ThreatQuotient

SentinelOne CDF

Version 1.1.0

September 16, 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 **3**
Support **4**
Integration Details **5**
Introduction **6**
Installation **7**
Configuration **8**
SentinelOne Threats 8
SentinelOne Applications 10
ThreatQ Mapping **12**
SentinelOne Threats 12
SentinelOne Threat Notes (supplemental) 19
SentinelOne Applications 20
SentinelOne Vulnerabilities (supplemental) 22
Average Feed Run **24**
SentinelOne Threats and SentinelOne Threat Notes 24
SentinelOne Applications and SentinelOne Vulnerabilities 25
Change Log **26**

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	1.1.0
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

SentinelOne is a cloud EDR product. Agents are deployed to computers/endpoints, monitoring and reporting back any malicious activity to the SentinelOne dashboard. The ThreatQ integration for SentinelOne allows the ingestion of various reports and detections from SentinelOne.

The integrations provides the following feeds:

- **SentinelOne Threats** - ingests any threats/incidents from SentinelOne.
- **SentinelOne Threat Notes** (supplemental) - fetches notes associated with a given threat/incident.
- **SentinelOne Applications** - ingests reports on vulnerable applications.
- **SentinelOne Vulnerabilities** (supplemental) - fetches the CVEs associated with a given application.

The integration ingests the following system objects:

- Attack Patterns
  - Attack Pattern Attributes
- Incidents
  - Incident Attributes
- Indicators
  - Indicator Attributes
- Reports
  - Report Attributes

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
   - Select the individual feeds to install, when prompted, and click on **Install**.

     > 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).

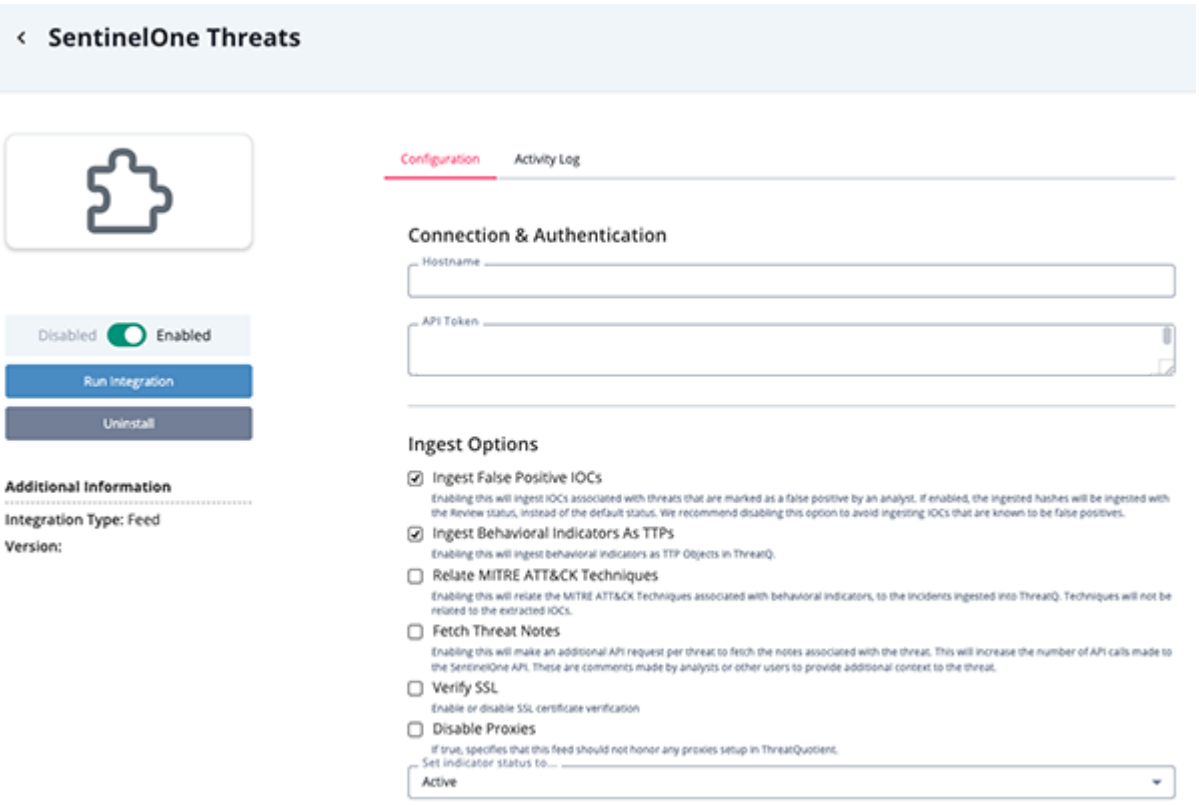
   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

