RSA® NETWITNESS®
Intel Feeds
Implementation Guide

Symantec DeepSight™ Intelligence

Jeffrey Carlson, RSA Partner Engineering
Last Modified: June 17th, 2016

RSA READY

Solution Summary

Actionable intelligence provides the necessary context and technical details surrounding a threat so teams can quickly assess cyber risk and implement proactive controls. Stay ahead of evolving threats with curated threat intelligence by DeepSight experts. Experienced teams harness the visibility provided by the Symantec Global Intelligence Network, the largest civilian threat collection network and track over 700,000 global adversaries worldwide. By making DeepSight Intelligence available as a custom feed within RSA NetWitness, organizations can defend themselves against an increasingly diverse set of threats while managing an ever-expanding universe of devices, users and data all fluidly entering and leaving the network

RSA NetWitness Features	
Symantec DeepSight Intelligence	
Feed format	csv
Collection method	http, local file
Feed Collection Frequency	Hourly, Daily, Weekly

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Symantec DeepSight 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.

> **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 every customer environment. It is recommended that customers make sure Symantec DeepSight is properly configured and secured before deploying to a production environment. For more information, please refer to the Symantec DeepSight documentation or website.**

Symantec DeepSight Configuration

Symantec DeepSight integrates with RSA NetWitness via a .csv data feed. DeepSight provides a number of feeds in .csv format, such as IP Reputation, URL Reputation, Advanced IP Reputation, and Advanced Domain/URL Reputation. For the purposes of this guide, the **Advanced IP Reputation** feed is being used, but other feeds could be used in much the same manner, depending on the requirements of your organization.

> **Important: You will need to remove any commas from field entries in the .csv file. Please see the Known Issues section of this guide for more information.**

Datafeed files can be downloaded from DeepSight in a number of different ways, such as manually downloading them from the DeepSight Portal, via a Python script, or via the DeepSight Web Services API. Choose the method that works best for your organization. These files will need to be made available to RSA NetWitness via a one-time upload, or hosted on an HTTP Server if the feed is setup as a recurring feed.

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 Concentrator Configuration

In order to add custom metadata entries for Symantec DeepSight, 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 .csv 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**.

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 NetWitness documentation at **http://sadocs.emc.com**

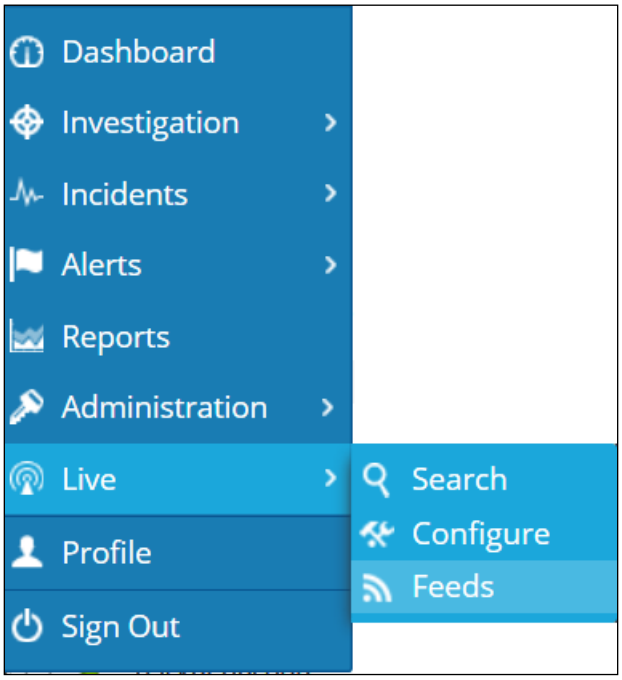
> **! Important: Make sure to back up the index-concentrator-custom.xml file before making any changes, as improper XML syntax can cause the Concentrator services to fail on startup**

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

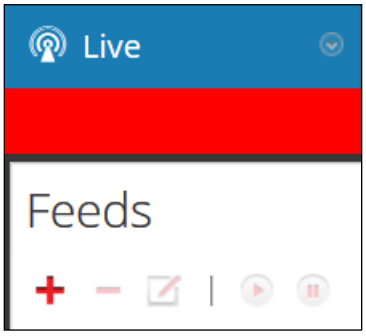
RSA NetWitness Packet Decoder Configuration

RSA NetWitness Feed Configuration

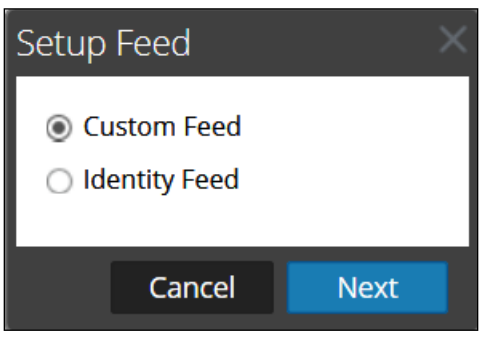
1. From the RSA NetWitness Dashboard Select **Live**, **Feeds**.



