ThreatQuotient

Cisco AMP for Endpoints Operation Guide

Version 1.0.1

May 08, 2023

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	1.0.1
Compatible with ThreatQ Versions	>= 4.34.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/cisco-amp-for-endpoints-operation

Introduction

The Cisco AMP for Endpoints operation enriches ThreatQ objects with context obtained from the Cisco AMP for Endpoints API.

The operation is compatible with SHA-256 indicator types and provides the following actions:

- **Get Application Blocking List** - retrieves the list of application blocking file lists.
- **Blacklist Application** - blacklists an application hash.
- **Query Events** - queries for hits.

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 integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration file on your local machine

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

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

Configuration

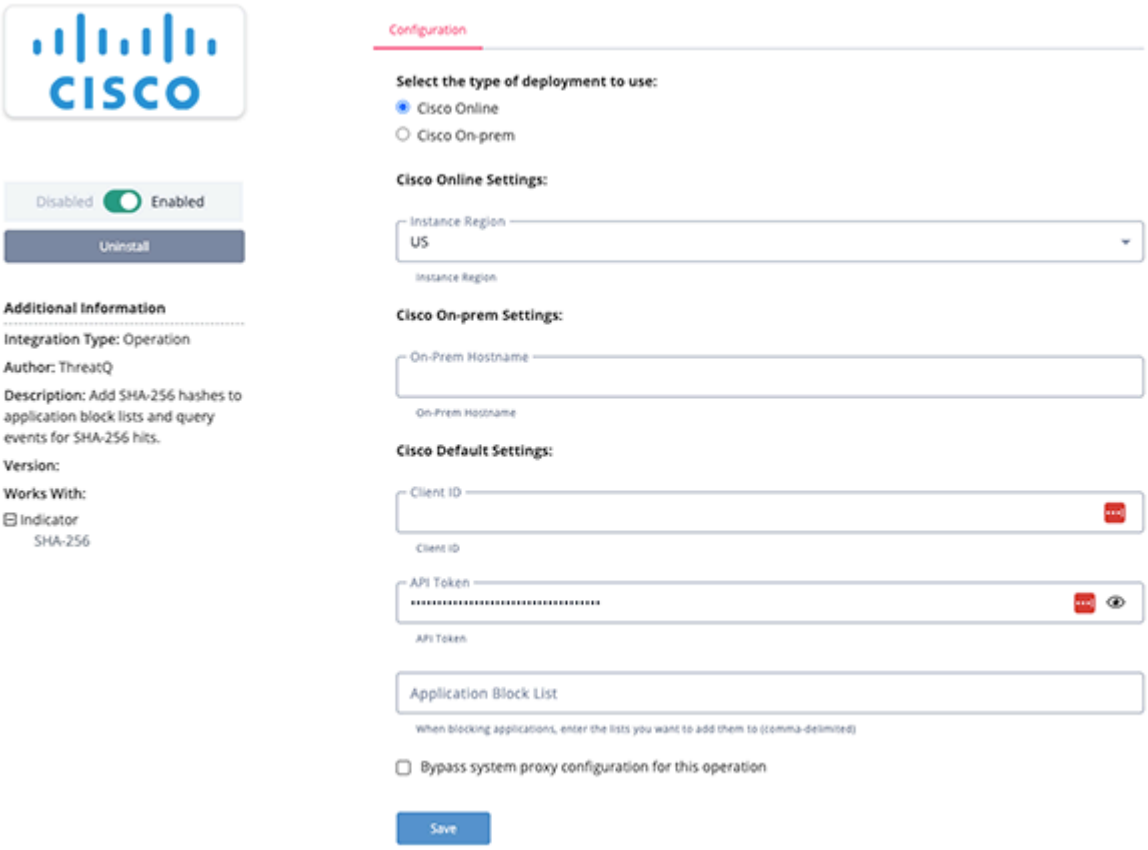
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

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

PARAMETER	DESCRIPTION
Select the Type of Deployment to use	Select the deployment type. Options include **Online** and **On-Prem**.
Cisco Online Settings	If using the Online deplyoment method, select the Cisco AMP for Endpoints Instance Region. Options include: ◦ US (default) ◦ EU ◦ APJC
Cisco On-Prem Settings	If using the On-Prem deployment method, enter the Cisco AMP for Endpoints Instance On-prem Hostname.
Client ID	The Cisco AMP for Endpoints Client ID.
API Token	The Cisco AMP for Endpoints API Token.
Application Control List	List of application block lists to add the submitted hash to.

