RSA® NETWITNESS®
Intel Feeds
Implementation Guide

Recorded Future Cyber Threat Intelligence

Daniel R Pintal, RSA Partner Engineering
Last Modified: October 30, 2018

RSA READY

Solution Summary

Recorded Future arms you with real-time threat intelligence so you can proactively defend your organization against cyber-attacks. With billions of indexed facts, and more added every day, Recorded Future's patented Web Intelligence Engine continuously analyzes the entire web to give you unmatched insight into emerging threats.

NetWitness imports the intelligence from Recorded Future and enhances the events collected from third party sources by appending threat intelligence metadata when and where needed.

By using NetWitness Event Stream Analysis (ESA) for notification the events and the combined threat intelligence can be used to create alerts to advise security staff of potential malicious activity.

RSA NetWitness Features	
Recorded Future Cyber Threat Intelligence	
Feed format	xml, csv
Collection method	https, http, local file
Feed Collection Frequency	Hourly, Daily, Weekly

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Recorded Future integrations 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 Recorded Future 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 the Recorded Future content is properly configured.

Intelligence Feed	File Function
Feed Contents	IP address or Domain Name, Threat Feed Provider, Risk, Risk Score, Threat type and Evidence Details (URL).

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 **https://community.rsa.com/community/products/netwitness**.

Log Decoder Configuration

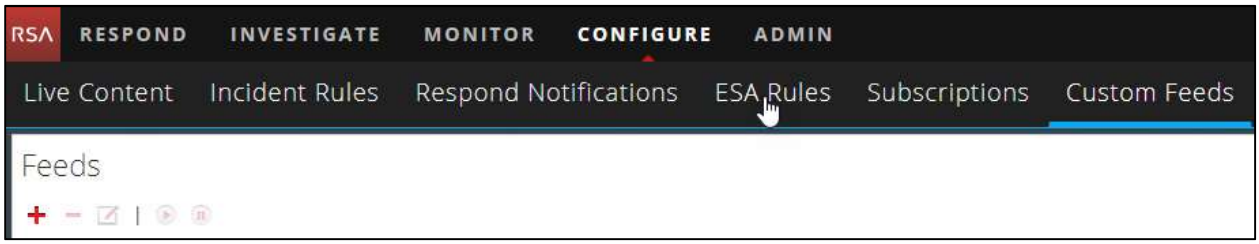
1. Edit the **table-map-custom.xml** on the Log Decoder and add new keys to be parsed.

Example table-map-custom.xml.

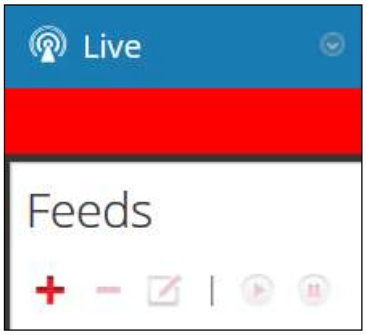
```
<mappings>

	<mapping envisionName="risk_info" nwName="risk.info" flags="None"
format="Text"/>
	<mapping envisionName="risk" nwName="risk" flags="None" format="Text"/>
	<mapping envisionName="threat_category" nwName="threat.category"
flags="None" format="Text"/>
	<mapping envisionName="IntelCardURL" nwName="IntelCardURL" flags="None"
format="Text"/>

</mappings>
```

RSA NetWitness Feed Configuration

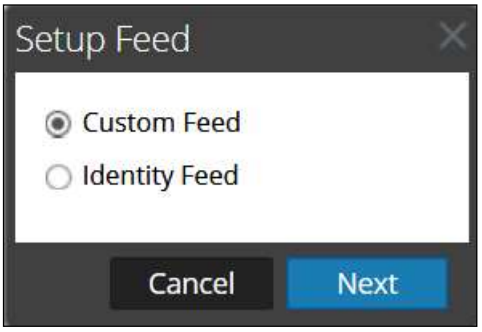
1. From the RSA NetWitness Dashboard select **Configure, Custom Feeds**.



