RSA® NETWITNESS®
Security Operations
Implementation Guide

Siemplify ThreatNexus 2.5

Jeffrey Carlson, RSA Partner Engineering
Last Modified: January 4th, 2018

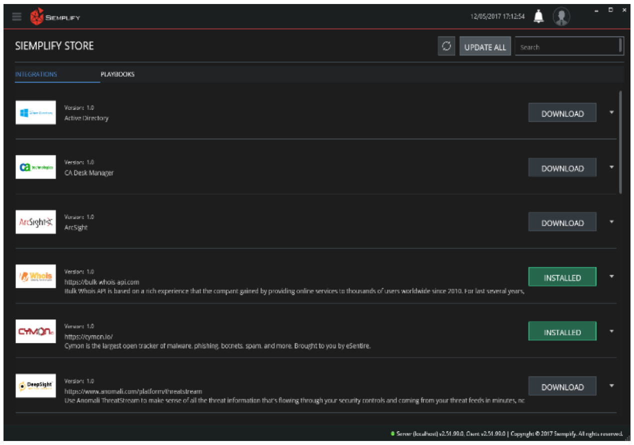
Solution Summary

Siemplify ThreatNexus is a security orchestration and incident response platform purpose built for the security team to navigate the full spectrum of security operations – all from a single pane of glass.

ThreatNexus integrates with most existing security solutions, RSA NetWitness included, creating an integrated fabric that unifies the disparate tools & systems across the security landscape. With this centralized management system, analysts can manage all aspects of threat response with deeper enrichment and investigation capabilities, utilizing automated actions and enabling human intervention where appropriate.

RSA NetWitness enrichment can be used to power advanced data driven playbooks within ThreatNexus. For example, network traffic analysis to identify actual suspicious hosts or users from NetWitness to distinguish between regular common mistakes, False Positive, and malicious activity. The queried information can be matched against other systems or online Threat Intelligence to provide further fidelity.

Deploying the integration consists of downloading the RSA NetWitness integration through Siemplify's online store, and then supplying the credentials and servers' details. A detailed configuration guide can be found in this document.



Version: 1.0
Active Directory
DOWNLOAD

Version: 1.0
CA Desk Manager
DOWNLOAD

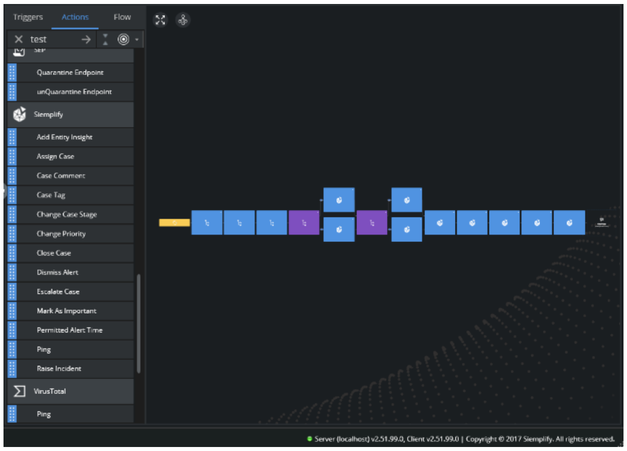
Version: 1.0
ArcSight
DOWNLOAD

Version: 1.0
https://bulk whois api.com
Bulk Whois API is based on a rich experience that the compant gained by providing online services to thousands of users worldwide since 2010. For last several years,
INSTALLED

Version: 1.0
https://cymon.io/
Cymon is the largest open tracker of malware, phishing, botnets, spam, and more. Brought to you by eSentire.
INSTALLED

Version: 1.0
https://www.anomali.com/platform/threatstream
Use Anomali ThreatStream to make sense of all the threat information that's flowing through your security controls and coming from your threat feeds in minutes, nc
DOWNLOAD

Server (localhost) v2.51.99.0, Client v2.51.99.0 | Copyright © 2017 Siemplify. All rights reserved.



Server (localhost) v2.51.99.0, Client v2.51.99.0 | Copyright © 2017 Siemplify. All rights reserved.

