Course Content

1. Introduction to CyberArk Privileged Access Management
   - Overview
   - Challenges and Threats
   - Protect Privilege, Break Chain
   - Key features of CyberArk PAM
   - The System Architecture
   - System interfaces and utilities
   - Online help and customer community
2. User Management
   - User Management Overview
   - Pre-Defined Users and Groups
   - User Management in PrivateArk Client
   - Transparent User Management
   - Authorizations
   - Directory Management
3. Policies and Platforms
   - CyberArk password management logic and flow
   - Master Policy
   - Create and manage Platforms
4. Access Control (Safes)
   - Overview (Vault Model, Safes)
   - Designing a Safe Model
   - Access Control Concepts
   - Granular Safe Permissions
   - Creating and Managing Safes
5. Account Management (Part 1)
   - Add Accounts
   - Account Management Operations
6. Account Management (Part 2)
   - Linked Accounts
   - SSH Key Management
7. Dependent Platforms
   - Configure various types of Dependent Platforms

8. Privileged Access Workflow
   - Allow transparent connections
   - Require users to specify reason for access
   - Dual Control
   - Exclusive Passwords
   - One-time Passwords

9. Discovery and Onboarding (Part 1)
   - Account Onboarding Methods
   - Accounts Discovery
   - Automatic Onboarding Rules

10. Discovery and Onboarding (Part 2)
   - Add Multiple accounts from a file
   - Continuous Accounts Discovery via PTA
   - Onboarding accounts via the REST API

11. Privilege Session Management (Part 1)
   - Privileged Session Manager (PSM)
   - Connection Components
   - PSM Ad-Hoc Connections
   - HTML5 Gateway
   - PSM for Windows
   - PSM for SSH

12. Privilege Session Management (Part 2)
   - Recordings
   - Manage Recordings
   - Session Audits
   - Active Session Monitoring

13. Privileged Threat Analytics
   - Functionality of Privileged Threat Analytics (PTA)
   - Data sources used by the PTA
   - Different attacks and risks detected by the PTA
   - Alert flow by the PTA
   - PTA Automatic responses
   - Session analysis and response flow

14. Reports
   - Types of reports that are available
   - Permissions required to run different reports
   - Reports Generation using the PVWA and PrivateArk Client
   - Reports Generation using Export Vault Data Utility

15. PAM Self Hosted Architecture
- System Architecture review
- Vault Security Controls
- Vault Encryption and Key Management
- Inside Vault, PVWA, CPM, PSM
- Internal Safes and Users
- Direct Communication with Vault
- Communicating with Vault vis REST

16. Backup and Restore
- Vault Backup and Restore Overview
- Replicate Utility
- Installing and Setup
- Test Backup and Restore
- Set up Scheduled Backups

17. Disaster Recovery
- Architecture
- Set up Disaster Recovery
- Vault Failover
- Component Failover
- Returning to Primary Vault

18. System Monitoring and Common Administrative Tasks
- Monitor the system health via various methods (REST, Email, SIEM, SNMP)
- Monitor replications
- Perform common administrative tasks related to system maintenance

19. Trouble Shooting
- Flow for troubleshooting issues in the CyberArk environment
- Locate and manage the log files generated by the Vault and various components
- Configure and use the x-Ray agent

20. Trouble Shooting Common Issues
- User authentication
- Component connectivity to the Vault
- Automatic password management by CPM
- Launching privileged sessions via PSM