SentinelOne Threats

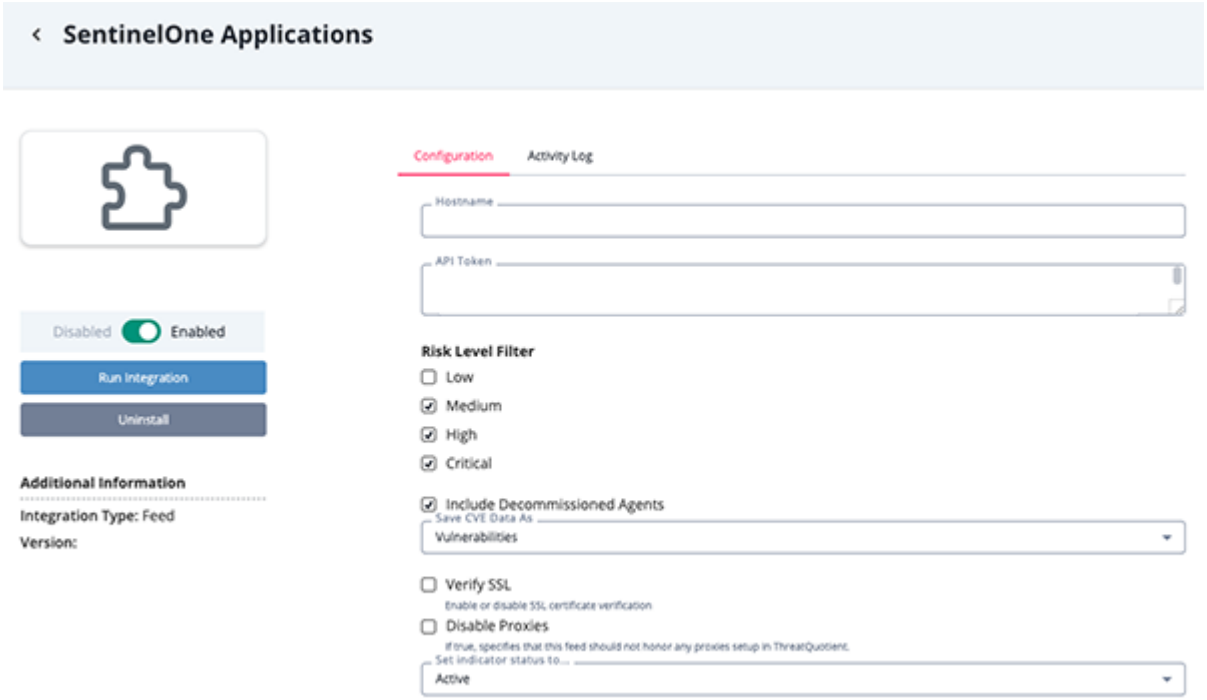
PARAMETER	DESCRIPTION
Hostname	Your SentinelOne hostname.
API Token	Your SentinelOne API Token. This can be generated by accessing the My User section in SentinelOne and clicking on **Generate API Key**.
Ingest False Positive IOCs	Enable this option to ingest IOCs associated with threats that are marked as a false positive by an analyst. If enabled, the ingested hashes will be ingested with the Review status opposed to the default status. **ThreatQuotient recommends disabling this option to avoid ingesting IOCs that are known to be false positives.**
Ingest Behavioral Indicators as TTPs	Enable this option to ingest behavioral indicators as TTP Objects in ThreatQ.

PARAMETER	DESCRIPTION
Relate MITRE ATT&CK Techniques	Enable this option to relate the MITRE ATT&CK Techniques associated with behavioral indicators, to the Incidents ingested into ThreatQ. Techniques will not be related to the extracted IOCs.
Fetch Threat Notes	Enable this option to make an additional API request per threat to fetch the notes associated with the threat. This will increase the number of API calls made to the SentinelOne API. These are comments made by analysts or other users to provide additional context to the threat.
Verify SSL	Enable this option if the feed should verify the SSL certificate.
Disable Proxies	Enable this option to have the feed ignore proxies set in the ThreatQ UI.



