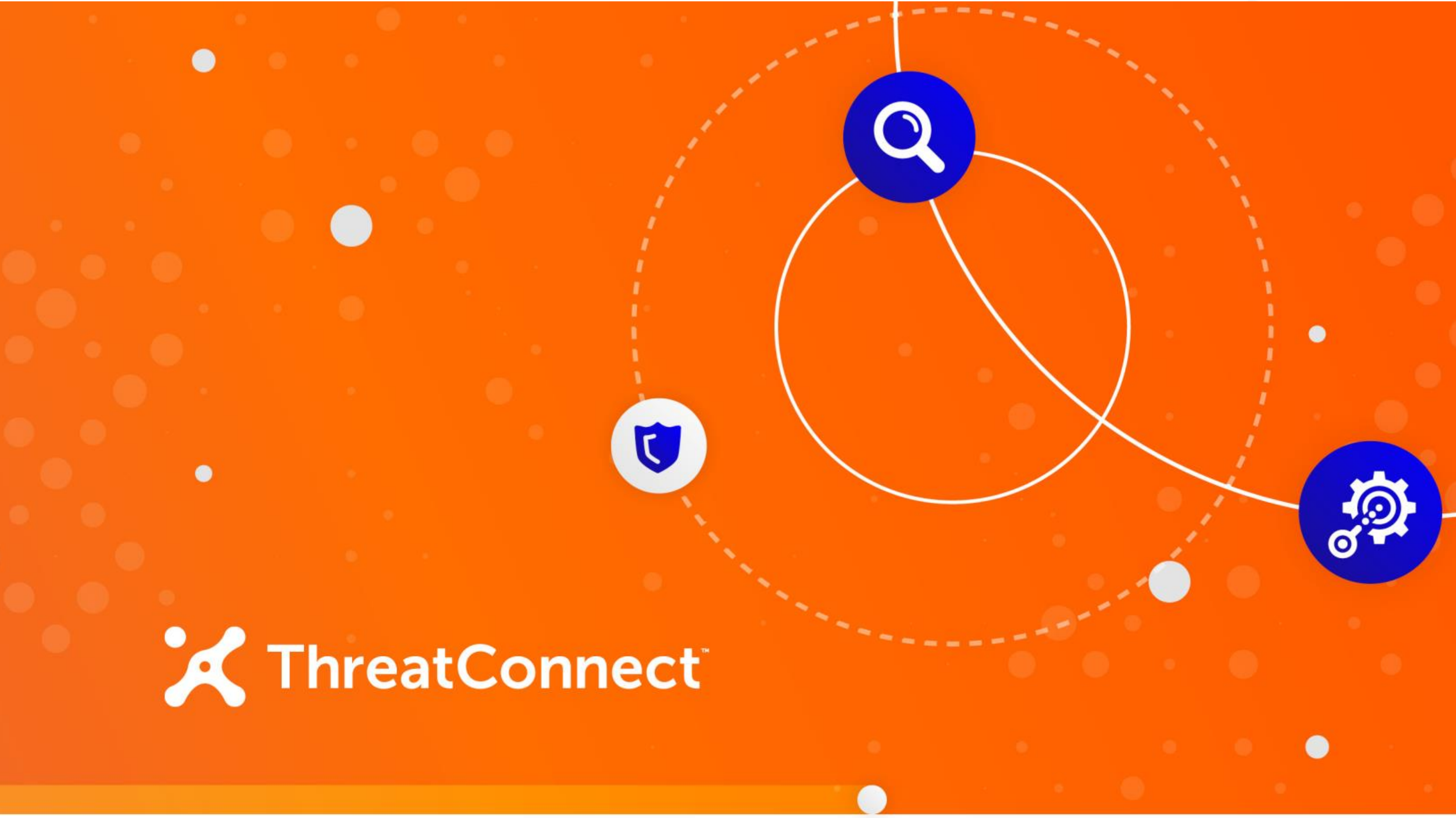


ThreatConnect® App for IBM® QRadar®

User Guide

SOFTWARE VERSION 2.0

SEPTEMBER 30, 2021

30043-02 EN Rev. A

TABLE OF CONTENTS

OVERVIEW

The ThreatConnect app for IBM QRadar aggregates logs from IBM QRadar and combines them with threat intelligence in the ThreatConnect platform, enabling 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. It is built on the QRadar GUI app framework and can be installed directly from within the IBM Security App Exchange. General information about the app can be found at https://exchange.xforce.ibmcloud.com/hub/extension/bd7c346432082b104374eba1391837de.

This app operates in the QRadar environment, with information flow running from QRadar to ThreatConnect. It is complementary to the IBM QRadar app for ThreatConnect, which operates in the ThreatConnect environment, uploading Indicators from ThreatConnect to QRadar reference sets. See *IBM QRadar App for ThreatConnect User Guide* for more information.

Software Version 2.0 has identical functionality to Software Version 1.0, but has been revised to function with Python® 3 and the updated QRadar application environment.

