Mandiant

SECURONIX INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validates that security tools are writing log events to Securonix to ensure compliance with security policies and regulations
- Collects events generated by security tools that write to Securonix 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.

API Calls

API	Usage
`/Snypr/ws/spotter/index/search`	Query for events and correlated alerts from Securonix
`/Snypr/ws/token/generate`	Retrieve an authentication token from Securonix

Supported Versions

Securonix SNYPR (Latest)

Before You Begin

To configure this integration, you need:

- A valid username and password for a user with permissions to use the API endpoints described in the previous step
- The hostname or IP address of your Securonix instance

Configure Security Validation

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

   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 Securonix instance.
7. Enter a **Port** value. The default is **443**.
8. Enter the **Database Type**. The default is **mssql**.
9. Enter the **Username** and **Password** for the account that can use API endpoints.
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: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
12. Optional: Add or remove **Queries** and **Correlation Queries**, as needed. A default value for **Correlation Queries** is provided.
13. Optional: Modify the **Page Size** value for requests to the upstream server. The default is **500**.
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: Change the **TimeZones** value. The default is **UTC**.
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. 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.

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)**.

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 Securonix SNYPR

Identify or create credentials to access Securonix with read access, at minimum.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
/Snypr/ws/token/generate	Get API access token for all calls
/Snypr/ws/spotter/index/search?query=(query)...	Timeboxed Query for getting events from Securonix

Update the Security Validation Platform

Prerequisites

Information to gather before you start:

- Identify the hostname used to access Securonix SNYPR
- Identify the port used for Securonix communication
- Identify the username and password for your Securonix account

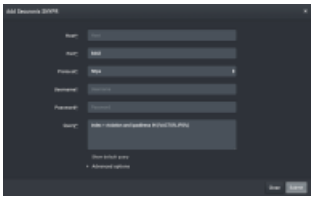
Configuration

 You can add this as either a Local or Remote Integration.

TO ADD THE SECURONIX SNYPR INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Securonix SNYPR**.
3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.
4. Review and update the Query as needed.

   The %ACTOR_IPS% variable can be used in all queries. This improves event matching.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12ddc9cba0017c2f7e1d/n/securonix-snypr.png)

Securonix SNYPER Integration

5. Expand **Advanced options**.
6. (Optional) Update **Query time**, if necessary.
7. (Optional) Update the **Page size**, if necesary.
8. (Optional) Enable **Verify SSL**, if necessary.
9. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
10. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will only be used when you run Email Actions.
11. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

    If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

12. Identify the field name mappings for the following (there could be multiple of each, depending on log sources and configuration):
    - Source IP
    - Destination IP
    - Source Port
    - Destination
    - Port
    - Event Source Host
    - Host
    - Event Start Time (timestamp)
    - Event Unique ID
    - Event Signature ID
    - Event Description
    - Email Sender
    - Email Recipient

- Email Subject
- URL
- Username

13. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
14. (Optional) 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.

15. (Optional) Assign a **Name**.
16. (Optional) Choose **Yes** to save suspicious events.
17. Click **Submit**.

Securonix SNYPER Integration - advanced options

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 SECURONIX SNYPR

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.