RSA® NETWITNESS®
Intel Feeds Implementation Guide

Soltra Edge 2.8

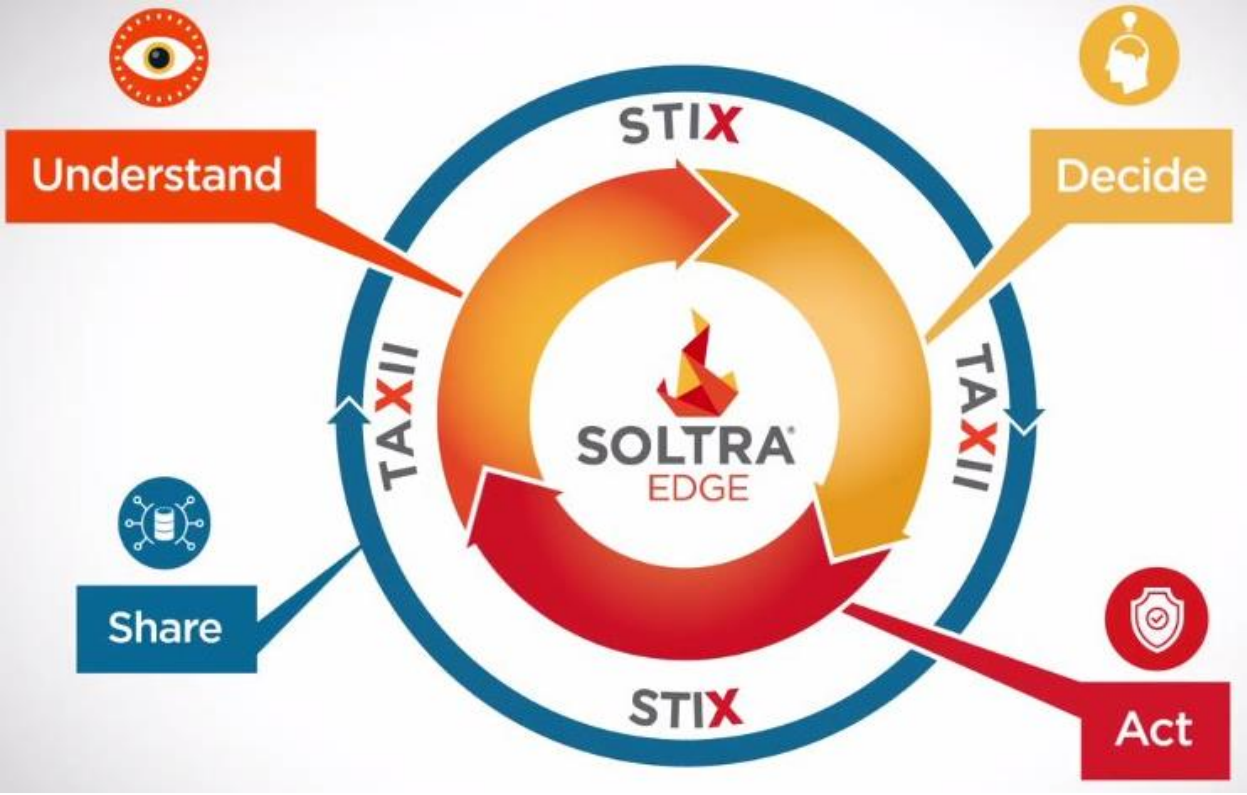
Jeffrey Carlson, RSA Partner Engineering
Last Modified: August 16th, 2016

RSA READY

Solution Summary

Soltra Edge takes large amounts of complex threat information across communities, people and devices and analyzes, prioritizes, and routes it to users in real-time. This enables seamless integration across security lifecycle solutions (threat intelligence, firewalls, intrusion detection, anti-virus, etc.) By leveraging the STIX standard, Soltra 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	
Soltra Edge 2.8	
Feed format	STIX
Collection method	http, local file
Feed Collection Frequency	Hourly, Daily, Weekly



Partner Product Configuration

Before You Begin

This section provides instructions for configuring Soltra Edge with RSA NetWitness. This document is not intended to suggest optimum installations or configurations.

