ThreatQuotient

Exploit DB CDF Guide

Version 2.0.0

May 17, 2022

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

Not Actively Supported

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 **Not Actively Supported**.

Integrations, apps, and add-ons designated as **Not Actively Supported** are not supported by ThreatQuotient's Customer Support team.

While you can report issues to ThreatQ's Customer Support team regarding the integration/app/add-on, you are solely responsible for ensuring proper functionality and version compatibility of Not Supported designations with the applicable ThreatQuotient software.

If unresolvable functional or compatibility issues are encountered, you may be required to uninstall the integration/app/add-on from your ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

> ⚠ For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply to issues caused by Not Actively Supported integrations/apps/add-ons.

Versioning

- Current integration version `2.0.0`
- Compatible with ThreatQ versions >= `4.45.0`

Introduction

The Exploit DB CDF allows analysts to automatically ingest Exploit Reports from Exploit DB, a website that provides open-source intelligence around exploits, into ThreatQ.

The integration provides the the following feed:

- **Exploit DB** - ingests verified and unverified exploits from Exploit DB.

The integration ingests the following system objects:

- Indicators
  - Indicator Attributes
- Reports
  - Report Attributes.

The Exploit DB CDF replaces the existing ThreatQ Exploit DB Connector.

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 integration.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

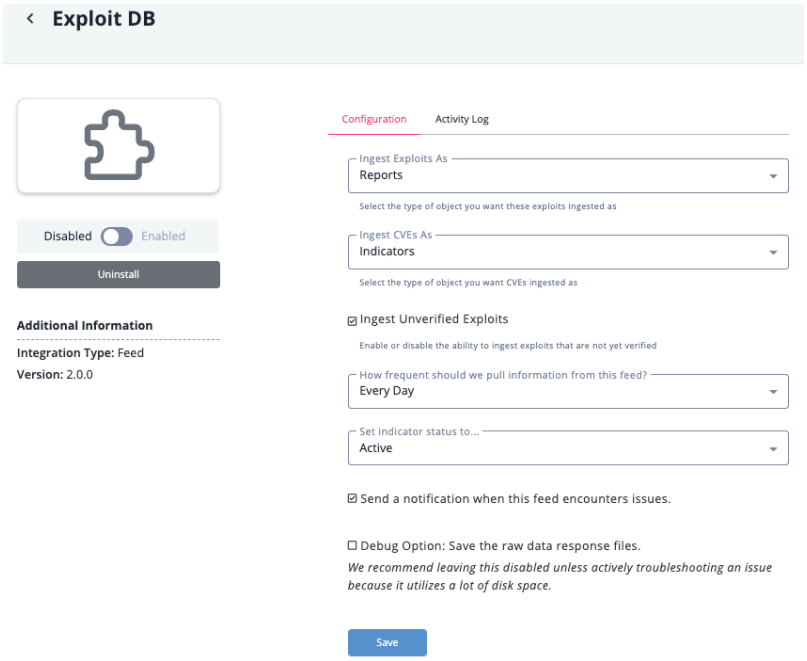
To configure the integration:

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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Ingest Exploits As	Select how to ingest Exploits into ThreatQ. Options include: ◦ Reports (default) ◦ Malware ◦ Vulnerabilities > You have the option of selecting two or all types.
Ingest CVEs As	Select how to ingest CVEs into ThreatQ. Options include: ◦ Indicators (default) ◦ Vulnerabilities > You have the option of selecting two or all types.
Ingest Unverified Exploits	Select whether or not to ingest unverified exploits. This option is selected by default.



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.

Known Issue / Limitations

- The Exploit DB API does not allow time-fencing. Users will need to check the last result of each request to verify that it falls within the last run timeframe.

Change Log

- **Version 2.0.0**
  - Initial Release of the CDF - replaces the Exploit DB Custom Connector.
  - Added the option to ingest CVEs as Vulnerabilities.
  - Added the option to choose what objects the exploits are ingested as.
  - Removed the option to ingest the vulnerable applications (actual binaries).