Mandiant

SOPHOS CLOUD INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validate that security tools are writing log events to Sophos Cloud to ensure compliance with security policies and regulations
- Collect events generated by security tools that write to Sophos Cloud to test the efficacy and configuration of security controls using Security Validation jobs

API Calls

API	Usage
`/gateway/siem/v1/events`	Retrieve a list of events from Sophos Cloud
`/gateway/siem/v1/alerts`	Retrieve a list of alerts from Sophos Cloud

Supported Versions

Sophos Cloud

Before You Begin

To configure this integration, you need:

- API Token
- API Key

Get an API Token and API Key

1. Open Sophos Central's admin console.
2. Go to Global Settings and select API Token Management.
3. Click Add Token, enter the necessary information, and save your changes.
4. Make a note of both the authorization token and API key.

Configure Security Validation

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

   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. Optional: Change the **HttpProtocols** value to determine what protocol is used for requests (**Https** or **Http**).
6. Enter the **Host** for the Sophos Cloud instance. The default is **api1.central.sophos.com**.
7. Enter a **Port** value. The default is **443.**
8. Enter the **Api Key** and **Api Token** that you generated.
9. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
10. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
11. 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. Configure correlation queries:
    i. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
    ii. Modify the **Correlation Query Interval**, if necessary (minutes).
d. 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.

e. Select **Save Suspicious Events**.
f. Modify the **Event Time Adjustment** (seconds). The default is **0**.
g. 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.

12. 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).