Configuring the Palo Alto Cortex XDR Universal Data Insights Connector

Configuration

1. Log in to IBM Cloud Pak for Security.
2. In the navigation pane, click the Settings icon.
3. From the menu, click **Connections** > **Data sources**.
4. On the Data Sources tab, click **Connect a data source**.
5. Select the data source type and then click **Next**.
6. Configure the connection to allow IBM Cloud Pak for Security to connect to the data source. The following fields are available:

Connection name

Assign a name to uniquely identify the data source connection. You can create multiple connection instances to a data source so it would be good to clearly set them apart by name. Only alphanumeric characters and the following special characters are allowed.

Connection description

Write a description to indicate the purpose of the data source connection. You can create multiple connection instances to a data source, so it is useful to clearly indicate the purpose of each connection by description. Only alphanumeric characters and the following special characters are allowed.

App Host (optional)

To use the Edge Gateway App Host to host the containers that are required for communication between the data sources and IBM Cloud Pak for Security, select an App Host. Note that the Edge Gateway App Host must be V1.6 or newer.

Management IP address or Hostname
Specify the hostname or IP address of the data source so that IBM Cloud Pak for Security can communicate with it.

Host port (optional)

Set the port number that is associated with the data source host. The default port is <DEFAULT CAN DIFFER FOR DATA SOURCE>.

7. Set the query parameters to control the behavior of the search query on the data source. The following fields are available:

Concurrent search limit

The number of simultaneous connections that can be made between Cloud Pak for Security and the data source. The default limit for the number of connections is 4.

Query search timeout limit

The time limit in minutes for how long the query is run on the data source. The default time limit is 30. When the value is set to zero, there is no timeout. If the query takes longer than 1 min, it is likely to indicate a problem.

Result size limit

The maximum number of entries or objects that are returned by search query. The default result size limit is 10,000. The value must not be less than 1 and must not be greater than 10,000.

Query time range

The time range in minutes for the search, represented as the last X minutes. The default is 5 minutes.

8. Click **Add a Configuration**.

9. Configure **identity and access**:

a. In the **Configuration name** field, enter a unique name to describe the access configuration and distinguish it from the other access configurations for this data source connection that you might set up. Only alphanumeric characters and the following special characters are allowed.

b. In the **Configuration description** field, enter a unique description to describe the access configuration and distinguish it from the other access configurations for this data source connection that you might set up. Only alphanumeric characters and the following special characters are allowed.

c. In the **Api key** field, enter the Api key.

d. In the **Api Key Id** field, enter the Api key id.

e. In the **Tenant** field, enter the Tenant.

f. Click **Add**.

g. Click **Edit access** and choose which users can connect to the data source and the type of access.

h. To save your configuration and establish the connection, click **Done**.

You can see the data source connection configuration that you added under Connections on the data source settings page. A message on the card indicates connection with the data source.
You can add other connection configurations for this data source that have different users and different data access permissions.