ACE MULTIPASS
Cybersécurité - Méthodes agiles

FICHE DE FORMATION

Organisme de formation

Formation Gestion Des Identités & Fédération

Formation de 4 jours consacrée à la gestion des identités et des accès (IAM) : authentification, autorisation, cryptographie, PKI, fédération et SSO, jusqu'à l'IAM dans le cloud (Azure, AWS) et la mobilité (BYOD/MDM) — pour concevoir, évaluer et piloter une stratégie IAM d'entreprise.

DURÉE	PRIX	HORAIRES
4 jours	**2 800 €**	**9h00 - 17h00** *(pause déjeuner de 1h30 à midi)*

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation, les participants seront capables de :

- Distinguer et mettre en œuvre les mécanismes d'identification, d'authentification et d'autorisation, y compris forte et multifacteur.
- Choisir un modèle de contrôle d'accès adapté (DAC, MAC, RBAC, ABAC).
- Maîtriser les fondamentaux de la cryptographie et concevoir une infrastructure à clés publiques (PKI).
- Élaborer une stratégie de gestion des certificats et des autorités de certification.
- Mettre en œuvre une fédération d'identités et une authentification unique (SSO) avec les protocoles du marché (SAML, OpenID Connect).
- Déployer l'IAM dans des environnements cloud (Azure, AWS) et pour les usages mobiles/BYOD.
- Évaluer et construire une stratégie IAM globale adaptée au contexte de son entreprise.

PUBLIC CIBLE ET PRÉREQUIS

Toute personne en charge de la sécurité de l'entreprise (RSSI, responsables sécurité systèmes/réseaux) et professionnels chargés d'élaborer ou d'évaluer une stratégie de gestion des identités (entreprise, B2B, Internet).

Connaissances de base en systèmes, réseaux et sécurité informatique. Maîtrise du système d'exploitation Windows.

PROGRAMME

Module 1 · Les enjeux d'une stratégie de gestion des identités (1h30)

- Pourquoi structurer la gestion des identités : sécurité, conformité, expérience utilisateur, maîtrise des coûts.
- Ce que recouvre la gestion des identités (IAM) : périmètre, acteurs, cycle de vie d'une identité.
- Les grandes approches selon le contexte : entreprise interne, B2B, grand public (Internet).

Module 2 · Identification, authentification et autorisation (2h)

- Distinguer identification, authentification et autorisation : trois notions souvent confondues.
- L'authentification forte : principes et cas d'usage.
- La biométrie comme facteur d'authentification : possibilités et limites.
- L'authentification multifacteur (MFA) avec les terminaux mobiles.

Module 3 · Administration et gouvernance des identités (1h)

- Le cycle de vie d'une identité : création, modification, suspension, suppression.
- Les principes de gouvernance : revues d'habilitations, séparation des tâches, traçabilité.
- Le rôle des processus d'administration dans la réduction des risques.

Module 4 · Les annuaires et bases de données d'authentification (2h)

- L'annuaire centralisé face à l'approche fédérative : avantages et limites de chaque modèle.
- Les annuaires LDAP v3 : structure, schéma, réplication.
- Sécuriser les accès à l'annuaire : LDAPS, LDAP/TLS.
- Contrôle et audit des accès aux objets de l'annuaire, publication de certificats.

Module 5 · Les modèles de contrôle d'accès (1h30)

- Comparer les grandes méthodes de gestion des autorisations : DAC, MAC, RBAC, ABAC.
- Les listes de contrôle d'accès (ACL) : fonctionnement et cas d'usage.
- Choisir le bon modèle selon le contexte organisationnel.

Module 6 · Notions de cryptographie pour l'IAM (2h)

- Le chiffrement symétrique et asymétrique : principes et usages respectifs.
- Le condensé (hash) et la signature numérique : garantir intégrité et authenticité.
- La notion de certificat numérique comme brique de confiance.

Module 7 · Implémentation matérielle de la cryptographie (1h)

- Stocker les clés privées sur des jetons matériels (Cartes à puce, Yubikey…) et modules de sécurité matériels (HSM).
- Le recours aux conteneurs matériels pour la protection des clés.
- Comparer les niveaux de sécurité selon le mode de stockage choisi.

Module 8 · Infrastructure à clés publiques (PKI) : les fondamentaux (2h)

- Les certificats X.509 v3 et leur rôle dans une infrastructure PKI.
- Définir une identité dans une infrastructure à clés publiques.
- Déterminer la durée de vie des certificats et contrôler l'accès via les certificats d'attributs.

Module 9 · Élaborer une stratégie de gestion des certificats (2h)

- Sécuriser les clés privées : archivage automatique, agent de récupération de clés.
- Associer des identités à des certificats et distribuer des certificats de confiance.
- Publier les listes de certificats révoqués (CRL) et gérer la hiérarchie des autorités de certification (CA racine, intermédiaire, émettrice).
- Renforcer la sécurité avec une CA racine hors connexion ; évaluer la confiance envers des CA externes et respecter une politique de certification.

Module 10 · Les protocoles d'authentification et de propagation (2h)

- Les protocoles de propagation des identités : SAML, SOAP.
- Sécuriser les échanges XML : XML Encryption, XML Signature.
- Le rôle de ces protocoles dans l'interopérabilité entre systèmes.

