RSA NETWITNESS

This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview** **(https://docs.mandiant.com/home/msv-integrations-overview)**.

This integration is remote capable.

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. IP address used to access the RSA NetWitness concentrator.
2. Port for the concentrator communication (default is 50105).
3. Identify whether the protocol is HTTP or HTTPS for connections to the RSA NetWitness concentrator port.
4. Identify or create the credentials to access RSA NetWitness's concentrator.
5. Identify the field name mappings for the following:

   There could be multiple of each, depending on log sources and configuration.

   a. Source IP
   b. Destination IP
   c. Source Port
   d. Destination Port
   e. Event Start Time (timestamp)
   f. Event Unique ID
   g. Event Signature ID
   h. Event Description
   i. Event Source Host

Configuration

TO ADD THE RSA NETWITNESS INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **RSA NetWitness**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62982c7dad331e21d9050edf/n/netwitness.png)

RSA NetWitness Integration

3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.
4. (Optional) Enter information in the **Query** dialog box to query for base events. Click **Show default query** to see the default query information.
5. Expand **Advanced options**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62982c7dad331e21d9050ee2/n/netwitness-adv.png)

RSA NetWitness Integration (Advanced Options)

6. (Optional) Update the **User Agent**.
7. To enable a query for ESA alerts, check the **Enable query for Alerts** check box.
8. (Optional) Enter information in the **Alert Query** dialog box to query for ESA alerts.

> The default time for an alert can be up to 30 minutes off from when the event fired. If this is the case you must add another field to your alerts with the proper time and add that time to the start_time field map for correlations to work properly.

9. Review the field name mappings; update as necessary.
   a. Inputs are enclosed by square brackets `[]`.
   b. Inputs are columns that could contain the info (`["time"]`).
   c. If there could be multiple commas, enclosed in one set of brackets, encompassed in quotes, and separated by commas (`["msg.id","reference.id", "rid"]`).
10. (Optional) Assign a **Name**.
11. (Optional) Choose **Yes** to save suspicious events.
12. Click **Submit**.

Verify Connectivity

TO VERIFY CONNECTIVITY TO RSA NETWITNESS

Click **Test** to verify that:

- The Director can communicate with NetWitness on the port and protocol specified.
- Credentials are valid and working.