ThreatQuotient

A Securonix Company

SOCRadar CDF

Version 2.0.0

August 17, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	2.0.0
Compatible with ThreatQ Versions	>= 5.19.0
Support Tier	ThreatQ Supported

Introduction

The SOCRadar CDF allows ThreatQ users to pull in data, such as feeds, leaks, alarms, and vulnerabilities, from SOCRadar's API.

SOCRadar is an Extended Threat Intelligence (XTI) tool that is enriched with External Attack Surface Management and Digital Risk Protection. SOCRadar's XTI product combines External Attack Surface Management, Digital Risk Protection, and Cyber Threat Intelligence modules to improve your security posture.

The integration provides the following feeds:

- **SOCRadar Threat Feed** - ingests indicators from SOCRadar's Threat Feeds.
- **SOCRadar Leaks** - ingests leaked credentials for identities within your organization's SOCRadar tenant.
- **SOCRadar Alarms** - ingests alarms from your organization's SOCRadar tenant.
- **SOCRadar Vulnerabilities** - ingests vulnerabilities related to your organization's assets, tracked in your SOCRadar tenant.

The integration ingests the following system object types:

- Assets
- Events
- Identities
- Indicators
- Vulnerabilities

Prerequisites

The following is required to run the integration:

- A SOCRadar License & 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
6. Select the individual feeds to install, when prompted and click **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.

The feed(s) 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:

Threat Feed Parameters

PARAMETER	DESCRIPTION
Feed URLs	Enter a line-separated list of Feed URLs to pull into ThreatQ.
Seen Count Threshold	Enter the minimum number of times an IOC has been seen before ingesting. The default value is 1.
Context Filtering	Select the pieces of context to include with each IOC. Options include: ◦ Tags (default) ◦ Verdict (default) ◦ Classification (default) ◦ Affected Sector (default) ◦ Domain Registration Date ◦ Page Title ◦ File Type ◦ MIME Type ◦ Report Link

PARAMETER	DESCRIPTION
	◦ Score (default) ◦ VirusTotal Score (default) ◦ Category (default) ◦ Related Filename Not all context is available for every IOC.
Geolocation Filtering	Select the pieces of geolocation to include with each IOC. Options include: ◦ ASN ◦ ASN Organization ◦ City ◦ Country Code (default) ◦ Country ◦ Latitude ◦ Longitude ◦ Region ◦ Zip Code Not all context is available for every IOC.

Leaks Parameters

PARAMETER	DESCRIPTION
API Key	Enter your Company API Key to authenticate with the SOCRadar API.
Company ID	Enter your Company ID to fetch data only for your tenant.
Leak Type Filtering	Select the types of leaks to ingest into ThreatQ. Options include: ◦ Employee (default) ◦ VIP Employee (default) ◦ Customer ◦ Botnet Market
Context Filtering	Select the pieces of context to include with each leak event. This will help you filter out any unnecessary data. You may want to filter out information such as the raw passwords, as they may contain sensitive information. Options include: ◦ Tags (default) ◦ Password (Redacted) (default) ◦ Taw Password ◦ Company Domain (default) ◦ Leak Source (default) ◦ Password Type ◦ Line Number ◦ Is False Positive (default) ◦ False Positive Notes (default) ◦ Alarm Link

Incidents Parameters

PARAMETER	DESCRIPTION
API Key	Enter your Company API Key to authenticate requests to the SOCRadar API.
Company ID	Enter your Company ID to retrieve data associated with your tenant.
Results per Page	Specify the number of results to retrieve per API request. The maximum value is `100`. *(default: 100)*
Severity Filtering (Optional)	Select the severity level used to filter incidents. Select `All` to retrieve incidents across all severity levels. Options include: ◦ All *(default)* ◦ Info ◦ Low ◦ Medium ◦ High ◦ Critical
Status Filtering (Optional)	Select the status used to filter incidents. Select `All` to retrieve incidents across all statuses. Options include: ◦ All *(default)* ◦ Open ◦ Closed ◦ On Hold
Main Type Selection (Optional)	Select one or more main incident types to ingest into ThreatQ. If no value is selected, incidents from all main types are retrieved.

