RSA® NETWITNESS®
Security Operations Implementation Guide

CyberSponse CyOps 4.9

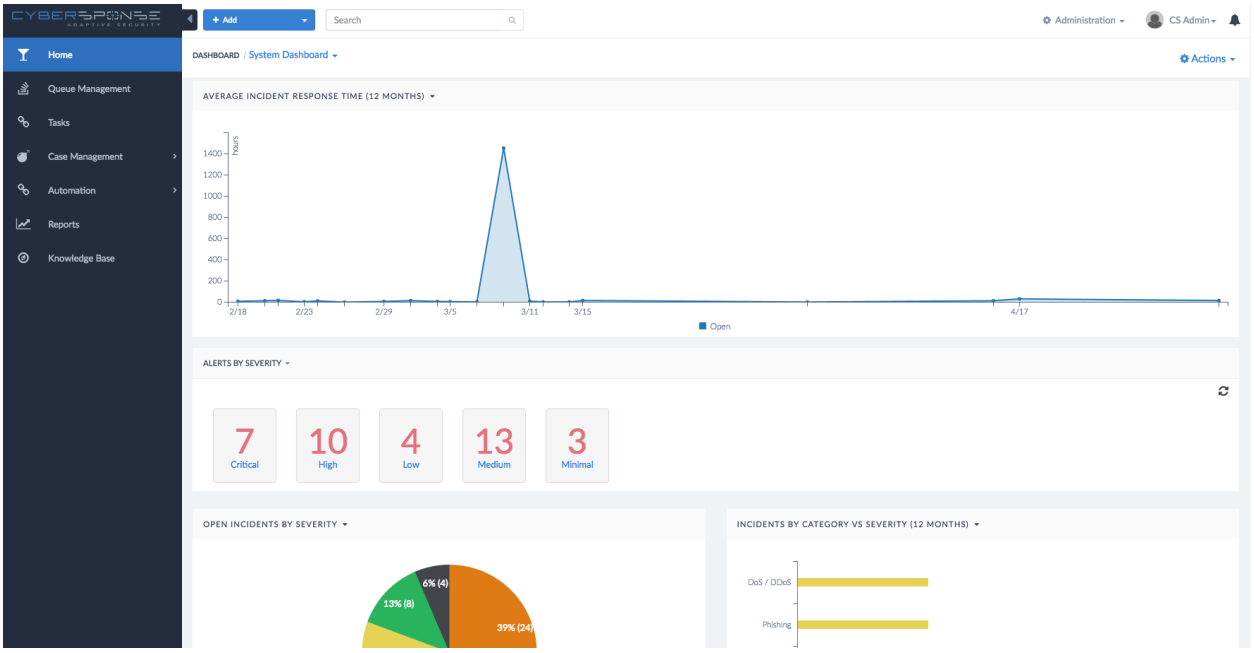
Jeffrey Carlson, RSA Partner Engineering
Last Modified: 07/22/2017

RSA READY

Solution Summary

CyberSponse CyOps integrates with RSA NetWitness to automate the collection of evidence related to a given security alert/incident and to make that data actionable to an incident responder. CyberSponse leverages the NetWitness REST API to query for meta data and/or PCAPs associated to a user, ip, or domain. The information gathered from NetWitness is then used in automated workflows that enable incident responders or analysts to quickly remediate incidents based on the data gathered. CyberSponse also provides the ability to leverage custom NetWitness queries to gather meta and/or PCAPs and store them in CyberSponse.

Deployment is as simple as configuring your NetWitness concentrator connection details in CyberSponse and enabling one or more available CyberSponse playbooks.



Partner Product Configuration

Before You Begin

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

CyberSponse CyOps Configuration

Configuring access to RSA NetWitness in CyberSponse requires configuring two components: connectors and playbooks. Connectors are the integration points that allow you to interact with NetWitness programmatically. Playbooks enable you to use the data sent to and retrieved from the connector in workflows.

Connectors are essentially APIs, while playbooks are the area users spend time implementing their processes.

It is recommended to create a NetWitness user that has API access permissions before configuring the connector.

Configuring Connectors

1. Login to CyberSponse and go to **Automation**->**Connectors**.
2. Click **Configure** next to the RSA NetWitness Connector (*figure 2 below*)
3. Create a new Connector Configuration (*figure 3 below*):
    a. Create a unique **Configuration Name.**
    b. Input an **Address**. (Normally a broker or concentrator).
    c. Input your **Username**.
    d. Input your **Password**.
    e. Input your RSA NetWitness API **Port**.

f. Input the **protocol** your API uses (http/https).

g. Check the box for **Verify SSL** if you have valid certificates on your RSA NetWitness appliance.

