ThreatQuotient

A Securonix Company

Securonix Unified Defense SIEM CDF

Version 1.2.0 rev-b

August 14, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

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

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2025 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: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.2.0
Compatible with ThreatQ Versions	>= 5.12.0
Support Tier	ThreatQ Supported

Introduction

The Securonix Unified Defense SIEM CDF for ThreatQ enables analysts to ingest statistical reports and identities from Securonix.

The integrations provides the following feeds:

- **Securonix - Identities** - pulls all users that interact with the IT infrastructure of the organization.
- **Securonix - Incidents** - pulls incidents from Securonix.
- **Securonix - Top Threats** - pulls top threat reports from Securonix.
- **Securonix - Top Violations** - pulls top violation reports from Securonix.
- **Securonix - Top Violators** - pulls top violators reports from Securonix.
- **Securonix - Top Violators by User** - pulls top violations reports by the user from Securonix.

The integration ingests the following system objects:

- Identities
- Incidents
- Reports

Prerequisites

The following is required to utilize the integration:

- A Securonix instance.
- The Hostname or IP Address for the Securonix instance.
- Securonix Username and Password.
    - This account must be assigned the following role: `ROLE_API`.

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:

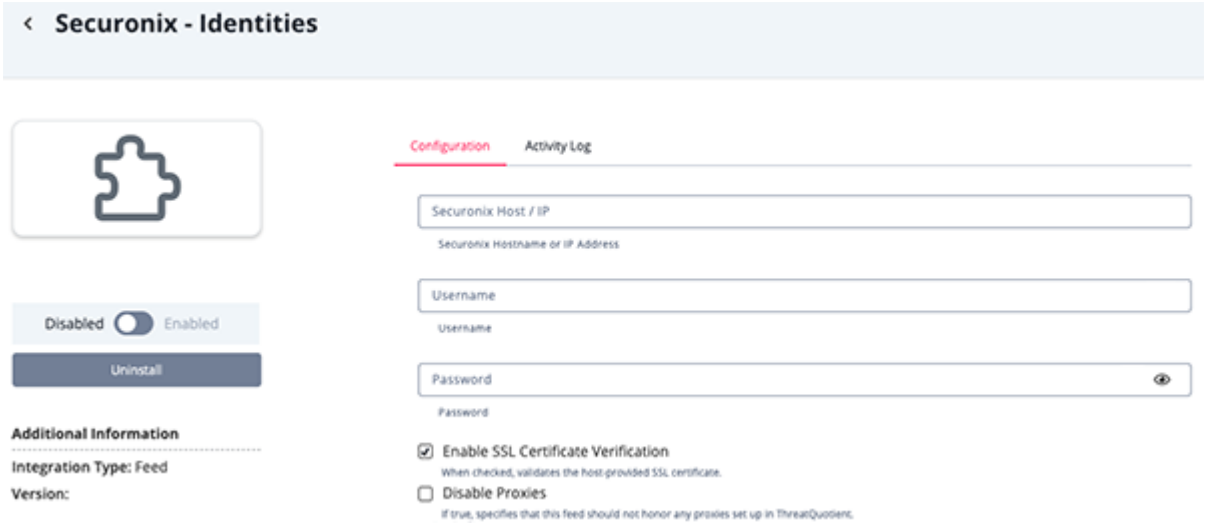
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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:

Securonix - Identities Parameters

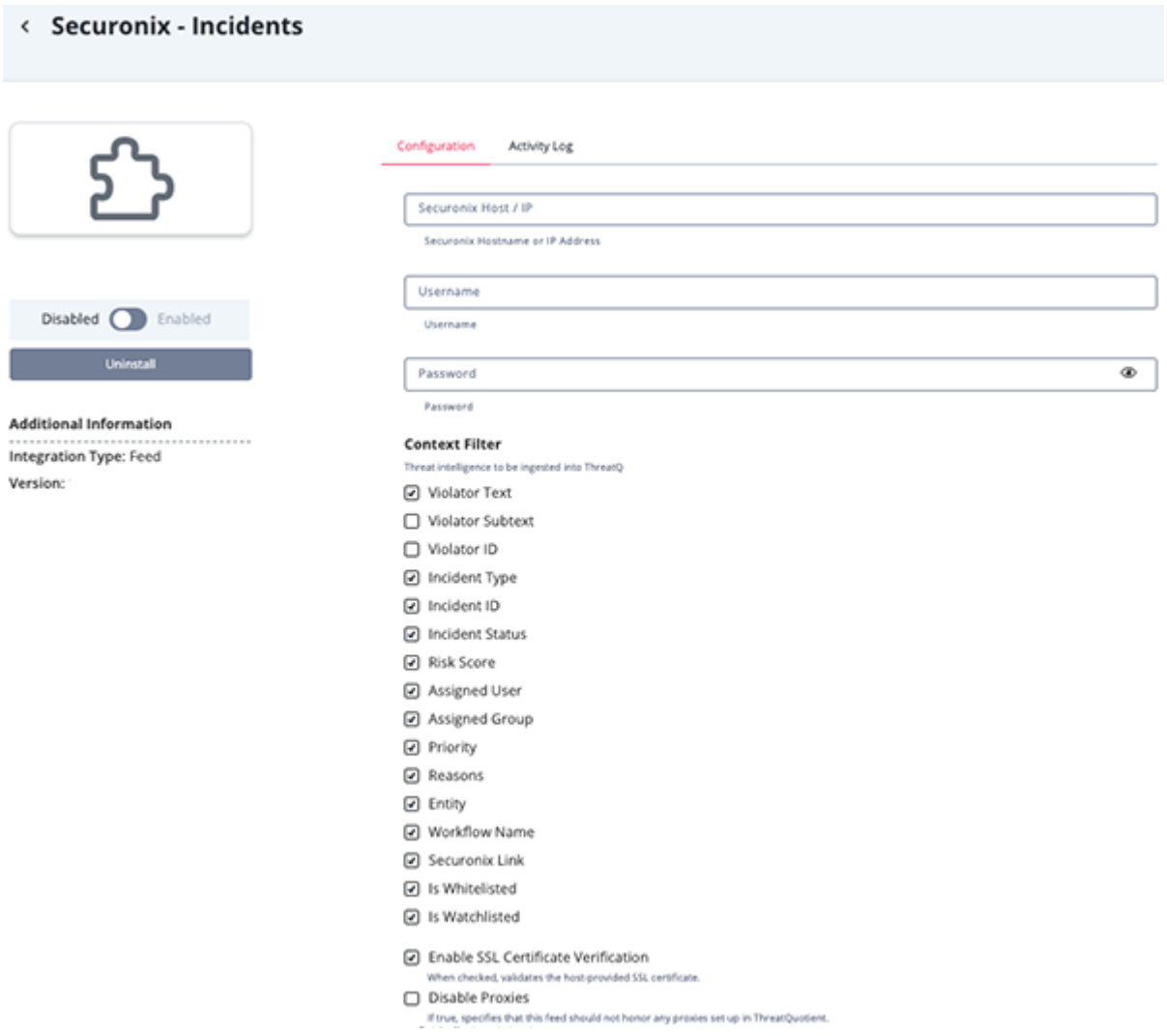
PARAMETER	DESCRIPTION
Securonix Host / IP	Enter your Securonix Hostname or IP Address.
Securonix Username	Enter your Secuornix username.
Securonix Password	Enter the password associated with the username above.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.



Securonix - Incidents Parameters

PARAMETER	DESCRIPTION
Securonix Host / IP	Enter your Securonix Hostname or IP Address.
Securonix Username	Enter your Secuornix username.
Securonix Password	Enter the password associated with the username above.
Context Filter	Select the threat intelligence you to be ingested into ThreatQ. Options include: ◦ Violator Text *(default)* ◦ Violator Subtext ◦ Violator ID ◦ Incident Type *(default)* ◦ Incident ID *(default)* ◦ Incident Status *(default)* ◦ Risk Score *(default)* ◦ Assigned User *(default)* ◦ Assigned Group *(default)* ◦ Priority *(default)* ◦ Reasons *(default)* ◦ Entity *(default)* ◦ Workflow Name *(default)* ◦ Securonix Link *(default)* ◦ Is Whitelisted *(default)*

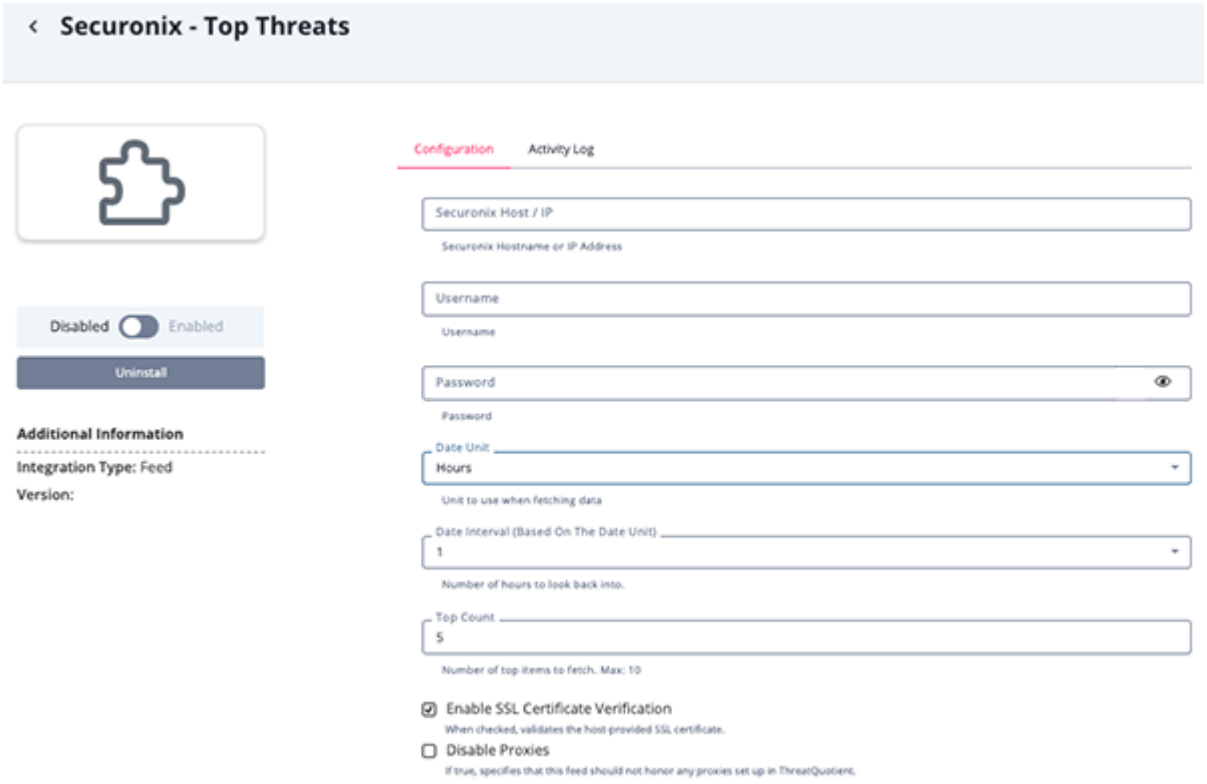
PARAMETER	DESCRIPTION
	◦ Is Watchlisted *(default)*
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.