PARAMETER	DESCRIPTION
Sub Type Selection (Optional)	Select one or more incident subtypes to ingest into ThreatQ. If no value is selected, incidents from all subtypes are retrieved.
Alarm Title Filtering (Optional)	Select one or more alarm titles to ingest into ThreatQ. If no value is selected, incidents associated with all alarm titles are retrieved.
Alarm Type IDs (Optional)	Enter a comma-separated list of alarm type IDs to filter incidents.
Notification IDs (Optional)	Enter a comma-separated list of notification IDs to filter incidents.
Alarm IDs (Optional)	Enter a comma-separated list of alarm IDs to filter incidents.
Rule IDs (Optional)	Enter a comma-separated list of rule IDs to filter incidents.
Context Filtering	Select the contextual data to include with each incident. Options include: ◦ Tags *(default)* ◦ Main Type *(default)* ◦ Sub Type *(default)* ◦ Generic Title *(default)* ◦ Severity *(default)* ◦ Status *(default)* ◦ Company Name *(default)* ◦ Source *(default)* ◦ Category *(default)* ◦ Maintainer *(default)* ◦ First Seen Date

PARAMETER	DESCRIPTION
	◦ Last Update Date ◦ Update Frequency ◦ Related CVEs *(default)* ◦ Related Attack Patterns *(default)* ◦ Assets (IPs & Domains) *(default)* ◦ CPEs ◦ Alarm Response *(default)* ◦ Detection and Analysis ◦ Default Mitigation Plan ◦ Post Incident Analysis ◦ Compliance Framework ◦ Control Item ◦ Compliance Description ◦ Alarm Link ◦ Has Status Reason Note ◦ Status Reason Note
Ingest CVEs As	Select how CVEs are represented in ThreatQ. Select `CVEs` to ingest each CVE as a CVE Indicator object. Select `Vulnerabilities` to ingest each CVE as a Vulnerability object. Options include: ◦ CVEs ◦ Vulnerabilities *(default)*

Vulnerabilities Parameters

PARAMETER	DESCRIPTION
API Key	Enter your Company API Key to authenticate requests to the SOCRadar API.
Company ID	Enter your Company ID to retrieve data associated with your tenant.
Ingest CVEs As	Select how CVEs are represented in ThreatQ. Select `CVEs` to ingest each CVE as a CVE Indicator object, or select `Vulnerabilities` to ingest each CVE as a Vulnerability object. Options include: ◦ CVEs ◦ Vulnerabilities *(default)*
Results per Page	Specify the number of results to retrieve per API request. Supported values range from `1` to `1000`. *(default: 500)*
Search Text (Optional)	Enter a free-text search value to filter vulnerability results.
Vulnerability Status Reason Filtering (Optional)	Select one or more status reasons to filter vulnerability results. Options include: ◦ Investigating ◦ Pending Info ◦ Legal Review ◦ Vendor Assessment ◦ Resolved ◦ False Positive ◦ Duplicate ◦ Processed Internally

PARAMETER	DESCRIPTION
	◦ Mitigated ◦ Not Applicable
Vulnerability Type Filtering (Optional)	Select one or more vulnerability types to filter results. Options include: ◦ Exploited ◦ CISA Known Exploited ◦ Ransomware ◦ Weaponized
Vulnerability Status Filtering (Optional)	Select one or more vulnerability statuses to filter results. Options include: ◦ Open ◦ On Hold ◦ Closed
Vulnerability Filtering (Optional)	Enter a vulnerability identifier or free-text value to filter results.
Vulnerability Severity Filtering (Optional)	Select one or more severity levels to filter vulnerability results. Options include: ◦ Critical ◦ High ◦ Medium ◦ Low ◦ Info
Affected Software Filtering (Optional)	Enter a software name to retrieve vulnerabilities associated with the specified software.

PARAMETER	DESCRIPTION
Asset Filtering (Optional)	Enter an asset value to retrieve vulnerabilities associated with the specified asset.
Scan Type Filtering (Optional)	Select one or more scan types to filter vulnerability results. Options include: ◦ Active ◦ Passive
Product Type Filtering (Optional)	Select one or more product types to filter vulnerability results. Options include: ◦ Website Vulnerability ◦ Third Party Products ◦ SSL Certificate ◦ IP Address ◦ Operating Systems ◦ Network Services ◦ Other ◦ Network System Vulnerability
Alarm ID Filtering (Optional)	Enter an alarm ID to retrieve vulnerabilities associated with the specified alarm.
Context Filtering	Select the contextual data to include with each vulnerability. Options include: ◦ CVSS Score *(default)* ◦ Severity *(default)* ◦ Alarm Status *(default)* ◦ Scan Type *(default)* ◦ Affected Asset *(default)* ◦ Affected Software *(default)*