4. Click **Next**.
5. Disable any RSA NetWitness actions you don't want exposed to playbooks (*figure 4 below*).
6. Click **Update**.

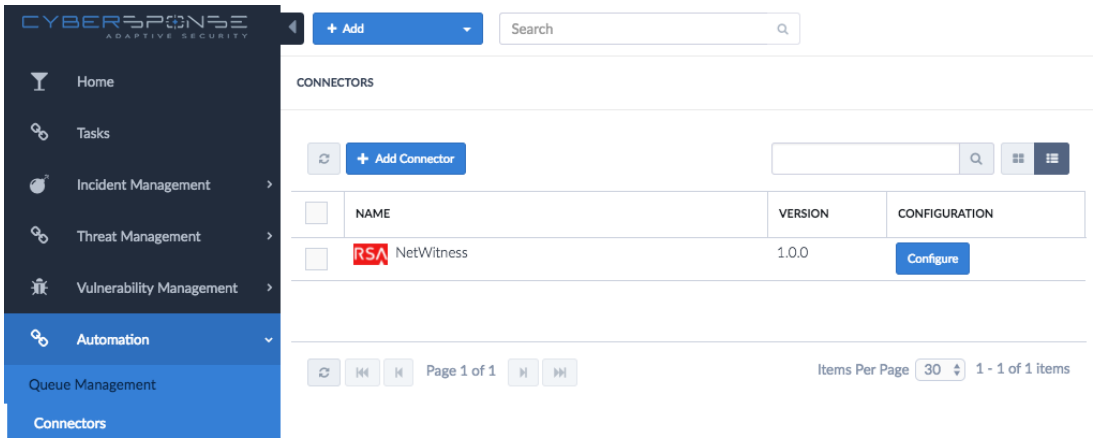


Figure 1 - Configuring credentials in the encrypted container

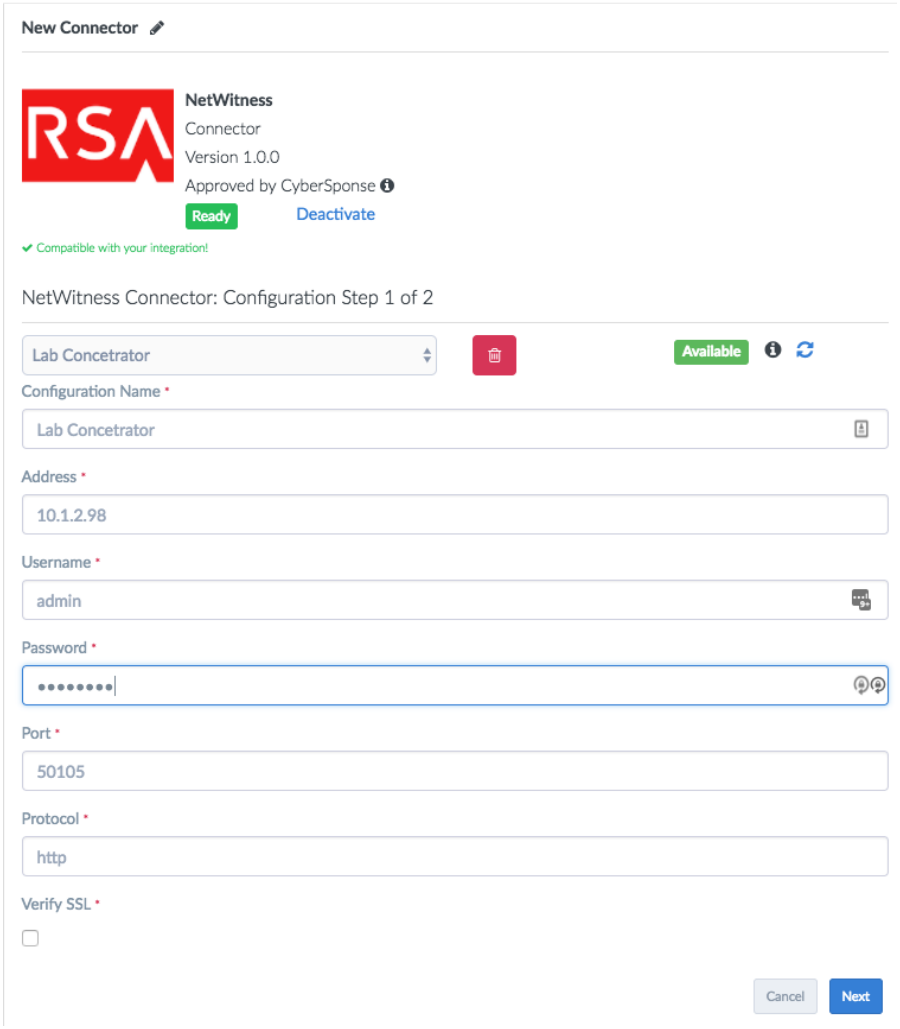


Figure 3 – Example RSA NetWitness Connector Configuration

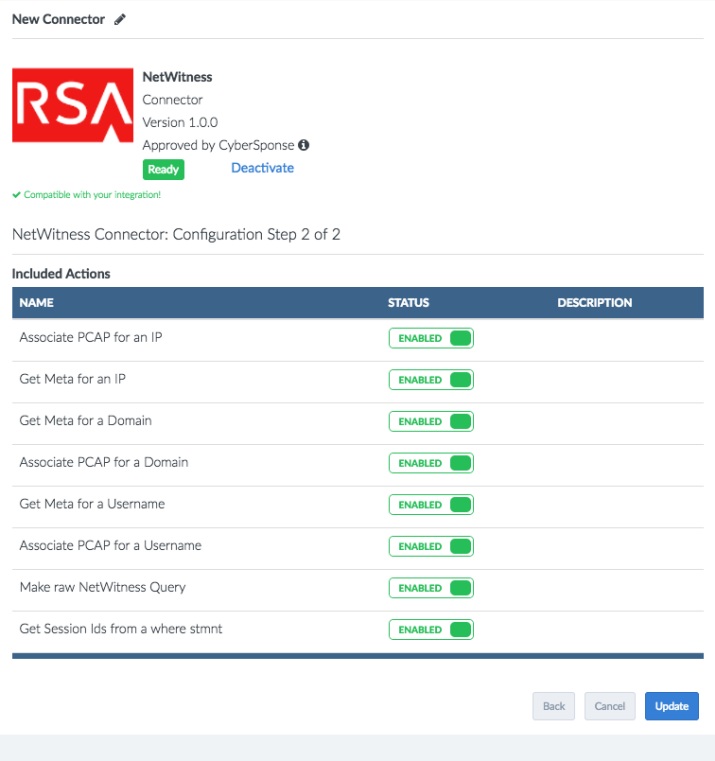


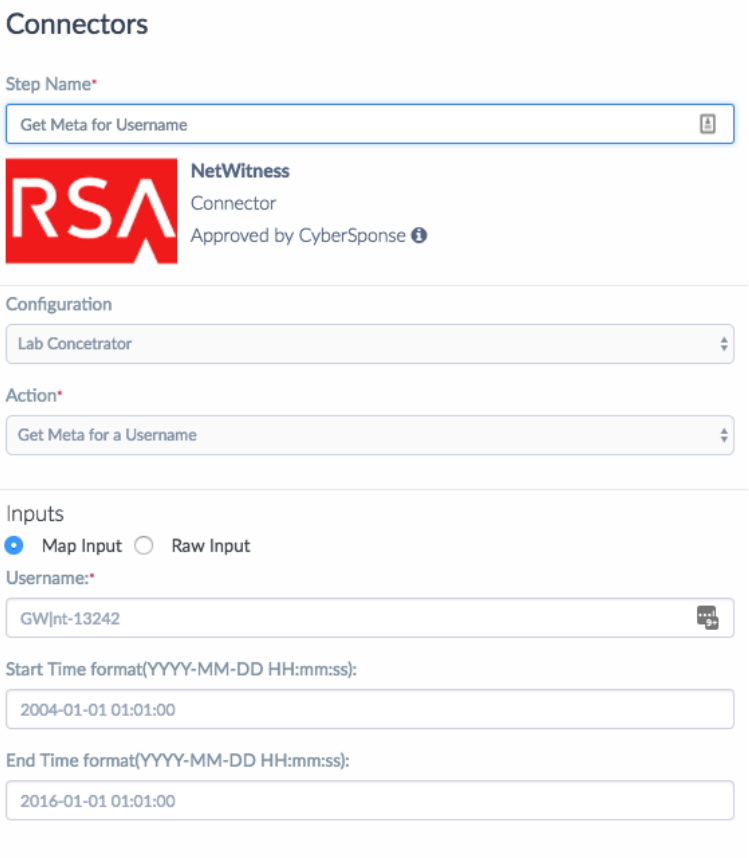
Figure 4 – RSA NetWitness Connector Actions

Using Connector Actions

Example playbooks for each connector action are pre-installed with the connector for quick customization, or to use as templates for custom playbooks. To view them:

1. Go to **Automation->Playbooks**.
2. Click on **NetWitness**.
3. Playbook Connector overview (*see figure 5 below*):
    a. **NetWitness Meta from Username** (Connector Action: **Get Meta for a Username**)
        i. **Username** (Required) – The username to search for.
        ii. **Start Time (**Optional) – The start time for the search.
        iii. **End Time (**Optional) – The end time for the search.

