ThreatQuotient

A Securonix Company

Censys ASM CDF

Version 1.0.0

August 04, 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

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	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The Censys ASM CDF integration allows ThreatQ to automatically ingest risk instances from Censys ASM. These risk instances are generated by Censys ASM's continuous scanning of the internet and provide information about an organization's internet-facing assets, including vulnerabilities, misconfigurations, and other security issues. By ingesting these risk instances into ThreatQ, security teams can correlate them with other threat intelligence and security data to gain a more comprehensive view of their organization's security posture and identify potential risks.

The integration provides the following feed:

- **Censys ASM Risk Instances -** ingests risk instances from Censys ASM.

The integration ingests the following object types:

- Assets
- Indicators (CVEs)
- Events (Risk Instances)
- Vulnerabilities

Prerequisites

The following is required to run the integration:

- A Censys ASM API key.

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:

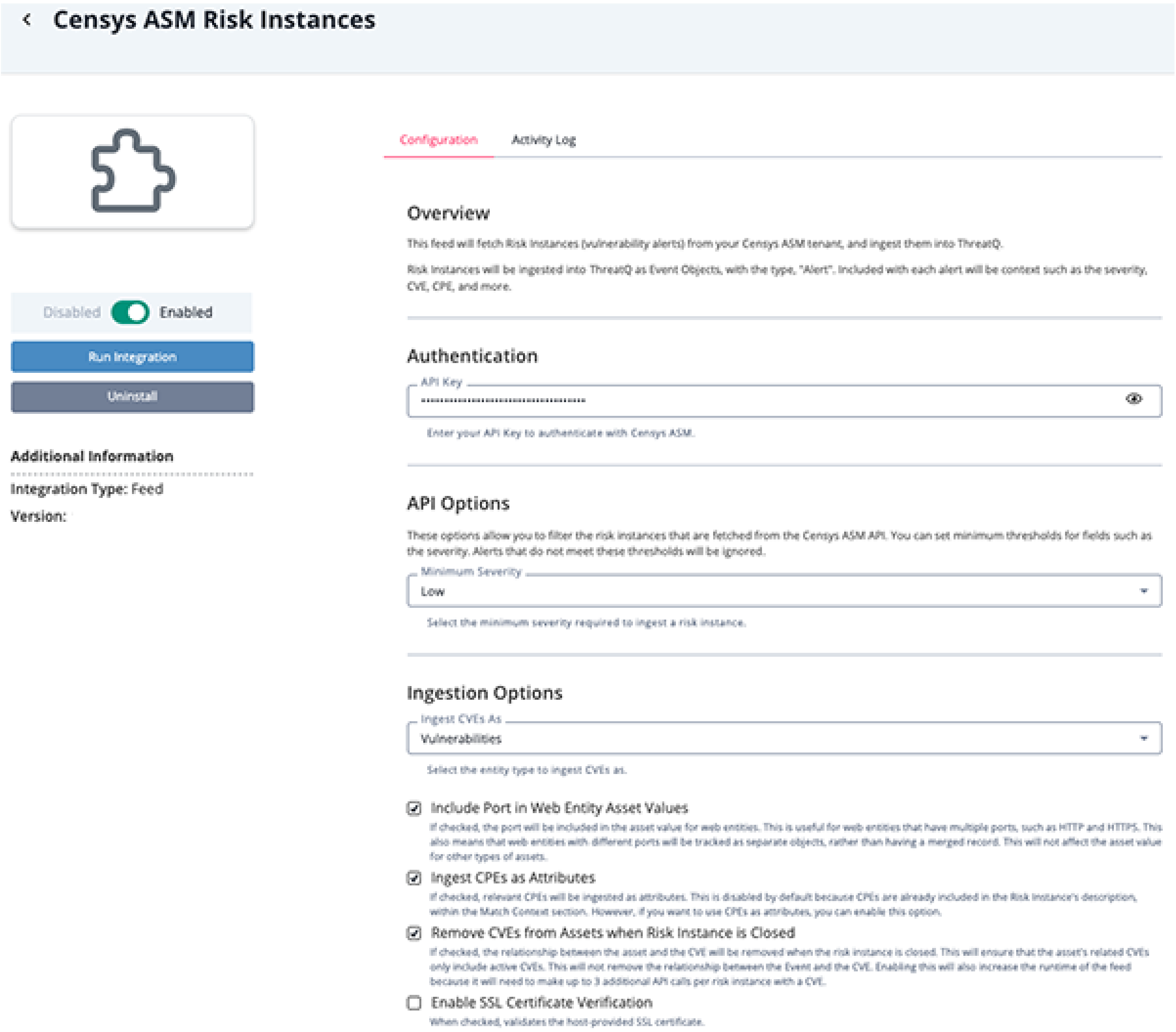
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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
API Key	Enter your API Key to authenticate with Censys ASM.
Minimum Severity	Select the minimum severity required to ingest a risk instance. Options include: ◦ Low ◦ Medium *(default)* ◦ High ◦ Critical
Ingest CVEs As	Select the entity type to ingest the CVEs as in the ThreatQ platform. Options include: ◦ Vulnerabilities *(default)* ◦ Indicators (Type: CVE)
Include Port in Web Entity Asset Values	Enable this parameter to include the port in the asset value for web entities. This parameter is disabled by default. This is useful for web entities that have multiple ports, such as HTTP and HTTPS. This also means that web entities with different ports will be tracked as separate objects, rather than having a merged record. This will not affect the asset value for other types of assets.

