# RSA® NETWITNESS®
# Security Operations Implementation Guide

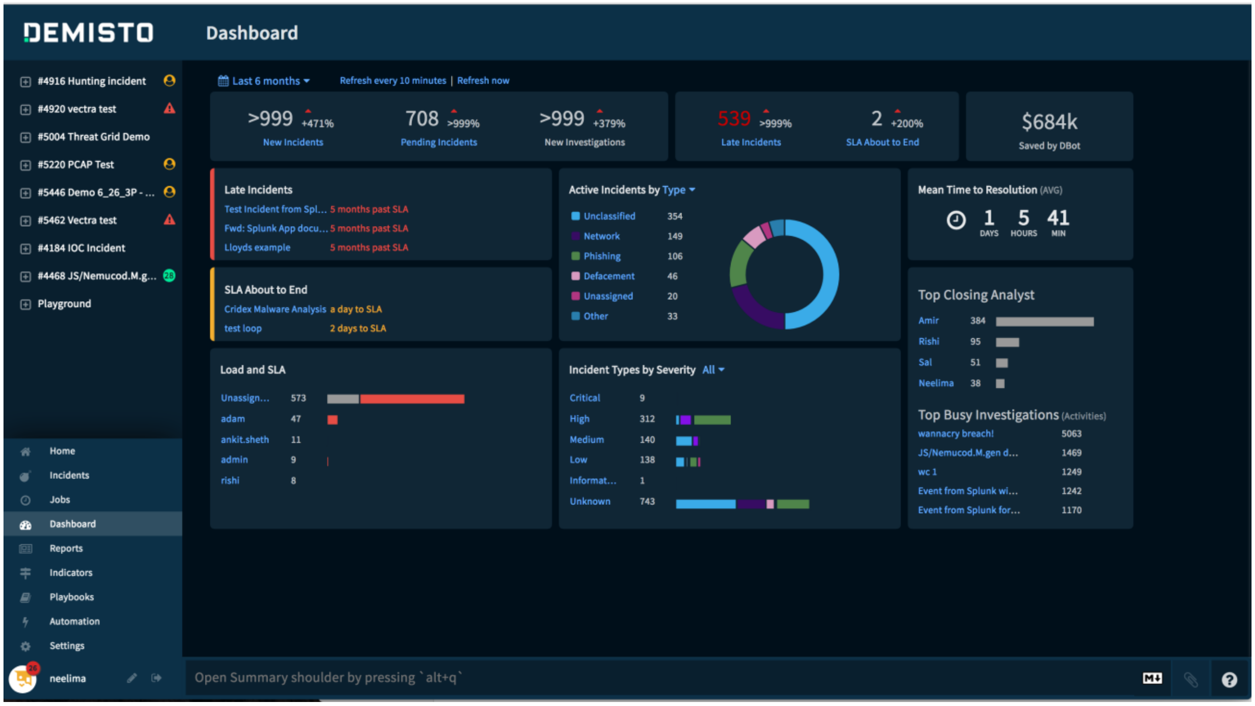
# Demisto Enterprise 3.0

Jeffrey Carlson, RSA Partner Engineering
Last Modified: July 19th, 2017

## Solution Summary

The RSA NetWitness® integration allows Demisto enterprise to:

- Respond to RSA Security Analytics incidents using Demisto playbooks
- Do Time-based event correlation to enrich investigations
- Pull packets captures and add packet captures from external sources into NetWitness®.



>999 +471% New Incidents

708 >999% Pending Incidents

>999 +379% New Investigations

539 >999% Late Incidents

2 +200% SLA About to End

$684k Saved by DBot

Late Incidents

| | |
|---|---|
| Test Incident from Spl... | 5 months past SLA |
| Fwd: Splunk App docu... | 5 months past SLA |
| Lloyds example | 5 months past SLA |

SLA About to End

| | |
|---|---|
| Cridex Malware Analysis | a day to SLA |
| test loop | 2 days to SLA |

Active Incidents by Type

| | |
|---|---|
| Unclassified | 354 |
| Network | 149 |
| Phishing | 106 |
| Defacement | 46 |
| Unassigned | 20 |
| Other | 33 |

Mean Time to Resolution (AVG)

1 DAYS 5 HOURS 41 MIN

Top Closing Analyst

| | |
|---|---|
| Amir | 384 |
| Rishi | 95 |
| Sal | 51 |
| Neelima | 38 |

Load and SLA

| | |
|---|---|
| Unassign... | 573 |
| adam | 47 |
| ankit.sheth | 11 |
| admin | 9 |
| rishi | 8 |