    NOTE: If start time and end time are not supplied, the search is run for 24 hours prior to the time it is executed.



b. **NetWitness PCAP from IP** (Connector Action: **Associate PCAP for an IP**)

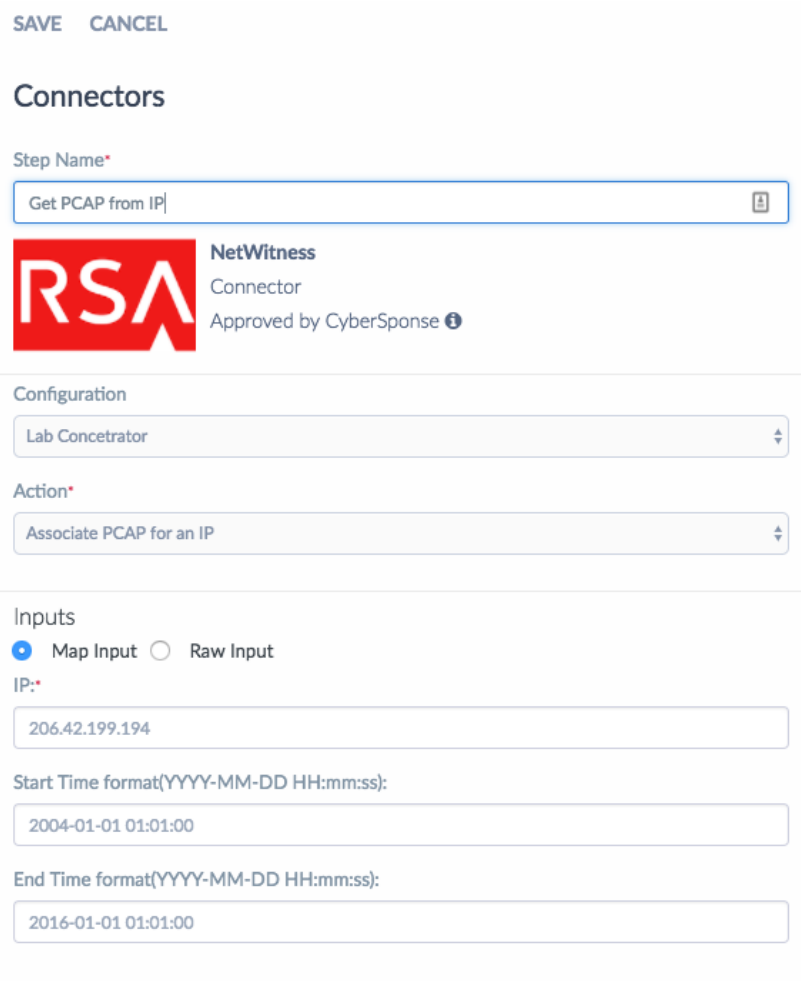
   i. **IP** (Required) – The IP to search for.

   ii. **Start Time (**Optional) – The start time for the search.

   iii. **End Time (**Optional) – The end time for the search.

NOTE: If start time and end time are not supplied, the search is run for 24 hours prior to the time it is executed.

NOTE: This searches for ip.src OR ip.dst



c. **NetWitness Meta from Domain** (Connector Action: **Get Meta for a Domain**)

