Mandiant

PALO ALTO NETWORKS CORTEX XDR

> 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

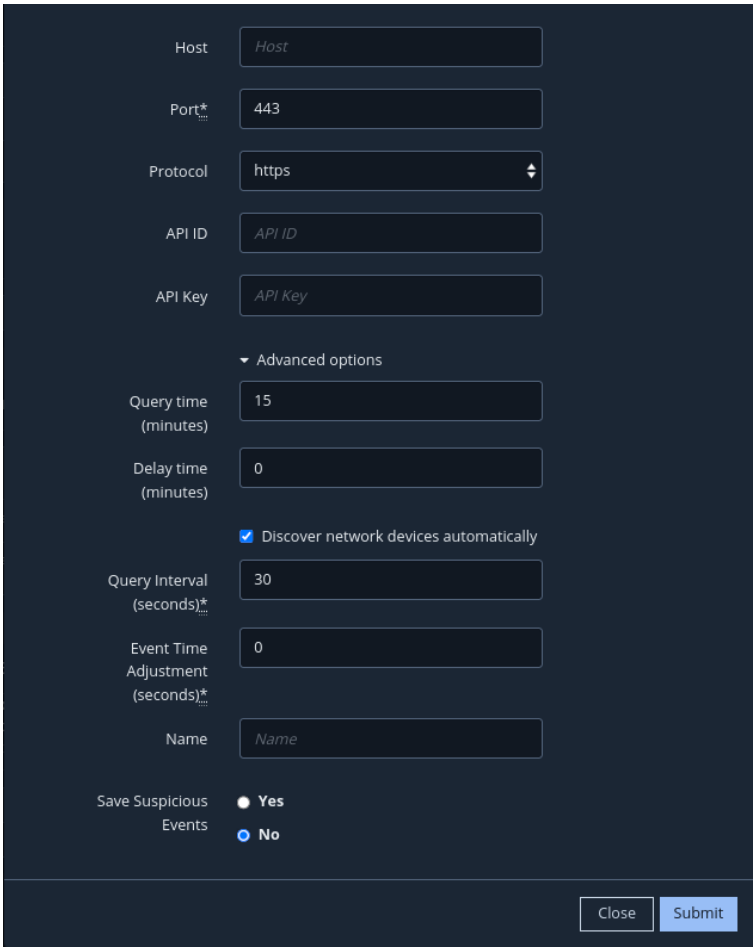
Add the Cortex XDR Integration to the Security Validation Platform

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)**.