ThreatQuotient

Securonix IOC Exports Guide

Version 1.0.0

April 05, 2023

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 © 2023 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.

Export Details

ThreatQuotient provides the following details for this export:

Current Guide Version	1.0.0
Support Tier	ThreatQ Supported

Introduction

Securonix IOC exports enable the dissemination of prioritized IOCs from ThreatQ to Securonix, to be used for log enrichment and policy alerts.

Creating the Export

The following section will detail how to create the exports in ThreatQ.

> See the Managing Exports topic for more details on ThreatQ exports.

1. Select the **Settings icon > Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Click **Add New Export**

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:

<table>
<tr><th>FIELD</th><th>VALUE</th></tr>
<tr><td><b>Type of information you would like to export?</b></td><td>Indicators</td></tr>
<tr><td><b>Output type</b></td><td>custom</td></tr>
<tr><td><b>Special Parameters</b></td><td><pre>indicator.type=IP Address&indicator.score>=3&indicator.
deleted=N&indicator.status=Active</pre>You will need to configure different exports per IOC type you’d want to export to Securonix. This means, changing the indicator.type special parameter above to match the corresponding IOC type.</td></tr>
<tr><td><b>Output Template</b></td><td><pre>#
tpi_ioc,tpi_risk,tpi_src_organization,tpi_description,tpi_malware,tpi_dt_firs
tseen {foreach $data as $indicator} {$indicator.value|json_encode},"{if
$indicator.score lte 3}Low{elseif $indicator.score lte 6}Medium{elseif
$indicator.score lte 9}High{elseif $indicator.score gt 9}Very High{/
if}","ThreatQ",{if $indicator.description}{$indicator.description|
json_encode}{else}""{/if},{if !empty($indicator.Malware)}
{$indicator.Malware[0].value}{else}""{/if},{$indicator.created_at|
json_encode} {/foreach}</pre></td></tr>
</table>

6. Click on **Save Settings** and enable the export via the On/Off toggle switch.
7. Click on the export URL with the data.

Example Output

tpi_ioc,tpi_risk,tpi_src_organization,tpi_description,tpi_malware,tpi_dt_firstseen

```
"13.84.134.105","Very High","ThreatQ","","","2021-04-20 21:14:26"
"13.92.233.22","Very High","ThreatQ","","","2021-04-20 21:14:26"
"52.171.135.15","Very High","ThreatQ","","","2021-04-20 21:14:28"
"3.134.125.175","Very High","ThreatQ","",njRAT,"2021-05-04 15:14:29"
"3.14.182.203","Very High","ThreatQ","",njRAT,"2021-05-04 15:14:29"
"67.209.195.198","Very High","ThreatQ","",QakBot,"2021-05-04 15:14:51"
"47.146.32.175","Very High","ThreatQ","",Emotet,"2021-05-05 15:14:41"
"79.134.225.7","Very High","ThreatQ","",AsyncRAT,"2021-05-06 15:14:28"
```

````
"3.22.15.135","Very High","ThreatQ","",njRAT,"2021-05-06 15:14:47"
"3.131.147.49","Very High","ThreatQ","",njRAT,"2021-05-06 15:14:47" ```
````

