RSA® NETWITNESS®

Intel Feeds Implementation Guide

PhishMe Intelligence

Jeffrey Carlson, RSA Partner Engineering

Last Modified: 02/02/2018

Solution Summary

PhishMe Intelligence provides accurate and timely alerts so that you can be ready to take fast action when under attack. PhishMe Analysts and Researchers work to analyze and verify phishing threats delivering ransomware, key loggers, RATs, and other types of crimeware. This high-fidelity data is delivered in multiple forms to effectively prepare and respond to attacks. PhishMe Intelligence is available via a restful API to access machine-readable threat intelligence (MRTI) in STIX format. By leveraging the STIX standard, PhishMe Threat Intelligence data can be imported into RSA NetWitness to diagnose infected corporate systems, and proactively detect or defend against attacks before they happen.

RSA NetWitness Features	
PhishMe Intelligence	
Feed format	STIX xml
Collection method	http or local file
Feed Collection Frequency	Hourly, Daily, or Weekly

Partner Product Configuration

Before You Begin

This section provides instructions for configuring PhishMe Threat Intelligence 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 PhishMe 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 PhishMe Threat Intelligence is properly configured and secured before deploying to a production environment. For more information, please refer to the PhishMe documentation or website.

PhishMe Threat Intelligence Configuration

PhishMe Threat Intelligence integrates with RSA NetWitness via STIX XML files. Structured Threat Information Expression (STIX™) is a structured language for describing cyber threat information so it can be shared, stored, and analyzed in a consistent manner. RSA NetWitness supports the import of STIX Indicators and STIX Observables.

STIX files can be generated via the PhishMe Threat Intelligence universal integration. For more information on configuration this integration, consult the documentation links below:

- **https://www.threathq.com/documentation/display/MAD/_Configuration+Guide**
- **https://www.threathq.com/documentation/display/MAD/_Technical+Requirements**

To acquire this integration (and assistance if needed) please reach out to **support@phishme.com** with this request.

Note that STIX files with multiple observables or indicators must have only one `</stix:STIX_Package>` element in the XML. In RSA NetWitness, a STIX (.xml) feed of type Indicator or Observable which contains properties such as the IP addresses, File hashes, Domain names, and URLs are supported.

RSA NetWitness Configuration

RSA NetWitness Custom Feed Configuration

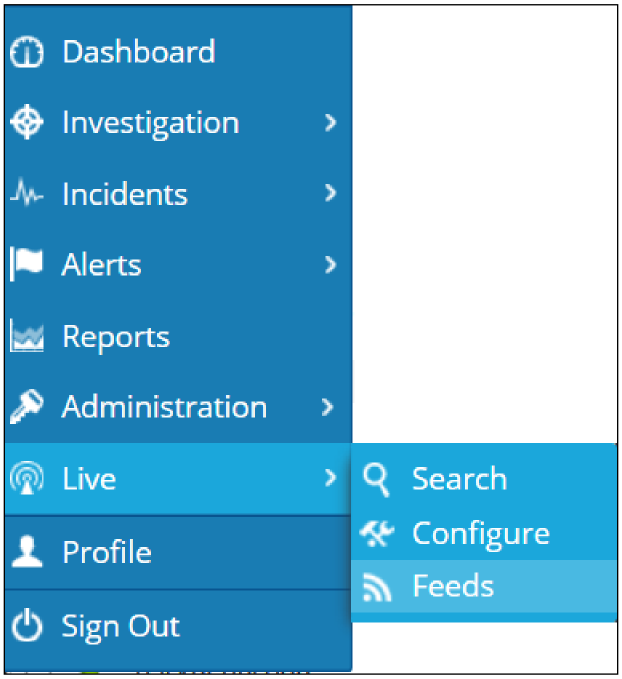
Depending on your deployment and if you have elected to add an RSA NetWitness Log Decoder and/or Packet Decoder follow the steps below for your integration.