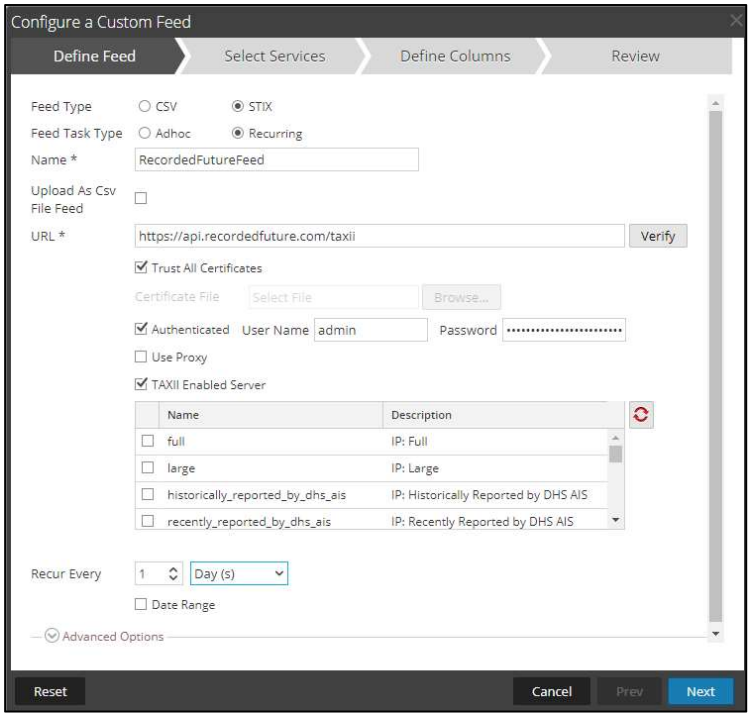
2. Select the + in Feeds to setup a new feed source.



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

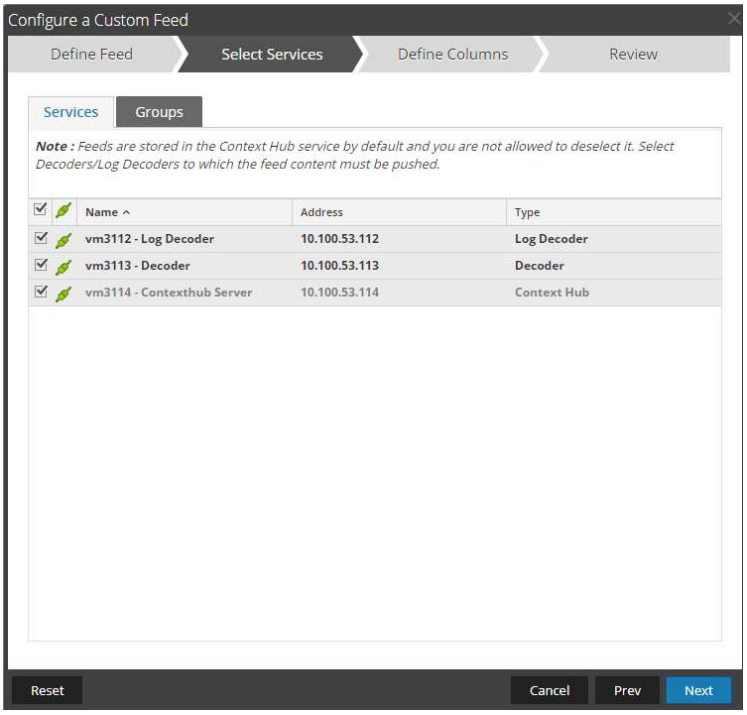


4. Select **STIX** > **Recurring** > Enter a **Name** > URL> **Authenticated** > **User** > **TAXII Enabled Server** > **STIX Feed** > and set **Recur Every** for a defined period, select **Next**.