PARAMETER	DESCRIPTION
	◦ Title *(default)* ◦ Affected Product *(default)* ◦ Affected Product Version *(default)* ◦ Port ◦ CPEs ◦ Alarm Link ◦ History

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

SOCRadar Threat Feed

The SOCRadar Threat Feed ingests indicators of compromise from the aggregated threat feeds that can be created in SOCRadar. Curate your own collection of threat feeds from the SOCRadar platform and ingest them into ThreatQ.

`GET https://platform.socradar.com/api/threat/intelligence/feed_list/{id}.json`

Sample Response:


```
[
  {
    "extra_info": {
      "classification": "MALICIOUS",
      "file_type": "XLS",
      "first_seen_date": "2023-07-15 07:55:56",
      "last_analyze_date": "2023-07-15T07:57:43",
      "mime_type": "application/vnd.ms-excel",
      "seen_count": 254,
      "subcategory": "macro_hunter",
      "vt_score": 28
    },
    "feed":
"76ccf59f41fe4881f6c679248fee163e6045f97d013a1ce7e34d172bdad532d5",
    "feed_type": "hash",
    "first_seen_date": "2023-07-15 08:57:50",
    "latest_seen_date": "2023-07-30 19:03:45",
    "maintainer_name": "Inquest DFI - Malicious"
  },
  {
    "extra_info": {
      "classification": "MALICIOUS",
      "file_type": "OLE",
      "first_seen_date": "2023-07-15 05:34:21",
      "last_analyze_date": "2023-07-15T05:42:20",
      "mime_type": "application/cdfv2",
      "seen_count": 257,
      "subcategory": "macro_hunter",
      "vt_score": 28
```

```
    },
    "feed":
"f6a12e0263463e53381f00b30d104d59485889c428a17811716bdfd2de80a00d",
    "feed_type": "hash",
    "first_seen_date": "2023-07-15 06:42:41",
    "latest_seen_date": "2023-07-30 19:03:45",
    "maintainer_name": "Inquest DFI - Malicious"
  }
]
```

ThreatQuotient provides the following default mapping for this feed:

> Mappings are based on each item within the API response array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.feed	Indicator Value	.feed_type	N/A	.first_seen_date	The feed_type field is mapped to the ThreatQ type
.extra_info.name	Indicator Value	Filename	.first_seen_date	N/A	If Related Filename selected in Context Filtering
.extra_info.tags	Indicator Tag	N/A	N/A	Spyware	If Tags selected in Context Filtering
.extra_info.geo_location.AsnCode	Attribute	ASN	.first_seen_date	14061	If ASN selected in Geolocation Filtering
.extra_info.geo_location.AsnName	Attribute	ASN Organization	.first_seen_date	DigitalOcean LLC	If ASN Organization selected in Geolocation Filtering
.extra_info.geo_location.CityName	Attribute	City	.first_seen_date	Santa Clara	If City selected in Geolocation Filtering
.extra_info.geo_location.CountryCode	Attribute	Country Code	.first_seen_date	US	If Country Code selected in Geolocation Filtering
.extra_info.geo_location.CountryName	Attribute	Country	.first_seen_date	United States of America	If Country selected in Geolocation Filtering
.extra_info.geo_location.Latitude	Attribute	Latitude	.first_seen_date	N/A	If Latitude selected in Geolocation Filtering
.extra_info.geo_location.Longitude	Attribute	Longitude	.first_seen_date	N/A	If Longitude selected in Geolocation Filtering
.extra_info.geo_location.RegionName	Attribute	Region	.first_seen_date	California	If Region selected in Geolocation Filtering
.extra_info.geo_location.ZipCode	Attribute	Zip Code	.first_seen_date	95050	If Zip Code selected in Geolocation Filtering
.extra_info.asn_name	Attribute	ASN Organization	.first_seen_date	N/A	If ASN Organization selected in Geolocation Filtering
.extra_info.country_code	Attribute	Country Code	.first_seen_date	N/A	If Country Code selected in Geolocation Filtering
.extra_info.country_name	Attribute	Country	.first_seen_date	N/A	If Country selected in Geolocation Filtering
.extra_info.domain_register_date	Attribute	Domain Registration Date	.first_seen_date	N/A	If Domain Registration Date selected in Context Filtering
.extra_info.sector	Attribute	Affected Sector	.first_seen_date	N/A	If Affected Sector selected in Context Filtering
.extra_info.title	Attribute	Page Title	.first_seen_date	N/A	If Page Title selected in Context Filtering

