CYBERARK ENDPOINT PRIVILEGE MANAGER FOR MICROSOFT SENTINEL INTEGRATION

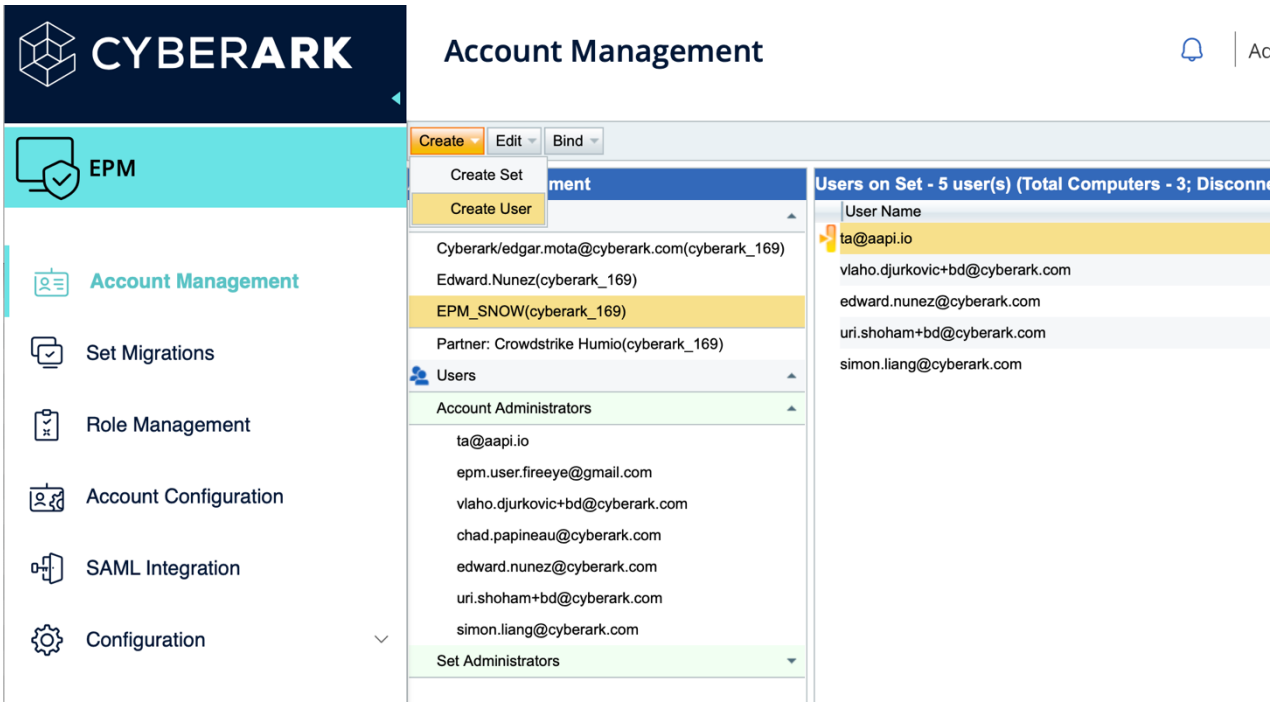
March 2023

1 INTEGRATION OVERVIEW

The Microsoft Sentinel integration with CyberArk EPM allows security administrators to ingest data by pulling application events and policy audit activity from CyberArk EPM into Microsoft Sentinel to be used for analysis and threat modeling procedures.

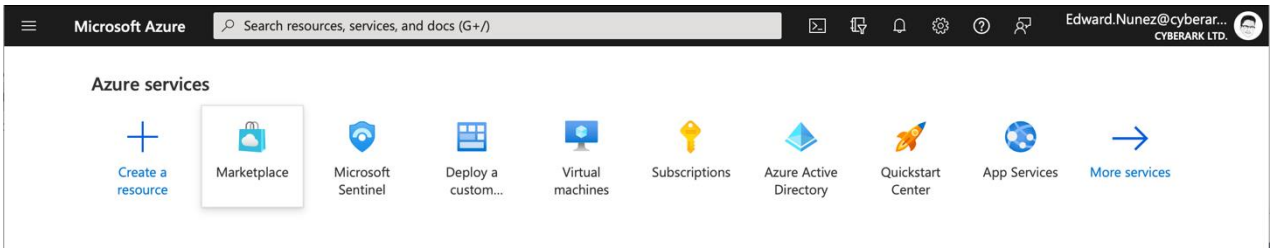
2 DEFINE USER FOR API CONNECTION

The integration requires to have a user to be defined in CyberArk EPM to be used for authentication by the EPM API. Logged in as an EPM administrator, navigate to Administration and then Account Management; Click “Create” → “Create User”, fill in the details for the User, then give access to the the Sets to be pulling data from.

