LOGRHYTHM SQL

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 not remote capable.

Update LogRhythm SQL

- Verify you have the latest LogRhythm Knowledge Base updates added to your instance. These updates contain rules and identifiers for various actors and actions.
- Disable LogMart on any log sources where it is not explicitly required. The resources used by LogMart can cause delays when Actions are run.

Update the Validation Platform

Prerequisites

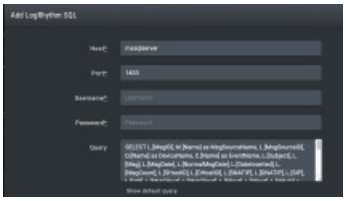
Information to gather before you start:

- Identify the host (name or IP) and Port information.
- Have a valid account for LogRhythm SQL.

Configuration

TO ADD THE LOGRHYTHM SQL INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **LogRhythm SQL**.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e0c9cba0017c2f7e34/n/logrhythm-sql.png)

LogRhythm SQL Integration

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

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12dfc9cba0017c2f7e2e/n/logrhythm-sql-adv.png)

5. (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.

6. (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.
7. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will be only be used when you run Email Actions.
8. (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.

   If you find that LogRhythm SQL is matching too many noisy logs, we recommend you add MsgSourceID to the WHERE clause in the Host CLI Actions query. For example, WHERE L.[NormalMsgDate] = '%START_TIME%' AND L.[MsgSourceID] = 1. If the events are still too noisy, consider adjusting your Risk Based Priority (RBP) settings in LogRhythm.

9. (Optional) Select **Discover network devices automatically**.
10. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
11. (Optional) Assign a **Name**.
12. (Optional) Choose **Yes** to save suspicious events.
13. Click **Submit**.

Verify Connectivity

TO VERIFY CONNECTIVITY

Click **Test** to verify that:

- The Director can communicate with the LogRhythm SQL host on the port specified.
- The LogRhythm SQL credentials are valid and working.