DEPENDENCIES

ThreatConnect Dependencies

NOTE: All ThreatConnect dependencies will be provided by default to subscribing ThreatConnect Cloud customers. Private Instance customers can enable these settings during configuration on the *Account Settings* ***screen within their Private Instance of ThreatConnect.***

- ThreatConnect version 6.0 or newer
- ThreatConnect Application Programming Interface (API) URL
- ThreatConnect API ID
- ThreatConnect API Secret Key
- ThreatConnect API Owner

QRadar Dependencies

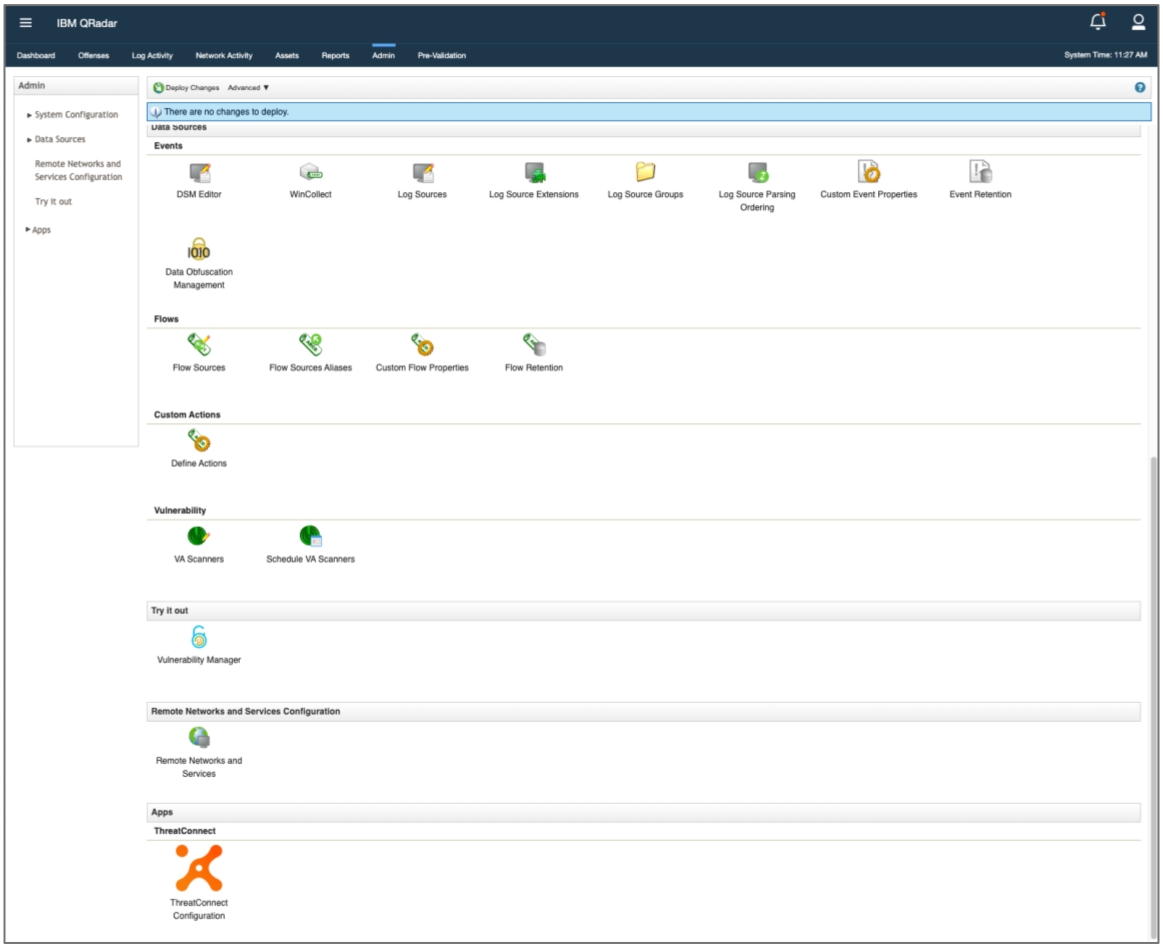
- QRadar version 7.4.2 or newer
- Connectivity between QRadar and ThreatConnect

INSTALLATION

The app is offered through the QRadar App Exchange. It can be installed from Extension Management or manually with a .zip file. Upload, installation, and management instructions can be found at https://www.ibm.com/docs/en/qsip/7.4?topic=content-installing-extensions-by-using-extensions-management.

CONFIGURATION

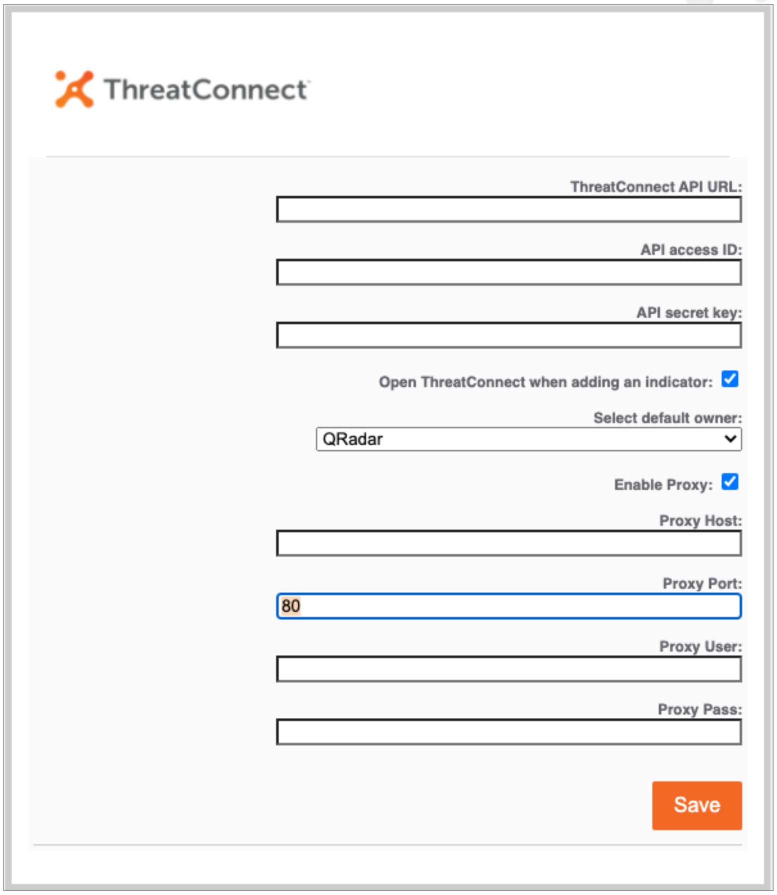
1. Log into QRadar, and select the **Admin** tab from the default screen.
2. Scroll down to the bottom of the screen, and double-click the **ThreatConnect Configuration** icon under the **Apps** section (Figure 1).