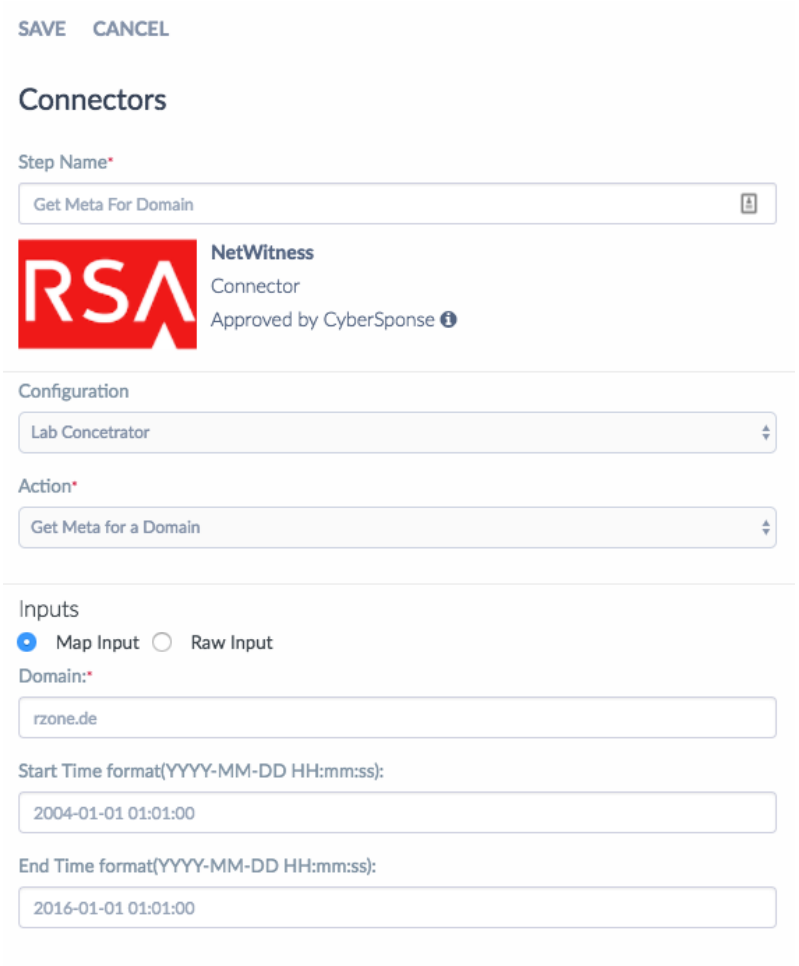
   i. **Domain** (Required) – The Domain to search for.

   ii. **Start Time (**Optional) – The start time for the search.

   iii. **End Time (**Optional) – The end time for the search.

NOTE: If start time and end time are not supplied, the search is run for 24 hours prior to the time it is executed.

NOTE: This searches for domain.src OR domain.dst



d. **NetWitness PCAP from Domain** (Connector Action: **Associate PCAP for a Domain**)

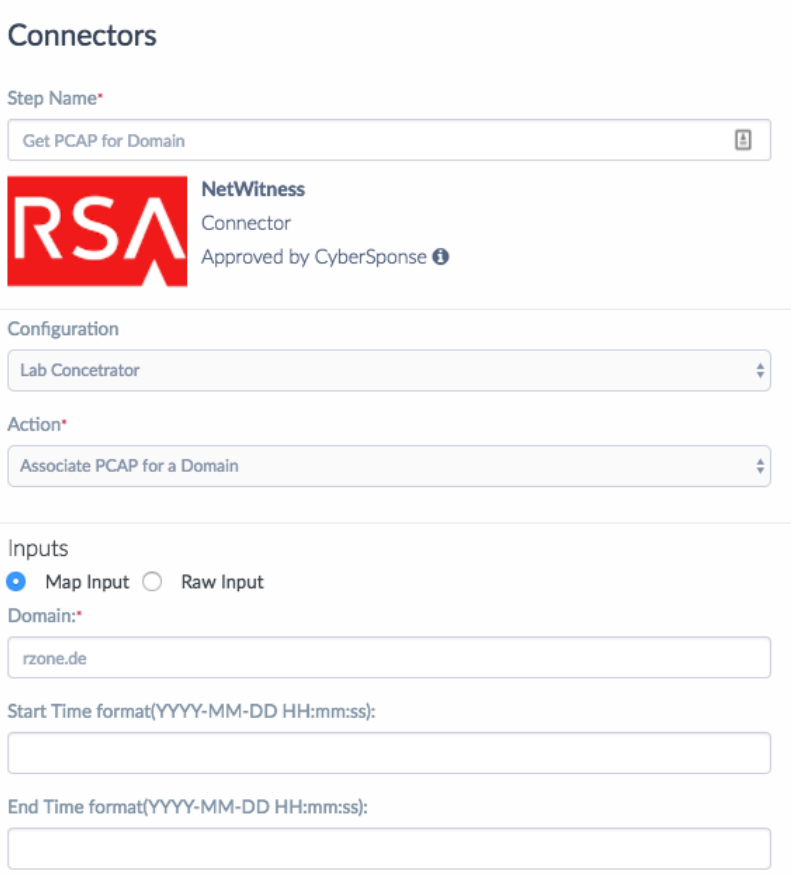
   i. **Domain** (Required) – The Domain to search for.

   ii. **Start Time (**Optional) – The start time for the search.

   iii. **End Time (**Optional) – The end time for the search.

