

ThreatQuotient

A Securonix Company



SOCRadar CDF

Version 1.0.1

July 20, 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	3
Support	4
Integration Details	5
Introduction	6
Prerequisites	7
Installation	8
Configuration	9
Threat Feed Parameters	9
Leaks Parameters	12
Alarms Parameters	14
Vulnerabilities Parameters	17
ThreatQ Mapping	19
SOCRadar Threat Feed	19
SOCRadar Leaks	23
SOCRadar Alarms	28
SOCRadar Vulnerabilities	44
Average Feed Run	47
SOCRadar Threat Feed	47
SOCRadar Leaks	47
SOCRadar Alarms	48
SOCRadar Vulnerabilities	48
Known Issues / Limitations	49
Change Log	50

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.

Copyright © 2026 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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	1.0.1
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.

< SOCRadar Threat Feed



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

Feed Settings

Feed URLs can be found by navigating to the "Threat Feed / IOC" tab within SOCRadar. On the right side of the page, you'll see your feeds under the "My Collections" section. Click on the "API Links" button under the collection you want to get the ID for, and select the "JSON" option. Lastly, use the "Copy To Clipboard" button to copy the URL.

Enter a line-separated list of feed URLs to pull into ThreatQ

Data Filtering

The following options will give you more control over the data that is ingested from the SOCRadar API

A number representing the minimum amount of times an IOC must have been seen to be ingested. This allows you to filter out IOCs that may not be as relevant.

Context Filtering

Select the pieces of context you want to include with each IOC. This will help you filter out any unnecessary data. Note, not all context is available for every IOC, as it depends on the feed it came from.

- ☒ Tags
- ☒ Verdict
- ☒ Classification
- ☒ Affected Sector
- ☒ Score
- ☒ VirusTotal Score
- ☒ Category
- ☒ Domain Registration Date
- ☒ Page Title
- ☒ File Type
- ☒ MIME Type
- ☒ Report Link
- ☒ Related Filename

Geolocation Filtering

Select the pieces of geolocation context you want to include with each IOC. This will help you filter out any unnecessary data. Note, not all context is available for every IOC, as it depends on the feed it came from.

- ☒ ASN
- ☒ ASN Organization
- ☒ City
- ☒ Country Code
- ☒ Country
- ☒ Latitude
- ☒ Longitude
- ☒ Region
- ☒ Zip Code

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: <table> <tr> <td>◦ Tags (default)</td><td>◦ Password Type</td></tr> <tr> <td>◦ Password (Redacted) (default)</td><td>◦ Line Number</td></tr> <tr> <td>◦ Taw Password</td><td>◦ Is False Positive (default)</td></tr> <tr> <td>◦ Company Domain (default)</td><td>◦ False Positive Notes (default)</td></tr> <tr> <td>◦ Leak Source (default)</td><td>◦ Alarm Link</td></tr> </table>	◦ Tags (default)	◦ Password Type	◦ Password (Redacted) (default)	◦ Line Number	◦ Taw Password	◦ Is False Positive (default)	◦ Company Domain (default)	◦ False Positive Notes (default)	◦ Leak Source (default)	◦ Alarm Link
◦ Tags (default)	◦ Password Type										
◦ Password (Redacted) (default)	◦ Line Number										
◦ Taw Password	◦ Is False Positive (default)										
◦ Company Domain (default)	◦ False Positive Notes (default)										
◦ Leak Source (default)	◦ Alarm Link										

< SOCRadar Leaks



Disabled ☐ Enabled ☒

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

Authentication

To get your Company API Key, login to SOCRadar and use the sidebar to navigate to "Settings -> API Options". To get your Company ID, login to SOCRadar, and use the sidebar to navigate to "Settings -> Company Settings". Then, copy the ID from your browser's URL bar. It should be an all-numeric ID.

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.

Data Filtering

The following options will give you more control over the data that is ingested from the SOCRadar API

☐ Ignore False Positives

Enabling this will not ingest items marked as False Positives

Leak Type Filtering

Select the types of leaks you want to ingest into ThreatQ.

☒ Employee

☒ VIP Employee

☐ Customer

☐ Botnet Market

Context Filtering

Select the pieces of context you want 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.

☒ Tags

☒ Password (Redacted)

☐ Raw Password

☒ Company Domain

☒ Leak Source

☒ Leak Type

Alarms 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.
Ignore False Positives	Enabling this will not ingest items marked as False Positives.
Severity Filtering	Select the severities for incidents you want to ingest into ThreatQ. Options include: ◦ Info ◦ Low ◦ Medium (default) ◦ High (default)
Main Type Selection	Optional - enter a comma-separated list of main types of Incidents to ingest into ThreatQ. Any main type not included in this list will not be ingested. Leaving this empty will ingest all Incidents.
Sub Type Selection	Optional - enter a comma-separated list of sub types of Incidents to ingest into ThreatQ. Any sub type not included in this list will not be ingested.
Context Filtering	Select the pieces of context to include with each leak event. This will help you filter out any unnecessary data. Options include: ◦ Tags (default) ◦ Main Type (default) ◦ Assets (IPs and Domains) (default) ◦ CPEs

PARAMETER	DESCRIPTION
	◦ Sub Type (default) ◦ Group Name (default) ◦ Severity (default) ◦ Related CVEs (default) ◦ CVSS Score (default)
	◦ Is False Positive (default) ◦ Is Resolved ◦ Resolved Date ◦ Alarm Link
Ingest CVEs As	Select the entity type to ingest CVEs as. Options include: ◦ CVEs (default) ◦ Vulnerabilities

< SOCRadar Alarms



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration

Activity Log

Authentication

To get your Company API Key, login to SOCRadar and use the sidebar to navigate to "Settings -> API Options". To get your Company ID, login to SOCRadar, and use the sidebar to navigate to "Settings -> Company Settings". Then, copy the ID from your browser's URL bar. It should be an all-numeric ID.

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.

Data Filtering

The following options will give you more control over the data that is ingested from the SOCRadar API

☐ Ignore False Positives

Enabling this will not ingest items marked as False Positives

Severity Filtering

Select the severities for incidents you want to ingest into ThreatQ.

☐ Info

☐ Low

☒ Medium

☒ High

Main Type Selection (Optional)

Enter a comma-separated list of main types of incidents to ingest into ThreatQ. Any main type not included in this list will not be ingested. Leaving this empty will ingest all incidents.

Sub Type Selection (Optional)

Enter a comma-separated list of sub types of incidents to ingest into ThreatQ. Any sub type not included in this list will not be ingested.

