CrowdStrike ZTA Conditional Access

Business Development

Name of Company: CrowdStrike

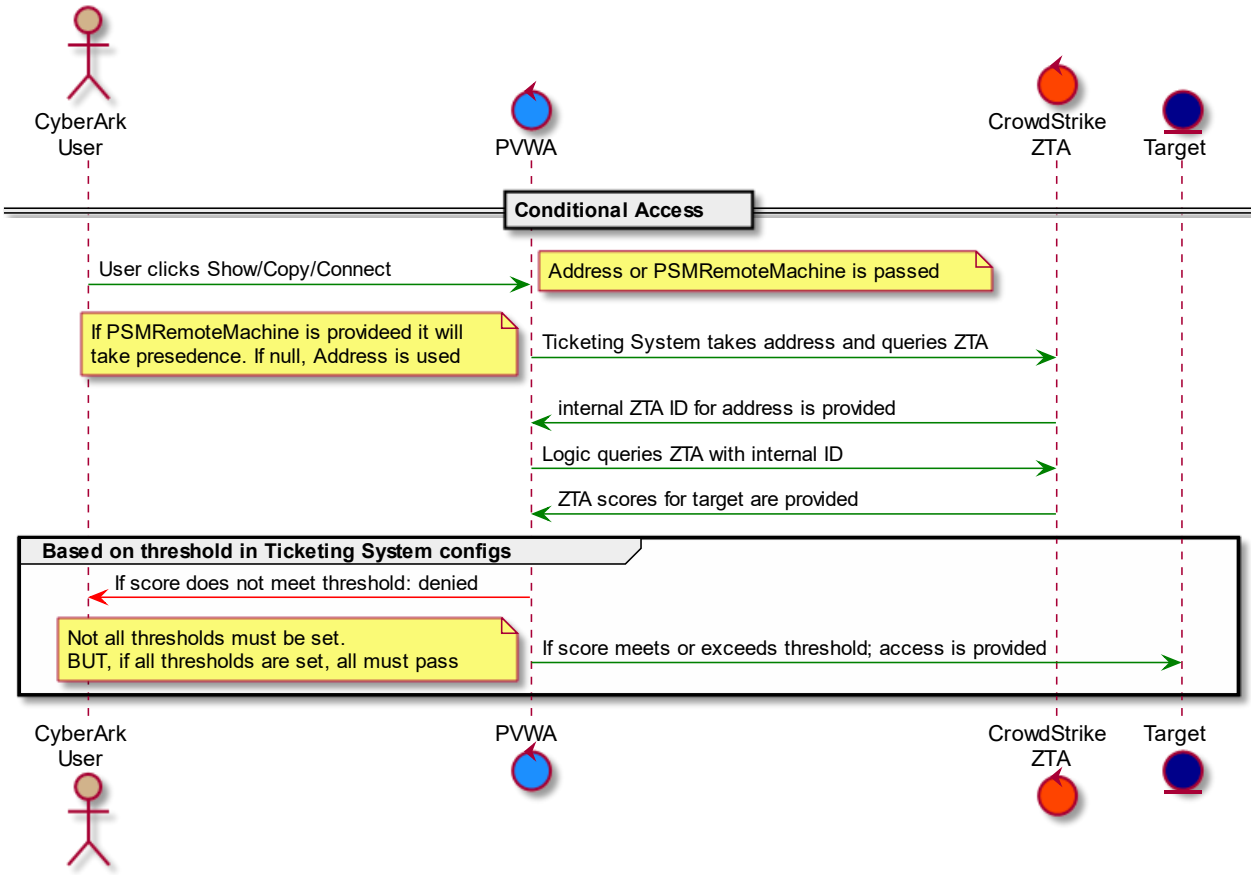
Website: www.crowdstrike.com

Name of Product: CrowdStrike ZTA

Date: June 2021

Intent

This integration leverages the CrowdStrike Zero Trust Assessment (ZTA) solution to identify endpoints out of compliance. The ZTA agent will scan the endpoints and provide three scores (overall, os, sensor_config) that are retrieved at the time of access. The integration allows for the admin to configure a minimum threshold which will allow or deny access based on the score returned from the ZTA API.



Implementation

Prerequisites

- CrowdStrike API access (API Account) vaulted
- PVWA Ticketing Integration enabled and configured
- CrowdStrike Conditional Access downloadable content

Setup CrowdStrike ZTA

1. Open a File Explorer and navigate to:

%install_drive%\inetpub\wwwroot\PasswordVault\bin

2. Place the following files into the **bin** folder:
   CyberArk.CrowdStrikeZTA.dll
   RestSharp.dll
3. In an administrative cmd or powershell window perform an **iisreset**
4. **Create an account object** that houses the CrowdStrike ZTA API

