

RSA[®] NETWITNESS[®]
Intel Feeds
Implementation Guide

ThreatConnect[®]
Threat Intelligence Platform

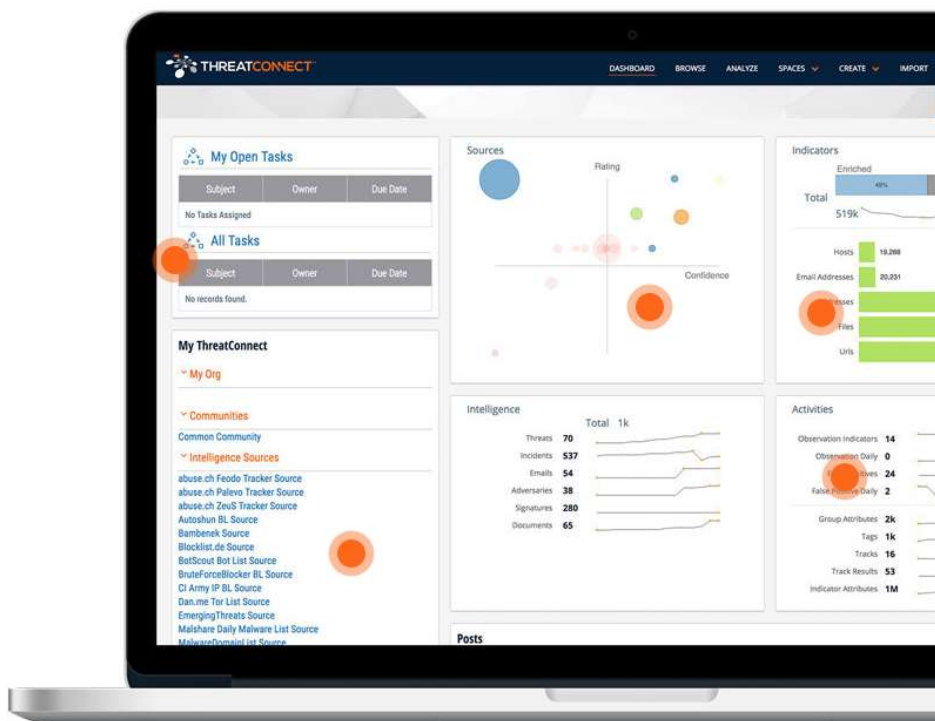
Daniel R. Pintal, RSA Partner Engineering
Last Modified: November 28, 2018

Solution Summary

Organizations of all sizes suffer from fragmentation of their security operations. When security teams don't collaborate and tools don't communicate, critical gaps emerge. Today's adversaries are smart. They know how to exploit these vulnerabilities to compromise your business' and your customers' data. ThreatConnect helps you close the gaps in your security practice once and for all.

ThreatConnect is a software platform that unites your entire security team, your partners, and your industry peers together behind a cohesive, intelligence-driven defense. Working together in ThreatConnect, everyone benefits from the collective talents and knowledge of the group. By making ThreatConnect intelligence data available in RSA NetWitness, you're able to build processes to identify the most relevant threats, proactively protect your network, and quickly respond to incidents in a measurable way.

RSA NetWitness Features	
ThreatConnect Threat Intelligence Platform	
Feed format	CSV
Collection method	http, local file
Feed Collection Frequency	Hourly, Daily, Weekly



Partner Product Configuration

Before You Begin

This section provides instructions for configuring the ThreatConnect Threat Intelligence Platform with RSA NetWitness. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All ThreatConnect components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

! > Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure ThreatConnect Threat Intelligence Platform is properly configured and secured before deploying to a production environment. For more information, please refer to the ThreatConnect Threat Intelligence Platform documentation or website.

ThreatConnect Threat Intelligence Platform Configuration

1. The ThreatConnect Threat Intelligence Platform integrates with RSA NetWitness via a .csv data feed. The .csv files are generated by the RSA NetWitness App for ThreatConnect running on the ThreatConnect Integrations Server. The data provided in the feed are configurable within ThreatConnect based on various criteria available within the job configuration.

