

CYBERARK ENDPOINT PRIVILEGE MANAGER FOR MICROSOFT SENTINEL INTEGRATION

March 2023

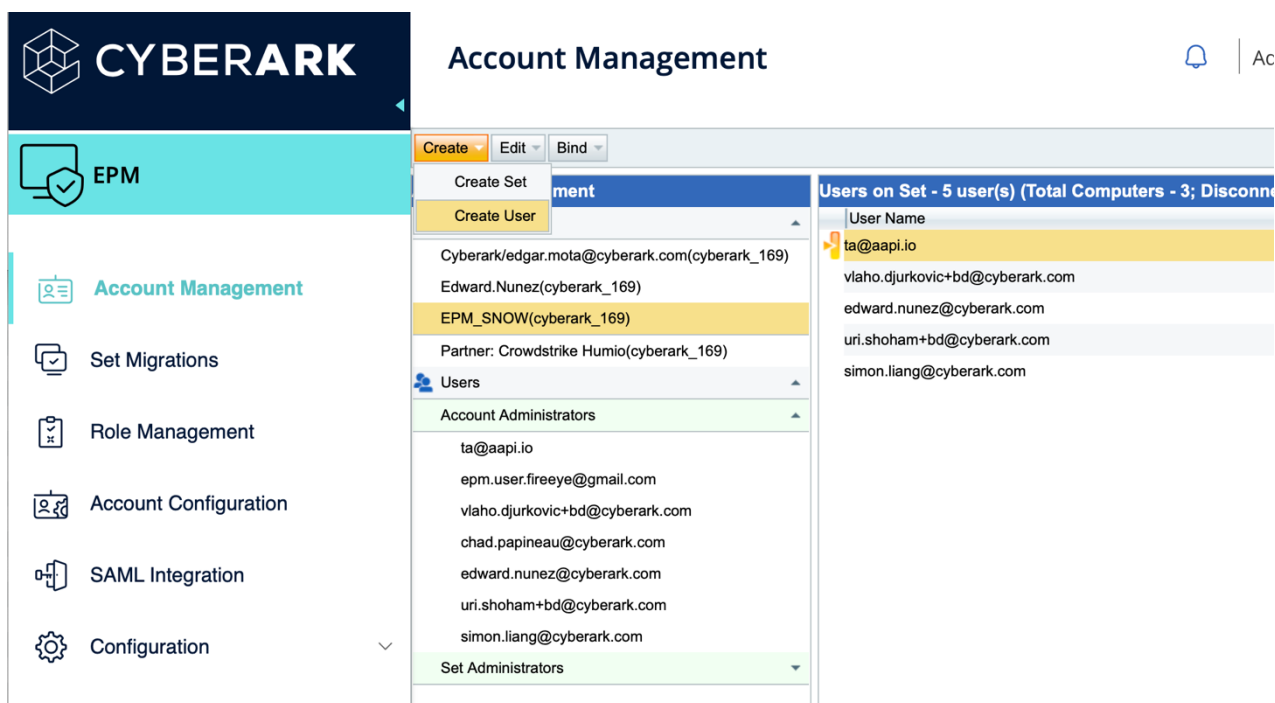


1 INTEGRATION OVERVIEW

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

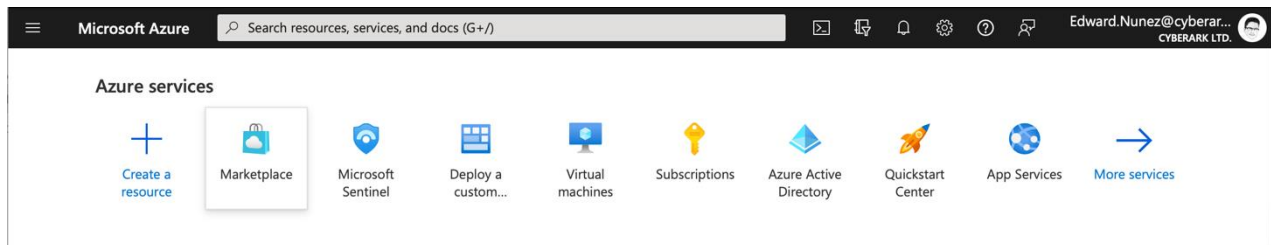
The integration requires to have a user to be defined in CyberArk EPM to be used for authentication by the EPM API. Logged in as an EPM administrator, navigate to Administration and then Account Management; Click "Create" → "Create User", fill in the details for the User, then give access to the the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