Partner Product Configuration

Before You Begin

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

Siemplify ThreatNexus Configuration

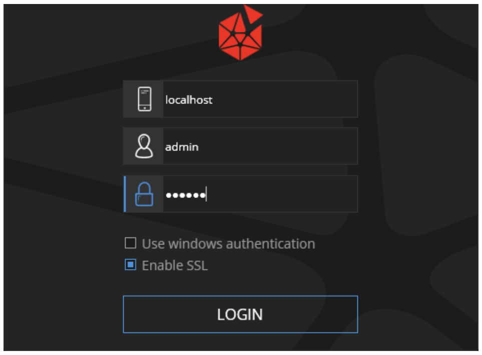
The Siemplify ThreatNexus store consists of a list of supported integrations. Each integration denotes one or more associated 'actions' and their corresponding credential configurations. To set up an integration, go to the Siemplify's store, search for the integration you need, and click install. Once the integration is installed, a configuration of essential parameters is needed (such as credentials or API keys), for the integration to function properly.

Installing the RSA NetWitness Integration

In order to properly configure the integration, you only need the credentials to the NetWitness appliance. If you have different credentials for different NetWitness servers, please refer to the Siemplify's *ThreatNexus MSSP* documentation.

To configure the Integration inside ThreatNexus, perform the following steps:

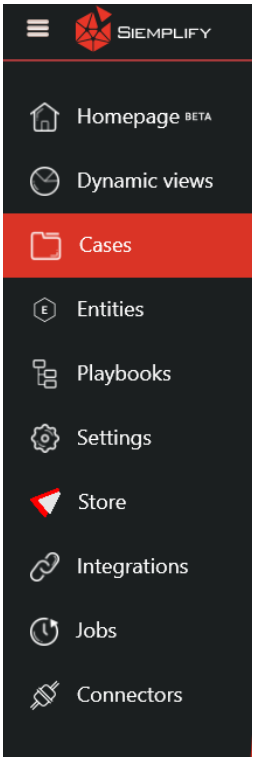
1. Log into ThreatNexus client:



localhost
admin
••••••

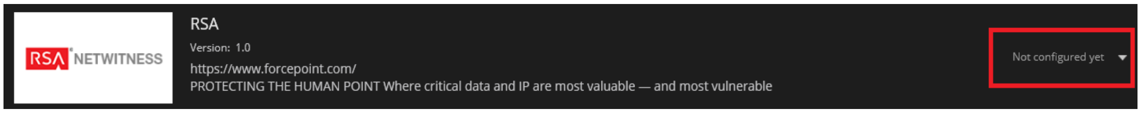
□ Use windows authentication
☑ Enable SSL

2. Press on the **menu** button (Top left) and choose **Store**. A list of all supported integrations will appear:



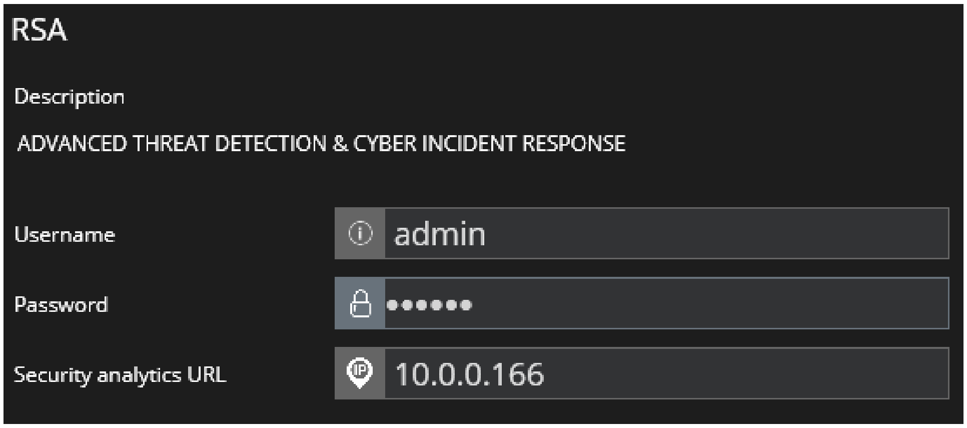
3. Find the **RSA NetWitness** integration and click the **DOWNLOAD** button on the right side of the screen. Wait until the button changed to **INSTALLED**.

4. Press on the **menu** button (Top left) and choose **Integrations**. A list of all installed integrations will be displayed. The RSA NetWitness integration should appear on that list, showing as - **Not configured yet** in gray. Press on the integration and fill in any details the integration requires. The NetWitness integration requires credentials to the appliance as well as the IP address of the SA server.