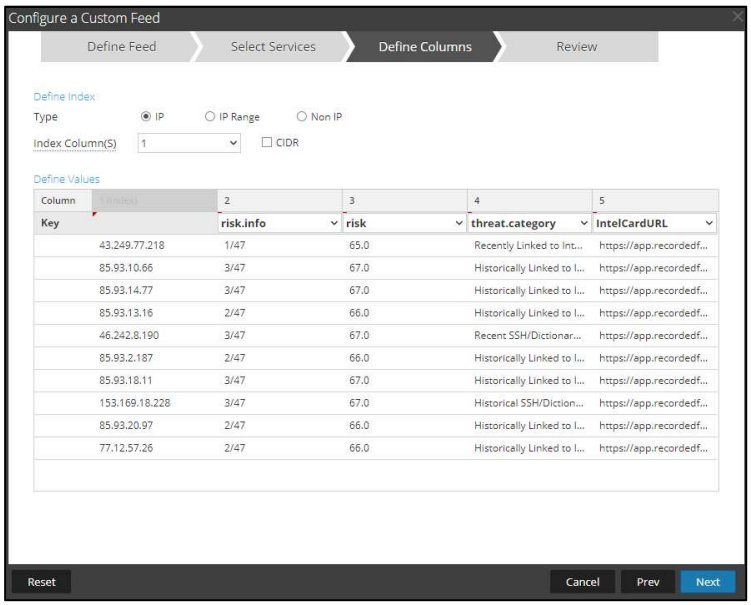


! > Important: Contact Recorded Future to discuss key elements of your STIX Feed.

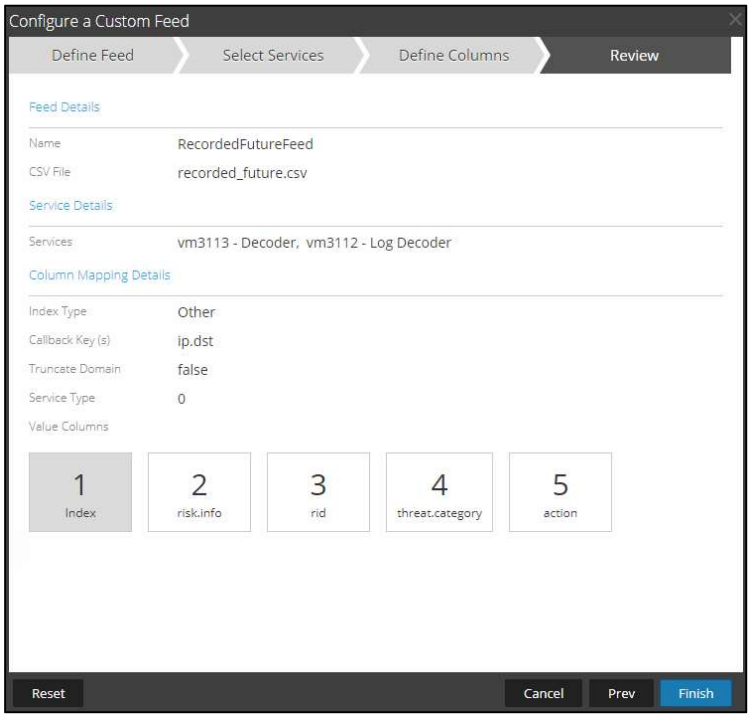
5. Depending on your NetWitness installation select **Log Decoder**, **Packet Decoder** or both if installed.



6. Define the Index as Type **IP**, **Index Column 1**, and use **Callback Key (S) ip.dst**. Set the header of each column as needed and select **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 completes 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.

9. Once completed and if you have any events which correlate to an address listed in Recorded Futures threat intelligence the Risk, Risk.Info, Threat.Category and IntelCardURL will be appended to the Event Analysis as meta.

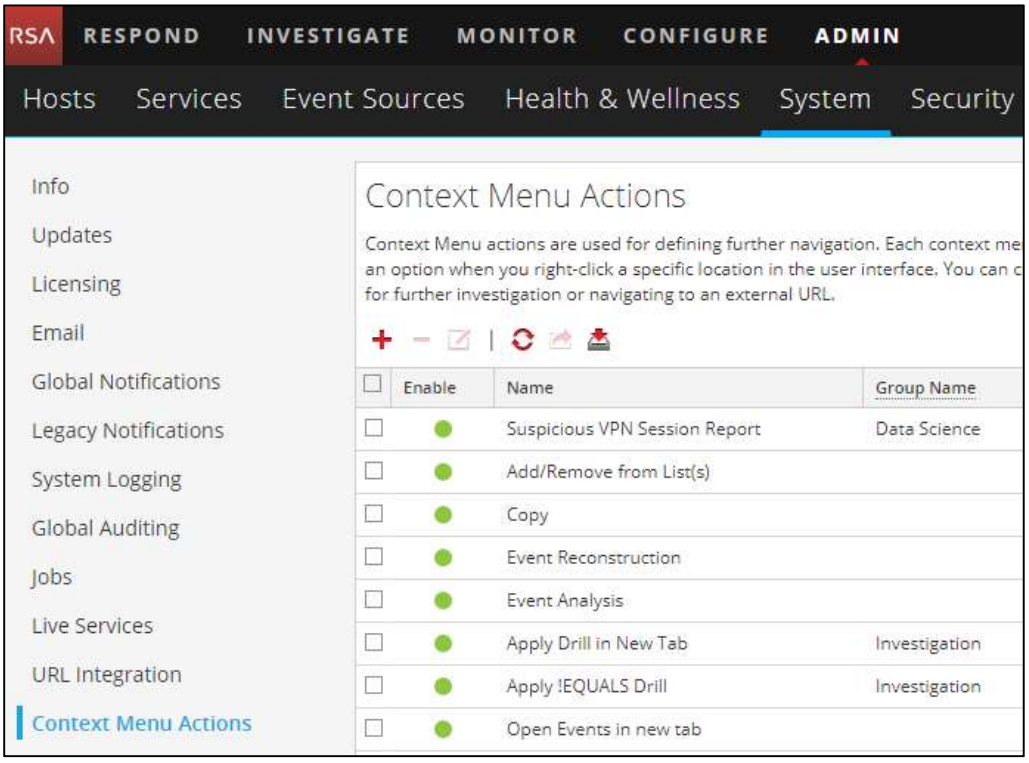
Log source example collected from NetWitness Investigator:

Packet source example collected from NetWitness Investigator:

NetWitness Context Menu Actions (Optional)

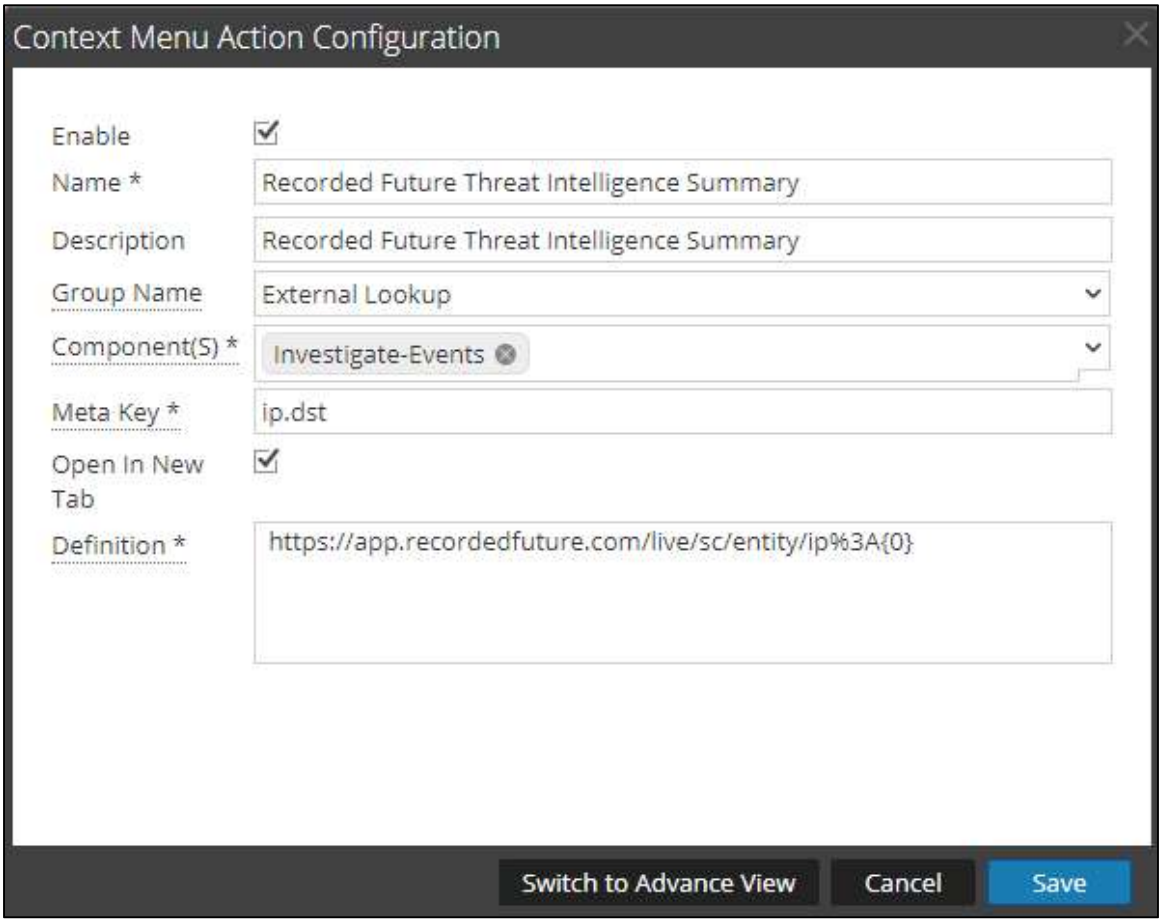
To enhance the integration and provide Analysts with additional functionality add NetWitness Context Menu Actions. This feature will allow Analysts to use Context Menu Actions to quickly open a link to the Threat Analytics provider to perform further investigation of the IP address.