Vulnerabilities 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.
Ignore False Positives	Enabling this will not ingest items marked as False Positives.
Ingest CVEs As	Select the entity type to ingest CVEs as. Options include: ◦ CVEs (default) ◦ Vulnerabilities
Max Count	Enter the number of objects to return per run. The default value is 500.



SOCRadar API does not support pagination, and often times, requesting too much data will result in an API timeout. Lower this value if you are receiving 524 errors.

< SOCRadar Vulnerabilities



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

Authentication

To get your Company API Key, login to SOCRadar and use the sidebar to navigate to "Settings -> API Options". To get your Company ID, login to SOCRadar, and use the sidebar to navigate to "Settings -> Company Settings". Then, copy the ID from your browser's URL bar. It should be an all-numeric ID.

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.

Data Filtering

The following options will give you more control over the data that is ingested from the SOCRadar API

☒ Ignore False Positives

Enabling this will not ingest items marked as False Positives

Ingest CVEs As

Select the entity type you want to ingest CVEs as. If you select "CVEs", the CVE will be ingested as a CVE Indicator Object. If you select "Vulnerabilities", the CVE will be ingested as a Vulnerability Object

Request Settings

The following options will give you more control over how data is requested from SOCRadar

Max Count

This SOCRadar API does not support pagination, and often times, requesting too much data will result in an API timeout. If you are receiving 524 errors, please lower this number.

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.filename	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.geolocation.AsnCode	Attribute	ASN	.first_seen_date	14061	If ASN selected in Geolocation Filtering
.extra_info.geolocation.AsnName	Attribute	ASN Organization	.first_seen_date	DigitalOcean LLC	If ASN Organization selected in Geolocation Filtering
.extra_info.geolocation.CityName	Attribute	City	.first_seen_date	Santa Clara	If City selected in Geolocation Filtering
.extra_info.geolocation.CountryCode	Attribute	Country Code	.first_seen_date	US	If Country Code selected in Geolocation Filtering
.extra_info.geolocation.CountryName	Attribute	Country	.first_seen_date	United States of America	If Country selected in Geolocation Filtering
.extra_info.geolocation.Latitude	Attribute	Latitude	.first_seen_date	N/A	If Latitude selected in Geolocation Filtering
.extra_info.geolocation.Longitude	Attribute	Longitude	.first_seen_date	N/A	If Longitude selected in Geolocation Filtering
.extra_info.geolocation.RegionName	Attribute	Region	.first_seen_date	California	If Region selected in Geolocation Filtering
.extra_info.geolocation.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
.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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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
.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:

```
{
  "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 align=\"justify\"><tbody><tr><td
style=\"vertical-align: top; width: 150px;\"><b>Breach Domain:</b></
td><td style=\"padding-left: 8px; padding-bottom: 5px;\"><a
href=\"Apollo.io\" target=\"_blank\">Apollo.io</a></td></tr><tr><td
style=\"vertical-align: top; width: 150px;\"><b>Breach date:</b></
td><td style=\"padding-left: 8px; padding-bottom: 5px;\">01 July
2018</td></tr><tr><td style=\"vertical-align: top;\"><b>Publishing
date:</b></td><td style=\"padding-left: 8px; padding-bottom: 5px;
\">07 Nov 2020</td></tr><tr><td style=\"vertical-align: top; width:
150px;\"><b>Compromised accounts:</b></td><td style=\"padding-left:
8px; padding-bottom: 5px;\">126M</td></tr><tr><td style=\"vertical-
align: top;\"><b>Compromised data:</b></td><td style=\"padding-left:
8px; padding-bottom: 5px;\">person_name,
person_first_name_unanalyzed, person_last_name_unanalyzed,
person_name_unanalyzed_lowercase, person_title, person_functions,
person_seniority, person_email_status_cd,
person_extrapolated_email_confidence, person_email, person_phone,
```

```

person_sanitized_phone, person_email_analyzed, person_linkedin_url,
person_detailed_function, person_title_normalized,
primary_title_normalized_for_faceting,
sanitized_organization_name_unanalyzed, person_location_city,
person_location_city_with_state_or_country, person_location_state,
person_location_state_with_country, person_location_country,
person_location_postal_code, job_start_date,
current_organization_ids, modality, prospected_by_team_ids,
person_excluded_by_team_ids, relavence_boost,
person_num_linkedin_connections, person_location_geojson,
predictive_scores, person_vacuumed_at, random, _index, _type, _id,
_score</td></tr><tr><td style=\"vertical-align: top; width: 150px;
\"><b>Detailed info:</b></td><td style=\"padding-left: 8px; padding-
bottom: 5px;\">https://raidforums.com/Thread-Apollo-Database-Leaked-
Download</td></tr></tbody></table>\n",
    "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"
},
{
    "password": "NULL",
    "raw_password": "NULL",
    "consolidated_alarm_id": null,
    "alarm_id": null,
    "company_id": 14412,
    "domain": "example.com",
    "email": "jane.doe@example.com",
    "file_name": "",
    "file_unique_id": "2e612bb73c2849e7b9d8fd45b08c7139",
    "index_time": "1630627200.0",
    "info": "<table align=\"justify\"><tbody><tr><td
style=\"vertical-align: top; width: 150px;\"><b>Breach Domain:</b></
td><td style=\"padding-left: 8px; padding-bottom: 5px;\"><a

