ProconsulAcademy

Corso di Identity & Access Management

Prerequisiti

I candidati, per la selezione e partecipazione al corso di formazione, dovranno essere in possesso di laurea e/o diploma e che abbiano una conoscenza base dell'ambito IT e conoscenza della lingua inglese.

Obiettivi

Il corso prevede l'obiettivo di fornire le competenze di base necessarie per poter operare su piattaforme IAM installate su sistemi Linux.
Le competenze acquisite consentiranno di conoscere quali sono le componenti software ed i protocolli utilizzati di una tipica soluzione di Identity & Access Management, quali funzionalità implementabili e le relative modalità attuali e innovative di applicazione.
Saranno inoltre acquisite conoscenze riguardanti alcune normative e regolamentazioni internazionali applicabili e relative all'ambito di Identity & Access Management.

Modulo 1 - Linux OS e Networking: 80 ore (teoria e laboratorio)

Obiettivo di questo modulo è fornire le informazioni per installare, configurare e amministrare un sistema Linux. Fornire inoltre una base di preparazione sistemistica orientata ad amministratori di sistema, affrontare problematiche reali, confrontare Linux con altri sistemi operativi e fare diretti riferimenti al mondo Internet. Verranno inoltre fornite tutte le competenze necessarie a supportare e implementare architetture di sistemi e reti aziendali operativamente sostenibili, altamente disponibili e soprattutto sicure. Verranno forniti gli strumenti per identificare e tradurre i requisiti in un'architettura tecnica completa.

Fondamenti di Linux ed Elementi Networking

- Introduzione al SO, installazione e configurazione di base
- Interazione con il FS
- User profilig, permissions e attributes
- Editing e manipolazione di testi
- Processi
- Bash shell scripting
- Gestione aggiornamenti e pacchetti
- Virtualizzazione
- Servizi (SSH, FTP,…)
- Elementi di networking (apparati LAN/WAN, architetture di base, protocolli standard)
- Amministrazione rete - Elementi base e comandi *Shell*

Modulo 2 - Identity & Access Management: 70 ore

In questo modulo verranno fornite tutte quelle competenze necessarie a gestire l'intero processo (applicazione di policy appropriate, impiego di strumenti tecnologici e di integrazione - API) per gestire le informazioni riguardanti l'identità degli utenti e controllarne l'accesso alle risorse aziendali.

Identity Management

- Introduzione IDM framework
- Customer Digital Identity e Workforce Digital Identity
- Life cycle trasformazione delle digital identity
- Trusted source e riconciliazione delle identità
- Target systemprovisioning e riconciliazione di accounts
- Workflow approvativi

- Roles, Policies e regole SoD
- Access Review e Certification process

Access Management

- Introduzione AM framework
- Web Application protection
- Reverse proxy ed agent
- Identity store ed LDAP
- Web Single Sign On
- Authentication e Authorization (RBAC/ABAC)
- Adaptive authentication (risk based)
- Multifactor authentication
- SAML Federation Identity e Service Provider
- Introduzione alle modalità di autenticazione passwordless
- Definizione e utilizzo di JWT Tokens
- Introduzione ai protocolli standard OAuth, OpenID, FIDO2

IAM Compliance Regulations

- Introduzione a: PSD2, GDPR, NIST, PCI DSS, SOX, HIPAA

Modulo 3 - Laboratorio: 60 ore

- Installazione e configurazione di piattaforme di Identity Access Management
- Introduzione ed uso di piattaforme di Identity Access Management