There are no changes to deploy.

Figure 1

3. The ThreatConnect login window will be displayed (Figure 2).



ThreatConnect

ThreatConnect API URL:

API access ID:

API secret key:

Open ThreatConnect when adding an indicator: ☑

Select default owner: QRadar

Enable Proxy: ☑

Proxy Host:

Proxy Port: 80

Proxy User:

Proxy Pass:

Figure 2

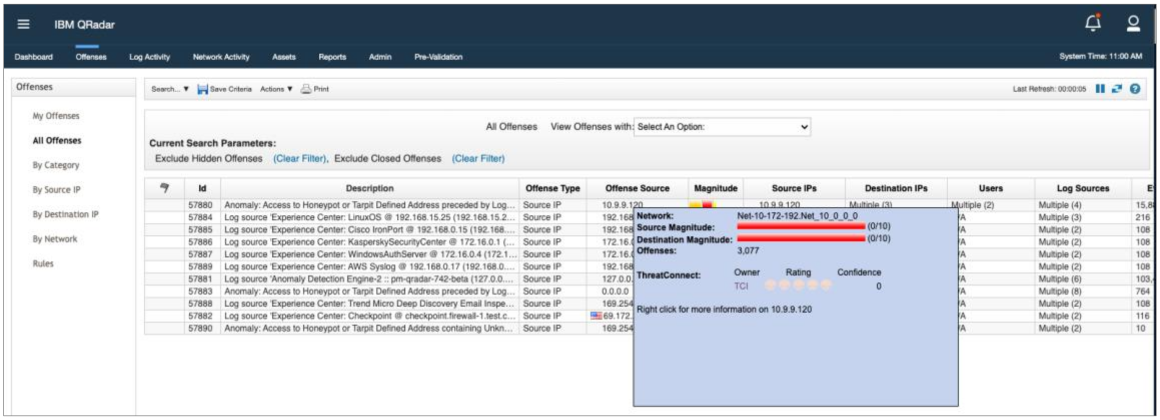
- **ThreatConnect API URL**: Enter a URL ending in **/api**, such as **https://threatconnect.company.com/api**.
- **API access ID**: Enter the API access ID that was created by your ThreatConnect administrator.
- **API secret key**: Enter the API secret key corresponding to the API access ID.
- **Open ThreatConnect when adding an indicator**: Select this checkbox to have ThreatConnect open when an Indicator is added.
- **Select default owner**: Select the default owner in ThreatConnect. The owner will usually be your Organization.
- **Enable Proxy**: Select this checkbox to enter proxy configuration parameters.
  - **Proxy Host**: Enter the name of the proxy host.
  - **Proxy Port**: Enter the proxy port.
  - **Proxy User**: Enter the proxy username (optional).
  - **Proxy Pass**: Enter the proxy password (optional).

4. Click the **Save** button to complete the login configuration.

USING THE APP

The app enables hover-over metadata enrichment for Host, URL, and Address Indicators in QRadar via API calls to ThreatConnect.

1. To view the metadata for a particular Indicator, locate an Indicator in the **Dashboard**, **Offenses**, **Log Activity,** or **Assets** tab and hover the cursor over it (Figure 3).



All Offenses View Offenses with: Select An Option:

Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	E
	57880	Anomaly: Access to Honeypot or Tarpit Defined Address preceded by Log...	Source IP	10.9.9.120		10.9.9.120	Multiple (3)	Multiple (2)	Multiple (4)	15,8
	57884	Log source 'Experience Center: LinuxOS @ 192.168.15.25 (192.168.15.2...	Source IP	192.168				A	Multiple (3)	216
	57885	Log source 'Experience Center: Cisco IronPort @ 192.168.0.15 (192.168....	Source IP	192.168				A	Multiple (2)	108
	57886	Log source 'Experience Center: KasperskySecurityCenter @ 172.16.0.1 (...	Source IP	172.16.				A	Multiple (2)	108
	57887	Log source 'Experience Center: WindowsAuthServer @ 172.16.0.4 (172.1...	Source IP	172.16.				A	Multiple (2)	108
	57889	Log source 'Experience Center: AWS Syslog @ 192.168.0.17 (192.168.0....	Source IP	192.168				A	Multiple (2)	108
	57881	Log source 'Anomaly Detection Engine-2 :: pm-qradar-742-beta (127.0.0....	Source IP	127.0.0.				A	Multiple (6)	103,
	57883	Anomaly: Access to Honeypot or Tarpit Defined Address preceded by Log...	Source IP	0.0.0.0				A	Multiple (8)	764
	57888	Log source 'Experience Center: Trend Micro Deep Discovery Email Inspe...	Source IP	169.254				A	Multiple (2)	108
	57882	Log source 'Experience Center: Checkpoint @ checkpoint.firewall-1.test.c...	Source IP	69.172.				A	Multiple (2)	116
	57890	Anomaly: Access to Honeypot or Tarpit Defined Address containing Unkn...	Source IP	169.254				A	Multiple (2)	10

