Mandiant

DARKTRACE INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validate that security tools are writing log events to Darktrace to ensure compliance with security policies and regulations
- Collect events generated by security tools that write to Darktrace to test the efficacy and configuration of security controls 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.

To configure an integration, this document walks you through the following high-level steps:

1. **Configure the third-party technology**
2. **Configure Security Validation**
3. **Verify connectivity**

API calls

API	Usage
`/details`	Retrieve a list of events from Darktrace
`/modelbreaches`	Retrieve a list of model breaches from Darktrace
`/status`	Used to test connectivity and authentication settings
`/advancedsearch/api/search`	Run queries and retrieve a list of events

Supported versions

Darktrace Threat Visualizer v6.1

Preparation

To configure this integration, you need:

- The hostname or IP address of your Darktrace instance
- API Secret (Private Token)
- API Key (Public Token)

Acquire an API token pair

1. Log into Darktrace Threat Visualizer with an account that has permission to access and modify the System Config page
2. Navigate to the System Config page, then select "Settings" from the left-hand menu
3. Locate the "API Token" subsection and click "New"
4. Make a note of the Public and Private Token, as the Private Token will not be displayed again.

The integration calls to Darktrace are signed with a timestamp in UTC. This is a requirement of the API Authentication HMAC Signature.

Configure Security Validation

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

   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. Enter the **Host** value for the Darktrace instance as a hostname or IP address.
6. Enter a **Port** value. The default is **443**.
7. Optional: Change the **HttpProtocols** value to determine what protocol is used for requests (**Http** or **Https**).
8. Enter the **Api Key** and **Api Secret**.
9. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
10. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
11. Optional: Check **Use Advanced Search Endpoint** if you want to use this endpoint for queries. Customer-defined queries run only when this setting is enabled.

    The macros for this option are `%IPS%` and `%HOSTNAMES%`, resulting in the following queries:

    ```
    DEFAULT_QUERIES = [
       {
          "name": "IP Query",
          "query": f"@fields.src_ip:({IPS}) OR @fields.dest_ip:({IPS})",
       },
       {
          "name": "Hostname Query",
          "query": f"@fields.host:({HOSTNAMES})",
       },
    ]
    ```

12. 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.

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.
    - 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).

This integration is remote capable.

Update integration

Identify or create an API key for use with the Validation Platform. This is done by signing into Darktrace and going to Admin > Config > API Token Generate.

API calls

The following API calls are used by the Validation Platform.

Purpose	Call
Verify we can read devices	`/devices?seensince=7days`
Get Device Specific Details by IP	`/devices?ip=:ip`
Get Events for Device within specific timeframe	`/details?did=:did&starttime=:start_time&endtime=:end_time`

Update the Validation platform

Prerequisites

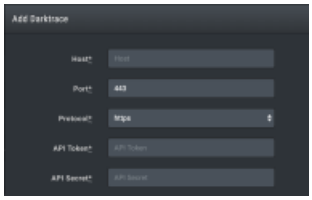
Information to gather before you start:

- Hostname
- Port
- API Key
- API Secret

Configuration

TO ADD THE INTEGRATION

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



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e9c9cba0017c2f7e8d/n/darktrace1.png)

Darktrace Integration

3. Enter the **Host** and **Port**.
4. Select the **Protocol**.
5. Enter the **API Token** and **API Secret**.
6. Expand **Advanced options**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e7c9cba0017c2f7e7a/n/darktrace-adv.png)

Advanced section of Darktrace Integration

7. (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.

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

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.

If you see the following error, either the API Key or the API Secret is incorrect or there is a time mismatch:

```
Api signature Error
```

Requests to API are signed with a timestamp. If the requesting machine (Director or Remote Actor) is out of time sync more than a few minutes, the requests will fail.