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

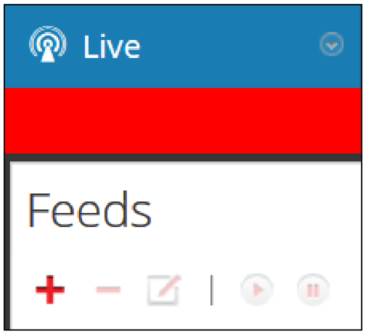
Log Decoder Configuration

RSA NetWitness Feed Configuration

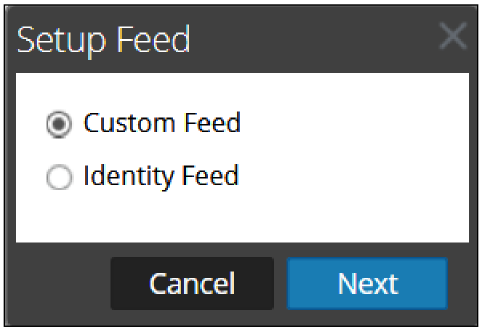
1. From the RSA NetWitness Dashboard Select **Live**, **Feeds**.



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



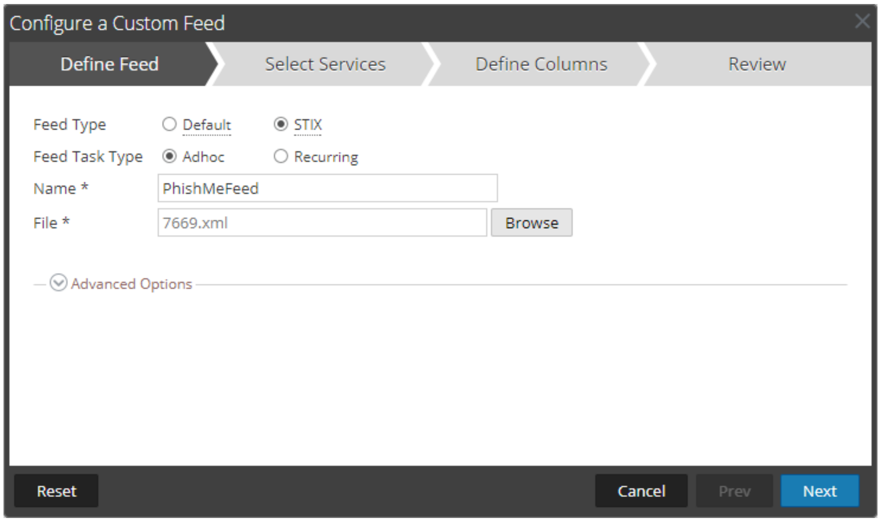
3. Select the **Custom Feed** radio button within the Setup Feed pop-up window and select **Next**.



Setup Feed

● Custom Feed
○ Identity Feed

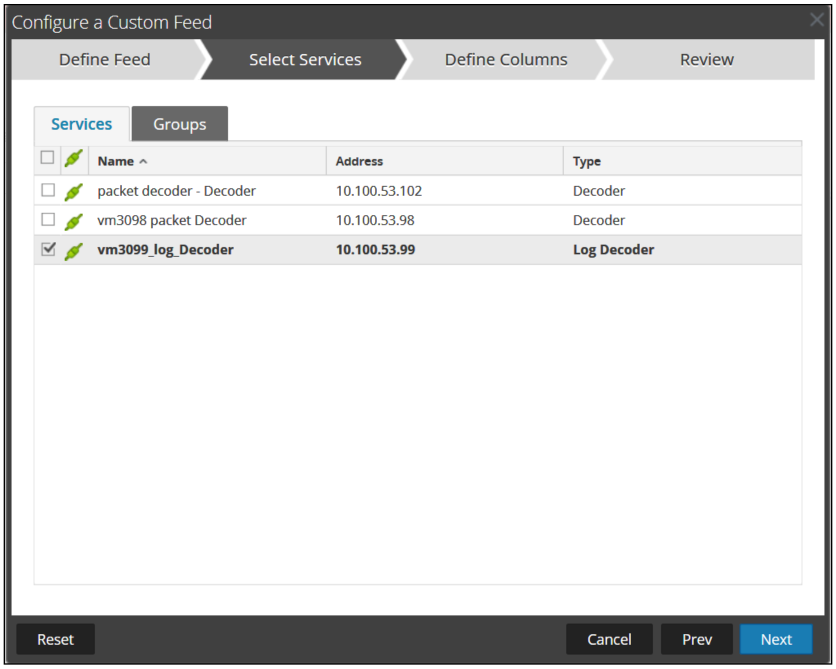
4. Set STIX and the Feed Type. Select **Adhoc** if you are uploading the file once or the **Recurring** radio button if you plan to automate the feed. Enter the **URL** of the Feed provider and select how often to pull the feed by setting the **Recur Every** option and select **Next**.