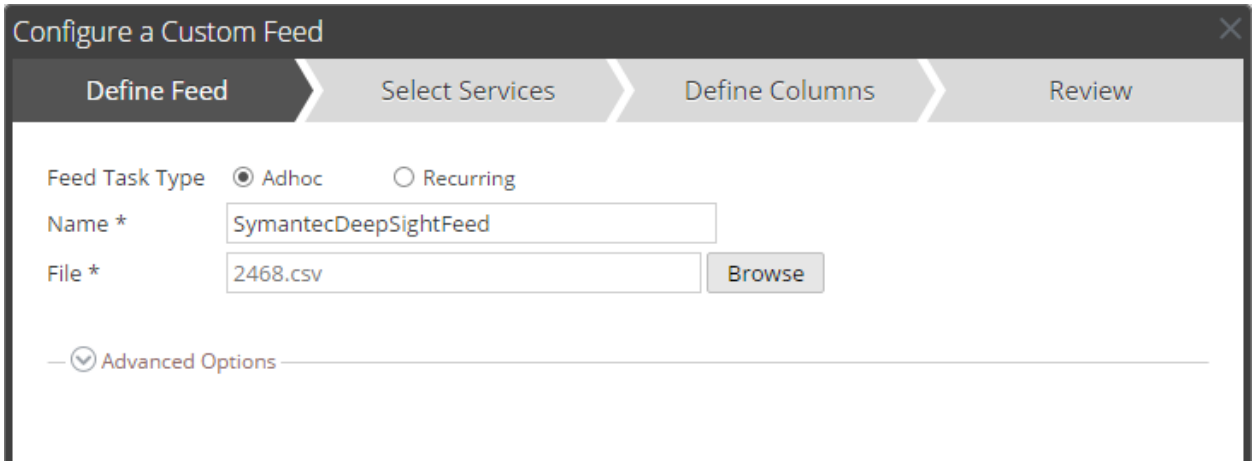
2. Select the + in the Live Feeds Window to setup the feed.