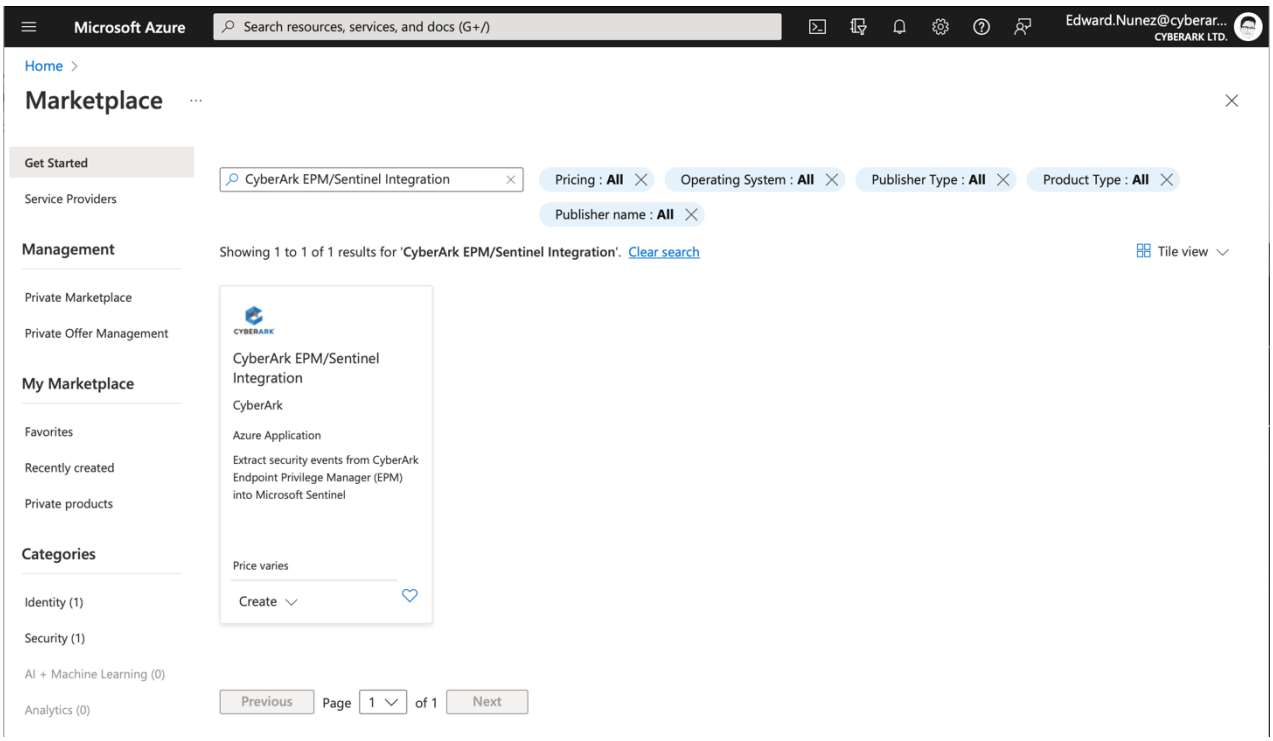


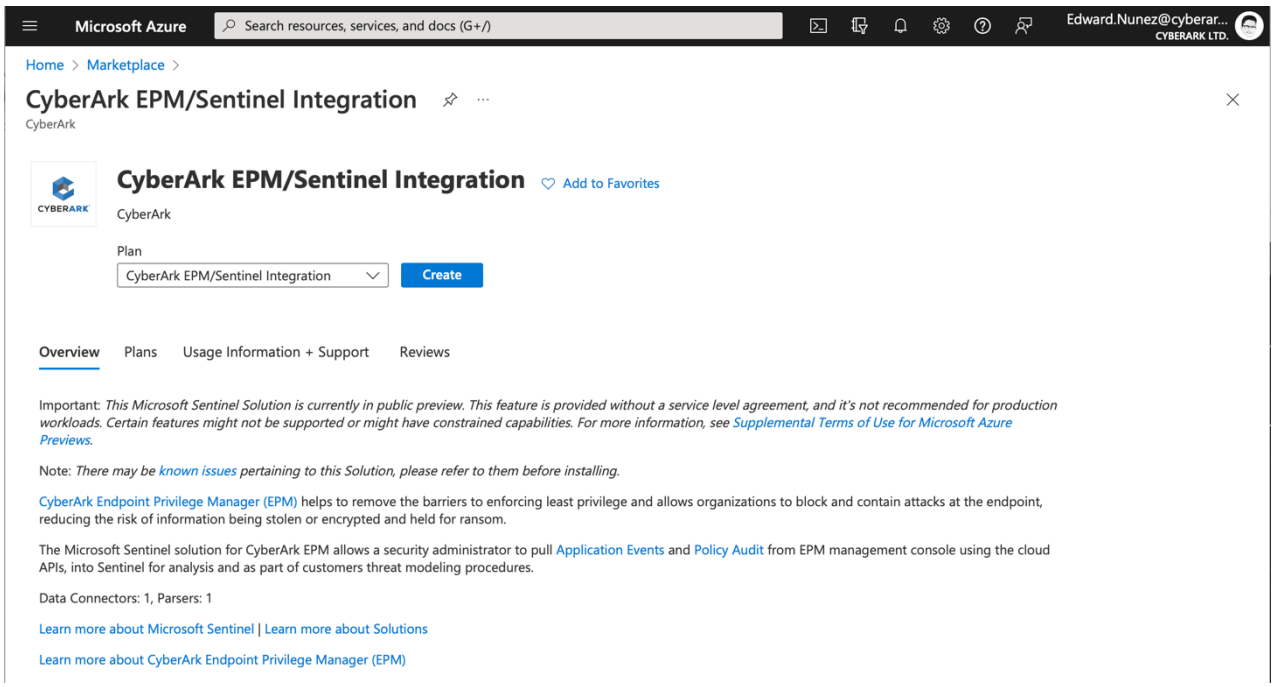
3 ADD INTEGRATION FROM AZURE MARKETPLACE

The installation is a two step process. Step 1 is to install the Integration Solution from Microsoft Azure Marketplace.

