ThreatQuotient

A Securonix Company

Google SecOps IOC Exporter Action

Version 1.1.0

August 29, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.1.0
Compatible with ThreatQ Versions	>= 6.0.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Google SecOps IOC Exporter Action for ThreatQ enables the automatic dissemination of IOCs from a ThreatQ data collection to Google SecOps. The exported IOCs are exported in the UDM format, as entities. The UDM format is a universal JSON format that is compatible with SecOps' API. These entities can then be used within SecOps's rules editor (YARA-L) to create rules to trigger alerts.

The integration provides the following action:

- **Google SecOps IOC Exporter** - enables the automatic dissemination of IOCs from a ThreatQ data collection to Google SecOps.

The action is compatible with the following indicator types:

- Email Address
- FQDN
- IP Address
- IPv6 Address
- MD5
- SHA-1
- SHA-256
- URL

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- A Google SecOps account.
- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the the following indicator objects:
  - Email Address
  - FQDN
  - IP Address
  - IPv6 Address
  - MD5
  - SHA-1
  - SHA-256
  - URL

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

> ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

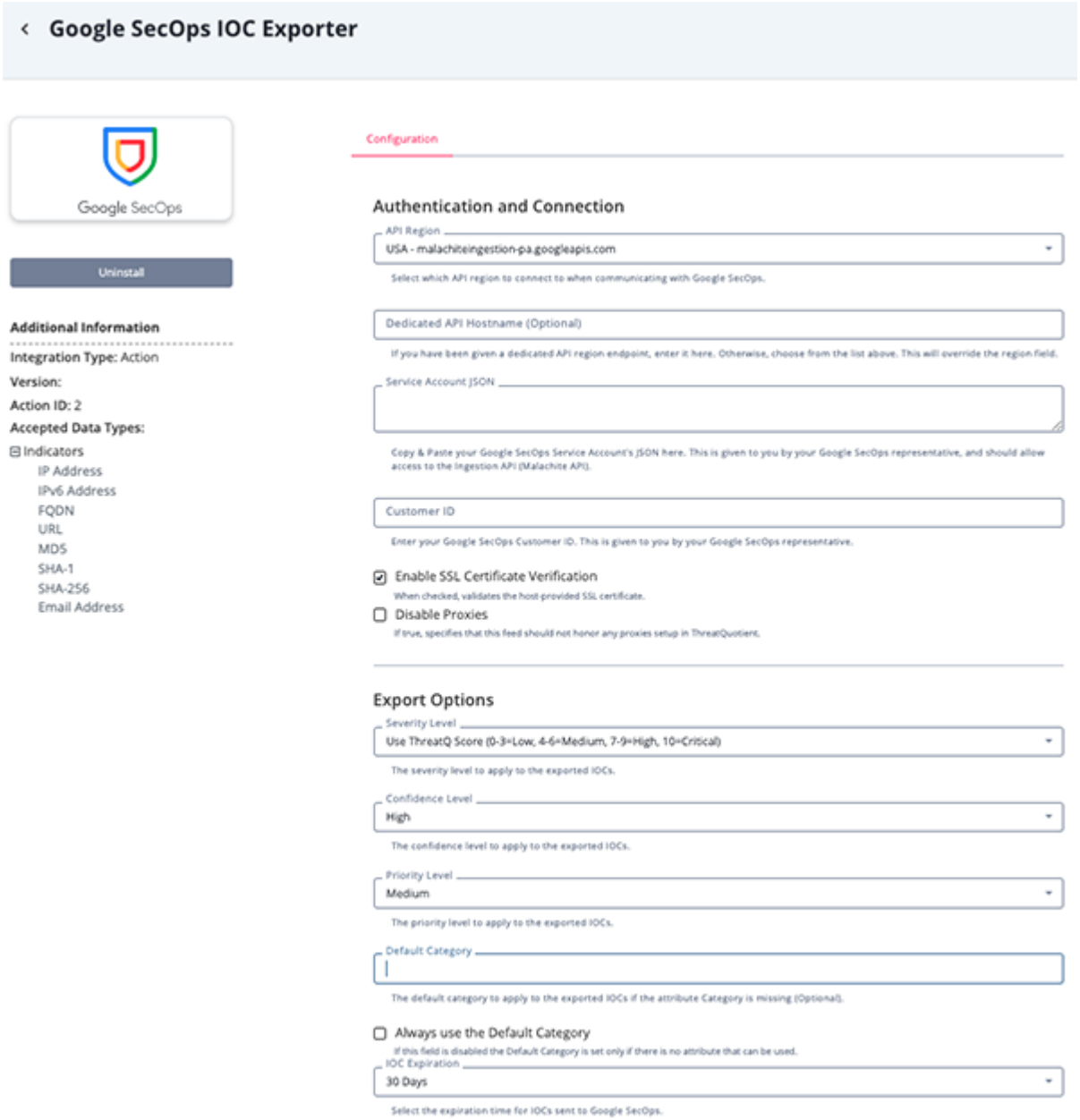
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
API Region	Select the API region to connect to when communicating with Google SecOps. Options include: ◦ `USA - malachiteingestion-pa.googleapis.com` *(default)* ◦ `Europe - europe-malachiteingestion-pa.googleapis.com` ◦ `London - europe-west2-malachiteingestion-pa.googleapis.com` ◦ `Singapore - asia-southeast1-malachiteingestion-pa.googleapis.com`
Dedicated API Hostname	Optional - Enter a dedicated API region endpoint. Any entry in this field will override the selection made in the **API Region** field above.
Service Account JSON	Enter your Google SecOps Service Account's JSON.
Customer ID	Enter your Google SecOps Customer ID.

PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Severity Level	Select the default severity level to apply to IOCs. Options include: ◦ Use ThreatQ Score (0-3=Low, 4-6=Medium, 7-9=High, 10=Critical) *(default)* ◦ Low ◦ Medium ◦ High ◦ Critical Informational ◦ Unknown
Confidence Level	Select the default confidence level to apply to IOCs. Options include: ◦ Low ◦ Medium ◦ High *(default)* ◦ Unknown
Priority Level	Select the default priority level to apply to IOCs. Options include: ◦ Low ◦ Medium *(default)* ◦ High ◦ Unknown
Default Category	Optional - enter a default category to be applied if the attribute category is missing.
Always Use the Default Category	Enable this parameter if the default category should always be set using the **Default Category** value. Disable this parameter to only set the default category is there is no attribute that can be used. This parameter is disabled by default.

PARAMETER	DESCRIPTION
IOC Expiration	Select the expiration time for IOCs sent to Google SecOps. Options include: ◦ 7 Days ◦ 30 Days *(default)* ◦ 60 Days ◦ 90 Days ◦ 180 Days ◦ 365 Days ◦ 0 Days ◦ Never
Attributes to Export	Enter a comma-separated list of attributes that should be exported as detection fields. The default value is `Is Bot, Is TOR, Is VPN, VPN Service, Actor, Organization`.
Use Original Source	Enable this parameter to have the IOC's source listed first in ThreatQ. Disabling this parameter will result to source being listed as `ThreatQ`. This parameter is disabled by default.
Export Tags	Enable this parameter to export tags as either tags or labels based on their entity type. This parameter is disabled by default.
Export Related Adversaries	Enable this parameter to export a related adversary as an association. This parameter is disabled by default.
Export Related Malware	Enable this parameter to export related malware as an association. This parameter is disabled by default.
ThreatQ Hostname	Enter your ThreatQ instance's Hostname or IP Address.
Objects Per Run	The max number of objects to send to this action per run. The default value is 100.



5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Google SecOps IOC Exporter	Enables the automatic dissemination of IOCs from a ThreatQ data collection to Google SecOps.	Indicators	IP Address, IPv6 Address, FQDN, URL, MD5, SHA-1, SHA-256, Email Address

Google SecOps IOC Exporter

The Google SecOps IOC Exporter action enables the automatic dissemination of IOCs from a ThreatQ data collection to Google SecOps.

`POST https://malachiteingestion-pa.googleapis.com/v2/entities:batchCreate`

Sample Request:

```
[
  {
    "customer_id": "12345",
    "entities": [
      {
        "entity": {
          "file": {
            "sha1": "4b6224893be96a22e448caefb51803f783d06567",
            "tags": [
              "malicious"
            ],
            "attribute": {
              "labels": []
            }
          }
        },
        "metadata": {
          "collected_timestamp": "2024-04-12T11:54:05Z",
          "description": "",
          "entity_type": "FILE",
          "vendor_name": "ThreatQuotient",
          "product_name": "ThreatQ",
          "source_labels": [
            {
              "key": "threat_source",
              "value": "Cisco Threat Grid"
            }
          ],
          "threat": {
            "about": {
              "file": {
                "sha1": "4b6224893be96a22e448caefb51803f783d06567",
                "tags": [
                  "malicious"
                ]
              }
            },
            "category": "SOFTWARE_MALICIOUS",
            "category_details": [
              "Botnet"
            ],
```

```
            "confidence": "HIGH_CONFIDENCE",
            "detection_fields": [
              {
                "key": "threatq_Is_Tor",
                "value": "False"
              }
            ],
            "severity": "LOW",
            "priority": "MEDIUM_PRIORITY",
            "alert_state": "NOT_ALERTING",
            "threat_status": "ACTIVE",
            "threat_name": "Malware - QAQ",
            "threat_feed_name": "Cisco Threat Grid",
            "threat_id": "1",
            "url_back_to_product": "https://threatq.online/indicators/1/
details"
          },
          "interval": {
            "start_time": "2024-04-17T14:01:37Z",
            "end_time": "2024-04-24T14:01:37Z"
          }
        }
      }
    ]
  }
]
```