Securonix - Top Threats Parameters

PARAMETER	DESCRIPTION
Securonix Host / IP	Enter your Securonix Hostname or IP Address.
Securonix Username	Enter your Secuornix username.
Securonix Password	Enter the password associated with the username above.
Date Unit	Select the unit of measurement when fetching top threats. Options include: ◦ Days *(default)* ◦ Hours
Date Interval (Based on the Date Unit)	Select how far back the feed should look back based on the measurement type selected in the **Date Unit** parameter. **Example**: if you selected `Days` as the measurement for the **Date Unit** parameter and entered `4` in this parameter, the feed interval will be the past 4 days. Options include: **Date Unit: Hours** ◦ 1 ◦ 2 ◦ 6 ◦ 12 ◦ 24 *(default)* ◦ 48 ◦ 72 ◦ 60 ◦ 90 **Date Unit: Days** ◦ 7 *(default)* ◦ 14 ◦ 21 ◦ 30 ◦ 60 ◦ 90
Top Count	Enter the top number of items to fetch. The default value is 5.

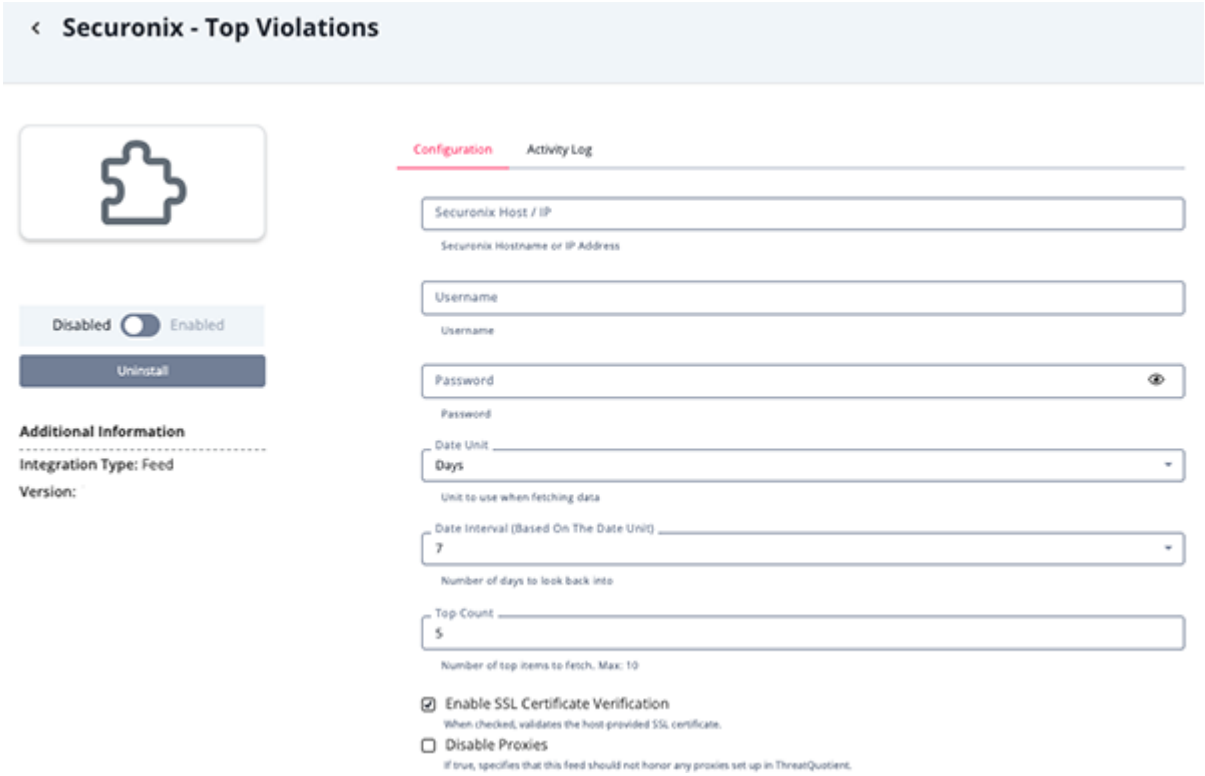
PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.



