Course Contents: Advanced CyberArk PAS Version 11.1

Course Duration - Around 50+ Hours

- **Before you start (Pre-requisites for Hands-On, on your local desktop or laptop):**
  1. Hardware Requirements: **16 GB RAM**, i3 2nd Generation onwards or equivalent Processor, 50+ GB HDD.
  2. Buy the course online (Click on "Take This Course" button)
  3. Start the course and download the Five CyberArk PAS Virtual Box Images (From **Curriculum**), follow the video instructions on how to set it up, ask for one to one support in case any issues.
  4. We cover all major aspects of CyberArk PAS in a 100% practical, use case-oriented manner, with lab exercises.

- **Below Contents will be covered:**
  5. Understand the CyberArk Privileged Account Security(PAS) Solution Architecture in greater details with full practicality and conceptual understanding; the components includes - The **Enterprise Password Vault**(EPV) standalone as well as with Two Node **High-Availability** EPV with the storage server, **DR** Vault, The Password Vault Web Access Interface(**PVWA**), Remote Control Client, PrivateArk Administrative Interface, Privileged Session Manager(**PSM**), Privileged Session Manager SSH Proxy (**PSMP**), The Central Policy Manager (**CPM**), Application Identity Manager(**AIM**), On-Demand Privileges Manager(**OPM**), Back & Restore (**Replicate**), The Password Upload Utility, SDK Interfaces, Administrative APIs and **Upgrade** process for PAS infrastructure (Standalone Vault, High Availability Vault, CPM, PVWA, PSM and DR Site).
  6. **High Availability**(cluster) deployment of CyberArk Digital Vault
     - Pre-requisites – Network, AD DS and DNS, OS Level Clustering, SAN Storage and adding storage to Cluster.
     - Cluster Topology
     - Cluster installation on 2 nodes
     - Configuration of CyberArk Vault Cluster Services – IP, Storage, Core Services
     - Defining Dependencies
     - Cluster Failover Testing – All Three Scenarios
       A. Node Crash
       B. Cluster Service or Network Failure
       C. Manual Migration of CyberArk Services from One node to another & vice-a-versa
     - Overview of High Availability using **CVM**
  7. Understand concept of **Distributed Vault** (Master/Satellite/Master Candidate and Vault Promotion)
  8. **Install** the CyberArk Secure Digital Vault and understand the various security layers, hardening, Security Layers, Encryption and cover the environment that is created on the Vault server, as well as how to administer the Vault environment.
  9. Understand the Central Policy Manager (**CPM**) and install the Central Policy Manager (CPM) as well as cover the environment that is created on the CPM server during the installation, also go through the user and safes that are created in the Vault and the relevant log files of the CPM.

10. Understand the Password Vault Web Access (**PVWA**) functionality along with pre-requisites and install the Password Vault Web Access (PVWA) and go through the environment that is created as part of the installation with the users and safes that are created in the Vault and the relevant log files.
11. Understand the functionality and benefits of implementing and using the Privileged Session Manager (**PSM**), the architecture and flows of the PSM server in the network, also observe the users and safes that are added to the Vault as part of the installation as well as local environment that is created on the server.
12. Understand the built-in users also the steps in order to configure transparent user management using the wizard as well as the manual process by integration with LDAP Server (**Active Directory**).
13. Integrate CyberArk Digital Vault with LDAP Server (**Active Directory**), SMTP Server (**MS Exchange**) & Event Notification Engine (**ENE**), SIEM (**Splunk**) practically and understand how to integrate **SNMP** and **RADIUS**.
14. Perform **Radius Configuration** as Authentication Provider and test the integration.
15. Handling CyberArk platforms to manage passwords/accounts in the network also how to edit the password management policy (**Master Policy**) as well as the steps to create safes and accounts in the Vault. The session will go over all the settings in the Master Policy as well as the basic configurations at the Platform level.
16. Understand the Application Identity Manager (**AIM**), its benefits, deployment options and internal workings. Hands on with different configuration options for different platforms.
17. Install and configure the **AIM** Agent on a Windows and Unix Server.
18. Understand the On-Demand Privilege Manager (**OPM**) product and the need for OPM for Unix and the benefits over the existing SUDO solution, the flow as well as the internal workings of the OPM product.
19. Account On-Boarding of large number of Accounts to the Vault in an automatic manner using **Accounts Discovery Utility** as well as the **Password Upload Utility**.
20. **Onboarding Rules** – (As part of the Accounts Discovery Utility), hands on in creating & managing predefined rules that automatically onboard newly discovered accounts.
21. Onboarding and handling **Privileged Accounts in AWS** (like EC2 Instance, IAM User Accounts etc.)
22. Understand the **safe design** and how to build **Access Control** also understand how to assign permissions to various safes in order to implement the relevant level of access control for safes in the Vault.
23. Understand the **Fault Tolerance** for the various components of the CyberArk PAS components with High Availability (HA) Vault, a Disaster Recovery (DR) Vault and how to back up the Vault.
24. Observe the various types of **reports** like the reports generated in the Private Ark Client and the PVWA as well as the permissions needed to generate the reports and various options.
25. Hands on in **Administrative tasks** like Creating and Managing Locations, Users & Groups; Creating and Managing Safes and Owners; Transparent User Management by Managing Directory Maps, modifying External User Accounts, managing Safe Ownership for LDAP Users and Groups; Working with Master Policy and Managing Platforms.
26. On board new accounts of various types – Linux, Linux SSH keypairs, Windows Local Accounts, Windows Domain Accounts, Oracle DB, Microsoft SQL Server Management Studio etc.
27. Perform daily operation and **maintenance tasks** - start/stop, observe logs for various components, important configuration files and known issues with troubleshooting steps.
28. **Privileged Session Manager SSH Proxy** or PSMP - Installation and end to end Implementation with PSM SSH Proxy with AD Bridge and PSMP Environment with testing & troubleshooting.

29. Configure **X Forwarding for PSM and PSMP** initiated sessions on *NIX Servers, to cover GUI based Installation and Configuration.
30. Backup & Restore using **Replicate** Utility with practical examples.
31. **Disaster Recovery** - Concept, Architecture, Installation & Environment, Understanding Active Mode, DR Mode and Failover process with CPMs, PSMs, PVWAs pointing to DR Vault, Manual Failback from DR to PROD & testing with understanding need of reverse replication.
32. Working with **CPM Usages** feature
33. Custom User Mapping / Directory Mapping
34. Secure Connect usage & feature
35. Usages of Master Account and Master CD
36. Implement and explore RemoteApp feature
37. Dual Control & Workflows
38. **Multiple, Distributed Component Architecture & Installation**: CPM, PVWA, and PSM
39. Learn how to do **upgrade from 9.6 to 11.1**
40. Hands on with **Logon Accounts** (Linux) and **Reconciliation Accounts** (Windows) using CPM
41. Troubleshooting & going through list of all important configuration and log files of all components (Vault, CPM, PSM, PVWA, PSMP, AIM, OPM etc.).

Note: We do not provide installers and licenses for Vault, High Availability, DR, upgrade, exchange and radius, rest all installers are provided for practicals.

It is a 100% practical course, all use cases will be demonstrated practically, keeping real time scenarios in mind.