

OPENSEARCH INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validates that security tools are writing log events to Opensearch to ensure compliance with security policies and regulations
- Collects events generated by security tools that write to Opensearch to test the efficacy and configuration of security controls using Security Validation jobs
- Provides ability to match alerts generated by watcher. There are three ways to get alert correlation working.
 - Create your watcher rule to write a "base_event_uids" property to the top level of your alert. This should be the ids of base events as an array of strings. Works for alerts generated from one, or many events.
 - Create your watcher to save the _id property of the base event to the top level of your alert. Works for alerts generated from one event only
 - Create your watcher to save the results of a search to the top level of your alerts (i.e. save hits property of the search into alert hits property). Works for alerts generated from one, or many events.

API Calls

API	Usage
/	Basic health check endpoint
/_cat/indices	List indices
/_search	Retrieve results from query
/_{target}/_search/point_in_time	Start paginated query

Supported Versions

Opensearch 2.9+


Before You Begin

To configure this integration, you need:

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

Configure the Integration in Security Validation

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

 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. Enter the **Host** value (hostname or IP address) of your Opensearch instance.
7. Enter a **Port** value. The default is **443**.
8. Enter the **Username** and **Password** for the user with permissions to use API endpoints.
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. Enter values for the **Target**. This can be a comma-separated list of data streams, indices, and index aliases to search. Wildcard (*) expressions are supported. Examples: `index_one` , `index_one,index_two` , `index_*` , `cluster_one:index_one` , `cluster_*.*`
12. Optional: Change **Queries**, if needed. Default values are provided: **IP Query**, **Hostname Query**, **DNS Query**, and **Email Query**.
13. 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.

14. Optional: Modify the **Page Size** for each request to an upstream server, if needed. The default is **500**.
15. 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.

16. 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 \(https://docs.mandiant.com/home/msv-managing-integrations\)](https://docs.mandiant.com/home/msv-managing-integrations).