

RSA® NETWITNESS®
Intel Feeds
Implementation Guide

Recorded Future Cyber Threat Intelligence

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

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

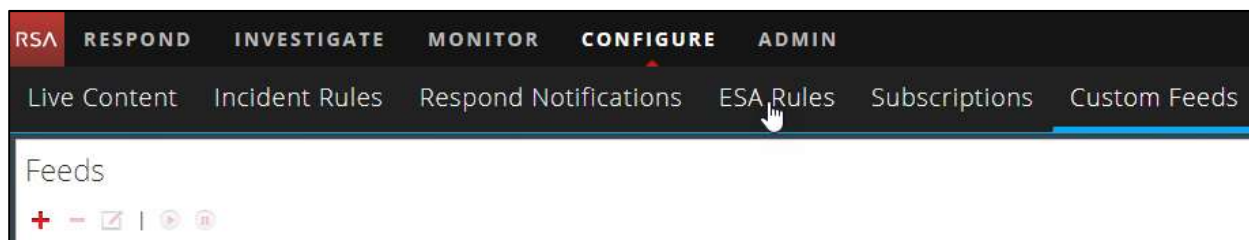
1. Edit the **table-map-custom.xml** on the Log Decoder and add new keys to be parsed.

Example table-map-custom.xml.

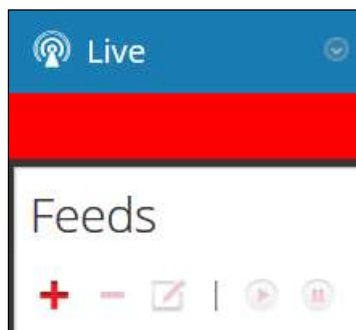
```
<mappings>
  <mapping envisionName="risk_info" nwName="risk.info" flags="None"
format="Text"/>
  <mapping envisionName="risk" nwName="risk" flags="None" format="Text"/>
  <mapping envisionName="threat_category" nwName="threat.category"
flags="None" format="Text"/>
  <mapping envisionName="IntelCardURL"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

RSA NetWitness Feed Configuration

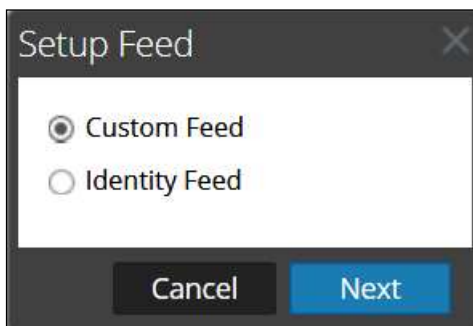
1. From the RSA NetWitness Dashboard select **Configure, Custom Feeds**.



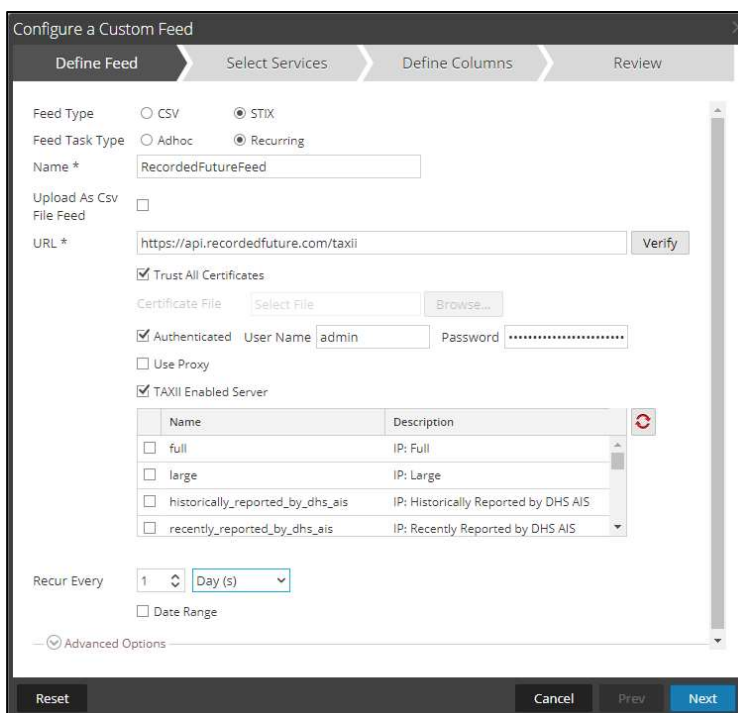
2. Select the **+** in Feeds to setup a new feed source.



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**.