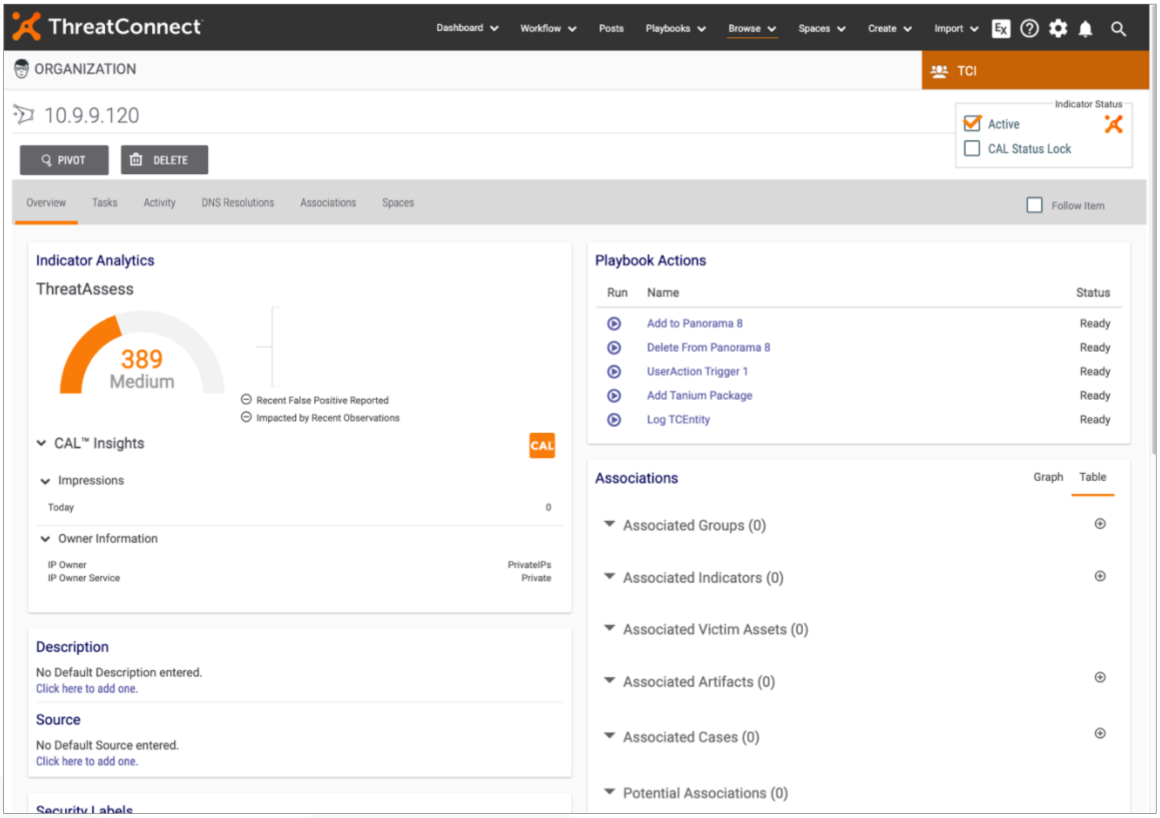
Network: Net-10-172-192.Net_10_0_0_0
Source Magnitude: (0/10)
Destination Magnitude: (0/10)
Offenses: 3,077

ThreatConnect:	Owner	Rating	Confidence
	TCI	●●●●●	0

Right click for more information on 10.9.9.120

Figure 3

2. To view the Details screen for the Indicator in ThreatConnect, click on the Owner. The Indicator's **Details** screen will be displayed in a new window (Figure 4).



10.9.9.120

Indicator Status
☑ Active
☐ CAL Status Lock

Indicator Analytics

ThreatAssess

389
Medium

⊖ Recent False Positive Reported
⊖ Impacted by Recent Observations

CAL™ Insights

Impressions

Today 0

Owner Information

IP Owner PrivateIPs
IP Owner Service Private

Description

No Default Description entered.
Click here to add one.

Source

No Default Source entered.
Click here to add one.