The ThreatConnect Threat Intelligence Platform feed consists of the following files:

Filename	File Function
Feed Contents	IP Addresses, Indicators, Owner, Rating, Confidence, ThreatAssess Rating, ThreatAssess Confidence, ThreatConnect URL

ThreatConnect Prerequisites

- Active ThreatConnect Application Programming Interface (API) Key
- ThreatConnect® Integrations Server
- Trusted certificate installed for the ThreatConnect Integrations Server (see the **Appendix** of the **ThreatConnect Integrations Server Installation Guide** for detailed instructions)
- Bulk Export enabled for each Source from which data are to be pulled in ThreatConnect

ThreatConnect Configuration Parameters

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

Table 1

Name	Description
ThreatConnect API Path	<i>Required</i> – This parameter is a unique identifier assigned by the analysis system.
ThreatConnect API Access ID	<i>Required</i> – This parameter is the ThreatConnect API Access ID created via the ThreatConnect Web UI.
ThreatConnect API Secret Key	<i>Required</i> – This parameter is the ThreatConnect API Secret Key provided when creating an API account in the ThreatConnect Web UI.
Filter ThreatConnect Indicators by owner	<i>Required</i> – This parameter is the owners in ThreatConnect on which to filter.
Filter ThreatConnect Indicators by tags	<i>Optional</i> – This parameter is the tags in ThreatConnect on which to filter.
ThreatConnect Indicator types on which to filter	<i>Optional</i> – This parameter is the type of Indicators in ThreatConnect on which to filter.
Filter ThreatConnect Indicators by rating	<i>Optional</i> – This parameter is the minimum rating of Indicators in ThreatConnect on which to filter.
Filter ThreatConnect Indicators by confidence	<i>Optional</i> – This parameter is the minimum confidence of Indicators in ThreatConnect on which to filter.
Logging Level	<i>Optional (default: info)</i> – This parameter is the logging level for this job. Possible values are debug, info, warning, error, and critical.
Apply Proxy to ThreatConnect API Connection	<i>Optional (default: false)</i> – This parameter indicates whether to apply a proxy to the ThreatConnect API connection.

ThreatConnect Job Configuration

For detailed instructions on how to create a new job, please see the article **Creating Jobs using TC Exchange Apps** found in the ThreatConnect Knowledge Base:

<http://kb.threatconnect.com/customer/en/portal/articles/2190957-creating-jobs-using-tc-exchange-apps>

Once the job is configured, the job wizard will provide a URL and credentials (if configured) for the .csv file. This URL is the one that will be entered in the RSA NetWitness Live Feeds section detailed later.

RSA NetWitness Configuration

RSA NetWitness Custom Feed Configuration

Depending on your deployment and if you have elected to add an RSA NetWitness Log Decoder and/or Packet Decoder follow the steps below for your integration.

To extend the functionality of RSA NetWitness Feeds for use with NetWitness rules and notifications please refer to <http://sadocs.emc.com/>.

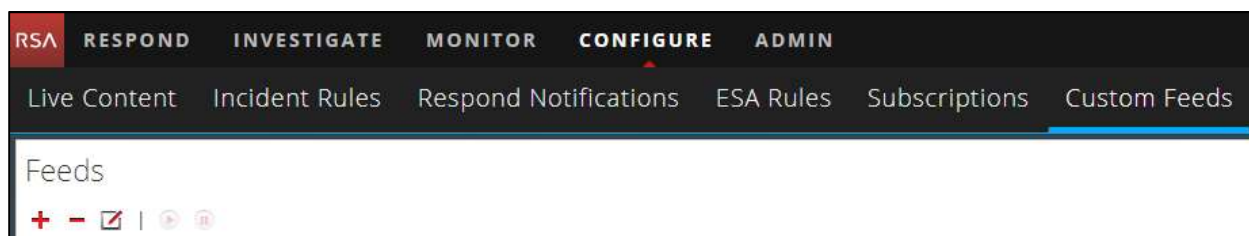
RSA NetWitness Prerequisites

- The RSA NetWitness server should be able to connect to the ThreatConnect Integrations Server over HTTP on port 443 or another port specified in the Feed URL.
- A certificate from the ThreatConnect Integrations Server should be installed under RSA NetWitness Trusted CAs.
- Modify the **table-map-custom.xml** file on the Log Decoder/Collector. Use the xml contained within **Appendix A** to update the table-map-custom.xml file.

