

# ThreatQuotient



## Securonix SNYPR CDF

Version 1.0.1

June 28, 2025

### ThreatQuotient

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 **ThreatQ Supported**

### Support

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

# Contents

|   |           |
|---|-----------|
| Warning and Disclaimer .....                    | 3         |
| Support .....                                   | 4         |
| Integration Details.....                        | 5         |
| Introduction .....                              | 6         |
| Prerequisites .....                             | 7         |
| Installation.....                               | 8         |
| Configuration .....                             | 9         |
| Incidents Parameters .....                      | 9         |
| Top Violations and Top Threats Parameters ..... | 10        |
| <b>ThreatQ Mapping.....</b>                     | <b>12</b> |
| Securonix SNYPR - Incidents .....               | 12        |
| Securonix SNYPR - Top Threats .....             | 16        |
| Securonix SNYPR - Top Violations .....          | 18        |
| <b>Average Feed Run.....</b>                    | <b>20</b> |
| Securonix SNYPR - Incidents .....               | 20        |
| Securonix SNYPR - Top Threats .....             | 20        |
| Securonix SNYPR - Top Violations .....          | 21        |
| <b>Change Log .....</b>                         | <b>22</b> |

# 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](mailto: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      | 1.0.1             |
| Compatible with ThreatQ Versions | >= 5.12.1         |
| Support Tier                     | ThreatQ Supported |

# Introduction

The Securonix SNYPR CDF for ThreatQ enables analysts to automatically ingest incidents & statistic reports from Securonix SNYPR.

The integration provides the following feeds:

- **Securonix SNYPR - Incidents** - pulls incidents from Securonix SNYPR into ThreatQ as incident objects.
- **Securonix SNYPR - Top Threats** - pulls top threat reports from Securonix SNYPR into ThreatQ as report objects.
- **Securonix SNYPR - Top Violations** - pulls top violation reports from Securonix SNYPR into ThreatQ as report objects.

The integration ingests the following system objects:

- Reports
- Incidents



See the Securonix Exports topic on the ThreatQ Help Center for steps on how to export Securonix data.

# Prerequisites

The integration requires the following:

- A Securonix SNYPR username and password.
- A Securonix hostname or IP Address.

# Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
  - Drag and drop the file into the dialog box
  - Select **Click to Browse** to locate the integration file on your local machine



ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to [configure and then enable](#) the feed.



# Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

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



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

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

## Incidents Parameters

| PARAMETER           | DESCRIPTION  |
|---------------------|--|
| Securonix Host / IP | Your Securonix Hostname or IP Address.   |
| Securonix Username  | Your Securonix Username.   |
| Securonix Password  | Your Securonix Password.   |
| Context Filter      | <p>Select the threat intelligence to be ingested into ThreatQ.<br/>Options include:</p> <ul style="list-style-type: none"> <li>◦ Violator Text (default)</li> <li>◦ Violator Subtext</li> <li>◦ Violator ID</li> <li>◦ Incident Type (default)</li> <li>◦ Incident ID (default)</li> <li>◦ Assigned Group (default)</li> <li>◦ Priority (default)</li> <li>◦ Reasons (default)</li> <li>◦ Entity (default)</li> <li>◦ Workflow Name (default)</li> <li>◦ Securonix Link (default)</li> </ul> |

| PARAMETER | DESCRIPTION  |
|-----------|--|
|           | <ul style="list-style-type: none"> <li>◦ Incident Status (default)</li> <li>◦ Risk Score (default)</li> <li>◦ Assigned User (default)</li> <li>◦ Is Whitelisted (default)</li> <li>◦ Is Watchlisted (default)</li> </ul> |

### < Securonix SNYPR - Incidents



Disabled ☒ Enabled

Run Integration

Uninstall

#### Additional Information

Integration Type: Feed  
Version:

#### Configuration Activity Log

Securonix Host / IP

Securonix Hostname or IP Address

Username

Username

Password

Password

#### Context Filter


Threat Intelligence to be ingested into ThreatQ

- ☒ Violator Text
- ☐ Violator Subtext
- ☐ Violator ID
- ☒ Incident Type
- ☒ Incident ID
- ☒ Incident Status
- ☒ Risk Score
- ☒ Assigned User
- ☒ Assigned Group
- ☒ Priority
- ☒ Reasons
- ☒ Entity
- ☒ Workflow Name
- ☒ Securonix Link

## Top Violations and Top Threats Parameters

| PARAMETER           | DESCRIPTION                            |
|---------------------|--|
| Securonix Host / IP | Your Securonix Hostname or IP Address. |
| Securonix Username  | Your Securonix Username.               |

| PARAMETER                              | DESCRIPTION   |
|--|---|
| Securonix Password                     | Your Securonix Password.  |
| Date Unit                              | The unit to use when fetching the top threats/violations.<br>The default setting is <b>Days</b> . |
| Date Interval (Based on the Date Unit) | The number of days/hours to look back into.<br>The default setting is 7.                          |
| Top Count                              | The number of top items to fetch.<br>The default setting is 5.                                    |



Disabled
☒
Enabled

Run Integration

Uninstall

**Additional Information**


---

Integration Type: Feed  
Version:

Configuration
Activity Log

Securonix Host / IP

Securonix Hostname or IP Address

Username

Username

Password

Password

Date Unit

Days

Date Interval (Based on the Date Unit)

7

Top Count

5

- Review any additional settings, make any changes if needed, and click on **Save**.
- Click on the toggle switch, located above the *Additional Information* section, to enable it.

# ThreatQ Mapping

## Securonix SNYPR - Incidents

The Securonix SNYPR - Incidents feed periodically pulls incidents from Securonix SNYPR 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": [
            "Resource: Symantec Email DLP"
          ],
          "violatorSubText": "1096",
          "entity": "Users",
          "workflowName": "SOCTeamReview",
          "url": "https://saaspocapp2t14wptp.securonix.net/Snypr/configurableDashboards/view?type=incident&id=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=incident&id=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=incident&id=100181",
        "isWhitelisted": false,
        "watchlisted": true
    }
]
}
}
}
}
}

```

ThreatQuotient provides the following default mapping for the `result.data.incidentItems[]` JSON path:

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

The following keys are used to format the incident value:

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

The following keys are formatted into the title template:

```
.lastUpdateDate | Securonix Incident: {{violatorText}} ({{violatorSubText}}) [Priority: {{priority}}; Risk Score: {{riskscore}}; ID: {{incidentId}}] | N/A
```

## Securonix SNYPR - Top Threats

The Securonix SNYPR - Top Threat feed periodically pulls top threat reports from Securonix SNYPR 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 model 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 model 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  | N/A   |
| .Response.Docs[.Threat model name | Report Attribute   | Top Threat                           | N/A            | Privileged IT User-Sabotage  | N/A   |

The following keys are used to format the incident value:

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

## Securonix SNYPR - Top Violations

The Securonix SNYPR - Top Violations feed periodically pulls top violation reports from Securonix SNYPR 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   | N/A   |
| .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 incident value:

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

# 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 SNYPR - Incidents

| METRIC              | RESULT   |
|---------------------|----------|
| Run Time            | 1 minute |
| Incidents           | 3        |
| Incident Attributes | 45       |

## Securonix SNYPR - Top Threats

| METRIC            | RESULT   |
|-------------------|----------|
| Run Time          | 1 minute |
| Report            | 1        |
| Report Attributes | 32       |

## Securonix SNYPR - Top Violations

| METRIC            | RESULT   |
|-------------------|----------|
| Run Time          | 1 minute |
| Report            | 1        |
| Report Attributes | 118      |

---

# Change Log

- **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