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.extra_info.score	Attribute	Score	.first_seen_date	N/A	If Score selected in Context Filtering. Updatable
.extra_info.classification	Attribute	Classification	.first_seen_date	MALICIOUS	If Classification selected in Context Filtering. Updatable
.extra_info.file_type	Attribute	File Type	.first_seen_date	file_type	If File Type selected in Context Filtering
.extra_info.type	Attribute	File Type	.first_seen_date	windows_exe_(x86-32)	If File Type selected in Context Filtering and IOC is a hash
.extra_info.mime_type	Attribute	MIME Type	.first_seen_date	mime_type	If MIME Type selected in Context Filtering
.extra_info.sub_category	Attribute	Category	.first_seen_date	macro_hunter	If Category selected in Context Filtering
.extra_info.vt_score	Attribute	VirusTotal Score	.first_seen_date	28	If VirusTotal Score selected in Context Filtering
.extra_info.report_link	Attribute	Report Link	.first_seen_date	N/A	If Report Link selected in Context Filtering and IOC is a hash
.extra_info.verdict	Attribute	Verdict	.first_seen_date	malicious	If Verdict selected in Context Filtering
.maintainer_name	Attribute	Source	.first_seen_date	Inquest DFI - Malicious	N/A

SOCRadar Leaks

The SOCRadar Leaks feed ingests leaked credentials for identities within your organization's SOCRadar tenant.

`GET https://platform.socradar.com/api/leaks/company/{company_id}/latest`

Sample Response (truncated):


```
{
  "is_success": true,
  "message": "Success",
  "response_code": 200,
  "data": [
    {
      "password": "NULL",
      "raw_password": "NULL",
      "consolidated_alarm_id": null,
      "alarm_id": null,
      "company_id": 14412,
      "domain": "example.com",
      "email": "john.doe@example.com",
      "file_name": "",
      "file_unique_id": "2e612bb73c2849e7b9d8fd45b08c7139",
      "index_time": "1630627200.0",
      "info": "<table>...breach details...</table>",
      "line_number": "",
      "password_type": "raw",
      "tags": "SOCRadar Internal Service",
      "leak_type": "EMPLOYEE",
      "extra_info": {
        "leak_source": "SOCRadar Internal Service"
      },
      "id": 18950559,
      "source": null,
      "is_false_positive": false,
      "false_positive_notes": null,
      "insert_date": "2023-07-28T10:29:59.294897",
      "update_date": "2023-07-28T10:29:59.294898"
    }
```

```
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

> Mappings are based on each item within the `data` key from the API response.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.leak_type, .email`	Event Title	Leak	`.insert_date`	EMPLOYEE - jane.doe@example.com	Fields concatenated together to form title.
`.email`	Identity Value	N/A	`.insert_date`	john.doe@gmail.com	N/A
`.extra_info.leak_source`	Attribute	Source	`.insert_date`	SOCRadar Internal Service	If Leak Source selected in Context Filtering
`.is_false_positive`	Attribute	Is False Positive	`.insert_date`	false	If Is False Positive selected in Context Filtering.Updatable
`.false_positive_notes`	Attribute	False Positive Notes	`.insert_date`	N/A	If False Positive Notes selected in Context Filtering
`.leak_type`	Attribute	Leak Type	`.insert_date`	EMPLOYEE	If Leak Type selected in Context Filtering
`.password_type`	Attribute	Password Type	`.insert_date`	raw	If Password Type selected in Context Filtering
`.line_number`	Attribute	Line Number	`.insert_date`	N/A	If Line Number selected in Context Filtering
`.file_name`	Attribute	Filename	`.insert_date`	N/A	If Filename selected in Context Filtering
`.domain`	Attribute	Company Domain	`.insert_date`	example.com	If Company Domain selected in Context Filtering
`.raw_password`	Attribute	Raw Password	`.insert_date`	N/A	If Raw Password selected in Context Filtering
`.password`	Attribute	Password	`.insert_date`	N/A	If Password selected in Context Filtering
`.alarm_id`	Attribute	Alarm Link	`.insert_date`	N/A	If Alarm Link selected in Context FilteringConcatenated with the portal URL & company ID
`.tags[]`	Tag	N/A	`.insert_date`	SOCRadar Internal Service	If Tags selected in Context Filtering

SOCRadar Incidents

The SOCRadar Incidents feed ingests incidents from your organization's SOCRadar tenant.

`GET https://platform.socradar.com/api/company/{company_id}/incidents/v4`

Sample Response (truncated):