Packet/Log Decoder Configuration

RSA NetWitness Feed Configuration

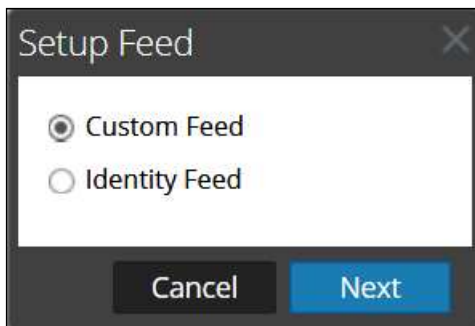
1. From the RSA NetWitness Dashboard select **Configure, Custom Feeds**.



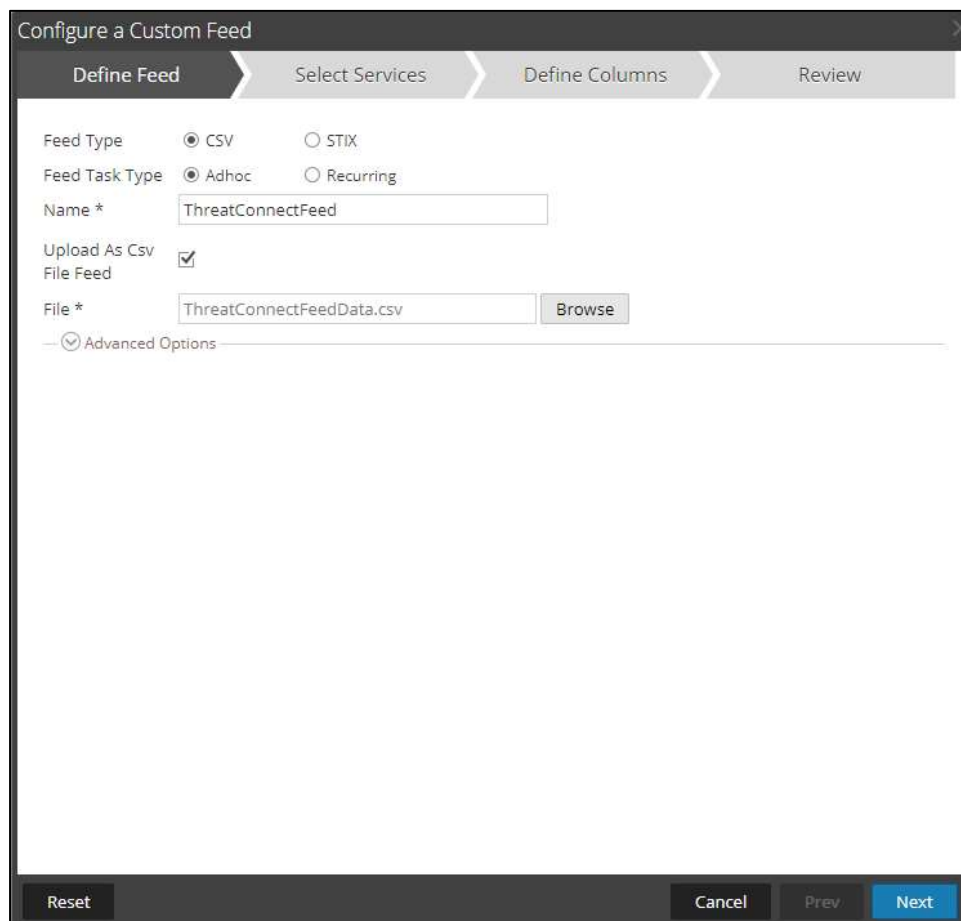
2. Select the **+** in the Live Feeds Window to setup the feed.



