ThreatQuotient

Cybereason CDF Guide

Version 1.0.0

August 09, 2021

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

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 `1.0.0`
- Supported on ThreatQ versions >= `4.45.0`

Introduction

Cybereason is an EDR tool used to monitor, detect, and prevent malware from executing in an internal host machine. The Cybereason CDF for ThreatQ enables you to ingest Malware Alerts that are generated in the Cybereason platform.

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 parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
Cybereason Host and Port	Your Cybereason host and port (if required).
Username	Your Cybereason Username.
Password	Your Cybereason Password.
Needs Attention Only	Enabling this will only ingest malware alerts that "need attention."
Malware Types	Select one or more malware types to ingest for alerts: • Known Malware • Unknown Malware • Fileless • App Control

5. Review the **Settings** configuration, 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

The Cybereason Alerts feed enables ThreatQ to ingest any Events and Indicators from Cybereason.

`POST {host}/rest/malware/query`


```
{
  "data": {
    "malwares": [
      {
        "guid": "-1682067831.-373350822606094116",
        "timestamp": 1605611665000,
        "name": "wmplayer.exe",
        "type": "UnknownMalware",
        "elementType": "File",
        "machineName": "w7-cbr-se2",
        "status": "Detected",
        "needsAttention": false,
        "referenceGuid": "-1682067831.-373350822606094116",
        "referenceElementType": "File",
        "score": 0.6942690445239349,
        "detectionValue": "0630086e4eb057a1a3b89642cc0213ee",
        "detectionValueType": "DVT_FILE",
        "detectionEngine": "StaticAnalysis",
        "malwareDataModel": {
          "@class": ".BaseFileMalwareDataModel",
          "type": "UnknownMalware",
          "detectionName": null,
          "filePath": "c:\\program files (x86)\\windows media player\\wmplayer.exe"
        },
        "id": {
          "guid": "-1682067831.-373350822606094116",
          "timestamp": 1605611665000,
          "malwareType": "UnknownMalware",
          "elementType": "File"
        },
        "schedulerScan": false
      },
      {
        "guid": "-1682067831.-373350822606094116",
        "timestamp": 1605611498000,
        "name": "wmplayer.exe",
        "type": "UnknownMalware",
        "elementType": "File",
        "machineName": "w7-cbr-se2",
        "status": "Detected",
        "needsAttention": false,
        "referenceGuid": "-1682067831.-373350822606094116",
        "referenceElementType": "File",
        "score": 0.6942690445239349,
        "detectionValue": "0630086e4eb057a1a3b89642cc0213ee",
        "detectionValueType": "DVT_FILE",
        "detectionEngine": "StaticAnalysis",
```

```
      "malwareDataModel": {
        "@class": ".BaseFileMalwareDataModel",
        "type": "UnknownMalware",
        "detectionName": null,
        "filePath": "c:\\program files (x86)\\windows media player\\wmplayer.exe"
      },
      "id": {
        "guid": "-1682067831.-373350822606094116",
        "timestamp": 1605611498000,
        "malwareType": "UnknownMalware",
        "elementType": "File"
      },
      "schedulerScan": false
    }
  ],
  "totalResults": 2,
  "hasMoreResults": false
},
"status": "SUCCESS",
"message": ""
}
```

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.malwares[].[name&type&malwareDataModel.detectionName&status&detectionEngine]	Event.Title	Malware	data.malwares[].timestamp	gsecdump.exe - Application.Hacktool.Gsecdump.E - Prevented via AntiVirus	Event Title is made by adding all the values from the respective keys
.data.malwares[].malwareDataModel.filePath	Related.Indicator.Value	File Path	data.malwares[].timestamp	c:\program files (x86)\windows media player\wmplayer.exe	N/A
.data.malwares[].name	Related.Indicator.Value	Filename	data.malwares[].timestamp	wmplayer.exe	N/A
.data.malwares[].detectionValue	Related.Indicator.Value	MD5	data.malwares[].timestamp	0630086e4eb057a1a3b89642cc0213ee	N/A
.data.malwares[].machineName	Event.Attribute	Host Machine	data.malwares[].timestamp	WIN-123-123	N/A
.data.malwares[].needsAttention	Event.Attribute	Needs Attention	data.malwares[].timestamp	Yes	N/A
.data.malwares[].detectionValueType	Event.Attribute	Detection Value Type	data.malwares[].timestamp	DVT_FILE	N/A
.data.malwares[].type	Event.Attribute & Indicator.Attribute	Malware Type	data.malwares[].timestamp	KnownMalware	N/A
.data.malwares[].malwareDataModel.detectionName	Event.Attribute & Indicator.Attribute	Detection	data.malwares[].timestamp	Gen:Variant.Mimikatz.10	N/A
.data.malwares[].elementType	Event.Attribute & Indicator.Attribute	Element Type	data.malwares[].timestamp	File	N/A
.data.malwares[].detectionEngine	Event.Attribute & Indicator.Attribute	Detection Engine	data.malwares[].timestamp	AntiVirus	N/A
.data.malwares[].score	Event.Attribute & Indicator.Attribute	Cybereason Score	data.malwares[].timestamp	0.76273662732	N/A

Average Feed Run

METRIC	RESULT
Run Time	4 minutes
Events	951
Event Attributes	5,875
Indicators	143
Indicator Attributes	984

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 1.0.0**
  - Initial release