Configure a Custom Feed

Define Feed | Select Services | Define Columns | Review

Feed Type: CSV STIX

Feed Task Type: Adhoc Recurring

Name *: RecordedFutureFeed

Upload As Csv File Feed:

URL *: https://api.recordedfuture.com/taxii [Verify]

Trust All Certificates

Certificate File: [Select File] [Browse...]

Authenticated User Name: admin Password: [Masked]

Use Proxy

TAXII Enabled Server

	Name	Description
<input type="checkbox"/>	full	IP: Full
<input type="checkbox"/>	large	IP: Large
<input type="checkbox"/>	historically_reported_by_dhs_ais	IP: Historically Reported by DHS AIS
<input type="checkbox"/>	recently_reported_by_dhs_ais	IP: Recently Reported by DHS AIS

Recur Every: 1 [Day (s)]

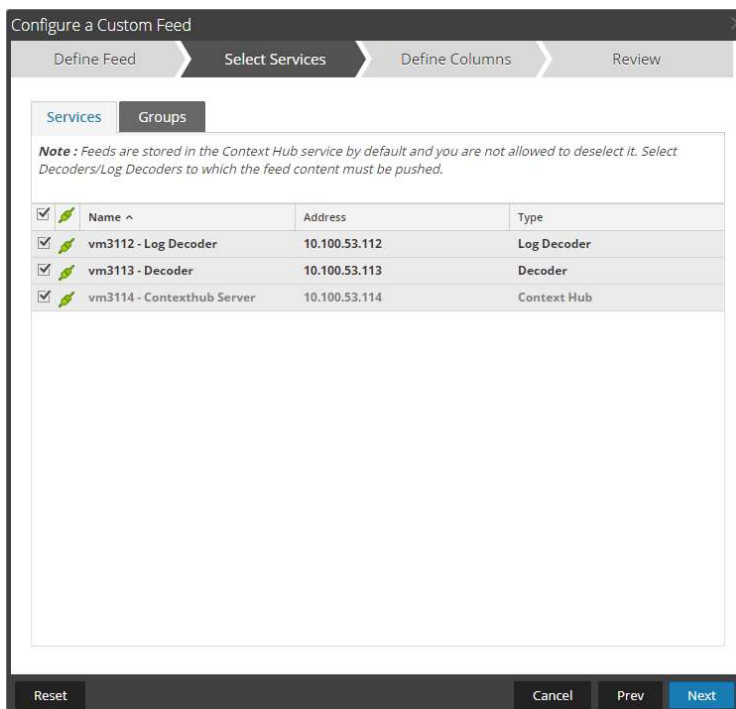
Date Range

Advanced Options

Reset Cancel Prev Next

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

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



Configure a Custom Feed

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

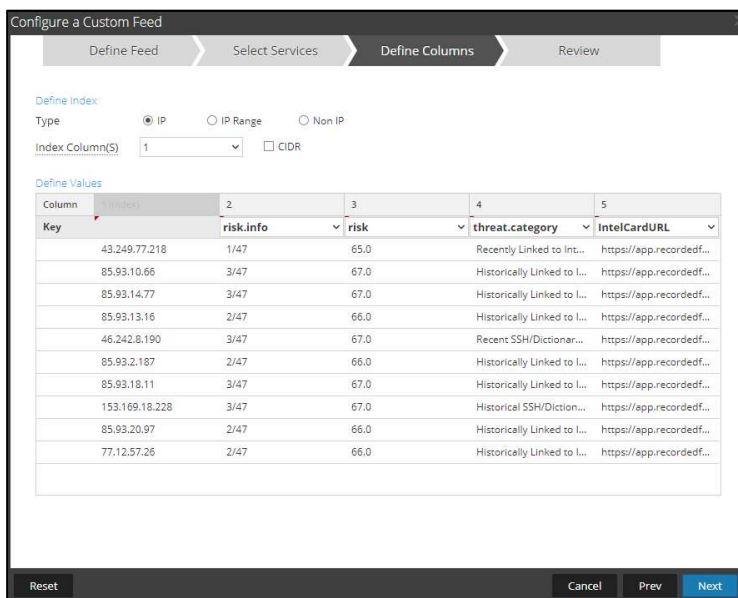
Services | Groups

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

Reset | Cancel | Prev | **Next**

- 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**.