```



```
href=\"Apollo.io\" target=\"_blank\">Apollo.io</a></td></tr><tr><td
style=\"vertical-align: top; width: 150px;\"><b>Breach date:</b></
td><td style=\"padding-left: 8px; padding-bottom: 5px;\">01 July
2018</td></tr><tr><td style=\"vertical-align: top;\"><b>Publishing
date:</b></td><td style=\"padding-left: 8px; padding-bottom: 5px;
\">07 Nov 2020</td></tr><tr><td style=\"vertical-align: top; width:
150px;\"><b>Compromised accounts:</b></td><td style=\"padding-left:
8px; padding-bottom: 5px;\">126M</td></tr><tr><td style=\"vertical-
align: top;\"><b>Compromised data:</b></td><td style=\"padding-left:
8px; padding-bottom: 5px;\">person_name,
person_first_name_unanalyzed, person_last_name_unanalyzed,
person_name_unanalyzed_downcase, person_title, person_functions,
person_seniority, person_email_status_cd,
person_extrapolated_email_confidence, person_email, person_phone,
person_sanitized_phone, person_email_analyzed, person_linkedin_url,
person_detailed_function, person_title_normalized,
primary_title_normalized_for_faceting,
sanitized_organization_name_unanalyzed, person_location_city,
person_location_city_with_state_or_country, person_location_state,
person_location_state_with_country, person_location_country,
person_location_postal_code, job_start_date,
current_organization_ids, modality, prospected_by_team_ids,
person_excluded_by_team_ids, relavance_boost,
person_num_linkedin_connections, person_location_geojson,
predictive_scores, person_vacuumed_at, random, _index, _type, _id,
_score</td></tr><tr><td style=\"vertical-align: top; width: 150px;
\"><b>Detailed info:</b></td><td style=\"padding-left: 8px; padding-
bottom: 5px;\">https://raidforums.com/Thread-Apollo-Database-Leaked-
Download</td></tr></tbody></table>\n",
  "line_number": "",
  "password_type": "raw",
  "tags": "SOCRadar Internal Service",
  "leak_type": "EMPLOYEE",
  "extra_info": {
    "leak_source": "SOCRadar Internal Service"
  },
  "id": 18950558,
  "source": null,
  "is_false_positive": false,
  "false_positive_notes": null,
  "insert_date": "2023-07-28T10:29:59.276880",
  "update_date": "2023-07-28T10:29:59.276881"
}
```

```
]
}
```

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 Filtering. Concatenated with the portal URL & company ID
.tags[]	Tag	N/A	.insert_date	SOCRadar Internal Service	If Tags selected in Context Filtering

SOCRadar Alarms

The SOCRadar Alarms feed ingests alarms from your organization's SOCRadar tenant.

GET https://platform.socradar.com/api/company/{company_id}/incidents/v2

Sample Response:

```
{
  "is_success": true,
  "message": "Success",
  "response_code": 200,
  "data": [
    {
      "id": 1483868,
      "insert_date": "2023-08-01T09:24:18.861480",
      "is_resolved": false,
      "resolved_by": null,
      "resolved_date": null,
      "alarm_risk_level": "INFO",
      "alarm_type_details": {
        "alarm_main_type": "Internet Asset Inventory
Monitoring",
        "alarm_sub_type": "Asset Discovery",
        "alarm_group_name": "",
        "alarm_generic_title": "New Digital Asset(s)
Discovery",
        "alarm_default_risk_level": "INFO"
      },
      "extra_info": {},
      "alarm_related_assets": [],
      "alarm_related_entities": [],
      "alarm_notification_texts": {
        "id": 1483558,
        "alarm_title": "New Digital Asset(s) Detected",
        "alarm_mitigation_plan": "<ul>\n
<li>\n
Make sure that the newly detected asset is added to the digital asset
inventory.\n
</li> \n
<li>\n
Identify risks and weaknesses on the asset(s).\n
"
```

```

</li> \n
<li>\n
Make vulnerability scans and perform security checks on the asset(s).
\n
</li>\n
<li>\n
If
any weaknesses found should be mitigated according to the risk level
they comprise.\n
</li> \n
</ul>",

    "alarm_html": "<html>\n<head>\n    <meta
name=\"viewport\" content=\"width=device-width\"/>\n\n    <meta http-
equiv=\"Content-Type\" content=\"text/html; charset=UTF-8\"/>\n
<title>SOCRadar | Incident Notification</title>\n    <style
type=\"text/css\">\n        * {\n            font-family: \"Helvetica
Neue\", \"Helvetica\", \"Arial\", \"sans-serif\";\n        }\n\n
#entities_table hr {\n            display: none;\n        }\n    </
style>\n</head>\n<body bgcolor=\"#efefef\" \n        style='background-
image: url(\"https://platform.socradar.com/static/img/
mybg.png\");padding: 1px ;width: 100% ;height: 100%;'>\n<table
role=\"presentation\" align=\"center\" cellpadding=\"0\"
cellspacing=\"0\" border=\"0\" \n        style=\"width:100%;border-
collapse: collapse;\">\n    <tbody>\n        <tr>\n            <td
style=\"background-color:#efefef\">\n                <table
role=\"presentation\" align=\"center\" cellpadding=\"0\"
cellspacing=\"0\" border=\"0\" \n                    style=\"margin-
top:25px; margin-right: auto; margin-left: auto;min-width: 680px;
max-width: 680px;border-collapse: collapse;\">\n
<tbody>\n                <tr>\n                    <td
style=\"padding-top: 0;padding-bottom: 0\">\n
<table align=\"center\" role=\"presentation\" cellpadding=\"0\"
cellspacing=\"0\" border=\"0\" \n                    style=\"width:100%;max-width:680px;margin:0 auto;border-collapse:
collapse;\">\n                        <tbody>\n
<tr>\n                            <td align=\"center\" \n
style=\"background-color: #424265; padding:10px 50px 10px 50px;\">\n
<table role=\"presentation\" align=\"center\" cellpadding=\"0\"
cellspacing=\"0\" border=\"0\" \n                            style=\"width: 100%;margin-top:5px;margin-bottom:5px;border-collapse:
collapse;\">\n                                <tr>\n
<td align=\"center\" style=\"padding-top: 5px;padding-bottom: 5px;
\"><img\n
src=\"https://platform.socradar.com/static/img/socradar-logo-
inverse.png\" width=\"160\" \n

```

```

style=\" max-width: 160px; width: 100%\"/>\n
</td>\n
</tr>\n
</table>\n
</tbody>\n
</table>\n
</tr>\n
</tbody>\n
</table>\n
<table
role=\"presentation\" align=\"center\" cellpadding=\"0\"
cellspacing=\"0\" border=\"0\" style=\"margin-
right: auto; margin-left: auto;min-width: 680px; max-width:
680px;border-collapse: collapse;\">\n
<tr>\n
<td style='padding-top: 0;padding-bottom:
0;'>\n
<table align=\"center\"
role=\"presentation\" cellpadding=\"0\" cellspacing=\"0\"
border=\"0\" style=\"width:680px;max-
width:680px;background-color:#ffffff;Margin:0 auto; border-
collapse:collapse\">\n
<tr>\n
<td style=\"background-color: #ffffff; padding:10px 50px 10px 50px;
\">\n
<p style=\"text-align:
left ;\"><span\n
style='font-size:12px;font-family:\"Helvetica Neue\", \"Helvetica\",
\"Arial\", \"sans-serif\">We have identified incidents amongst\n
your assets,\n
please check
them carefully.</span></p>\n
<table role=\"presentation\" align=\"center\" cellpadding=\"0\"
cellspacing=\"0\" border=\"0\" style=\"margin-top: 10px;width: 100%;border-collapse: collapse;\">\n
<tr>\n
<td width=\"180px;\" style=\"padding-top: 2px;padding-bottom: 2px;
\">\n
<span
style='font-size:12px;font-family:\"Helvetica Neue\", \"Helvetica\",
\"Arial\", \"sans-serif\">Incident ID </span>\n
</td>\n
<td
style=\"padding-top: 2px;padding-bottom: 2px;\">\n
<a style=\"text-decoration:None; color:#6B3343\" \n
href=\"https://platform.socradar.com/company/14412/incidents/
1483868\">\n
<span style='font-size:12px;font-family:\"Helvetica Neue\",
\"Helvetica\", \"Arial\", \"sans-serif\">1483868</span>\n
<span style=\"vertical-align:top\">&#128279;</span>\n
</a>\n
</td>\n
</tr>\n
</tbody>\n
</table>\n
<td width=\"180px;\">\n

