RSA® NETWITNESS®
Security Operations Implementation Guide

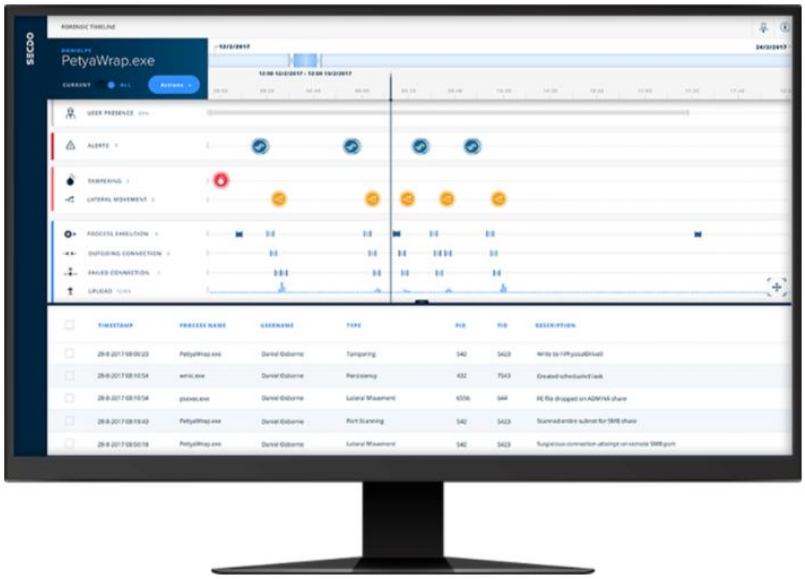
Secdo Platform

Jeffrey Carlson, RSA Partner Engineering
Last Modified: November 27th, 2017

RSA READY

Solution Summary

Secdo integrates with RSA NetWitness to automatically correlate alerts with historical and real-time endpoint data to reveal the full context of each alert – including root cause, attack chain, damage assessment, and more. Secdo offers a wide array of surgical response and remediation tools, enabling rapid, remote, and precise containment and cleanup of all threats from any one or several endpoints or servers at once. Secdo provides unmatched endpoint visibility at the thread-level – the single-most granular view possible into endpoints – along with insights and unlimited querying capabilities, to enable threat hunting of advanced and new attacks missed by other detection systems. Secdo makes it easy for security teams to create their own traditional or behavioral indicators of compromise (IOCs or BIOCs) to proactively identify and clock activity that matches or resembles the criteria provided.

