

RSA® NETWITNESS®
Logs
Implementation Guide

CyberX Platform 2.0

Jeffrey Carlson, RSA Partner Engineering
Last Modified: 01/30/2018

Solution Summary

The integration of CyberX with RSA NetWitness enables a unified approach to IT and OT security in the corporate SOC. Purpose-built for OT security, the CyberX platform combines continuous network monitoring and deep packet inspection with ICS-specific behavioral anomaly detection and military-grade threat intelligence, providing analysts with deep, real-time situational awareness into the specialized ICS protocols, assets, and threats found in OT environments.

RSA NetWitness Features	
CyberX CyberX Platform	
Integration package name	Common Event Format
Device display name within NetWitness	cyberx_cyberx_security_platform
Event source class	ICS
Collection method	Syslog

RSA NetWitness Community

The RSA NetWitness Community is an online forum for customers and partners to exchange technical information and best practices with each other. All NetWitness customers and partners are invited to register and participate in the [RSA NetWitness Community](#).

Release Notes

Release Date	What's New In This Release
01/29/2018	Initial support for CyberX Platform

! > Important: The RSA NetWitness CEF parser is dependent on the partner adhering to the CEF Rules outlined in the *ArcSight Common Event Format (CEF) Guide*.

Eg. Jan 18 11:07:53 host CEF:Version | Device Vendor | Device Product | Device Version | Signature ID | Name | Severity | [Extension]

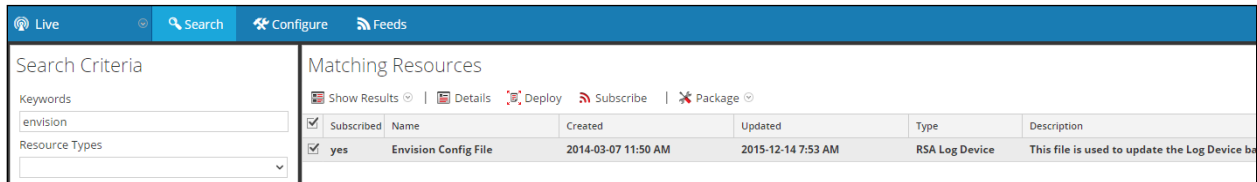
RSA NetWitness Configuration

Deploy the *enVision Config File*

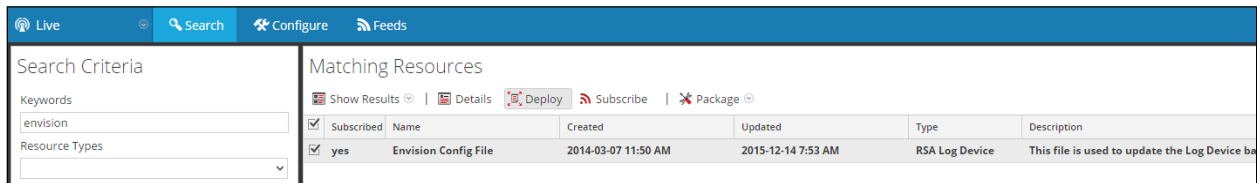
In order to use the RSA Common Event Format (CEF) parser, you must first deploy the *enVision Config File* from the **NetWitness Live** module. Log into NetWitness and perform the following actions:

! > Important: Using this procedure will overwrite the existing `table_map.xml`.

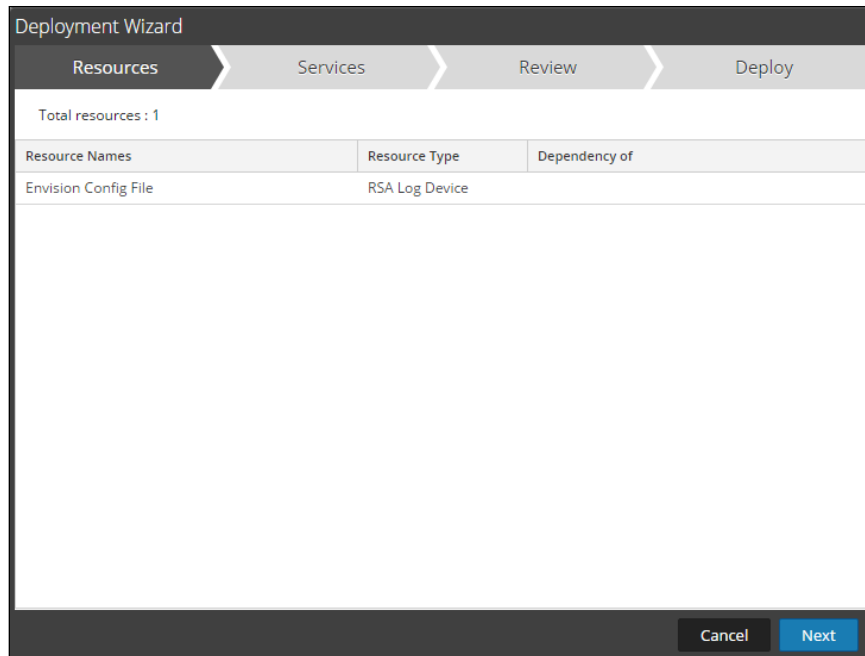
1. From the NetWitness menu, select **Live > Search**.
2. In the keywords field, enter: **enVision**.
3. NetWitness will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