```

```

style="max-width:180px; width:180px;padding-top: 2px;padding-bottom:
2px;">\n
style='font-size:12px;font-family:"Helvetica Neue", "Helvetica",
"Arial", "sans-serif"'>Title</span>\n
</td>\n\n
<td
style="padding-top: 2px;padding-bottom: 2px;">\n
<span style='font-size:12px;font-family:"Helvetica Neue",
"Helvetica", "Arial", "sans-serif"'>New Digital Asset(s)
Detected</span>\n
\n
</td>\n
</tr>\n
\n
<tr>\n
<td width="180px;">\n
style="max-width:180px; width:180px;padding-top: 2px;padding-bottom:
2px;">\n
style='font-size:12px;font-family:"Helvetica Neue", "Helvetica",
"Arial", "sans-serif"'>Incident Product </span>\n
</td>\n
<td
style="padding-top: 2px;padding-bottom: 2px;">\n
<span style='font-size:12px;font-family:"Helvetica Neue",
"Helvetica", "Arial", "sans-serif"'>\n
\n
Attack
Surface Management\n
\n
</span>\n
</td>\n
</tr>\n
\n\n
\n
<tr>\n
<td
width="180px;">\n
style="max-width:180px; width:180px;padding-top: 2px;padding-bottom:
2px;">\n
style='font-size:12px;font-family:"Helvetica Neue", "Helvetica",
"Arial", "sans-serif"'>Incident Main Type </span>\n
</td>\n
<td
style="padding-top: 2px;padding-bottom: 2px;">\n
<span style='font-size:12px;font-family:"Helvetica Neue",
"Helvetica", "Arial", "sans-serif"'>\n
\n
Internet
Asset Inventory Monitoring\n
\n
</span>\n
</td>\n
</tr>\n
\n\n
<tr>\n
<td
width="180px;">\n

```

```

style="max-width:180px; width:180px; padding-top: 2px;padding-
bottom: 2px;">\n
<span style='font-size:12px;font-family:"Helvetica Neue",
"Helvetica", "Arial", "sans-serif"'>Incident Sub Type </span>\n
</td>\n
<td
style="padding-top: 2px;padding-bottom: 2px;"><span style='font-
size:12px;font-family:"Helvetica Neue", "Helvetica", "Arial",
"sans-serif"'>\n
\n
Asset
Discovery\n
\n
</span>\n
</td>\n
</tr>\n
\n
<tr>\n
<td width="180px;"\n
style="max-width:180px; width:180px; padding-top: 2px;padding-
bottom: 2px; vertical-align: top;">\n
<span style='font-size:12px;font-family:"Helvetica Neue",
"Helvetica", "Arial", "sans-serif"'>Assets </span>\n
</td>\n
<td
style="padding-top: 2px;padding-bottom: 2px;max-width: 700px;word-
wrap: break-word;">\n
<span style='font-size:12px;font-family:"Helvetica Neue",
"Helvetica", "Arial", "sans-serif"'>\n
\n\n
\n
EXAMPLE\n
<br>\n
</span>\n
</td>\n
</tr>\n
\n
<tr>\n
<td width="180px;"\n
style="max-width:180px; width:180px;padding-top: 2px;padding-bottom:
2px;">\n
<span
style='font-size:12px;font-family:"Helvetica Neue", "Helvetica",
"Arial", "sans-serif"'>Risk Level </span>\n
</td>\n
<td
style="padding-top: 2px;padding-bottom: 2px;">\n
<table>\n
<tr>\n
<td style="border-radius: .25em;margin: 2px;background-color:
#57889c;">\n
<span\n
style="display: inline-block; padding: .2em .6em .3em;font-size:
75%;font-weight: 700;color: #fff;text-align: center;white-space:

```



```

nowrap;vertical-align: baseline;border-radius: .25em;background-
color: #57889c;">INFO</span>\n
</td>\n
</tr>\n
</table>\n
</td>\n
</tr>\n
\n
</table>\n
</td>\n
</tr>\n\n
<!--##### BEGIN SHARE BLOCK #####\n
<tr>\n
  |
```

```

</table>\n
</tr>\n
#####-->\n\n
</td>\n
</tr>\n
</tbody>\n
</table>\n
<table role=\"presentation\" align=\"center\"
cellpadding=\"0\" cellspacing=\"0\" border=\"0\" \n
style=\"margin-right: auto; margin-left: auto;min-width: 680px; max-
width: 680px;border-collapse: collapse;\">\n
<tr>\n
<td style='padding-top: 0;padding-bottom:
0;'\n
<table align=\"center\"
role=\"presentation\" cellpadding=\"0\" cellspacing=\"0\"
border=\"0\" \n
style=\"width:680px;max-
width:680px;background-color:#ffffff;Margin:0 auto;border-collapse:
collapse;\">\n
<tr>\n
<td style='padding:10px 50px
10px 50px;'\n
<table role=\"presentation\" align=\"center\" cellpadding=\"0\"
cellspacing=\"0\" \n
border=\"0\" \n
style=\"margin-top:8px;margin-bottom:10px;width: 100%;border-
collapse: collapse;border-bottom: 2px solid #424266;\">\n
<tbody>\n
<tr>\n
<td width=\"180px\" \n
style='color:#424266;height: 30px;'\n
<span style='font-size:18px;font-weight:500;font-family:\"Helvetica
Neue\", \"Helvetica\", \"Arial\", \"sans-serif\"'\n
Description\n
span>\n
</td>\n
</tr>\n
<tr>\n
<td style=\"border-bottom:2px solid #424266;\"></td>\n
</tr>\n
</tbody>\n
</table>\n
\n
<table role=\"presentation\" role=\"presentation\" align=\"center\" \n
cellpadding=\"0\" cellspacing=\"0\" border=\"0\" \n
style=\"margin-top: 5px;margin-bottom: 5px;width: 100%;border-
collapse: collapse\">\n
\n
\n
<tr>\n
<td style=\"padding: 5px 8px 5px 0;width: 100%;text-align: left;\">\n
<span style='font-size:12px;font-family:\"Helvetica Neue\",
\"Helvetica\", \"Arial\", \"sans-serif\"'\n
>SOCRadar constantly
monitors the digital world and notifies when it discovers new assets
about your company. The asset(s) of your company has been detected!</