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

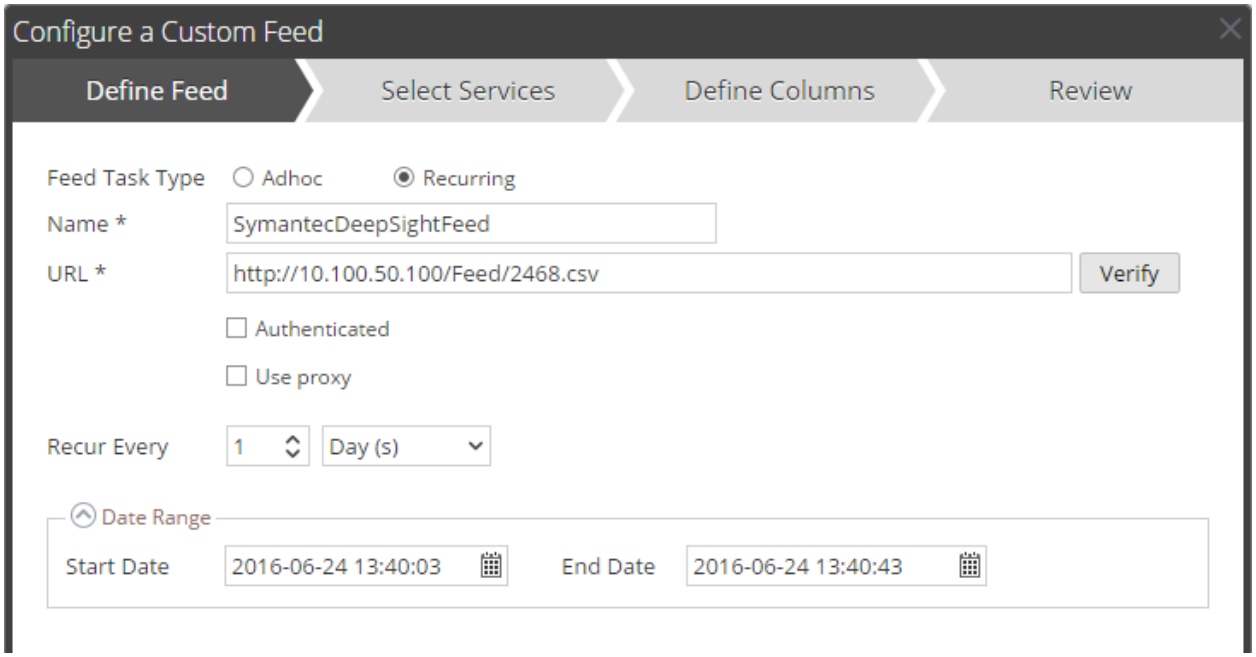


4. Select **Adhoc** if you are uploading the file once or the **Recurring** radio button if you plan to automate the feed.

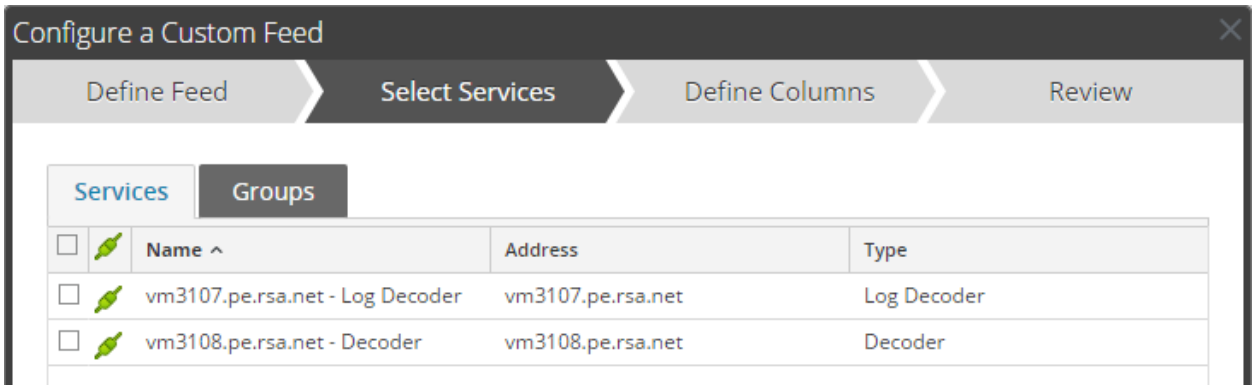


Note that if the feed will be recurring, you will need to host the .csv on an HTTP server and keep it updated via a script or some other means.