Securonix - Top Violations Parameters

PARAMETER	DESCRIPTION
Securonix Host / IP	Enter your Securonix Hostname or IP Address.
Securonix Username	Enter your Secuornix username.

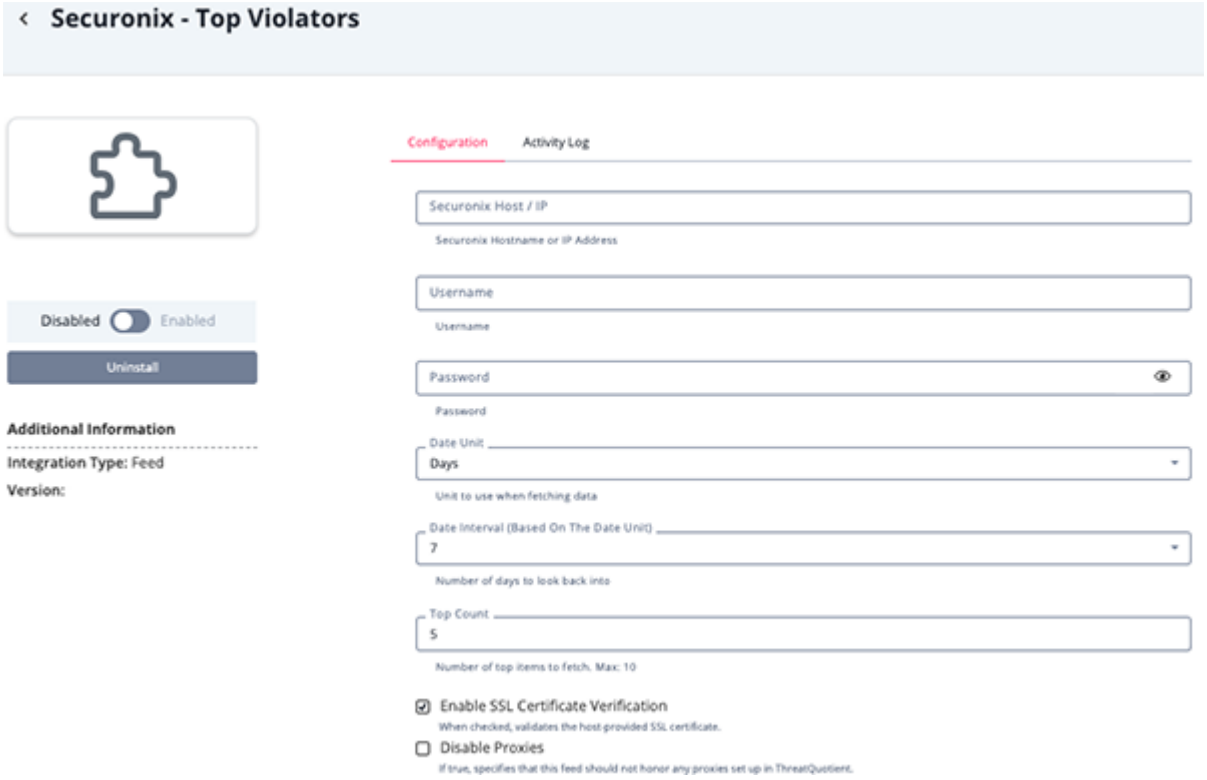
PARAMETER	DESCRIPTION
Securonix Password	Enter the password associated with the username above.
Date Unit	Select the unit of measurement when fetching top threats. Options include: ◦ Days *(default)* ◦ Hours
Date Interval (Based on the Date Unit)	Select how far back the feed should look back based on the measurement type selected in the **Date Unit** parameter. **Example**: if you selected `Days` as the measurement for the **Date Unit** parameter and entered `4` in this parameter, the feed interval will be the past 4 days. Options include: **Date Unit: Hours** ◦ 1 ◦ 2 ◦ 6 ◦ 12 ◦ 24 *(default)* ◦ 48 ◦ 72 ◦ 60 ◦ 90 **Date Unit: Days** ◦ 7 *(default)* ◦ 14 ◦ 21 ◦ 30 ◦ 60 ◦ 90
Top Count	Enter the top number of items to fetch. The default value is 5.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.



Securonix - Top Violators Parameters

PARAMETER	DESCRIPTION
Securonix Host / IP	Enter your Securonix Hostname or IP Address.
Securonix Username	Enter your Secuornix username.
Securonix Password	Enter the password associated with the username above.
Date Unit	Select the unit of measurement when fetching top threats. Options include: ◦ Days *(default)* ◦ Hours

