Mandiant

PALO ALTO NETWORKS CORTEX XDR INTEGRATION WITH SECURITY VALIDATION

This integration collects events generated by Palo Alto Networks Cortex XDR to test the efficacy and configuration of the security control 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
`/public_api/v1/api_keys/validate/`	Used to test connectivity and authentication settings
`/public_api/v1/alerts/get_alerts_multi_events`	Retrieve a list of alerts from Palo Alto Networks Cortex XDR

Supported Versions

Palo Alto Networks Cortex XDR API v1

Before You Begin

To configure this integration, you need:

- API Key
- API Key ID
- The hostname or IP address of your Palo Alto Networks Cortex XDR instance

Configure Security Validation

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

   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 Palo Alto Networks Cortex XDR instance.
7. Enter a **Port** value. The default is **443**.
8. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
9. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
10. Enter the **API Key** and **API Key Id** values that you generated.
11. Optional: Change the **API Key Type**, if needed.

12. Optional: Add **Alert Sources**, if needed. These should resolve to supported alert source filters.
13. Optional: Select **Enable Queries** if you want to allow additional calls to the XQL endpoint.

    This endpoint has a limited daily quota, depending on the size/frequency of your queries you may need to purchase additional query units. See **Running XML Query APIs** (https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-API-Reference/Running-XQL-Query-APIs) for more information.

14. Optional: Add **Queries**, if needed. A default for **IP Query** is provided.
15. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **100**.
16. 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.

17. 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.

}

18. 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).

Cortex XSOAR from Palo Alto Networks is a security orchestration, automation, and response (SOAR) platform that unifies case management, automation, real-time collaboration, and threat intel management to serve security teams across the incident lifecycle.

This integration is remote capable.

This integration requires three steps:

1. Create Credentials to Access Cortex XDR via API from the Security Validation Platform.
2. Add the Cortex XDR Integration to the Security Validation Platform.
3. Verify connectivity.

Create Credentials to Access Cortex XDR via API from the Security Validation Platform

- Identify the hostname used to access Palo Alto Cortex XDR.
- Identify the port used for Palo Alto Cortex XDR communication.
- Identify the ID and Key used to access the Palo Alto Cortex XDR API.

See the **Cortex XDR API documentation** (https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-api/cortex-xdr-api-overview/get-started-with-cortex-xdr-apis) for information on generating and accessing these values.

API Calls

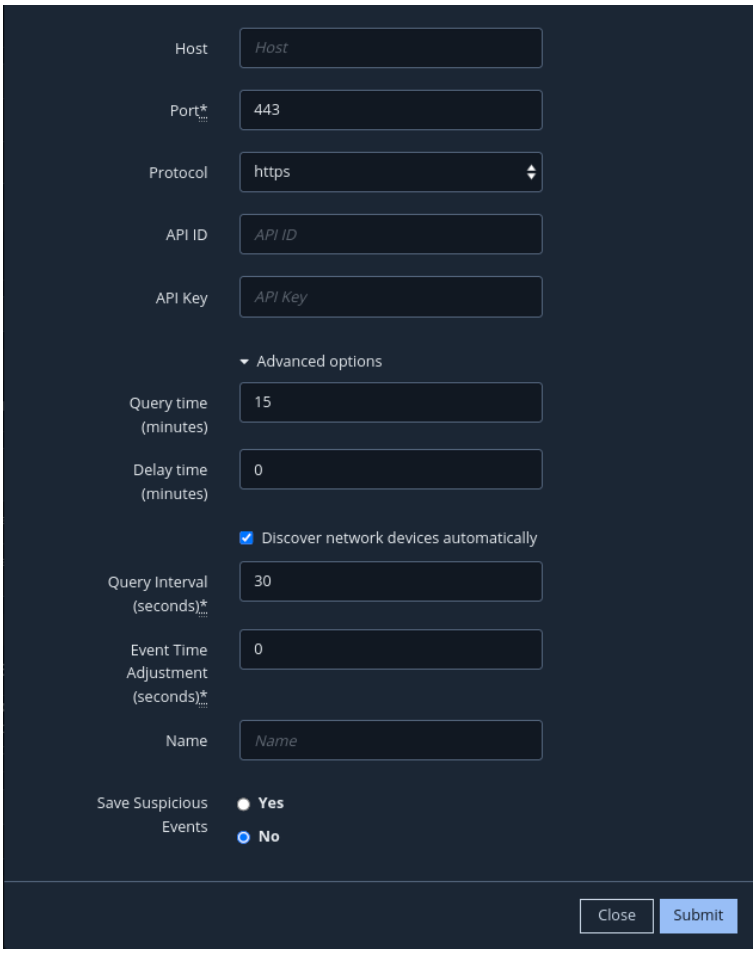
The following API calls are used by the Validation Platform:

Purpose	Call
Get list of events	/public_api/v1/incidents/get_incidents
Get event data	/public_api/v1/incidents/get_incident_extra_data

Add the Cortex XDR Integration to the Security Validation Platform

1. Go to **Settings** > **Integrations.**
2. Click **Add Integration > Palo Alto Cortex XDR**.

   You can add this as either a Local or Remote integration.
3. Enter information for the **Host**, **Port**, and **Protocol**.
4. Enter your Cortex XDR **API ID** and **API Key**.
5. Expand **Advanced options**.
6. Modify the **Query Time** (optional), **Delay Time** (optional), **Query Interval,** and **Event Time Adjustment**, if necessary.
7. (Optional) Assign a **Name**.
8. (Optional) Choose **Yes** to save suspicious events.
9. 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. To learn more about setting up the rule and assignment, see **Proxy Settings (https://docs.mandiant.com/home/msv-proxy-rules)**.

Verify connectivity

Click the Action menu and select **Test Palo Alto Cortex XDR attributes** to verify that:

- The Director can communicate with the Cortex XDR host on the port and protocol specified.
- The Cortex XDR credentials are valid and working.

Troubleshooting

In the event of an error, please provide the exact error message from Cortex XDR. If requested by Mandiant Support, please also provide appropriate logs from Cortex XDR. Instructions for exporting logs can be found in the **Cortex XDR Log Format Documentation (https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Prevent-Administrator-Guide/Log-Formats)**.