RSA
Version: 1.0
https://www.forcepoint.com/
PROTECTING THE HUMAN POINT Where critical data and IP are most valuable — and most vulnerable

Not configured yet



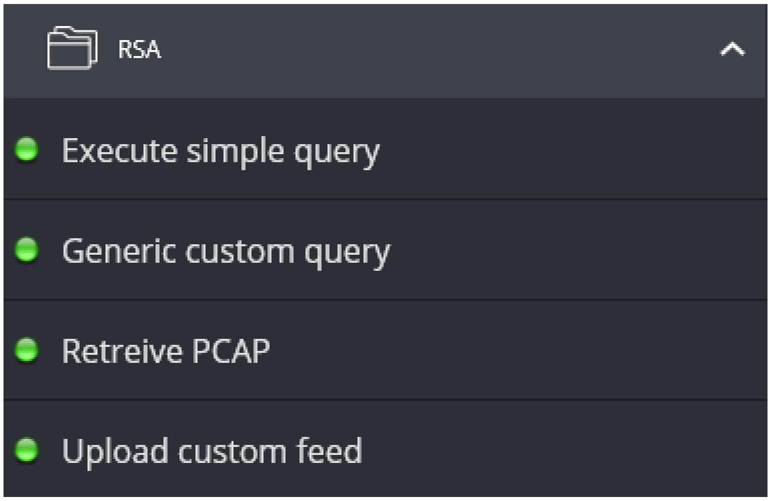
RSA

Description

ADVANCED THREAT DETECTION & CYBER INCIDENT RESPONSE

Username	admin
Password	••••••
Security analytics URL	10.0.0.166

5. Once all the information is entered, hit **Save**. You can test the connectivity with the NetWitness appliance with the **Test** button.
6. RSA NetWitness' actions are now ready to be used both in playbooks and as a manual action during case investigation.



Using the RSA NetWitness Integration

Siemplify can retrieve three types of relevant data from NetWitness. All three are based on a custom query either prepared by Siemplify ThreatNexus or the playbook author.

Metadata: Returns the queried events' metadata in a table for all the events that meet the query

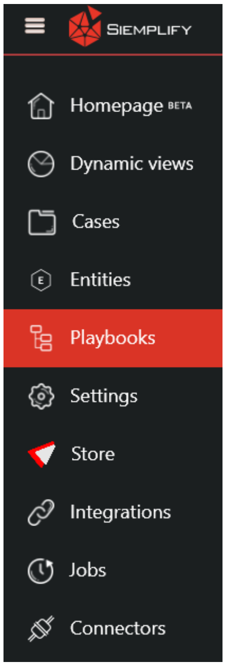
PCAP: Returns a PCAP file containing all the PCAPs of all the query matched events as an attachment to the case (Can be downloaded to further investigate)

Raw logs: Returns the raw syslog as sent by the various security appliances to NetWitness.

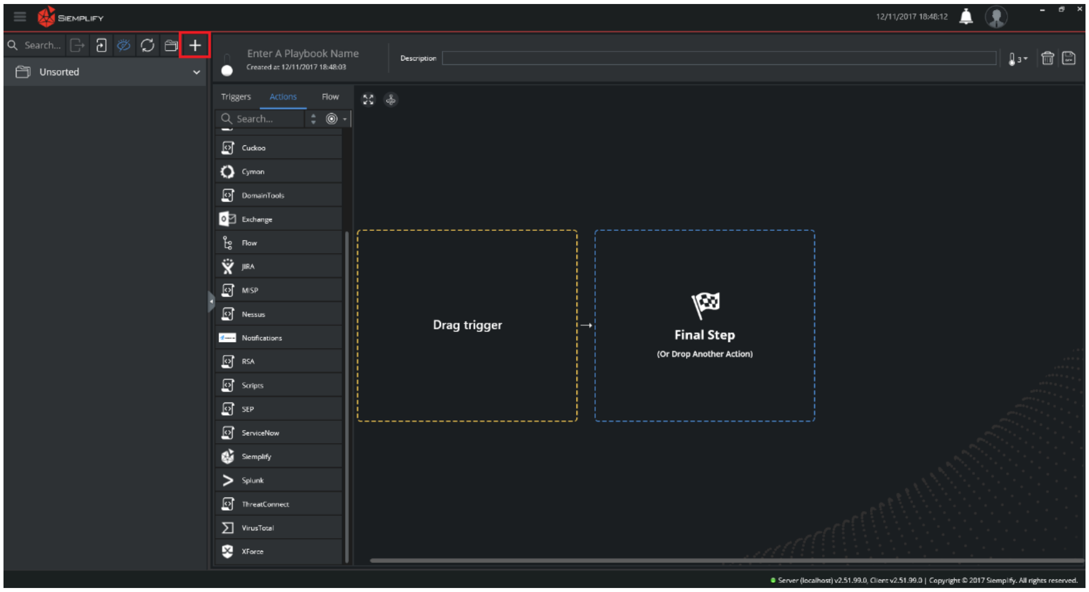
These data types can be queried either as part of a playbook or manually for the analyst to observe. Alternatively, this data can be used inside a playbook to enhance the playbook's decision making. For example, if a virus found alert is generated, Siemplify ThreatNexus could query NetWitness for similar signatures or file hashes around the environment, or look for further communication of the affected host and compare it to other hosts in order to identify suspicious activity (Threat intelligence feeds could also be correlated).