Configure a Custom Feed

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

Define Index

Type IP IP Range Non IP

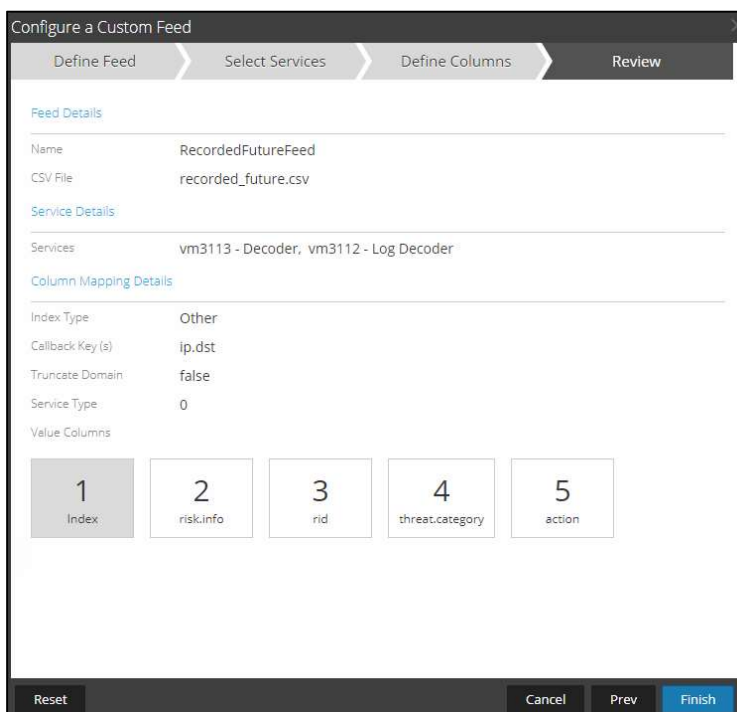
Index Column(S) 1 CIDR

Define Values

Column	(Index)	2	3	4	5
Key		risk.info	risk	threat.category	IntelCardURL
	43.249.77.218	1/47	65.0	Recently Linked to Int...	https://app.recordedf...
	85.93.10.66	3/47	67.0	Historically Linked to I...	https://app.recordedf...
	85.93.14.77	3/47	67.0	Historically Linked to I...	https://app.recordedf...
	85.93.13.16	2/47	66.0	Historically Linked to I...	https://app.recordedf...
	46.242.8.190	3/47	67.0	Recent SSH/Dictionar...	https://app.recordedf...
	85.93.2.187	2/47	66.0	Historically Linked to I...	https://app.recordedf...
	85.93.18.11	3/47	67.0	Historically Linked to I...	https://app.recordedf...
	153.169.18.228	3/47	67.0	Historical SSH/Diction...	https://app.recordedf...
	85.93.20.97	2/47	66.0	Historically Linked to I...	https://app.recordedf...
	77.12.57.26	2/47	66.0	Historically Linked to I...	https://app.recordedf...

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 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.

Feeds						
Name	Trigger	Disk Usage	Created	Last Run Time	Status	Progress
<input checked="" type="checkbox"/> RecordedFutureFeed	Once	-	2018-05-15 14:28:46	2018-05-15 14:28:46	Completed	<div style="width: 100%; height: 10px; background-color: green;"></div>

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:

```
<> 192.168.188.130 -> 85.93.12.101
<> sessionid : 195013
device.ip : 10.100.169.12
medium : 32
device.type : ██████████
device.class : Analysis
version : 3.0.0
event.type : ██████████
event.desc : Attack was detected and stopped by ██████████
user.src : DESKTOP-CL6EITR/admin
host.src : DESKTOP-CL6EITR
netname : other dst
risk.info : 2/47
risk : 86.0
threat.category : Historically Linked to Intrusion Method | Recent Positive Malware Verdict
IntelCardURL : https://app.recordedfuture.com/live/sc/entity/ip%3A85.93.12.101
netname : private src
direction : outbound
AttackedModule : GlobalGetAtomName
LastStackFunCall : ntdll.dll | <space><space>0x0006F60C<space>{<space><space><space><space>NtGetContextThread<space>|<space><space><space><space>0x76F50000
