RSA® NETWITNESS®
Security Operations Implementation Guide

DFLabs IncMan version 4.5+

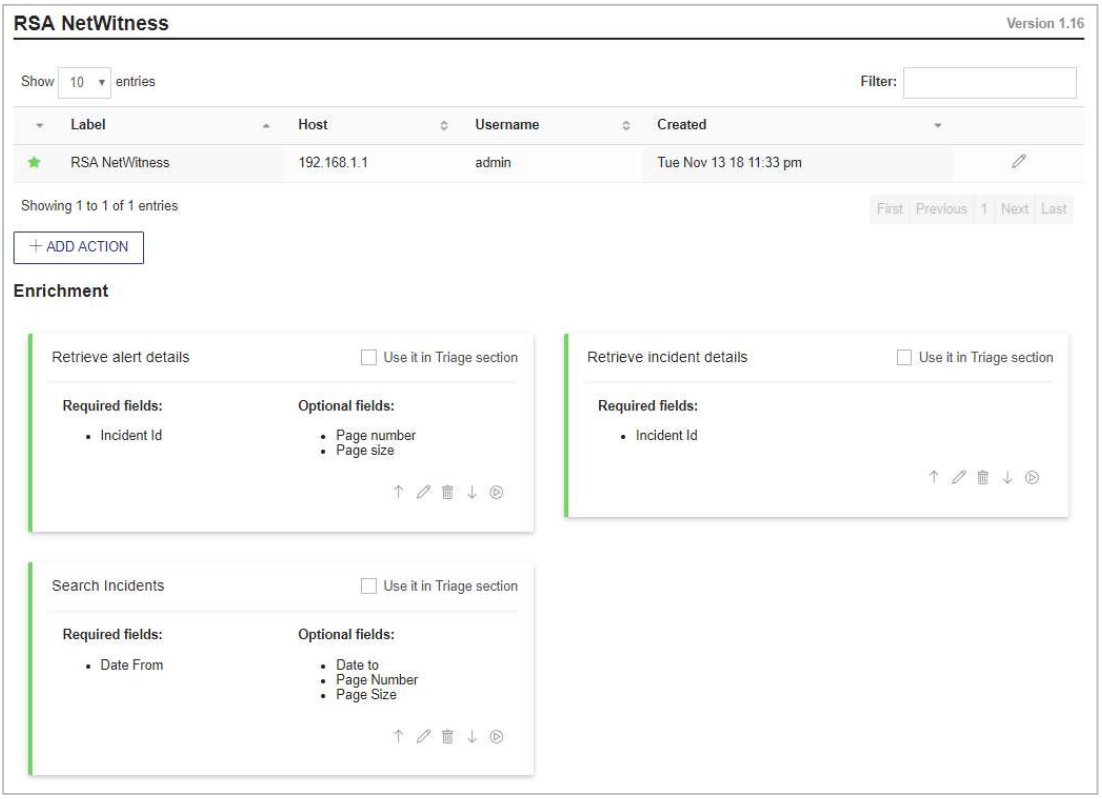
Daniel R. Pintal, RSA Partner Engineering
Last Modified: November 20, 2018

RSA READY

Solution Summary

DFLabs integration and RSA NetWitness enable joint customers to automate and orchestrate actions with NetWitness and other third-party security solutions through the IncMan SOAR platform to enable a faster, more efficient response to security events.

Using IncMan SOAR's Rapid Response Runbooks, joint customers can automatically perform actions in RSA NetWitness Logs and Packets and Incident Management to correlate events, add context to incidents and enrich incident and alert data with other third-party sources.



IncMan SOAR's integration with **RSA NetWitness Logs and Packets** allows users to:

- ✓ Query Logs
- ✓ Retrieve Log Data

IncMan SOAR's integration with **RSA NetWitness Incident Management** allows users to:

- ✓ Search Incidents
- ✓ Retrieve Incident Details
- ✓ Retrieve Alert Details

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the DFLabs IncMan 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 and install the required components.

