ThreatQuotient

Qualys Knowledgebase CDF

Version 1.0.0

April 29, 2024

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

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	>= 5.25.0
Support Tier	ThreatQ Supported

Introduction

The Qualys Knowledgebase CDF ingests vulnerabilities from the Qualys Knowledgebase into the ThreatQ platform.

The integration provides the following feed:

- **Qualys Knowledgebase Vulnerabilities** - ingests vulnerabilities from Qualys Knowledgebase.

The integration ingests the following system object types:

- Indicators
- Vulnerabilities

> The Qualys Knowledgebase CDF replaces the Qualys Knowledgebase Connector.

Prerequisites

The following is required for the integration:

- Qualys Hostname
- Qualys Username
- Qualys password associated with the username

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

   > 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 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.

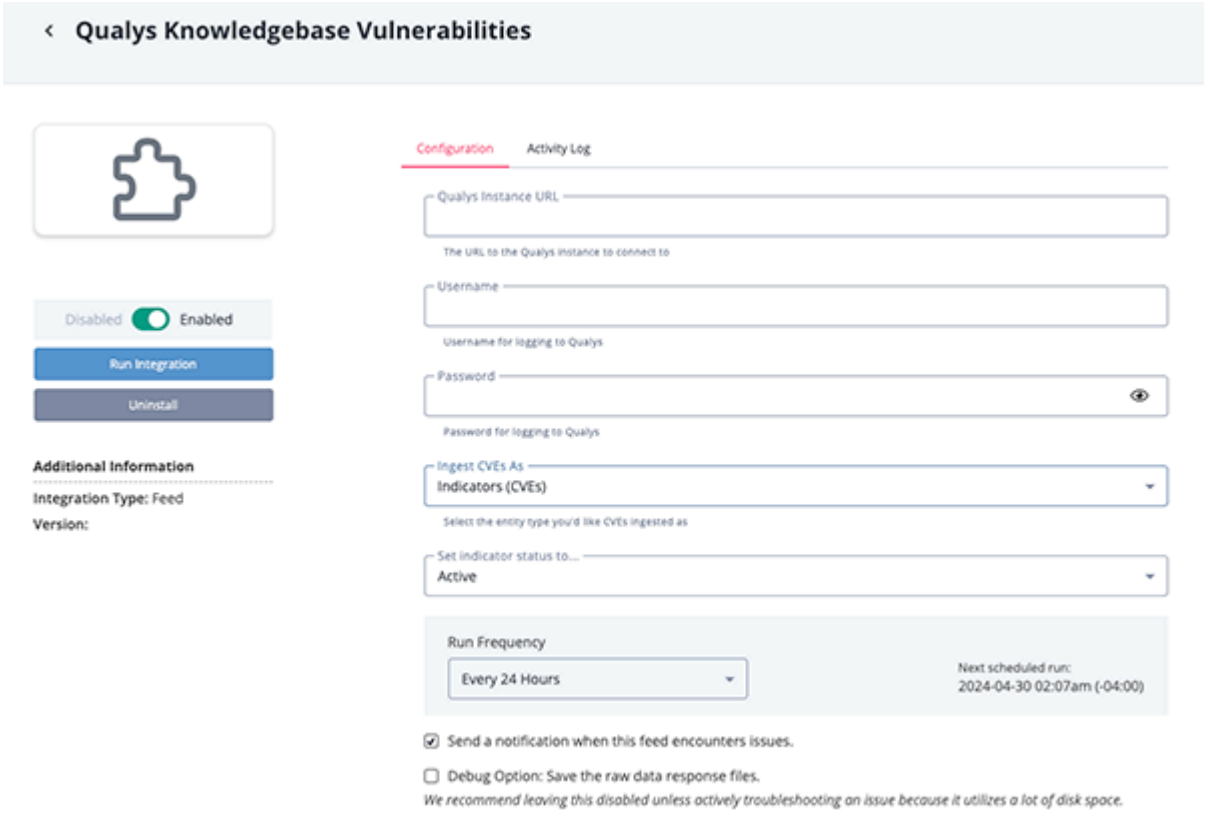
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** 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
Qualys Instance URL	Enter your Qualys instance URL.
Username	Enter your Qualys username.
Password	Enter your Qualys password associated with the username above.
Ingest CVEs As	Select how to ingest CVEs into the ThreatQ platform. Options include **Indicators** and **Vulnerabilities**.



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

Qualys Knowledgebase Vulnerabilities

The Qualys Knowledgebase Vulnerabilities feed pulls the list of vulnerabilities from Qualys Knowledgebase and ingests them into ThreatQ.

