RSA® NETWITNESS®
Intel Feeds Implementation Guide

Anomali STAXX 3.0

Jeffrey Carlson, RSA Partner Engineering
Last Modified: 09/28/2017

RSA READY

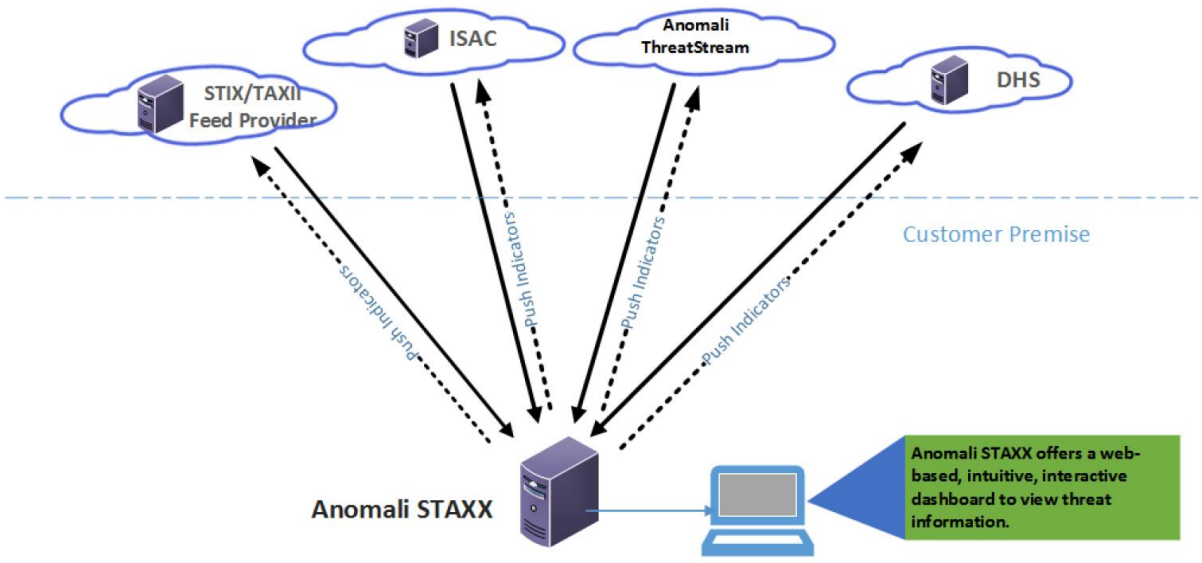
Solution Summary

Anomali STAXX is a free client that lets you access any STIX or TAXII compatible threat intelligence. STAXX can connect to any public, community or paid third-party source. You can also import threat intelligence into Anomali STAXX and push (upload) selected observables to other STIX/TAXII servers.

Anomali STAXX includes an easy-to-use interface to view threat information received through STIX/TAXII feeds in interactive dashboards, as shown in the following figure. You can run a keyword search to look for a specific observable, search for an observable type over a time range of your choice, and drill-down to any of the Anomali platforms—Anomali STAXX, Anomali Reports, Anomali ThreatStream—to investigate the observable further. You can also import observables, export search results, and push observables to other STIX/TAXII servers from these dashboards.

By integrating Anomali STAXX with RSA NetWitness, organizations can consolidate threat data and bring a consolidated feed into RSA NetWitness for alerting and enrichment.

RSA NetWitness Features	
Anomali STAXX 3.0	
Feed format	csv (via python script)
Collection method	http or file
Feed Collection Frequency	as needed



