

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

REST API

Security > Google Security Operations > Reference

On this page TIPCommon.adapters TIPCommon.base TIPCommon.rest data_models Module encryption Module ...

Send feedback

TIPCommon 2.1.0

The TIPCommon 2.1.0 library contains the following modules:

TIPCommon.adapters

- PubSubAdapter

TIPCommon.base

- parse_case_attachment()
- parse_case_comment()
- Action
 - _soar_action
 - _api_client
 - _name
 - _action_start_time
 - _logger
 - _params
 - global_context
 - _entity_types
 - _entities_to_update
 - json_results
 - _attachments
 - _contents
 - _data_tables
 - _html_reports
 - _links
 - _entity_insights
 - _case_insights
 - _result_value
 - _output_message
 - _error_output_message
 - action_start_time
 - api_client
 - attachments
 - case_insights
 - contents
 - data_tables
 - entities_to_update
 - entity_insights
 - entity_types

POERTFOLIO SAMPLE

- `error_output_message`
- `execution_state`
- `html_reports`
- `is_first_run`
- `links`
- `logger`
- `name`
- `output_message`
- `params`
- `result_value`
- `run()`
- `soar_action`
- `EnrichAction`
 - `enrichment_data`
 - `entity_results`
 - `global_context`
- `ActionParamType`
 - `BOOLEAN`
 - `CASE_PRIORITIES`
 - `CLOSE_CASE_REASONS`
 - `CLOSE_ROOT_CAUSE`
 - `CODE`
 - `CONTENT`
 - `DDL`
 - `EMAIL_CONTENT`
 - `ENTITY_TYPE`
 - `MULTI_VALUES`
 - `NULL`
 - `PASSWORD`
 - `PLAYBOOK_NAME`
 - `STAGE`
 - `STRING`
 - `USER`
- `Attachment`
 - `title`
 - `filename`
 - `file_contents`
 - `additional_data`
- `CaseAttachment`
 - `attachment_id`
 - `attachment_type`
 - `description`
 - `is_favorite`
- `CaseComment`
 - `comment`
 - `comment_for_client`
 - `modification_time_unix_time_in_ms_for_client`
 - `last_editor`
 - `last_editor_full_name`
 - `is_deleted`
 - `creator_user_id`
 - `creator_full_name`

POERTFOLIO SAMPLE

- comment_id
 - comment_type
 - case_id
 - is_favorite
 - modification_time_unix_time_in_ms
 - creation_time_unix_time_in_ms
 - alert_identifier
- CaseInsight
 - title
 - triggered_by
 - content
 - severity
 - insight_type
 - entity_identifier
 - additional_data
 - additional_data_type
 - additional_data_title
- CasePriority
 - CRITICAL
 - HIGH
 - INFORMATIONAL
 - LOW
 - MEDIUM
- CaseStage
 - ASSESSMENT
 - IMPROVEMENT
 - INCIDENT
 - INVESTIGATION
 - RESEARCH
 - TRIAGE
- CloseCaseOrAlertInconclusiveRootCauses
 - NO_CLEAR_CONCLUSION
- CloseCaseOrAlertMaintenanceRootCauses
 - LAB_TEST
 - OTHER
 - RULE_UNDER_CONSTRUCTION
- CloseCaseOrAlertMaliciousRootCauses
 - EXTERNAL_ATTACK
 - INFRASTRUCTURE_ISSUE
 - IRRELEVANT_TCP_UDP_PORT
 - MISCONFIGURED_SYSTEM
 - OTHER
 - SIMILAR_CASE_IS_ALREADY_UNDER_INVESTIGATION
 - SYSTEM_APPLICATION_MALFUNCTION
 - SYSTEM_CLOCKED_THE_ATTACK
 - UNFORESEEN_EFFECTS_OF_CHANGE
 - UNKNOWN
- CloseCaseOrAlertNotMaliciousRootCauses
 - EMPLOYEE_ERROR
 - HUMAN_ERROR
 - LAB_TEST
 - LEGIT_ACTION