Incident Types by Severity All

| | |
|---|---|
| Critical | 9 |
| High | 312 |
| Medium | 140 |
| Low | 138 |
| Informat... | 1 |
| Unknown | 743 |

Top Busy Investigations (Activities)

| | |
|---|---|
| wannacry breach! | 5063 |
| JS/Nemucod.M.gen d... | 1469 |
| wc 1 | 1249 |
| Event from Splunk wi... | 1242 |
| Event from Splunk for... | 1170 |

Open Summary shoulder by pressing `alt+q`

Demisto Enterprise integrates with:

**RSA NetWitness® Logs and Packets**

- Runs queries
- Pulls packets captures and add packet captures from external sources into NetWitness.

**RSA NetWitness® Incident Management**

- Provides ability to fetch, create update or close incidents, and search events.

# Partner Product Configuration

## *Before You Begin*

This section provides instructions for configuring Demisto 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.

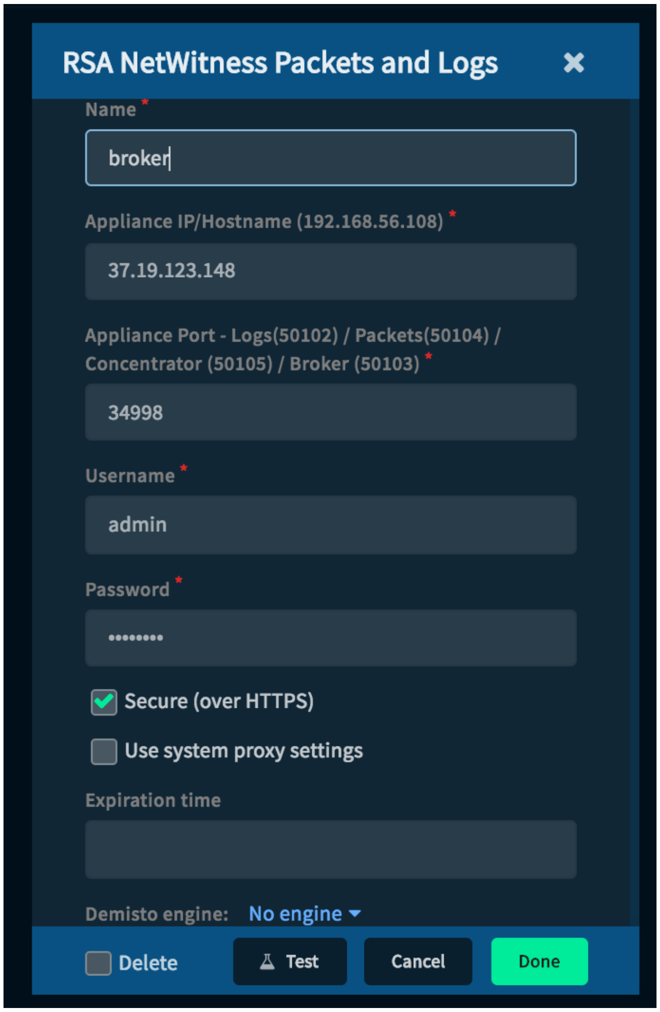
All Demisto components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

**! 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 Demisto Enterprise is properly configured and secured before deploying to a production environment. For more information, please refer to the Demisto Enterprise documentation or website.**

## *Demisto Enterprise Configuration*

To configure Demisto Enterprise to integrate with RSA NetWitness, perform the following steps:

1. Deploy Demisto Enterprise 3.x version and above.
2. Go to **Settings > Integrations > Servers & Services**
3. Locate the **RSA NetWitness Packets and Logs** integration by searching for it using the search box on the top of the page.



RSA NetWitness Packets and Logs

Name *

broker

Appliance IP/Hostname (192.168.56.108) *

37.19.123.148

Appliance Port - Logs(50102) / Packets(50104) / Concentrator (50105) / Broker (50103) *

34998

Username *

admin

Password *

••••••••

☑ Secure (over HTTPS)

☐ Use system proxy settings

Expiration time

Demisto engine: No engine

4. Click **Add instance** to create and configure a new integration. You should configure the following settings:

| | |
|---|---|
| **Name:** | A textual name for the integration instance. |
| **Appliance IP/Hostname:** | The hostname or IP address of the appliance being used. |
| **Appliance Port:** | The appliance port being used. Make sure that the appliance is reachable with respect to IP address and port. |
| **Username and Password:** | The username and password, or toggle to Credentials. |
| **Do Not Validate Server Certificate:** | Select to avoid server certification validation. You may want to do this in case Demisto cannot validate the integration server certificate (due to a missing CA certificate). |
| **Demisto Engine:** | If relevant, select the engine that acts as a proxy to the server. Engines are used when you need to access a remote network segment and there are network devices such as proxies, firewalls, etc. that prevent the Demisto server from accessing the remote networks. |