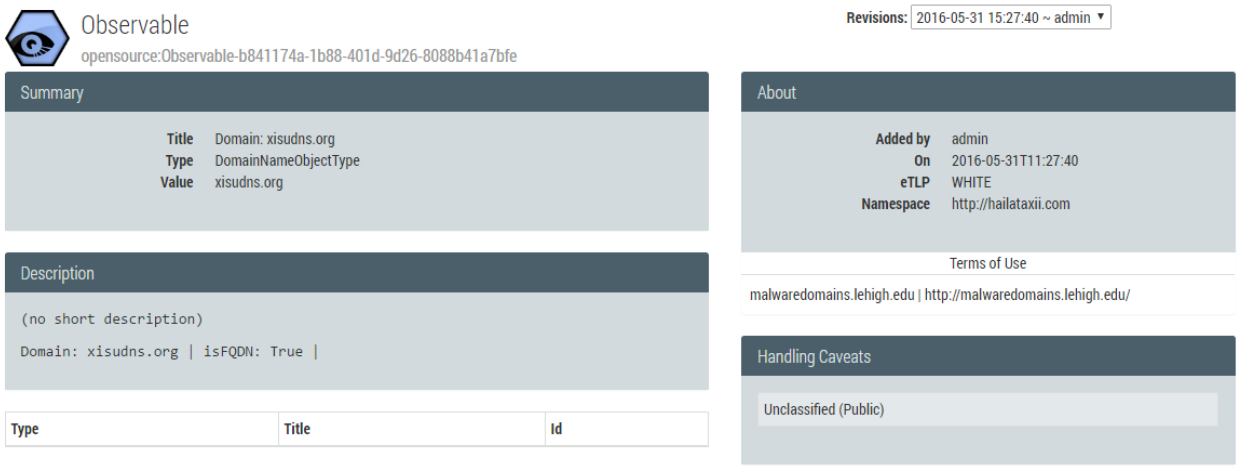
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Soltra Edge 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 environment. It is recommended that customers make sure Soltra Edge is properly configured and secured before deploying to a production environment. For more information, please refer to the Soltra Edge documentation or website.**

Soltra Edge Configuration

Soltra Edge integrates with RSA NetWitness via a STIX XML data feed. 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. Security analytics supports the import of STIX Indicators and STIX Observables:



STIX files can either be manually downloaded from Soltra Edge, or can also be generated via the Trusted Automated eXchange of Indicator Information (TAXII™) API. For more information on using the TAXII API, consult the Soltra Edge product docs which contains a Sample Python Client found here:

http://docs.soltra.com/edge-2/python-client-push-pull.html

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

NetWitness Concentrator Configuration

In order to add custom metadata entries for Soltra Edge, you will need to edit the **index-concentrator-custom.xml** file. This allows you to define additional custom fields that are specific to the data contained in your STIX feed file. **Appendix A** contains a sample entry, and demonstrates how custom keys can be defined. These entries correspond to the mapping table found in **Appendix B**.

For more information on the STIX support in RSA NetWitness, consult the RSA NetWitness Documentation found here:

http://sadocs.emc.com/0_en-us/088_SA106/31_LiveResMgmt/20_AddProc/MngCustFds/CrCustFd

Please note that this information is being provided for example only, so it is best to review and understand the material contained in the Appendix in order to make a determination as to which metadata keys are relevant for your organization.

For more information on making changes to the Concentrator configuration, consult the **Index Customization** section of the SA documentation at **http://sadocs.emc.com**

Important: Make sure to back up the index-concentrator-custom.xml file before making any changes, as improper XML syntax can cause the Concentrator services to fail on startup

Once you have made the necessary changes, restart the Concentrator and Packet Decoder.