```

```

span>\n
td>\n
\n
</table>\n
\n
\n
<table
role=\"presentation\" align=\"center\" cellpadding=\"0\"
cellspacing=\"0\"\n
border=\"0\"\n
style=\"margin-top: 5px;margin-bottom: 10px;width: 100%;border-
collapse: collapse\"\n
id=\"entities_table\">\n
\n
<tr>\n
style='font-size:12px;font-family:\"Helvetica Neue\", \"Helvetica\",
\"Arial\", \"sans-serif\";padding-right: 8px; max-width: 600px; word-
break: break-word;'\>\n
\n
style=\"width: 100%\">\n
<tr>\n
<td style='font-size:12px;font-family:\"Helvetica Neue\",
\"Helvetica\", \"Arial\", \"sans-serif\"'>\n
<span class=\"hydra-block\"><span style=\"font-size:12px;font-
family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-serif'; display:
block; padding-bottom:2px; white-space:normal; word-break: break-all;
\" class=\"hydra-p\"><strong>Websites</strong></span><table
style=\"width:100%\" class=\"hydra-table\"><tr class=\"hydra-
tr\"><td style=\"padding:3px; padding-right:6px; white-space:
nowrap\"><span style=\"font-size:12px;font-family:'Helvetica Neue',
'Helvetica', 'Arial', 'sans-serif'; display: block; padding-
bottom:2px; white-space:no-wrap; \" class=\"hydra-p\"><strong>Asset</
strong></span></td><td style=\"padding:3px; padding-right:6px; white-
space: normal\"><span style=\"font-size:12px;font-family:'Helvetica
Neue', 'Helvetica', 'Arial', 'sans-serif'; display: block; padding-
bottom:2px; white-space:normal; word-break: break-all; \"
class=\"hydra-p\"><strong>Type</strong></span></td><td
style=\"padding:3px; padding-right:6px; white-space: nowrap\"><span
style=\"font-size:12px;font-family:'Helvetica Neue', 'Helvetica',
'Arial', 'sans-serif'; display: block; padding-bottom:2px; white-
space:no-wrap; \" class=\"hydra-p\"><strong>Source</strong></span></
td></tr><tr class=\"hydra-tr\"><td style=\"padding:3px; padding-
right:6px; white-space: nowrap\"><span style=\"font-size:12px;font-
family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-serif'; display:
block; padding-bottom:2px; white-space:no-wrap; \" class=\"hydra-

```

```
p">http://example.com</span></td><td style=\"padding:3px; padding-
right:6px; white-space: normal\"><span style=\"font-size:12px;font-
family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-serif'; display:
block; padding-bottom:2px; white-space:normal; word-break: break-all;
\" class=\"hydra-p\">Active Website</span></td><td
style=\"padding:3px; padding-right:6px; white-space: nowrap\"><a
target=\"_blank\" rel=\"noreferrer\" style=\"\" class=\"hydra-a\"
href=https://platform.socradar.com/app/company/14412/asm/dfp?
assetType=website&assetName=http://example.com><span style=\"font-
size:12px;font-family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-
serif'; display: block; padding-bottom:2px; white-space:normal; word-
break: break-all; \" class=\"hydra-p\">example.com</span></a></td></
tr><tr class=\"hydra-tr\"></tr></table><span style=\"display: block;
width: 100%; height: 1px; border-bottom: 1px solid #e4e4e4; margin-
bottom: 10px; margin-top: 10px;\" class=\"hydra-separator\"></
span><span style=\"font-size:12px;font-family:'Helvetica Neue',
'Helvetica', 'Arial', 'sans-serif'; display: block; padding-
bottom:2px; white-space:normal; word-break: break-all; \"
class=\"hydra-p\"><strong>DNS Records</strong></span><table
style=\"width:100%\" class=\"hydra-table\"><tr class=\"hydra-
tr\"><td style=\"padding:3px; padding-right:6px; white-space:
nowrap\"><span style=\"font-size:12px;font-family:'Helvetica Neue',
'Helvetica', 'Arial', 'sans-serif'; display: block; padding-
bottom:2px; white-space:no-wrap; \" class=\"hydra-p\"><strong>Asset</
strong></span></td><td style=\"padding:3px; padding-right:6px; white-
space: normal\"><span style=\"font-size:12px;font-family:'Helvetica
Neue', 'Helvetica', 'Arial', 'sans-serif'; display: block; padding-
bottom:2px; white-space:normal; word-break: break-all; \"
class=\"hydra-p\"><strong>Type</strong></span></td><td
style=\"padding:3px; padding-right:6px; white-space: nowrap\"><span
style=\"font-size:12px;font-family:'Helvetica Neue', 'Helvetica',
'Arial', 'sans-serif'; display: block; padding-bottom:2px; white-
space:no-wrap; \" class=\"hydra-p\"><strong>Source</strong></span></
td></tr><tr class=\"hydra-tr\"><td style=\"padding:3px; padding-
right:6px; white-space: nowrap\"><span style=\"font-size:12px;font-
family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-serif'; display:
block; padding-bottom:2px; white-space:no-wrap; \" class=\"hydra-
p\">apple-domain-verification=un3ateee...</span></td><td
style=\"padding:3px; padding-right:6px; white-space: normal\"><span
style=\"font-size:12px;font-family:'Helvetica Neue', 'Helvetica',
'Arial', 'sans-serif'; display: block; padding-bottom:2px; white-
space:normal; word-break: break-all; \" class=\"hydra-p\">TXT</
span></td><td style=\"padding:3px; padding-right:6px; white-space:
```

```

nowrap\"><a target=\"_blank\" rel=\"noreferrer\" style=\"\"
class=\"hydra-a\" href=https://platform.socradar.com/app/company/
14412/asm/dfp?assetType=domain&assetName=groove.example.com><span
style=\"font-size:12px;font-family:'Helvetica Neue', 'Helvetica',
'Arial', 'sans-serif'; display: block; padding-bottom:2px; white-
space:normal; word-break: break-all; \" class=\"hydra-
p\">groove.example.com</span></a></td></tr><tr class=\"hydra-tr\"></
tr></table><span style=\"display: block; width: 100%; height: 1px;
border-bottom: 1px solid #e4e4e4; margin-bottom: 10px; margin-top:
10px;\" class=\"hydra-separator\"></span><span style=\"font-
size:12px;font-family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-
serif'; display: block; padding-bottom:2px; white-space:normal; word-
break: break-all; \" class=\"hydra-p\"><strong>Third Party Products</
strong></span><table style=\"width:100%\" class=\"hydra-table\"><tr
class=\"hydra-tr\"><td style=\"padding:3px; padding-right:6px; white-
space: nowrap\"><span style=\"font-size:12px;font-family:'Helvetica
Neue', 'Helvetica', 'Arial', 'sans-serif'; display: block; padding-
bottom:2px; white-space:no-wrap; \" class=\"hydra-p\"><strong>Asset</
strong></span></td><td style=\"padding:3px; padding-right:6px; white-
space: normal\"><span style=\"font-size:12px;font-family:'Helvetica
Neue', 'Helvetica', 'Arial', 'sans-serif'; display: block; padding-
bottom:2px; white-space:normal; word-break: break-all; \"
class=\"hydra-p\"><strong>Type</strong></span></td><td
style=\"padding:3px; padding-right:6px; white-space: nowrap\"><span
style=\"font-size:12px;font-family:'Helvetica Neue', 'Helvetica',
'Arial', 'sans-serif'; display: block; padding-bottom:2px; white-
space:no-wrap; \" class=\"hydra-p\"><strong>Source</strong></span></
td></tr><tr class=\"hydra-tr\"><td style=\"padding:3px; padding-
right:6px; white-space: nowrap\"><span style=\"font-size:12px;font-
family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-serif'; display:
block; padding-bottom:2px; white-space:no-wrap; \" class=\"hydra-
p\">Netsweeper</span></td><td style=\"padding:3px; padding-right:6px;
white-space: normal\"><span style=\"font-size:12px;font-
family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-serif'; display:
block; padding-bottom:2px; white-space:normal; word-break: break-all;
\" class=\"hydra-p\">Network Services</span></td><td
style=\"padding:3px; padding-right:6px; white-space: nowrap\"><a
target=\"_blank\" rel=\"noreferrer\" style=\"\" class=\"hydra-a\"
href=https://platform.socradar.com/app/company/14412/asm/dfp?
assetType=technology&assetName=Netsweeper><span style=\"font-
size:12px;font-family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-
serif'; display: block; padding-bottom:2px; white-space:normal; word-
break: break-all; \" class=\"hydra-p\">http://example.com</span></