```
{
  "data": {
    "alarms": [
      {
        "ai_decision": null,
        "alarm_asset": "198.202.211.1",
        "alarm_id": 85396551,
        "alarm_related_assets": [
          {
            "key": "ip_address",
            "value": "198.202.211.1"
          },
          {
            "key": "domain_name",
            "value": [
              "www.threatq.com",
              "groove.threatq.com"
            ]
          }
        ],
        "alarm_related_entities": [
          {
            "key": "url",
            "value": "Portugal Abuse Open Feed - Phishing"
          }
        ],
        "alarm_response": "IP verification, threat assessment,
traffic blocking...",
        "alarm_risk_level": "MEDIUM",
        "alarm_text": "This alarm indicates the detection of a
blacklisted IP address...",
        "alarm_type_details": {
          "alarm_compliance_list": [
```

```
            {
              "control_item": "Article 32 - Security of processing",
              "description": "The detection of an IP address on a
blacklist...",
              "name": "GDPR"
            }
          ],
          "alarm_default_mitigation_plan": "Continuously monitor IP
reputation...",
          "alarm_default_risk_level": "MEDIUM",
          "alarm_detection_and_analysis": "Integrate the output into
cybersecurity systems...",
          "alarm_generic_title": "IP Address Reputation (Blacklist)",
          "alarm_main_type": "Brand Protection",
          "alarm_post_incident_analysis": "",
          "alarm_sub_type": "Reputation"
        },
        "alarm_type_id": 23,
        "approved_by": "Auto Approve",
        "company_id": "14412",
        "company_name": "THREATQUOTIENT",
        "content": {
          "blacklist_item": {
            "defanged_blacklist_item_data": "198.202.211.1",
            "defanged_domains": [
              "www.threatq.com",
              "groove.threatq.com"
            ]
          },
          "category": "Phishing",
          "desctription": "This feed compiles phishing campaigns...",
          "first_seen_date": "2026-02-12 18:59:07 UTC",
          "last_update_date": "2026-02-12 18:59:07 UTC",
          "maintainer": "Seguranca Informatica",
          "source": "Portugal Abuse Open Feed - Phishing",
          "update_frequency": "1 hour"
        },
        "date": "2026-02-13 18:41:27",
        "has_status_reason_note": false,
        "is_approved": true,
        "notification_id": 8174747,
        "status": "OPEN",
```