RSA Security Analytics Custom Feed Configuration

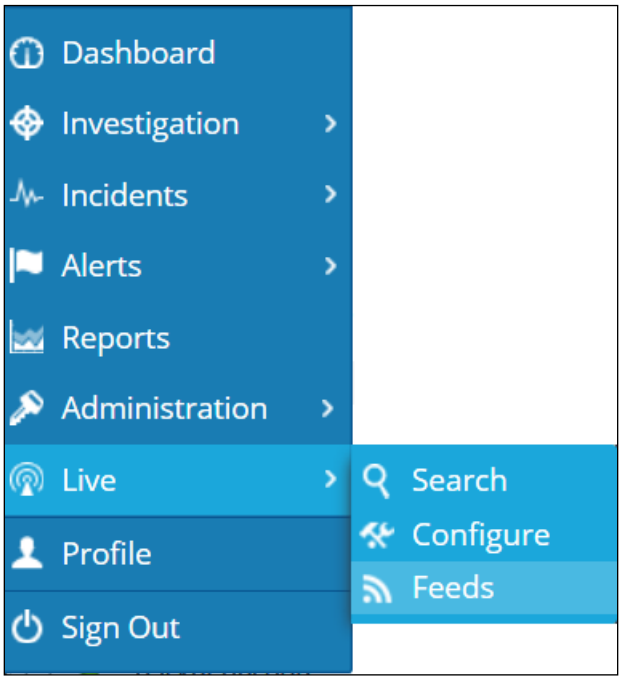
Depending on your deployment and if you have elected to add an RSA SA Log Decoder and/or Packet Decoder follow the steps below for your integration.

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

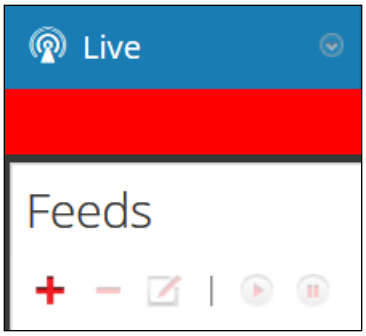
Packet Decoder Configuration

RSA Security Analytics Feed Configuration

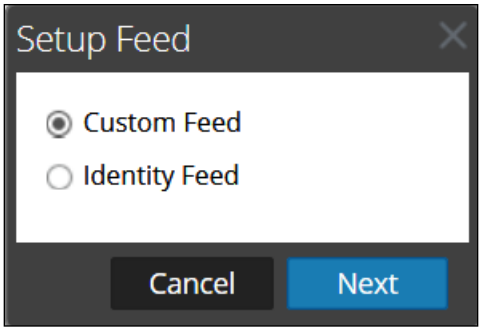
1. From the RSA SA Dashboard Select **Live**, **Feeds**.



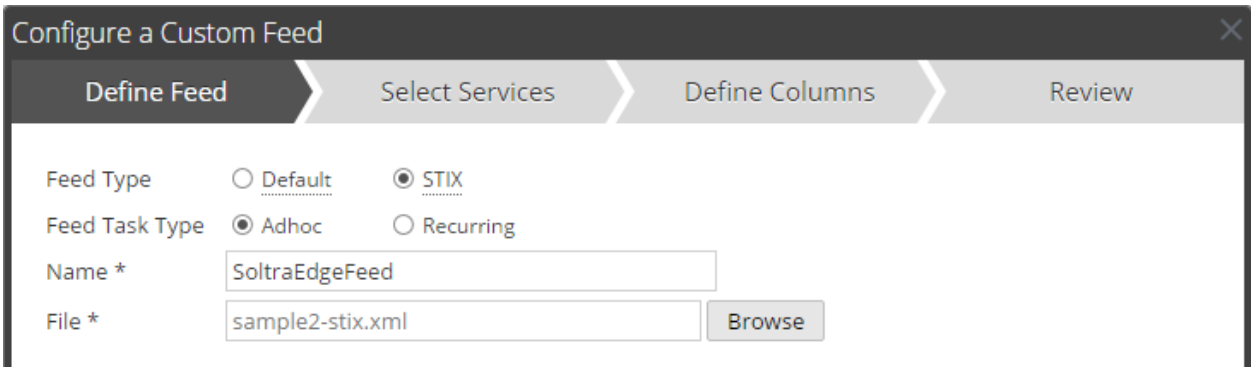
2. Select the + in the Live Feeds Window to setup the feed.