`POST {{QUALYS_HOSTNAME}}/api/2.0/fo/knowledge_base/vuln`

Sample Body:

```
{
  "action": "list",
  "details": "Basic",
  "last_modified_after": "2024-04-23T00:00:00Z",
  "last_modified_before": "2024-04-24T00:00:00Z"
}
```

Truncated Sample Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
        "https://qualysapi.qg2.apps.qualys.com/api/2.0/fo/knowledge_base/vuln/
knowledge_base_vuln_list_output.dtd">
<!-- This report was generated with an evaluation version of  //-->
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-04-23T07:36:41Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>38173</QID>
                <VULN_TYPE>Vulnerability or Potential Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>2</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[SSL Certificate - Signature Verification Failed
Vulnerability]]>
                </TITLE>
                <CATEGORY>General remote services</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2022-02-28T13:28:19Z</
LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2003-01-29T20:37:41Z</PUBLISHED_DATETIME>
                <PATCHABLE>0</PATCHABLE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
                        <PRODUCT>
                            <![CDATA[dns_server]]>
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[multi-vendor]]>
```

```
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
                        <ID>
                            <![CDATA[Joomla! Security]]>
                        </ID>
                        <URL>
                            <![CDATA[https://developer.joomla.org/security-
centre/894-20230201-core-improper-access-check-in-webservice-endpoints.html]]>
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2023-23752]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2023-23752]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                    <![CDATA[An SSL Certificate associates an entity (person,
organization, host, etc.) with a Public Key. ]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                    <![CDATA[By exploiting this vulnerability, man-in-the-
middle attacks in tandem with DNS cache poisoning can occur.]]>
                </CONSEQUENCE>
                <SOLUTION>
                    <![CDATA[Please install a server certificate signed by a
trusted third-party Certificate Authority.]]>
                </SOLUTION>
                <PCI_FLAG>1</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="5">
                        <![CDATA[Easy_Exploit]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="8">
                        <![CDATA[No_Patch]]>
                    </THREAT_INTEL>
                </THREAT_INTELLIGENCE>
                <DISCOVERY>
                    <REMOTE>1</REMOTE>
                </DISCOVERY>
            </VULN>
```

```
        </VULN_LIST>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
        <!-- This report was generated with an evaluation version of  //-->
        <!-- CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the
QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no
warranty that the information contained in this report is complete or error-
free. Copyright 2023, Qualys, Inc. //-->
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].TITLE	Vulnerability Value	N/A	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	Certificate - Signature Verification Failed Vulnerability	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].DIAGNOSIS	Vulnerability Description	N/A	N/A	An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key.	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].QID	Vulnerability Attribute	Qualys Id	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	38173	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].VULN_TYPE	Vulnerability Attribute	Vulnerability Type	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	Vulnerability or Potential Vulnerability	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].SEVERITY_LEVEL	Vulnerability Attribute	Severity	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	2	Value updated at ingestion.
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CATEGORY	Vulnerability Attribute	Category	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	General remote services	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].PATCHABLE	Vulnerability Attribute	Patchable	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	NO	Mapped to YES/NO. Value updated at ingestion.
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].PCI_FLAG	Vulnerability Attribute	PCI Flag	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	1	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].SOFTWARE_LIST.SOFTWARE[].PRODUCT	Vulnerability Attribute	Product	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	dns_server	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].SOFTWARE_LIST.SOFTWARE[].VENDOR	Vulnerability Attribute	Vendor	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	multi-vendor	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].VENDOR_REFERENCE_LIST.VENDOR_REFERENCE.ID	Vulnerability Attribute	Vendor Reference Id	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	Joomla! Security	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].VENDOR_REFERENCE_LIST.VENDOR_REFERENCE.URL	Vulnerability Attribute	Vendor Reference URL	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	https://developer.joomla.org/security-centre/894-20230201-core-improper-access-check-in-webservice-endpoints.html	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.BASE	Vulnerability Attribute	CVSS Base Score	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	Value updated at ingestion.
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.TEMPORAL	Vulnerability Attribute	CVSS Temporal	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	Value updated at ingestion
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.ACCESS.VECTOR	Vulnerability Attribute	CVSS Access Vector	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.ACCESS.COMPLEXITY	Vulnerability Attribute	CVSS Access Complexity	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.IMPACT.CONFIDENTIALITY	Vulnerability Attribute	CVSS Confidentiality Impact	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.IMPACT.INTEGRITY	Vulnerability Attribute	CVSS Integrity Impact	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.IMPACT.AVAILABILITY	Vulnerability Attribute	CVSS Availability Impact	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.AUTHENTICATION	Vulnerability Attribute	CVSS Authentication	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.EXPLOITABILITY	Vulnerability Attribute	CVSS Exploitability	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.REMEDIATION_LEVEL	Vulnerability Attribute	CVSS Remediation Level	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.REPORT_CONFIDENCE	Vulnerability Attribute	CVSS Report Confidence	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVE_LIST.CVE[].ID	Related Indicator/ Vulnerability Value	CVE	N/A	CVE-2023-23752	Ingested according to `Ingest CVEs As`

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	2 minutes
Vulnerabilities	1,291
Vulnerability Attributes	5,005

Change Log

- **Version 1.0.0**
  - Initial release