ThreatQuotient

Palo Alto Unit 42 Reports CDF Guide

Version 1.0.0

February 14, 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

Integration Details 5
Introduction 6
Installation 7
Configuration 8
ThreatQ Mapping 10
    Palo Alto Unit 42 Reports 10
Average Feed Run 12
Change Log 13

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	1.0.0
Compatible with ThreatQ Versions	>= 4.35.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/palo-alto-unit-42-reports-cdf

Introduction

The Palo Alto Unit 42 Reports CDF for ThreatQ enables an analyst to automatically ingest OSINT intelligence published by Palo Alto Networks.

The integration provides the following feed:

- **Palo Alto Unit 42 Reports** - ingests Reports, Campaigns, Attack Patterns, Indicators, Signatures and Courses of Action.

The integration ingests the following system objects:

- Reports
- Campaigns
- Attack Patterns
- Indicators
- Signatures
- Courses of Action

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:

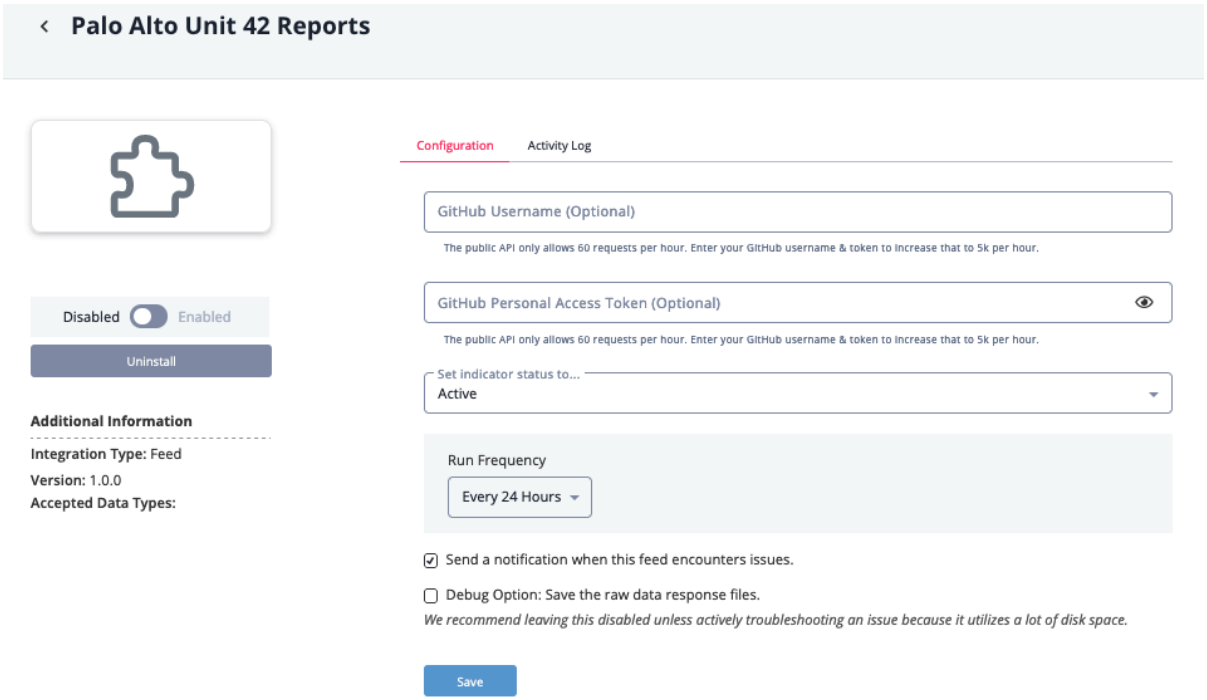
1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** option from the *Category* dropdown (optional).

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

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

PARAMETER	DESCRIPTION
GitHub Username	Optional - Your GitHub username.
GitHub Personal Access Token	Optional - Your GitHub username.

> The public API only allows 60 request per hour. Using your GitHub username and access token will increase that value to 5,000 per hour.



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

Palo Alto Unit 42 Reports

The Palo Alto Unit 42 Reports feed automatically pulls public STIX reports from the Palo Alto Unit 42 GitHub Repository.

```
GET https://api.github.com/repos/pan-unit42/iocs/contents/stix2-reports/report_json
```

Sample Response:


```
[
  {
    "name": "CodeCov_Breach.json",
    "path": "stix2-reports/report_json/CodeCov_Breach.json",
    "sha": "4167ae1042f55117e3b914527be5865626f27c5c",
    "size": 26793,
    "url": "https://api.github.com/repos/pan-unit42/iocs/contents/stix2-reports/report_json/CodeCov_Breach.json?
ref=master",
    "html_url": "https://github.com/pan-unit42/iocs/blob/master/stix2-reports/report_json/CodeCov_Breach.json",
    "git_url": "https://api.github.com/repos/pan-unit42/iocs/git/blobs/4167ae1042f55117e3b914527be5865626f27c5c",
    "download_url": "https://raw.githubusercontent.com/pan-unit42/iocs/master/stix2-reports/report_json/
CodeCov_Breach.json",
    "type": "file",
    "_links": {
      "self": "https://api.github.com/repos/pan-unit42/iocs/contents/stix2-reports/report_json/CodeCov_Breach.json?
ref=master",
      "git": "https://api.github.com/repos/pan-unit42/iocs/git/blobs/4167ae1042f55117e3b914527be5865626f27c5c",
      "html": "https://github.com/pan-unit42/iocs/blob/master/stix2-reports/report_json/CodeCov_Breach.json"
    }
  },
  {
    "name": "Defray777_TA.json",
    "path": "stix2-reports/report_json/Defray777_TA.json",
    "sha": "52cc89146040292b17a9a1d740ba6c1f4da710f0",
    "size": 86057,
    "url": "https://api.github.com/repos/pan-unit42/iocs/contents/stix2-reports/report_json/Defray777_TA.json?
ref=master",
    "html_url": "https://github.com/pan-unit42/iocs/blob/master/stix2-reports/report_json/Defray777_TA.json",
    "git_url": "https://api.github.com/repos/pan-unit42/iocs/git/blobs/52cc89146040292b17a9a1d740ba6c1f4da710f0",
    "download_url": "https://raw.githubusercontent.com/pan-unit42/iocs/master/stix2-reports/report_json/
Defray777_TA.json",
    "type": "file",
    "_links": {
      "self": "https://api.github.com/repos/pan-unit42/iocs/contents/stix2-reports/report_json/Defray777_TA.json?
ref=master",
      "git": "https://api.github.com/repos/pan-unit42/iocs/git/blobs/52cc89146040292b17a9a1d740ba6c1f4da710f0",
      "html": "https://github.com/pan-unit42/iocs/blob/master/stix2-reports/report_json/Defray777_TA.json"
    }
  }
]
```

Each JSON file in the response is passed to ThreatQ's STIX parser, and the results are passed directly to the API. As such, there are no custom mappings for this feed.

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.

METRIC	RESULT
Run Time	3 minutes
Attack Patterns	88
Attack Pattern Attributes	1,830
Campaigns	11
Campaign Attributes	11
Courses Of Action	69
Course Of Action Attributes	69
Indicators	1,663
Indicator Attributes	5,190
Reports	25
Report Attributes	75
Signatures	1,670
Signature Attributes	5,013

Change Log

- **Version 1.0.0**
  - Initial release