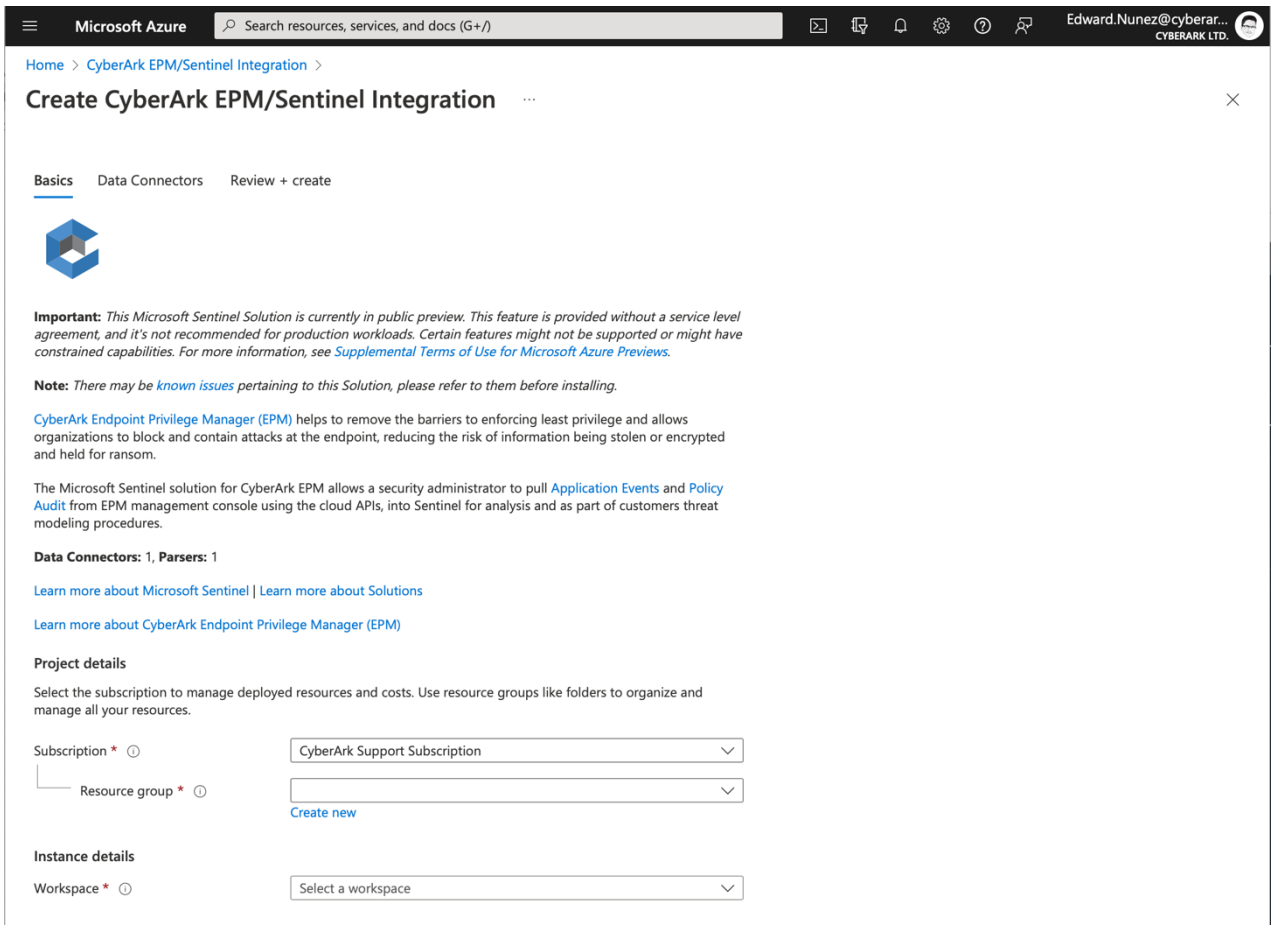


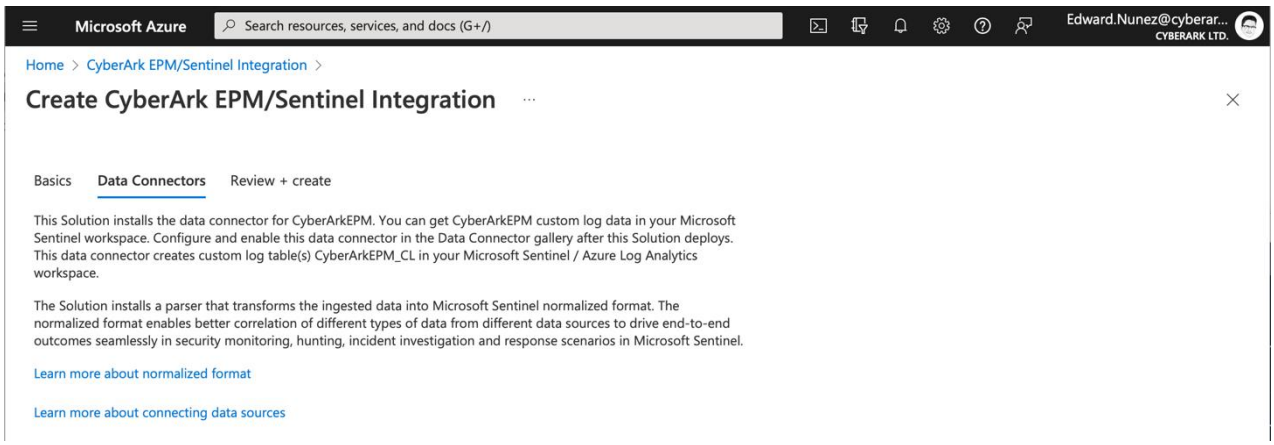
Find “CyberArk Endpoint Privilege Manager for Microsoft Sentinel”





Then, click “Create”, provide the information requested, review and create it.