Security Labels

Playbook Actions

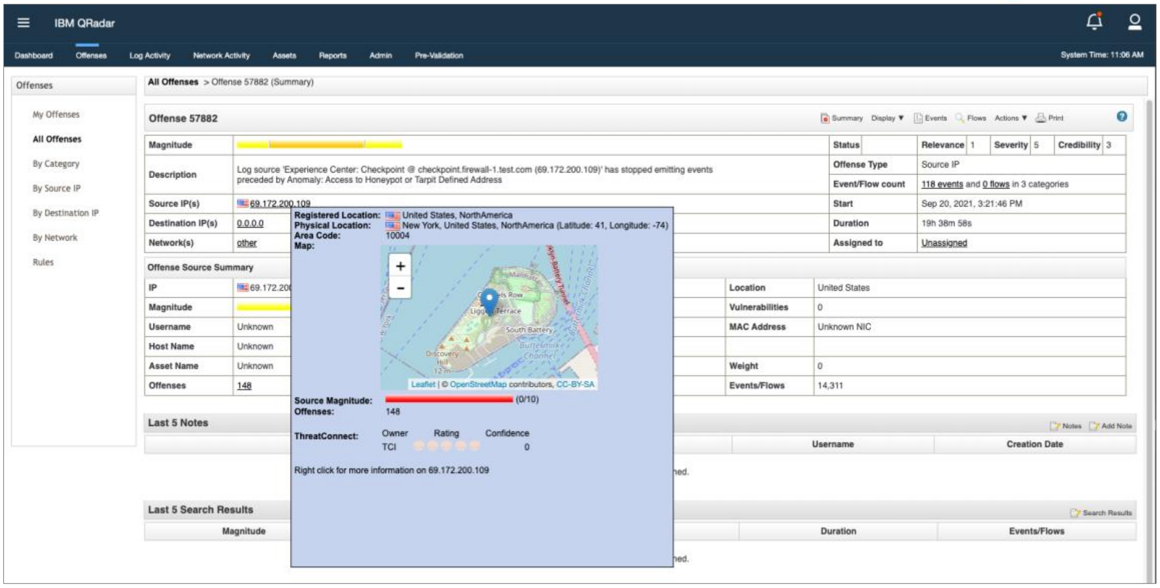
Run	Name	Status
⦿	Add to Panorama 8	Ready
⦿	Delete From Panorama 8	Ready
⦿	UserAction Trigger 1	Ready
⦿	Add Tanium Package	Ready
⦿	Log TCEntity	Ready

Associations

- Associated Groups (0)
- Associated Indicators (0)
- Associated Victim Assets (0)
- Associated Artifacts (0)
- Associated Cases (0)
- Potential Associations (0)

Figure 4

3. Hover-over metadata enrichment is also available in the detail view of an Offense, which may be accessed by clicking on a given **Offense Source** in QRadar (Figure 5).



Offense 57882

Magnitude		Status	
Description	Log source 'Experience Center: Checkpoint @ checkpoint.firewall-1.test.com (69.172.200.109)' has stopped emitting events preceded by Anomaly: Access to Honeypot or Tarpit Defined Address	Relevance 1 · Severity 5 · Credibility 3	
		Offense Type	Source IP
		Event/Flow count	118 events and 0 flows in 3 categories
Source IP(s)	69.172.200.109	Start	Sep 20, 2021, 3:21:46 PM
Destination IP(s)	0.0.0.0	Duration	19h 38m 58s
Network(s)	other	Assigned to	Unassigned

Registered Location: United States, NorthAmerica
Physical Location: New York, United States, NorthAmerica (Latitude: 41, Longitude: -74)
Area Code: 10004
Map:
Source Magnitude: (0/10)
Offenses: 148

ThreatConnect:	Owner	Rating	Confidence
	TCI		0

Right click for more information on 69.172.200.109

Offense Source Summary

IP	69.172.20	Location	United States
Magnitude		Vulnerabilities	0
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	148	Events/Flows	14,311

Last 5 Notes

	Username	Creation Date

ned.

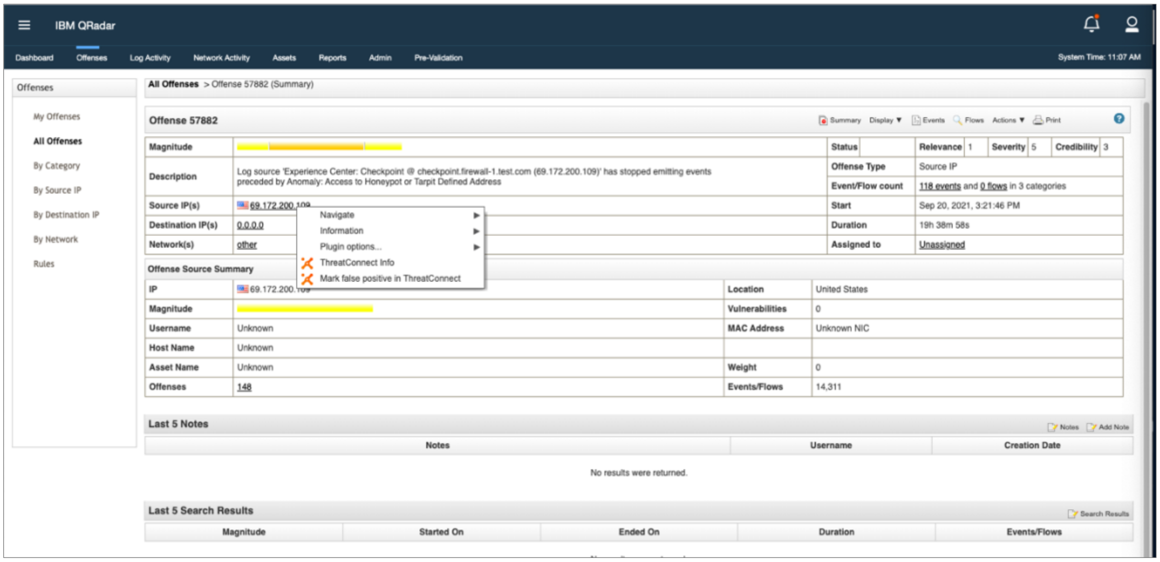
Last 5 Search Results

Magnitude		Duration	Events/Flows

ned.

Figure 5

4. To mark an Indicator as a false positive, right-click on the Indicator and select **Mark false positive in ThreatConnect** (Figure 6).



