Mandiant

CYLANCE INTEGRATION WITH SECURITY VALIDATION

This integration collects events generated by Cylance to test the efficacy and configuration of the security control using Security Validation jobs.

Use this document to configure the integration using one of the following methods:

- MSI (Supported and recommended for new integration configurations)
- Legacy (Supported for existing integration configurations)

Configure MSI Integration

This method is the recommended approach for configuring new integrations in Security Validation.

API Calls

API	Usage
`/auth/v2/token`	Retrieve an authentication token from Cylance
`/devices/v2`	Retrieve a list of devices and the associated threats from Cylance

Supported Versions

Cylance API v2

Before You Begin

To configure this integration, you need:

- The hostname or IP address of your Cylance instance
- App ID
- App Secret
- Tenant ID

Create a new Application in Cylance

1. Log into Cylance Console as an administrator.
2. Navigate to **Settings > Integrations**.
3. Click "Add Application", then fill in an Application Name and the desired privileges.
4. Click "Save", then make a note of the App ID and App Secret that are displayed.

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > Cylance**.

   You can add this as either a Direct or Remote Integration.
3. Enter a meaningful **Integration Name**.
4. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all outbound connections go through a proxy, first, set up a **Proxy Rule** (https://docs.mandiant.com/home/msv-proxy-rules).
5. Change the **HttpProtocols** to use for requests. (**Https** or **Http**.)
6. For the **Host**, enter the hostname of your Cylance instance.
7. Enter a **Port** value. The default is **443**.

8. Choose the API version (**V1** or **V2**) for **CarbonBlackResponseApiVersion**.
9. Enter the **App Id** and **App Secret** that you configured.
10. Enter the **Tenant Id** of your Cylance instance.
11. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
12. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
13. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **500**.
14. Optional: Modify the **Field Map** values, as necessary.

    - Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
    - When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.

15. Optional: Expand **Advanced options** and update the information as necessary.
    a. 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.

    b. Update **Query Interval** (seconds).
    c. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
    d. Modify the **Correlation Query Interval**, if necessary (minutes).
    e. Select **Discover network devices automatically**, the default and recommended option.

    If unselected, reported events won't include product information for any matching network security technology.

    f. Select **Save Suspicious Events**.
    g. Modify the **Event Time Adjustment** (seconds). The default is **0**.
    h. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events and 10 alerts.

16. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.
2. From the Direct Integrations table, click ⋮ **> Test** to verify that:
    - The Director can communicate with the integration host on the port and protocol specified.
    - The integration credentials are valid and working.

For more information on setting up queries, see **Manage Integrations (https://docs.mandiant.com/home/msv-managing-integrations)**.

Configure Legacy Integration

> 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)**.

Cylance maintains a history of threats and does not report new threats of the same type. If you want Actions to be identified each time they are run, you must delete Quarantined items in Cylance before running the Action.

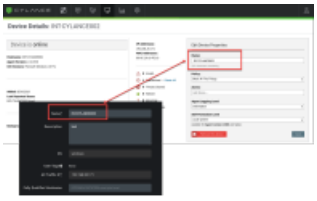
TO DELETE QUARANTINED ITEMS IN CYLANCE

In the Cylance Portal, navigate to the Device representing the Validation Platform Actor and delete all the Quarantined items.

Update Cylance

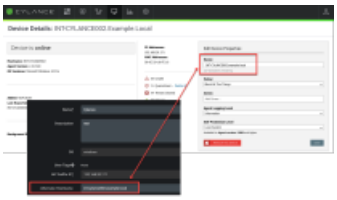
Add a Device entry in Cylance for each Endpoint Actor in the Validation Platform from which you want to receive Cylance events.

- The name of the Device entry in Cylance must match either the Validation Platform Actor Name or its Alternate Hostname.
  If the names do not match, events will not be related correctly.
- This entry must have Read permissions for Devices, Threat, and User.
- The device names in Cylance and the Actors configured in the platform are automatically synced every 15 minutes.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e9c9cba0017c2f7e8c/n/cylance-actor-option1.png)

Cylance Device name matching Actor Name



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e6c9cba0017c2f7e72/n/cylance-actor-option2.png)

Cylance Device name matching Actor's Alternate Hostname

Update the Validation Platform

Prerequisites

Information to gather before you start:

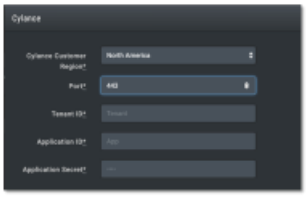
- Cylance Port information.
- Cylance Tenant ID, Application ID, and Application Secret.

Configuration

TO ADD THE CYLANCE INTEGRATION

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

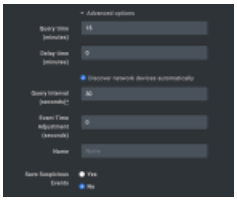
> You can add this as either a Local or Remote Inetgration.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e2c9cba0017c2f7e47/n/cylance.png)

Cylance Integration

3. Choose the **Cylance Customer Region**.
4. (Optional) Update the default **Port**.
5. Enter the **Tenant ID** and **Application ID**.
6. Enter the **Application Secret**.
7. Expand **Advanced options**.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12d8c9cba0017c2f7de2/n/cylance-adv.png)

Cylance Integration (Advanced Options)

8. (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.

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

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 CYLANCE

Click **Test** to verify that:

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

Error: Invalid JWT Payload

There are two places you might see this error:

- In the UI when running the test query
- In the logs when Cylance tries to match events during a Job

There are several possible causes of this issue:

1. (Most Common) - The Time on the Director is out of sync with the Cylance Server by +/- 15 minutes. The Cylance Server uses NTP to stay accurate.
2. The Keys that were entered were mistyped or copy/pasted wrong.
3. The wrong key may have been used. For example, entering the App Token into the App Secret field.
4. (Unconfirmed) The Cylance keys being used are expired or not recognized by Cylance.