To use RSA NetWitness integration in Siemplify ThreatNexus, simply create a new playbook and drag the wanted actions to it, as explained below:

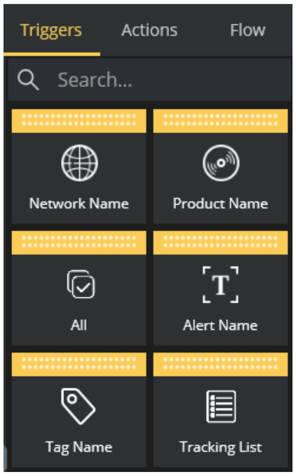
1. First, go to the **Playbooks** tab:



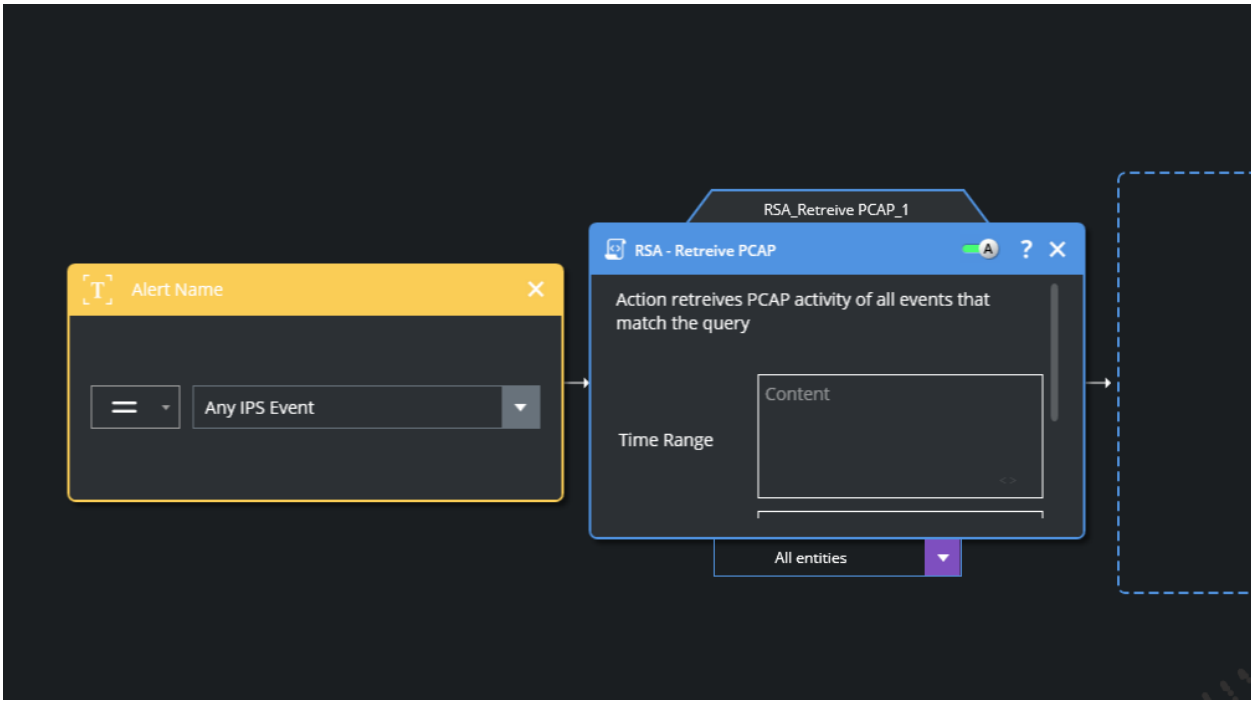
2. Then, create a new workflow using the **Plus** sign at the top left side of the screen:



3. Now, choose a **trigger** for the playbook. A trigger is what attaches the playbook to alerts and starts the automation. To use the trigger, drag it from the list to the yellow square.



