

TRELLIX ENDPOINT DETECTION AND RESPONSE WITH SECURITY VALIDATION

This integration lets you collect events generated by Trellix Endpoint Detection and Response (EDR) to test the efficacy and configuration of the security control using Security Validation jobs.

API Calls

API	Usage
<code>/edr/v2/alerts</code>	Retrieves detections and alerts from the Trellix EDR

Supported Versions

API v2

Before You Begin

To configure this integration, you need:

- A valid `client_id`, `client_secret` and `x-api-key` for a user with permissions to access the API endpoints. Get the `x-api-key` from your Trellix on-boarding email. Also, you can navigate to the Trellix API Access Management page to fetch the API key.
- The hostname or IP address of your Trellix EDR Manager instance.
- Ensure the Trellix EDR Manager is accessible from your network.

Configure the Integration in Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > Trellix Endpoint Detection & Response (EDR)**.



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**, change the value if needed. The default is **api.manage.trellix.com**.
7. Enter a **Port** value. The default is **443**.
8. Enter the **Client Id** and **Client Secret** values that you generated.
9. Enter the **Authorization URL**. The default is **https://auth.trellix.com/auth/realms/IAM/protocol/openid-connect/token**.
10. Enter the **x-api-key** value that's used to access the required API endpoints.
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: Change **Queries**, if needed. A default value is provided.
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: Modify the **Page Size** value for requests to the upstream server. The default is **500**.

16. 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.

17. 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>).