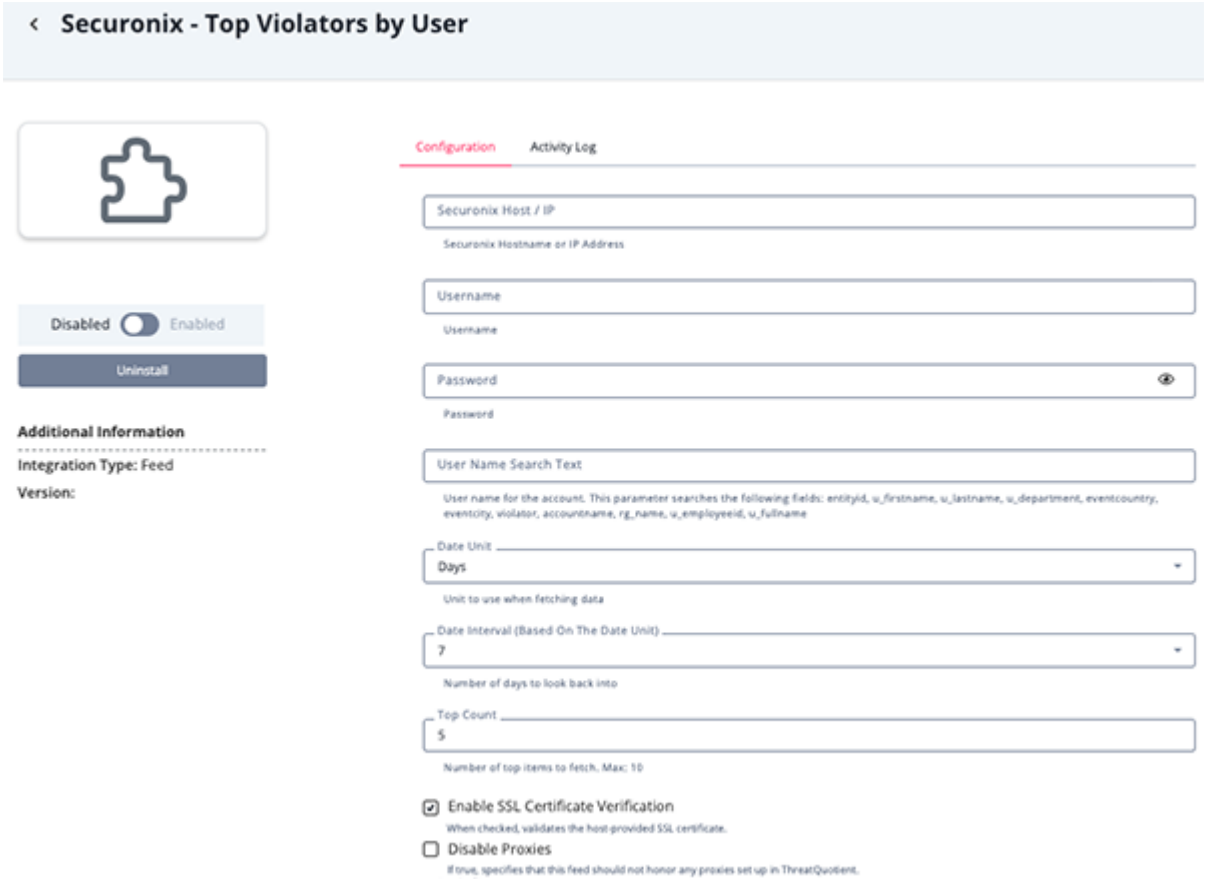
PARAMETER	DESCRIPTION
Date Interval (Based on the Date Unit)	Select how far back the feed should look back based on the measurement type selected in the **Date Unit** parameter. **Example**: if you selected `Days` as the measurement for the **Date Unit** parameter and entered `4` in this parameter, the feed interval will be the past 4 days. Options include: **Date Unit: Hours** ◦ 1 ◦ 2 ◦ 6 ◦ 12 ◦ 24 *(default)* ◦ 48 ◦ 72 ◦ 60 ◦ 90 **Date Unit: Days** ◦ 7 *(default)* ◦ 14 ◦ 21 ◦ 30 ◦ 60 ◦ 90
Top Count	Enter the top number of items to fetch. The default value is 5.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.



Securonix - Top Violators by User Parameters

PARAMETER	DESCRIPTION
Securonix Host / IP	Enter your Securonix Hostname or IP Address.
Securonix Username	Enter your Secuornix username.
Securonix Password	Enter the password associated with the username above.
User Name Search Text	Enter an account username to be used to search against the following fields: `entityid`, `u_firstname`, `u_lastname`, `u_department`, `eventcountry`, `eventcity`, `violator`, `accountname`, `rg_name`, `u_employeeid`, and `u_fullname`

PARAMETER	DESCRIPTION
Date Unit	Select the unit of measurement when fetching top threats. Options include: ◦ Days *(default)* ◦ Hours
Date Interval (Based on the Date Unit)	Select how far back the feed should look back based on the measurement type selected in the **Date Unit** parameter. **Example**: if you selected `Days` as the measurement for the **Date Unit** parameter and entered `4` in this parameter, the feed interval will be the past 4 days. Options include: **Date Unit: Hours** ◦ 1 ◦ 2 ◦ 6 ◦ 12 ◦ 24 *(default)* ◦ 48 ◦ 72 ◦ 60 ◦ 90 **Date Unit: Days** ◦ 7 *(default)* ◦ 14 ◦ 21 ◦ 30 ◦ 60 ◦ 90
Top Count	Enter the top number of items to fetch. The default value is 5.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.