For more information on Demisto engines see: **https://demisto.zendesk.com/hc/en-us/articles/226274727-Settings-Integrations-Engines**

| | |
|---|---|
| **Require Users to Enter Additional Password:** | Select whether you'd like an additional step where users are required to authenticate themselves with a password. |

5. Press the **Test** button to validate connection.

   If you are experiencing issues with the service configuration, please contact Demisto support at **support@demisto.com**

6. After completing the test successfully, press the **Done** button.

Once the connection to RSA NetWitness is configured, it can be used in Demisto Playbooks in a number of different ways, some examples of which are described below.

## *Demisto Enterprise Examples*

The following are example scenarios for the integration between Demisto and RSA NetWitness:

### Respond to RSA NetWitness Incidents Using Demisto Playbooks

Demisto polls RSA NetWitness Incident Management for new incidents every minute. Once a new incident comes in, Demisto triggers a new incident, chooses a playbook according to incident metadata, and starts running it automatically. The playbook enriches any external IP addresses and domains using reputation sources, and cross-checks them against the internal IOC database aggregated from ISACs and threat feeds. If it sees any hits, the playbook will raise the severity of the incident. It will check if the endpoint is a member of the business-critical server OU in Active Directory, and if not, it will isolate the communicating endpoint using any available EDR/NAC integration, until it can be investigated and cleaned. Then it will choose the best analyst to assign based on its analysis of SOC behavior that it learns over time, assigns the Demisto incident to that analyst, and optionally updates the assignee back into RSA Incident Management as well.

If the playbook finds nothing, it will simply fill in the required fields for the purposes of KPI tracking and analytics, then auto-close the incident. Analysts will only ever see incidents that are of interest, and the other incidents will be conveniently filed away for review if the need arises.

### Time-Based Event Correlation in NetWitness to Enrich Investigations

When an incident is triggered from another alerting source, Demisto Enterprise can query RSA Incident Management for events plus or minus 5 minutes around the time of the alert for the suspected endpoint, in order to enrich the investigation.

### Malware Phishing URLs - Did Anyone Click? Were They Infected?

Demisto runs the automated phishing investigation playbook, and in certain cases, concludes that the email included URLs hosted on malicious domains that infect the user's machine with malware. The next step is to discover all of the users and endpoints in the enterprise who may have also received the email, clicked on the link, and been infected. Demisto will run a query against RSA NetWitness to discover any communication with the malicious domains. If any communication is found, Demisto will also check the HTTP response to see whether the domain was already taken down, or the request was blocked by other threat mitigation measures. If the sessions returned by RSA NetWitness show that a response was received, it will immediately open new investigations on each of the endpoints involved, to check for infections. It will also record the Line of Business of the users who clicked on the link to prioritize Phishing Awareness Training for those departments.

### IOC-Based Communication Hunting

The SOC receives an update from a partner or ISAC including IPs and Domains belonging to a threat actor. Demisto will ingest the email with the STIX attachment, add the indicators to its internal database, and proceed to automatically hunt for any recorded communication with the malicious IPs and Domains. Demisto will run queries against all 7 connected instances of RSA NetWitness, and if any hits are discovered, they will be displayed in a table for the analyst to review. Demisto will auto-raise the incident's severity, pick the best analyst to assign to the incident, and send them an email alert. Demisto will also send a message to the #alerts channel on the SOC's internal Slack team.

## Certification Checklist for RSA NetWitness

Date Tested: July 7th, 2017

| Certification Environment | | |
|---|---|---|
| **Product Name** | **Version Information** | **Operating System** |
| RSA NetWitness | 10.6.3 | Virtual Appliance |
| Demisto Enterprise | 3.0 | |
| | | |

| 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 | N/A |
| 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 Incident Management** | |
| Retrieve NetWitness Incidents | ✓ |
| Retrieve NetWitness Alerts | ✓ |
| Retrieve NetWitness Events | ✓ |
| Retrieve NetWitness Device Info | ✓ |
| **RSA NetWitness Intel Feeds** | |
| Update NetWitness Intel Feed (CSV, STIX) | N/A |

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