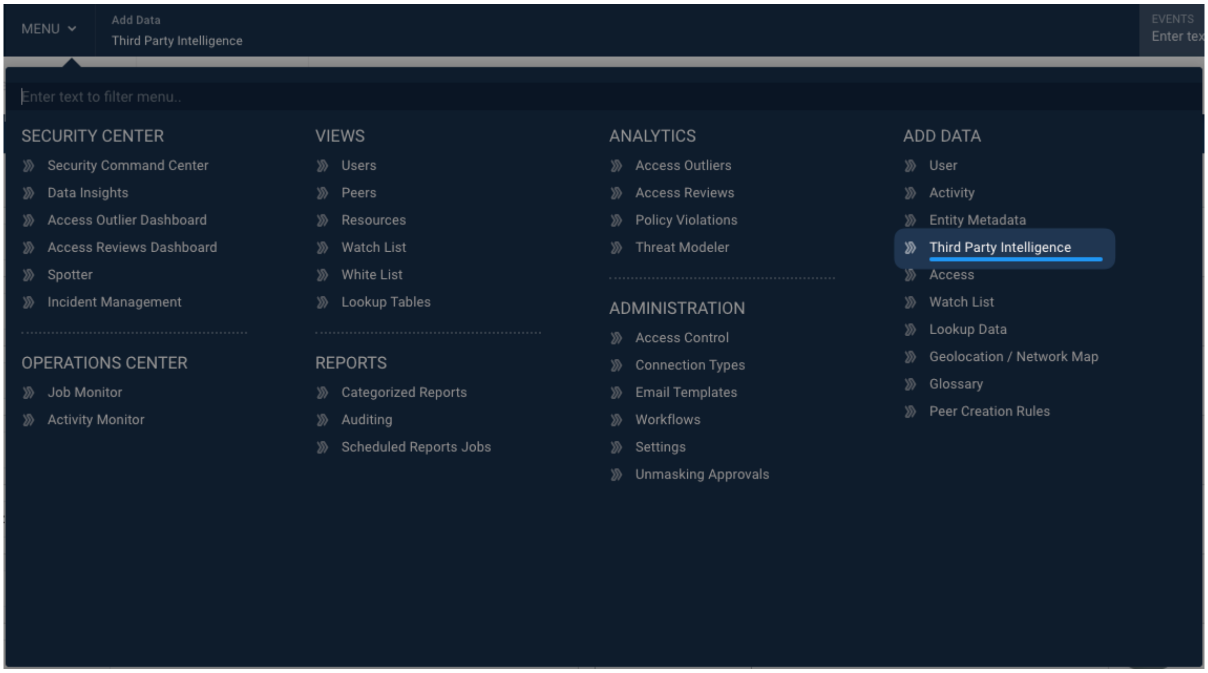
Configuring Imports into Securonix

The following section contains ThreatQ-specific instructions. You can view Securonix's guides on importing Third-Party Intelligence can be found at the links below.

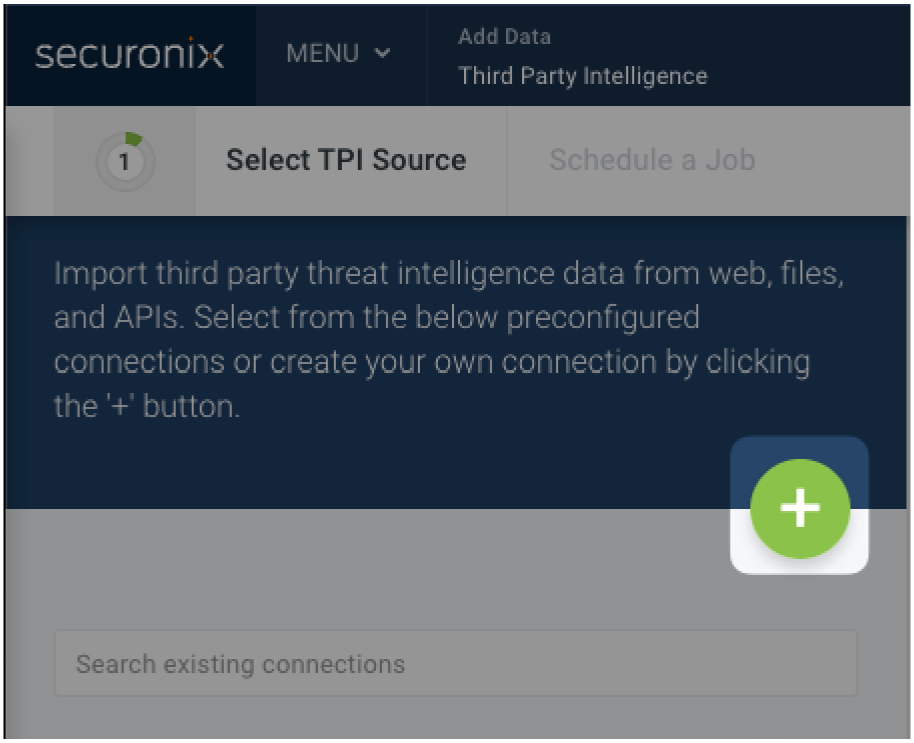
- Import Third-Party Intelligence | SNYPR 6.3.1 | Cloud
- Attributes by Field Group

Configuring a new TPI Source (Third-Party Intelligence)

1. Log into Securonix SNYPR.
2. Click on the **MENU** and navigate to **ADD DATA -> Third Party Intelligence**.



3. Click on the **+** button to create a new TPI Source.



Import third party threat intelligence data from web, files, and APIs. Select from the below preconfigured connections or create your own connection by clicking the '+' button.

