Mandiant

CYBEREASON

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 Cybereason

Identify or create credentials to access Cybereason with read access, at minimum.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Cybereason Host and Port.
- Cybereason account with read access, at minimum.

Configuration

TO ADD THE CYBEREASON INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Cybereason**.
3. Enter the **Host** information.
4. Update the default **Port** and **Protocol** information if necessary (Port may be 8443 instead of 443 if it is hosted by Cybereason).
5. Enter the **Username** and **Password**.
6. Expand **Advanced options**.
7. (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.

8. Enable and configure the **Malware query**.
9. (Optional) Assign a **Name**.

10. Click **Submit**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12dfc9cba0017c2f7e30/n/cybereason-1.png)

Cybereason 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 CYBEREASON

Click **Test** to verify that:

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