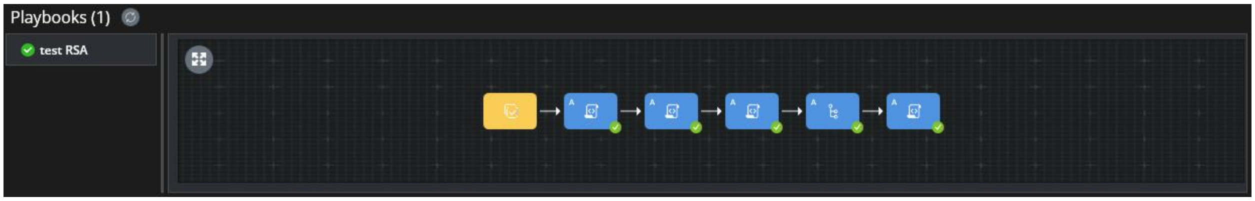
4. Then, go to the **Actions** tab, and search for your desired action. In this case, we will search for **RSA** and drag the action to the playbook.



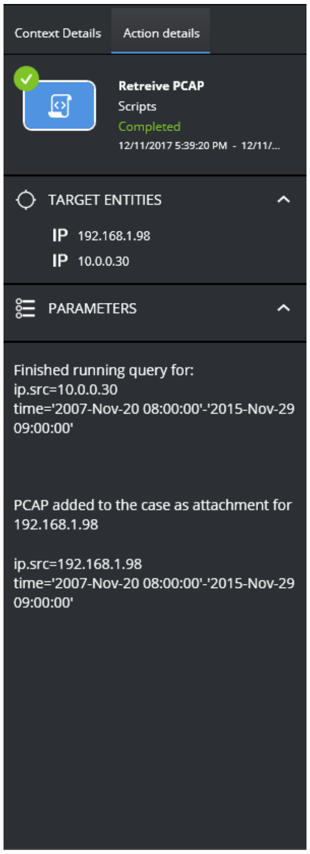
Action retreives PCAP activity of all events that match the query

5. Fill in wanted parameters for the action and hit **save** (Top right side of the screen). Don't forget to activate the playbook, using the slide-bar next to the playbook's name, and give the playbook a name before saving.

6. Now, when an alert that triggers the workflow is ingested, the workflow will be attached to it and will look like the following:



7. By clicking on any of the finished actions in the playbook, the action's result is presented. For example, the following is a result of the PCAP extraction:



Context Details | Action details

Retreive PCAP
Scripts
Completed
12/11/2017 5:39:20 PM - 12/11/...

TARGET ENTITIES

IP 192.168.1.98
IP 10.0.0.30

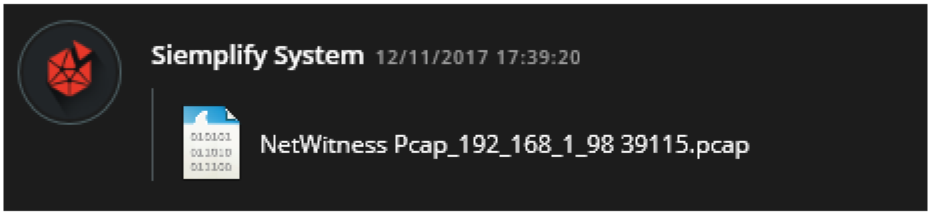
PARAMETERS

Finished running query for:
ip.src=10.0.0.30
time='2007-Nov-20 08:00:00'-'2015-Nov-29 09:00:00'

PCAP added to the case as attachment for 192.168.1.98

ip.src=192.168.1.98
time='2007-Nov-20 08:00:00'-'2015-Nov-29 09:00:00'

8. Here we can see that the action queried the NetWitness with two queries, and that one returned a result PCAP that was attached to the case. The PCAP can be downloaded from the case wall and viewed with a suitable application.



Siemplify System 12/11/2017 17:39:20

NetWitness Pcap_192_168_1_98 39115.pcap

These actions can accept inputs from previous actions, which enables a much deeper automatic investigation to either prepare a detailed report to an analyst or act on its own.

In addition, Siemplify ThreatNexus periodically queries NetWitness for incidents and ingest any newly appended alerts from each incident into its case pull. These alerts are converted into Siemplify's alerts and are grouped with other existing alerts if a connection was found. Playbooks are then attached to the new alerts to automate triage, investigation and remediation process.

Certification Checklist for RSA NetWitness

Date Tested: December 5, 2017

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.4.0	Virtual Appliance
Siemplify ThreatNexus	2.5.1	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
Ingest incidents from NetWitness	N/A
RSA NetWitness Intel Feeds	
Update NetWitness Intel Feed (CSV, STIX)	N/A

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