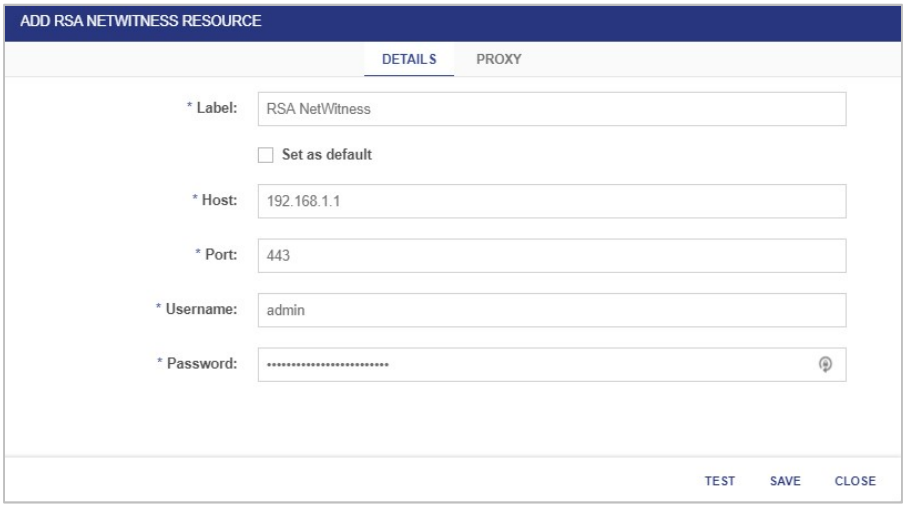
All DFLabs IncMan components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

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 DFLabs Incman is properly configured and secured before deploying to a production environment. For more information, please refer to the DFLabs Incman documentation or website.

DFLabs IncMan Configuration

To add the RSA Netwitness integration to DFLabs IncMan SOAR:

1. Log in to the DFLabs Community Portal and click **Solutions**.
2. Search for **RSA NetWitness** and download the appropriate integration files.
3. Log in to your IncMan SOAR instance.
4. Go to **Configuration** > **External Sources** > **Integrations** and click **Add New Integration**.
5. Select the RSA NetWitness integration files downloaded from the DFLabs Community Portal.
6. Click **+ Add Resource** and enter the appropriate configuration parameters (example below).



7. Click **Test** to confirm you are able to connect to your RSA NetWitness instance successfully.
8. Click **Save**.

DFLabs IncMan Example Use Cases

Enriching Endpoint Detection Alerts

An alert is generated by the organization's EDR solution indicating that an internal host has been observed communicating with a potentially malicious external host. This alert automatically generates an incident within IncMan SOAR. The Incident Template used to create the incident includes a Runbook, which will be used to automatically enrich the initial alert data, prioritize the alert, and take automated containment actions, if appropriate. IncMan SOAR will automatically query any threat intelligence resources configured by the organization to determine the possible threat posed to the organization. IncMan SOAR will then automatically query RSA NetWitness to determine which hosts have been observed communicating with the potentially malicious IP address initially observed by the EDR solution. Finally, IncMan SOAR will automatically query the organization's IT asset management solution to gather information regarding the internal hosts which have been communicating with the potentially malicious external host. Based on the results from this automated data enrichment process, the organization may create rules which adjust the severity of the incident, reassign the incident, or take automated containment action.

Pivoting from an Initial RSA NetWitness Alert

An alert is generated by RSA NetWitness indicating that an internal host has been observed connecting to a malicious URL. This alert automatically generates an incident within IncMan SOAR. The Incident Template used to create the incident includes a Runbook, which will be used to automatically enrich the initial alert data, prioritize the alert, and take automated containment actions, if appropriate. IncMan SOAR will automatically query any threat intelligence resources configured by the organization to determine the possible threat posed to the organization, as well as gather any other domains, IP addresses or file hashes which are known to have been associated with the malicious URL. After gathering this enriched information, IncMan SOAR will perform additional queries in RSA NetWitness and any other internal log sources to determine if there is any evidence of any of the other IoCs provided by the organization's threat intelligence sources. Based on the results from these additional searches, the organization may create rules which adjust the severity of the incident, reassign the incident, or take automated containment action across all potentially compromised hosts, not just the initially reported host.

Certification Checklist for RSA NetWitness

Date Tested: November 20, 2018

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	11.2	Virtual Appliance
DFLabs IncMan	4.5	CentOS

RSA NetWitness Test Case	Result
Inline Query/Enrichment Incidents (NetWitness API)	
Query NetWitness Incidents	✓
Alerts (RestAPI)	
Query NetWitness for Alerts	✓
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	N/A
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