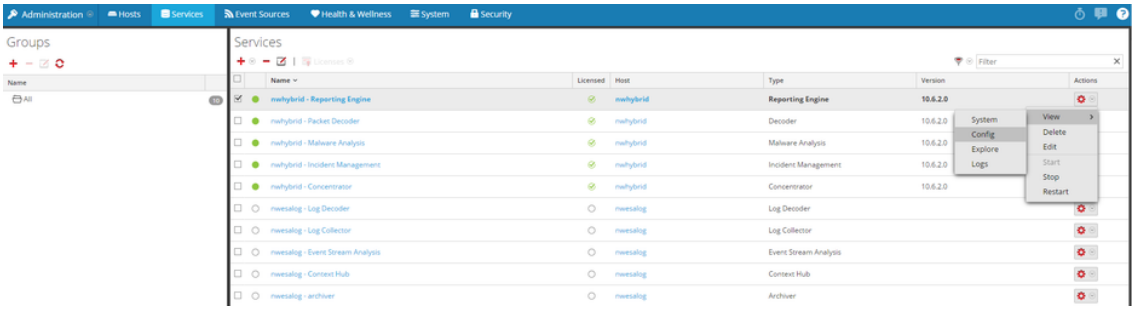


RSA NetWitness Configuration

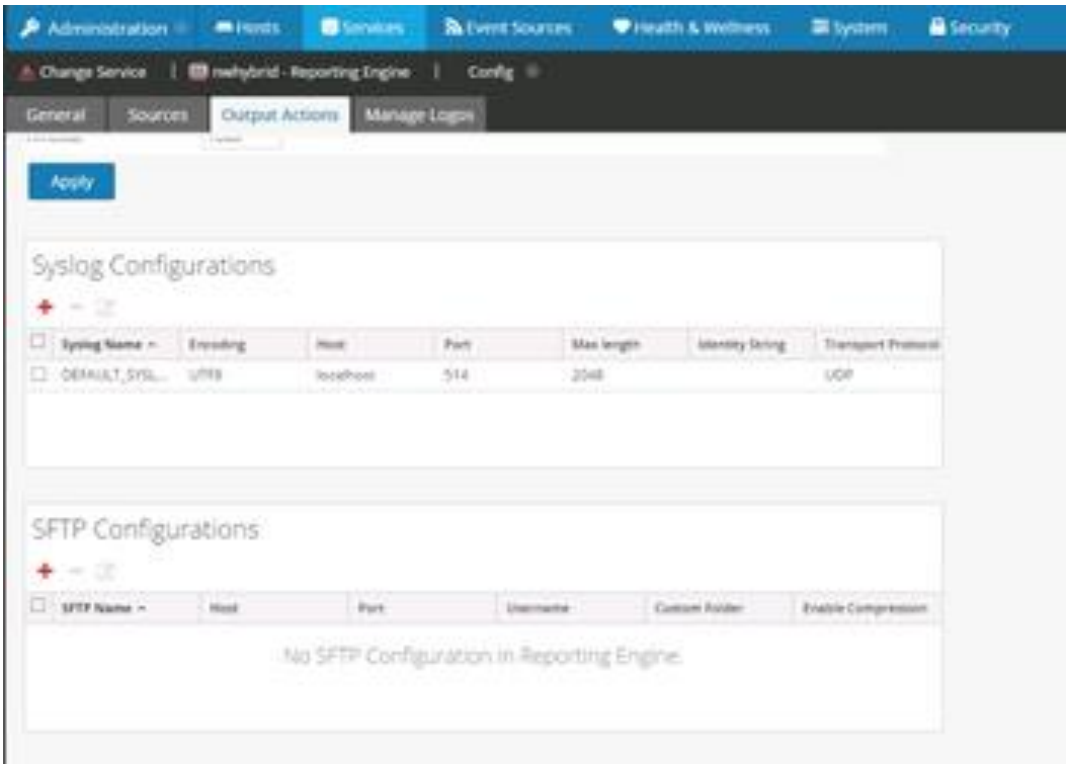
RSA NetWitness sends alerts and events to Secdo Platform via CEF-formatted syslog messages. For more information on the out of the box CEF Meta Keys in RSA NetWitness visit: **https://community.rsa.com/docs/DOC-74333**

1. Login to the RSA NetWitness System:

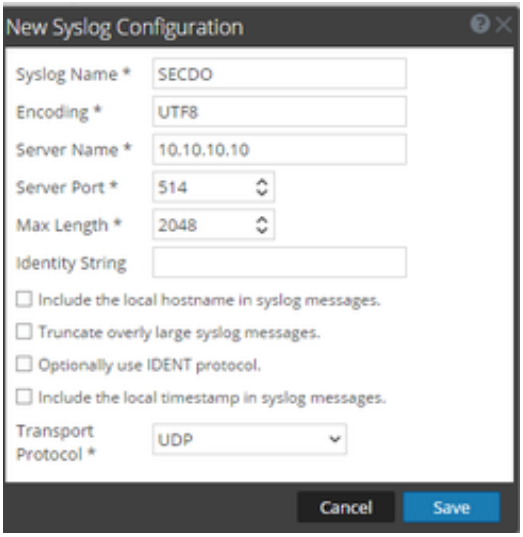
2. Navigate to **Administration > Services > Reporting Engine > Actions > View > Config:**