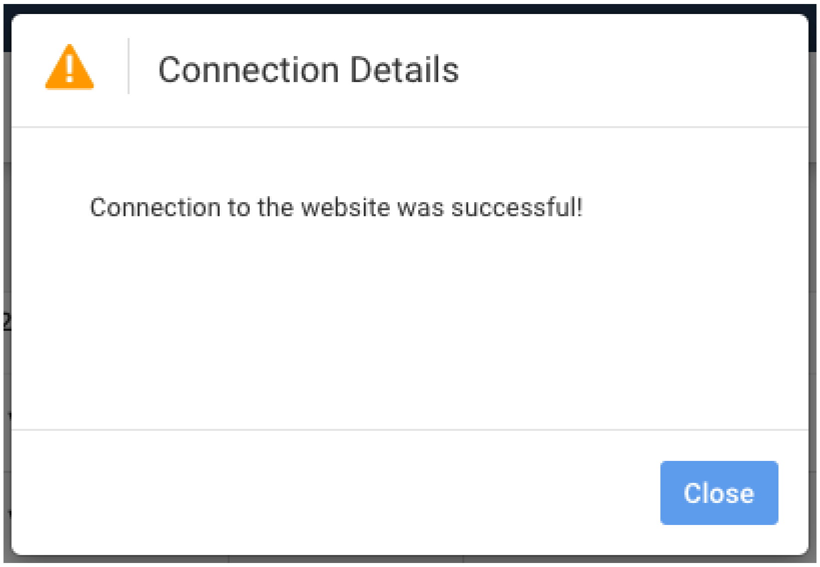
4. Enter the following values for the connection:

VALUE	DESCRIPTION
Connection Name	This can be any name you choose but you should be able to identify the export you are disseminating from ThreatQ. **Example**: ThreatQ_IP_Blacklist The name cannot contain any spaces.
Connection Method	Web
URL	Copy and paste the ThreatQ Export URL. Make sure to remove the limit parameter (i.e. limit=10) from the URL.

VALUE	DESCRIPTION
Filename	The filename can be any name you choose but you should be able to identify the export you are disseminating from ThreatQ. **Example**: threatq_ip_blacklist.csv This may be overwritten by Securonix after saving.
TPI Type	Update this field to type of IoC you are exporting from ThreatQ.
Parser Type	Delimited
Column Delimiter	,
Contains Column Identifier	No
Delete Old TPI Data	Yes
Exclude Header	Yes
Header Lines	1
Exclude Footer	No
Criticality	Select the Criticality to use.
Modify Criticality	Select either Yes or No.

5. Once the configuration has been completed, click the **Test Connection** button in Securonix.

Example of Successful Connection:

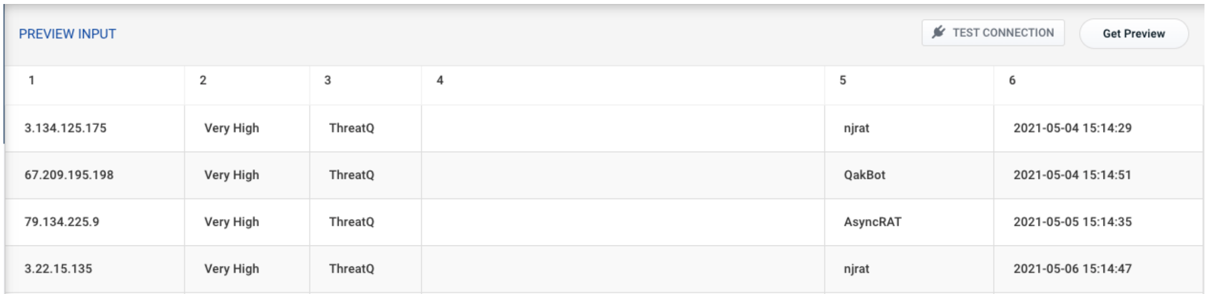


Connection Details

Connection to the website was successful!

6. Once the connection is successful, click on the **Get Preview** button to view a preview of the Export.

Preview Example:



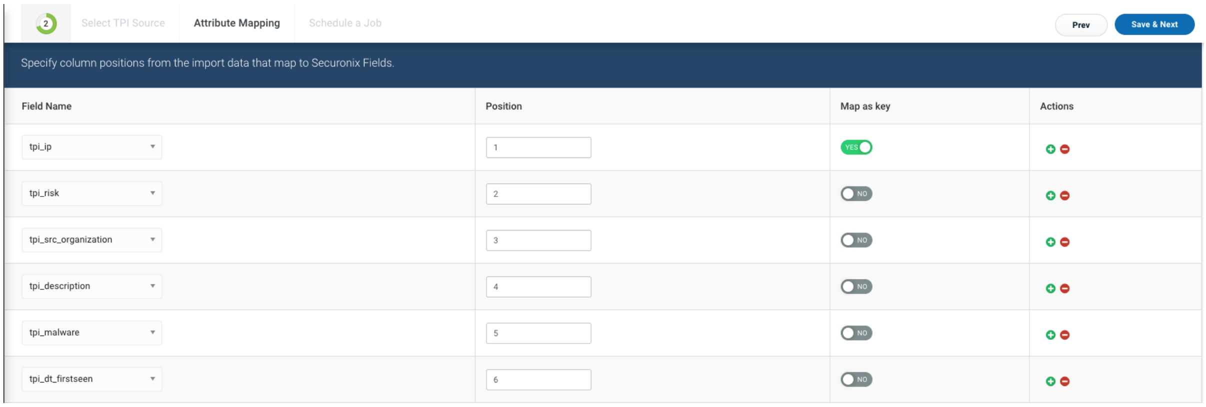
1	2	3	4	5	6
3.134.125.175	Very High	ThreatQ		njrat	2021-05-04 15:14:29
67.209.195.198	Very High	ThreatQ		QakBot	2021-05-04 15:14:51
79.134.225.9	Very High	ThreatQ		AsyncRAT	2021-05-05 15:14:35
3.22.15.135	Very High	ThreatQ		njrat	2021-05-06 15:14:47

