

Identity-First Security et PAM

2 jours (14 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

1 470 € HT par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 03/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Définir les principes de l'Identity-First Security et leur lien avec le Zero Trust
- Identifier les menaces actuelles liées aux identités humaines et non humaines (API, services et machines)
- Concevoir une architecture cible intégrant IAM, IGA et PAM dans une approche unifiée
- Mettre en oeuvre les concepts clés du PAM moderne : JIT, EPM, vault, session management et audit
- Définir un plan de déploiement et d'industrialisation (processus, outillage, automatisation et Intelligence Artificielle (IA))
- Elaborer des scénarios de défense et de détection des attaques centrées sur l'identité.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Ingénieurs et architectes sécurité (IAM, PAM, infra, cloud et DevSecOps), experts et responsables cybersécurité (RSSI adjoints et leaders Zero Trust), administrateurs systèmes / Cloud / AD en charge des comptes à privilèges, chefs de projets techniques impliqués dans des programmes IAM / PAM / Zero Trust.

Prérequis

Avoir une connaissance des fondamentaux réseau, systèmes et sécurité (AD, LDAP, TLS et segmentation), une connaissance pratique de l'authentification / autorisation (SSO, MFA, RBAC / ABAC, OAuth2 / OIDC et SAML) et une expérience terrain sur au moins une technologie IAM ou annuaire d'entreprise. Avoir des notions de base sur la journalisation, la corrélation d'événements et les SOC / SIEM.

Programme

1 Pendant votre formation

Identity-First Security et PAM

Jour 1 – Matin

Contexte et paradigme Identity-First

- Paysage des menaces récentes centré identité
 - Montée des attaques basées sur l'identité, APT identity-centric et compromission de SaaS / Entra ID / IdP
 - Explosion des identités non humaines (API, IoT et services et workloads Cloud)
- Principes et définitions de l'Identity-First Security
 - De la défense périmétrique à l'identité comme nouveau périmètre
 - Place de l'Identity-First dans les architectures Zero Trust (NIST SP 800-207 et ISO 27001 IAM)
- Cadres de référence et tendances structurantes
 - Alignement avec Zero Trust, CIAM, IGA, PAM, CIEM et ITDR
 - Rôle de l'Intelligence Artificielle (IA) et de l'analytique comportementale dans la protection des identités

Cartographie des identités et des modèles d'accès

- Typologie des identités et des surfaces d'attaque
 - Identités humaines (employés, partenaires, administrateurs, comptes d'urgence...)
 - Identités non humaines (robots, microservices, clés API, IoT, workloads Cloud...)
- Modèles d'authentification et d'autorisation modernes
 - Authentification : MFA, phishing-resistant, passkeys, biométrie et RBA
 - Autorisation : RBAC, ABAC, policy-based access et Continuous Access Evaluation
- Gouvernance et cycle de vie des identités
 - Jointure / mobilité / départ, revue de droits, recertification et orphan accounts
 - Convergence IAM / PAM et centralisation de la vue des identités et des privilèges

Exemples de travaux pratiques (à titre indicatif)

- Construction d'une matrice identités / applications / privilèges pour un SI
- Identification des comptes à privilèges, comptes techniques, secrets dispersés et risques associés

Jour 1 – Après-midi

Fondamentaux et évolution du PAM

- Rappels et limites du PAM "traditionnel"
 - Vault de mots de passe, bastion, gestion de sessions, rotation et audit
 - Limitations face au cloud, au remote work, à DevOps et aux environnements hybrides
- PAM moderne et intégration Zero Trust
 - Just-In-Time (JIT) access, Just-Enough-Access (JEA), EPM et approches passwordless
 - Intégration IAM / PAM, CIEM, micro segmentation et contrôle d'accès contextuel
- Tendances modernes : IA, blockchain et Cloud native PAM
 - IA pour détection d'anomalies, risk-based access et réponse automatique
 - PAM Cloud native, PAM pour IoT / OT et innovations blockchain (journaux immuables, smart contracts)

Exemples de travaux pratiques (à titre indicatif)

- Evaluation d'un cas d'usage réel au regard des bonnes pratiques PAM récentes
- Elaboration d'une feuille de route de modernisation PAM (quick wins et chantiers structurants)

Architecture Identity-first et design de haut niveau

- Référentiels d'architecture et patterns clés
 - Architecture CHEZ (CIAM-PAM unifiés) et autres modèles d'architecture intégrée
 - Positionnement des briques : IdP, IGA, PAM, CIEM, EDR / XDR, SIEM / SOAR et secrets management
- Flux critiques et chemins d'attaque identitaires
 - Chemins d'attaque sur les identités : phishing, token theft, consent phishing, relay et abuse d'API
 - Lateral movement via comptes à privilèges, shadow admins et services mal protégés
- Principes de design d'une architecture cible
 - Enforcing least privilege, segmentation des rôles et privilèges et réduction des comptes permanents
 - Centralisation des politiques, logs et supervision identity-centric