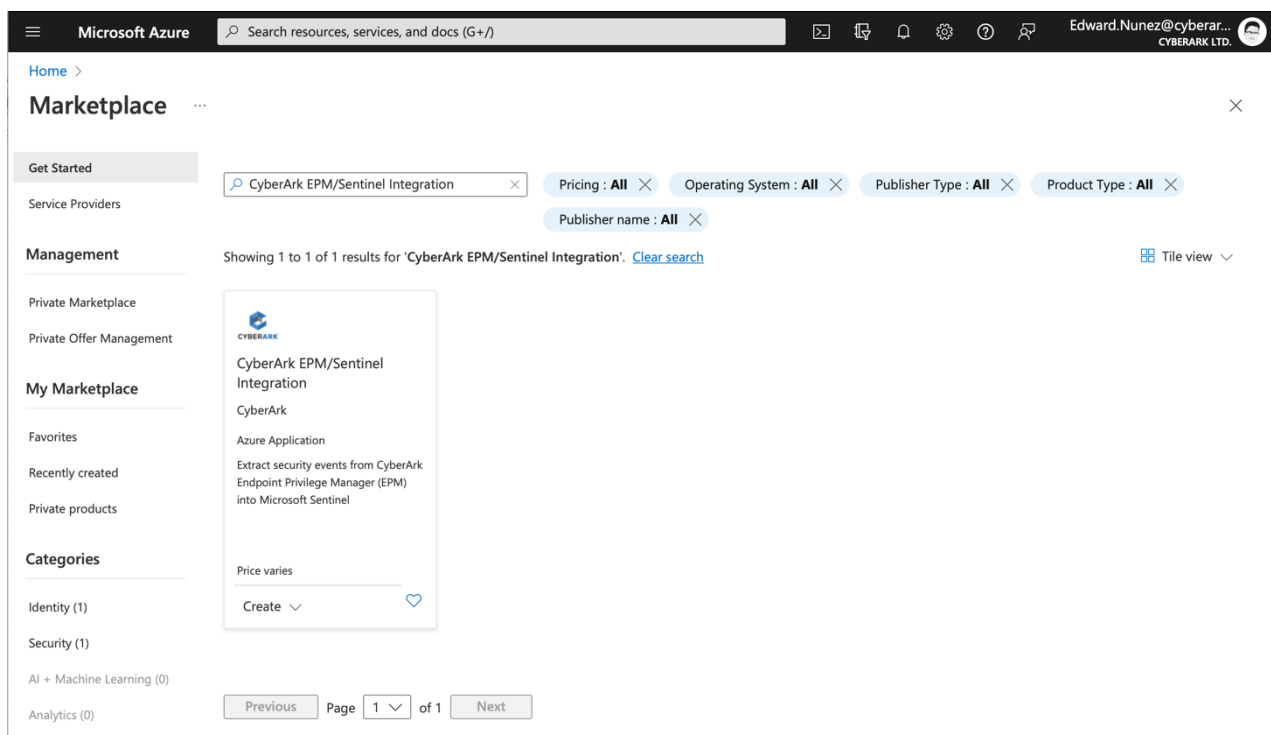
The screenshot displays the CyberArk Account Management interface. The left sidebar shows the navigation menu with options: EPM, Account Management (selected), Set Migrations, Role Management, Account Configuration, SAML Integration, and Configuration. The main content area is titled 'Account Management' and features a 'Create' dropdown menu with options 'Create Set' and 'Create User'. The 'Create User' option is selected, leading to a form for creating a new user. The form includes fields for 'User Name' (ta@aapi.io), 'Email' (ta@aapi.io), 'Password' (EPM_SNOW(cyberark_169)), and 'Partner: CrowdStrike Humio(cyberark_169)'. Below the form, there are sections for 'Users' and 'Account Administrators'. The 'Users' section lists several email addresses, including ta@aapi.io, epm.user.fireeye@gmail.com, viaho.djurkovic+bd@cyberark.com, chad.papineau@cyberark.com, edward.nunez@cyberark.com, uri.shoham+bd@cyberark.com, and simon.liang@cyberark.com. The 'Account Administrators' section is currently empty.

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”



Microsoft Azure
Search resources, services, and docs (G+/)

Edward.Nunez@cyberar...
CYBERARK LTD.

Home > Marketplace >

CyberArk EPM/Sentinel Integration
CyberArk


CyberArk EPM/Sentinel Integration
Add to Favorites

Plan
CyberArk EPM/Sentinel Integration
Create

Overview
Plans
Usage Information + Support
Reviews

Important: This Microsoft Sentinel Solution is currently in public preview. This feature is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

Note: There may be [known issues](#) pertaining to this Solution, please refer to them before installing.

CyberArk Endpoint Privilege Manager (EPM) helps to remove the barriers to enforcing least privilege and allows organizations to block and contain attacks at the endpoint, reducing the risk of information being stolen or encrypted and held for ransom.

The Microsoft Sentinel solution for CyberArk EPM allows a security administrator to pull [Application Events](#) and [Policy Audit](#) from EPM management console using the cloud APIs, into Sentinel for analysis and as part of customers threat modeling procedures.

Data Connectors: 1, Parsers: 1

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

[Learn more about CyberArk Endpoint Privilege Manager \(EPM\)](#)

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

Microsoft Azure

Search resources, services, and docs (G+)

Edward.Nunez@cyberar...
CYBERARK LTD.

Home > CyberArk EPM/Sentinel Integration >

Create CyberArk EPM/Sentinel Integration

Basics

Data Connectors

Review + create



Important: This Microsoft Sentinel Solution is currently in public preview. This feature is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

Note: There may be [known issues](#) pertaining to this Solution, please refer to them before installing.