Partner Product Configuration

Before You Begin

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

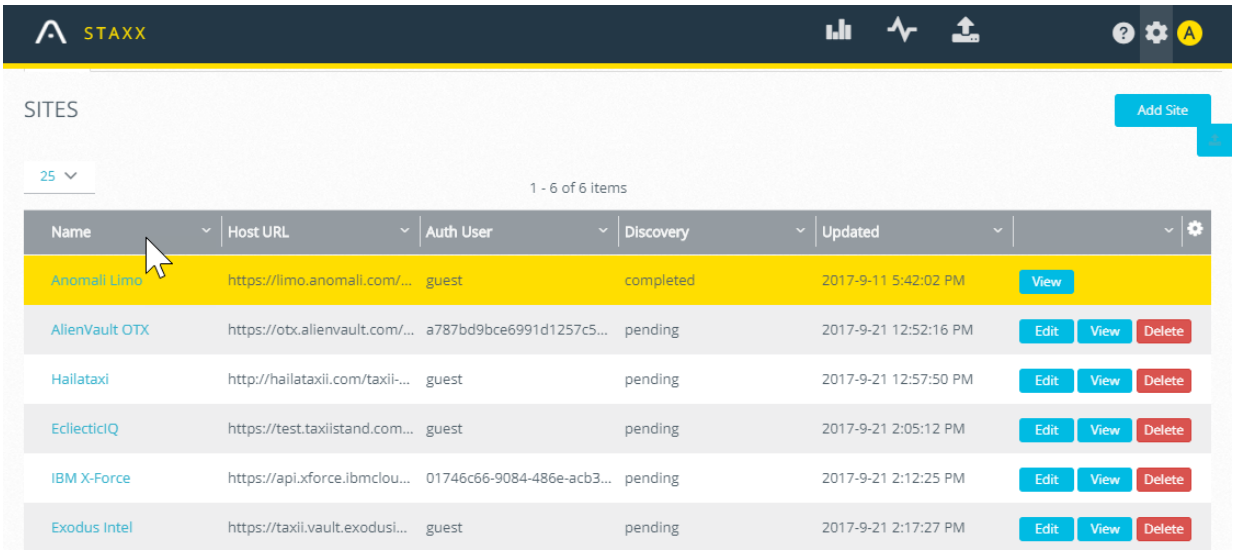
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All STAXX 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 Anomali STAXX is properly configured and secured before deploying to a production environment. For more information, please refer to the Anomali STAXX documentation or website.**

Anomali STAXX Configuration

After installing and configuring the Anomali STAXX virtual machine, you can select an initial TAXII service other than Anomali Limo. The wizard will step you through the manual feed configuration process. Once you have configured a number of TAXII servers, you should see them listed from the **SITES** section of the STAXX settings:



Once data has been ingested from the various threat intelligence sources, you will see data in the dashboards of the Anomali STAXX web interface. The dashboards allow you to view and interactively search for threat observables received through the threat feeds, and investigate an observable on Anomali's platforms for deeper insights.

The Anomali STAXX Dashboard provides a summary of all observables stored on Anomali STAXX in the specified time period. Several graphical views within Dashboard show observables by observable type, severity, source (of the observable), confidence, and so on.

Exporting Data from Anomali STAXX

Anomali STAXX is essentially a TAXII client and not a TAXII server. Since RSA NetWitness does not currently support TAXII, it is necessary to use the STAXX API to export a filtered set of data from STAXX, and output a CSV file for use as a feed in RSA NetWitness.

On the Anomali Forums website, there is a sample python script that queries the STAXX API and pulls down data, which can be found here:

https://forum.anomali.com/t/python-sample-script-staxx-api/1020

An example script, which has been modified to work with RSA NetWitness (anomali-staxx.py.zip) is provided as part of this integration.

! Important: The anomali-staxx.py script file is provided for example only. It may need to be modified to fit the needs of your organization.

The filter in the included script looks for the following criteria to reduce the data brought in to just what is required and relevant:

```
query = "(severity=medium OR severity=high OR severity=very-high) AND
itype='mal_ip'"
```

This query can be updated to include indicators that are relevant to what you are trying to accomplish.

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 Threat Intel Metakeys

As part of this integration, you may want to add a few more metakeys that could be useful for use specifically with threat intel data to bring more context to events.

For example, these metakeys can be added to the **index-concentrator-custom.xml**:

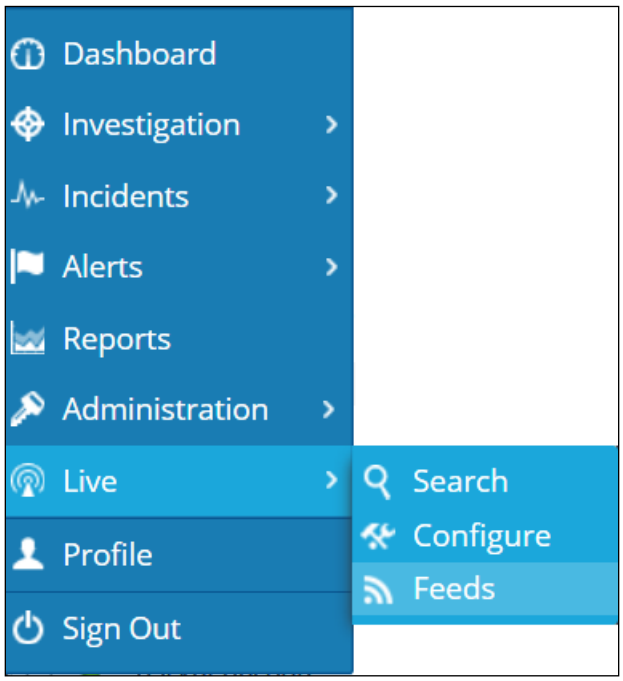
```
<key description="Intel Date" level="IndexValues" name="intel.date"
format="UInt32" valueMax="5000" defaultAction="Closed"/>
<key description="Intel Confidence" level="IndexValues" name="intel.conf"
format="Text" valueMax="5000" defaultAction="Closed"/>
<key description="Intel ID" level="IndexValues" name="intel.id" format="Text"
valueMax="5000" defaultAction="Closed"/>
<key description="Intel TLP" level="IndexValues" name="intel.tlp"
format="Text" valueMax="100" defaultAction="Closed"/>
<key description="Intel Type" level="IndexValues" name="intel.type"
format="Text" valueMax="100" defaultAction="Closed"/>
```

For more information on working with custom keys, visit the RSA NetWitness documentation at:

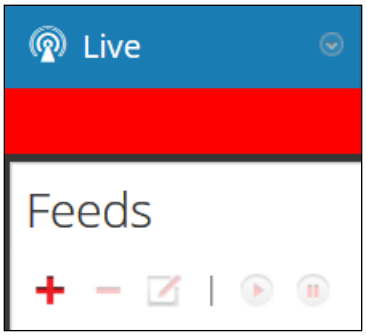
https://community.rsa.com/docs/DOC-78049

RSA NetWitness Analytics Feed Configuration

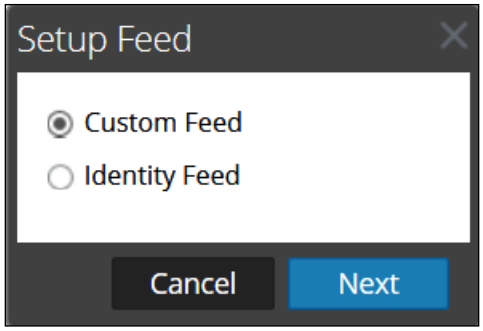
1. From the RSA NetWitness Dashboard Select **Live**, **Feeds**.



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



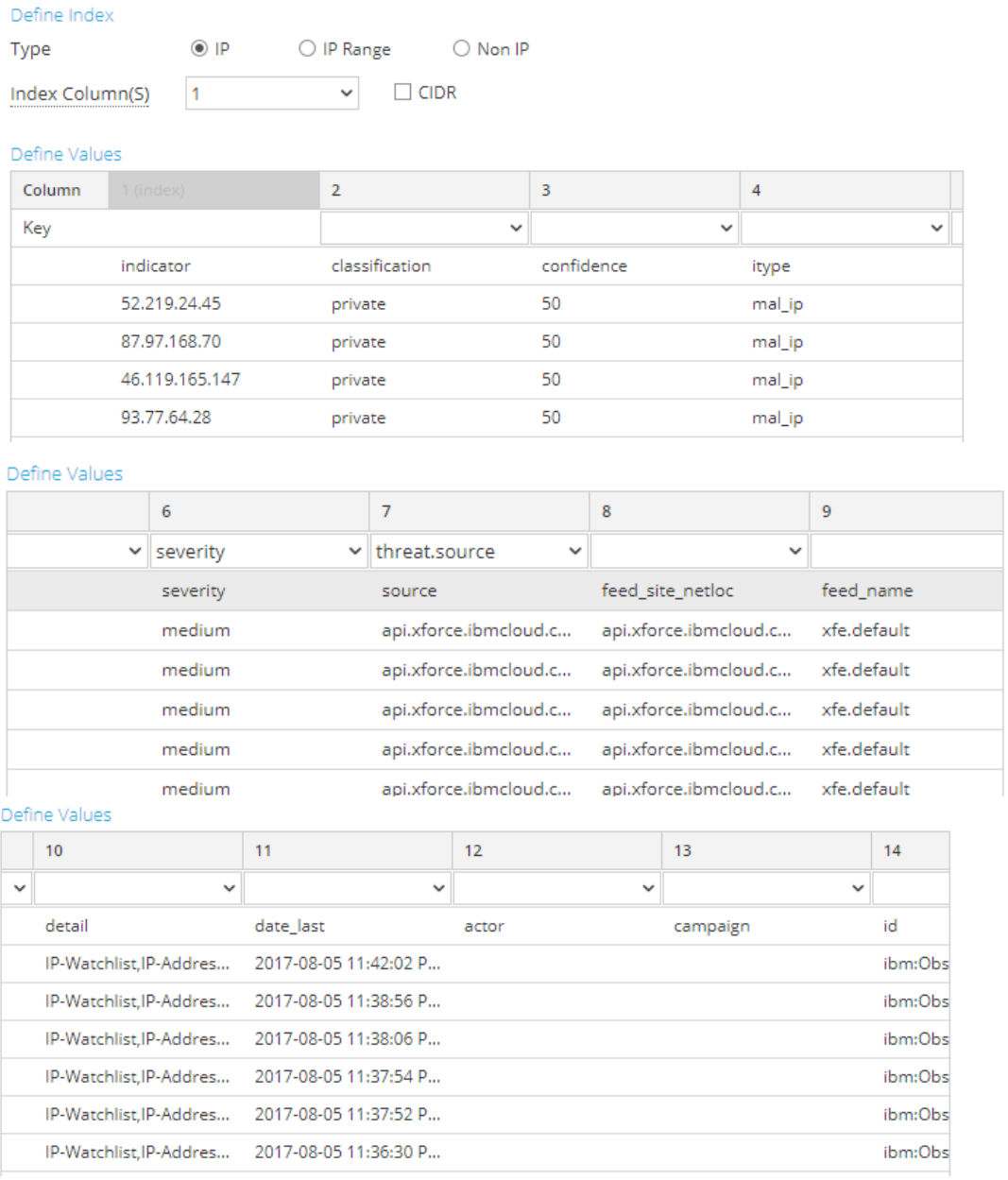
3. Select the **Custom Feed** radio button within the Setup Feed pop-up window and select **Next**.



