



Proofpoint Conditional Access

Proofpoint Targeted Attack Protection (TAP) Integration

Business Development

Name of Company: Proofpoint

Website: www.Proofpoint.com

Name of Product: TAP – Targeted Attack Protection

Date: September 2020



Intent

The Proofpoint Targeted Attack Protection (TAP) Integration uses the CyberArk SCIM Discovery module to poll the Proofpoint solution in order to identify users that have been exposed to attacks by clicking on a phishing link, as well as identifying users that are very attacked people as determined by Proofpoint's proprietary Attack Index. The Attack Index quantifies a person's risk based on Actor Type, Targeting Type, Threat Type and Attack Volume. With this information, such users can be added and removed from groups identified in the SCIM discovery configurations. As users attempt to access vaulted credentials through the PVWA, the Conditional Access Integration with Proofpoint can be used to confirm whether the user should be allowed to be exposed to the credentials requested. Other scenarios and use cases can be implemented using the resulting CyberArk groups being synchronized and/or updated from information available from Proofpoint.

Proofpoint Conditional Access

By using the PVWA Ticketing System Integration framework, a conditional access flow can be defined by verifying whether the requesting user is a member of a group which is populated by the previous workflows, and denying access to show and copy functionality if a user has been identified to have clicked on a phishing link.

You can link the results of the integration between CyberArk and Proofpoint for Proofpoint Phishing to this one.

Implementation

Prerequisites

- PVWA Ticketing Integration enabled and configured

Configure Proofpoint Conditional Access in the PVWA

1. Log into the PVWA server
2. Open a File Explorer and navigate to:
%install_drive%\inetpub\wwwroot\PasswordVault\bin
3. Place the **ProofpointSIEM.dll** file and subsequent binaries into the **bin** folder
4. In an administrative cmd or powershell window perform an **iisreset**

Configuring Proofpoint Conditional Access Ticketing Integration

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

1. Go to **Administration** tab -> **Options**; Expand **Ticketing Systems**; Ensure **Ticketing Systems** is set to **Enabled**
2. Right-click on **Ticketing Systems** -> **Add System**
Name: Proofpoint SIEM Validator
Assembly: CyberArk.ProofpointSIEM
3. Right-click on **Proofpoint SIEM Validator** -> **Add Connection Details**
Safe: SCIM Config (replace for the Safe where the account is stored)
File: Client-account
4. Right-click on **Ticketing Parameters** -> **Add System Configuration**
5. Right-click on **System Configuration** -> **Add Parameter**
Do this for the relevant parameters needed, see following table.

Name	Value
ForbiddenGroup	Create and input a group name that will be used to house users that have been identified as phished users. Example: VeryAttackedPeople
SCIMServerBaseURL	The Base URL for the SCIM Server. Example: http://enterprisescimserver:8080
AllowRevealOnHttpStatus	Optional parameter that will allow access if there is a communication error Example: 503,502,504,404
ProxyURL	Optional parameter allowing communication through a proxy Example: http://proxyserver:8888
FailsafeBypassCode	Optional parameter allowing for a break glass code to input into the ticketing prompt to override access
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 system. Please check the communication settings
DenyErrorMessage	Free text string that displays if a user has been denied access. Example: "You have been blocked by Proofpoint"