CyberArk Endpoint Privilege Manager (EPM) helps to remove the barriers to enforcing least privilege and allows organizations to block and contain attacks at the endpoint, reducing the risk of information being stolen or encrypted and held for ransom.

The Microsoft Sentinel solution for CyberArk EPM allows a security administrator to pull [Application Events](#) and [Policy Audit](#) from EPM management console using the cloud APIs, into Sentinel for analysis and as part of customers threat modeling procedures.

Data Connectors: 1, **Parsers:** 1

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

[Learn more about CyberArk Endpoint Privilege Manager \(EPM\)](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

CyberArk Support Subscription

Resource group *

[Create new](#)

Instance details

Workspace *

Select a workspace

Microsoft Azure

Search resources, services, and docs (G+)

Edward.Nunez@cyberar...
CYBERARK LTD.

Home > CyberArk EPM/Sentinel Integration >

Create CyberArk EPM/Sentinel Integration

Basics

Data Connectors

Review + create

This Solution installs the data connector for CyberArkEPM. You can get CyberArkEPM custom log data in your Microsoft Sentinel workspace. Configure and enable this data connector in the Data Connector gallery after this Solution deploys. This data connector creates custom log table(s) CyberArkEPM_CL in your Microsoft Sentinel / Azure Log Analytics workspace.

The Solution installs a parser that transforms the ingested data into Microsoft Sentinel normalized format. The normalized format enables better correlation of different types of data from different data sources to drive end-to-end outcomes seamlessly in security monitoring, hunting, incident investigation and response scenarios in Microsoft Sentinel.

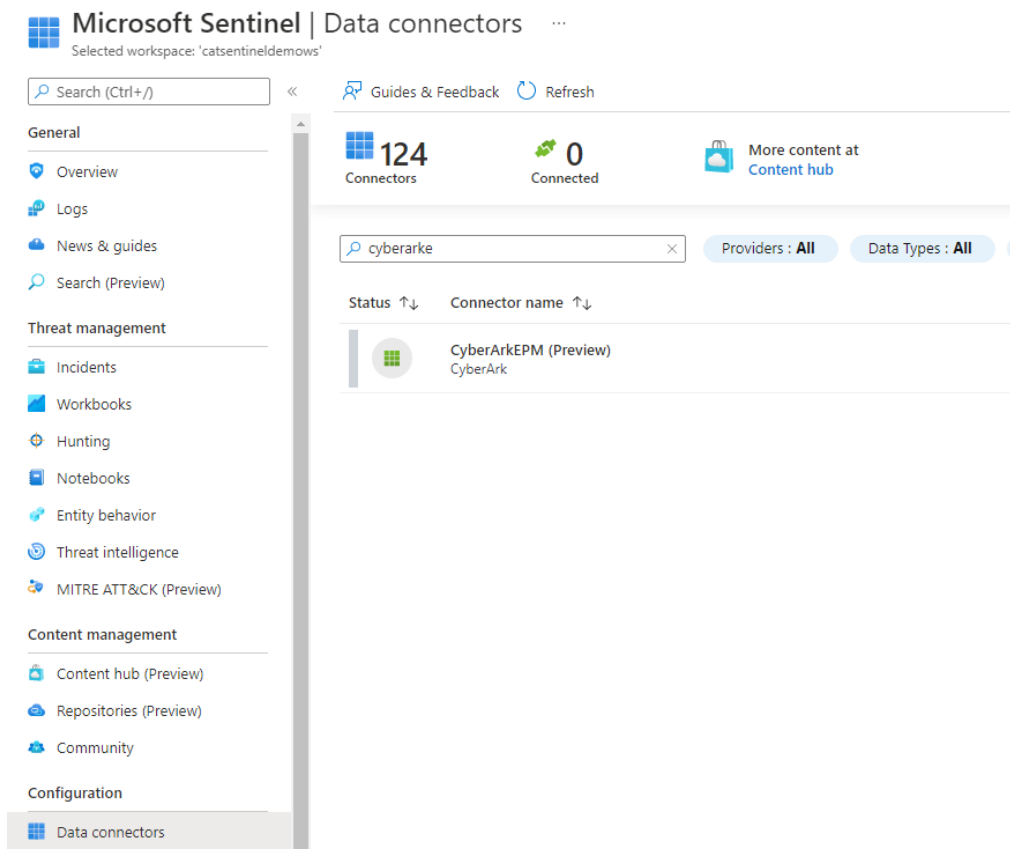
[Learn more about normalized format](#)

[Learn more about connecting data sources](#)

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

--

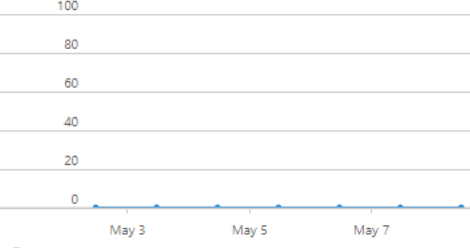
Related content


0
 Workbooks


1
 Queries


0
 Analytics rules templates

Data received [Go to log analytics](#)



Open connector page