SentinelOne Applications

PARAMETER	DESCRIPTION
Hostname	Your SentinelOne hostname.
API Token	Your SentinelOne API Token. This can be generated by accessing the My User section in SentinelOne and clicking on **Generate API Key**.
Risk Level Filter	Select the risk levels for the ingested reports. Options Include: ◦ Low ◦ Medium ◦ High ◦ Critical
Include Decommissioned Agents	Check the checkbox to indicate that vulnerable applications from decommissioned agents should be included. This parameter is not selected by default.
Save CVE Data as	Use the checkboxes to select whether to import CVEs as Vulnerability objects, Indicator objects, or both. Options Include: ◦ Indicator (default) ◦ Vulnerability
Verify SSL	Enable this option if the feed should verify the SSL certificate.
Disable Proxies	Enable this option to have the feed ignore proxies set in the ThreatQ UI.



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

SentinelOne Threats

This feed enables ThreatQ to ingest any threats/incidents from SentinelOne.

`GET https://<hostname>/web/api/v2.1/threats`

Sample Response:


```
{
  "data": [
    {
      "agentDetectionInfo": {
        "accountId": "433241117337583618",
        "accountName": "SentinelOne",
        "agentDomain": "WORKGROUP",
        "agentIpV4": "192.168.15.128",
        "agentIpV6": "fe80::c515:245:4d1c:dd5a",
        "agentLastLoggedInUserName": "Admin",
        "agentMitigationMode": "detect",
        "agentOsName": "Windows 10 Home",
        "agentOsRevision": "19041",
        "agentRegisteredAt": "2020-10-09T15:26:27.714827Z",
        "agentUuid": "3d061b5e88b6422ba111b22d5102f838",
        "agentVersion": "4.4.2.143",
        "externalIp": "71.121.180.128",
        "groupId": "991892612147246915",
        "groupName": "Default Group",
        "siteId": "991892612138858306",
        "siteName": "Threat Quotient"
      },
      "agentRealtimeInfo": {
        "accountId": "433241117337583618",
        "accountName": "SentinelOne",
        "activeThreats": 0,
        "agentComputerName": "DESKTOP-NBF06HK",
        "agentDecommissionedAt": true,
        "agentDomain": "WORKGROUP",
        "agentId": "998482485444708204",
        "agentInfected": false,
        "agentIsActive": false,
        "agentIsDecommissioned": true,
        "agentMachineType": "laptop",
        "agentMitigationMode": "protect",
        "agentNetworkStatus": "connected",
        "agentOsName": "Windows 10 Home",
        "agentOsRevision": "19041",
        "agentOsType": "windows",
```

```
        "agentUuid": "3d061b5e88b6422ba111b22d5102f838",
        "agentVersion": "4.4.2.143",
        "groupId": "991892612147246915",
        "groupName": "Default Group",
        "networkInterfaces": [],
        "operationalState": "na",
        "rebootRequired": false,
        "scanAbortedAt": null,
        "scanFinishedAt": "2020-10-09T15:43:32.446707Z",
        "scanStartedAt": "2020-10-09T15:27:30.437044Z",
        "scanStatus": "finished",
        "siteId": "991892612138858306",
        "siteName": "Threat Quotient",
        "userActionsNeeded": []
      },
      "id": "998516837801102892",
      "indicators": [
        {
          "category": "Hiding/Stealthiness",
          "description": "The majority of sections in this PE have high
entropy, a sign of obfuscation or packing.",
          "ids": [29],
          "tactics": []
        }
      ],
      "mitigationStatus": [
        {
          "action": "quarantine",
          "actionsCounters": {
            "failed": 0,
            "notFound": 0,
            "pendingReboot": 0,
            "success": 1,
            "total": 1
          },
          "agentSupportsReport": true,
          "groupNotFound": false,
          "lastUpdate": "2020-10-09T16:35:41.189765Z",
          "latestReport": "/threats/mitigation-report/998517327284768348",
          "status": "success"
        }
      ],