3. Next, click on the **Output Actions** tab and scroll down to the **Syslog Configurations** section.

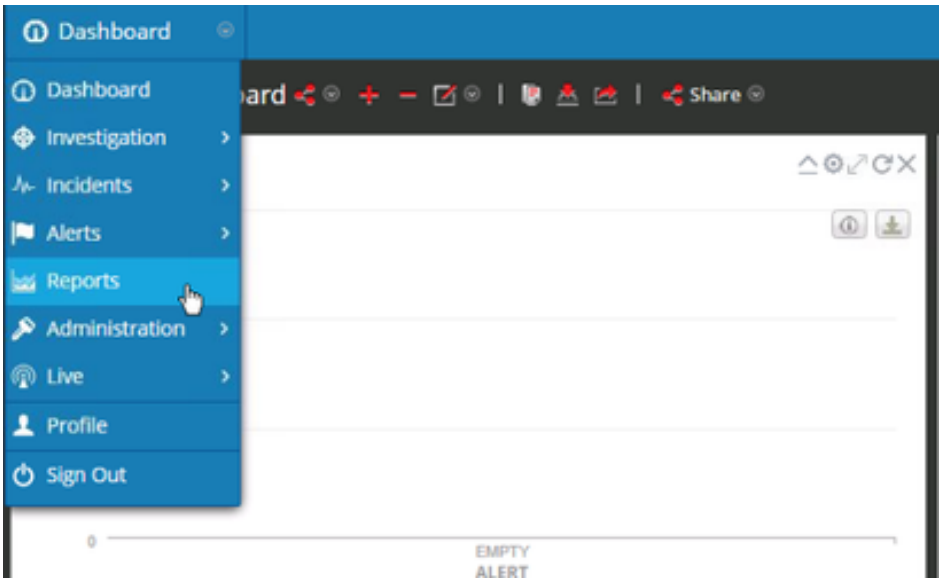


4. Create a new syslog output using the + button and add the data shown in the image below.
5. Set the Server Name to the IP or FQDN of the SECDO server you will be forwarding Syslog events too.