PARAMETER	DESCRIPTION
Ingest CPEs as Attributes	Enable this parameter to ingest relevant CPEs as attributes. This is disabled by default as CPEs are already included in the Risk Instance's description within the Match Context section.
Remove CVEs from Assets when Risk Instance is Closed	Enable this parameter to remove the relationship between the asset and the CVE when the risk instance has closed. This will ensure that the asset's related CVEs only include active CVEs. This will not remove the relationship between the Event and the CVE. ⚠ Enabling this parameter will also increase the runtime of the feed because it will need to make up to 3 additional API calls per risk instance with a CVE.
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.



Censys ASM Risk Instances

Additional Information

Integration Type: Feed

Version:

Overview

This feed will fetch Risk Instances (vulnerability alerts) from your Censys ASM tenant, and ingest them into ThreatQ.

Risk Instances will be ingested into ThreatQ as Event Objects, with the type, "Alert". Included with each alert will be context such as the severity, CVE, CPE, and more.

Authentication

API Key: ••••••••••••••••••••••••••••••••••••

Enter your API Key to authenticate with Censys ASM.

API Options

These options allow you to filter the risk instances that are fetched from the Censys ASM API. You can set minimum thresholds for fields such as the severity. Alerts that do not meet these thresholds will be ignored.

Minimum Severity: Low

Select the minimum severity required to ingest a risk instance.

Ingestion Options

Ingest CVEs As: Vulnerabilities

Select the entity type to ingest CVEs as.

☑ Include Port in Web Entity Asset Values

If checked, the port will be included in the asset value for web entities. This is useful for web entities that have multiple ports, such as HTTP and HTTPS. This also means that web entities with different ports will be tracked as separate objects, rather than having a merged record. This will not affect the asset value for other types of assets.

☑ Ingest CPEs as Attributes

If checked, relevant CPEs will be ingested as attributes. This is disabled by default because CPEs are already included in the Risk Instance's description, within the Match Context section. However, if you want to use CPEs as attributes, you can enable this option.

☑ Remove CVEs from Assets when Risk Instance is Closed

If checked, the relationship between the asset and the CVE will be removed when the risk instance is closed. This will ensure that the asset's related CVEs only include active CVEs. This will not remove the relationship between the Event and the CVE. Enabling this will also increase the runtime of the feed because it will need to make up to 3 additional API calls per risk instance with a CVE.

☐ Enable SSL Certificate Verification

When checked, validates the host-provided SSL certificate.

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

Censys ASM Risk Instances

The Censys ASM Risk Instance feed ingests risk instances along with the affected assets discovered by Censys ASM. Risk instances will be ingested as Event objects (Alerts) and will be related to the affected assets. When a vulnerability is detected, the underlying CVE will be ingested into ThreatQ and related to the affected assets.

The CVE will be unrelated from the asset when a vulnerable asset has been fixed if the **Remove CVEs from Assets when Risk Instance is Closed** parameter has been enabled. In this case, the Event object will remain related to the asset.

