Mandiant

TREND AI VISION ONE INTEGRATION WITH SECURITY VALIDATION

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

API Calls

API	Usage
`/v3.0/healthcheck/connectivity`	Health check
`/v3.0/search/detections`	Retrieve events
`/v3.0/search/endpointActivities`	Optional: Retrieve endpoint activities
`/v3.0/workbench/alerts`	Retrieve alerts

Supported Versions

v3 API

Before You Begin

To configure this integration, you need:

- A Trend AI Vision One API Key
- The hostname of the API Server for your region (**https://automation.trendmicro.com/xdr/Guides/Regional-Domains**)

Generate an API Key

1. Sign in to your Trend AI Vision One console.
2. Select **Administration**.
3. Select **Add API Key**.
4. Enter any name for the application, select the SIEM role, and click **Add**.
5. Copy the API Key value, then 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 > Trend AI Vision One**.

   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 Trend AI Vision One instance. The default is **api.xdr.trendmicro.com**.
7. Enter a **Port** value. The default is **443.**
8. Enter the **Api Key** 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: Modify the **FieldMapModel** values, as necessary.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- 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.

12. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **500**.
13. 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.

14. 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.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- 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)**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.