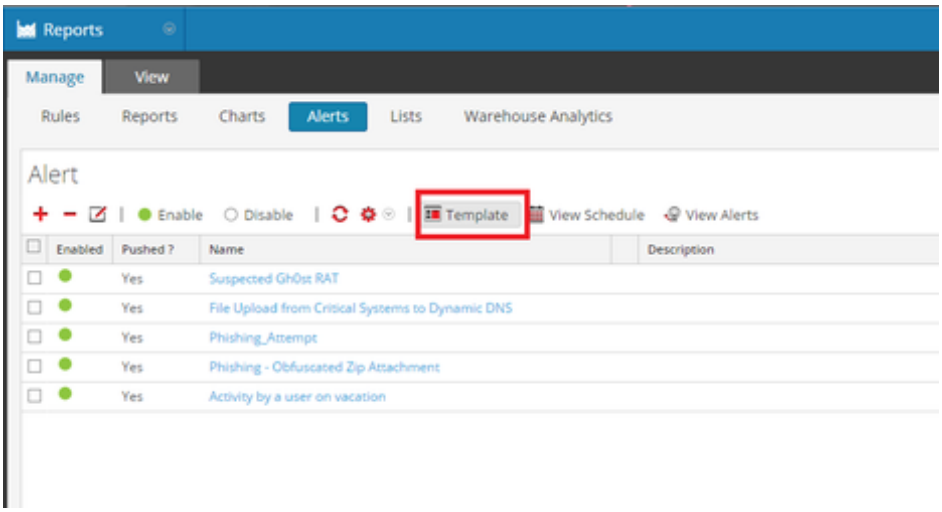


6. Click **Save.**

7. Navigate to the **Reports** section.

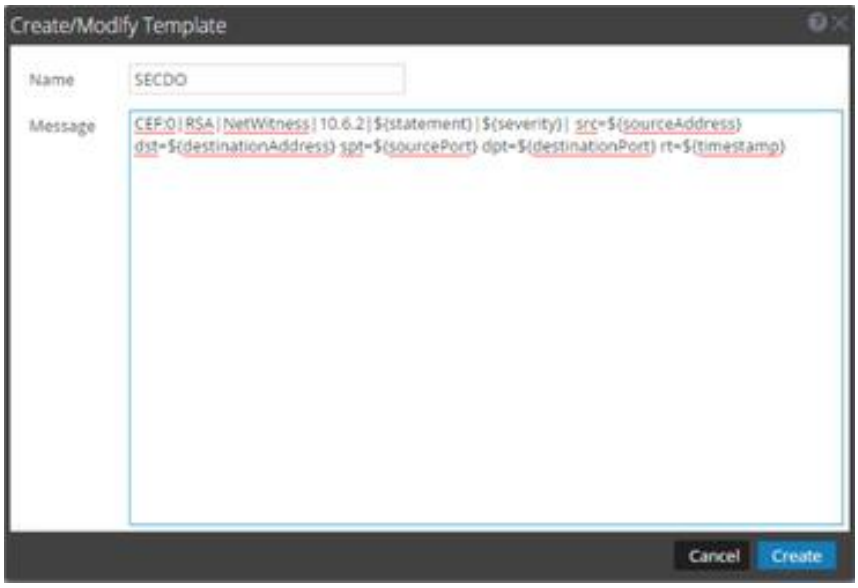


8. Next, click on the **Alerts** button under the **Manage** tab, then the **Template** button.

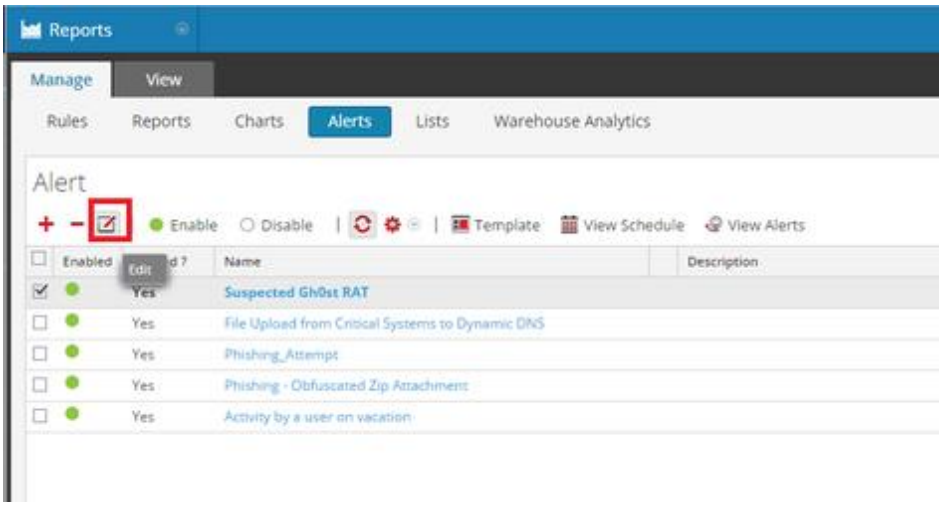


9. Now create a new **Template** as show below.

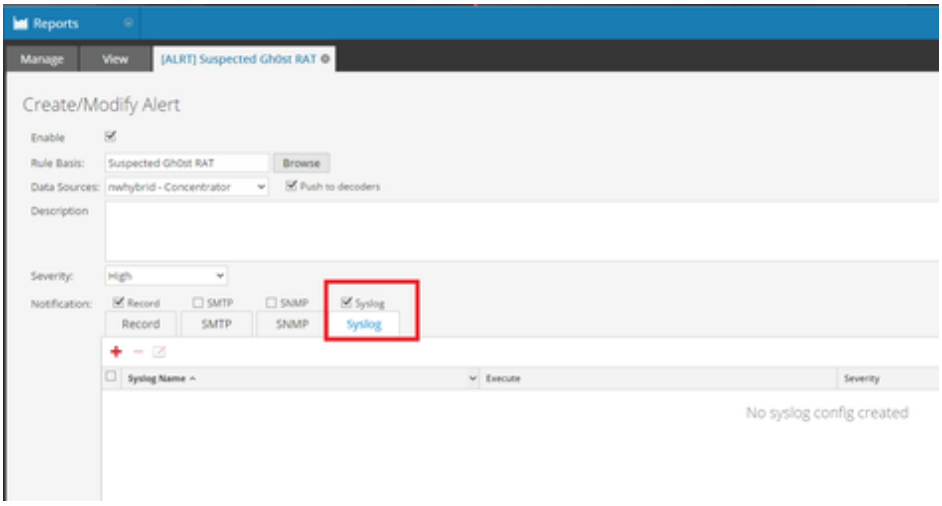
   CEF:0|RSA|NetWitness|10.6.2|${statement}|$severity}| src={sourceAddress} dst=${destinationAddress} spt=${sourcePort} dpt=${destinationPort} rt=${timestamp}