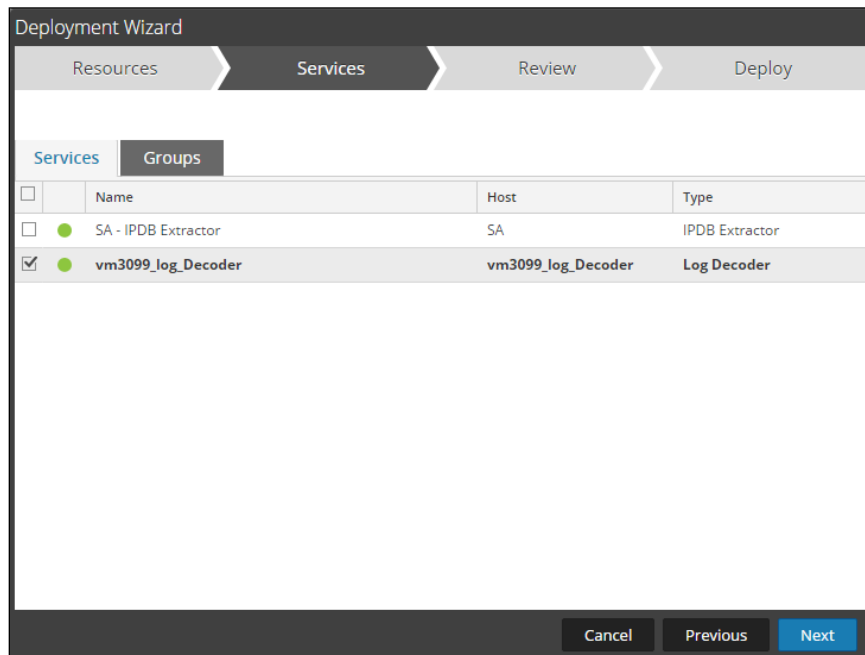
5. Click **Deploy** in the menu bar.