`POST https://app.censys.io/api/v2/risk-instances/search`

```
{
    "total": 1495,
    "nextPage": 2,
    "risks": [
        {
            "id": 1333,
            "context": {
                "ip": "15.12.135.98",
                "name": "",
                "port": 443,
                "type": "host",
                "service": "HTTPS",
                "transport": "TCP"
            },
            "displayName": "HTTP Missing Common Security Headers",
            "severity": "medium",
            "status": "closed",
            "firstComputedAt": "2024-11-06T16:22:12Z",
            "lastUpdatedAt": "2024-11-11T14:02:52Z",
            "lastComputedAt": "2024-11-06T16:22:12Z",
            "categories": [
                [
                    "Misconfiguration",
                    "Service Misconfiguration",
                    "Web Misconfiguration"
                ]
            ],
            "type": {
                "id": "missing-common-security-headers",
                "name": "HTTP Missing Common Security Headers",
                "description": "This service did not present any common
security headers, such as CSP, CORS, or STS. The lack of these headers may make
the affected service a target.",
                "remediations": [
                    "Configure the affected service with security headers, such 
as CSP, CORS, or STS."
                ],
                "subjectType": "SERVICE",
                "contextType": "host",
                "enabled": true,
                "config": {},
                "severity": "medium",
                "recommendedSeverity": "medium",
                "categories": [
                    [
                        "Misconfiguration",
                        "Service Misconfiguration",
                        "Web Misconfiguration"
                    ]
                ],
                "riskCount": 157,
                "activeRiskCount": 129,
                "events": [],
                "lastUpdatedAt": "2024-09-18T22:58:58Z",
                "addedAt": "2022-08-30T16:34:41Z",
                "references": [
                    "https://github.com/projectdiscovery/nuclei-templates",
                    "https://github.com/projectdiscovery/nuclei-templates/blob/
18d54f52049460541d5600ade977772f309ac382/misconfiguration/http-missing-
security-headers.yaml"
                ],
                "confidence": "moderate"
            }
        },
        {
            "id": 1708,
            "context": {
                "ip": "52.12.87.14",
                "name": "",
                "port": 80,
                "type": "host",
                "service": "HTTP",
                "transport": "TCP"
            },
            "displayName": "Vulnerable microsoft internet_information_services 
[CVE-2007-0087]",
            "severity": "high",
            "status": "closed",
            "firstComputedAt": "2024-11-06T16:22:12Z",
            "lastUpdatedAt": "2024-11-11T14:02:52Z",
            "lastComputedAt": "2024-11-06T16:22:12Z",
            "categories": [
                [
                    "Vulnerability",
                    "Software Vulnerability",
                    "CVE"
                ]
            ],
            "type": {
                "id": "cve:microsoft-internet_information_services-
CVE-2007-0087",
                "name": "Vulnerable microsoft internet_information_services
[CVE-2007-0087]",
                "description": "This software has a known vulnerability that
could be exploited by an attacker. The Common Vulnerabilities and Exposures
(CVE) system provides a reference-method for publicly known information-
security vulnerabilities and exposures.",
                "remediations": [
                    "Update the software to the latest version to mitigate the
risk of exploitation."
                ],
                "subjectType": "SOFTWARE",
                "contextType": "host",
                "enabled": true,
                "config": {},
                "severity": "high",
                "recommendedSeverity": "high",
                "categories": [
                    [
                        "Vulnerability",
                        "Software Vulnerability",
                        "CVE"
                    ]
                ],
                "riskCount": 60,
                "activeRiskCount": 52,
                "events": [],
                "lastUpdatedAt": "2024-11-06T21:06:39Z",
                "addedAt": "2024-07-29T18:55:14Z",
                "cvss_v2": 7.8,
                "rollupName": "Vulnerable microsoft
internet_information_services",
                "references": [
                    "https://nvd.nist.gov/vuln/detail/CVE-2007-0087"
                ],
                "confidence": "strong"
            },
            "matchContext": {
                "found": {
                    "services.software.uniform_resource_identifier":
"cpe:2.3:a:microsoft:internet_information_services:10.0:*:*:*:*:*:*:*"
                }
            }
```

```
        }
    ]
}
```