Application Block List	Enter application block lists to add the submitted hash to.



5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Get Application Blocking List	Get list of application blocking file lists	Indicators	SHA-256
Blacklist Application	Blacklist application hash	Indicators	SHA-256
Query Events	Query events for hits	Indicators	SHA-256

Get Application Blocking List

The Get Application Blocking List action is used to get the list of application blocking file lists.

```
GET https://<region>/v1/file_lists/application_blocking
```

Sample Response:


```
{
    "version": "v1.2.0",
    "metadata": {
        "links": {
            "self": "https://api.amp.cisco.com/v1/file_lists/application_blocking"
        },
        "results": {
            "total": 3,
            "current_item_count": 3,
            "index": 0,
            "items_per_page": 500
        }
    },
    "data": [
        {
            "name": "Execution Blacklist",
            "guid": "747633c2-6a94-46dd-8d4a-97986d682252",
            "type": "application_blocking",
            "links": {
                "file_list": "https://api.amp.cisco.com/v1/file_lists/747633c2-6a94-46dd-8d4a-97986d682252"
            }
        },
        {
            "name": "Malware Blacklist",
            "guid": "f1866f7f-8a9d-4608-9ccc-537d72693c0e",
            "type": "application_blocking",
            "links": {
                "file_list": "https://api.amp.cisco.com/v1/file_lists/f1866f7f-8a9d-4608-9ccc-537d72693c0e"
            }
        },
        {
            "name": "ThreatQ Blacklist",
            "guid": "bd1a015b-f775-41ed-9883-ec64cca97bb3",
            "type": "application_blocking",
            "links": {
                "file_list": "https://api.amp.cisco.com/v1/file_lists/bd1a015b-f775-41ed-9883-ec64cca97bb3"
            }
        }
    ]
}
```


The available blocking lists available are extracted from `.data[].name`.

Blacklist Application

The Blacklist Application is used to blacklist an application hash.

```
GET https://<region>/v1/file_lists/<block_list_guid>/files/<sha256>>
```

The following configuration parameters are available for this action:

OPTION	DESCRIPTION
Description	A description of the hash.
Override Application Block Lists	Overrides the lists in the operation configuration.

Sample Response:

```
{
    "version": "v1.2.0",
    "metadata": {
        "links": {
            "self": "https://api.amp.cisco.com/v1/file_lists/bd1a015b-f775-41ed-9883-ec64cca97bb3/files/
5a0d64cc41bb8455f38b4b31c6e69af9e7fd022b0ea9ea0c32c371def24d67f1"
        }
    },
    "data": {
        "sha256": "5a0d64cc41bb8455f38b4b31c6e69af9e7fd022b0ea9ea0c32c371def24d67f1",
        "source": "Created by entering SHA-256 via Public api.",
        "links": {
            "file_list": "https://api.amp.cisco.com/v1/file_lists/bd1a015b-f775-41ed-9883-ec64cca97bb3"
        }
    }
}
```

Query Events

The Query Events action is used to query events for hits.

`GET https://<region>/v1/events`

The following configuration parameters are available for this action:

OPTION	DESCRIPTION
Query for	Query for **Detected SHA-256** or **Application SHA-256**.
Number of days back to get events from	Number of days back to get events from.
Maximum number of results	The maximum number of events that are queried.

