SUMO LOGIC

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 Sumo Logic

TO UPDATE SUMO LOGIC

1. Generate a Sumo Logic API Access ID/Key pairing specifically for the Validation Platform's use. Refer to the **Sumo Logic Documentation** (https://help.sumologic.com/Manage/Security/Access-Keys) for instructions.

   Sumo Logic may not recognize the `validation.cloud` FQDN extension. When you configure your API Access ID/Key in Sumo Logic's admin console, you do not need to specify the domain.

2. Create a Sumo Logic account with sufficient permissions. Read permissions are required, at minimum.
3. (Optional) Create a custom field for the event_time field Security Validation uses. The default time in Sumo Logic may be incorrect because it is based on ingest time, not detect time. If you are concerned about this, you can create a new field, such as timestamp, to capture the required info. An example of this is shown in the code below. For additional details, see Sumo Logic's documentation on formatDate.

```
| formatDate(toLong(timestamp*1000),"MM-dd-yyyy'T'HH:mm:ss'Z'") as event_time
```

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify the Sumo Logic host used to access the Sumo Logic cloud. The host is visible in the URL after logging in to the Sumo Logic web user interface.
2. API Access ID/Key.
3. Sumo Logic credentials.
4. 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 Signature ID
   f. Event Name
   g. Event Source Host
   h. Event Time

Mandiant

Configuration

TO ADD THE SUMO LOGIC INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Sumo Logic**.
3. Select the Host.
3. Enter the **API Access ID** and **Key**.
4. Review and update the **Query** to include instance-specific field names.

   The default queries can be viewed by clicking **Show default query**.

5. Expand **Advanced options**.
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 platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. 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, this configuration impacts the pass/fail results for AEDA monitors.

7. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

   If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

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**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12dbc9cba0017c2f7e05/n/sumo.png)

Sumo Logic Integration

Set up Proxy Assignment

If all outbound connections go through a proxy, you may want to set up a proxy definition and assignment for your integration. For information on setting up your proxy rules, see **Proxy Rules (https://docs.mandiant.com/home/msv-proxy-rules)**.

Verify connectivity

TO VERIFY CONNECTIVITY TO SUMO LOGIC

Click **Test** to verify that:

- The Director can communicate with Sumo Logic using the API access information on the port and protocol specified.
- User credentials are working.