3. Select the **Custom Feed** radio button within the Setup Feed pop-up window and select **Next**.

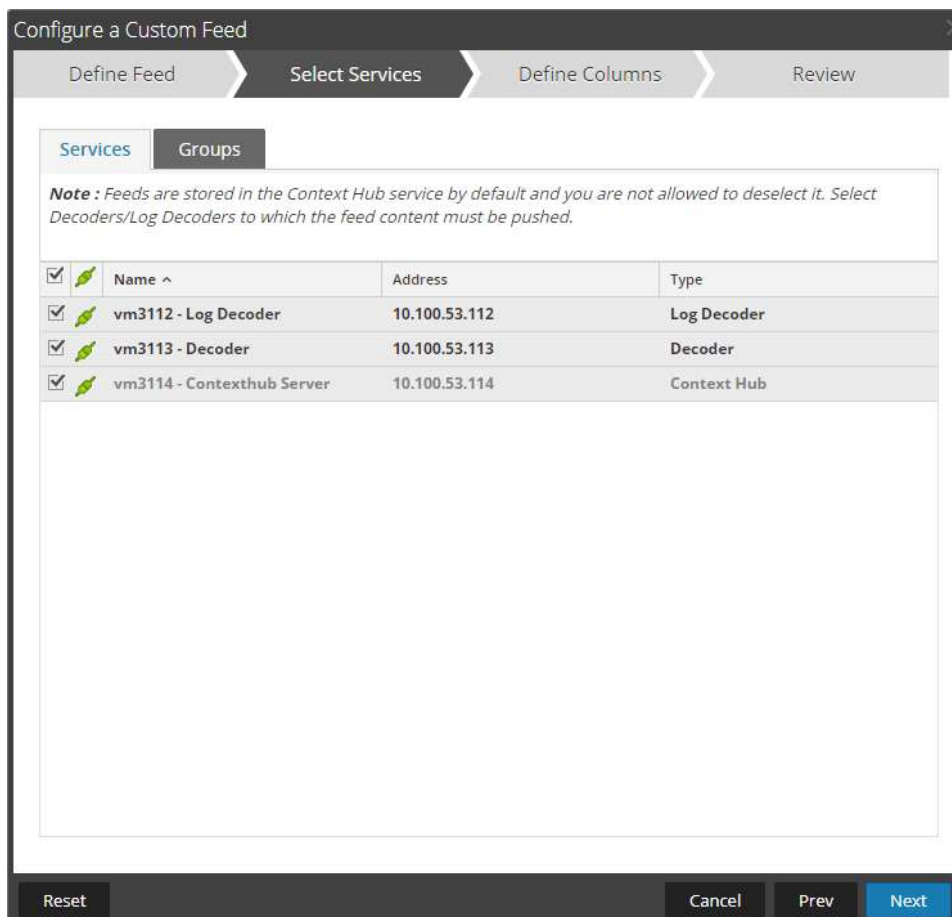


4. Select **Adhoc** if you are uploading the file once or the **Recurring** radio button if you plan to automate the feed. Enter the **URL** of the Feed provider and select how often to pull the feed by setting the **Recur Every** option and select **Next**.



! > Important: If using an XML feed you must configure the RSA NetWitness Advanced Options and use an XML Feed File.

5. Select the **RSA NetWitness Log Decoder Service** checkbox and select **Next**.







Configure a Custom Feed

Define Feed | **Select Services** | Define Columns | Review

Services | Groups

Note : Feeds are stored in the Context Hub service by default and you are not allowed to deselect it. Select Decoders/Log Decoders to which the feed content must be pushed.

<input checked="" type="checkbox"/>	 Name ^	Address	Type
<input checked="" type="checkbox"/>	 vm3112 - Log Decoder	10.100.53.112	Log Decoder
<input checked="" type="checkbox"/>	 vm3113 - Decoder	10.100.53.113	Decoder
<input checked="" type="checkbox"/>	 vm3114 - Contexthub Server	10.100.53.114	Context Hub

Reset | Cancel | Prev | **Next**

!> Important: NetWitness Feed integrations can support integrations with the NetWitness Log Decoder and Packet Decoder individually or separately.

6. Define the **Type** as **IP** and **Index Column 1** (IP Address Field). Set the header of each column as needed. If the custom keys you have added are not available from the drop-down list, type them in. An example mapping table is provided in [Appendix B](#). Select **Next** to continue.

Configure a Custom Feed

Define Feed > Select Services > Define Columns > Review

Define Index

Type IP IP Range Non-IP

Index Column(S) 2 CIDR

Define Values

Column	1	2	3	4
Key			tc.owner	tc.rating
Address	52.191.197.178		admin	3.0
Address	171.22.171.177		admin	3.0
Address	171.22.176.81		admin	3.0
Address	171.31.0.5		admin	3.0
Address	193.108.18.80		admin	3.0
Address	185.43.181.41		admin	3.0
Address	171.17.232.62		admin	3.0
Address	171.22.62.137		admin	3.0
Address	149.154.167.91		admin	3.0
Address	171.22.160.46		admin	3.0

