

IA100 Identity & Access Management - Inhalte gemäß IDPro® Inc.

Kurzbeschreibung:

Teilnehmer erhalten eine praxisnahe Einführung in Identity & Access Management (IAM). Vermittelt wird ein unabhängiger Überblick über technische und organisatorische Grundlagen, ausgerichtet am IDPro® Book of Knowledge. Behandelt werden zentrale Methoden des Identitäts- und Rechtemanagements sowie die Vorbereitung auf die internationale CIDPRO™ Zertifizierung der IDPro® Inc.

Zielgruppe:

Sie möchten die CIDPRO™ Zertifizierung angehen? Sie sind (Quer-)Einsteiger mit soliden IT-Kenntnissen oder Experte im IT-Umfeld?

Anwendungsmanager, Projektleiter, Berater, Architekten, Systemintegratoren, Administratoren sowie Service- & Risikomanager im IT-Bereich bilden zudem den Kern der Zielgruppe für dieses IAM-Training.

Voraussetzungen:

Praktische Vorkenntnisse im Bereich Identity & Access Management sind für dieses IAM-Training keine zwingende Voraussetzung. Für dieses IAM-Training werden solide IT-Kenntnisse zu Anwendungen, Betriebssystemen, Infrastrukturkomponenten und/oder Cloudplattformen benötigt. Kenntnisse der Informationssicherheit und Schutzziele sowie IT-Sicherheit sind von Vorteil. Technische Vorkenntnisse über relevante Standards (SAML, OAuth, OIDC, SCIM, SPML, etc.) sowie solides IT-Know-how erleichtern den erfolgreichen Abschluss der CIDPRO™ Zertifizierung.

Um als Professional die Zertifizierungsprüfung zum international anerkannten CIDPRO™ für Identity & Access Management anzugehen, sind umfassende Vorkenntnisse der Kernthemen erforderlich!

Sonstiges:

Dauer: 3 Tage

Preis: 2550 Euro plus Mwst.

Ziele:

Am Ende des Kurses verfügen Sie über einen Gesamtüberblick zur Umsetzung eines herstellerunabhängigen Identity & Access Managements mit folgenden Schwerpunkten:

- Grundlagen der Identity Governance & Administration (IGA)
- Grundlagen des Identity & Access Management (IAM) - Customer/Consumer IAM
- Überblick und Erläuterung von Zusammenhängen privilegierter Zugriffe (PxM), Zugriffe auf APIs und Microservices
- Erstellung digitaler Identitäten: Identifikation, Authentisierung und Autorisierung
- Grundlegende Einblicke in gesetzliche Vorgaben zum Schutz der Personendaten (GDPR)
- Grundlagen zu Föderation, IAM Architekturen, Multi-Faktor Authentisierung (MFA, FIDO2)
- Grundlagen der Access Control und Autorisierung
- Management technischer Konten - Projektmanagement für IAM
- Einblick in den praktischen Betrieb von IAM-Lösungen als Kursabrandung

Mit diesem Kurs können Sie sich auf die die Prüfung sowie die Zertifizierung zum "**CIDPRO™, Certified Identity Professional**" vorbereiten und werden für diese zugelassen.

Die Prüfung können Sie nach dem Kurs online bei der IDPro® Inc ablegen. Sie besteht aus 150 Fragen, die in 180 Minuten beantwortet werden müssen. Genaue Informationen zu den Prüfungsmodalitäten finden Sie [hier](#).

Die Prüfung und die Zertifizierung sind nicht Bestandteil dieses Kurses.

Inhalte/Agenda:

- Dieses – in Europa einzigartige – qSkills Training bietet einen generischen und ganzheitlichen Überblick über das gesamte Identitäts- und Rechtemanagement, unabhängig von den eingesetzten Werkzeugen und deren Umsetzung.
- - ◆ **Kurze Einführung in die Grundlagen der Identity Governance & Administration (IGA) und IAM**
 - ◆ **Kernkomponenten, Fachbegriffe und deren Zusammenhänge**
 - ◆ ◊ Workflows für Joiner/Mover/Leaver Prozesse
 - ◆ ◊ Rollen, Profile, Rechte, Attribute
 - ◆ ◊ Provisionierung vs. Föderation
 - ◆ **Administrative Verwaltung vs. Zugriff zur Laufzeit**
 - ◆ ◊ Admin-Time und Runtime - Bedeutung und Auswirkung
 - ◆ ◊ Verwaltung der Identitäten
 - ◆ ◊ Verwaltung der Zugriffsrechte
 - ◆ ◊ Lebenszyklus von Identitäten (Rollen und Rollenmodelle)
 - ◆ **Cloud-Consumer- und Customer IAM**
 - ◆ ◊ Auswirkung von GDPR und DSGVO - Consent und Selbstbestimmung
 - ◆ ◊ Dezentrale IDs - der Mythos SSI. Wie souverän kann eine ID sich verwalten?
 - ◆ ◊ Gesetze und Regelungen, die IAM beeinflussen
 - ◆ ◊ Identifier und Benutzernamen
 - ◆ ◊ Account Wiederherstellung
 - ◆ **Zugriffs-Management / Access Control**
 - ◆ ◊ Kritische Aufgaben zur Laufzeit
 - ◆ ◊ Policy basierte Access Control Verfahren
 - ◆ ◊ MAC / DAC / RBAC / ABAC und andere
 - ◆ ◊ PIP, PDP, PEP, PAP - wozu das alles?
 - ◆ ◊ SAML, OAuth, OIDC und was dazu gehört