ThreatQuotient

SentinelOne CDF Guide

Version 1.0.0

May 10, 2021

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

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

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.

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.41.0`

Introduction

SentinelOne is an 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.

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

   SentinelOne Threats

PARAMETER	DESCRIPTION
Hostname	Your SentinelOne hostname.
Username	Your SentinelOne username.
Password	Your SentinelOne password.
Ingest Threat Indicators as	Select the objects to ingest as threat indicators. Options Include: • TTPs (default) • Patterns

SentinelOne Applications

PARAMETER	DESCRIPTION
Hostname	Your SentinelOne hostname.
Username	Your SentinelOne username.
Password	Your SentinelOne password.
Risk Level Fitler	Select the risk levels for the ingesed reports. Options Include: • None • 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

5. Review any additional feed 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

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

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


```
{
    "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-NBFO6HK",
                "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-NBFO6HK\\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
    }
}
```

ThreatQ 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	Formatted as "<agentDomain>/<agentComputerName>: <threatName> - <classification>"
.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
.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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].threatInfo.filePath	Indicator.Value	File Path	.data[].threatInfo.identifiedAt	\Device\Harddisk Volume3\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.Attribute / 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 / Attack Pattern.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 / Attack Pattern.Attribute	Category	.data[].threatInfo.createdAt	Hiding/Stealthiness	N/A

SentinelOne Threat Notes (supplemental)

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

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


```
{
        "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
        }
}
```


ThreatQ 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	Indicator.Attribute	Note	.data[].createdAt	N/A	N/A

SentinelOne Applications

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

This feed enables ThreatQ to ingest reports on vulnerable applications.


```
{
    "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
    }
}
```

ThreatQ 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)

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

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


```
{
    "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"
    }
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREA TQ 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.Attribute / Vulnerability.Attribute	Description	.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 Runs

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 1.0.0
  - Initial release