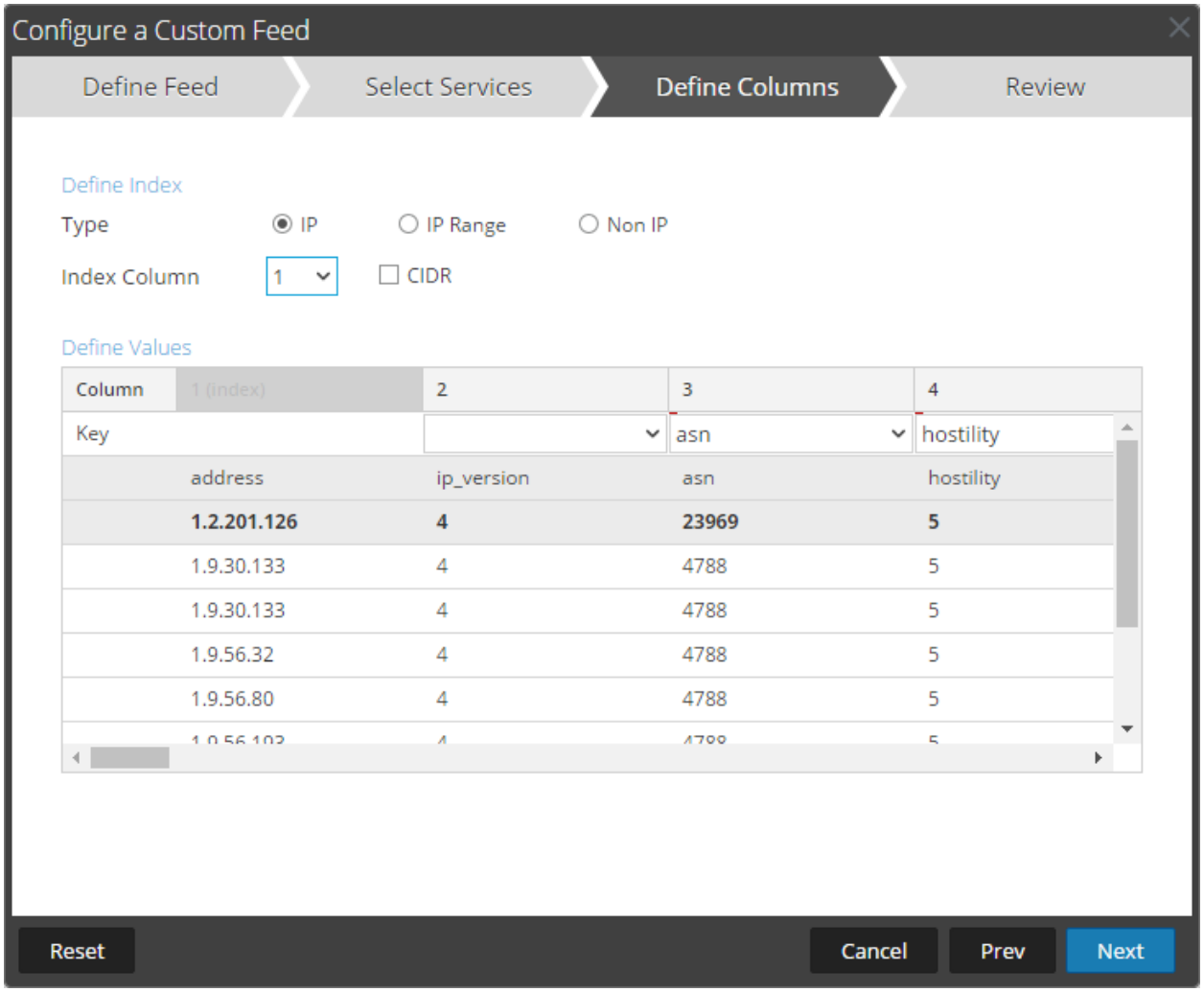
5. Enter the **URL** of the file location and select how often to pull the feed by setting the **Recur Every** option and select **Next**.



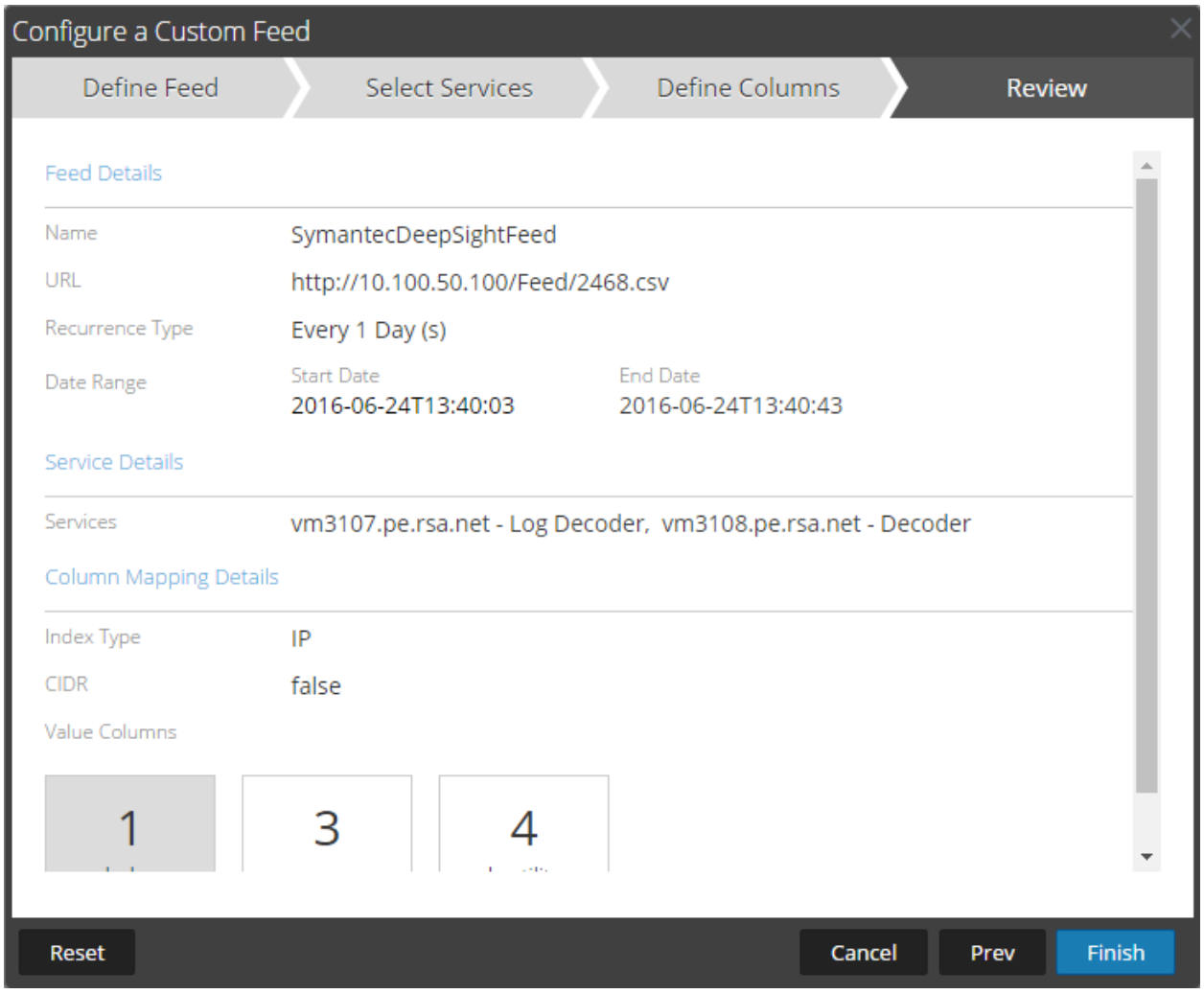
6. Select the RSA NetWitness Packet Decoder Service checkbox and select **Next**.



