SECURITY ONION - ELSA

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 Security Onion - ELSA

TO UPDATE SECURITY ONION - ELSA

1. Create a username.
2. If using API authentication, identify the token to be used.

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Host and port used for Security Onion - ELSA (defaults are auto-populated).
2. Identify whether the protocol is HTTP or HTTPS for connections.
3. Identify or create the credentials to access Security Onion.

Configuration

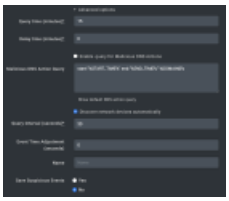
TO ADD THE SECURITY ONION - ELSA INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Security Onion - ELSA**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12d8c9cba0017c2f7ddb/n/so-elsa-836.png)

Security Onion ELSA Integration

3. If necessary, change the **Host** and **Port**.
4. Choose the **Protocol** and **Credential type**.
5. Enter the credentials. Expand Advanced options.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12d7c9cba0017c2f7dd6/n/so-elsa-adv.png)

Security Onion ELSA Integration

6. (Optional) Update **Query time** and **Delay time**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

> If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

7. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
8. (Optional) Select **Discover network devices automatically**.
9. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
10. (Optional) Assign a **Name**.
11. (Optional) Choose **Yes** to save suspicious events.
12. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO SECURITY ONION - ELSA

Click **Test** to verify that:

- The Director can communicate with Security Onion - ELSA with the host, port, and credentials provided.

Run a Malicious or Captive DNS Action and then review the last run query to verify:

- The custom DNS query works as expected (if configured).