CyberArk PAM Administration
Course Agenda

Description

The CyberArk Privileged Access Management (PAM) Administration course covers CyberArk's Privilege On-premises Solution. CyberArk administrators or 'Vault Admins' gain extensive hands-on experience in administrating the solution, using our step-by-step exercise guide and dedicated lab environment.

This course provides the participant with the knowledge and skills required to administer, monitor, and troubleshoot an existing Privilege On-premises implementation. The course includes discussions on Privilege On-premises Architecture, Password Management, Session Management and Privileged Threat Analytics, along with software concepts including monitoring, and troubleshooting.

Target Audience

Individuals who will be responsible for the administration of the solution

Anyone who is interested in learning about or will be required to perform initial configuration and set up of the CyberArk solution.

Objectives

Upon completion of this course the participant will be able to:

- Describe the system architecture and flows
- Successfully manage passwords (Verification, Change and Reconciliation)
- Onboard accounts
- Configure sessions to be directed through a PSM
- Monitor recorded sessions
- Use the PTA to monitor the network for privileged related threats
- Modify Master Policy settings
- Produce reports on various system and user activities
- Monitor the CyberArk implementation
- Describe and configure the various logs that are available to troubleshoot problems
- Utilize the knowledge base and other available resources to resolve problems
- Perform common administrative tasks

Topics

The course includes the following topics:

- Overview of threats and the CyberArk PAM Solution
- Managing Users and Groups
- Access Control
- CyberArk Privileged Account Security Administration
- Onboarding Accounts
- Password Management
- Session Management
- Privileged Threat Analytics
- Reports
- Backup and Restore
- Disaster Recovery
- Vault Security
- Monitoring the System
- Common Tasks
- Basic Troubleshooting

PREREQUISITES

Technical

A computer that is able to connect to the Internet as well as a browser that supports HTML 5

Skytap Checker

WebEx Checker

Sales Force Checker

Knowlege

Basic networking knowledge

Basic Windows administration knowledge

Duration

4 days

DAY ONE	
Topic/Task	**Description/Activity**
Introduction to CyberArk PAM	▪ High level overview of common Privileged Access threats and how to mitigate them ▪ Overview of the CyberArk PAM solution ▪ Detailed description of the various components of the Privilege On-premises solution ▪ Description of how various components communicate with the Vault ▪ Description of system utilities
User Management	▪ Description of various User types ▪ Logging in to the system using the Master User ▪ How to unlock a suspended user ▪ How to reset a user's password
Policies and Platforms	▪ Configuration the Master Policy ▪ Duplicating Platforms ▪ Managing Platforms
Access Control	▪ Considerations for designing a safe model ▪ Naming conventions for a safe design model ▪ Creating Safes ▪ Managing Access Control to Accounts
Accounts (Part 1)	▪ Add Accounts ▪ Verify and Change Accounts

DAY TWO	
Topic/Task	**Description/Activity**
Accounts (Part 2)	▪ Configure Linked Accounts ▪ Reconcile Accounts ▪ Mange SSH key accounts
Dependents	▪ Manage Dependents (Usages)
Privileged Access Workflows	▪ Configure Reason for access ▪ Configure Dual Control ▪ Configure One-time passwords ▪ Configure Exclusive Access
Discovery and Onboarding (Part 1)	▪ On Boarding Methods ▪ Accounts Discovery ▪ Automatic Onboarding Rules
Discovery and Onboarding (Part 2)	▪ Add Multiple Accounts from file ▪ Continuous Discovery (PTA) ▪ REST API Onboarding Methods

DAY THREE	
Topic/Task	**Description/Activity**
Privileged Session Management (Part 1)	▪ PSM ▪ Manage PSM Connection Components ▪ PSM Ad-Hoc Connections ▪ HTML5 GW ▪ PSM for Windows ▪ PSM for SSH
Privileged Session Management (Part 2)	▪ Recordings ▪ Live Monitoring ▪ Auditing ▪ Manage PSM Recordings
Privileged Threat Analytics (PTA)	▪ Functionality ▪ Data sources ▪ Detectable Attacks and Risks ▪ Alert flow ▪ Automatic Response ▪ Session analysis and response flow
Reports	▪ Overview of Reports ▪ PrivateArk Client Reports ▪ PVWA Reports
Privilege On-premises Architecture	▪ System architecture and protocols ▪ Component main conf and log files ▪ Components Internal safes and users

DAY FOUR	
Topic/Task	**Description/Activity**
Backup and Restore	▪ Backup methods ▪ Configure the Backup solution (Replication) ▪ Perform Backup ▪ Perform Restore ▪ Configure periodic backup
Replications and Disaster Recovery	▪ Configure the Disaster Recovery solutiob ▪ Test Disaster Recovery
Vault Security	▪ Vault security controls ▪ Vault Encryption and Key Management
System Monitoring	▪ Monitor the Privilege On-premises components ▪ Validate periodic replications of the system ▪ Perform common administrative tasks related to system maintenance
Common Issues	▪ User Authentication issues ▪ Component Connectivity issues ▪ Account Management (CPM) issues ▪ Privileged Session Management (PSM) issues
Troubleshooting	▪ Available Resources ▪ Knowledge Base ▪ Documentation ▪ Troubleshooting Methodologies ▪ Log Files Location ▪ Configure log debug level