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

Securonix - Identities

The Securonix - Identities feed pulls all users that interact with the IT infrastructure of the organization. These users can include employees, contractors, temporary workers, partners, vendors, suppliers, and customers.

```
GET https://{{host}}/Snypr/ws/spotter/index/search?query=index=users
```

Sample Response:


```
{
  "applicationTz": "EST5EDT",
  "available": false,
  "error": false,
  "events": [
    {
      "createdate": "1674680867000",
      "customfield13": "805306368",
      "customfield2": "CN=Yashasvi Nijhawan,OU=HR,DC=ionxsecure,DC=com",
      "customfield5": "0",
      "customfield6": "0",
      "customfield7": "20220919190515.0Z",
      "customfield8": "20211207045039.0Z",
      "employeeid": "ynijhawan",
      "firstname": "Yashasvi",
      "fullname": "Yashasvi Nijhawan",
      "lastname": "Nijhawan",
      "lastsynctime": "1674681012000",
      "masked": "false",
      "preferredname": "Yashasvi Nijhawan",
      "status": "1",
      "statusdescription": "66048",
      "tenantid": "2",
      "tenantname": "a1t1sipi",
      "usercriticality": "Low",
      "userriskscore": "0.01",
      "usertimezoneoffset": "UTC"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.events[].fullname	Identity Value	N/A	.events[].createdate	`Yashasvi Nijhawan`	N/A
.events[].employeeid	Identity Attribute	Employee ID	.events[].createdate	`ynijhawan`	N/A
.events[].usercriticality	Identity Attribute	User Criticality	.events[].createdate	`Low`	Updatable
.events[].usertimezoneoffset	Identity Attribute	User Timezone	.events[].createdate	`UTC`	N/A
.events[].userriskscore	Identity Attribute	User Risk Score	.events[].createdate	`0.01`	Updatable
.events[].lastsynctime	Identity Attribute	User Last Sync Time	.events[].createdate	`1674681012000`	Updatable .Timestamp value

Securonix - Incidents

The Securonix - Incidents feed pulls incidents from Securonix into ThreatQ as incident objects.

`GET https://{{host}}/companies/{{domain}}/Snypr/ws/incident/get`

Sample Response:


```
{
  "status": "OK",
  "result": {
    "data": {
      "totalIncidents": 1.0,
      "incidentItems": [
        {
          "violatorText": "Cyndi Converse",
          "lastUpdateDate": 1566293234026,
          "violatorId": "96",
          "incidentType": "RISK MODEL",
          "incidentId": "100181",
          "incidentStatus": "COMPLETED",
          "riskscore": 0.0,
          "assignedUser": "Account Access 02",
          "assignedGroup": "Administrators",
          "priority": "None",
          "reason": [
            "Threat Model: AWS - CLOUD ACCOUNT COMPROMISE AND DATA EXFILTRATION
DETECTED",
            {
              "Policies": [
                "Authentication detected from a rare geolocation on Cloud",
                "AWS - Potential MFA Bypass",
                "Successful Login From Malicious IP",
                "AWS - Suspicious Privilege Escalation Compared to Peers",
                "AWS - Suspicious Access Key Creation",
                "AWS - GuardDuty Disabled",
                "AWS - CloudTrail Logging Stopped",
                "Potential RDS Database Exfiltration Detected",
                "Potential Data Exfiltration via DynamoDB Scan or Query",
                "AWS - Possible S3 Data Exfiltration"
              ]
            }
          ],
          "violatorSubText": "1096",
          "entity": "Users",
          "workflowName": "SOCTeamReview",
          "url": "https://saaspocapp2t14wptp.securonix.net/Snypr/
configurableDashboards/view?type=incidentid=100181",
          "isWhitelisted": false,
          "watchlisted": false
```