```



```
a></td></tr><tr class=\"hydra-tr\"><td style=\"padding:3px; padding-
right:6px; white-space: nowrap\"><span style=\"font-size:12px;font-
family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-serif'; display:
block; padding-bottom:2px; white-space:no-wrap; \" class=\"hydra-
p\">WPEngine</span></td><td style=\"padding:3px; padding-right:6px;
white-space: normal\"><span style=\"font-size:12px;font-
family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-serif'; display:
block; padding-bottom:2px; white-space:normal; word-break: break-all;
\" class=\"hydra-p\">CMS</span></td><td style=\"padding:3px; padding-
right:6px; white-space: nowrap\"><a target=\"_blank\"
rel=\"noreferrer\" style=\"\" class=\"hydra-a\" href=https://
platform.socradar.com/app/company/14412/asm/dfp?
assetType=technology&assetName=WPEngine><span style=\"font-
size:12px;font-family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-
serif'; display: block; padding-bottom:2px; white-space:normal; word-
break: break-all; \" class=\"hydra-p\">http://example.com</span></
a></td></tr><tr class=\"hydra-tr\"><td style=\"padding:3px; padding-
right:6px; white-space: nowrap\"><span style=\"font-size:12px;font-
family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-serif'; display:
block; padding-bottom:2px; white-space:no-wrap; \" class=\"hydra-
p\">AuthentXware</span></td><td style=\"padding:3px; padding-
right:6px; white-space: normal\"><span style=\"font-size:12px;font-
family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-serif'; display:
block; padding-bottom:2px; white-space:normal; word-break: break-all;
\" class=\"hydra-p\">Network Services</span></td><td
style=\"padding:3px; padding-right:6px; white-space: nowrap\"><a
target=\"_blank\" rel=\"noreferrer\" style=\"\" class=\"hydra-a\"
href=https://platform.socradar.com/app/company/14412/asm/dfp?
assetType=technology&assetName=AuthentXware><span style=\"font-
size:12px;font-family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-
serif'; display: block; padding-bottom:2px; white-space:normal; word-
break: break-all; \" class=\"hydra-p\">http://example.com</span></
a></td></tr><tr class=\"hydra-tr\"><td style=\"padding:3px; padding-
right:6px; white-space: nowrap\"><span style=\"font-size:12px;font-
family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-serif'; display:
block; padding-bottom:2px; white-space:no-wrap; \" class=\"hydra-
p\">PHP</span></td><td style=\"padding:3px; padding-right:6px; white-
space: normal\"><span style=\"font-size:12px;font-family:'Helvetica
Neue', 'Helvetica', 'Arial', 'sans-serif'; display: block; padding-
bottom:2px; white-space:normal; word-break: break-all; \"
class=\"hydra-p\">Web Frameworks</span></td><td style=\"padding:3px;
padding-right:6px; white-space: nowrap\"><a target=\"_blank\"
rel=\"noreferrer\" style=\"\" class=\"hydra-a\" href=https://
```

```
platform.socradar.com/app/company/14412/asm/dfp?
assetType=technology&assetName=PHP><span style=\"font-size:12px;font-
family:'Helvetica Neue', 'Helvetica', 'Arial', 'sans-serif'; display:
block; padding-bottom:2px; white-space:normal; word-break: break-all;
\" class=\"hydra-p\">http://example.com</span></a></td></tr><tr
class=\"hydra-tr\"></tr></table><span style=\"display: block; width:
100%; height: 1px; border-bottom: 1px solid #e4e4e4; margin-bottom:
10px; margin-top: 10px;\" class=\"hydra-separator\"></span></span>\n
</td>\n
</tr>\n
table>\n
td>\n
\n
\n
\n
\n
<table role=\"presentation\" align=\"center\" cellpadding=\"0\"
cellspacing=\"0\" \n
border=\"0\" \n
style=\"margin-top:8px;margin-bottom:10px; width: 100%;\">\n
<tr>\n
width=\"180px\" style='color:#424266;height: 30px;'\n
<span style='font-size:18px;font-weight:500;font-family:\"Helvetica
Neue\", \"Helvetica\", \"Arial\", \"sans-serif\"'\n
Mitigation\n
span>\n
</tr>\n
<td style=\"border-bottom:2px solid #424266;\"></td>\n
</tr>\n
</table>\n
<table role=\"presentation\" align=\"center\" cellpadding=\"0\"
cellspacing=\"0\" \n
border=\"0\" \n
style=\"margin-top: 5px;margin-bottom: 5px;width: 100%;border-
collapse: collapse\">\n
<tr>\n
style='padding: 5px 8px 5px 0; width: 100%;text-align: left;'\n
<span style='font-size:12px;font-family:\"Helvetica Neue\",
\"Helvetica\", \"Arial\", \"sans-serif\"'\n
<li>\n
Make sure that the newly detected asset is added to the digital asset
inventory.\n
</li> \n
<li>\n
```

```

Identify risks and weaknesses on the asset(s).\n
</li> \n
<li>\n
Make vulnerability scans and perform security checks on the asset(s).\n
\n                                     </li>\n
<li>\n                                     If\n
any weaknesses found should be mitigated according to the risk level\n
they comprise.\n
</li> \n
</ul></span>\n                                     </td>\n
</tr>\n                                     </table>\n
\n                                     </td>\n
</tr>\n                                     </tbody>\n
</table>\n                                     </td>\n                                     </tr>\n
</tbody>\n                                     </table>\n                                     <table\n
role=\"presentation\" align=\"center\" cellpadding=\"0\"\n
cellspacing=\"0\" border=\"0\" \n                                     style=\"margin:\n
0px auto;;min-width: 680px;max-width: 680px; width:680px;border-\n
collapse: collapse;\">\n                                     <tbody>\n
<tr>\n                                     <td style='padding-top: 0;padding-bottom:\n
0;'>\n                                     <table align=\"center\"\n
role=\"presentation\" cellpadding=\"0\" cellspacing=\"0\"\n
border=\"0\" \n                                     style=\"width:100%;max-\n
width:680px;Margin:0 auto;border-collapse: collapse;\">\n
<tbody>\n                                     <tr>\n
<td>\n                                     <table\n
role=\"presentation\" align=\"center\" cellpadding=\"0\"\n
cellspacing=\"0\" border=\"0\" \n                                     style=\"width: 100%;border-collapse: collapse;\">\n
<tbody>\n                                     <tr>\n
<td align=\"center\" \n                                     style='font-size:12px;padding-bottom:1em;padding-top: 1em;color:\n
#808080;'>\n                                     <a\n
href=\"https://platform.socradar.com/\"><span\n
style='font-size:11px;font-family:\"Helvetica Neue\", \"Helvetica\", \n
\"Arial\", \"sans-serif\"'>SOCRadar</span></a>\n
|\n                                     <a href=\"https://\n
socradar.io/blog/\"><span\n
style='font-size:11px;font-family:\"Helvetica Neue\", \"Helvetica\", \n
\"Arial\", \"sans-serif\"'>Blog</span></a>\n
|\n                                     <a href=\"https://\n
socradar.io/company/about/\"><span\n
style='font-size:11px;font-family:\"Helvetica Neue\", \"Helvetica\",

