ThreatQuotient



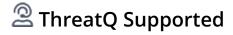
Securonix SNYPR CDF

Version 1.0.1

June 28, 2025

ThreatQuotient

20130 Lakeview Center Plaza Suite 400 Ashburn, VA 20147



Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893



Contents

Warning and Disclaimer	3
Support	
Integration Details	
Introduction	<i>6</i>
Prerequisites	7
Installation	
Configuration	<u>c</u>
Incidents Parameters	
Top Violations and Top Threats Parameters	10
ThreatQ Mapping	
Securonix SNYPR - Incidents	12
Securonix SNYPR - Top Threats	16
Securonix SNYPR - Top Violations	18
Average Feed Run	20
Securonix SNYPR - Incidents	20
Securonix SNYPR - Top Threats	20
Securonix SNYPR - Top Violations	21
Change Log	22



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@threatg.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 >= 5.12.1

Versions

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	Select the threat intelligence to be ingested into ThreatQ. Options include: Violator Text (default) (default) Violator Subtext Priority (default) Violator ID Reasons (default) Incident Type Entity (default) (default) Workflow Name Incident ID (default) (default) Securonix Link (default)		

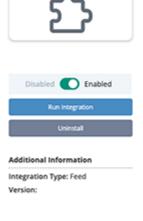


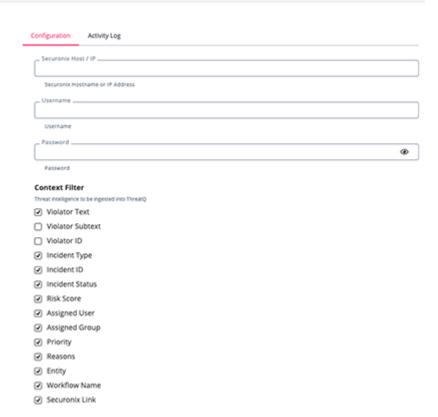
PARAMETER

DESCRIPTION

- Incident Status (default)
- Risk Score (default)
- Assigned User (default)
- Is Whitelisted (default)
- Is Watchlisted (default)

Securonix SNYPR - Incidents





Top Violations and Top Threats Parameters

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

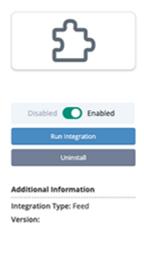


PARAMETER

DESCRIPTION

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

Securonix SNYPR - Top Threats





- 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 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
data.incidentItems[]. <see note=""></see>	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.incidentltems[].violatorText	Incident Attribute	Violator Text	N/A	Cyndi Converse	User-configurable
data.incidentltems[].violatorSubText	Incident Attribute	Violator Subtext	N/A	1096	User-configurable
data.incidentltems[].violatorld	Incident Attribute	Violator ID	N/A	96	User-configurable
data.incidentItems[].incidentType	Incident Attribute	Incident Type	N/A	RISK MODEL	User-configurable
data.incidentltems[].incidentld	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:// saaspocapp2t14wpt p.securonix.net/ Snypr/ configurableDashb oards/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	ls 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 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=""></see>	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=""></see>	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