Mandiant

SENTINELONE INTEGRATION WITH SECURITY VALIDATION

This integration collects events generated by SentinelOne 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
`/web/api/v2.1/threats`	Returns threats detected on endpoints with the SentinelOne agent installed

Supported Versions

SentinelOne API v.2.1

Before You Begin

To configure this integration, you need:

- The hostname of your SentinelOne instance
- A SentinelOne API Key

Generate a SentinelOne API Key

1. Login to the SentinelOne Management Console as the user you want to authorize API requests with.
2. From the **Help** menu, select **API Doc**.
3. In the API Doc, navigate to **Users → Generate API Token**.
4. Select **Run on console**.
5. Select **Run API query**.
6. Copy the value of the token key displayed in the **RESPONSE** section of the page and paste it to a safe location for use in the integration configuration.

Configure Security Validation

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

   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 SentinelOne instance.
7. Enter a **Port** value. The default is **443**.

8. Optional: Change the **SentinelOneAPIVersion**, if needed. The default is **V2.1**.
9. Enter the **Api Key** value that you generated.
10. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
11. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
12. Optional: Add **Queries** as needed. A default is provided.
13. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **500**.
14. 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.

15. 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

Mandiant

> 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)**.

The SentinelOne Integration uses SentinelOne's API to function correctly. Versions 2.0 and 2.1 of the SentinelOne API are supported.

The API request that the SentinelOne integration uses is bound by time limits. The time on the Director and Actor must be kept synchronized, or else no events will match.

This integration is remote capable.

Update SentinelOne

TO UPDATE SENTINELONE

1. Define a username that will be attached to the API key that the Validation Platform will use. The username must have at least Site Viewer access.
2. Use the SentinelOne Portal to generate an API key that can be used in the integration setup in the Director.

Update Security Validation

Prerequisites

Information to gather before you start:

- The SentinelOne API key.
- The name of the host where SentinelOne is installed.
- The Actor configured with the exact name of the host that is running SentinelOne (shown in the SentinelOne Portal).

Configuration

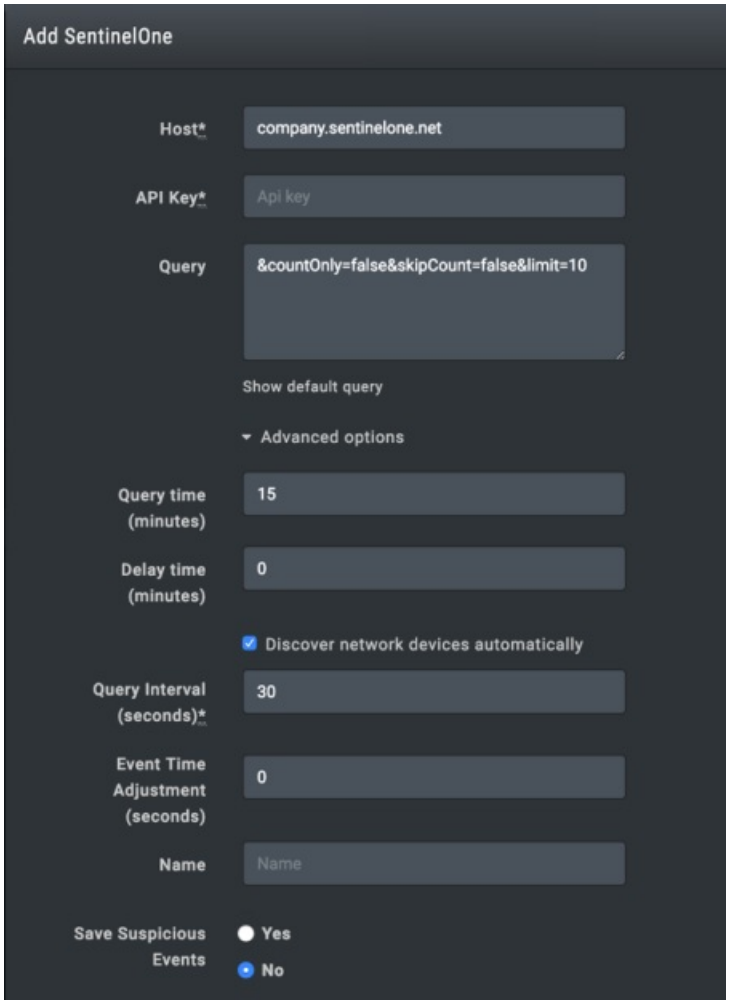
TO ADD THE SENTINELONE INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **SentinelOne**.
3. Enter the **Host**.
   This is the SentinelOne address given to the customer by SentinelOne.
4. Enter the **API Key**.
5. Select the **API Version**.
6. (Optional) Update the **Query**.
7. Expand **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. (Optional) Clear **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**.



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 SENTINEL ONE

Click **Test** to verify that:

- The Director can communicate with the Sentinel One IP address on the port specified.
- The API key is working and has the necessary privileges.