6. Select **Next**.

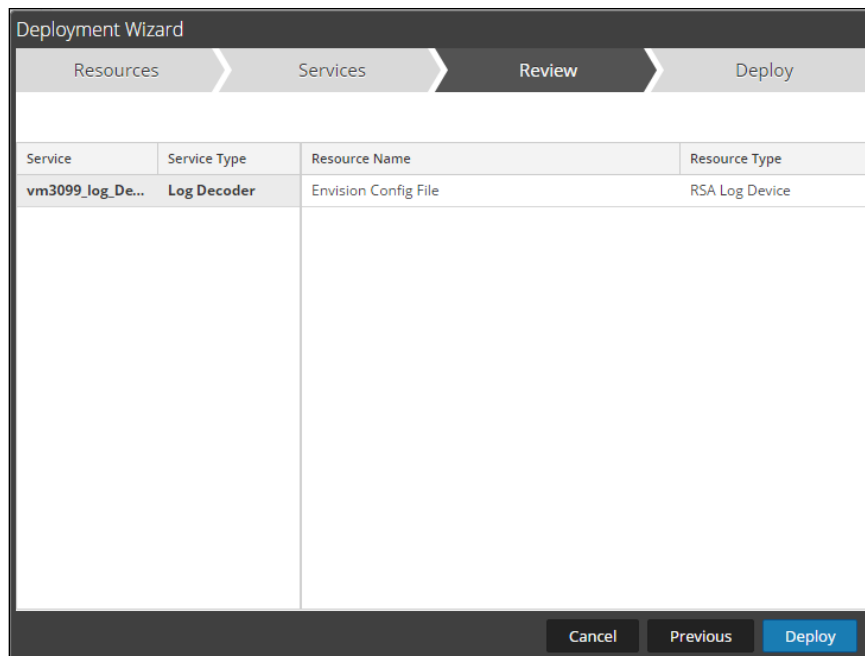


7. Select the **Log Decoder** and select **Next**.

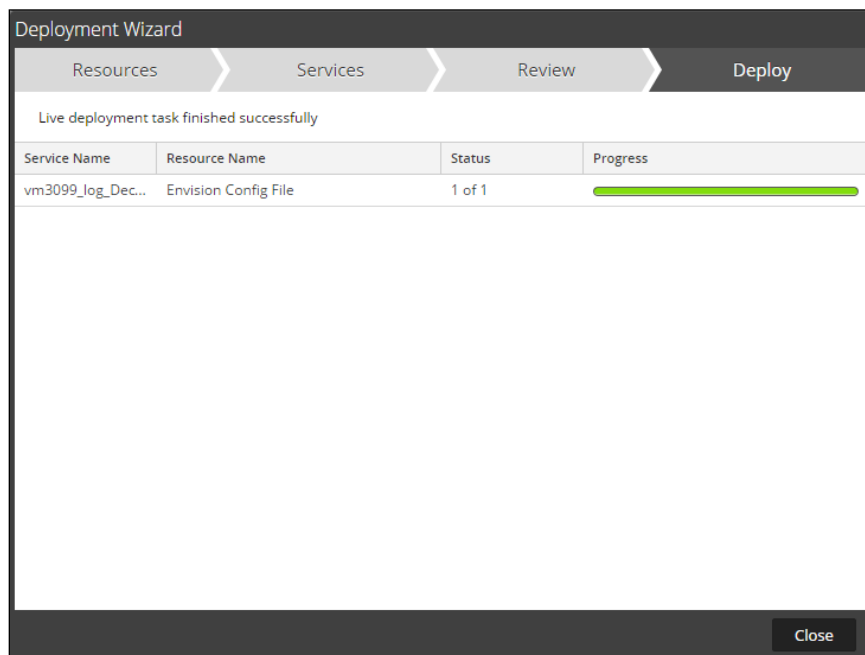


!> Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



9. Select **Close**, to complete the deployment of the Envision Config file.



Deploy the Common Event Format (CEF) Parser

Next, you will need to deploy the *Common Event Format* parser from the **NetWitness Live** module. Log into NetWitness and perform the following actions:

10. From the NetWitness menu, select **Live > Search**.
11. In the keywords field, enter: **CEF**

Search Criteria

Keywords

Resource Types

Tags

Required Meta Keys

Generated Meta Values

Resource Created Date:
Start Date End Date

Resource Modified Date:
Start Date End Date

12. RSA NetWitness will display the **Common Event Format** in Matching Resources.

Live Search Configure Feeds						
Search Criteria		Matching Resources				
Keywords <input type="text" value="cef"/>	<div style="display: flex; justify-content: space-between;"> Show Results Details Deploy Subscribe Package </div>					
Resource Types <input type="text"/>	<input type="checkbox"/>	Subscribed	Name	Created	Updated	Type
	<input type="checkbox"/>	no	Common Event Format	2014-09-17 8:49 PM	2015-05-08 7:46 PM	RSA Log Device
						10.4 or higher.Log Device content for event s...

13. Select the checkbox next to **Common Event Format**.

Live Search Configure Feeds						
Search Criteria		Matching Resources				
Keywords <input type="text" value="cef"/>	<div style="display: flex; justify-content: space-between;"> Show Results Details Deploy Subscribe Package </div>					
Resource Types <input type="text"/>	<input checked="" type="checkbox"/>	Subscribed	Name	Created	Updated	Type
	<input checked="" type="checkbox"/>	no	Common Event Format	2014-09-17 8:49 PM	2015-05-08 7:46 PM	RSA Log Device
						10.4 or higher.Log Device content for event s...

14. Click **Deploy** in the menu bar.

Live Search Configure Feeds						
Search Criteria		Matching Resources				
Keywords <input type="text" value="cef"/>	<div style="display: flex; justify-content: space-between;"> Show Results Details Deploy Subscribe Package </div>					
Resource Types <input type="text"/>	<input checked="" type="checkbox"/>	Subscribed	Name	Created	Updated	Type
	<input checked="" type="checkbox"/>	no	Common Event Format	2014-09-17 8:49 PM	2015-05-08 7:46 PM	RSA Log Device
						10.4 or higher.Log Device content for event s...