```



```

\"Arial\", \"sans-serif\"'>About</span></a>\n
</td>\n                                </tr>\n
</tbody>\n                                </table>\n
<table role=\"presentation\" align=\"center\" cellpadding=\"0\"
cellspacing=\"0\" border=\"0\" \n
style=\"width: 100%;border-collapse: collapse;\">\n
<tbody>\n                                <tr>\n
<td align=\"center\" \n
style='color:#808080; font-size:11px;padding-bottom:1em;padding-top:
1em;'>\n                                <span
style='font-size:10px;font-family:\"Helvetica Neue\", \"Helvetica\",
\"Arial\", \"sans-serif\"'>\n
Â© Copyright 2023\n
SOCRadar<br>651 N Broad St. Suite 205 Middletown â€¢ DE â€¢ 19709 â€¢
USA\n                                </span>\n
</td>\n                                </tr>\n
</tbody>\n                                </table>\n
</td>\n                                </tr>\n
</tbody>\n                                </table>\n                                </
td>\n                                </tr>\n                                </tbody>\n                                </
table>\n                                </td>\n                                </tr>\n                                </tbody>\n                                </table>\n                                </body>\n                                </
html>\",
                                \"alarm_text\": \"\",
                                \"insert_date\": \"2023-08-01T09:24:19.948520\"
                                },
                                \"update_date\": \"2023-08-01T09:24:18.861481\",
                                \"last_notification_date\": \"2023-08-01T09:24:49.846459\",
                                \"is_notified\": true,
                                \"is_false_positive\": false,
                                \"alarm_assets\": [
                                    \"EXAMPLE\"
                                ],
                                \"alarm_mitigation\": \"<ul>\n
<li>\n
Make sure that the newly detected asset is added to the digital asset
inventory.\n
</li> \n
<li>\n
Identify risks and weaknesses on the asset(s).\n
</li> \n
<li>\n
Make vulnerability scans and perform security checks on the asset(s).
\n                                </li>\n

```

```

</li>\n
any weaknesses found should be mitigated according to the risk level
they comprise.\n
</li> \n
</ul>" ,
    "alarm_post_incident_analysis": "",
    "alarm_detection_and_analysis": "",
    "alarm_response": "",
    "tags": "SSL|domain|website|IP|asset|asm"
  }
]
}