Offense 57882

Magnitude		Status	
Description	Log source 'Experience Center: Checkpoint @ checkpoint.firewall-1.test.com (69.172.200.109)' has stopped emitting events preceded by Anomaly: Access to Honeypot or Tarpit Defined Address	Relevance 1 · Severity 5 · Credibility 3	
		Offense Type	Source IP
		Event/Flow count	118 events and 0 flows in 3 categories
Source IP(s)	69.172.200.109	Start	Sep 20, 2021, 3:21:46 PM
Destination IP(s)	0.0.0.0	Duration	19h 38m 58s
Network(s)	other	Assigned to	Unassigned

Offense Source Summary

IP	69.172.200.109	Location	United States
Magnitude		Vulnerabilities	0
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	148	Events/Flows	14,311

Last 5 Notes

Notes	Username	Creation Date

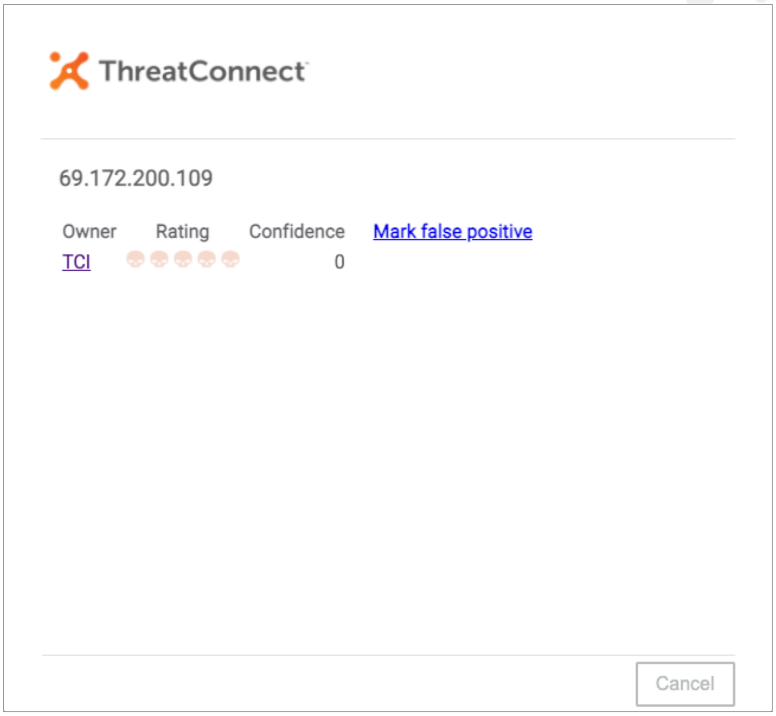
No results were returned.

Last 5 Search Results

Magnitude	Started On	Ended On	Duration	Events/Flows

Figure 6

5. To view ThreatConnect data on the Indicator in a separate window, right-click on the Indicator and select **ThreatConnect Info**. A window containing ThreatConnect metadata for the Indicator will be displayed (Figure 7). False positives can also be marked from this window.

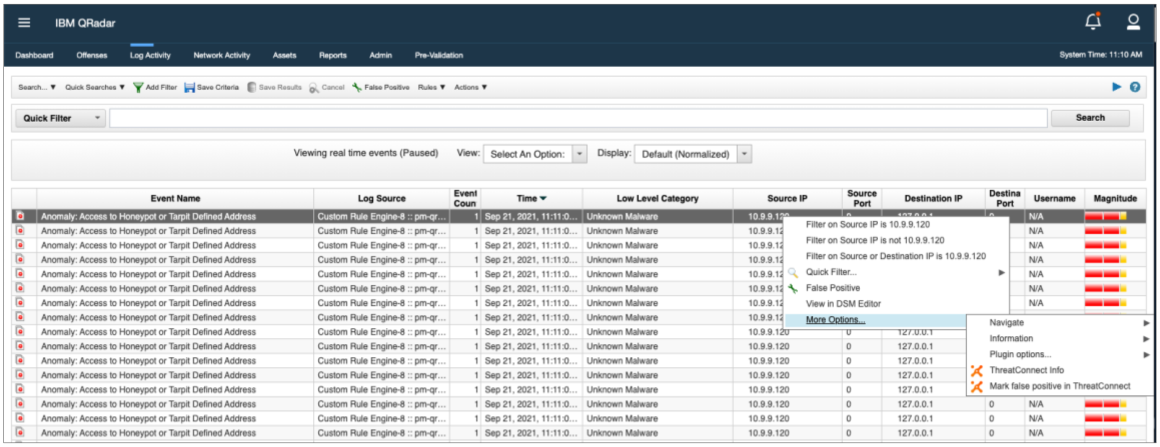


69.172.200.109

Owner	Rating	Confidence	Mark false positive
TCI		0	

Figure 7

6. From some views in QRadar, the **Mark false positive in ThreatConnect** and **ThreatConnect Info** options are accessed by right-clicking and selecting **More Options...** (Figure 8).