NOTE: If start time and end time are not supplied, the search is run for 24 hours prior to the time it is executed.

NOTE: This searches for domain.src OR domain.dst



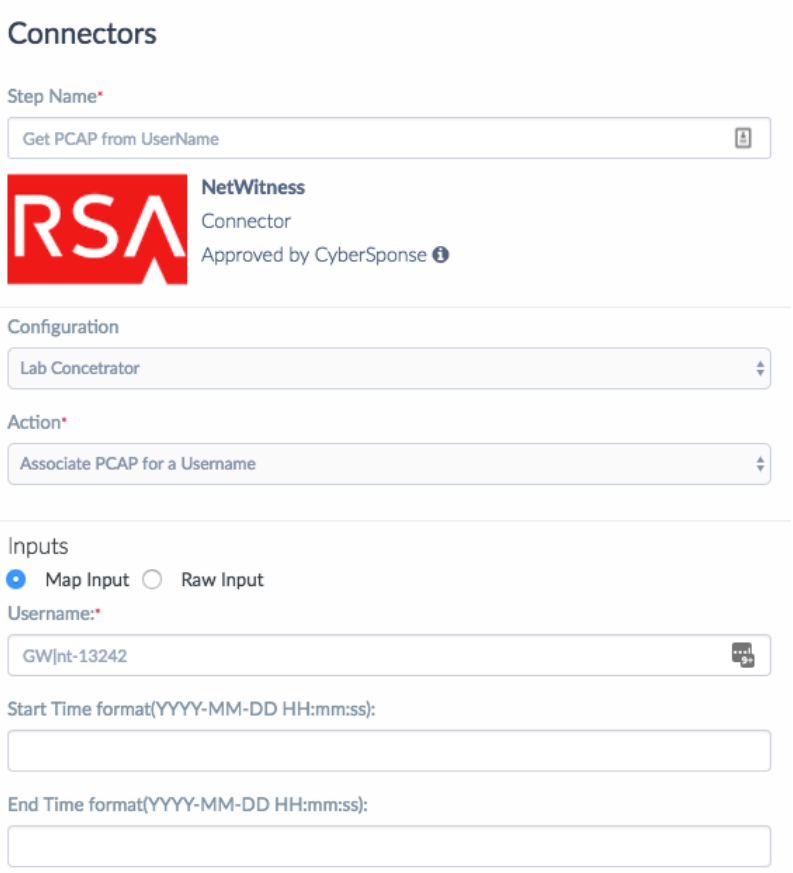
e. **NetWitness PCAP from Username** (Connector Action: **Associate PCAP for a Username)**

   i. **Username** (Required) – The Username to search for.

   ii. **Start Time (**Optional) – The start time for the search.

   iii. **End Time (**Optional) – The end time for the search.

NOTE: If start time and end time are not supplied, the search is run for 24 hours prior to the time it is executed.



f. **NetWitness Meta from IP** (Connector Action: **Get Meta for an IP**)

   i. **IP** (Required) – The IP to search for.

   ii. **Start Time (**Optional) – The start time for the search.

   iii. **End Time (**Optional) – The end time for the search.

NOTE: If start time and end time are not supplied, the search is run for 24 hours prior to the time it is executed.