Reset Cancel Prev Next

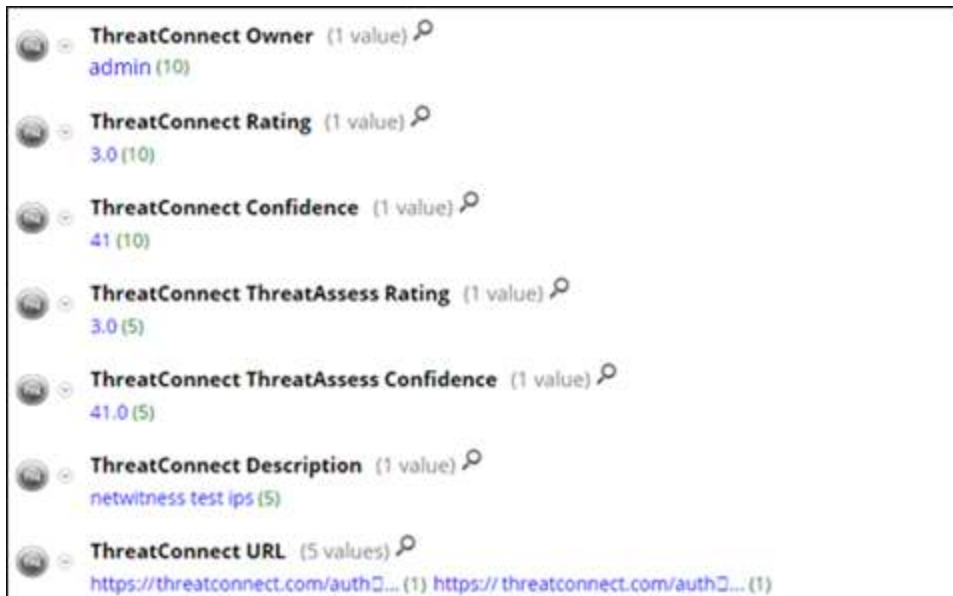
7. Select **Finish** to complete the setup of the Feed Integration.

8. Initially the status will appear as **Waiting** and the Progress will be **yellow** until RSA NetWitness complete's the transfer of the Feed. Once completed the Status will display **Completed** and the Progress will be **green**. Depending on the size of the feed it may take some time for RSA NetWitness to download all Threat Intel from your provider.

Feeds						
Name	Trigger	Disk Usage	Created	Last Run Time	Status	Progress
<input checked="" type="checkbox"/> NWThreatFeed	Once	-	2018-10-12 14:56:12	2018-10-12 14:56:12	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>

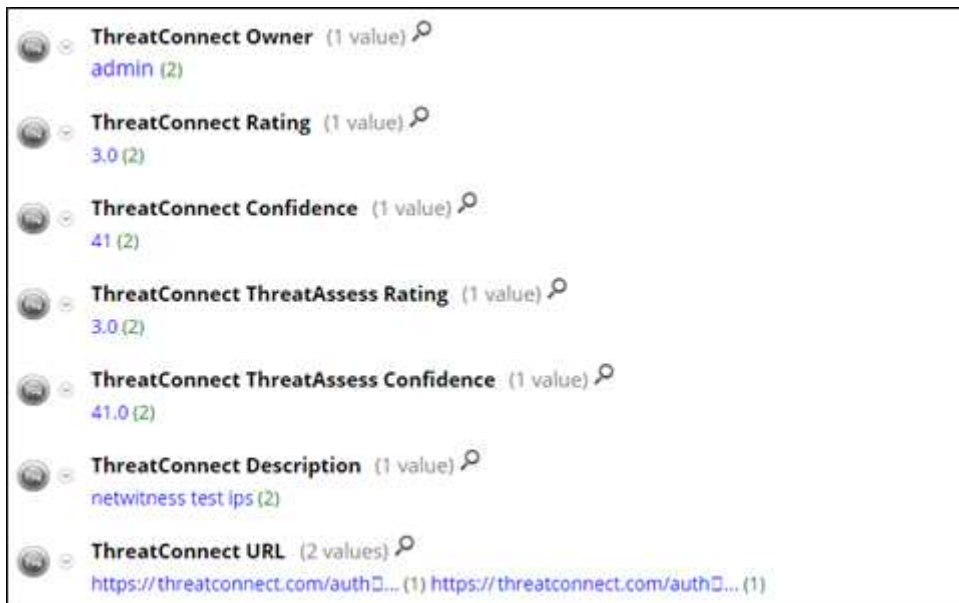
9. Once completed and if you have any threat events, the meta will appear as normal text.

