

ThreatQuotient



Google Chronicle IOC Exporter Action

Version 1.0.0

May 28, 2024

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 3

Support 4

Integration Details..... 5

Introduction 6

Prerequisites 7

Installation..... 8

Configuration 9

Actions 12

 Google Chronicle IOC Exporter 13

Use Case Example..... 15

Change Log 16

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.

Copyright © 2024 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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	1.0.0
-----------------------------	-------

Compatible with ThreatQ Versions	>= 6.0.1
-------------------------------------	----------

ThreatQ TQO License Required	Yes
---------------------------------	-----

Support Tier	ThreatQ Supported
--------------	-------------------

Introduction

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

The integration provides the following action:

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

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 Chronicle 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
Chronicle API Region	Select the API region to connect to when communicating with Google Chronicle. Options include: <ul style="list-style-type: none"> ◦ USA - malachiteingestion-pa.googleapis.com ◦ 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 Chronicle API Region field above.
Service Account JSON	Enter your Google Chronicle Service Account's JSON.
Chronicle Customer ID	Enter your Google Chronicle Customer ID.

PARAMETER	DESCRIPTION
Default Severity Level	The default severity level to apply to IOCs. Options include: <ul style="list-style-type: none">◦ Use ThreatQ Score (0-3=Low, 4-6=Medium, 7-9=High, 10=Critical) (default)◦ Low◦ Medium◦ High◦ Critical Informational◦ Unknown
Default Confidence Level	The default confidence level to apply to IOCs. Options include: <ul style="list-style-type: none">◦ Low◦ Medium◦ High (default)◦ Unknown
Default Priority Level	The default priority level to apply to IOCs. Options include: <ul style="list-style-type: none">◦ Low◦ Medium (default)◦ High◦ Unknown
IOC Expiration	Expiration time for IOCs sent to Google Chronicle. Options include: <ul style="list-style-type: none">◦ 7 Days◦ 30 Days (default)◦ 60 Days◦ 90 Days◦ 180 Days◦ 365 Days◦ Never
ThreatQ Hostname	Your ThreatQ instance's Hostname or IP Address.
Objects Per Run	The max number of objects to send to this action per run.

[<](#) Google Chronicle IOC Exporter



Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 16

Accepted Data Types:

Indicators

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

Configuration

Chronicle API Region
USA - malachiteingestion-pa.googleapis.com

Select which API region to connect to when communicating with Google Chronicle

Dedicated API Hostname (Optional)

If you have been given a dedicated API region endpoint, enter it here. Otherwise, choose from the list above. This will override the region field.

Service Account JSON

Copy & Paste your Google Chronicle Service Account's JSON here. This is given to you by your Google Chronicle representative, and should allow access to the Ingestion API (Malachite API).

Chronicle Customer ID

Enter your Google Chronicle Customer ID. This is given to you by your Google Chronicle representative.

Default Severity Level
Use ThreatQ Score (0-3=Low, 4-6=Medium, 7-9=High, 10=Critical)

The default severity level to apply to IOCs when they don't already have a severity level.

Default Confidence Level
High

The default confidence level to apply to IOCs when they don't already have a confidence level.

Default Priority Level
Medium

The default priority level to apply to IOCs when they don't already have a priority level.

IOC Expiration
30 Days

Select the expiration time for IOCs sent to Google Chronicle.

- 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 Chronicle IOC Exporter	Enables the automatic dissemination of IOCs from a ThreatQ data collection to Google Chronicle	Indicators	IP Address, IPv6 Address, FQDN, URL, MD5, SHA-1, SHA-256, Email Address

Google Chronicle IOC Exporter

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

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

Sample Request:

```
[
  {
    "entity":{
      "file":{
        "sha1":"4b6224893be96a22e448caefb51803f783d06567"
      }
    },
    "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"
          }
        },
        "category":"SOFTWARE_MALICIOUS",
        "category_details":"",
        "confidence":"HIGH_CONFIDENCE",
        "severity":"LOW",
        "priority":"MEDIUM_PRIORITY",
        "alert_state":"NOT_ALERTING",
        "threat_status":"ACTIVE",
        "threat_name":"Malware - QAQ",
        "threat_feed_name":"",
        "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"
      }
    }
  }
]
```

```
}  
]
```

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 Chronicle 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 Chronicle IOC Exporter.

Change Log

- Version 1.0.0
 - Initial release