LastModuleLoaded : 0x764C0000<space>|<space><space><space>0x76501000<space>|<space><space><space>0x41000<space>|<space><space><space><space>C:/Windows/System32/UI/Animation.dll<space>
(FileDescription:Windows<space><space>Animation<space><space>Manager;ProductName:Microsoft<space><space>Windows<space><space>Operating<space><space>System;Ve
CommandLine : C:/Program<space><space>Files<space><space>{x86}/Internet<space><space>Explorer/ie/ieexplore.exe<space><space>SCODEF:4B4B<space><space>CREDAT:9476<space><space>/prefetch:2
ParentPrCmdLine : C:/Program<space><space>Files/Internet<space><space>explorer/ie/ieexplore.exe
CodeProcessed : 0x76fbf60c<space><space>RET<space><space>0x8
ParentSignature : 8dea16e513f70e1a98be6ec48439b5499d2c740247716f6bcb990b7c305ec0e0
starttime : 2018-Mar-06 13:25:37.000
msg.id : ██████████
event.cat.name : Other.Default
device.disc : 100
did : vm3112
rid : 215
ip.all : 10.100.169.12
user.all : DESKTOP-CL6EITR/admin
host.all : DESKTOP-CL6EITR
ip.all : 85.93.12.101
ip.all : 192.168.188.130
- Hide Additional Meta Event Analysis
```

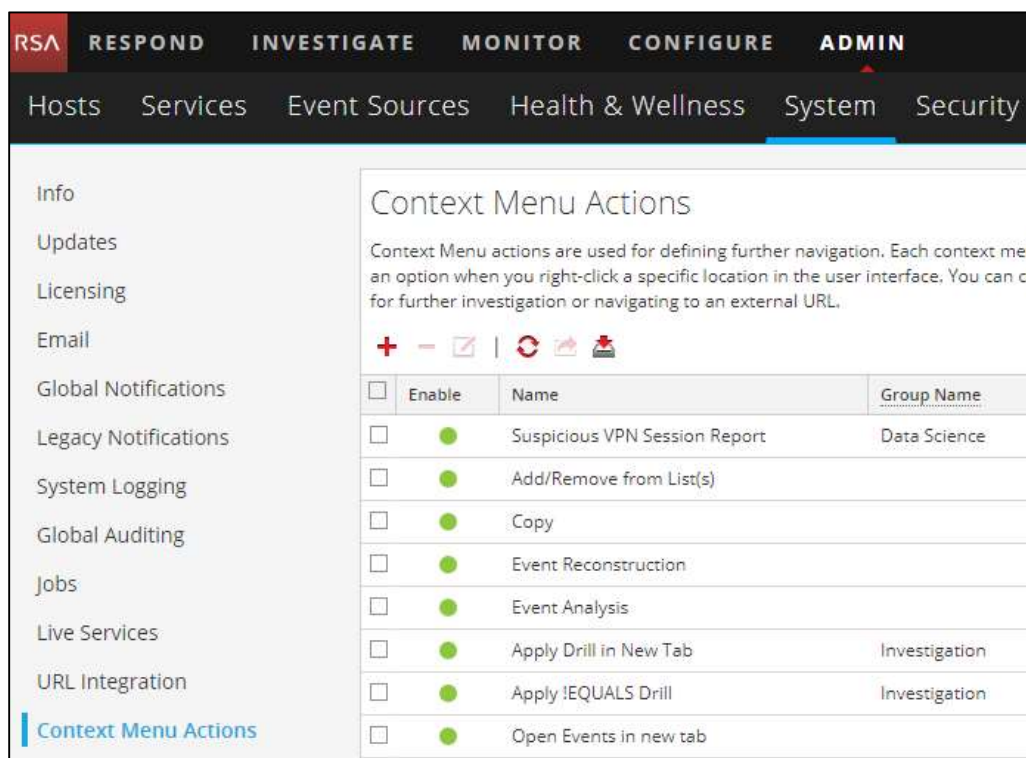

Packet source example collected from NetWitness Investigator:

```
<-> 00:1B:8F:30:40:00 -> 00:50:56:A4:33:85
<-> 10.100.169.12 -> 43.249.77.218
🔴 64781 -> 514
<-> sessionid : 195021
📄 payload : 7139
📄 medium : 1
<-> eth.type : IP
<-> ip.proto : TCP
🔴 tcp.flags : 27
🔗 service : OTHER
📄 streams : 1
📄 packets : 10
🕒 lifetime : 0
📄 netname : other dst
📄 netname : private src
📄 direction : outbound
📄 sourcefile : RecordedFuture_Morphise_43.249.77.218.pcap
📍 country.dst : Hong Kong
📍 city.dst : Mong Kok
📍 latdec.dst : 22.3167
📍 longdec.dst : 114.1667
📍 org.dst : Guochao Group limited
📄 analysis.session : not top 20 dst
📄 inv.category : operations
📄 inv.context : event analysis
📄 inv.context : flow analysis
📄 feed.name : investigation
⚠️ risk.info : 1/47
📄 risk : 65.0
🔗 threat.category : Recently Linked to Intrusion Method
📄 IntelCardURL : https://app.recordedfuture.com/live/sc/entity/ip%3A43.249.77.218
📄 did : vm3113
📄 rid : 194802
📄 eth.all : 00:1B:8F:30:40:00
📄 eth.all : 00:50:56:A4:33:85
📄 ip.all : 10.100.169.12
📄 ip.all : 43.249.77.218
<-> ipv6.proto : TCP
📄 port.src.all : 64781
📄 port.all : 64781
```

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.



