ThreatQuotient

Cyjax CDF Guide

Version 1.0.0

February 16, 2021

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

Support
Email: info@cyjax.com

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.

Contents

Versioning

- Current integration version: 1.0.0
- Supported on ThreatQ versions >= 4.42.0

Introduction

The Cyjax CDF allows users to ingest incident reports and indicators of compromise from incidents and honeypots.

This integration provides two feeds:

- Cyjax Indicators of Compromise
- Cyjax Incident Reports

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
Access Token	The API Access Token Credential

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

Cyjax Indicators of Compromise

The Indicators of Compromise API allows you to retrieve information about IOC. Indicators come in multiple forms, including files (hashes), IP addresses, domains, and URLs. They are collected from multiple sources, including past incidents and honeypots.

The Access token User Field is required for the feed endpoint. The endpoints utilized by this feed are as follows:

GET https://api.cyberportal.co/indicator-of-compromise - returns the IOC data, e.g.:


```
[
  {
    "type": "FileHash-SHA1",
    "value": "23873bf2670cf64c2440058130548d4e4da412dd",
    "industry_type": [
      "Financial",
      "Telecommunication"
    ],
    "handling_condition": "GREEN",
    "discovered_at": "2020-10-27T10:57:52+0000",
    "description": "WellMess malware analysis report",
    "source": "https://cymon.co/report/incident/view?id=69077"
  },
  {
    "type": "IPv4",
    "value": "176.119.29.37",
    "industry_type": [
      "Government",
      "Infrastructure",
      "healthcare",
      "pharmaceutical",
      "IT",
      "Politics",
      "Media",
      "NGO",
      "Education"
    ],
    "handling_condition": "GREEN",
    "discovered_at": "2020-10-27T10:57:52+0000",
    "description": "WellMess malware analysis report",
    "source": "https://cymon.co/report/incident/view?id=69077"
  },
  {
    "type": "FileHash-MD5",
    "value": "d1fb179527218836f3326c3219a3db5f",
    "industry_type": [
      "Government",
      "Infrastructure",
      "healthcare",
      "pharmaceutical",
      "IT",
      "Politics",
      "Media",
      "NGO",
```

```
        "Education"
      ],
      "handling_condition": "GREEN",
      "discovered_at": "2020-10-27T10:57:52+0000",
      "description": "WellMess malware analysis report",
      "source": "https://cymon.co/report/incident/view?id=69077"
    }
]
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.results[].type	indicator	type	SHA-256	Indicator type mapped to ThreatQ type.
.results[].value	indicator	value	391a8a9969cd5ab94d0772998b97bab5d82b44a69239185e421fcb1560b6ef54	
.results[].description	indicator	description	WellMess malware analysis report	
.results[].handling_condition	indicator.attribute	Handling Condition	GREEN	
.results[].source	indicator.attribute	Source	https://cymon.co/report/incident/view?id=69077	The link to the incident report.
.results[].industry_type	indicator.attribute	Industry type	Financial	
.results[].discovered_at	indicator.attribute	Discovered at	2021-01-14 12:36:09-00:00	
.results[].type	indicator.attribute	Cyjax IOC type	FileHash-SHA256	Cyjax indicator type.

Cyjax Incident Reports

The incident reports resource allows you to retrieve incident reports written by Cyjax analysts.

The Access token User Field is required to set the feed endpoint.

The endpoints utilized by this feed are as follows:

- GET https://api.cyberportal.co/report/incident - returns the incident reports data, e.g.:


```
[
  {
    "id": 69078,
    "title": "Amazon fires employees for leaking customer data to unaffiliated third party",
    "content": "
     Amazon has sent out an email to customers telling them that it has recently fired employees responsible for leaking customer data to an unaffiliated third-party. This was in violation of company policies. Only those believed to have been affected have been contacted.
     \r\n
     The company claims that only user email addresses and phone numbers were exposed in this incident, and no other information related to the account was shared. It is currently unclear how many customers have been affected, and whether only UK customers were victims, or if it affected users worldwide.
     \r\n
     Analyst comment: A similar incident to this occurred in January 2020, when Amazon-owned Ring fired multiple employees for improperly accessing customer video data. Corporate espionage is a common threat that can be difficult to mitigate, as it can be caused by a number of factors: scorned employees, monetary gain, or even simple human error. These types of risks can never be completely avoided, but systems can be put in place to control them.",
    "source": "https://www.vice.com/en/article/dy8zwz/amazon-fired-employee-leaking-customer-emails",
    "last_update": "2020-10-27T11:42:55+0000",
    "severity": "low",
    "source_evaluation": "always-reliable",
    "impacts": {
      "others": "minimal-impact",
      "retail": "minimal-impact"
    },
    "tags": [
      "Amazon",
      "Corporate espionage",
      "email address",
      "EMEA",
      "Europe",
      "global",
      "inside threat",
      "Leaks",
      "phone number",
      "UK",
      "unauthorised access"
    ],
    "countries": [
      "United Kingdom"
    ],
    "techniques": [],
    "software": [],
    "ioc": [],
    "ioc_count": 0
  }
]
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.results[].title	Report	N/A	Amazon fires employees for leaking customer data to unaffiliated third party	
.results[].content	Report.Description	N/A	Report description.	
.results[].published_at	Report.published_at	N/A	2021-01-14 12:36:09-00:00	
.results[].severity	Report.Attribute	Severity	Medium	
.results[].source	Report.Attribute	Source	https://some-website.com	The incident report source.
.results[].source_evaluation	Report.Attribute	Source evaluation	Always reliable	
.results[].impacts	Report.Attribute	Impact	Others: Minimal Impact	
.results[].countries	Report.Attribute	Country	Germany, Portugal	
.results[].tags	Report.Attribute	Tag	Politics	
.results[].techniques	Related TTP	N/A	Right-to-Left Override	
.results[].software	Related TTP	N/A	Hi-Zor"	
.results[].ioc[].type	Related Indicator.Type	See IOC Mapping table	SHA-256	Indicator type mapped to ThreatQ type
.results[].ioc[].value	Related Indicator	N/A	391a8a9969cd5ab94d0772998b97bab5d82b44a69239185e421fcb1560b6ef54	
.results[].ioc[].description	Related Indicator.Description	N/A	WellMess malware analysis report	
.results[].ioc[].handling_condition	Related Indicator.Attribute	Handling Condition	GREEN	
.results[].ioc[].source	Related Indicator.Attribute	Source	https://cymon.co/report/incident/view?id=69077	The link to the incident report.
.results[].ioc[].industry_type	Related Indicator.Attribute	Industry type	Financial	
.results[].ioc[].discovered_at	Related Indicator.Attribute	Discovered at	2021-01-14 12:36:09-00:00	
.results[].ioc[].type	Related Indicator.Attribute	Cyjax IOC type	FileHash-SHA256	Cyjax indicator type.

IOC Mapping

The following table shows how IoCs from Cyjax are mapped to ThreatQ Indicator Types:

CYJAX TYPE	THREATQ INDICATOR TYPE
IPv4	IP Address
IPv6	IPv6 Address
URL	URL
Email	Email Address
Hostname	FQDN
Domain	FQDN
FileHash-SHA1	SHA-1
FileHash-SHA256	SHA-256
FileHash-MD5	MD5
FileHash-SSDEEP	Fuzzy Hash

Average Feed Run

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.

Cyjax Indicators of Compromise

METRIC	RESULT
Run Time	2 minutes
Indicators	234
Indicator Attributes	2,192

Cyjax Incident Reports

METRIC	RESULT
Run Time	2 minutes
Indicators	789
Indicator Attributes	7,290
Reports	34
Report Attributes	928
TTPs	104

Change Log

- **Version 1.0.0**
  - Initial release