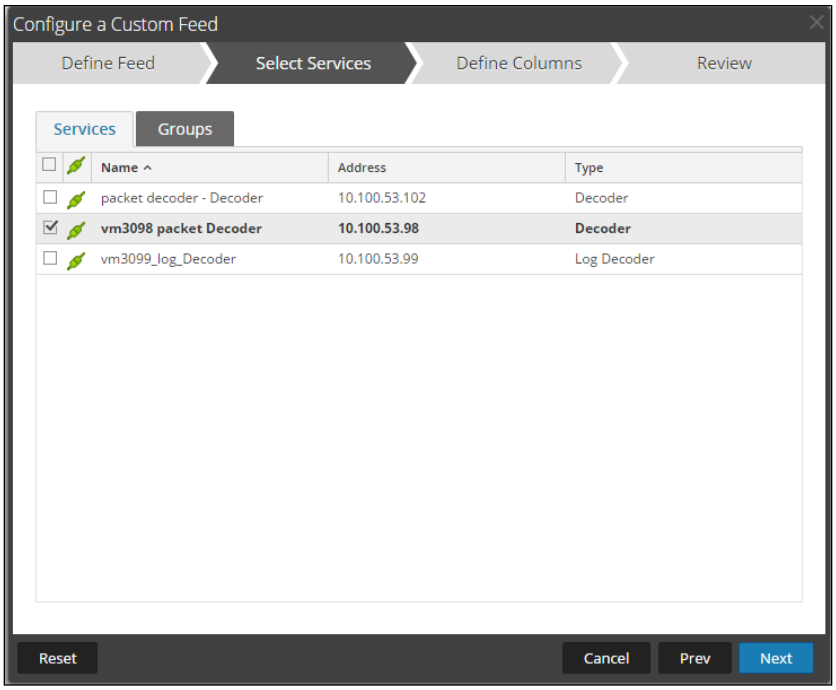
4. Set the recurrence options for the feed. The .csv file can either hosted locally on the web root directory or on a remote web server.

5. The mappings for this example are as follows:

   ip - column 1
   threat.category - itype
   severity - severity
   threat.source - source
   intel.tlp - tlp



6. Select the RSA NetWitness Packet Decoder Service checkbox 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**.

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

direction : outbound
threat.category : mal_ip
severity : medium
threat.source : api.xforce.ibmcloud.com:xfe.default
intel.tlp : TLP:WHITE

Certification Checklist for RSA NetWitness

Date Tested: September 22nd, 2017

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.4	Virtual Appliance
Anomali STAXX	3.0	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