_entities_to_custom_list("WhiteListed H

Result behavior

Adds the WhiteListed HOSTs category.

Result value

[<SiemplifyDataModel.CustomList object at 0x000000003476E10>, <Sie

add_attachment

```
add_attachment(file_path, case_id=None, alert_identifier=None, desc
```

Add an attachment to the case wall.

Parameters

Param name	Param type	Definition	Possible values
file_path	{string}	File path	"C:\Program Files (x86)\Google\Chrome\Application\chrom
case_id	{string}	Case identifier	234
alert_identifier	{string}	Alert identifier	12345
description	{string}	The description for the file	N/A
is_favorite	boolean	N/A	True/False

Returns

{long} attachment_id

Example

Input: Explicitly, File path, description, and `is_favorite`. Implicitly, `case_id` and `alert_identifier`.

```
from SiemplyfyAction import SiemplyfyAction
siemplyfy = SiemplyfyAction()
result = siemplyfy.add_attachment("C:\Program Files (x86)\Google\Ch
```

Result behavior

The file mentioned in the path will be attached to case ID 234 and the attachment ID will be returned.

Result value

5 [The attachment ID]

add_comment

```
add_comment(comment, case_id=None, alert_identifier=None)
```

Add a new comment to a specific case.

Parameters

Param name	Param type	Definition	Possible values	Comments
comment	{string}	Comment to be added to case wall	N/A	N/A
case_id	{string}	Case identifier	234	If a <code>case_id</code> is not provided, the current case will be used. None by default (optional)
alert_identifier	{string}	Alert identifier	12345	If an <code>alert_identifier</code> is not provided, the current alert will be used. None by default (optional)

Returns

NoneType

Example

```
from SiemplyfyAction import SiemplyfyAction
siemplyfy = SiemplyfyAction()
comment = "Ran some tests on the hash and it seems fine"
siemplyfy.add_comment(comment=comment)
```

Result behavior

The specified comment is added to the current case.

Result value

None

add_entity_insight

```
add_entity_insight(domain_entity_info, message, triggered_by=None,
```

Add an entity insight to the case it is being used in.

Parameters

Param name	Param type	Definition	Possible values	Comments
domain_entity_info	{DomainEntityInfo}	The entity object that represents an entity to add insight to	N/A	N/A
message	{string}	Insight message	N/A	N/A
triggered_by	{string}	Integration name	N/A	If no integration name is provided, the selected integration for the action will be used. None by default (optional)
original_requesting_user	{string}	Requesting user	N/A	None by default (optional)

Returns

{boolean} True if success. Otherwise, False .

Example

Result behavior

Result value

add_entity_to_case

```
add_entity_to_case(entity_identifier, entity_type, is_internal, is_
```

Add an entity to the current case.

Parameters

Param name	Param type	Definition	Possible values	Comments
entity_identifier	{string}	Entity identifier	192.0.2.1, example.com	N/A
entity_type	{string}	Entity type	"ADDRESS"	N/A
is_internal	{boolean}	N/A	Internal/External	N/A
is_suspicious	{boolean}	N/A	Suspicious/Not suspicious	N/A
is_enriched	{boolean}	N/A	True/False	False by default
is_vulnerable	{boolean}	N/A	True/False	False by default
properties	{dict}	{"Property1":"PropertyValue", "Property2":"PropertyValue2"}	N/A	N/A

Returns

NoneType

If there is an existing Entity, the following error appears: /

```
500 Server Error: Internal Server Error for url:
https://localhost:8443/api/external/v1/sdk/CreateEntity?
format=snake: \ "ErrorMessage\":"Cannot add entity
[Identifier:Entities Identifies -
Type:siemply.parameters[] to alert [MONITORED MAILBOX
<EXAMPLE@EXAMPLE.COM> _633997CB-D23B-4A2B-92F2-
AD1D350284FF] in case [12345] because the entity already
exists >there.\"
```

Example

```
from SiemplyAction import SiemplyAction
siemply = SiemplyAction()
siemply.add_entity_to_case(entity_identifier, entity_type, is_int
```

Result behavior

This function will add a new entity to the case if it is not present in the case.

Result value

None

add_tag

```
add_tag(tag, case_id=None, alert_identifier=None)
```

Add a new tag to a specific case.

Parameters

Param name	Param type	Definition	Possible values	Comments
tag	{string}	Tag to be added	Any string to be used as a tag	N/A
case_id	{string}	Case identifier	12345	If a case_id is not provided, then the current case ID will be used. None by default (optional)
alert_identifier	{string}	Alert identifier	123	If an alert_identifier is not provided, then the current alert ID will be used. None by default(optional)