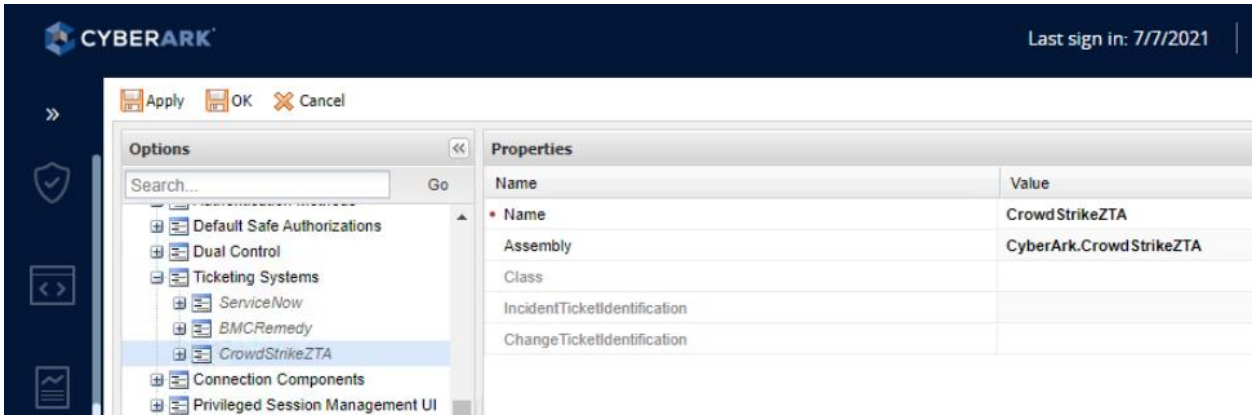
Configuring CrowdStrike ZTA Ticketing Integration

Enable and configure Ticketing in the PVWA in accordance with the documentation found at https://docs.cyberark.com

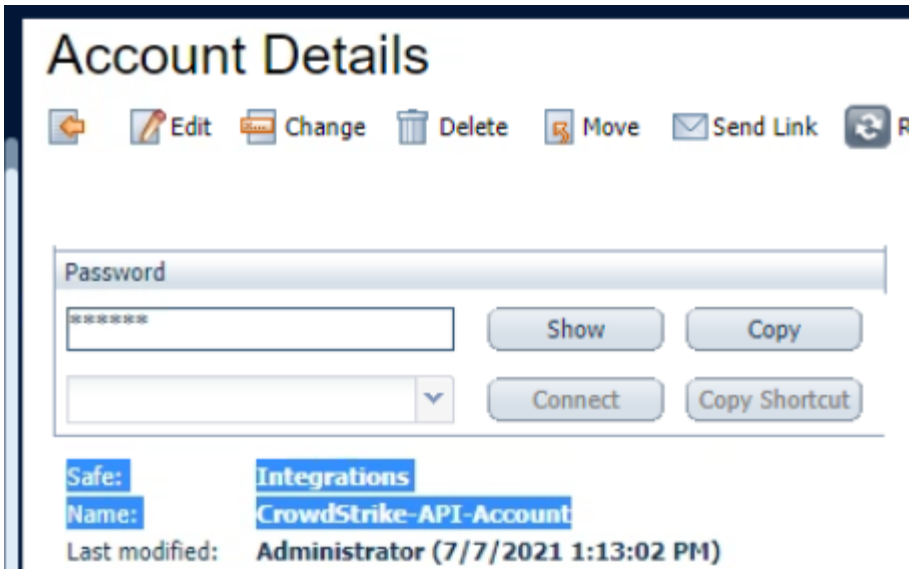
1. Log into the PVWA with a user that has access to the **Configuration Options**
2. Go to **Administration** tab -> **Options**; Expand **Ticketing Systems**
3. Ensure **Ticketing Systems** is set to **Enabled**
4. Right-click on **Ticketing Systems** -> **Add System**