15. Select **Next**.

Deployment Wizard

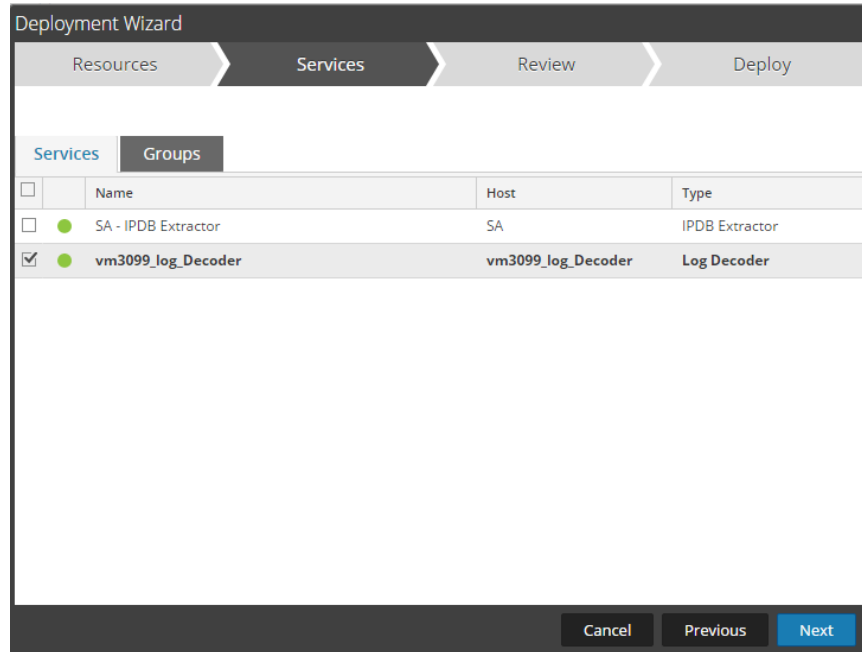
Resources > Services > Review > Deploy

Total resources : 1

Resource Names	Resource Type	Dependency Of
Common Event Format	RSA Log Device	

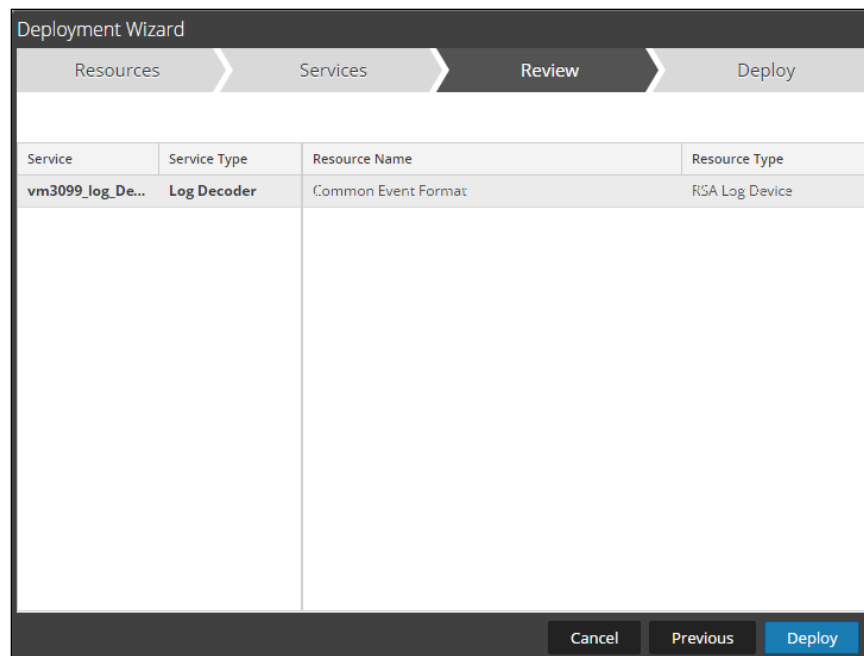
Cancel Next

16. Select the **Log Decoder** and Select **Next**.

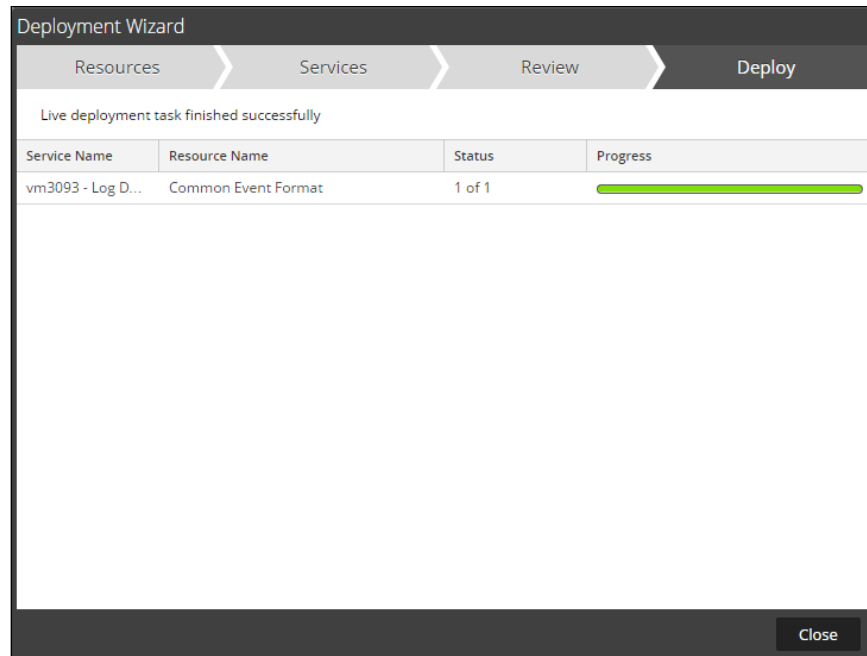


! > Important: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

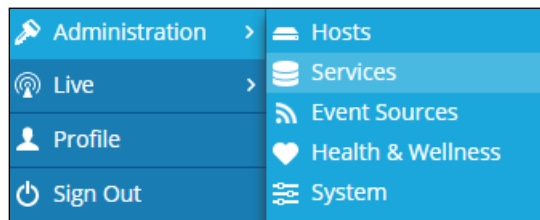
17. Select **Deploy**.




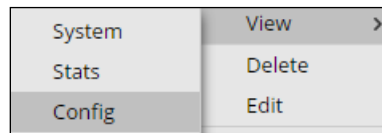
18. Select **Close**, to complete the deployment of the Common Event Format parser.



19. Ensure that the CEF Parser is enabled on the Log Decoder(s) by selecting **Administration, Services** from the NetWitness Dashboard.



20. Locate the Log Decoder and click the gear  to the right and select **View, Config**.



21. **Check** the box next to the cef Parser within the Service Parsers Configuration and select **Apply**.



22. Restart the **Log Decoder services**.


```
<device2meta device="websense" metaName="policyname" label="Policy"/>
<device2meta device="mcafeewg" metaName="virusname" label="Virus
Name"/>
<device2meta device="bit9" metaName="checksum" label="File Hash"/>
<device2meta device="mcafeereconnex" metaName="policyname"/>
<device2meta device="cyberx_cyberx_security_platform"
metaName="severity.desc" label="Severity Description"/>