Module 11 · La gestion fédérée des identités et le SSO (2h)

- Le principe de l'authentification unique (SSO) et ses bénéfices.
- Garantir l'interopérabilité grâce aux revendications (claims) et aux normes ouvertes du secteur.
- La vision du méta-système d'identités : fédérer sans centraliser.

Module 12 · Étude de cas : gestion fédérée avec Microsoft ADFS (1h)

- Authentification locale et accès distant dans une architecture ADFS.
- Concevoir des applications basées sur les revendications avec SAML.
- Abstraction des protocoles WS-Trust et WS-Federation : ce qu'ils apportent concrètement.

Module 13 · Fédération des identités avec Microsoft Azure (1h30)

- Étendre un Active Directory sur site vers Azure.
- Mettre en œuvre l'authentification unique avec Azure pour les applications SaaS.
- Garantir l'interopérabilité et la portabilité des identités entre environnements.

Module 14 · Fédération avec AWS et interopérabilité multi-cloud (1h30)

- La fédération Amazon AWS : s'authentifier avec les rôles IAM d'Amazon.
- Connecter une identité Microsoft fédérée aux services et instances Amazon.
- Simplifier la gestion des identités entre systèmes grâce au protocole SCIM.

Module 15 · Gestion des identités pour la mobilité et le BYOD (1h30)

- Les enjeux spécifiques de l'IAM pour les terminaux mobiles et les usages BYOD.
- Enregistrer des appareils mobiles à l'aide de certificats.
- Configurer le protocole SCEP (Simple Certificate Enrollment Protocol), avec l'exemple d'un MDM (Microsoft Intune) et de périphériques réseau.

Module 16 · Synthèse : élaborer une stratégie IAM globale (1h30)

- Retour sur les grandes briques abordées durant la formation.
- Grille d'évaluation d'une solution de gestion des identités pour un contexte entreprise, B2B ou Internet.
- Facteurs clés de succès et pièges courants d'un projet IAM.

LISTE DES ATELIERS ET DÉMONSTRATIONS

- Atelier 1 : utilisation des lacunes protocolaires
- Démo 2 : simuler un échange de clés Diffie-Hellman
- Atelier 3 : installation et configuration d'un serveur SSH
- Atelier 4 : utilisation d'OpenSSL pour échanger de manière sécurisée
- Atelier 5 : magasin de certificats Microsoft
- Atelier 6 : mise en œuvre d'une autorité de certification racine Microsoft
- Atelier 7 : mise en œuvre d'une autorité de certification intermédiaire Microsoft
- Atelier 8 : configuration et émission d'un certificat utilisateur
- Atelier 9 : authentification web par certificat
- Atelier 10 : échange d'e-mail sécurisé
- Atelier 11 : authentification web Firefox et signature électronique de document PDF et Word
- Atelier 12 : inscription d'un utilisateur carte à puce par un agent d'inscription
- Atelier 13 : archivage et restauration de certificat
- Atelier 14 : configuration SSO avec ADFS
- Démo 15 : installer et configurer Azure AD Connect
- Démo 16 : utiliser AWS SSO pour s'intégrer avec Azure AD
- Démo 17 : fédération AWS IAM avec Azure AD

- Démo 18 : configurer le protocole d'inscription des certificats simple (SCEP)

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Chaque session peut être adaptée aux besoins des personnes en situation de handicap. Nous invitons les participants concernés à nous en informer avant le début de la formation, afin d'examiner ensemble les aménagements possibles : conditions d'accès aux salles, adaptation des supports et des méthodes pédagogiques, ou réorganisation du planning de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

L'animation des sessions s'appuie sur des outils variés : supports audiovisuels, documents remis aux stagiaires, mises en application pratiques accompagnées de leurs corrigés pour les formations à vocation opérationnelle, et études de cas concrets ou retours d'expérience pour les sessions à caractère plus théorique.

À la fin de chaque session, ACE-MULTIPASS remet aux stagiaires un questionnaire de satisfaction, dont les résultats sont ensuite examinés par l'équipe pédagogique.

Une feuille de présence est signée à chaque demi-journée et remise en fin de parcours ; une attestation de suivi de formation est également délivrée aux stagiaires ayant participé à l'intégralité de la session.

COMPÉTENCES DU FORMATEUR

Nos intervenants sont choisis pour leur expertise dans les domaines qu'ils enseignent. Chacun est sélectionné par notre équipe pédagogique, qui vérifie à la fois sa maîtrise technique du sujet et ses aptitudes à transmettre et animer un groupe. Ils justifient généralement de cinq à dix ans d'expérience professionnelle au minimum, et occupent ou ont occupé des fonctions à responsabilité dans leur secteur d'activité.

MODALITÉS D'ÉVALUATION

Tout au long du parcours, le formateur mesure la progression des stagiaires à travers différents exercices : questionnaires à choix multiples, mises en situation ou exercices pratiques.

Un test de positionnement est par ailleurs réalisé avant et après la formation, afin de mesurer les compétences acquises par chaque participant.