10. Edit the alert that you would like to syslog to SECDO on the **Alerts** page under the **Manage** tab.

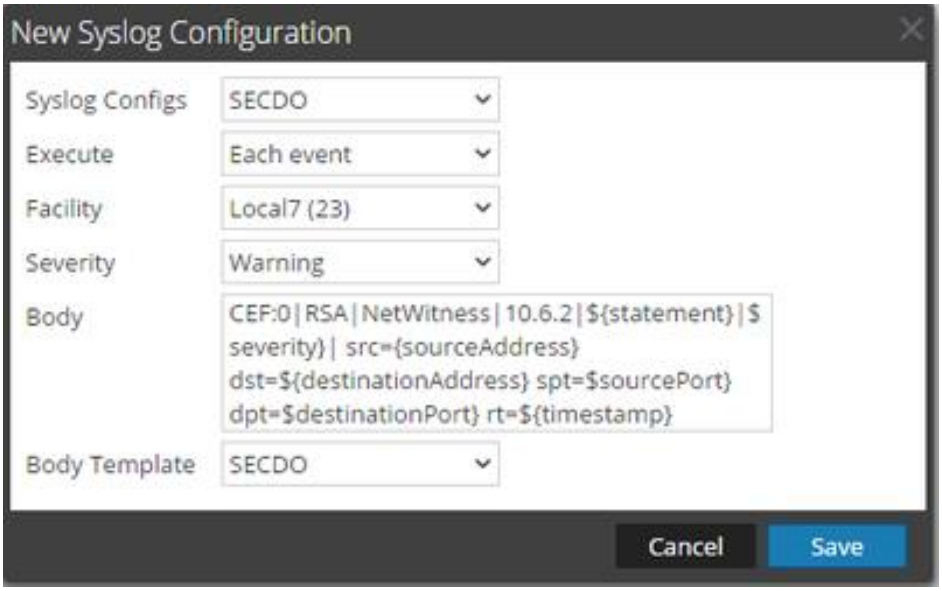


11. Make sure to check the Syslog checkbox as shown below, then add a new Syslog config as shown below.



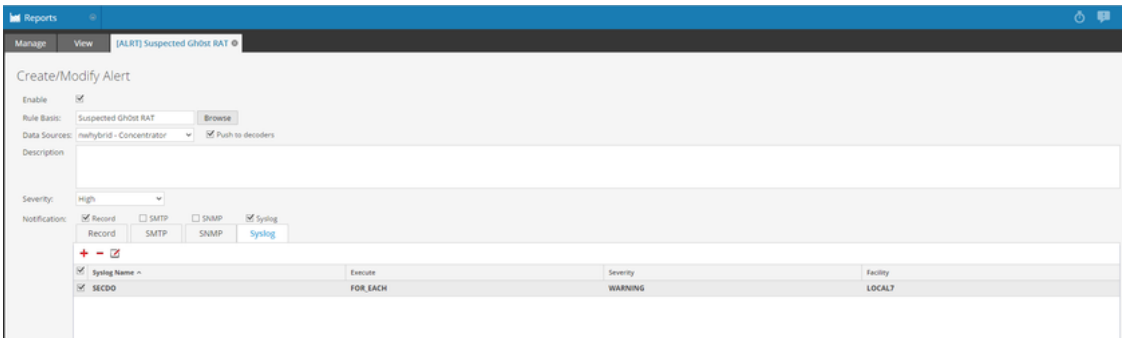
12. Now click on the + to add the Syslog Server

13. The following window will popup. Fill it out as shown below. Note that selecting the Body Template **SECDO** will populate the **Body** field:



14. Click **Save.**

15. Now you should see the following:



16. Now click **save** and you're finished.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Secdo 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 Secdo components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

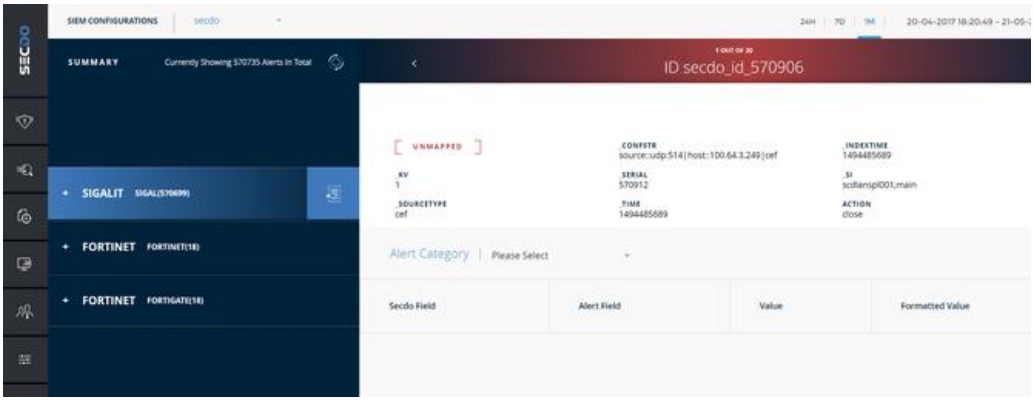
> **Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure Secdo is properly configured and secured before deploying to a production environment. For more information, please refer to the Secdo documentation or website.**

Secdo Configuration

Create an overview of the steps that will be taken to provide interoperability. Use the overview steps as headings for each section as you document the integration.