      "threatInfo": {
        "analystVerdict": "true_positive",
        "analystVerdictDescription": "True positive",
        "automaticallyResolved": true,
        "browserType": null,
        "certificateId": "",
        "classification": "Trojan",
        "classificationSource": "Cloud",
```

```
        "cloudFilesHashVerdict": "black",
        "collectionId": "998516837809491501",
        "confidenceLevel": "malicious",
        "createdAt": "2020-10-09T16:34:42.837573Z",
        "detectionEngines": [
          {
            "key": "pre_execution_suspicious",
            "title": "On-Write Static AI - Suspicious"
          }
        ],
        "detectionType": "static",
        "engines": ["On-Write DFI - Suspicious"],
        "externalTicketExists": false,
        "externalTicketId": null,
        "failedActions": false,
        "fileExtension": "EXE",
        "fileExtensionType": "Executable",
        "filePath": "\\Device\\HarddiskVolume3\\Users\\Admin\\AppData\\Local\
\Packages\\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\\AC\\#!001\\MicrosoftEdge\
\Cache\\1R49I5S2\\angelx[1].exe",
        "fileSize": 730624,
        "fileVerificationType": "NotSigned",
        "identifiedAt": "2020-10-09T16:34:42.698000Z",
        "incidentStatus": "resolved",
        "incidentStatusDescription": "Resolved",
        "initiatedBy": "agent_policy",
        "initiatedByDescription": "Agent Policy",
        "initiatingUserId": null,
        "initiatingUsername": null,
        "isFileless": false,
        "isValidCertificate": false,
        "maliciousProcessArguments": null,
        "md5": null,
        "mitigatedPreemptively": false,
        "mitigationStatus": "mitigated",
        "mitigationStatusDescription": "Mitigated",
        "originatorProcess": "MicrosoftEdgeCP.exe",
        "pendingActions": false,
        "processUser": "DESKTOP-NBF06HK\\Admin",
        "publisherName": "",
        "reachedEventsLimit": false,
        "rebootRequired": false,
        "sha1": "06cf2ee722da1726b799da60efcc99c54f6c549a",
        "sha256": null,
        "storyline": "B88994CA52DF6B5E",
        "threatId": "998516837801102892",
        "threatName": "angelx[1].exe",
        "updatedAt": "2020-11-09T09:18:40.894268Z"
      },
      "whiteningOptions": ["hash", "path"]
```

```
    }
  ],
  "pagination": {
    "nextCursor": null,
    "totalItems": 1
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].agentRealtimeInfo.agentComputerName + .data[].agentRealtimeInfo.agentDomain + .data[].threatInfo.threatName + .data[].threatInfo.classification	Incident.Value	N/A	.data[].threatInfo.createdAt	WORKGROUP/DESKTOP-NBF06HK: angelx[1].exe - Trojan	Formated as `<agentDomain>/<agentComputerName>: <threatName> - <classification>`
.data[].*	Incident Description	N/A	N/A	N/A	Various fields concatenated together to build the HTML description.
.data[].agentRealtimeInfo.agentIsActive	Incident.Attribute	Agent Is Active	.data[].threatInfo.createdAt	False	N/A
.data[].agentRealtimeInfo.agentComputerName	Incident.Attribute	Agent Computer Name	.data[].threatInfo.createdAt	DESKTOP-NBF06HK	N/A
.data[].agentRealtimeInfo.agentIsDecommissioned	Incident.Attribute	Agent Is Decommissioned	.data[].threatInfo.createdAt	True	N/A
.data[].agentRealtimeInfo.agentDomain	Incident.Attribute	Agent Domain	.data[].threatInfo.createdAt	WORKGROUP	N/A
.data[].agentRealtimeInfo.agentInfected	Incident.Attribute	Agent Is Infected	.data[].threatInfo.createdAt	False	N/A
.data[].agentRealtimeInfo.agentMachineType	Incident.Attribute	Agent Machine Type	.data[].threatInfo.createdAt	Laptop	N/A
.data[].agentRealtimeInfo.agentNetworkStatus	Incident.Attribute	Agent Network Status	.data[].threatInfo.createdAt	connected	N/A
.data[].agentRealtimeInfo.agentOsName	Incident.Attribute	Agent Operating System	.data[].threatInfo.createdAt	Windows 10 Home	N/A