</ExtensionKey>
<ExtensionKey cefName="cs1Label" metaName="cs_fld" />

<ExtensionKey cefName="cs2" metaName="cs_fld">
    <device2meta device="bit9" metaName="v_instafname"
label="installerFilename"/>
    <device2meta device="cyberx_cyberx_security_platform"
metaName="alert.type" label="Alert Type"/>
</ExtensionKey>
<ExtensionKey cefName="cs2Label" metaName="cs_fld"/>

</DEVICEMESSAGES>
```

Edit the table-map-custom.xml file

!> Important: The Table-Map-Custom.xml file is not overwritten by NetWitness Live during updates, however it is important to maintain backups of the file in the event of a typing error or unforeseen event.

1. Using WinSCP or other application to access the RSA NetWitness Log Decoder open a connection and locate the /etc/netwitness/ng/envision/etc/ folder.
2. If one exists, backup the table-map-custom.xml and then edit the existing table-map-custom.xml file.
3. Add the following entries to the table map to bring in the values from the cs1 and cs2 keys:

```
<mapping envisionName="alert.type" nwName="alert.type" flags="None"/>
<mapping envisionName="severity.desc" nwName="severity.desc" flags="None" />
```

4. There may be a number of keys that are marked as **Transient** by default that will not show up in an event unless they are changed to **None**. For example, application, msg, and severity are all keys that may need to be modified depending on your environment.

