Palo Alto Cortex XDR Integration

Palo Alto Cortex XDR Integration

Using the Cortex XDR APIs, you can integrate Cortex XDR with third-party apps or services to ingest alerts and to leverage alert stitching and investigation capabilities. The APIs allows you to manage incidents in a ticketing or automation system of your choice by reviewing and editing the incident's details, status, and assignee. Using the APIs, you can also retrieve information on the endpoints, create installation package, perform response actions directly on the endpoint and more.

Alerts

The Cortex XDR Alerts API is used to retrieve alerts generated by Cortex XDR based on raw endpoint data. A single alert might include one or more local endpoint events, each event generating its own document on Elasticsearch.

The Palo Alto XDR integration requires both an API key and API key ID, both which can be retrieved from the Cortex XDR UI.

API

Before you can begin using Cortex XDR APIs, you must generate the following items from the Cortex XDR app:

Value	Description
API Key	The API Key is your unique identifier used as the `Authorization:{key}` header required for authenticating API calls. Depending on your desired security level, you can generate two types of API keys, Advanced or Standard, from your Cortex XDR app.
API Key ID	The API Key ID is your unique token used to authenticate the API Key. The header used when running an API call is `x-xdr-auth-id:{key_id}`.
FQDN	The FQDN is a unique host and domain name associated with each tenant. When you generate the API Key and Key ID, you are assigned an individual FQDN.

Create Cortex API Key:

The following steps describe how to generate the necessary key values:

1. Get your Cortex XDR API Key:
    1. In Cortex XDR, navigate to **Settings** > **Configurations** > **Integrations** > **API Keys**.
    2. Select **+ New Key**.
    3. Choose the type of API Key you want to generate based on your desired security level: **Advanced** or **Standard**. The Advanced API key hashes the key useing a

nonce, a random string, and a timestamp to prevent replay attacks. cURL does not support this but is suitable with scripts. Use the provided script to create the advanced API authentication token.

Note: To integrate with Cortex XSOAR you must generate an Advanced Key.

4. If you want to define a time limit on the API key authentication, mark **Enable Expiration Date** and select the expiration date and time. Navigate to **Settings** > **Configurations** > **Integrations** > **API Keys** to track the **Expiration Time** field for each API key. In addition, Cortex XDR displays a API Key Expiration notification in the Notification Center one week and one day prior to the defined expiration date.
5. Provide a comment that describes the purpose for the API key, if desired.
6. Select the desired level of access for this key. You can select from the list of existing **Roles**, or you can select **Custom** to set the permissions on a more granular level. Roles are available according what was defined in the hub as described in the Manage Roles section of the Cortex XDR Administrator's Guide.
7. **Generate** the API Key.
8. Copy the API key, and then click **Done**. This value represents your unique `Authorization:{key}`.

Note: You will not be able to view the API Key again after you complete this step. Ensure that you copy it before closing the notification.

Cortex XDR API Key ID

Get your Cortex XDR API Key ID.

1. In the API Keys table, locate the **ID** field.
2. Note your corresponding **ID** number. This value represents the `x-xdr-auth-id:{key_id}` token.

Note: This key id will be used for integrations with elastic.

Cortex XDR API FQDN

Get your FQDN.

1. Right-click your API key and select **View Examples**.
2. Copy the **CURL Example** URL. The example contains your unique FQDN:

`https://api-{fqdn}/public_api/v1/{name of api}/{name of call}/` You can use the **CURL Example** URL to run the APIs.

If you need further assistance, kindly contact our support at info@cytechint.com for prompt assistance and guidance.

Revision #1
Created 12 November 2024 03:48:16
Updated 12 November 2024 05:28:50