

ThreatQuotient



Infoblox SOC Insights CDF

Version 1.1.0

May 13, 2024

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 3
- Support 4
- Integration Details..... 5
- Introduction 6
- Prerequisites 7
- Installation..... 8
- Configuration 9
- ThreatQ Mapping..... 11
 - Infoblox SOC Insights 11
 - Get Indicators (Supplemental)..... 13
 - Get Assets (Supplemental) 14
 - Get Events (Supplemental)..... 15
- Average Feed Run..... 16
- Change Log 17

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 © 2024 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	1.1.0
Compatible with ThreatQ Versions	>= 5.22.0
Support Tier	ThreatQ Supported

Introduction

The Infoblox SOC Insights CDF ingest Incidents from Infoblox and its related data.

The integration provides the following feeds:

- **Infoblox SOC Insights** - retrieves the IDs of Infoblox incidents.
- **Get Indicators (Supplemental)** - retrieves all the indicators for each Incident.
- **Get Assets (Supplemental)** - retrieves all the assets for each Incident.
- **Get Events (Supplemental)** - retrieves all the events for each Incident.

The integration ingests the following system objects:

- Assets
- Events
- Incidents
- Indicators

Prerequisites

The following is required by the integration:

- An Infoblox Token.

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.

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:

PARAMETER	DESCRIPTION
Token	Enter your InfoBlox Token.
Status	Select the Status to receive. Options include Open and Closed . This field is set to Open by default.
Priority	Select the Priority to receive. Options include: <ul style="list-style-type: none"> ◦ High ◦ Medium ◦ Low ◦ All (default)

< InfoBlox - SOC Insights



Disabled ☐ Enabled ☒

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

Token 

Status
Active

Priority
All

Set indicator status to...
Active

Run Frequency

Every 24 Hours

☒ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Save

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

Infoblox SOC Insights

The Infoblox SOC Insights retrieves the ID of an incident based on the user's configuration settings.

GET <https://csp.infoblox.com/api/v1/insights>

Sample Response:

```
{
  "insightList": [
    {
      "tClass": "TI-CONFIGURATIONISSUE",
      "tFamily": "OPENRESOLVER",
      "insightId": "ae414970-8878-42f5-9192-6c3319254b3a",
      "feedSource": "Insight Detection Framework",
      "startedAt": "2024-03-27T23:00:00Z",
      "threatType": "Open Resolver",
      "status": "Active",
      "persistentDate": "2024-03-27T15:00:00Z",
      "numEvents": "1472",
      "mostRecentAt": "2024-05-02T11:42:06Z",
      "eventsNotBlockedCount": "1472",
      "dateChanged": "0001-01-01T00:00:00Z",
      "priorityText": "MEDIUM"
    }
  ]
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
insightList[].feedSource + insightList[].insightId	Incident.Value	N/A	insightList[].startedAt	Insight Detection Framework - ae414970-8878-42f5-9192-6c3319254b3a	We concatenate the 2 values so the Incident value is unique
insightList[].priorityText	Incident.Attribute	Priority	insightList[].startedAt	MEDIUM	Attribute updated if already exists
insightList[].status	Incident.Attribute	Status	insightList[].startedAt	Active	Attribute updated if already exists
insightList[].threatType	Incident.Attribute	Threat Type	insightList[].startedAt	Open Resolver	N/A
insightList[].feedSource	Incident.Attribute	Feed Source	insightList[].startedAt	Insight Detection Framework	N/A
insightList[].tFamily	Incident.Attribute	Family	insightList[].startedAt	OPENRESOLVER	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
insightList[].tcClass	Incident.Attribute	Class	insightList[].startedAt	TI-CONFIGURATIONISSUE	N/A
indicators[].indicator	Related Indicator.Value	FQDN	indicators[].timeMin	shadowserver.org	N/A
indicators[].confidence	Related Indicator.Attribute	Confidence Level	indicators[].timeMin	3	Attribute updated if already exists
indicators[].threatLevelMax	Related Indicator.Attribute	Threat Level Max	indicators[].timeMin	1	Attribute updated if already exists
indicators[].action	Related Indicator.Attribute	Action	indicators[].timeMin	Not Blocked	N/A
assets[].qip	Related Asset.Value	N/A	assets[].timeMin	107.178.234.206	N/A
assets[].threatIndicatorDistinctCount	Related Asset.Attribute	Threat Indicator Distinct Count	assets[].timeMin	1	Attribute updated if already exists
assets[].threatLevelMax	Related Asset.Attribute	Threat Level Max	assets[].timeMin	2	Attribute updated if already exists
events[].class + events[].threatFamily + events[].property	Related Event.Value	Incident	events[].detected	TI-CONFIGURATIONISSUE - OPENRESOLVER - dnsscan.shadowserver.org	We concatenate the 3 values so we can create the event
events[].confidenceLevel	Related Event.Attribute	Confidence Level	events[].detected	High	Attribute updated if already exists
events[].action	Related Event.Attribute	Action	events[].detected	Allow - No Log	N/A
events[].policy	Related Event.Attribute	Policy	events[].detected	DoH	N/A
events[].class	Related Event.Attribute	Class	events[].detected	TI-CONFIGURATIONISSUE	N/A
events[].threatFamily	Related Event.Attribute	Threat Family	events[].detected	OPENRESOLVER	N/A
events[].threatLevel	Related Event.Attribute	Threat Level	events[].detected	Low	Attribute updated if already exists
events[].deviceIp	Related Event.Indicator	IP Address	events[].detected	107.178.235.14	N/A

Get Indicators (Supplemental)

The Get Indicators supplemental feed retrieves all the indicators for each Incident.

GET <https://csp.infoblox.com/api/v1/insights/{{insightId}}/indicators>

Sample Response:

```
{
  "indicators": [
    {
      "action": "Not Blocked",
      "confidence": "3",
      "count": 703,
      "threatLevelMax": "1",
      "indicator": "shadowserver.org",
      "timeMax": "2024-05-02T11:00:00.000",
      "timeMin": "2024-04-02T13:00:00.000"
    },
    {
      "action": "Not Blocked",
      "confidence": "3",
      "count": 980,
      "threatLevelMax": "1",
      "indicator": "parrotdns.com",
      "timeMax": "2024-04-29T11:00:00.000",
      "timeMin": "2024-04-02T13:00:00.000"
    }
  ]
}
```

Get Assets (Supplemental)

The Get Assets supplemental feed retrieves all the assets for each Incident.

GET <https://csp.infoblox.com/api/v1/insights/{{insightId}}/assets>

Sample Response:

```
{
  "assets": [
    {
      "count": 355,
      "qip": "107.178.234.206",
      "threatLevelMax": "2",
      "threatIndicatorDistinctCount": "1",
      "timeMax": "2024-05-01T23:00:00.000",
      "timeMin": "2024-05-01T23:00:00.000"
    },
    {
      "count": 500,
      "qip": "107.178.234.197",
      "threatLevelMax": "2",
      "threatIndicatorDistinctCount": "2",
      "timeMax": "2024-05-01T15:00:00.000",
      "timeMin": "2024-05-01T15:00:00.000"
    },
    {
      "count": 765,
      "qip": "107.178.235.12",
      "threatLevelMax": "2",
      "threatIndicatorDistinctCount": "2",
      "timeMax": "2024-05-01T15:00:00.000",
      "timeMin": "2024-05-01T15:00:00.000"
    },
    {
      "count": 865921,
      "qip": "42.42.42.2",
      "threatLevelMax": "2",
      "threatIndicatorDistinctCount": "163",
      "timeMax": "2024-04-29T12:00:00.000",
      "timeMin": "2024-04-02T10:00:00.000"
    }
  ]
}
```

Get Events (Supplemental)

The Get Events supplemental feed retrieves all the events for each Incident.

GET <https://csp.infoblox.com/api/v1/insights/{{insightId}}/events>

Sample Response:

```
{
  "events": [
    {
      "confidenceLevel": "High",
      "source": "unknown",
      "action": "Allow - No Log",
      "policy": "DoH",
      "deviceIp": "107.178.235.14",
      "query": "dnsscan.shadowserver.org",
      "queryType": "A",
      "class": "TI-CONFIGURATIONISSUE",
      "threatFamily": "OPENRESOLVER",
      "detected": "2024-05-02 11:42:06 +0000 UTC",
      "property": "dnsscan.shadowserver.org",
      "user": "unknown",
      "threatLevel": "Low"
    },
    {
      "confidenceLevel": "High",
      "source": "unknown",
      "action": "Allow - No Log",
      "policy": "DoH",
      "deviceIp": "107.178.234.206",
      "query": "dnsscan.shadowserver.org",
      "queryType": "A",
      "class": "TI-CONFIGURATIONISSUE",
      "threatFamily": "OPENRESOLVER",
      "detected": "2024-05-01 23:42:09 +0000 UTC",
      "property": "dnsscan.shadowserver.org",
      "user": "unknown",
      "threatLevel": "Low"
    }
  ]
}
```

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.

METRIC	RESULT
Run Time	1 minute
Assets	4
Asset Attributes	9
Events	352
Event Attributes	2,112
Incidents	2
Incident Attributes	12
Indicators	6
Indicator Attributes	6

Change Log

- **Version 1.1.0**
 - Added three new supplemental endpoints: **Get Indicators**, **Get Assets**, **Get Events**.
 - Removed deprecated **Get Details** supplemental endpoint.
 - The integration now ingests Event type objects in addition to indicators, incidents, and assets.
- **Version 1.0.0**
 - Initial release