IBM® QRadar® App for ThreatConnect® User Guide

Software Version 3.0

Integration Guide

March 9, 2023

30032-06 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 I F: 703.229.4489
www.ThreatConnect.com

Table of Contents

Overview

The IBM QRadar App for ThreatConnect is designed to upload Indicators from ThreatConnect to QRadar reference sets. Several filters are available to narrow the scope of Indicators retrieved from ThreatConnect, including Threat Rating, Confidence Rating, owner, Indicator type, and date of last modification. Once uploaded to QRadar, Indicators can be used to define filters and rules.

The QRadar integration operates in two modes: Indicator upload and Indicator deprecation. In Indicator upload, Indicators are uploaded to a QRadar reference set. In Indicator deprecation, Indicators are deleted from a QRadar reference set if they have been deprecated in ThreatConnect (i.e., they no longer meet the filtering criteria for the Job). Note that this configuration means that two Jobs need to be defined for every set of Indicators synced with QRadar.

This App operates in the ThreatConnect environment, with information flow running from ThreatConnect to QRadar. It is complementary to the ThreatConnect App for IBM QRadar, which operates in the QRadar environment, providing instant Indicator enrichment in QRadar from data in ThreatConnect and allowing users to look up and create Indicators or report false positives to ThreatConnect from within QRadar. See *ThreatConnect App for IBM QRadar User Guide* for more information.

Dependencies

ThreatConnect Dependencies

- Active ThreatConnect Application Programming Interface (API) key

Note: All ThreatConnect dependencies will be provided by default to subscribing ThreatConnect Cloud customers. Customers on Dedicated Cloud and On-Premises instances can enable these settings on the **Account Settings** screen within their ThreatConnect instance.

QRadar Dependencies

- Active IBM QRadar user account with System Administrator and API permissions

Configuration Parameters

Parameter Definitions

The parameters defined in Table 1 apply to the configuration parameters during the Job-creation process.

Table 1

Name	Description	Required?
API User	The ThreatConnect API user account.	Yes
QRadar API URL	The QRadar hostname or IP address.	Yes
QRadar API Username	The QRadar username.	No
QRadar API Password	The QRadar password.	No
QRadar API Authorization Token	The QRadar authorization token (in lieu of a QRadar username and password).	No
Verify SSL Cert	Specifies whether to verify the API host's QRadar SSL certificate during the connection. The default value is **False** (i.e., the checkbox is not selected).	No
Built-In Reference Data	The built-in QRadar reference set into which ThreatConnect Indicators will be imported. Accepted values include the following: • Phishing Senders • Phishing Subjects • Phishing URLs • Phishing IPs • Spam Senders	No

	- Malware Senders - Malware URLs - Malware Hostnames - Malware IPs - Malicious URLs - Botnet IPs - Botnet C&C IPs - Anonymizer IPs - Malware Hashes MD5 - Malware Hashes SHA - Rogue Process Names	
QRadar Reference Set	The custom QRadar reference set into which ThreatConnect Indicators will be imported.	No
Fallback QRadar Reference Type	The QRadar reference set type to create if the QRadar reference set doesn't exist. The default value is **ALNIC**.	Yes
QRadar Time to Live	The QRadar time to live interval (e.g., "1 month" or "5 minutes"). The default value is **1 month**.	No
Add Metadata to Reference Table	Specifies whether metadata (i.e., Confidence Rating, Threat Rating, ThreatAssess score, owner, creation date, and the date when the App last ran) should be added to the QRadar reference table. **Warning**: Adding metadata to the QRadar reference table requires several API calls and may cause the App to run slowly.	No

ThreatConnect Owners	The ThreatConnect owner whose Indicators will be sent to IBM QRadar. **Note**: Only one owner may be selected. To run this App for more than one owner, a separate Job must be set up for each owner.	Yes
ThreatConnect Indicator Types	The type(s) of Indicators that will be sent to IBM QRadar. Accepted values include the following: - Address - Email Address - File - Host - URL	No
Last Run	The last time the App ran. Data modified since this date will be included on the first run. Thereafter, the date will be automatically updated each time the job successfully completes. The default value is **30 days ago**.	No
TQL	A custom ThreatConnect Query Language (TQL) query for filtering Indicators. If using this parameter, do not use any other filter-based parameters (**ThreatConnect Owners**, **Indicator Types**, **Include Tags**, **Exclude Tags**, **Minimum ThreatAssess Score**, **Minimum Threat Rating**, **Minimum Confidence Rating**, and **Maximum False Positive Count**), as doing so will cause the App to error out.	No

Include Tags	The Tag(s) that Indicators must include in order to be sent to IBM QRadar. Indicators must include **at least one** of the specified Tags in order to be sent.	No
Exclude Tags	The Tag(s) that Indicators must exclude in order to be sent to IBM QRadar. Indicators that include **any** of the specified Tags will not be sent.	No
Minimum ThreatAssess Score	The minimum ThreatAssess score that Indicators must have in order to be sent to IBM QRadar.	No
Minimum Threat Rating	The minimum Threat Rating that Indicators must have in order to be sent to IBM QRadar.	No
Minimum Confidence Rating	The minimum Confidence Rating that Indicators must have in order to be sent to IBM QRadar.	No
Maximum False Positive Count	The maximum number of false positives that Indicators can have in order to be sent to IBM QRadar. When used, only Indicators with a false positive count less than or equal to the specified value will be sent.	
Logging Level	Determines the verbosity of the logging output for the application.	No

QRadar Configuration

When configuring a QRadar integration Job, the filtering parameters should be used to narrow the scope of Indicators retrieved as much as possible. Note that filtering parameters are combined such that the union of all filters defines the set of Indicators selected. The API has a limit of 5,000 Indicators for each QRadar integration Job. Each time the Indicator upload Job runs, it will consider only Indicators modified or created since the last time the Job ran.

To define the Indicator deprecation Job, configure the parameters with the same values as for the Indicator upload Job, but enable the **deprecation** flag. The Indicator deprecation Job does not have to be on the same schedule or interval as the Indicator upload Job. In fact, performance improves when the Jobs are staggered such that there are roughly two Indicator upload Jobs for each deprecation Job.