Export Options

The following are export option for the action:

- The tags for `FQDN`, `URL`, `MD5`, `SHA-1`, `SHA-256` are exported using `.entities[].entity.tags[]`, for the rest of the indicators `.entities[].entity.attribute.labels[]` is used.
- `.entities[].metadata.collected_timestamp` - the timestamp when the indicator was created in ThreatQ.
- `.entities[].metadata.entity_type` - computed according to `Entity Type Mapping` table.
- `.entities[].metadata.source_labels[].value` - all the sources of the indicator.
- `.entities[].metadata.threat.category_details` - value of the user configuration `Default Category` if `Always use the Default Category` is true or no attribute named `Category` exists.
- `.entities[].metadata.threat.category` - computed according to `Category Mapping` table.
- `.entities[].metadata.threat.detection_fields` - all the attributes specified in user configuration `Attributes To Export` that the indicator has. the came of the attribute is prepended with `threatq`.
- `.entities[].metadata.threat.threat_name` - the first value of the attribute `Malware Family`.
- `.entities[].metadata.threat.threat_feed_name` - the first source of the indicator if user configuration `Use Original Source` is True, otherwise `ThreatQ`.
- `.entities[].metadata.threat.threat_id` - the indicator's ID from ThreatQ
- `.entities[].metadata.product_entity_id` - the indicator's ID from ThreatQ
- `.entities[].metadata.interval.start_time` - the timestamp when the action is run

Entity Type Mapping

The following table displays mapping between ThreatQ Indicators and Google SecOps Entities.

THREATQ INDICATOR TYPE	GOOGLE SECOPS ENTITY TYPE
FQDN	DOMAIN_NAME
Email Address	USER
IP Address	IP_ADDRESS
IPv6 Address	IP_ADDRESS
MD5	FILE
SHA-1	FILE
SHA-256	FILE
URL	URL

Category Mapping

The following table displays mapping between ThreatQ Indicators and Google SecOps Categories.

THREATQ INDICATOR TYPE	GOOGLE SECOPS CATEGORY
FQDN	NETWORK_MALICIOUS
Email Address	UNKNOWN_CATEGORY
IP Address	NETWORK_MALICIOUS
IPv6 Address	NETWORK_MALICIOUS
MD5	SOFTWARE_MALICIOUS
SHA-1	SOFTWARE_MALICIOUS
SHA-256	SOFTWARE_MALICIOUS
URL	NETWORK_MALICIOUS

Use Case Example

1. A Threat Analyst identifies a collection of supported objects they would like to enrich.
2. The Threat Analyst adds the Google SecOps IOC Exporter Action to a Workflow.
3. The Threat Analyst configures the action with the desired parameters, and enables the Workflow.
4. The Workflow executes all Actions in the graph, including Google SecOps IOC Exporter.

Change Log

- **Version 1.1.0**
  - Rebranded the integration name from **Google Chronicle IOC Exporter Action** to **Google SecOps IOC Exporter Action**.
  - Added the following configuration parameters:
    - **Enable SSL Certificate Verification** - determine if the action should validate the host-provided SSL certificate.
    - **Disable Proxies** - determine if the action should honor proxies set in the ThreatQ UI.
    - **Default Category** - enter a default category to be applied if the attribute category is missing.
    - **Always Use the Default Category** - configure if the default category should always be set using the **Default Category** value or only when there is not an attribute.
    - **Attributes to Export** - enter a comma-separated list of attributes that should be exported as detection fields
    - **Use Original Source** - determine if the IOC's source will be listed first in ThreatQ.
    - **Export Tags** - determine if tags are exported.
    - **Export Related Adversaries** - determine if related adversaries are exported as an association.
    - **Export Related Malware** - determine if related malware are exported as an association.
  - Updated the following configuration parameter names:
    - **Chronicle API Region** is now **API Region**.
    - **Chronicle Customer ID** is now **Customer ID**.
    - **Default Severity Level** is now **Severity Level**.
    - **Default Confidence Level** is now **Confidence Level**.
    - **Default Priority Level** is now **Priority Level**.
  - Added additional export context as well as entity and category mapping tables to this guide.
- **Version 1.0.0**
  - Initial release