ThreatQ provides the following default mapping for this feed based on each item within the API response's `.risks` array:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.type.rollupName`, `.type.name`, `.context.name`, `.context.ip`, `.context.domain`, `.severity`	Event.Title	Risk Instance	`.firstComputedAt`	Vulnerable f5 nginx | Asset: 15.156.128.25 | Severity: Critical	Fields are concatenated together to build the title. Some fields may be empty.
`.status`	Event.Attribute	Status	`.firstComputedAt`	`open`	Updatable. The status of the risk instance.
`.categories[]`	Event.Attribute	Category	`.firstComputedAt`	`Misconfiguration`	The category of the risk instance.
`.confidence`, `.type.confidence`	Event.Attribute	Confidence	`.firstComputedAt`	`Strong`	Updatable. The confidence level of the risk instance. Title-cased.
`.metadata[].cloud`	Event.Attribute	Cloud Service	`.firstComputedAt`	`AWS`	The cloud service associated with the risk instance.
`.matchContext.found.services['tls.certificates.leaf_data.pubkey_algorithm']`	Event.Attribute	Public Key Algorithm	`.firstComputedAt`	`RSA`	The public key algorithm associated with the risk instance.
`.matchContext.found['services.tls.versions.tls_version']`	Event.Attribute	TLS Version	`.firstComputedAt`	`1.2`	The TLS version associated with the risk instance.
`.matchContext.found['services.tls.certificates.chain.fingerprint']`	Event.Attribute	Certificate Fingerprint	`.firstComputedAt`	N/A	The certificate fingerprint associated with the risk instance.
`.type.rollupName`, `.type.name`	Event.Attribute	Risk Type	`.firstComputedAt`	`Vulnerable f5 nginx`	The issue of the risk instance. `.type.name` is used only if `.type.rollupName` is missing
N/A	Event.TAG	N/A	N/A	`Closed`	For events with `.status` 'closed'
`.severity`	Event.Attribute, Vulnerability.Attribute, Indicator.Attribute	Severity	`.firstComputedAt`	`Critical`	Updatable. The severity of the risk instance. Shared with the relevant CVEs. Title-cased.
`.type.subjectType`	Event.Attribute, Vulnerability.Attribute, Indicator.Attribute	Subject Type	`.firstComputedAt`	`SOFTWARE`	The subject type of the risk instance. Shared with the relevant CVEs. Title-cased.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.matchContext.found['services.service_name']`	Event.Attribute, Vulnerability.Attribute, Indicator.Attribute	Affected Service	`.firstComputedAt`	`nginx`	The service name associated with the risk instance. Shared with the relevant CVEs.
`.matchContext.found['services.software.uniform_resource_identifier']`	Event.Attribute, Vulnerability.Attribute, Indicator.Attribute	CPE	`.firstComputedAt`	`cpe:2.3:a:microsoft:internet_information_services:10.0:*:*:*:*:*:*:*`	User-configurable. The CPE is associated with the risk instance. Shared with the relevant CVEs.
`.context.cpe[]`	Event.Attribute, Vulnerability.Attribute, Indicator.Attribute	CPE	`.firstComputedAt`	`cpe:2.3:a:microsoft:internet_information_services:10.0:*:*:*:*:*:*:*`	User-configurable. The CPE is associated with the risk instance. Shared with the relevant CVEs.
`.type.cvss_v2`	Vulnerability.Attribute, Indicator.Attribute	CVSSv2 Base Score	`.firstComputedAt`	`7.8`	Updatable. The CVSSv2 score associated with the relevant CVEs
`.type.cvss_v3`	Vulnerability.Attribute, Indicator.Attribute	CVSSv3 Base Score	`.firstComputedAt`	`9.1`	Updatable. The CVSSv3 score associated with the relevant CVEs
`.context.ip` or `.context.name`	Asset.Value	Asset	`.firstComputedAt`	`52.12.87.14`	If `.context.type` is 'host'
`.context.name` or `.context.domain` or `.context.ip`	Asset.Value	Asset	`.firstComputedAt`	N/A	If `.context.type` is 'webentity'
`.context.domain` or `.context.name`	Asset.Value	Asset	`.firstComputedAt`	N/A	If `.context.type` is 'domain'
`.context.certificate` or `.context.name`	Asset.Value	Asset	`.firstComputedAt`	N/A	If `.context.type` is 'certificate'
`.context.type`, `identifier`, `.context.type`	Asset.Attribute	Censys ASM Link	`.firstComputedAt`	`https://app.censys.io/hosts/52.12.87.14`	Link constructed from multiple response parts. `Identifier` is one of:`.context.name` or `.context.domain` or `.context.ip` based on `.context.type`.
`.context.name`	Asset.Attribute	Hostname	`.firstComputedAt`	`acme.com`	The web-entity name associated with the risk instance.
`.context.ip`	Asset.Attribute	IP Address	`.firstComputedAt`	`52.12.87.14`	The IP address associated with the risk instance.
`.context.domain`	Asset.Attribute	Domain	`.firstComputedAt`	`acme.com`	The domain associated with the risk instance.
`.context.certificate`	Asset.Attribute	Certificate	`.firstComputedAt`	N/A	The certificate is associated with the risk instance.
`.context.port`	Asset.Attribute	Port	`.firstComputedAt`	`80`	The port associated with the risk instance.
`.context.type`	Asset.Attribute	Type	`.firstComputedAt`	`host`	The type of asset associated with the risk instance.
`.type.name`	Indicator.Value, Vulnerability.Value	CVE	`.firstComputedAt`	`CVE-2025-24121`	Relevant CVE associated with Risk Instance. Parsed using regular expressions.

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
Assets	333
Asset Attributes	1587
Events	565
Event Attributes	4,815
Indicators	43
Indicator Attributes	212

Change Log

- **Version 1.0.0**
  - Initial release