```

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
.alarm_notification_texts .alarm_title, .alarm_type_details.alarm_main_type, .alarm_type_details.alarm_sub_type, .alarm_risk_level	Event Title	Alarm	.insert_date	N/A	Fields are concatenated to form event title
.alarm_related_assets[].value	Asset	N/A	.insert_date	N/A	if the asset key is an ip, domain, or hostname
.alarm_related_assets[].value	Attribute	CPE	.insert_date	N/A	if the asset key is CPE and CPEs selected in Context Filtering
.alarm_related_entities[].value	Attribute	CVSS Score	.insert_date	N/A	if the entity key is CVSS and CVSS Score selected in Context Filtering. Updatable
.alarm_related_entities[].value	Indicator or Vulnerability	CVE	.insert_date	N/A	if the entity key is CVE and Related CVEs selected in Context Filtering
.tags[]	Tag	N/A	N/A	SSL, domain, website ,IP ,asset ,asm	if Tags selected in Context Filtering
.alarm_type_details.alarm_main_type	Attribute	Main Type	.insert_date	Internet Asset Inventory Monitoring	if Main Type selected in Context Filtering
.alarm_type_details.alarm_sub_type	Attribute	Sub Type	.insert_date	Asset Discovery	if Sub Type selected in Context Filtering
.alarm_type_details.alarm_group_name	Attribute	Group Name	.insert_date	N/A	if Group Name selected in Context Filtering
.alarm_risk_level	Attribute	Severity	.insert_date	INFO	if Severity selected in Context Filtering. Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.is_false_positive</code>	Attribute	Is False Positive	<code>.insert_date</code>	false	bool -> true/false. If Is False Positive selected in Context Filtering. Updatable
<code>.id</code>	Attribute	Alarm Link	<code>.insert_date</code>	https://platform.socradar.com/app/company/{{ user_fields.company_id }}/alarm-management?tab=approved&consolidatedAlarmId=1483868	Concatenated with portal URL & company ID if Alarm Link selected in Context Filtering.
<code>.is_resolved</code>	Attribute	Is Resolved	<code>.insert_date</code>	false	bool -> true/false. Updatable. If Is Resolved selected in Context Filtering
<code>.resolved_date</code>	Attribute	Resolved Date	<code>.insert_date</code>	N/A	If Resolved Date selected in Context Filtering

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/latest`

Sample Response:

```
{
  "is_success": true,
  "message": "Success",
  "response_code": 200,
  "data": [
    {
      "id": 3218556,
      "status": 1,
      "notes": null,
      "title": "Thirdparty Product \"\" Vulnerability
Detected",
      "vuln_details": {
        "id": 3218556,
        "alarm_id": 1495615,
        "alarm_mitigation": "<li>Since the vulnerability is
found through the passive scan, the server might have been patched or
hardened and this could be, therefore, a false positive. </li>\nIf
the vulnerability is not false positive;\n<li>Go to the network
service provider's website in order to find the required patched
version.</li>\n<li>Test the patched version in a mirrored production
environment and evaluate the stability of the patch</li>\n<li>An
investigation should take place to make sure these assets have been
hardened or patched against these vulnerabilities.</li>",
        "entity": "www.threatq.com",
        "entity_type": "domain",
        "extra_entities": [
          "141.193.213.10",
          "141.193.213.11"
        ]
      },
      "cvss": 1.9,
      "product": null,
      "version": null,
    }
  ]
}
```

```

        "vuln_date": "2023-08-06 19:45",
        "incident": 1495615,
        "cve": "CVE-2018-10545",
        "is_resolved": null,
        "is_archived": null,
        "is_false_positive": null,
        "incident_is_resolved": false,
        "incident_is_archived": false,
        "incident_is_false_positive": false,
        "cve_details": "An issue was discovered in PHP before
5.6.35, 7.0.x before 7.0.29, 7.1.x before 7.1.16, and 7.2.x before
7.2.4. Dumpable FPM child processes allow bypassing opcache access
controls because fpm_unix.c makes a PR_SET_DUMPABLE prctl call,
allowing one user (in a multiuser environment) to obtain sensitive
information from the process memory of a second user's PHP
applications by running gcore on the PID of the PHP-FPM worker
process."
    },
    {
        "id": 3218555,
        "status": 1,
        "notes": null,
        "title": "Thirdparty Product \"\" Vulnerability
Detected",
        "vuln_details": {
            "id": 3218555,
            "alarm_id": 1495615,
            "alarm_mitigation": "<li>Since the vulnerability is
found through the passive scan, the server might have been patched or
hardened and this could be, therefore, a false positive. </li>\nIf
the vulnerability is not false positive;\n<li>Go to the network
service provider's website in order to find the required patched
version.</li>\n<li>Test the patched version in a mirrored production
environment and evaluate the stability of the patch</li>\n<li>An
investigation should take place to make sure these assets have been
hardened or patched against these vulnerabilities.</li>",
            "entity": "www.threatq.com",
            "entity_type": "domain",
            "extra_entities": [
                "141.193.213.10",
                "141.193.213.11"
            ]
        }
    }
]

```

```

    },
    "cvss": 2.6,
    "product": null,
    "version": null,
    "vuln_date": "2023-08-06 19:45",
    "incident": 1495615,
    "cve": "CVE-2014-4721",
    "is_resolved": null,
    "is_archived": null,
    "is_false_positive": null,
    "incident_is_resolved": false,
    "incident_is_archived": false,
    "incident_is_false_positive": false,
    "cve_details": "The phpinfo implementation in ext/
standard/info.c in PHP before 5.4.30 and 5.5.x before 5.5.14 does not
ensure use of the string data type for the PHP_AUTH_PW,
PHP_AUTH_TYPE, PHP_AUTH_USER, and PHP_SELF variables, which might
allow context-dependent attackers to obtain sensitive information
from process memory by using the integer data type with crafted
values, related to a \"type confusion\" vulnerability, as
demonstrated by reading a private SSL key in an Apache HTTP Server
web-hosting environment with mod_ssl and a PHP 5.3.x mod_php."
  }
]
}

```

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
.cve	Indicator or Vulnerability Value	CVE	.vuln_date	CVE-2023-21391	N/A
.cvss	Attribute	CVSS Score	vuln_date	2.6	Updatable
.product	Attribute	Affected Product	.vuln_date	N/A	N/A
.version	Attribute	Affected Product Version	.vuln_date	N/A	N/A
.cve_details, .vuln_details.ent ity, .vuln_deteails.al arm_mitigation	Object Description	N/A	N/A	The phpinfo implementation in ext/ standard/...	Concatenated to form HTML

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 Alarms

METRIC	RESULT
Run Time	1 minutes
Events	25
Event Attributes	260
Assets	25
Vulnerability	207

SOCRadar Vulnerabilities

METRIC	RESULT
Run Time	1 minute
Vulnerabilities	207
Vulnerability Attributes	207

Known Issues / Limitations

- The Alarms feed API does not support pagination, so a max of 1k alarms will be fetched per feed run.
- The Alarms feed API currently does not filter the data correctly if `Main Type Selection` or `Sub Type Selection` contains more than one value. SOCRadar has been notified about this issue.
- The Leaks feed 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.
- The Vulnerabilities feed API does not support pagination, so the `Max Count` field must be used to limit the amount of data ingested. If you are running into timeout errors (524), lower the `Max Count` value.

Change Log

- **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