```
        },
        {
          "violatorText": "HENRY PATSUN",
          "lastUpdateDate": 1566293234026,
          "violatorId": "09",
          "incidentType": "RISK MODEL",
          "incidentId": "262170",
          "incidentStatus": "OPEN",
          "riskscore": 0.0,
          "assignedUser": "Account Access 02",
          "assignedGroup": "Administrators",
          "priority": "None",
          "reason": [
            "Number Of Threat: 5"
          ],
          "violatorSubText": "1009",
          "entity": "Users",
          "workflowName": "QA Workflow Basic",
          "url": "https://saaspocapp2t14wptp.securonix.net/Snypr/
configurableDashboards/view?type=incidentid=100181",
          "isWhitelisted": false,
          "watchlisted": false
        },
        {
          "violatorText": "172.17.6.112",
          "lastUpdateDate": 1566293234026,
          "violatorId": "96",
          "incidentType": "RISK MODEL",
          "incidentId": "250026",
          "incidentStatus": "OPEN",
          "riskscore": 0.0,
          "assignedUser": "Account Access 02",
          "assignedGroup": "Admin Admin",
          "priority": "None",
          "reason": [
            "Policy: SOAR_PlaybookPolicy"
          ],
          "violatorSubText": "1096",
          "entity": "IOC",
          "workflowName": "SOCTeamReview",
          "url": "https://saaspocapp2t14wptp.securonix.net/Snypr/
configurableDashboards/view?type=incidentid=100181",
          "isWhitelisted": false,
          "watchlisted": true
        }
      ]
    }
  }
}
```

ThreatQuotient provides the following default mapping for this feed based on pulling data out of the `result.data.incidentItems[]` JSON path:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
data.incidentItems[].<see note>	Incident Value	N/A	N/A	`Incident Value`	N/A
data.incidentItems[].isWhitelisted	Incident Tag	N/A	N/A	`whitelisted`	`whitelisted` If `True`
data.incidentItems[].watchlisted	Incident Tag	N/A	N/A	`watchlisted`	`watchlisted` If `True`
data.incidentItems[].workflowName	Incident Tag	N/A	N/A	`SOCTeamReview`	N/A
data.incidentItems[].assignedGroup	Incident Tag	N/A	N/A	`Administrators`	N/A
data.incidentItems[].violatorText	Incident Attribute	Violator Text	N/A	`Cyndi Converse`	User-configurable
data.incidentItems[].violatorSubText	Incident Attribute	Violator Subtext	N/A	`1096`	User-configurable
data.incidentItems[].violatorId	Incident Attribute	Violator ID	N/A	`96`	User-configurable
data.incidentItems[].incidentType	Incident Attribute	Incident Type	N/A	`RISK MODEL`	User-configurable
data.incidentItems[].incidentId	Incident Attribute	Incident ID	N/A	`100181`	User-configurable
data.incidentItems[].incidentStatus	Incident Attribute	Status	N/A	`COMPLETED`	User-configurable. Updatable
data.incidentItems[].riskscore	Incident Attribute	Risk Score	N/A	`0.0`	User-configurable. Updatable
data.incidentItems[].assignedUser	Incident Attribute	Assigned User	N/A	`Account Access 02`	User-configurable
data.incidentItems[].priority	Incident Attribute	Priority	N/A	`None`	User-configurable. Updatable
data.incidentItems[].reason[]	Incident Attribute	Reason	N/A	`Threat Model: AWS...`	User-configurable. If the value is string.
data.incidentItems[].reason.Policies[]	Incident Description	N/A	N/A	`Authentication detected from a rare...`	N/A
data.incidentItems[].entity	Incident Attribute	Entity	N/A	`Users`	User-configurable
data.incidentItems[].workflowName	Incident Attribute	Workflow	N/A	`SOCTeamReview`	User-configurable
data.incidentItems[].url	Incident Attribute	Securonix Link	N/A	`https://saaspocapp2t14wptp.securonix.net/Snypr/configurableDashboards/view?&type=incident&id=100181`	User-configurable
data.incidentItems[].isWhitelisted	Incident Attribute	Is Whitelisted	N/A	`True`	User-configurable. Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
data.incidentItems[].watchlisted	Incident Attribute	Is Watchlisted	N/A	`False`	User-configurable. Updatable

Keys used to format the incident value:

- `.violatorText` `.violatorSubText` `.reason` `.priority` `.riskscore` `.incidentId`

Selected keys are formatted into a title template `| .lastUpdateDate | Securonix Incident: {{violatorText}} ({{violatorSubText}}) {{value.reason}} [Priority: {{priority}}; Risk Score: {{riskscore}}; ID: {{incidentId}}] |`

Securonix - Top Threats

The Securonix - Top Threats feed pulls top threat reports from Securonix into ThreatQ as report objects.

```
GET https://{{host}}/Snypr/ws/sccWidget/getTopThreats
```

Sample Response:


```
{
  "Response": {
    "Date range": [
      "Jun 11, 2018 11:18:09 AM",
      "Sep 9, 2018 11:18:09 AM"
    ],
    "Total records": 8,
    "Docs": [
      {
        "Threat model id": 118,
        "Threat nodel name": "Patient Data Compromise",
        "Description": "No of Stages: 4, Risk Scoring Scheme:STATIC,
Weight:100.0",
        "Criticality": "Low",
        "No of violator": 1,
        "Generation time": 1532388410500
      },
      {
        "Threat model id": 194,
        "Threat nodel name": "Privileged IT User-Sabotage",
        "Description": "No of Stages: 4, Risk Scoring Scheme:STATIC,
Weight:100.0",
        "Criticality": "Medium",
        "No of violator": 1,
        "Generation time": 1532372629487
      }
    ]
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.Response.Date range	Report Value	N/A	N/A	`Securonix Top Threats: Jun 11, 2018 11:18:09 AM -> Sep 9, 2018 11:18:09 AM`	N/A
.Response.Docs[].<see note>	Report Description	N/A	N/A	N/A	See note below
.Response.Docs[].Threat model name	Report Attribute	Top Threat	N/A	`Privileged IT User-Sabotage`	N/A

Keys used to format the report description:

- `.Threat Model name`
- `.Threat Model id`
- `.Description`
- `.Criticality`
- `.No of violator`

Securonix - Top Violations

The Securonix - Top Violations feed pulls top violation reports from Securonix into ThreatQ as report objects.

```
GET https://{{host}}/Snypr/ws/sccWidget/getTopViolations
```