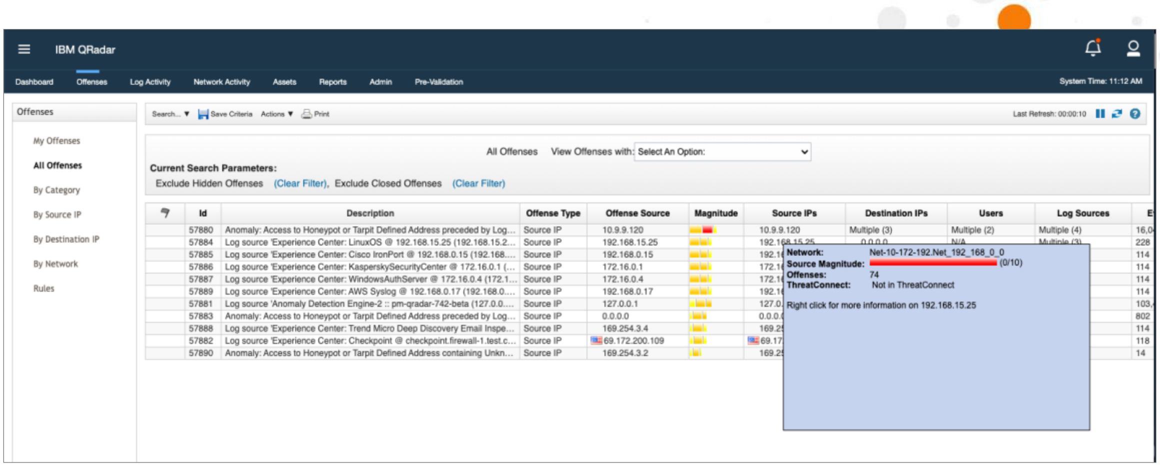


Viewing real time events (Paused) View: Select An Option: Display: Default (Normalized)

	Event Name	Log Source	Event Coun	Time	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Username	Magnitude
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.12	0	127.0.0.1	0	N/A	
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.12				N/A	
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.12				N/A	
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.12				N/A	
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.12				N/A	
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.12				N/A	
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.12				N/A	
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.12					
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.120	0	127.0.0.1			
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.120	0	127.0.0.1			
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.120	0	127.0.0.1			
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.120	0	127.0.0.1			
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.120	0	127.0.0.1			
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.120	0	127.0.0.1	0	N/A	
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.120	0	127.0.0.1	0	N/A	
	Anomaly: Access to Honeypot or Tarpit Defined Address	Custom Rule Engine-8 :: pm-qr...	1	Sep 21, 2021, 11:11:0...	Unknown Malware	10.9.9.120	0	127.0.0.1	0	N/A	

Figure 8

7. The hover-over feature will also show when an Indicator is not in ThreatConnect (Figure 9).



All Offenses View Offenses with: Select An Option:

Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

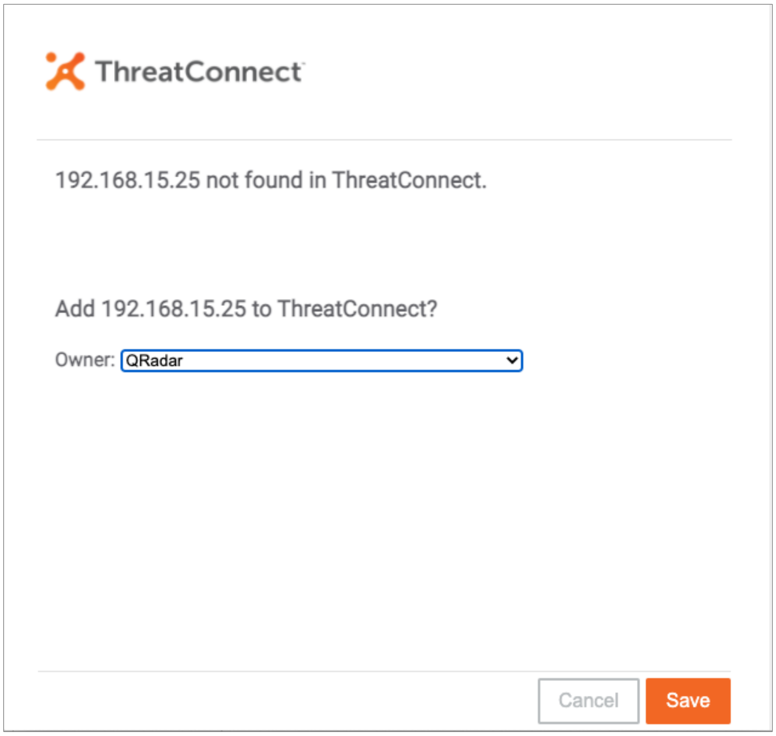
	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	E
	57880	Anomaly: Access to Honeypot or Tarpit Defined Address preceded by Log...	Source IP	10.9.9.120		10.9.9.120	Multiple (3)	Multiple (2)	Multiple (4)	16,0
	57884	Log source 'Experience Center: LinuxOS @ 192.168.15.25 (192.168.15.2...	Source IP	192.168.15.25		192.168.15.25	0.0.0.0	N/A	Multiple (3)	228
	57885	Log source 'Experience Center: Cisco IronPort @ 192.168.0.15 (192.168....	Source IP	192.168.0.15		192.1				114
	57886	Log source 'Experience Center: KasperskySecurityCenter @ 172.16.0.1 (...	Source IP	172.16.0.1		172.1				114
	57887	Log source 'Experience Center: WindowsAuthServer @ 172.16.0.4 (172.1...	Source IP	172.16.0.4		172.1				114
	57889	Log source 'Experience Center: AWS Syslog @ 192.168.0.17 (192.168.0....	Source IP	192.168.0.17		192.1				114
	57881	Log source 'Anomaly Detection Engine-2 :: pm-qradar-742-beta (127.0.0....	Source IP	127.0.0.1		127.0.				103,
	57883	Anomaly: Access to Honeypot or Tarpit Defined Address preceded by Log...	Source IP	0.0.0.0		0.0.0.				802
	57888	Log source 'Experience Center: Trend Micro Deep Discovery Email Inspe...	Source IP	169.254.3.4		169.25				114
	57882	Log source 'Experience Center: Checkpoint @ checkpoint.firewall-1.test.c...	Source IP	69.172.200.109		69.17				118
	57890	Anomaly: Access to Honeypot or Tarpit Defined Address containing Unkn...	Source IP	169.254.3.2		169.25				14

Network: Net-10-172-192.Net_192_168_0_0
Source Magnitude: (0/10)
Offenses: 74
ThreatConnect: Not in ThreatConnect

Right click for more information on 192.168.15.25

Figure 9

8. The Indicator can be added to ThreatConnect by right-clicking and selecting the **ThreatConnect Info** option. A window will be displayed asking if the Indicator should be added to ThreatConnect (Figure 10).



