ThreatQuotient

A Securonix Company

Palo Alto Threat Vault CDF

Version 1.0.0

August 18, 2025

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

Warning and Disclaimer 3
Support 4
Integration Details 5
Introduction 6
Prerequisites 7
Installation 8
Configuration 9
ThreatQ Mapping 11
Palo Alto Threat Vault 11
Average Feed Run 13
Known Issues / Limitations 14
Change Log 15

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	>= 5.29.0
Support Tier	ThreatQ Supported

Introduction

The Palo Alto Threat Vault CDF enables users to ingest IP addresses from Palo Alto's External Dynamic Lists (EDLs) via the Threat Vault API.

The integration provides the following feed:

- **Palo Alto Threat Vault** – retrieves and parses IP address data from Palo Alto Threat Vault EDLs.

The integration ingests the following indicator types:

- IP Address
- CIDR Block

This integration supports both individual IP addresses and CIDR ranges from multiple list types.

Prerequisites

The following is required to run the integration:

- A Palo Alto API Key is required. This key can be obtained from the customer service portal: **Assets → API Key Management → Threat Vault API**.

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 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. The feed will be added to the integrations page. You will still need to configure and enable it.

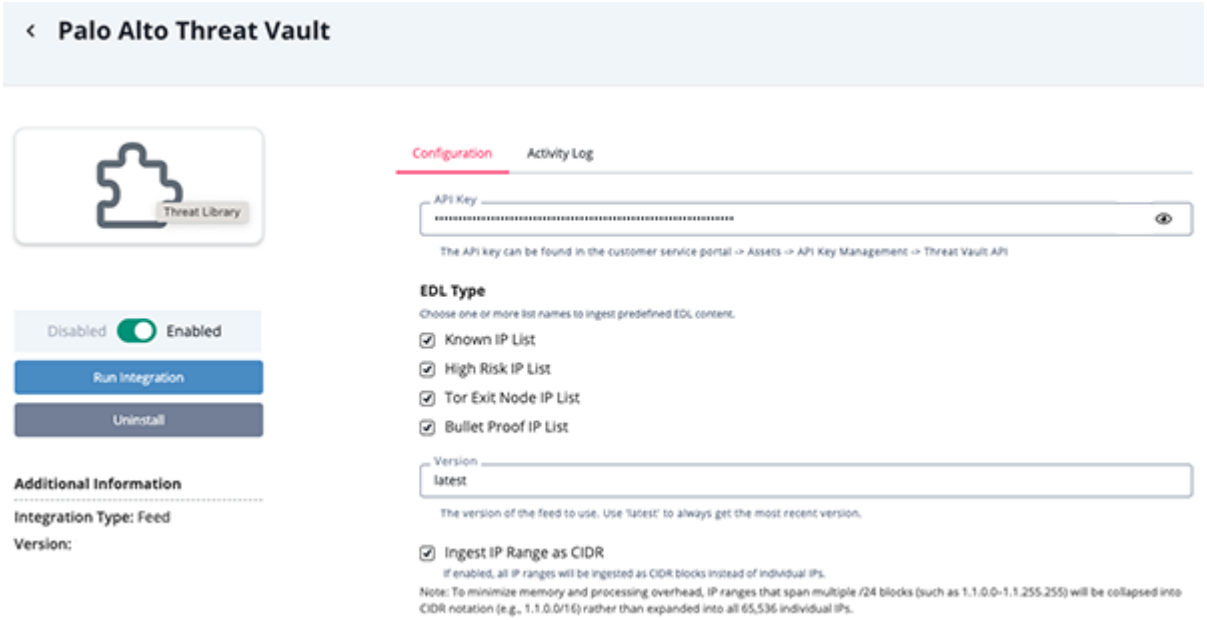
Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact Palo Alto Networks to obtain an API key.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** category.
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	The API key for Palo Alto Threat Vault, obtained via customer portal.
EDL Type	Select one or more EDL list names: • Known IP List (default) • High Risk IP List • Tor Exit Node IP List • Bullet Proof IP List
Version	The feed version to use. Set to `latest` to always retrieve the most current version.
Ingest IP Range as CIDR	If enabled, converts all IP ranges to CIDR blocks instead of expanding into individual IP addresses. > Large IP ranges (e.g., spanning multiple /24 blocks) are collapsed into CIDR notation to prevent excessive object creation.



5. Review settings and click **Save**.
6. Click the toggle switch to enable the feed.

ThreatQ Mapping

Palo Alto Threat Vault

The Palo Alto Threat Vault feed ingests IP addresses or CIDR blocks from Palo Alto Threat Vault EDLs based on the configured EDL Type.

`GET https://api.threatvault.paloaltonetworks.com/service/v1/edl?listformat=array&version=<VERSION>&name=<EDL LIST NAME>`

Sample Response (IP Addresses):

```
{
  "success": true,
  "count": 4000,
  "data": {
    "version": "5200",
    "name": "panw-known-ip-list",
    "ipaddr": [
      "1.0.218.230",
      "1.10.146.30"
    ]
  }
}
```

Sample Response (IP Ranges):

```
{
  "success": true,
  "count": 4,
  "data": {
    "version": "5200",
    "name": "panw-bulletproof-ip-list",
    "ipaddr": [
      "5.188.205.0-5.188.205.255",
      "80.85.155.0-80.85.155.255"
    ]
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
`data.ipaddr`	Indicator.Value	IP Address	`1.0.218.230`	N/A
`data.ipaddr`	Indicator.Value	CIDR Block	`136.1.1.0/24`	User-configurable; used if IP range is too large or "Ingest IP Range as CIDR" is enabled.
`data.version`	Indicator.Attribute	EDL Version	`5200`	N/A
`data.name`	Indicator.Attribute	EDL Name	`panw-bulletproof-ip-list`	N/A

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	6 minutes
Indicators	8,928
Indicator Attributes	17,898

Known Issues / Limitations

- Large IP ranges (e.g., spanning multiple /24 blocks) are collapsed into CIDR notation to prevent excessive object creation.

Change Log

- **Version 1.0.0**
  - Initial release