Configure a Custom Feed

Feed Type ○ Default ● STIX
Feed Task Type ● Adhoc ○ Recurring
Name * PhishMeFeed
File * 7669.xml

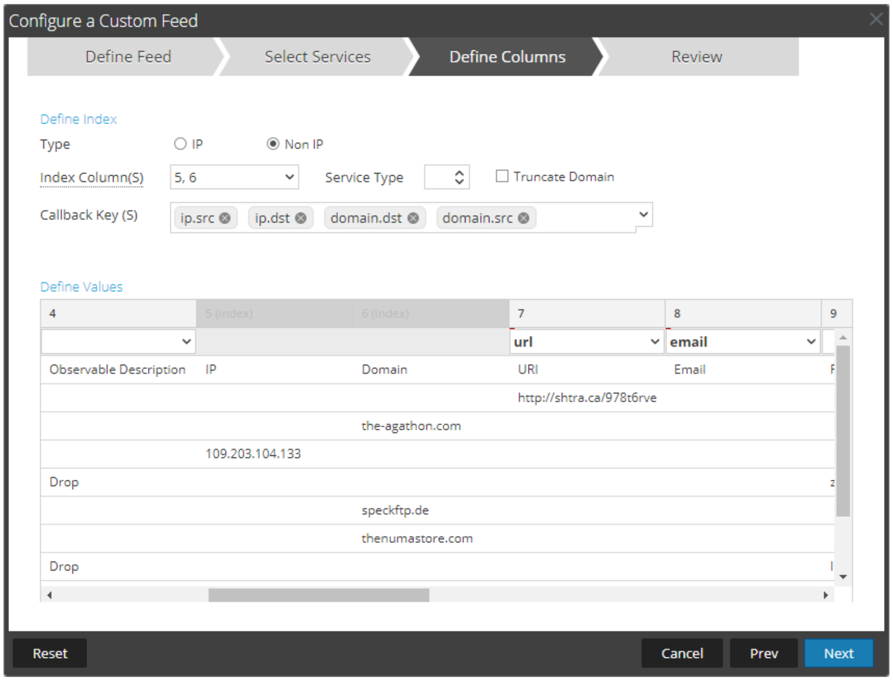
5. Select the log decoders and/or packet decoders you wish to push the feed to and select **Next**.



Configure a Custom Feed

□	Name ^	Address	Type
□	packet decoder - Decoder	10.100.53.102	Decoder
□	vm3098 packet Decoder	10.100.53.98	Decoder
☑	**vm3099_log_Decoder**	**10.100.53.99**	**Log Decoder**

6. In RSA NetWitness, only a STIX (.xml) feed of type **Indicator** or **Observable** which contains the properties such as IP addresses, File hashes, Domain names, and URLs are supported. Set the Type as **Non-IP** and select the column or columns you wish to index. Multiple **Index Columns** and Multiple **Callback Keys** can be supported as in the example below:



Configure a Custom Feed

Define Index

Type ○ IP ● Non IP

Index Column(S) 5, 6

Service Type

□ Truncate Domain

Callback Key (S) ip.src ip.dst domain.dst domain.src

Define Values

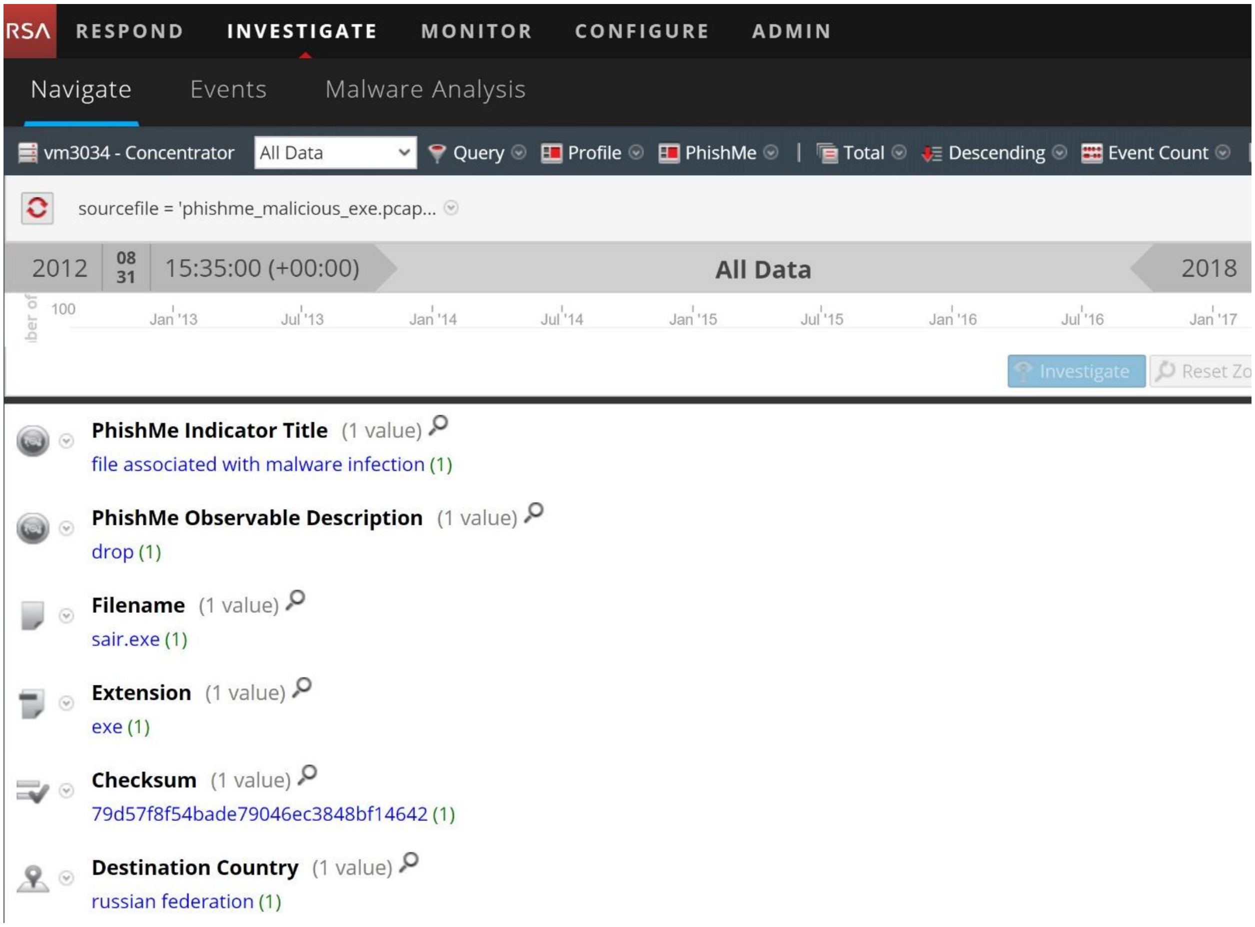
4	5 (index)	6 (index)	7	8	9
			url	**email**	
Observable Description	IP	Domain	URI	Email	F
			http://shtra.ca/978t6rve		
		the-agathon.com			
	109.203.104.133				
Drop					z
		speckftp.de			
		thenumastore.com			
Drop					l

Map any other relevant columns to either out of the box keys or custom keys you have added.

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 threat events, the meta will appear in RSA NetWitness Investigator:



sourcefile = 'phishme_malicious_exe.pcap...

PhishMe Indicator Title (1 value)
file associated with malware infection (1)

PhishMe Observable Description (1 value)
drop (1)

Filename (1 value)
sair.exe (1)

Extension (1 value)
exe (1)

Checksum (1 value)
79d57f8f54bade79046ec3848bf14642 (1)

Destination Country (1 value)
russian federation (1)

Certification Checklist for RSA NetWitness

Date Tested: February 2nd, 2018

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.5, 11.0	Virtual Appliance
PhishMe Intelligence	December 2017	Saas

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

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

Appendix A - Sample Custom Meta Keys

RSA NetWitness provides a number of out of the box keys that can be integrated with a custom feed such as threat.source, threat.category, threat.description, etc. If, however, you wish to create custom meta keys for use with a custom feed, such as PhishMe, you can do so following the instructions found here:

https://community.rsa.com/docs/DOC-80195

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.

```
<!-- *** Please insert your custom keys or modifications below this line *** -->

<key description="PhishMe Indicator Title" format="Text" level="IndexValues"
name="phish.title" valueMax="250000" defaultAction="Open"/>

<key description="PhishMe Observable Title" format="Text" level="IndexValues"
name="observ.title" valueMax="250000" defaultAction="Open"/>

<key description="PhishMe Observable Description" format="Text" level="IndexValues"
name="observ.desc" valueMax="250000" defaultAction="Open"/>
```