.data[].agentRealtimeInfo.siteName	Incident.Attribute	Site Name	.data[].threatInfo.createdAt	Threat Quotient	N/A
.data[].agentRealtimeInfo.mitigationStatus[].action data[].agentRealtimeInfo.mitigationStatus[].status	Incident.Attribute	Mitigation Action	.data[].threatInfo.createdAt	Quarantine - Success	Formatted as `<action> - <status>`, title-cased
.data[].threatInfo.analystVerdictDescription	Incident.Attribute / Indicator.Attribute	Analyst Verdict	.data[].threatInfo.createdAt	True positive	Any value except `Undefined`
.data[].threatInfo.classification	Incident.Attribute / Indicator.Attribute	Classification	.data[].threatInfo.createdAt	Trojan	N/A
.data[].threatInfo.classificationSource	Incident.Attribute	Classification Source	.data[].threatInfo.createdAt	Cloud	N/A
.data[].threatInfo.cloudFilesHashVerdict	Incident.Attribute / Indicator.Attribute	Cloud Verdict	.data[].threatInfo.createdAt	Black	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].threatInfo.confidenceLevel	Incident.Attribute / Indicator.Attribute	Confidence Level	.data[].threatInfo.createdAt	Malicious	title-cased
.data[].threatInfo.detectionEngines[].title	Incident.Attribute	Detection Engine	.data[].threatInfo.createdAt	On-Write Static AI - Suspicious	N/A
.data[].threatInfo.engines[]	Incident.Attribute	Engine	.data[].threatInfo.createdAt	On-Write DFI - Suspicious	N/A
.data[].threatInfo.fileExtension	Incident.Attribute	File Extension	.data[].threatInfo.createdAt	EXE	N/A
.data[].threatInfo.fileExtensionType	Incident.Attribute Indicator.Attribute	File Type	.data[].threatInfo.createdAt	executable	N/A
.data[].threatInfo.filePath	Indicator.Value	File Path	.data[].threatInfo.identifiedAt	\Device\HarddiskVolume3\Users\Admin\AppData...	N/A
.data[].threatInfo.fileVerificationType	Incident.Attribute	Signature Verification	.data[].threatInfo.createdAt	NotSigned	N/A
.data[].threatInfo.incidentStatusDescription	Incident.Attribute	Incident Status	.data[].threatInfo.createdAt	Resolved	N/A
.data[].threatInfo.initiatedByDescription	Incident.Attribute	Initiated By	.data[].threatInfo.createdAt	Agent Policy	N/A
.data[].threatInfo.md5	Indicator.Value	MD5	.data[].threatInfo.identifiedAt	N/A	N/A
.data[].threatInfo.mitigatedPreemptively	Incident.Attribute	Mitigated Preemptively	.data[].threatInfo.createdAt	False	N/A
.data[].threatInfo.mitigationStatusDescription	Incident.Attribute	Mitigation Status	.data[].threatInfo.createdAt	Mitigated	N/A
.data[].threatInfo.originatorProcess	Incident.Attribute	Originator Process	.data[].threatInfo.createdAt	MicrosoftEdgeCP.exe	N/A
.data[].threatInfo.sha1	Indicator.Value	SHA-1	.data[].threatInfo.identifiedAt	06cf2ee722da1726b799da60efcc99c54f6c549a	N/A
.data[].threatInfo.sha256	Indicator.Value	SHA-256	.data[].threatInfo.identifiedAt	N/A	N/A
.data[].threatInfo.threatId	Incident.Description / Indicator.Attribute	SentinelOne Link	.data[].threatInfo.createdAt	`https://<hostname>/incidents/threats/998516837801102892/overview`	Formated as `https://<hostname>/incidents/threats/<threatId>/overview`
.data[].threatInfo.threatName	Incident.Attribute / Indicator.Attribute	Threat Name	.data[].threatInfo.createdAt	angelx[1].exe	N/A
.data[].indicators[].description	TTP.Value	N/A	.data[].threatInfo.createdAt	The majority of sections in this PE have high entropy, a sign of obfuscation or packing.	N/A
.data[].indicators[].category	TTP.Attribute	Category	.data[].threatInfo.createdAt	Hiding/Stealthiness	N/A
.data[].indicators[].tactics[].techniques[].name	AttackPattern.Value	N/A	.data[].threatInfo.createdAt	T1234 - Sample Technique	TIDs mapped to values based on

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					Threat Library.
N/A	Incident.Tag	N/A	N/A	`false-positive`	Added when analyst verdict is False positive

SentinelOne Threat Notes (supplemental)

This supplemental feed fetches notes associated with a given threat/incident.

`GET https://<hostname>/web/api/v2.1/threats/<threat_id>/notes`

Sample Response:


```
{
        "data": [
                {
                        "createdAt": "2020-10-13T14:26:22.324599Z",
                        "creator": "John Doe",
                        "creatorId": "991892977211078596",
                        "edited": false,
                        "id": "1001351344132574596",
                        "text": "This is pretty malicious",
                        "updatedAt": "2020-10-13T14:26:22.324607Z"
                }
        ],
        "pagination": {
                "nextCursor": null,
                "totalItems": 2
        }
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].text, / data[].creator	Incident Description	Note	.data[].createdAt	N/A	Inserted into description table

SentinelOne Applications

This feed enables ThreatQ to ingest reports on vulnerable applications.

`GET https://<hostname>/web/api/v2.1/installed-applications`

Sample Response:


```
{
    "data": [
        {
            "agentComputerName": "IEWIN7",
            "agentDomain": "WORKGROUP",
            "agentId": "997055331565582336",
            "agentInfected": false,
            "agentIsActive": false,
            "agentIsDecommissioned": false,
            "agentMachineType": "desktop",
            "agentNetworkStatus": "connected",
            "agentOperationalState": "na",
            "agentOsType": "windows",
            "agentUuid": "d71b5dba05244409b9ba79eb55858370",
            "agentVersion": "3.1.4.50",
            "createdAt": "2020-10-07T16:11:52.447495Z",
            "id": "997055790674098282",
            "installedAt": "2018-03-07T07:52:52.953000Z",
            "name": "Microsoft .NET Framework 4.7.1",
            "osType": "windows",
            "publisher": "Microsoft Corporation",
            "riskLevel": "critical",
            "signed": false,
            "size": 0,
            "type": "app",
            "updatedAt": "2020-10-07T16:11:52.447498Z",
            "version": "4.7.02558"
        }
    ],
    "pagination": {
        "nextCursor": null,
        "totalItems": 1
    }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].name data[].riskLevel + .data[].agentDomain + .data[].agentComputerName	Report.Value	N/A	.data[].createdAt	Vulnerable App (Critical): Microsoft .NET Framework 4.7.1 - WORKGROUP/ IEWIN7	Formatted as "Vulnerable App (<riskLevel>): <name> - <agentDomain>/ <agentComputerName>"
.data[].agentComputerName	Report.Attribute	Agent Computer Name	.data[].createdAt	IEWIN7	N/A
.data[].agentDomain	Report.Attribute	Agent Domain	.data[].createdAt	WORKGROUP	N/A
.data[].agentMachineType	Report.Attribute	Agent Machine Type	.data[].createdAt	desktop	N/A
.data[].agentInfected	Report.Attribute	Agent Is Infected	.data[].createdAt	False	N/A
.data[].agentIsActive	Report.Attribute	Agent Is Active	.data[].createdAt	False	N/A
.data[].agentIsDecommissioned	Report.Attribute	Agent Is Decommissioned	.data[].createdAt	False	N/A
.data[].agentNetworkStatus	Report.Attribute	Agent Network Status	.data[].createdAt	connected	N/A
.data[].name	Report.Attribute	Vulnerable App	.data[].createdAt	Microsoft .NET Framework 4.7.1	N/A
.data[].osType	Report.Attribute	OS Type	.data[].createdAt	windows	N/A
.data[].publisher	Report.Attribute	App Publisher	.data[].createdAt	Microsoft Corporation	N/A
.data[].type	Report.Attribute	App Type	.data[].createdAt	app	N/A
.data[].riskLevel	Report.Attribute	Risk Level	.data[].createdAt	Critical	title-cased

SentinelOne Vulnerabilities (supplemental)

This supplemental feed fetches the CVEs associated with a given application.

`GET https://<hostname>/web/api/v2.1/private/installed-applications/<run_params.app_id>/cves`

Sample Response:


```
{
    "data": {
        "agentComputerName": "IEWIN7",
        "agentDomain": "WORKGROUP",
        "agentId": "997055331565582336",
        "agentInfected": false,
        "agentIsActive": false,
        "agentIsDecommissioned": false,
        "agentMachineType": "desktop",
        "agentNetworkStatus": "connected",
        "agentOperationalState": "na",
        "agentOsType": "windows",
        "agentUuid": "d71b5dba05244409b9ba79eb55858370",
        "agentVersion": "3.1.4.50",
        "createdAt": "2020-10-07T16:11:52.447495Z",
        "cves": [
            {
                "createdAt": "2019-11-10T12:57:47.925235Z",
                "cveId": "CVE-2018-8421",
                "description": "A remote code execution vulnerability exists
when Microsoft .NET Framework processes untrusted input, aka \".NET Framework
Remote Code Execution Vulnerability.\" This affects Microsoft .NET Framework
4.6, Microsoft .NET Framework 3.5, Microsoft .NET Framework 4.7/4.7.1/4.7.2,
Microsoft .NET Framework 3.0, Microsoft .NET Framework 3.5.1, Microsoft .NET
Framework 4.6.2/4.7/4.7.1/4.7.2, Microsoft .NET Framework 4.5.2, Microsoft .NET
Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.1/4.7.2, Microsoft .NET Framework
4.7.1/4.7.2, Microsoft .NET Framework 4.7.2, Microsoft .NET Framework 2.0.",
                "id": "756332566572392821",
                "link": "https://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2018-8421",
                "publishedAt": "2018-09-13 00:29:00",
                "riskLevel": "critical",
                "score": 9.8,
                "updatedAt": "2019-11-10T12:57:47.925242Z"
            }
        ],
        "id": "997055790674098282",
        "installedAt": "2018-03-07T07:52:52.953000Z",
        "name": "Microsoft .NET Framework 4.7.1",
        "osType": "windows",
        "publisher": "Microsoft Corporation",
```

```
        "riskLevel": "critical",
        "signed": false,
        "size": 0,
        "type": "app",
        "updatedAt": "2020-10-07T16:11:52.447498Z",
        "version": "4.7.02558"
    }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
data.cves[].cveId	Indicator.Value / Vulnerability.Value	CVE	.data.cves[].publishedAt	CVE-2018-8421	N/A
.data.cves[].description	Indicator.Description / Vulnerability.Description	N/A	.data.cves[].publishedAt	A remote code execution vulnerability exists when...	N/A
.data.cves[].link	Indicator.Attribute / Vulnerability.Attribute	Reference	.data.cves[].publishedAt	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8421	N/A
.data.cves[].riskLevel	Indicator.Attribute / Vulnerability.Attribute	Risk Level	.data.cves[].publishedAt	Critical	title-cased
.data.cves[].score	Indicator.Attribute / Vulnerability.Attribute	Score	.data.cves[].publishedAt	N/A	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.

SentinelOne Threats and SentinelOne Threat Notes

METRIC	RESULT
Run Time	1 min
Attack Patterns	8
Attack Pattern Attributes	8
Incidents	40
Incident Attributes	1,153
Indicators	33
Indicator Attributes	307

SentinelOne Applications and SentinelOne Vulnerabilities

METRIC	RESULT
Run Time	1 min
Indicators	1
Indicator Attributes	4
Reports	2
Report Attributes	22

Change Log

- **Version 1.1.0**
  - Performed the following updates to the **SentinelOne Threats** feed:
    - Added support for a rich text HTML description with full context of the threat.
    - Notes are now ingested into the description of the ingested Incidents, rather than as attributes.
    - Added support for updating certain attributes to prevent duplicates.
    - Added a new configuration parameter: **Ingest Behavioral Indicators as TTPs**.
    - Added a new configuration parameter: **Relate MITRE ATT&CK Techniques.** This gives users the ability to ingest related MITRE ATT&CK Techniques associated with each tactic used by the threat (optional via user field).
    - Added a new configuration parameter: **Fetch Threat Notes**. This makes fetching and ingesting notes optional via this parameter.
    - Added a new configuration parameter: **Ingest False Positive IOCs**. This gives users the ability to prevent IOCs from being ingested if the threat is marked as False Positive.
    - Added a tag called false-positive to Incidents and Indicators ingested from threats marked as False Positive by an analyst.
    - Removed the ability to ingest behavioral indicators as Attack Patterns.
    - Incidents are no longer ingested with a SentinelOne Link attribute, in favor of the link in the description.
  - Performed the following updates to the **SentinelOne Applications** feed:
    - Removed the option to fetch **Risk Level: None**.
    - The **Risk Level** parameter no longer defaults to **Low**.
    - Added the following new configuration parameters:
      - Verify SSL
      - Disable Proxies
  - Updated the minimum ThreatQ version to 5.12.1.
- **Version 1.0.1**
  - Updated authentication to API Token-based.
- **Version 1.0.0**
  - Initial release