Syslog



A screenshot of a Syslog interface showing seven metadata fields for ThreatConnect. Each field is represented by a circular icon with a magnifying glass, followed by the field name, its value, and a count in parentheses. The fields are: ThreatConnect Owner (1 value) with value 'admin (10)'; ThreatConnect Rating (1 value) with value '3.0 (10)'; ThreatConnect Confidence (1 value) with value '41 (10)'; ThreatConnect ThreatAssess Rating (1 value) with value '3.0 (5)'; ThreatConnect ThreatAssess Confidence (1 value) with value '41.0 (5)'; ThreatConnect Description (1 value) with value 'netwitness test ips (5)'; and ThreatConnect URL (5 values) with value 'https://threatconnect.com/auth... (1) https://threatconnect.com/auth... (1)'. The URL field shows two identical entries.

Packets

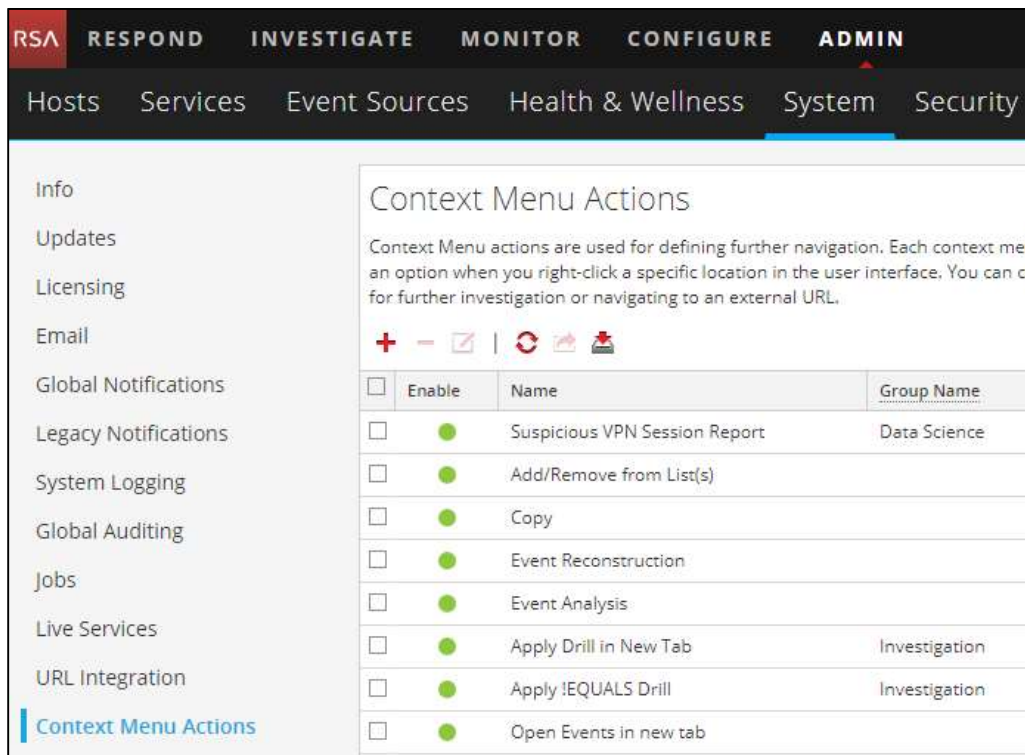


A screenshot of a Packets interface showing seven metadata fields for ThreatConnect. Each field is represented by a circular icon with a magnifying glass, followed by the field name, its value, and a count in parentheses. The fields are: ThreatConnect Owner (1 value) with value 'admin (2)'; ThreatConnect Rating (1 value) with value '3.0 (2)'; ThreatConnect Confidence (1 value) with value '41 (2)'; ThreatConnect ThreatAssess Rating (1 value) with value '3.0 (2)'; ThreatConnect ThreatAssess Confidence (1 value) with value '41.0 (2)'; ThreatConnect Description (1 value) with value 'netwitness test ips (2)'; and ThreatConnect URL (2 values) with value 'https://threatconnect.com/auth... (1) https://threatconnect.com/auth... (1)'. The URL field shows two identical entries.