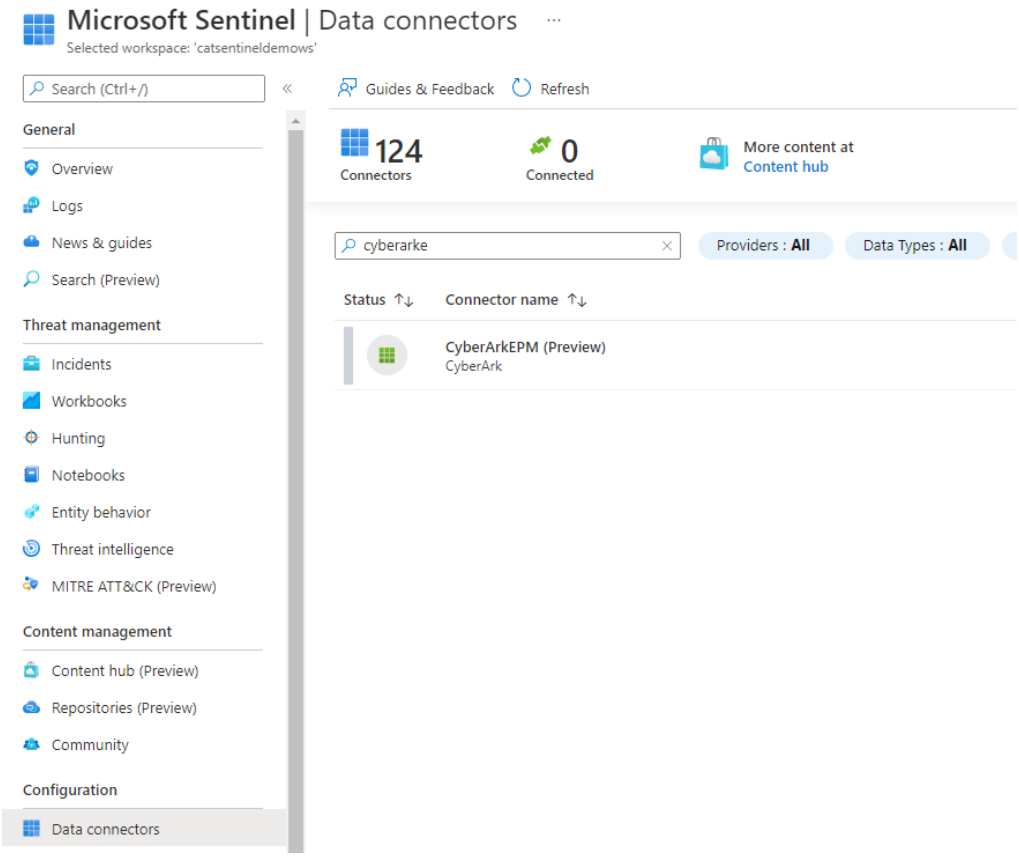




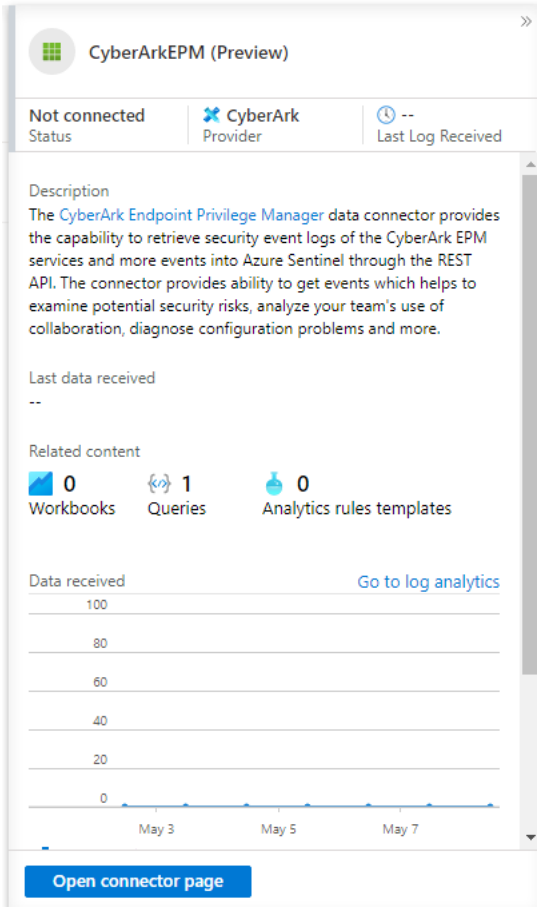
The CyberArk EPM for Microsoft Sentinel Integration data connector will be available for configuration in the instance specified.

4 CONFIGURE DATA CONNECTOR

Second step is to configure the data connector. For this, click on CyberArkEPM in the snapshot above and you will get a pane on the right. (snapshot below)



Click on “Open connector page” & in the next screen click on “Deploy to Azure” button. Clicking on deploy to azure button will take you to the screen which will take inputs about username, password and URL.


CyberArkEPM (Preview)
Not connected
Status
CyberArk
Provider
--
Last Log Received
Description
The CyberArk Endpoint Privilege Manager data connector provides the capability to retrieve security event logs of the CyberArk EPM services and more events into Azure Sentinel through the REST API. The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.
Last data received
--
Related content
0
Workbooks
1
Queries
0
Analytics rules templates
Data received
Go to log analytics
100
80
60
40
20
0
May 3
May 5
May 7
Open connector page