The screenshot shows the NetWitness Admin console interface. The top navigation bar includes RSA, RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The left sidebar lists various system components, with 'Context Menu Actions' highlighted. The main content area displays the 'Context Menu Actions' configuration page, which includes a table of existing actions and a '+ Add' button.

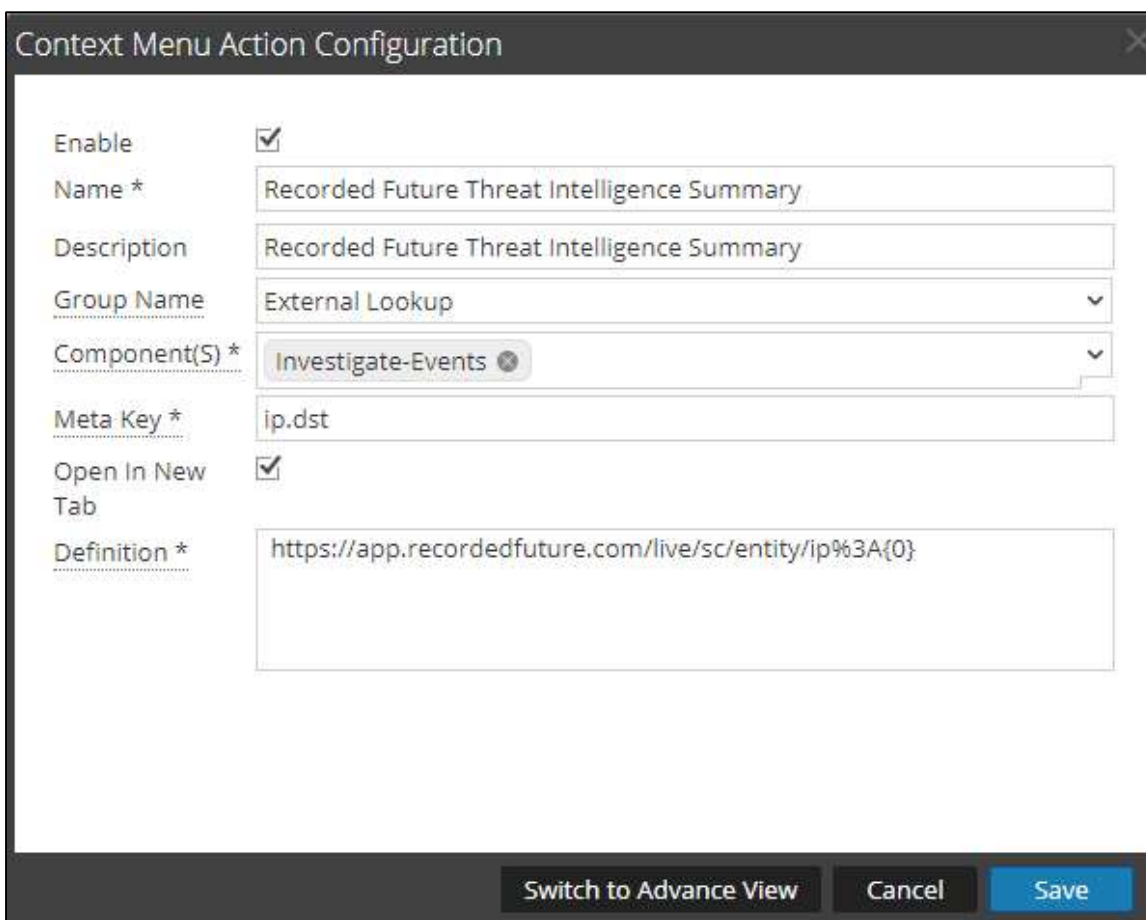
<input type="checkbox"/>	Enable	Name	Group Name
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Suspicious VPN Session Report	Data Science
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Add/Remove from List(s)	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Copy	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Event Reconstruction	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Event Analysis	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Apply Drill in New Tab	Investigation
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Apply !EQUALS Drill	Investigation
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Open Events in new tab	

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



This image is a close-up of the 'Context Menu Actions' configuration page, specifically focusing on the '+ Add' button (a red plus sign) located below the table of actions.