```
        "tags": [
          "reputation",
          "phishing",
          "public",
          "ip address",
          "blacklist"
        ],
        "title": "IP Address Detected in Blacklist"
      }
    ],
    "total_pages": 3,
    "total_records": 203
  },
  "is_success": true,
  "message": "Success",
  "response_code": 200
}
```


ThreatQuotient provides the following default mapping for this feed:

> Mappings are based on each item within the `data` key from the API response.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title, .alarm_type_details.alarm_main_type, .alarm_type_details.alarm_sub_type, .alarm_id`	`Event.Title`	`Incident`	`.date`	`IP Address Detected in Blacklist [Brand Protection] [Reputation] [Alarm ID: 85396551]`	`Primary object title. Fields are concatenated to form the event title.`
`.alarm_related_assets[].value`	`Related Asset`	`N/A`	`.date`	`example.com`	`User-configurable. If the asset key is ip, domain, hostname, ip_address, or domain_name, and Assets (IPs & Domains) is selected in Context Filtering.`
`.alarm_related_assets[].value`	`Event.Attribute`	`CPE`	`.date`	`cpe:2.3:a:openssl:openssl:*:*:*:*:*:*:*:*`	`User-configurable. If the asset key is CPE or cpe, and CPEs is selected in Context Filtering.`
`.alarm_related_entities[].value`	`Related Indicator.Value / Related Vulnerability .Value`	`CVE`	`.date`	`CVE-2024-12345`	`User-configurable. If the entity key is CVE or cve, and Related CVEs is selected in Context Filtering. Ingested according to Ingest CVEs As.`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.tags[]	Event.Tag	N/A	.date	blacklist	User-configurable. If Tags is selected in Context Filtering.
.alarm_type_details.alarm_main_type	Event.Attribute	Main Type	.date	Brand Protection	User-configurable. If Main Type is selected in Context Filtering.
.alarm_type_details.alarm_sub_type	Event.Attribute	Sub Type	.date	Reputation	User-configurable. If Sub Type is selected in Context Filtering.
.alarm_type_details.alarm_generic_title	Event.Attribute	Generic Title	.date	IP Address Reputation (Blacklist)	User-configurable. If Generic Title is selected in Context Filtering.
.alarm_risk_level	Event.Attribute	Severity	.date	MEDIUM	User-configurable. Updatable. If Severity is selected in Context Filtering.
.status	Event.Attribute	Status	.date	OPEN	User-configurable. Updatable. If Status is selected in Context Filtering.
.company_name	Event.Attribute	Company Name	.date	THREATQUOTIENT	User-configurable. If Company Name is selected in Context Filtering.
.content.source	Event.Attribute	Source	.date	Portugal Abuse Open Feed - Phishing	User-configurable. If Source is selected in Context Filtering.
.content.category	Event.Attribute	Category	.date	Phishing	User-configurable. If Category is selected in Context Filtering.
.content.maintainer	Event.Attribute	Maintainer	.date	Seguranca Informatica	User-configurable. If Maintainer is selected in Context Filtering.
.content.first_seen_date	Event.Attribute	First Seen Date	.date	2026-02-12 18:59:07 UTC	User-configurable. If First Seen Date is selected in Context Filtering.
.content.last_update_date	Event.Attribute	Last Update Date	.date	2026-02-12 18:59:07 UTC	User-configurable. If Last Update Date is selected in Context Filtering.
.content.update_frequency	Event.Attribute	Update Frequency	.date	1 hour	User-configurable. If Update Frequency is selected in Context Filtering.
.alarm_response	Event.Attribute	Response	.date	1. IP Address Verification...	User-configurable. If Alarm Response is selected in Context Filtering.
.alarm_type_details.alarm_detection_and_analysis	Event.Attribute	Detection and Analysis	.date	To utilize this alarm...	User-configurable. If Detection and Analysis is selected in Context Filtering.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.alarm_type_details.alarm_default_mitigation_plan	Event.Attribute	Default Mitigation Plan	.date	1. IP Address Monitoring...	User-configurable. If Default Mitigation Plan is selected in Context Filtering.
.alarm_type_details.alarm_post_incident_analysis	Event.Attribute	Post Incident Analysis	.date	N/A	User-configurable. If Post Incident Analysis is selected in Context Filtering.
.alarm_type_details.alarm_compliance_list[].name	Event.Attribute	Compliance Framework	.date	CCPA	User-configurable. If Compliance Framework is selected in Context Filtering. Entries where .name == "MITRE ATT&CK" are not ingested as this attribute.
.alarm_type_details.alarm_compliance_list[].control_item	Event.Attribute	Control Item	.date	1798.150(a)(1)	User-configurable. If Control Item is selected in Context Filtering. Entries where .name == "MITRE ATT&CK" are not ingested as this attribute.
.alarm_type_details.alarm_compliance_list[].description	Event.Attribute	Compliance Description	.date	If personal information...	User-configurable. If Compliance Description is selected in Context Filtering. Entries where .name == "MITRE ATT&CK" are not ingested as this attribute.
.alarm_type_details.alarm_compliance_list[].control_item	Related Attack Pattern	N/A	.date	TA0011 / T1588.001	User-configurable. Only when .alarm_compliance_list[].name == "MITRE ATT&CK" and Related Attack Patterns is selected in Context Filtering.
.alarm_id	Event.Attribute	Alarm Link	.date	https://platform.socradar.com/app/company/{company_id}/alarm-management?tab=approved&alarmId=85396551	User-configurable. If Alarm Link is selected in Context Filtering.
.has_status_reason_note	Event.Attribute	Has Status Reason Note	.date	true	User-configurable. If Has Status Reason Note is selected in Context Filtering. Only present when show_status_reason_change_note=true.
.status_reason_note	Event.Attribute	Status Reason Note	.date	Confirmed as false positive by SOC team	User-configurable. If Status Reason Note is selected in Context Filtering. Only present when show_status_reason_change_note=true.

SOCRadar Vulnerabilities

The SOCRadar Vulnerabilities feed ingests vulnerabilities related to your organization's assets, tracked in your SOCRadar tenant.