   Name: CrowdStrikeZTA

   Assembly: CyberArk.CrowdStrikeZTA



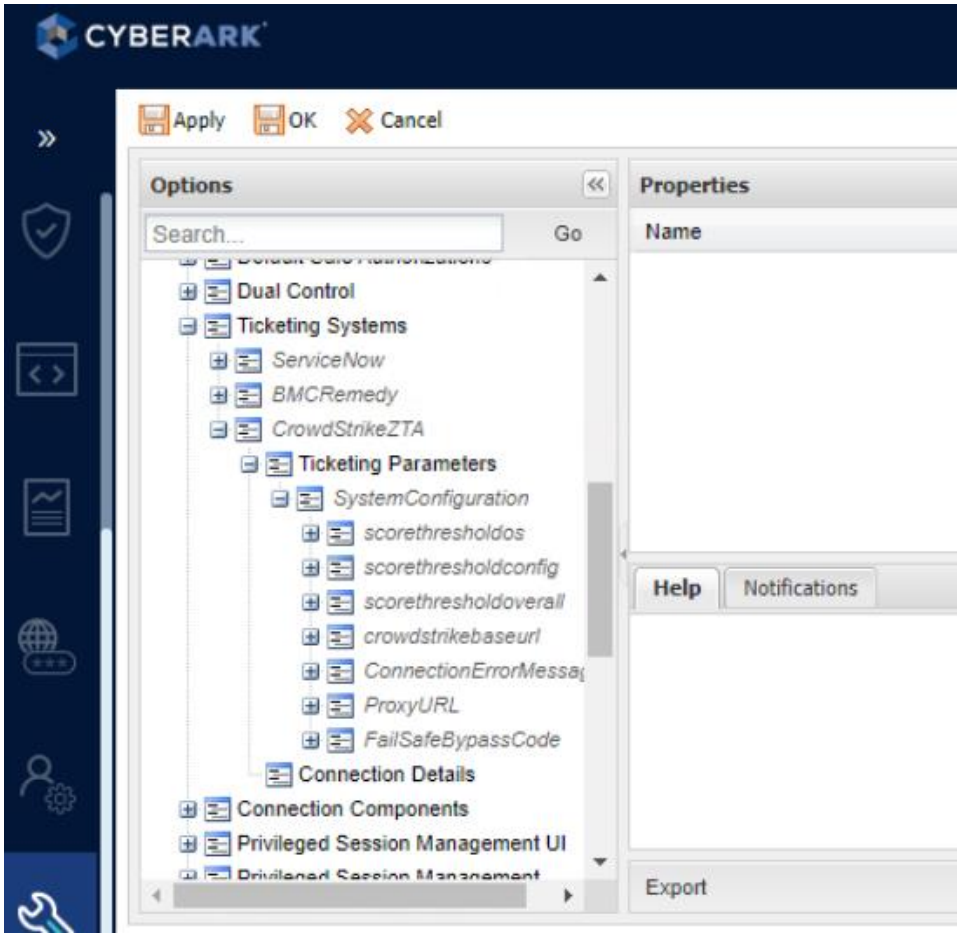
5. Right-click on **CrowdStrikeZTA** -> **Add Connection Details**
6. Provide the **Safe** and account object **Name** of the CrowdStrike ZTA API that was vaulted



7. Right-click on **Ticketing Parameters** -> **Add System Configuration**
8. Right-click on **System Configuration** -> **Add Parameter**

   Do this for the relevant parameters needed, see following table:

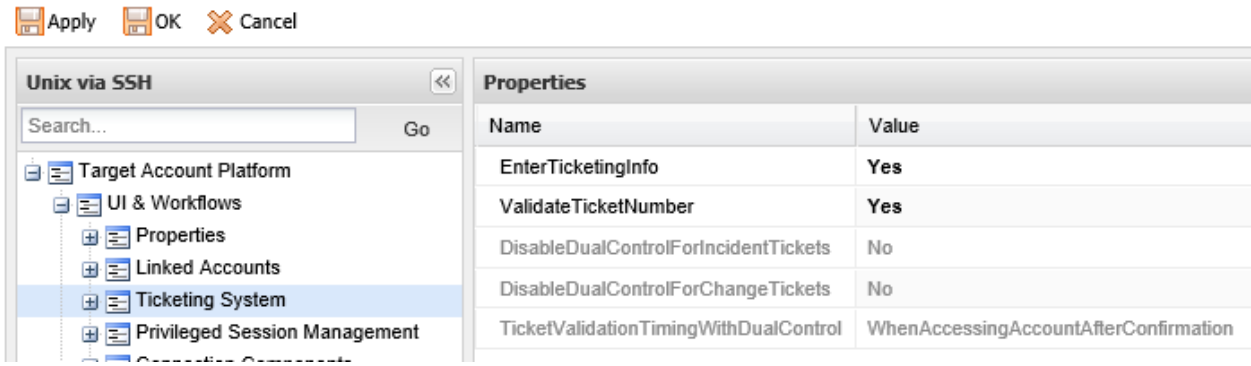
Name	Value
scorethresholdconfig	Score minimum for the Config field of the ZTA Score
scorethresholdoverall	Score minimum for the Overall field of the ZTA Score
scorethresholdos	Score minimum for the OS field of the ZTA Score
crowdstrikebaseurl	The Base URL for the Crowdstrike API
ConnectionErrorMessage	Free text string that displays if there is a communication error to the SCIM server Example: A connection error occurred while communicating with the ticketing syste Please check the communication settings
DenyErrorMessage	Free text string that displays if a user has been denied access. Example: “You have been blocked by Crowdstrike”



Enabling the Integration for Relevant Platforms

Enable the integration (Ticketing System) on platforms that you want to deny access to servers based on scores assigned by the CrowdStrike ZTA solution. Log-in to the PVWA as a vault administrator user, go to **Platform Management**. Select the platform that manages the account object that connects to an endpoint being managed by CrowdStrike and click on **Edit**:

If you do not already have an active Ticketing System, then expand **UI & Workflows**, click on **Ticketing System**, and set both **EnterTicketinginfo** and **ValidateTicketNumber** to **Yes**. Then click **OK**:



Note: If you have multiple ticketing systems you can enable only some of them for a specific platform, please refer to section "*Integrating with Ticketing Systems*" of the "*Privileged Account Security Implementation Guide*" documentation.