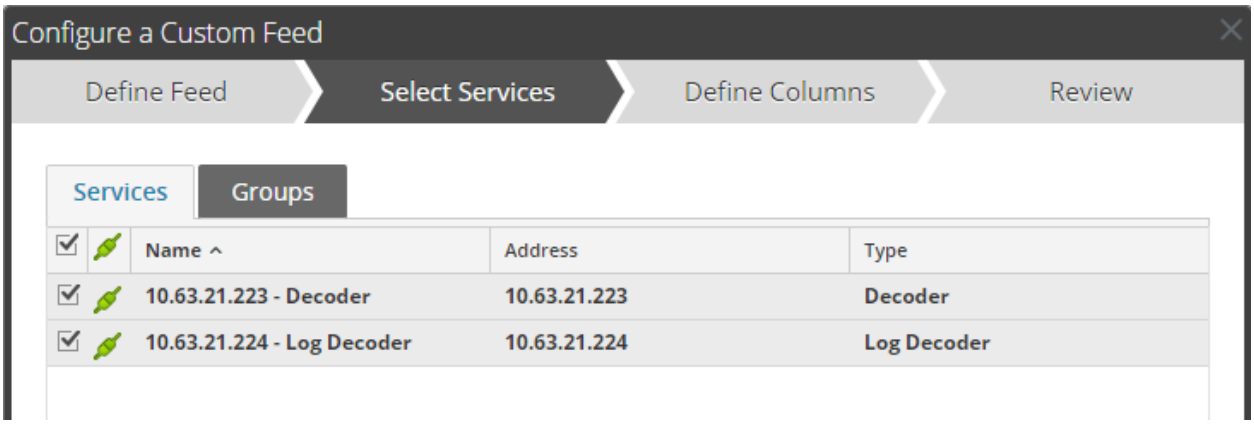
3. Select the **Custom Feed** radio button within the Setup Feed pop-up window and select **Next**.



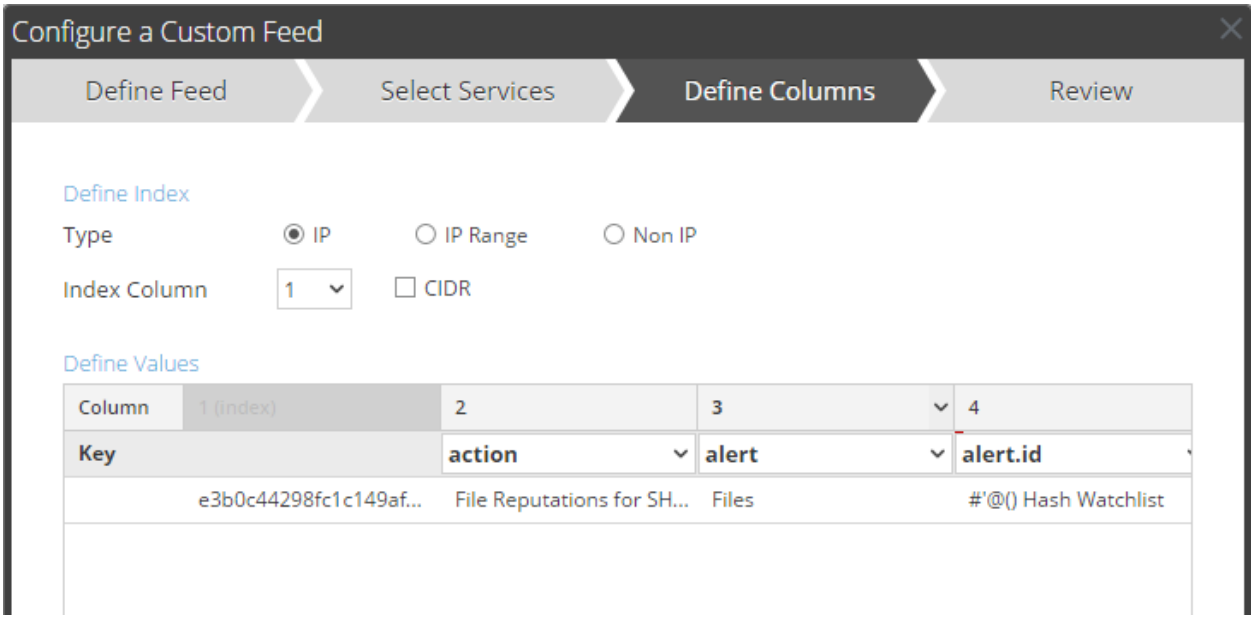
4. Select **STIX** as the Feed Type. Select **Adhoc** if you are uploading the file once or the **Recurring** radio button if you plan to automate the feed. Enter the **URL** of the Feed provider and select how often to pull the feed by setting the **Recur Every** option and select **Next**.