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

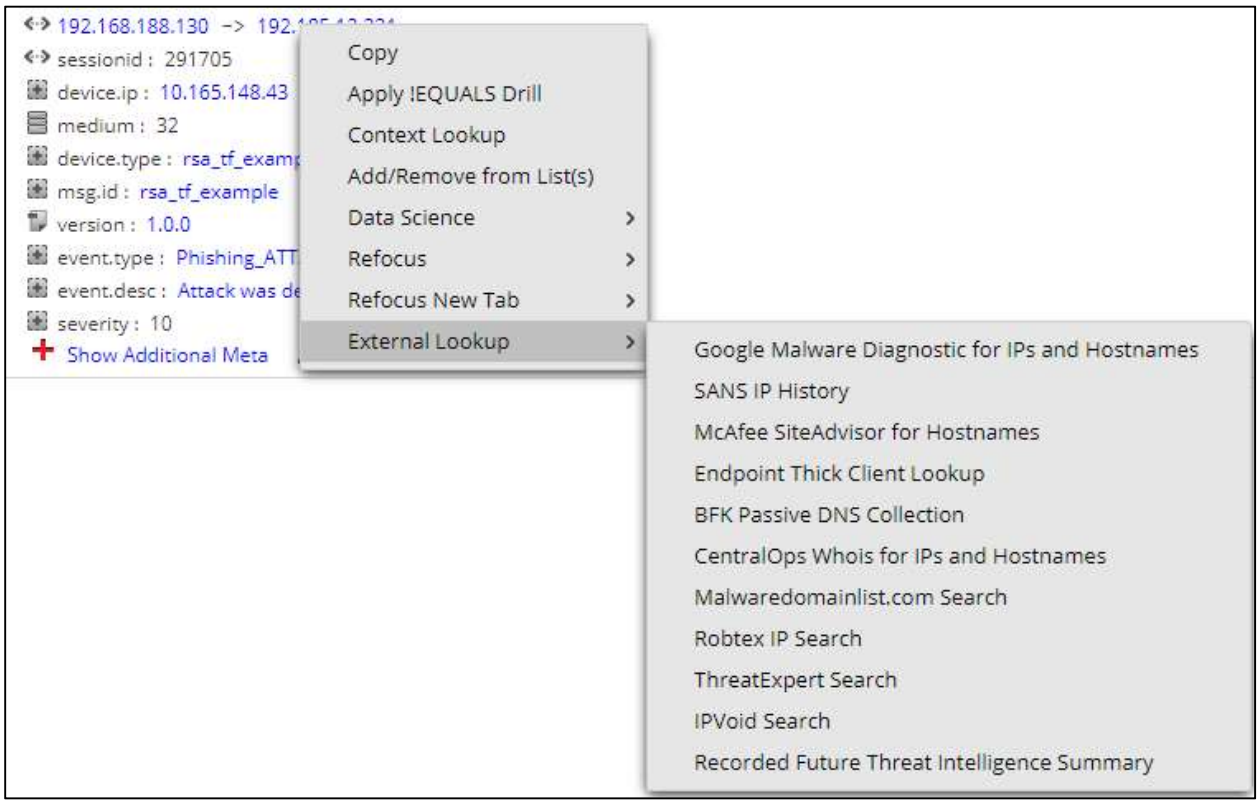


2. Select + to add a new Context Menu Action.

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.



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



Certification Checklist for RSA NetWitness

Date Tested: October 30, 2018

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	11.1.0	Virtual Appliance
Recorded Future	NA	NA

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

✓ = Passed, **X** = Failed, **-** = N/A