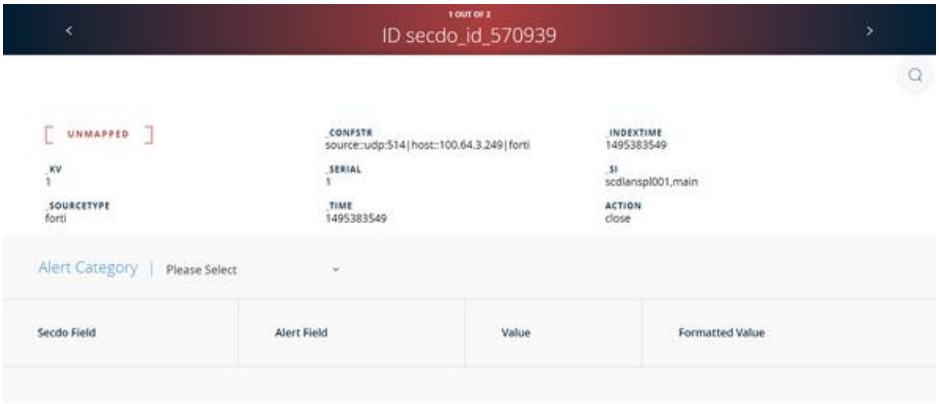
1. Login to Secdo, and switch to the relevant company.

2. Navigate to **https://<SECDOIP>/#/siemConfigurations**.



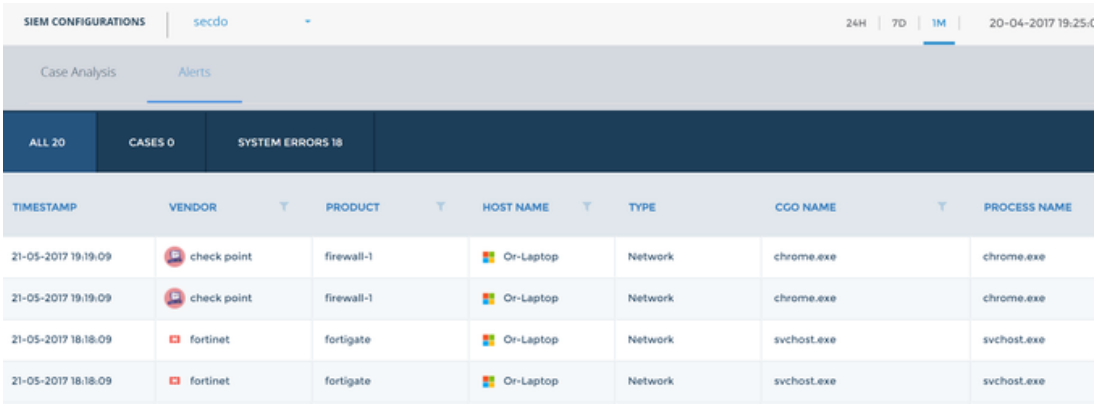
3. On the left side of the screen, the vendor/product pair should be seen once an alert in RSA NetWitness has been triggered.
4. Click on the new vendor/product pair

5. Click **Unmapped**.
6. Choose the relevant **Alert Category**, for example, **Outgoing connection event**.



7. Map the marked fields that are mandatory to map the alert with the data from the alert field by field

8. Hit **Save and Apply**.
9. Navigate to **https://<SECDOIP>/#/siemapp**
10. See the new alerts in the **Alerts** screen:



11. Right-click the relevant line and click on **Open Card** to see the event details:

Certification Checklist for RSA NetWitness

Date Tested: October 20th, 2017

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.4	Virtual Appliance
Secdo Platform	5.0	

RSA NetWitness Test Case	Result
Inline Query/Enrichment	
Query NetWitness for IP Info (source/destination IP)	N/A
Query NetWitness for User Info (usernames, user behavior)	N/A
Query NetWitness for Specific Meta (Other)	N/A
Retrieve NetWitness Log/Packet Data	N/A
Retrieve NetWitness PCAP files	N/A
Alerting / Incident Creation	
NetWitness alert via syslog	✓
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