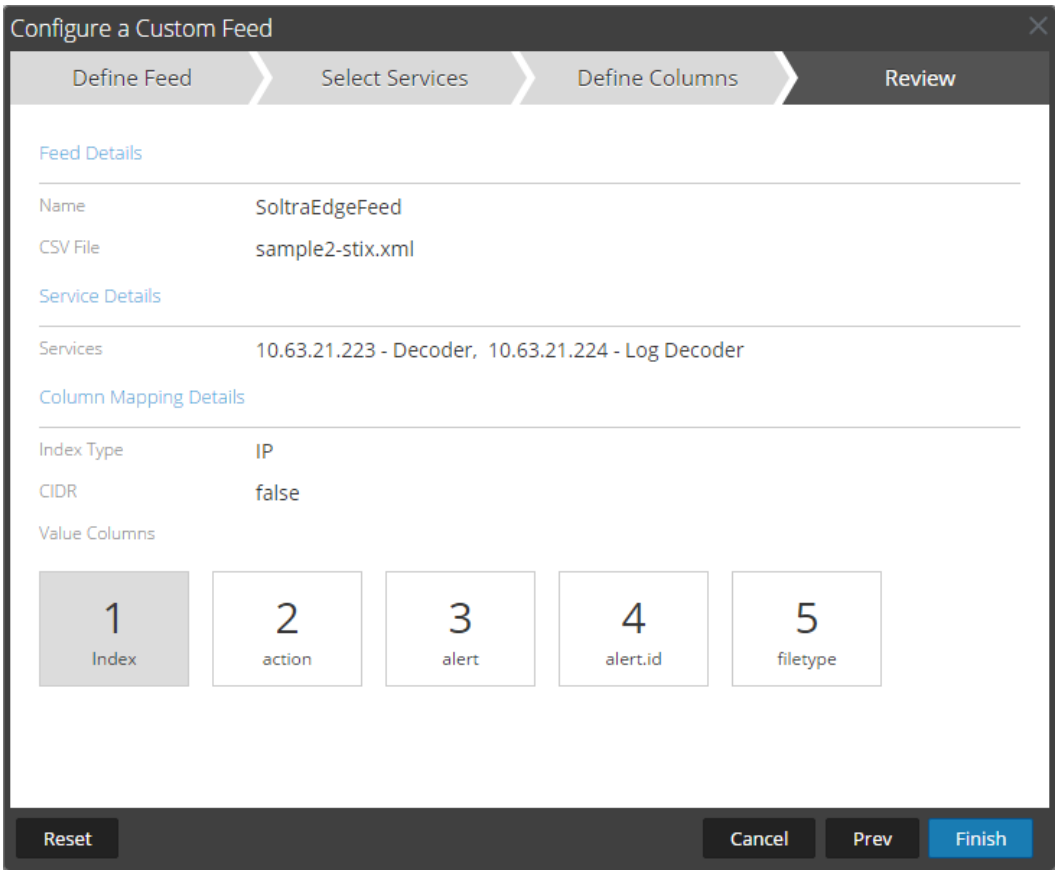
5. Select the **RSA SA Decoder Service checkbox** and select **Next**.



6. Define the Index as Type **Non IP**, **Index Column 1**. 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 SA 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 SA to download all Threat Intel from your provider.
9. Once completed and if you have any threat events, the meta will appear as normal text.

Certification Checklist for RSA NetWitness

Date Tested: July 4th, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.1	Virtual Appliance
Soltra Edge	2.8.1	Virtual Appliance

Security Analytics 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

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="Soltra Edge Title" format="Text" level="IndexValues"
name="sol.title" valuemax="250000" defaultAction="Open"/>

<key description="Soltra Edge Type" format="Text" level="IndexValues"
name="sol.type" valuemax="250000" defaultAction="Open"/>

<key description="Soltra Edge Indicated TTP" format="Text"
level="IndexValues" name="sol.indic.ttp" 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.

Soltra Fields	SA Meta	Custom Meta
Hash	**index**	
Soltra Edge Title		sol.title
Soltra Edge Type		sol.type
Soltra Edge Indicated TTP		sol.indic.ttp