Sample Response:


```
{
    "version": "v1.2.0",
    "metadata": {
        "links": {
            "self": "https://api.amp.cisco.com/v1/events?
detection_sha256=5a0d64cc41bb8455f38b4b31c6e69af9e7fd022b0ea9ea0c32c371def24d67fb"
        },
        "results": {
            "total": 1,
            "current_item_count": 1,
            "index": 0,
            "items_per_page": 500
        }
    },
    "data": [
        {
            "id": 5826659264906657801,
            "timestamp": 1621512020,
            "timestamp_nanoseconds": 460000000,
            "date": "2021-05-20T12:00:20+00:00",
            "event_type": "Threat Detected",
            "event_type_id": 1090519054,
            "detection": "W32.Variant:Stabuniq.15nx.1201",
            "detection_id": "5826659264906657801",
            "connector_guid": "a0e69f4b-2598-4102-a50d-de9ba994fde3",
            "group_guids": [
                "af1e7d79-880b-4aaf-84d4-06149fef0cd2"
            ],
```

```
            "severity": "Medium",
            "computer": {
                "connector_guid": "a0e69f4b-2598-4102-a50d-de9ba994fde3",
                "hostname": "Demo_Stabuniq",
                "external_ip": "173.142.132.97",
                "active": true,
                "network_addresses": [
                    {
                        "ip": "30.235.67.2",
                        "mac": "1c:96:e3:a2:aa:29"
                    }
                ],
                "links": {
                    "computer": "https://api.amp.cisco.com/v1/computers/a0e69f4b-2598-4102-a50d-de9ba994fde3",
                    "trajectory": "https://api.amp.cisco.com/v1/computers/a0e69f4b-2598-4102-a50d-de9ba994fde3/
trajectory",
                    "group": "https://api.amp.cisco.com/v1/groups/1f3e7f67-9cc1-457e-8870-69d86db80886"
                }
            },
            "file": {
                "disposition": "Blocklisted",
                "file_name": "jqs.exe",
                "file_path": "\\\\?\\C:\\Program Files\\7-Zip\\Update\\jqs.exe",
                "identity": {
                    "sha256": "5a0d64cc41bb8455f38b4b31c6e69af9e7fd022b0ea9ea0c32c371def24d67fb",
                    "sha1": "17db1bbaa1bf1b920e47b28c3050cbff83ab16de",
                    "md5": "f31b797831b36a4877aa0fd173a7a4a2"
                }
            }
        }
    ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].title	Event.Title	.data[].event_type	.data[].timestamp	<formatted>	Formatted based on the `.event_type`
.data[].date	Event.Happened_at	n/a	n/a	2020-05-13T13:09:02+00:00	
.data[].detection	Related Malware.Value	n/a	.data[].timestamp	W32.GenericKD: Malwaregen.21do.1201	
.data[].computer.network_addresses[].ip	Related Indicator.Value	IP Address	.data[].timestamp	45.139.251.184	
.data[].computer.network_addresses[].mac	Related Indicator.Value	MAC	.data[].timestamp	71:73:52:f3:13:8a	
.data[].computer.external_ip	Event.Attribute & Related Indicator.Attribute	Computer External IP	.data[].timestamp	151.140.44.204	
.data[].computer.active	Event.Attribute & Related Indicator.Attribute	Computer Is Active	.data[].timestamp	True	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].computer.hostname	Event.Attribute & Related Indicator.Attribute	Computer Hostname	.data[].timestamp	Demo_AMP_Intel	
.data[].computer.links.computer	Event.Attribute & Related Indicator.Attribute	Computer Group Link	.data[].timestamp	https://api.amp.cisco.com/v1/computers/763e3460-8cf2-49a8-be0c-6fa156f4e2fc	
