ThreatQuotient

Cisco AMP for Endpoints CDF Guide

Version 1.0.1

April 26, 2022

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

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.

Versioning

- Current integration version: `1.0.1`
- Compatible with ThreatQ versions >= `4.25.0`

Introduction

The Cisco AMP for Endpoints CDF enables a ThreatQ user to ingest events from Cisco AMP for Endpoints.

The CDF provides the following feed:

- **Cisco AMP for Endpoints Events** - ingests events from Cisco AMP for Endpoints.

The integration ingests the following system objects:

- Events
  - Event Attributes
- Indicators
  - Indicator Attributes
- Malware

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 feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.
6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

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 **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Client ID	Cisco AMP Client ID.
API Token	Cisco AMP API Client Token.
Region	Region of the Cisco AMP instance.

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.

ThreatQ Mapping

Cisco AMP for Endpoints Events

This feed allows a ThreatQ user to ingest events from Cisco AMP for Endpoints.

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


```
[
  {
    "data": [
      {
        "computer": {
          "active": true,
          "connector_guid": "a3e4eb31-24b7-4d4c-bc80-f31f3b49889c",
          "external_ip": "167.224.180.197",
          "hostname": "Demo_TeslaCrypt",
          "links": {
            "computer": "https://api.amp.cisco.com/v1/computers/a3e4eb31-24b7-4d4c-bc80-f31f3b49889c",
            "group": "https://api.amp.cisco.com/v1/groups/c3486bd8-4c40-4411-b80e-c1a857d40a12",
            "trajectory": "https://api.amp.cisco.com/v1/computers/a3e4eb31-24b7-4d4c-bc80-f31f3b49889c/trajectory"
          },
          "network_addresses": [
            {
              "ip": "188.198.174.15",
              "mac": "34:b6:39:91:08:c4"
            }
          ]
        },
        "connector_guid": "a3e4eb31-24b7-4d4c-bc80-f31f3b49889c",
        "date": "2020-05-13T13:45:07+00:00",
        "detection": "W32.DFC.MalParent",
        "detection_id": "6159258594551267599",
        "event_type": "Threat Detected",
        "event_type_id": 1090519054,
        "file": {
          "disposition": "Blocklisted",
          "file_name": "iodnxvg.exe",
          "file_path": "\\\\?\\C:\\Users\\Administrator\\AppData\\Roaming\\iodnxvg.exe",
          "identity": {
            "md5": "209a288c68207d57e0ce6e60ebf60729",
            "sha1": "e654d39cd13414b5151e8cf0d8f5b166dddd45cb",
            "sha256": "3372c1edab46837f1e973164fa2d726c5c5e17bcb888828ccd7c4dfcc234a370"
          }
          "parent": {
            "disposition": "Clean",
            "file_name": "Fax.exe",
            "identity": {
              "md5": "8b88ebbb05a0e56b7dcc708498c02b3e",
              "sha1": "cea0890d4b99bae3f635a16dae71f69d137027b9",
              "sha256": "9e1ec8b43a88e68767fd8fed2f38e7984357b3f4186d0f907e62f8b6c9ff56ad"
            },
        },
        "group_guids": ["c3486bd8-4c40-4411-b80e-c1a857d40a12"],
```

```
      "id": 6159258594551267599,
      "severity": "Medium",
      "timestamp": 1589377507,
      "timestamp_nanoseconds": 525000000
    }
  ],
  "metadata": {
    "links": {
      "prev": "https://api.amp.cisco.com/v1/events?limit=100&offset=800",
      "self": "https://api.amp.cisco.com/v1/events?limit=100&offset=900"
    },
    "results": {
      "current_item_count": 32,
      "index": 900,
      "items_per_page": 100,
      "total": 932
    }
  },
  "version": "v1.2.0"
 }
]
```


Response data will vary depending on the event type

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].<multiple_keys_used>	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	
.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/	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
				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	f9b02ad8d2515 7eebdb28 4631ff646316 dc606d5	Ingested if `.data[].file.parent .disposition != 'Clean'`
.data[].file.parent .identity.sha256	Related Indicator.Value	SHA-256	.data[].timestamp	fa1789236d05d 88dd10365 660defd6ddc8 a09fcddb36 918123794388 74390ddc	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	

Average Feed Run

METRIC	RESULT
Run Time	2 min
Events	296
Event Attributes	2,137
Indicators	401
Indicator Attributes	907
Malware	28

Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Change Log

- **Version 1.0.1**
  - Fixed an issue where responses from Cisco contained array objects that were missing a `computer` attribute.
  - Fixed an issue where responses from Cisco contained `Exploit Prevention` array objects that were missing attributes of the `file` attribute
- **Version 1.0.0**
  - Initial release