CYBERARK

CYBERARK ENDPOINT PRIVILEGE MANAGER

1. INTRODUCING CYBERARK ENDPOINT PRIVILEGE MANAGER

Key Concepts
System Architecture
Data Encryption
CyberArk Endpoint Privilege Manager SaaS Datasheet
CyberArk Endpoint Privilege Manager SaaS Infrastructure and Architecture
CyberArk Endpoint Privilege Manager Agents
Service and Data Security
Service Availability
Privacy
Data Retention

2. CONFIGURE CYBERARK ENDPOINT PRIVILEGE MANAGER

Configure User Account Control (UAC)
Log On as an Account Administrator
Create Sets and Set Administrators
Configure Role Management
Configure Account Settings
Configure SAML Integration

Collect Server Support Information
Install the CyberArk EPM Plugin

3. INSTALL AGENTS ON THE ENDPOINT MACHINES

Endpoint Machines: Supported Operating Systems
MacOS Internal Admin User
Install Agents Via a Software Distribution System
Install Agents Using McAfee ePO
Manually Install Agents
Protect Agents
Configure Agents for Client Certificate Mapping Authentication
Collect Agent Support Information
Upgrade and Uninstall Agents

4. WORK WITH THE SERVER

Log On as a Set Administrator
SaaS Only - Obtain a License
My Computers
Group By
Common
Predefined Groups
Custom Groups
My Computers Additional Features

5. POLICIES

Policy Priority
Applications
Table of Contents
Define the Policy Audit
Multi-factor and "Over-the-shoulder" Authentication
End-user UI
Application Groups
Advanced Application Policies
macOS Policies
Policy Templates
Additional Policy Management

6. WORK WITH THE INBOXES AND THE APPLICATION CATALOG

Work with the Privilege Management Inbox
Work with the Application Control Inbox
Work with the Application Catalog
Use the File Passport

7. WORK WITH THREAT DETECTION

Threat Detection Events
Threat Detection Reports

Configure Threat Intelligence Integration
CyberArk Application Risk Analysis
VirusTotal
National Software Reference Library
Configure Integration Settings
Create Credentials Rotation Policy
Use the Policy Audit
Track Policy Usage
Work with the Audit Video

8. REPORTING CAPABILITIES

View the Dashboard
McAfee ePO Reports
Advanced Configuration
Set Advanced Agent Configurations
Set Advanced Server Configurations
Set Video Recording Configurations
Set Custom Tokens
Set My Account

9. ENABLE AUTHORIZATION TOKENS

Offline Policy Authorization Generator Tool
Offline Policy Authorization Generator End-user UI
Configure the Request for Authorization Dialog Box

Request the Authorization Code
Create the Authorization Code
Authorization Token End-user UI
Create the Authorization Token

ENABLE EVENT FORWARDING TO THE CYBERARK VAULT

Create a CyberArk Vault User
Create a Safe and an Account
Configure Event Forwarding
Generate an Activity Report
Enable Third-party Event Forwarding
Configure Third-party Event Forwarding
Understanding the SysLog Messages

CUSTOMIZE THE END-USER INTERFACE

Dialogs
Create and Edit Dialog Boxes
Review Dialog Types
Limit the API calls in a set period of time
Limit the concurrent login sessions
API Commands
EPM authentication
Windows authentication
Get EPM version

Get Sets list

Get aggregated events

Get raw events

Get raw event details

BEST PRACTICES

Implement Privilege Management

Establish Trusted Sources

Monitor Your Applications

Create Policies

Reporting and Forensic Analysis

Use Restrictive Access Mode

Implement Application Control

Create Trusted Sources

Discover Unhandled Applications

Enforce Restrictive Access Mode

Test in a Lab

Pilot

Detect a Potential Security Threat

Security Best Practices

USE CASES TO BE COVERED DURING THE TRAINING

- Ensure Users have Least privilege on End user machines.
- Achieve Just in time Access to all the local Admin Access which ensures to reduce a huge operational effort and just in time access will support business continuity.
- Reduce exception counts, which will bring down our risk exposure.
- To have Application control (Licenced, Approved, freeware, open source, closed source, shareware, Graphic software, simulation software, educational software, exam-based software)
- Reduce utilization of unpatched / EOL applications usage
- Restriction on UAC, Applocker, LAPS, Credential Guard (security upon Microsoft credential manager)
- Restriction on local privileged Account and Session Management
- Build Fresh local admin access process.
- Boost Visibility on Admin Activity
- Have Governance
- Restriction on local privileged Account and Session Management

LAB - CYBERARK ENDPOINT PRIVILEGE MANAGER

CONTENTS . LAB ENVIRONMENT OVERVIEW

Network & User Environment Information

LAB : ACCOUNT MANAGEMENT

Set: Create a Set to Manage Windows Endpoints

Role: Create Custom Role for Auditor

Users: Bind EPM account as Set Administrator

LAB : POLICY MANAGEMENT

Application Groups: Create Custom Policies for All Endpoints & Users
Advanced Policies: Create Policies for All Endpoints & Users
Application Groups: Add Trusted Sources
Policy Administration: Add Known Good Applications to Run Normally
Policy Administration: Import Policies for Functional Users

LAB : EPM AGENT DEPLOYMENT

Install Endpoint Privilege Manager Agent

LAB : PRIVILEGE MANAGEMENT

Default Policies: Detect Privileged Unhandled Applications
Privilege Management Inbox: Collect & Review Events
Policy Administration: Create Policies Using Events
Access Control: Test & Verify Functional User Permissions

LAB : PRIVILEGE DEFENSE

Ransomware Protection
Privilege Threat Protection

LAB : SET ADMINISTRATION

EPM Tab in File Properties
Command-line Utility (vf_agent.exe) Files to be Ignored Always
Just in Time Access and Elevation

LAB : POLICY MANAGEMENT CHALLENGE

Challenge: Block Policy for an Unauthorized Application

CHALLENGE: ELEVATE POLICY TO ALLOW ADMIN TASKS FOR REMOTE USERS

LAB : LOGS & REPORTS

GENERATE REPORTS

SUMMARY & DASHBOARDS