```
GET https://platform.socradar.com/api/company/{company_id}/
vulnerabilities/v2/latest
```

Sample Response:


```
{
  "data": {
    "pagination": {
      "current_page": 1,
      "total_count": 3142,
      "total_pages": 1571
    },
    "records": [
      {
        "affected_software": "string",
        "alarm_id": 75695390,
        "alarm_status": "OPEN",
        "asset": "194.233.68.76",
        "asset_id": 9526219,
        "cvss": 2.2,
        "extra_info": {
          "cve_product": {
            "config_number": 0,
            "cpe": "cpe:2.3:a:oracle:mysql:-:*:*:*:*:*:*:*",
            "cpe_for_fulltext":
"cpe:2.3:a:oracle:mysql: :*:*:*:*:*:*:*",
            "icon_path": "string",
            "product": "mysql",
            "vendor": "oracle",
            "version": "-"
          },
          "history": [
            {
              "action": "OPEN",
              "date": "2025-11-06 09:23",
              "description": "Company Vulnerability Finding was
discovered.",
              "note": "string",
```

```
              "reason": "OPEN",
              "user": "test.user@testcompany.com"
            }
          ],
          "port": "3306",
          "severity": "LOW"
        },
        "id": 8082453,
        "scan_result": {
          "Asset": "194.233.68.76",
          "CVE": "CVE-2024-21232, CVE-2024-21243, CVE-2024-21244",
          "CVSS3 Score": "2.2",
          "CVSS3 Vector": "CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/
A:N",
          "Ports": "3306"
        },
        "scan_type": "ACTIVE",
        "vulnerability": "CVE-2024-21243",
        "vulnerability_date": "1955-08-31T12:40:10.857Z",
        "vulnerability_status": "OPEN"
      }
    ]
  },
  "is_success": true,
  "message": "Success",
  "response_code": 200
}
```


ThreatQuotient provides the following default mapping for this feed based on each item within `data.records` from the API response.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.vulnerability`	`Vulnerability.Value / Indicator.Value`	`CVE`	`.vulnerability_date`	`CVE-2024-21243`	`Primary object value. User-configurable. Ingested according to Ingest CVEs As.`
`.cvss`	`Vulnerability.Attribute / Indicator.Attribute`	`CVSS Score`	`.vulnerability_date`	`2.2`	`User-configurable. Updatable.`
`.extra_info.severity`	`Vulnerability.Attribute / Indicator.Attribute`	`Severity`	`.vulnerability_date`	`LOW`	`User-configurable. When Severity is selected in Context Filtering.`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.alarm_status	Vulnerability.Attribute / Indicator.Attribute	Alarm Status	.vulnerability_date	OPEN	User-configurable. When Alarm Status is selected in Context Filtering.
.scan_type	Vulnerability.Attribute / Indicator.Attribute	Scan Type	.vulnerability_date	ACTIVE	User-configurable. When Scan Type is selected in Context Filtering.
.asset	Related Asset	N/A	.vulnerability_date	groove.threatq.com	User-configurable. Ingested as a related asset when Affected Asset is selected in Context Filtering.
.asset	Vulnerability.Attribute / Indicator.Attribute	Affected Asset	.vulnerability_date	groove.threatq.com	User-configurable. When Affected Asset is selected in Context Filtering.
.affected_software	Vulnerability.Attribute / Indicator.Attribute	Affected Software	.vulnerability_date	Oracle MySQL	User-configurable. When Affected Software is selected in Context Filtering. Use when present.
.extra_info.title	Vulnerability.Attribute / Indicator.Attribute	Title	.vulnerability_date	Thirdparty Product "" Vulnerability Detected	User-configurable. When Title is selected in Context Filtering.
.extra_info.cve_product.product	Vulnerability.Attribute / Indicator.Attribute	Affected Product	.vulnerability_date	mysql	User-configurable. When Affected Product is selected in Context Filtering.
.extra_info.cve_product.version	Vulnerability.Attribute / Indicator.Attribute	Affected Product Version	.vulnerability_date	-	User-configurable. When Affected Product Version is selected in Context Filtering.
