ThreatQuotient

A Securonix Company

Palo Alto Unit 42 Threat Research Blog CDF

Version 1.0.0

September 23, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	>= 5.5.0
Support Tier	ThreatQ Supported

Introduction

The Palo Alto Unit 42 Threat Research Blog CDF integration ingests threat intelligence and research posts directly into the ThreatQ platform as Report objects. This ensures analysts have timely access to expert analysis on malware, vulnerabilities, threat actor activity, and emerging attack techniques to strengthen their cybersecurity defenses.

The integration provides the following feed:

- **Palo Alto Unit 42 Threat Research** - ingests blog posts as reports filtered by published time.

The integration ingests the following object types:

- Adversaries
- Indicators
- Malware
- Reports
- Vulnerabilities

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

   > 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.

The feed(s) 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:

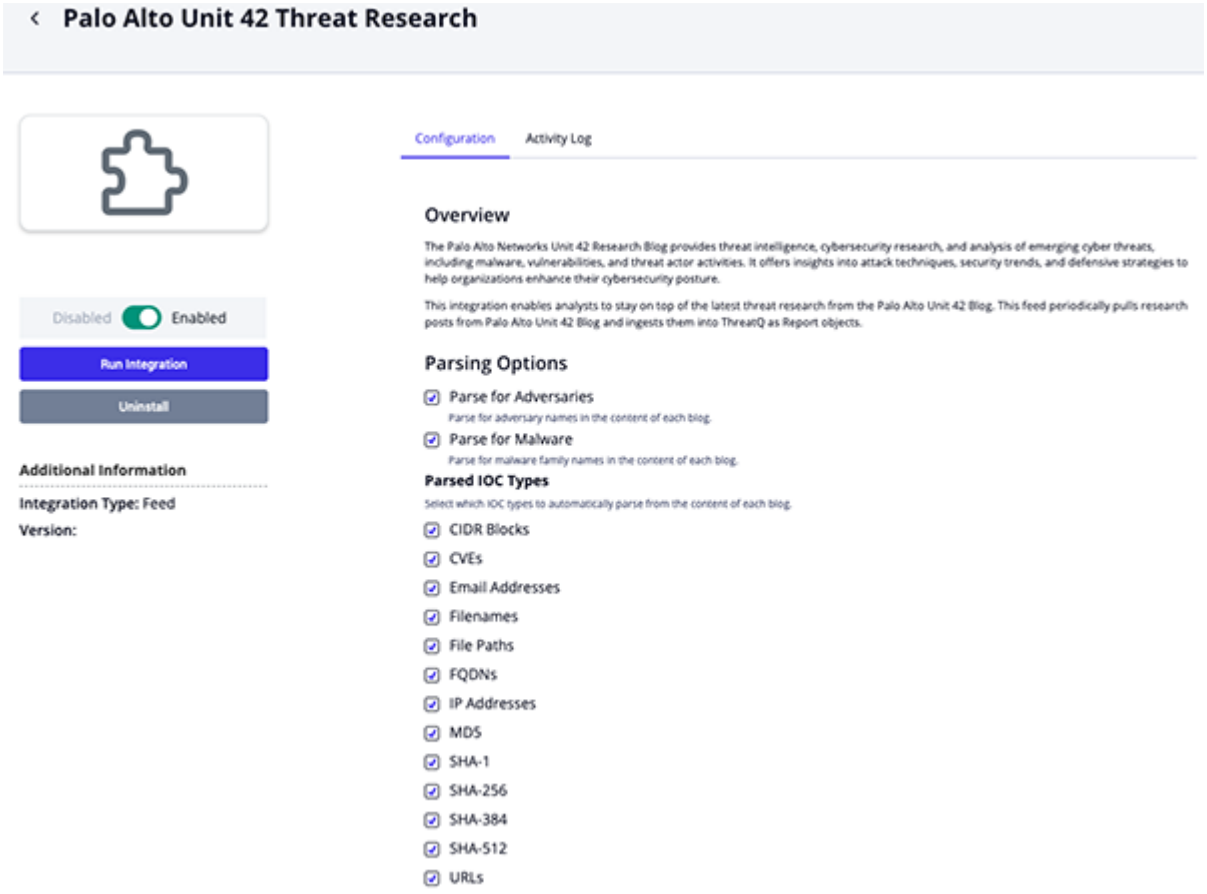
1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** option from the *Category* dropdown (optional).

   > 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
Parse for Adversaries	Enable this parameter to parse for adversary names in the content of each blog. This parameter is disabled by default.
Parse for Malware	Enable this parameter to parse for malware family names in the content of each blog. This parameter is disabled by default.
Parsed IOC Types	Select which IOC types to automatically parse from the content of each blog. Option include: ◦ CIDR Block ◦ CVEs *(default)* ◦ Email Address ◦ Filename ◦ File Path ◦ FQDN ◦ IP Address ◦ MD5 ◦ SHA-1 ◦ SHA-256 ◦ SHA-384 ◦ SHA-512 ◦ URL
Ingest CVEs As	Select the entity type to ingest CVEs as into the ThreatQ platform. Options include: ◦ Vulnerabilities *(default)* ◦ Indicators (Type: CVE)

PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.



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 Threat Research

The Palo Alto Unit 42 Threat Research feed periodically pulls security category blog posts from the Palo Alto Unit 42 Threat Research blog and ingests them into ThreatQ as report objects.

```
GET https://www.Palo Alto Unit 42 Blog.com/tag/security/
```

The output of this request is HTML, which is parsed for the title, author, date, links etc. The blog itself is then fetched.

```
GET https://www.Palo Alto Unit 42 Blog.com/{{ uri }}
```

ThreatQuotient provides the following default mapping for this feed based on the information parsed out of the blog's HTML content:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Report.Title	N/A	N/A	`CL-STA-0048: An Espionage Operation Against High-Value Targets in South Asia`	Parsed from the HTML
N/A	Report.Description	N/A	N/A	N/A	Parsed from the HTML
N/A	Report.Attribute	Published At	N/A	`September 05, 2024`	Parsed from the HTML
N/A	Report.Attribute	Author	N/A	`Tom Fakterman`	Parsed from the HTML
N/A	Report.Attribute	Category	N/A	`Threat Research`	Parsed from the HTML
N/A	Report.Tag	N/A	N/A	`GenAI`	Parsed from the HTML
N/A	Indicator.Value	<Various IOC Types>	N/A	N/A	User-Configurable. Parsed from the HTML
N/A	Vulnerability.Value	N/A	N/A	N/A	User-Configurable. CVEs parsed from the HTML
N/A	Malware.Value	N/A	N/A	N/A	User-configurable. Parsed from the HTML
N/A	Adversary.Name	N/A	N/A	N/A	User-configurable. Parsed from the HTML

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	1 minute
Indicators	20
Reports	1
Report Attributes	4

Known Issues / Limitations

- The feed utilizes **since** and **until** dates to make sure entries are not re-ingested if they haven't been updated.
- If you need to ingest historical blog posts, run the feed manually by setting the **since** date back.
- The feed will only return, at maximum, the first 3 pages of news posts from the Palo Alto Unit 42 Threat Research Blog.

Change Log

- **Version 1.0.0**
  - Initial release