Partner Product Configuration

Before You Begin

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

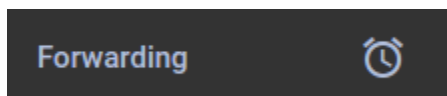
CyberX Platform Configuration

After completing the previous sections, you can now collect events from most sources supporting the Common Event Format (CEF). To do this, you must first create an RSA NetWitness forwarding rule on the CyberX Platform.

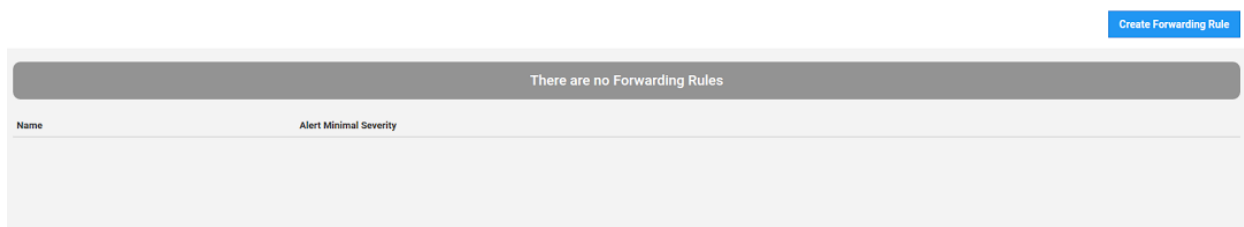
Configuring an RSA NetWitness Forwarding Rule

To create the forwarding rule, perform the following steps:

1. Log in as the admin user and choose **Forwarding** in the main menu:



2. To create a new forwarding rule, click the **Create Forwarding Rule** button:



3. The following **Create Forwarding Rule** screen will be opened:

Create Forwarding Rule

Name	<input type="text" value="Name"/>	Severity	<input type="text" value="▼"/>
Protocols	<input checked="" type="radio"/> All <input type="radio"/> Specific	Engines	<input checked="" type="radio"/> All <input type="radio"/> Specific
Actions	<div style="border: 1px solid #ccc; padding: 5px;">Action <input type="text" value="▼"/> 🗑️</div> <p>+ Add another action</p>		

4. Define the rule name, severity, protocols (all or specific) and engines (all or specific)

Create Forwarding Rule

Name	<input type="text" value="NetWitness forwarding"/>	Severity	<input type="text" value="Warning (and above) ▼"/>
Protocols	<input checked="" type="radio"/> All <input type="radio"/> Specific	Engines	All <input checked="" type="radio"/> Specific
			<div style="border: 1px solid #ccc; padding: 5px;"><input type="text" value="▼"/> Anomaly ✕ Malware ✕ Operational ✕ Policy Violation ✕</div>
Actions	<div style="border: 1px solid #ccc; padding: 5px;">Action <input type="text" value="▼"/> 🗑️</div> <p>+ Add another action</p>		

- Choose the action of **Send to NetWitness** and define the NetWitness machine IP, port & time zone.

Create Forwarding Rule

Name **Severity**

Protocols All Specific **Engines** All Specific

Anomaly
Malware
Operational
Policy Violation

Actions

Action

Host **Port**

Timezone

[+ Add another action](#)

- Click **Submit**, and the new rule will be available.

[Create Forwarding Rule](#)

Name	Alert Minimal Severity	More
NetWitness Forwarding	Warning	More

- To test the integration, choose **Send Test Message** from the **More** options. This option will create a test event in NetWitness

Certification Checklist for RSA NetWitness

Date Tested: January 29th, 2018

Certification Environment		
Product Name	Version Information	Operating System
RSA NetWitness	11.0	Virtual Appliance
CyberX Platform	2.3.3	Virtual Appliance

Security Analytics Test Case	Result
Device Administration	
Partner's device name appears in Device Parsers Configuration	✓
Device can be enabled from Device Parsers Configuration	✓
Device can be disabled from Device Parsers Configuration	✓
Device can be removed from Device Parsers Configuration	✓
Investigation	
Device name displays properly from Device Type	✓
Displays Meta Data properly within Investigator	✓

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