7. Define the **Type** as **IP** and **Index Column 1** (IP Address Field). Set the header of each column as needed. If the custom keys you have added are not available from the drop-down list, type them in. An example mapping table is provided in **Appendix B**. Select **Next** to continue.



8. Select **Finish**, to complete the setup of the Feed Integration.



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 a while for RSA NetWitness to download all Threat Intel from your provider.

9. Once the feed has completed, you should see additional metadata provided by Symantec DeepSight when perfoming an investigation if there is a match on an IP address contained in the feed file:

Certification Checklist for RSA NetWitness

Date Tested: June 22nd, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6	Virtual Appliance
Symantec DeepSight	June 2016 release	DeepSight Intelligence Portal

RSA NetWitness 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

Known Issues

When exporting a .csv feed from DeepSight, you will need to make sure that all commas have been removed from any field entries, or this will cause issues with the feed import. For example, if an organization is listed as "CompanyName, LLC", then it would be broken into two different fields – "CompanyName" and "LLC" which will interfere with the intended metadata mappings. To rectify this, remove the commas via a global find and replace or via a script that performs this function.

In the provided examples in Appendix A and Appendix B, dates have been excluded, as the native datatype for dates in NetWitness is "TimeT", which is a Unix epoc timestamp. DeepSight dates are provided in a standard MM/DD/YYYY format. If calculations or rules are not needed for dates, then they could potentially be imported as the "Text" datatype.

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="DeepSight ASN" format="Text" level="IndexValues" name="asn"
valuemax="250000" defaultAction="Open"/>

<key description="DeepSight Hostility" format="Text" level="IndexValues"
name="hostility" valuemax="250000" defaultAction="Open"/>

<key description="DeepSight Confidence" format="Text" level="IndexValues"
name="confidence" valuemax="250000" defaultAction="Open"/>

<key description="DeepSight Reputation Rating" format="Int32"
level="IndexValues" name="rep.rating" valuemax="250000"
defaultAction="Open"/>

<key description="DeepSight Organization Type" format="Text"
level="IndexValues" name="org.type" valuemax="250000" defaultAction="Open"/>

<key description="DeepSight NAICS" format="Text" level="IndexValues"
name="naics" valuemax="250000" defaultAction="Open"/>

<key description="DeepSight ISIC" format="Text" level="IndexValues"
name="isic" valuemax="250000" defaultAction="Open"/>

<key description="DeepSight Carrier" format="Text" level="IndexValues"
name="carrier" valuemax="250000" defaultAction="Open"/>

