

ThreatQuotient

A Securonix Company



Flashpoint VulnDB Action

Version 1.0.0

August 25, 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

Actions 11

 Flashpoint VulnDB CVE Enrichment 12

Enriched Data..... 13

Change Log 14

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.

Copyright © 2025 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Flashpoint VulnDB Action integration leverages the **Flashpoint VulnDB API** to enrich CVE records with additional context, providing deeper insights into vulnerabilities.

Flashpoint's **VulnDB** is a comprehensive vulnerability database designed to help organizations strengthen their risk management programs. It offers continuously updated intelligence, including vulnerabilities that may not be documented in other sources, and delivers timely alerts. By covering both end-user software and third-party libraries, VulnDB enables organizations to proactively identify and address security weaknesses across their IT environments.

The integration provides the following action:

- **Flashpoint VulnDB CVE Enrichment** - queries CVEs from the input collection against Flashpoint VulnDB

The integration is compatible with the following object types:

- Indicator
- Vulnerability

The integration enriches the following object types:

- Indicator
- Vulnerability



This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A ThreatQ data collection containing at least one of the following system objects:
 - CVE (Indicator)
 - Vulnerabilities with the name of a valid CVE ID
- A Flashpoint VulnDB License.



The VulnDB license is separate from Ignite & FP Tools ones.

- A Flashpoint VulnDB API Credentials.



The API Credentials key must have permissions to search for multiple CVEs.

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the zip 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



ThreatQ will inform you if the action already exists and will require user confirmation before proceeding. ThreatQ will also warn if the new version contains changes to the user configuration. The new configurations will overwrite existing ones and require confirmation.

6. The action will now be installed. You will still need to [configure](#) the action.

Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact Flashpoint 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 **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Client ID	Enter your Flashpoint VulnDB client ID to authenticate with the API.
Client Secret	Enter your client secret associated with the VulnDB client ID.
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
CVE Context Filter	<p>Select the context used to enrich the CVEs. Options include:</p> <ul style="list-style-type: none"> ◦ Access Vector ◦ Access Complexity ◦ Authentication ◦ Confidentiality Impact ◦ Integrity Impact ◦ Availability Impact ◦ Base Score ◦ Affected Vendors ◦ Affected Products
Ingest Flashpoint Vulnerability	Enable this parameter to ingest related Flashpoint vulnerabilities associated with the original CVEs. This parameter is enabled by default.

PARAMETER	DESCRIPTION
Vulnerability Context Selection	<p>Select the context to apply to ingested Flashpoint Vulnerabilities. Options include:</p> <ul style="list-style-type: none"> ◦ Affected Vendors ◦ Affected Products ◦ Authors ◦ VulnDB Link ◦ Attack Type ◦ Location ◦ Impact
Objects per run	Enter the maximum number of objects to process per-run. The default value is 500.

< Flashpoint VulnDB CVE Enrichment



Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 2

Accepted Data Types:

☒ Indicators

☐ CVE

☐ Vulnerability

Configuration

Authentication and Connection

Client ID

Enter your Flashpoint VulnDB client ID to authenticate with the API.

Client Secret

Enter your client secret associated with the VulnDB client ID.

☒ Enable SSL Certificate Verification

When checked, validates the host-provided SSL certificate.

☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

Ingestion Options

CVE Context Filter

Select the context used to enrich CVEs.

☒ Access Vector

☒ Access Complexity

☐ Authentication

☒ Confidentiality Impact

☒ Integrity Impact

☒ Availability Impact

☒ Base Score

☒ Affected Vendors

☒ Affected Products

5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Flashpoint VulnDB CVE Enrichment	Enriches indicators with Flashpoint VulnDB data.	Indicator, Vulnerability	CVE (Indicator)

Flashpoint VulnDB CVE Enrichment

The Flashpoint VulnDB CVE Enrichment action queries CVEs contained in a Threat Library collection against Flashpoint VulnDB API. The CVEs are saved in ThreatQ as CVE type indicators or Vulnerabilities.

POST https://vulndb.flashpoint.io/api/v1/vulnerabilities/cve_search

Sample Response:

```
{
  "results": [
    {
      "title": "VMware Multiple Products XHCI USB Controller...",
      "description": "Multiple VMware products contain a use-after-free...",
      "cve_id": "2020-4004",
      "vendors": [{"vendor": {"name": "VMware"}}],
      "products": [{"name": "VMware ESXi"}],
      "authors": [{"name": "Tianwen Tang"}],
      "cvss_metrics": [{"score": 4.6, "access_vector": "LOCAL"}]
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.cvss_metrics[].cve_id	Indicator/ Vulnerability.Value	CVE/ Vulnerability	.cvss_metrics[].generated_on	CVE-2020-4004	Prepended with CVE. Matches input collection type.
.cvss_metrics[].access_vector	Indicator/ Vulnerability.Attribute	CVSSv2 Access Vector	.cvss_metrics[].generated_on	LOCAL	User-configurable. Updatable.
.products[].name	Indicator/ Vulnerability.Attribute	Affected Product	.cvss_metrics[].generated_on	VMware ESXi	User-configurable.
.vendors[].vendor.name	Indicator/ Vulnerability.Attribute	Affected Vendor	.cvss_metrics[].generated_on	VMware	User-configurable.
.title	Related Vulnerability.Value	Vulnerability	.vulndb_published_date	VMware Multiple Products XHCI...	Ingested if "Ingest Flashpoint Vulnerability" enabled.
.authors[].name	Related Vulnerability.Attribute	Author	.vulndb_published_date	Tianwen Tang	User-configurable.

Enriched Data



Object counts and action runtime are supplied as generalities only. Objects returned by Flashpoint may differ based on API credentials, dataset size, and system resources.

METRIC	RESULT
Run Time	3 minutes
Indicators	200
Indicator Attributes	5,000

Change Log

- Version 1.0.0
 - Initial release