ThreatQuotient

SecureWorks AttackerDB CDF User Guide

Version 1.0.0

October 18, 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.

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	1.0.0
Compatible with ThreatQ Versions	>= 4.21.1
Support Tier	ThreatQ Supported

Introduction

The SecureWorks Attacker DB Connector installs two feeds and ingests threat intelligence data from the Secureworks Attacker Database. The two feeds installed are:

- SecureWorks AttackerDB Domain
- SecureWorks AttackerDB IP

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 parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
SecureWorks Token	Your SecureWorks token.

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

SecureWorks Attacker DB IP

Sample Response:

```
"WatchList","HostAddress","ReasonAdded","MemberSince","Latitude","Longitude","C
ountryCode","Location"
"CTU IP Coal Blacklist","23.227.197.130","Potential Kovter Trojan Variant POST
Outbound","2018-03-17T06:37:24Z","41.8466","-87.7172","US","Chicago, United
States"
"CTU IP Coal Blacklist","79.175.102.12","TrickBot Malware SSL Certificate -
Inbound","2018-04-19T06:37:07Z","44.833","20.5","RS","Belgrade, Serbia"
"CTU IP Coal Blacklist","104.243.42.22","Potential Kovter Trojan Variant POST
Outbound","2018-04-14T06:46:09Z","40.5527","-74.4582","US","Piscataway, United
States"
"CTU IP Coal Blacklist","108.61.18.118","Potential Kovter Trojan Variant POST
Outbound","2018-04-19T06:37:07Z","40.5527","-74.4582","US","Piscataway, United
States"
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
(first token)	Attribute	WatchList	CTU IP Coal Blacklist
2 (second token)	Indicator	HostAddress	23.227.197.130
3 (third token)	Attribute	ReasonAdded	TrickBot Malware SSL Certificate - Inbound
4 (forth token)	Indicator	MemberSince	2018-03-17T06:37:24Z
5 (fifth token)	Attribute	Latitude	41.8466
6 (sixth token)	Attribute Attribute	Longitude	-87.7172
7 (seventh token)	Attribute	CountryCode	US
8 (eighth token)	Attribute	Location	Chicago, United States

SecureWorks Attacker DB Domain

Sample Response:

```
"WatchList","HostAddress","ReasonAdded","MemberSince"
"CTU Domain Coal Blacklist","blacklist-test.secureworks.com","Test - Dell
SecureWorks AttackerDB Customer Test Event (non-
malicious)","2017-06-14T20:26:01Z",
"CTU Domain Coal Blacklist","differentia.ru","Gamarue  Andromeda Trojan Phone
Home","2018-02-17T05:30:10Z",
"CTU Domain Coal Blacklist","differentia.ru","Gamarue Andromeda Trojan Phone
Home","2018-02-17T05:30:10Z",
"CTU Domain Coal Blacklist","disorderstatus.ru","Gamarue  Andromeda Trojan
Phone Home","2018-02-17T05:30:10Z",
"CTU Domain Coal Blacklist","disorderstatus.ru","Gamarue Andromeda Trojan Phone
Home","2018-02-17T05:30:10Z",
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
1 (first token)	Attribute	WatchList	CTU IP Coal Blacklist
2 (second token)	Indicator	HostAddress	blacklist-test.secureworks.com
3 (third token)	Attribute	ReasonAdded	Gamarue Andromeda Trojan Phone Home
4 (forth token)	Indicator	MemberSince	2018-02-17T05:30:10Z

Change Log

- **Version 1.0.0**
  - Initial release