Sample Response:


```
{
  "Response": {
    "Date range": [
      "Jun 11, 2018 11:25:55 AM",
      "Sep 9, 2018 11:25:55 AM"
    ],
    "Total records": 38,
    "Docs": [
      {
        "Policy id": 9237,
        "Policy name": "Email to Competitor Domain",
        "Criticality": "Medium",
        "Violation entity": "Activityaccount",
        "Policy category": "ALERT",
        "Threat indicator": "Email to Competitor Domain",
        "Generation time": 1533250072115,
        "No of violator": 14,
        "Description": "Email to Competitor Domain"
      },
      {
        "Policy id": 9236,
        "Policy name": "Abnormal number of emails sent to external domain as
compared to peer members",
        "Criticality": "Low",
        "Violation entity": "Activityaccount",
        "Policy category": "ALERT",
        "Threat indicator": "Abnormal number of emails sent to external domain
as compared to peer members",
        "Generation time": 1533171483400,
        "No of violator": 1,
        "Description": "Abnormal number of emails sent to external domain as
compared to peer members"
      }
    ]
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.Response.Date range	Report Value	N/A	N/A	`Securonix Top Violations: Jun 11, 2018 11:25:55 AM -> Sep 9, 2018 11:25:55 AM`	N/A
.Response.Docs[].<see note>	Report Description	N/A	N/A	N/A	See note below
.Response.Docs[].Threat model name	Report Attribute	Top Violation	N/A	`Email to Competitor Domain`	N/A

The following keys are used to format the report description:

- `.Policy name`
- `.Policy id`
- `.Description`
- `.Policy category`
- `.Violation entity`
- `.Threat indicator`
- `.Criticality`
- `.No of violator`

Securonix - Top Violators and Top Violators by User

The Securonix - Top Violators feed pulls top violators reports from Securonix into ThreatQ as report objects.

Top Violators - `GET https://{{host}}/Snypr/ws/sccWidget/getTopViolators`
Top Violators by User - `GET https://{{host}}/Snypr/ws/sccWidget/getTopViolators?seatchtext{user}`

Sample Response:

```
{
    "Response": {
        "Date range": [
            "Jul 21, 2025 12:03:05 PM",
            "Jul 28, 2025 12:03:05 PM"
        ],
        "Total records": 1,
        "Docs": [{
                 "Generation time": 1753668482985,
                  "Name": "WIN-MIEVBBN67KJ\\ADMINISTRATOR ",
                  "Resource name": "WIN-MIEVBBN67KJ",
                  "Risk score": 8.6,
                  "Violator entity": "Activityaccount"
            }
        ]
    }
}
```

ThreatQuotient provides the following default mapping for these feeds:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.Response.Date range	Report Value	N/A	N/A	`Securonix Top Violators: Jul 21, 2025 12:03:05 PM -> Jul 28, 2025 12:03:05 PM`	N/A
.Response.Docs[].<see note>	Report Description	N/A	N/A	N/A	See note below
.Response.Docs[].Resource name	Report Attribute	Top Violators	N/A	`WIN-MIEVBBN67KJ`	N/A

The following keys are used to format the report description:

- `.Docs[].Name`
- `.Docs[].Risk score`
- `.Docs[].Violator entity`

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.

Securonix - Identities

METRIC	RESULT
Run Time	1 minute
Identity	113
Report Attributes	587

Securonix - Incidents

METRIC	RESULT
Run Time	1 minute
Incidents	3
Incident Attributes	45

Securonix - Top Violations

METRIC	RESULT
Run Time	1 minute
Report	1
Report Attributes	118

Securonix - Top Violators

METRIC	RESULT
Run Time	1 minute
Report	1
Report Attributes	3

Change Log

- **Version 1.2.0 rev-b**
  - Guide Update - updated **Prerequisites** chapter to include the required role, `ROLE_API`, for the Securonix user account.
- **Version 1.2.0 rev-a**
  - Guide Update - added information regarding the new **Securonix - Incidents** feed.
- **Version 1.2.0**
  - Renamed the integration to Securonix Unified Defense SIEM CDF.
  - Added the following new feeds:
    - **Securonix - Top Violators** -pulls top violators reports from Securonix.
    - **Securonix - Top Violators by User** - pulls top violations reports by the user from Securonix.
    - **Securonix - Identities** - pulls all users that interact with the IT infrastructure of the organization.
    - **Securonix - Incidents** - pulls incidents from Securonix.
  - Renamed the following feeds:
    - **Securonix SNYPR - Top Violations** is now **Securonix - Top Violations**.
    - **Securonix SNYPR - Top Threats** is now **Securonix Top Threats**.
    - **Securonix SNYPR - Incidents** is now **Securonix - Incidents**.
  - Removed the following feed:
    - Securonix SNYPR - Incidents.
  - Add the following configuration parameters to all feeds:
    - **Enable SSL Certificate Verification** - determine if the feed should validate the host-provided SSL certificate.
    - **Disable Proxies** - determine if the feed should honor proxies set in the ThreatQ UI.
- **Version 1.0.1**
  - Resolved an issue with the **Securonix SNTPR - Incidents** feed where dictionaries present in `data.incidentItems[].reason[]` would trigger feed run errors.
  - Updated the minimum ThreatQ version to 5.12.0
- **Version 1.0.0**
  - Initial release