

Course Agenda

Introduction to IAM and CIAM

1. Introduction to IAM and CIAM
2. Understand the fundamental concepts of Identity and Access Management (IAM) and how it differs from Customer IAM (CIAM).
3. Explore the importance of secure identity management for both internal users and external customers.

Cybersecurity Concepts

1. Dive into essential cybersecurity principles relevant to IAM and CIAM.
2. Learn about threat vectors, authentication methods, and best practices for protecting identities.

User Management

1. Learn how to create, manage, and authenticate user identities.
2. Explore user provisioning, deprovisioning, and life-cycle management.

Directory Integration

1. Understand how to integrate with existing directories (such as Active Directory) for user synchronization.
2. Configure directory connectors and mappings.

Single Sign-On Protocols

Study key SSO protocols, including:

- a. Security Assertion Markup Language (SAML)

- b. Open ID Connect (OIDC)
- c. Secure Web Authentication (SWA)

OIDC Integration

- a. Dive deeper into Open-ID Connect (OIDC) and its role in modern authentication.
- b. Implement OIDC flows for secure user sign-in.
- c. Understand tokens, authorization flows, and refresh tokens.
- d. Understanding Okta Authentication Models
- e. Compare and contrast Okta authentication models
- f. Choose the right model for your use case.

Application Integration

- 1. Explore integrating applications with Okta for seamless user access.
- 2. Set up application connectors and configure access policies.
- 3. User and Application Life-cycle Management
- 4. Manage user accounts throughout their life cycle (creation, updates, deactivation).
- 5. Handle application life cycle events (e.g., app updates, retirements).

Multi-Factor Authentication (MFA)

- 1. Implement MFA to enhance security.
- 2. Explore various MFA methods (SMS, push notifications, TOTP).

Various Policies in Okta

Explore the different policies available in Okta and provide detailed explanations

- 1. Enrolment Policy
- 2. Authentication Policy
- 3. Global Session Policy

Hands-on Projects

- 1. Apply the concepts learned through practical exercises.

2. Create an Okta environment, configure applications and policies, and then validate the theoretical concepts through practical testing

Authorization Servers

1. Understand OAuth 2.0 authorization servers.
2. Configure scopes, claims, and consent management.