## Description
Students will learn how to secure application account passwords and remove hard-coded credentials using CyberArk’s Application Identity Manager (AIM).

## Target Audience
Customers or partners who will implement CyberArk’s AIM solution and/or manage existing deployment.

## Objectives
After completion of this course each student will be able to:

- Install, configure, and implement CyberArk’s AIM solution according to CyberArk’s published implementation procedures.
- Define and describe CyberArk’s AIM system architecture, requirements, offerings, and workflow.
- Design and deploy an enterprise AIM environment following least privilege access principles.
- Administer and troubleshoot AIM to successfully query credentials from the Vault using the PasswordSDKs, SOAP/REST APIs, and managing data source connectivity using Application Server Credential Provider.

## Topics
The course includes the following topics:

- AIM technology overview
- Credential Provider installation and configuration
- Application provisioning and authentication
- Querying the Vault using the PasswordSDKs
- Enterprise implementation
- Central Credential Provider
- Application Server Credential Provider

## Technical Prerequisites
Verify and check the following prior to scheduled course:

- Computer with Internet connectivity
- Web browser that supports HTML5
- Test connectivity to following web-based services:
  - https://cloud.skytap.com/connectivity
  - http://www.webex.com/test-meeting.html

## Course Prerequisites
Successful completion of the Privileged Account Security (PAS) Fundamentals Course.

## Duration
2 days
## DAILY AGENDA

### DAY ONE

<table>
<thead>
<tr>
<th>Topic/Task</th>
<th>Description/Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Course Opening</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **Application Identity Manager (AIM) Overview** | • Privileged Account Security (PAS) Overview  
• Hard-Coded Credentials Overview  
• Application Identity Manager (AIM) Overview  
• AIM Offerings & Comparison Matrix  
• High-Level Use Cases |
| **Credential Provider**     | • Credential Provider Technology Overview  
• Architecture & Network Topology  
• Authentication Methods  
• Secure Cache Overview  
• High-Availability & Performance  
• Credential Provider Installation |
| **Administration**          | • Credential Provider Configuration Overview  
• Utilities & Commands Overview  
• Application Provisioning Overview  
• Password Management  
• Dual Account Provisioning |
| **Implementation**          | • Implementation Overview & Workflow  
• Planning & Design  
• Provider Installation & Configuration Practices  
• Application Provisioning Concepts  
• Implement PasswordSDK  
• Activate & Support |
| **Practical Exercise**      | Credential Provider (Windows & Linux)                     |
## DAY TWO

<table>
<thead>
<tr>
<th>Topic/Task</th>
<th>Description/Activity</th>
</tr>
</thead>
</table>
| **Central Credential Provider**   | ▪ Central Credential Provider Overview  
▪ Architecture & Topology           
▪ Authentication Methods            
▪ Application Authentication Workflow  
▪ High-Availability & Performance  
▪ Installation Overview            |
| **Application Server Credential Provider** | ▪ Application Server Credential Provider Overview  
▪ Architecture & Topology           
▪ Authentication Methods            
▪ Secure Cache                       
▪ High-Availability & Performance    
▪ Installation Workflow Overview    |
| **Troubleshooting**                | ▪ Documentation and Guides  
▪ Logging & Log Files Overview      
▪ Debug Levels                      
▪ Common Errors & Troubleshooting   |
| **Push Mode**                      | ▪ Push Mode Overview  
▪ Workflow & Network Communication  
▪ Supported Platforms Overview     
▪ Uses Cases Overview               |
| **Practical Exercise**             | **Configuring Dual Accounts**  
**Central Credential Provider**   
**Application Server Credential Provider**  
**Push Mode**                       
**Application Provisioning Bulk Upload** |