NetWitness Context Menu Actions (Optional)

To enhance the integration and provide Analysts with additional functionality add NetWitness Context Menu Actions. This feature will allow Analysts to use Context Menu Actions to quickly open a link to the Threat Analytics provider to perform further investigation of the IP address.

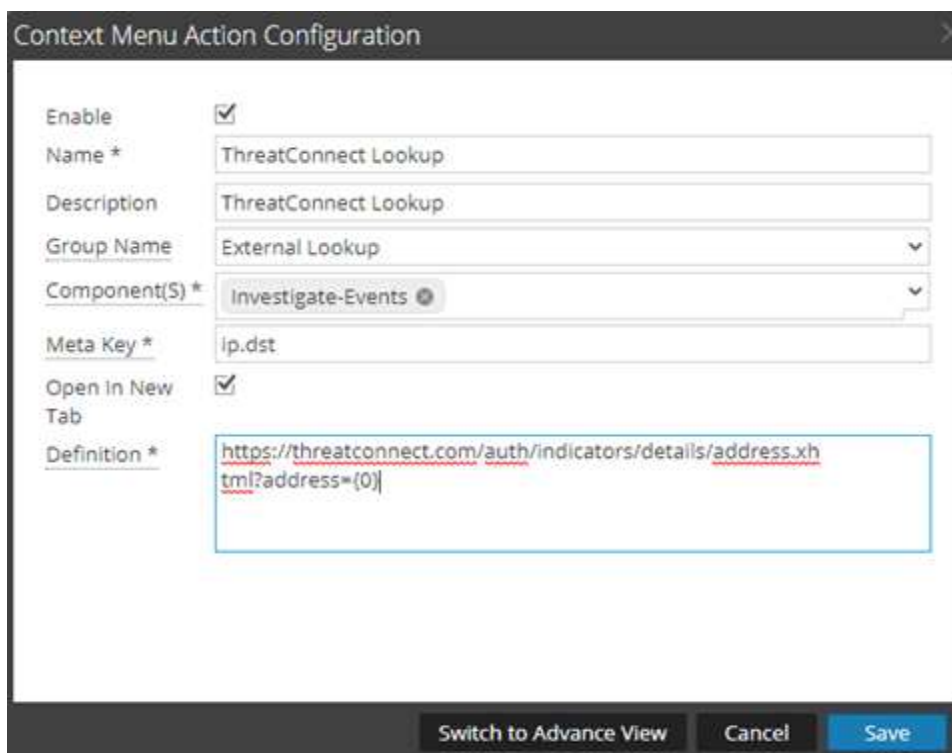
1. Login as a Netwitness Administrator and select **Admin, System, Context Menu Actions**.



2. Select **+** to add a new Context Menu Action.



3. Within Context Menu Action Configuration enter the following;
 - a) Select **Enable** checkbox.
 - b) Enter **Name** to appear as the option within the Context Menu Action.
 - c) Enter a **Description**.
 - d) From the Group Name drop down select **External Lookup**.
 - e) From the Components drop down select **Investigate-Events**.
 - f) For the Meta Key, enter **ip.dst**.
 - g) Select **Open in New Tab** checkbox.
 - h) The Definition field (URL) will be dependent on the Threat Intel provider. RSA NetWitness will replace the {0} field with the Meta Key value defined in step f above.