<key description="DeepSight Connection Type" format="Text"
level="IndexValues" name="conn.type" valuemax="250000" defaultAction="Open"/>

<key description="DeepSight Line Speed" format="Text" level="IndexValues"
name="line.speed" valuemax="250000" defaultAction="Open"/>

<key description="DeepSight IP Routing" format="Text" level="IndexValues"
name="ip.routing" valuemax="250000" defaultAction="Open"/>

<key description="DeepSight Anonymizer Status" format="Text"
level="IndexValues" name="anon.status" valuemax="250000"
defaultAction="Open"/>

<key description="DeepSight Proxy Type" format="Text" level="IndexValues"
name="proxy.type" valuemax="250000" defaultAction="Open"/>

<key description="DeepSight Proxy Level" format="Text" level="IndexValues"
name="proxy.level" valuemax="250000" defaultAction="Open"/>

<key description="DeepSight Top Level Domain" format="Text"
level="IndexValues" name="top.lvl.dom" valuemax="250000"
defaultAction="Open"/>

<key description="DeepSight Second Level Domain" format="Text"
level="IndexValues" name="sec.lvl.dom" valuemax="250000"
defaultAction="Open"/>

<key description="DeepSight Attack Name" format="Text" level="IndexValues"
name="attack.name" valuemax="250000" defaultAction="Open"/>
```

```
<key description="DeepSight Attack Category" format="Text"
level="IndexValues" name="attack.category" valuemax="250000"
defaultAction="Open"/>

<key description="DeepSight Attack Description" format="Text"
level="IndexValues" name="attack.desc" valuemax="250000"
defaultAction="Open"/>

<key description="DeepSight Uniquedomains Count Name" format="Int32"
level="IndexValues" name="domain.count" valuemax="250000"
defaultAction="Open"/>

<key description="DeepSight Registration Person" format="Text"
level="IndexValues" name="regist.person" valuemax="250000"
defaultAction="Open"/>

<key description="DeepSight Registration Email" format="Text"
level="IndexValues" name="regist.email" valuemax="250000"
defaultAction="Open"/>

<key description="DeepSight Registration Organization" format="Text"
level="IndexValues" name="regist.org" valuemax="250000"
defaultAction="Open"/>

<key description="DeepSight Registration City" format="Text"
level="IndexValues" name="regist.city" valuemax="250000"
defaultAction="Open"/>

<key description="DeepSight Registration Country" format="Text"
level="IndexValues" name="regist.country" valuemax="250000"
defaultAction="Open"/>

<key description="DeepSight Registration Registrar" format="Text"
level="IndexValues" name="regist.registrar" valuemax="250000"
defaultAction="Open"/>

<key description="DeepSight Registration Nameservers" format="Text"
level="IndexValues" name="regist.namesrv" valuemax="250000"
defaultAction="Open"/>

<key description="DeepSight Url Count" format="Int32" level="IndexValues"
name="url.count" valuemax="250000" defaultAction="Open"/>

<key description="DeepSight Url" format="Text" level="IndexValues"
name="ds.url" 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.

Symantec Fields	NetWitness Meta	Custom Meta
address	**index**	
ip_version		
asn		asn
hostility		hostility
confidence		confidence
consecutive_listings		
listing_ratio		
reputation_rating		rep.rating
first_seen		
last_seen		
attack_names_count		
organization_name	org.dst	
organization_type		org.type
naics		naics
isic		isic
continent		
country	country.dst	
country_code		
region		
state		
city	city.dst	
postal_code		
area_code		
time_zone		
latitude	latdec.dst	
longitude	longdec.dst	
carrier		carrier
connection_type		conn.type
line_speed		line.speed
ip_routing		ip.routing
anonymizer_status		anon.status
proxy_type		proxy.type
proxy_level		proxy.level
proxy_last-detected		
top-level_domain		top.lvl.dom

second-level_domain		sec.lvl.dom
attack_name		attack.name
attack_category		attack.cat
attack_description		attack.desc
uniquedomains_count		domain.count
domain_name	domain.dst	
registration_person		regist.person
registration_email		regist.email
registration_organization		regist.org
registration_city		regist.city
registration_state		
registration_postal_code		
registration_country		regist.country
registration_create_date		
registration_update_date		
registration_registrar		regist.registrar
registration_nameservers		regist.namesrv
url_count		url.count
url		ds.url