> If the connection was unsuccessful, please make sure that there is a proper route for Securonix (cloud) to communicate with ThreatQ (on-prem or cloud-hosted).

7. Click on **Save & Next** if you are satisfied with preview.

Attribute Mapping

The Attribute Mapping page takes the column indexes and maps them to specific fields that Securonix understands. In the example below, the **tpi_ip** field has been selected to **Map as Key**.



Specify column positions from the import data that map to Securonix Fields.

Field Name	Position	Map as key	Actions
tpi_ip	1	YES	⊕ ⊖
tpi_risk	2	NO	⊕ ⊖
tpi_src_organization	3	NO	⊕ ⊖
tpi_description	4	NO	⊕ ⊖
tpi_malware	5	NO	⊕ ⊖
tpi_dt_firstseen	6	NO	⊕ ⊖

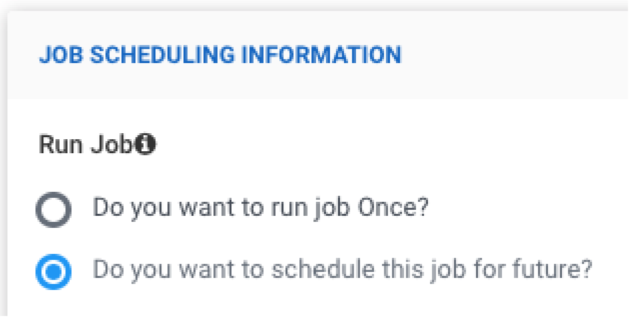
There are other IoCs that can be selected, instead of the tpi_ip in the example above, depending on the type of IoCs that you are exporting. Some examples of these types include (but are not limited to):

- tpi_hash
- tpi_domain
- tpi_url
- tpi_vulnerability
- tpi_risk
- tpi_src_organization
- tpi_description
- tpi_malware
- tpi_dt_firstseen

Scheduling a Job

To schedule futures jobs:

1. Navigate to the Job Scheduling Information section.
2. Select the radio box for the **Do you want to schedule this for for future** option.



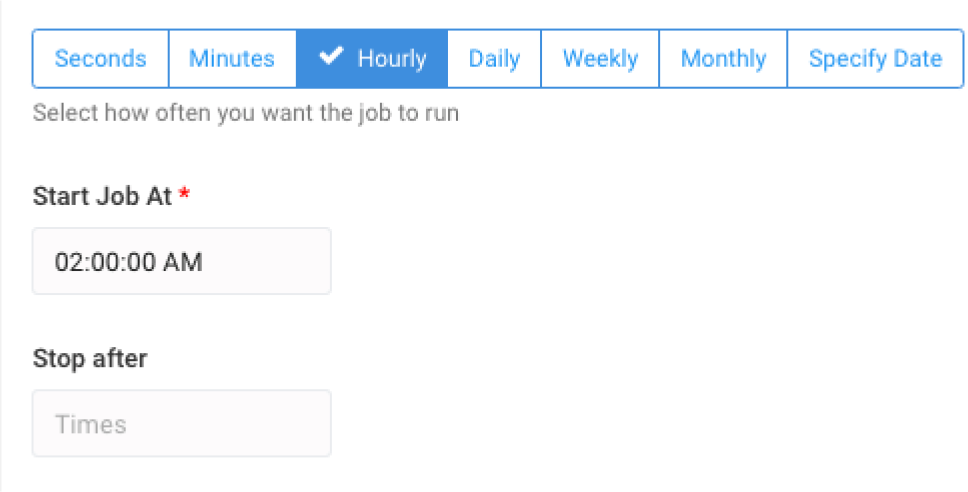
JOB SCHEDULING INFORMATION

Run Job

○ Do you want to run job Once?

● Do you want to schedule this job for future?

3. Use the UI provided to select how often to run the job.



Seconds | Minutes | ✓ Hourly | Daily | Weekly | Monthly | Specify Date

Select how often you want the job to run

Start Job At *

02:00:00 AM

Stop after

Times

> ThreatQuotient recommends running the job hourly.

4. Click on **Save**.

Change Log

- **Version 1.0.0**
  - Initial release