Context Menu Action Configuration

Enable

Name * ThreatConnect Lookup

Description ThreatConnect Lookup

Group Name External Lookup

Component(S) * Investigate-Events

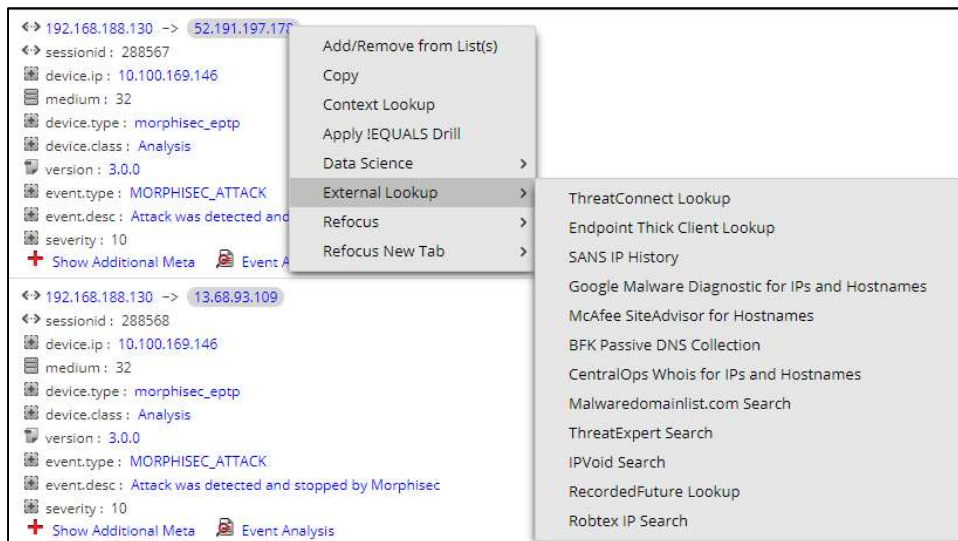
Meta Key * ip.dst

Open in New Tab

Definition * <https://threatconnect.com/auth/indicators/details/address.xhtml?address={0}>

Switch to Advance View Cancel Save

4. No restart is required the Context Menu Action is immediately available for use.



Certification Checklist for RSA NetWitness

Date Tested: November 28, 2018

Certification Environment		
Product Name	Version Information	Operating System
RSA NetWitness	11.2	Virtual Appliance
ThreatConnect Intelligence Platform	4.1	Services
ThreatConnect Integration Server	1.1	Service

NetWitness Test Case	Result
Investigation	
Threat Intelligence Feed is received through Decoder Meta	✓
Threat Intelligence Feed is received through Packet Decoder	✓

✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix A

NetWitness Log Decoder table-map-custom.xml

A sample snippet of entries into the **table-map-custom.xml** file is provided below. Please note that this is provided as an example only, as additional fields can be included or excluded as needed.

```
<mapping envisionName="tc.owner" nwName="tc.owner" flags="None" format="Text"/>
<mapping envisionName="tc.rating" nwName="tc.rating" flags="None" format="Float64"/>
<mapping envisionName="tc.confidence" nwName="tc.confidence" flags="None" format="Text"/>
<mapping envisionName="tc.threat.rating" nwName="tc.threat.rating" flags="None" format="Float64"/>
<mapping envisionName="tc.threat.conf" nwName="tc.threat.conf" flags="None" format="Float64"/>
<mapping envisionName="tc.desc" nwName="tc.desc" flags="None" format="Text"/>
<mapping envisionName="tc.url" nwName="tc.url" flags="None" format="Text"/>
```

NetWitness Concentrator index-concentrator-custom.xml

A sample snippet of entries into the **index-concentrator-custom.xml** file is provided below. Please note that this is provided as an example only, as additional fields can be included or excluded as needed.

```
<key description="ThreatConnect Owner" format="Text" level="IndexValues" name="tc.owner"
valuemax="250000" defaultAction="Open"/>
<key description="ThreatConnect Rating" format="Float64" level="IndexValues" name="tc.rating"
valuemax="250000" defaultAction="Open"/>
<key description="ThreatConnect Confidence" format="Float64" level="IndexValues"
name="tc.confidence" valuemax="250000" defaultAction="Open"/>
<key description="ThreatConnect ThreatAssess Rating" format="Float32" level="IndexValues"
name="tc.threat.rating" valuemax="250000" defaultAction="Open"/>
<key description="ThreatConnect ThreatAssess Confidence" format="Float64" level="IndexValues"
name="tc.threat.conf" valuemax="250000" defaultAction="Open"/>
<key description="ThreatConnect Description" format="Text" level="IndexValues" name="tc.desc"
valuemax="250000" defaultAction="Open"/>
<key description="ThreatConnect URL" format="Text" level="IndexValues" name="tc.url"
valuemax="250000" defaultAction="Open"/>
```

Appendix B

A sample mapping table is provided below. Please note that this is provided as an example only, as additional fields can be included or excluded as needed.

ThreatConnect Fields	NetWitness Meta	Custom Meta
Indicator	index	
Owner		tc.owner
Rating		tc.rating
Confidence		tc.confidence
ThreatAssess Rating		tc.threat.rating
ThreatAssess Confidence		tc.threat.conf
Description		tc.desc
Web URL		tc.url