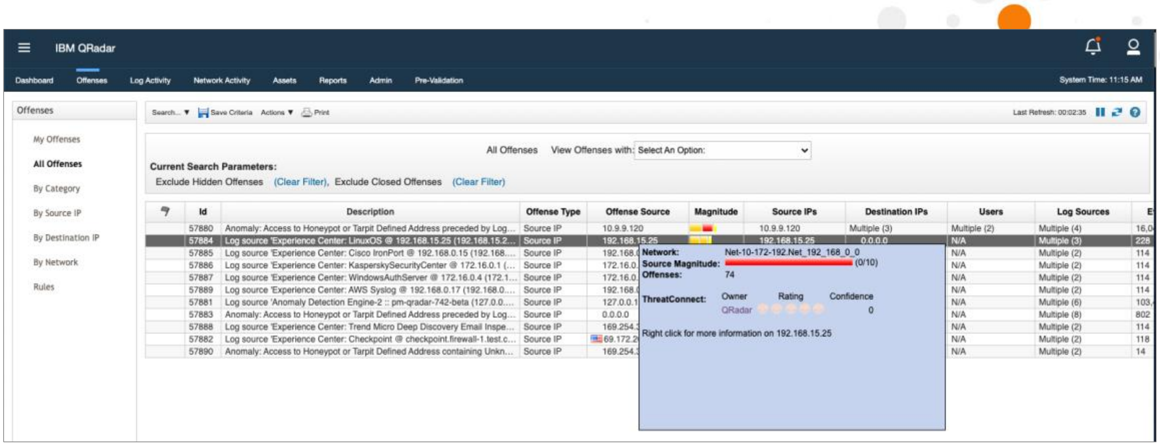
192.168.15.25 not found in ThreatConnect.

Add 192.168.15.25 to ThreatConnect?

Owner: QRadar

Figure 10

9. Select the Owner, and then click the **SAVE** button. The Indicator will now be added to ThreatConnect. Refresh the tab (e.g., **Log Activity**) by clicking on it, and then hover over the Indicator once more to see that it is now in ThreatConnect (Figure 11).



All Offenses View Offenses with: Select An Option:

Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	E
	57880	Anomaly: Access to Honeypot or Tarpit Defined Address preceded by Log...	Source IP	10.9.9.120		10.9.9.120	Multiple (3)	Multiple (2)	Multiple (4)	16,0
	57884	Log source 'Experience Center: LinuxOS @ 192.168.15.25 (192.168.15.2...	Source IP	192.168.15.25		192.168.15.25	0.0.0.0	N/A	Multiple (3)	228
	57885	Log source 'Experience Center: Cisco IronPort @ 192.168.0.15 (192.168....	Source IP	192.168.(				N/A	Multiple (2)	114
	57886	Log source 'Experience Center: KasperskySecurityCenter @ 172.16.0.1 (...	Source IP	172.16.0.				N/A	Multiple (2)	114
	57887	Log source 'Experience Center: WindowsAuthServer @ 172.16.0.4 (172.1...	Source IP	172.16.0.				N/A	Multiple (2)	114
	57889	Log source 'Experience Center: AWS Syslog @ 192.168.0.17 (192.168.0....	Source IP	192.168.(				N/A	Multiple (2)	114
	57881	Log source 'Anomaly Detection Engine-2 :: pm-qradar-742-beta (127.0.0....	Source IP	127.0.0.1				N/A	Multiple (6)	103,
	57883	Anomaly: Access to Honeypot or Tarpit Defined Address preceded by Log...	Source IP	0.0.0.0				N/A	Multiple (8)	802
	57888	Log source 'Experience Center: Trend Micro Deep Discovery Email Inspe...	Source IP	169.254.3				N/A	Multiple (2)	114
	57882	Log source 'Experience Center: Checkpoint @ checkpoint.firewall-1.test.c...	Source IP	69.172.2				N/A	Multiple (2)	118
	57890	Anomaly: Access to Honeypot or Tarpit Defined Address containing Unkn...	Source IP	169.254.3				N/A	Multiple (2)	14

Network: Net-10-172-192.Net_192_168_0_0
Source Magnitude: (0/10)
Offenses: 74

ThreatConnect: Owner Rating Confidence
QRadar 0

Right click for more information on 192.168.15.25

Figure 11

TROUBLESHOOTING

1. The hover-over functionality works only when the QRadar screen is stable and not actively loading. If hovering over an Indicator does not bring up a results box, it may be because the screen is refreshing. To stop the refreshing process, click the **Pause** button at the upper-right corner of the QRadar window. Then hover over the Indicator again.
2. QRadar often pulls its ThreatConnect results from cached data. To view completely current results, clear the cache by clicking the current tab (e.g., **Offenses**, **Log Activity**). Do not refresh the entire browser window, as doing so will cause the display to default to the **Dashboard** tab.