PRIVILEGED ACCESS MANAGEMENT (PAM) INSTALL AND CONFIGURE

DURATION - 4 DAYS

Description

The training provides the practical knowledge and technical skills to securely design, install, and configure the CyberArk Privileged Access Management (PAM) Solution. The student will gain valuable hands-on experience installing CyberArk components, configuring Authentication Types, and System Integrations (SIEM, SMTP, NTP), using our step-by-step exercise guide, official product documentation, and a dedicated lab environment.

Objectives

- Learn to install and configure the Privileged Access Management (PAM) solution securely following Best Practices.
- Be able to define and describe the CyberArk Privileged Account Security system architecture, requirements, and workflow processes.
- Understand how to secure and install Password Vault Web Access (PVWA) Central Policy Manager (CPM) and Privileged Session Manager (PSM) in a distributed or Load Balanced configuration.
- Learn how to integrate with external services, e.g., LDAP/S, NTP, SMTP, SYSLOG.
- Configure authentication mechanisms including multi-factor authentication using CyberArk, RADIUS, LDAP/S, PKI, and Windows.

Prerequisites

- PAM Administration

- Basic networking knowledge

- Basic Windows administration knowledge

- CyberArk Defender PAM certification (Partners)

Course Modules

1. Overview of the PAM Architecture

2. Enterprise Password Vault Security

3. Enterprise Password Vault Standalone and High Availability Installation

4. CPM

5. PVWA

6. PSM and PSMP Component Installations, including Standalone and Fault Tolerant options

7. System Integrations (e.g., SMTP, NTP, SNMP, LDAP/S)

8. Authentication Methods (e.g., RADIUS, PKI, LDAP/S, and Multi-Factor)

9. Reporting and Troubleshooting: Introduction to Cyber Ark