.data[].computer.links.group	Event.Attribute & Related Indicator.Attribute	Computer Link	.data[].timestamp	https://api.amp.cisco.com/v1/groups/2c4e257f-d91a-4559-bba5-5a75ca03f8c0	
.data[].computer.user	Event.Attribute & Related Indicator.Attribute	Computer User	.data[].timestamp	johndoe	
.data[].file.file_name	Related Indicator.Value	Filename	.data[].timestamp	opticare.exe	Ingested if `.data[].file.disposition != 'Clean'`
.data[].file.file_path	Related Indicator.Value	File Path	.data[].timestamp	\\?\C:\Users\Administrator\AppData\Local\Temp\opticare.exe	Ingested if `.data[].file.disposition != 'Clean'`
.data[].file.identity.md5	Related Indicator.Value	MD5	.data[].timestamp	b2e15a06b0cca8a926c94f8a8eae3d88	Ingested if `.data[].file.disposition != 'Clean'`
.data[].file.identity.sha1	Related Indicator.Value	SHA-1	.data[].timestamp	f9b02ad8d25157eebdb284631ff646316dc606d5	Ingested if `.data[].file.disposition != 'Clean'`
.data[].file.identity.sha256	Related Indicator.Value	SHA-256	.data[].timestamp	fa1789236d05d88dd10365660defd6ddc8a09fcddb3691812379438874390ddc	Ingested if `.data[].file.disposition != 'Clean'`
.data[].network_info.dirty_url	Related Indicator.Value	URL	.data[].timestamp	http://dak1otavola1ndos.com/h/index.php	
.data[].network_info.parent.identity.sha256	Related Indicator.Value	SHA-256	.data[].timestamp	72c027273297ccf2f33f5b4c5f5bce3eecc69e5f78b6bbc1dec9e58780a6fd02	Ingested if `.data[].network_info.parent.disposition != 'Clean'`
.data[].file.parent.file_name	Related Indicator.Value	Filename	.data[].timestamp	Fax.exe	Ingested if `.data[].file.parent.disposition != 'Clean'`
.data[].file.parent.file_path	Related Indicator.Value	File Path	.data[].timestamp	n/a	Ingested if `.data[].file.parent.disposition != 'Clean'`
.data[].file.parent.identity.md5	Related Indicator.Value	MD5	.data[].timestamp	b2e15a06b0cca8a926c94f8a8eae3d88	Ingested if `.data[].file.parent.`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					`disposition != 'Clean'`
.data[].file.parent.identity.sha1	Related Indicator.Value	SHA-1	.data[].timestamp	f9b02ad8d25157eebdb284631ff646316dc606d5	Ingested if `.data[].file.parent.disposition != 'Clean'`
.data[].file.parent.identity.sha256	Related Indicator.Value	SHA-256	.data[].timestamp	fa1789236d05d88dd10365660defd6ddc8a09fcddb3691812379438874390ddc	Ingested if `.data[].file.parent.disposition != 'Clean'`
.data[].file.parent.disposition	Related Indicator.Attribute	Disposition	.data[].timestamp	Malicious	
.data[].file.disposition	Event.Attribute & Related Indicator.Attribute	Disposition	.data[].timestamp	Clean	
.data[].severity	Event.Attribute	Severity	.data[].timestamp	Medium	
.data[].cloud_ioc.description	Event.Attribute	Description	.data[].timestamp	Microsoft Word launched PowerShell. This is indicative of multiple...	
.data[].cloud_ioc.short_description	Event.Attribute	Short Description	.data[].timestamp	W32.WinWord.Powershell	
.data[].error.description	Event.Attribute	Error	.data[].timestamp	Object name not found	
.data[].vulnerabilities[].cve	Related Indicator.Value	CVE	.data[].timestamp	CVE-2013-3346	
.data[].vulnerabilities[].score	Related Indicator.Attribute	Score	.data[].timestamp	10	
.data[].vulnerabilities[].url	Related Indicator.Attribute	Reference	.data[].timestamp	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-3346	
.data[].vulnerabilities[].name	Related Indicator.Attribute	Name	.data[].timestamp	Adobe Acrobat Reader	

Change Log

- **Version 1.0.1**
  - Added support for On-Prem deployments.
- **Version 1.0.0**
  - Initial release