SECURITY ONION - ELK

> 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 - ELK

Do the following to allow access to the API port via Security Onion's built-in Firewall.

TO ALLOW ACCESS TO THE API PORT

1. Run the `so-allow` command.
2. Choose option **e**.
3. Enter the `director's ip address` .

Update the Validation Platform

Prerequisites

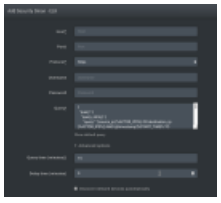
Information to gather before you start:

1. Host and port used for Security Onion - ELK.
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 - ELK INTEGRATION

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



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e6c9cba0017c2f7e76/n/sec-onion-elk.png)

Security Onion ELK Integration

3. Enter information for the **Host**, **Port**, **Username**, and **Password**.
4. Expand **Advanced options**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e1c9cba0017c2f7e43/n/sec-onion-elk1.png)

Security Onion ELK Field mappings

5. Review the field name mappings and update as necessary. Default mappings exist for Snort and Bro.
    a. You can use standard UNIX wildcards in the Index name, allowing you to match several index files (for example, `snort-*` matches `snort-123` and `snort-abc`).
    b. Inputs are enclosed by square brackets `[]`.
    c. Inputs point to the path location (`["_id"]`).
    d. Nested locations should be enclosed in one set of brackets, encompassed in quotes, and separated by commas (`["_source","src_ip"]`).
6. Add a new **Index** and configure those fields, if necessary.
7. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
8. (Optional) Select **Discover network devices automatically**.
9. (Optional) Assign a **Name**.
10. (Optional) Choose **Yes** to save suspicious events.
11. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO SECURITY ONION - ELK

Click **Test** to verify that:

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

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.