NOTE: This searches for ip.src OR ip.dst

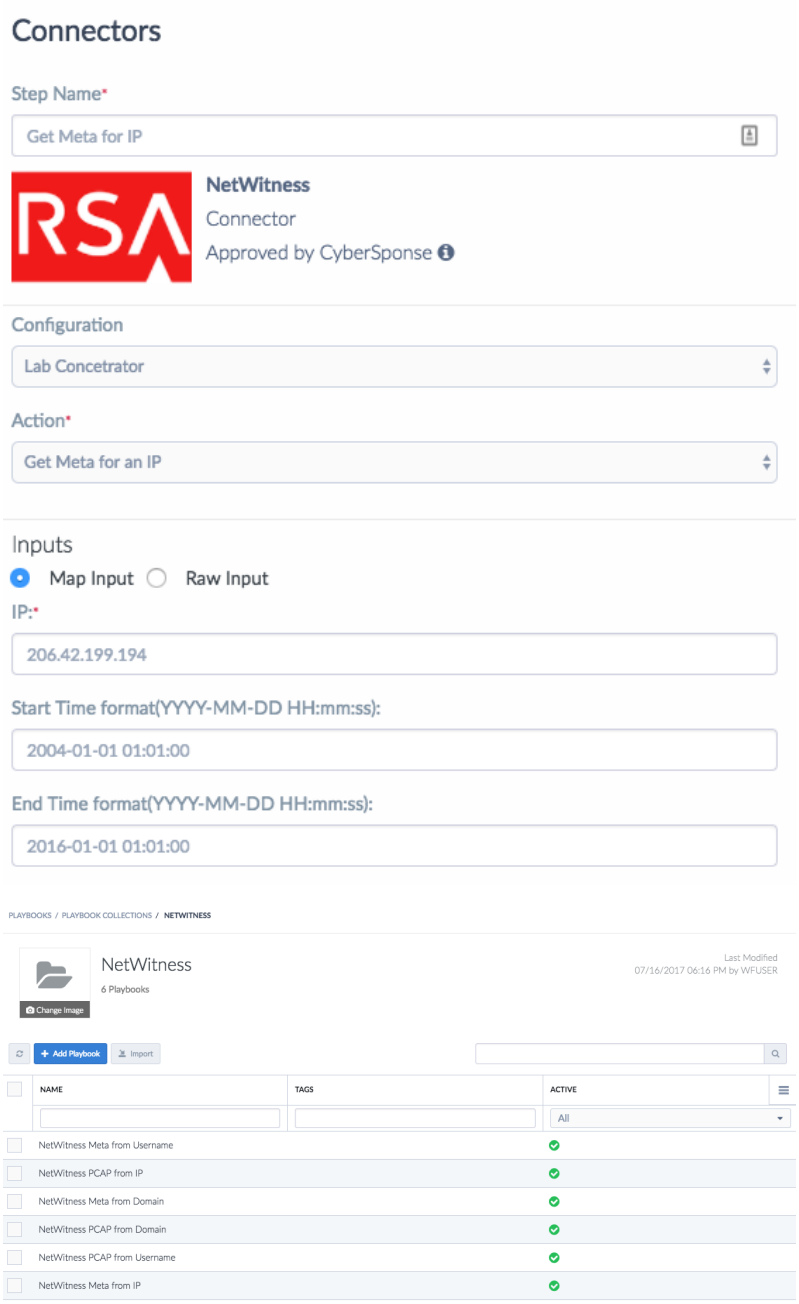


Figure 5 - Listing of playbooks related to RSA NetWitness

Connector Action Output

All connector actions provide output through the **Jinja Generator** to quickly access all returned data. You can view the output data by:

1. Creating a new **Set Variable** step.
2. Connecting it to your **NetWitness** action in the playbook.

3. Open the **Set Variable** step.
4. Click in the **value box** (This opens the **Jinja Generator**)
    a. Select the **Previous Steps Output**.
    b. Under your prior step select the **data**
    c. You will see a whole list of fields that can be returned for your action:

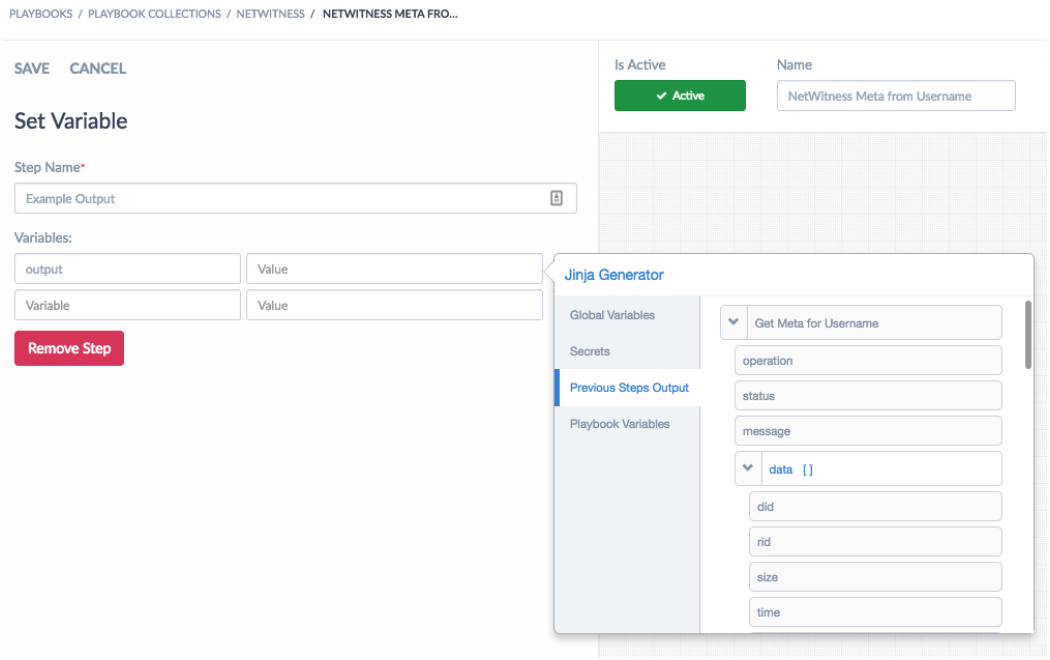


Figure 6 - Listing of playbooks related to RSA NetWitness

Solution Overview

CyberSponse has the ability to collect session metadata and/or a related PCAP file at this time. All playbooks can be used independently or in unison to get the required information.

Playbooks

Playbooks can be run automatically (as part of a workflow), or by manual activation. Under **Alerts**, click on any of the NetWitness actions:

Figure 7 - Action Menu for NetWitness

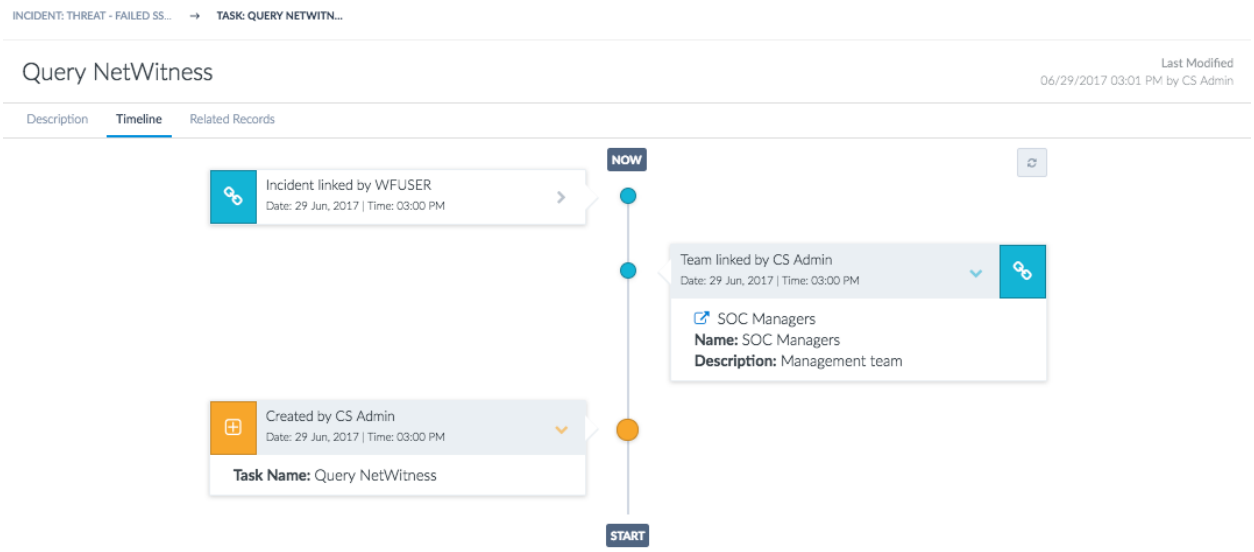


Figure 8 - Timeline view with Query NetWitness task

Certification Checklist for RSA NetWitness

Date Tested: June 30th, 2017

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.3	Virtual Appliance
CyOps	4.9.0.0	Virtual Appliance

RSA NetWitness Test Case	Result
Inline Query/Enrichment	
Query NetWitness for IP Info (source/destination IP)	✓
Query NetWitness for User Info (usernames, user behavior)	✓
Query NetWitness for Specific Meta (Other)	✓
Retrieve NetWitness Log/Packet Data	✓
Retrieve NetWitness PCAP files	✓
Alerting / Incident Creation	
NetWitness alert via syslog	N/A
NetWitness alert via email	N/A
NetWitness alert via ESA/scripting	N/A
Send alert to NetWitness (Syslog, CEF, or custom parser)	N/A
RSA NetWitness Intel Feeds	
Update NetWitness Intel Feed (CSV, STIX)	N/A

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