Exemples de travaux pratiques (à titre indicatif)

- Conception schématique d'une architecture cible pour une entreprise type
- Identification des points d'intégration IAM-PAM-SOC, des flux sensibles et des contrôles clés

Jour 2 – Matin

Mise en oeuvre opérationnelle d'un PAM moderne

- Modélisation des comptes à privilèges
 - Typologie : comptes admins, applicatifs, d'urgence et break-glass

- Inventaire automatisé, découverte continue, classification des comptes et secrets
- Politiques d'accès, JIT / JEA et EPM
 - Définition des politiques de JIT et élévation temporaire de privilèges
 - Endpoint Privilege Management, enforcement granulaire et contextuel des privilèges
- Journalisation, supervision et intégration SOC
 - Captures de sessions, logs détaillés, corrélation avec SIEM et alertes SOC
 - Indicateurs de performance et de risque autour des identités et privilèges

Exemples de travaux pratiques (à titre indicatif)

- Définition d'un jeu de politiques JIT / JEA pour plusieurs profils (admin AD, admin DB et DevOps)
- Spécification des besoins de logs / supervision pour intégration dans le SOC / SIEM

Scénarios d'attaques et défense centrée identité

- Scénarios d'attaque APT centrés identité
 - Chaînes d'attaque modernes : initial access, credential theft, session hijacking et abus de consentement
 - Exploitation des comptes à privilèges sur Cloud, SaaS et environnements hybrides
- Détection et réponse sur signaux identitaires
 - Identity Threat Detection and Response (ITDR) et signaux d'alerte clés
 - Corrélation identité, endpoint, réseau et Cloud pour interrompre la kill chain
- Renforcement continu et boucle d'amélioration
 - Utilisation des lessons learned, revues post-incident et ajustement des politiques
 - Automatisation de la réponse via SOAR avec signaux PAM / IAM / IdP

Exemples de travaux pratiques (à titre indicatif)

- Simulation guidée d'une attaque centrée sur les identités (scénario APT)
- Construction d'un plan de détection / réponse utilisant les capacités IAM / PAM / ITDR disponibles

Jour 2 – Après-midi

Intégration avec le Cloud, DevOps et IoT / OT

- PAM pour environnements Cloud et DevOps
 - Gestion des secrets dans les pipelines CI/CD, conteneurs et microservices
 - PAM pour consoles Cloud, privilèges temporaires et just-in-time sur ressources PaaS / IaaS
- PAM pour IoT / OT et identités techniques dispersées
 - Défis d'authentification et de gestion des privilèges pour IoT et OT
 - Patterns de sécurisation pour devices contraints, passerelles et plateformes IoT
- Innovations : blockchain, passwordless et convergence CIAM-PAM
 - Utilisation de journaux immuables et smart contracts pour la traçabilité des accès
 - Unification CIAM-PAM et bénéfices en termes de sécurité et conformité

Exemples de travaux pratiques (à titre indicatif)

- Définition d'un pattern type de gestion de secrets pour un pipeline CI/CD et un cluster Kubernetes
- Proposition de contrôles PAM spécifiques pour une plateforme IoT / OT exposée

Roadmap, gouvernance et adoption

- Gouvernance Identity-first et comités de pilotage
 - Rôles et responsabilités et gouvernance transverse IAM / PAM / Cloud / SOC
 - Alignement avec la conformité : audit, traçabilité, privacy et exigences réglementaires
- Roadmap de transformation Identity-First et PAM
 - Priorisation des chantiers : quick wins, remédiations critiques et projets structurants
 - Indicateurs de suivi et communication aux parties prenantes (IT, métiers et direction)
- Facteurs clés de succès et anti-patterns
 - Facteurs de succès projets IAM / PAM : sponsor, périmètre, intégration et opérations
 - Erreurs fréquentes : silos outils, manque d'inventaire, sur-privileges et sous-exploitation des logs

Exemples de travaux pratiques (à titre indicatif)

- Construction d'une roadmap sur 18-24 mois pour une organisation type
- Définition de 5 à 7 jalons clés, avec livrables, risques principaux et dépendances

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 2 février 2027 au 3 février 2027 (2 jours / 14 heures)

À distance

Du 2 février 2027 au 3 février 2027 À distance

- 2 février 2027 9h00 - 16h30
- 3 février 2027 9h00 - 16h30