.extra_info.port	Vulnerability.Attribute / Indicator.Attribute	Port	.vulnerability_date	3306	User-configurable. When Port is selected in Context Filtering.
.extra_info.cpe_list[]	Vulnerability.Attribute / Indicator.Attribute	CPE	.vulnerability_date	cpe:/a:mysql:mysql	User-configurable. One attribute per returned CPE value when CPEs is selected in Context Filtering.
.alarm_id	Vulnerability.Attribute / Indicator.Attribute	Alarm Link	.vulnerability_date	https://platform.socradar.com/app/company/{company_id}/alarm-management?tab=approved&alarmId=19384614	User-configurable. When Alarm Link is selected in Context Filtering.
.extra_info.history[]	Vulnerability.Attribute / Indicator.Attribute	History	.vulnerability_date	2023-08-19 06:06 OPEN Company Vulnerability Finding was discovered.	User-configurable. Optional flattened human-readable history entries when History is selected in Context Filtering.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.vulnerability, .extra_info.title, .asset, .extra_info.history[], .scan_result	Vulnerability.Description / Indicator.Description	N/A	N/A	N/A	Concatenated into the object description. Not user-configurable.

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.

SOCRadar Threat Feed

METRIC	RESULT
Run Time	16 minutes
Indicators	92,214
Indicator Attributes	275,204

SOCRadar Leaks

METRIC	RESULT
Run Time	1 minute
Events	1
Event Attributes	5
Identities	1

SOCRadar Incidents

METRIC	RESULT
Run Time	2 minutes
Assets	32
Attack Pattern	18
Events	203
Event Attributes	1,543
Vulnerability	207

SOCRadar Vulnerabilities

METRIC	RESULT
Run Time	2 minutes
Assets	7
Vulnerabilities	207
Vulnerability Attributes	4510

Known Issues / Limitations

- **SOCRadar Leaks** - the API currently returns a 500 Internal Server Error when only `VIP Employee` value is sent for Leak Type Filtering. The SOCRadar was notified about the problem.
- **SOCRadar Incidents:** Combining the `Main Type`, `Sub Type`, and `Alarm Title` filters may return fewer results than filtering by `Status` alone. This occurs because the SOCRadar API applies all selected filters together and requires exact value matches.

Change Log

- **Version 2.0.0**
  - **SOCRadar Alarms**
    - Renamed the **SOCRadar Alarms** feed to **SOCRadar Incidents**.
    - Updated the feed to use the `incidents/v4` API endpoint.
    - Added `All` and `Critical` options to the **Severity Filtering** parameter.
    - Added the following configuration parameters:
      - **Status Filtering**
      - **Alarm Title Filtering**
      - **Alarm Type ID**
    - Added new options to the **Context Filtering** parameter.
  - **SOCRadar Vulnerabilities**
    - Updated the feed to use the `vulnerabilities/v2/latest` API endpoint.
    - Removed the **Ignore False Positives** configuration parameter.
    - Added the following configuration parameters:
      - **Results per Page**
      - **Search Text**
      - **Vulnerability Status Reason Filtering**
      - **Vulnerability Type Filtering**
      - **Vulnerability Status Filtering**
      - **Vulnerability Filtering**
      - **Vulnerability Severity Filtering**
      - **Affected Software Filtering**
      - **Asset Filtering**
      - **Scan Type Filtering**
      - **Product Type Filtering**
      - **Alarm ID Filtering**
      - **Context Filtering**

    - **Known Issues and Limitations**
        - Added a known limitation for the **SOCRadar Incidents** feed documenting filtering behavior when **Status**, **Main Type**, **Sub Type**, and **Alarm Title** filters are used in combination.

- **Version 1.0.1**
    - Resolved an issue that prevented the **SOCRadar Alarms** feed from correctly filtering results when multiple values were configured for the **Main Type Selection** or **Sub Type Selection** parameters.

- **Version 1.0.0**
    - Initial release