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.

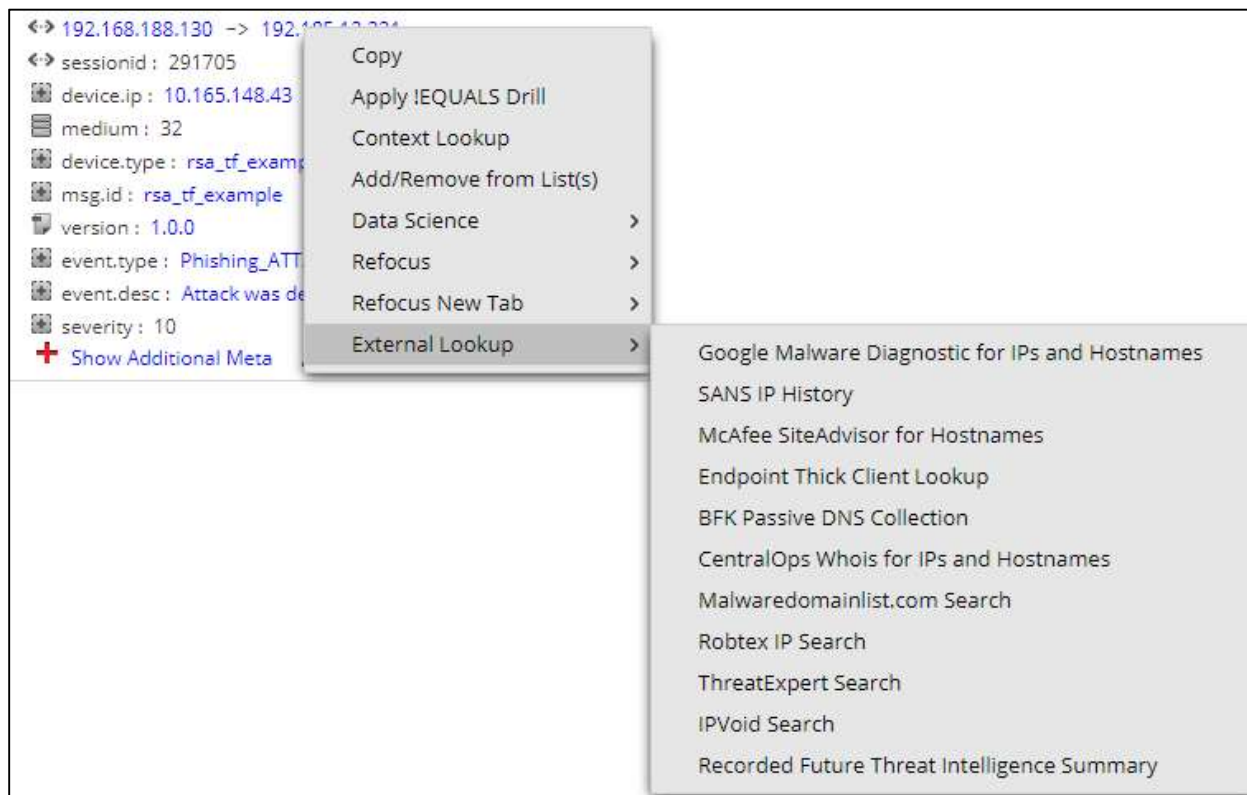


Context Menu Action Configuration

Enable	<input checked="" type="checkbox"/>
Name *	Recorded Future Threat Intelligence Summary
Description	Recorded Future Threat Intelligence Summary
Group Name	External Lookup
Component(S) *	Investigate-Events
Meta Key *	ip.dst
Open In New Tab	<input checked="" type="checkbox"/>
Definition *	https://app.recordedfuture.com/live/sc/entity/ip%3A{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: 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