Cybersécurité

Gestion des identités et des accès (IAM)

Vous allez apprendre à

- Comprendre les concepts clés de l'IAM et leur rôle dans la cybersécurité d'entreprise.
- Identifier les composants d'une architecture IAM (gestion des identités, des habilitations, authentification, fédération...).
- Cartographier les rôles, droits, et accès selon les principes de sécurité (RBAC, ABAC, Zero Trust).
- Découvrir les bonnes pratiques pour sécuriser les accès tout au long du cycle de vie utilisateur.
- Appréhender les normes, référentiels et outils liés à l'IAM (ISO 27001, NIST, outils IAM du marché).

Public visé

- Responsables IT, RSSI, analystes sécurité, gestionnaires d'habilitations.
- Consultants en cybersécurité, auditeurs techniques.
- Responsables RH ou métiers impliqués dans la gestion des droits.

Les objectifs de la formation

À la fin de la formation, les participants seront capables de :

- Définir ce qu'est l'IAM et pourquoi il est central dans une politique de cybersécurité.
- Décrire les principales fonctions et processus du cycle de vie des identités.
- Comprendre la gouvernance des accès et les modèles de droits (RBAC, SoD...).
- Identifier les enjeux métiers, techniques et organisationnels liés à l'IAM.
- Appréhender les solutions IAM du marché et les leviers de transformation.

Les prérequis de la formation

- Avoir des bases en systèmes d'information ou en cybersécurité.
- Une première exposition aux problématiques de gestion des accès est un plus.

Programme de la formation

- **Introduction : Pourquoi l'IAM est un pilier de la cybersécurité moderne**
- **Module 1 : Concepts fondamentaux – identités, rôles, habilitations**
  - Définition et objectifs de l'IAM.3
  - Terminologie : identité, provisionning, autorisation, SSO, MFA, fédération.
  - IAM vs IGA (Identity Governance & Administration).
  - Importance de l'IAM dans le cadre réglementaire (ISO, RGPD, NIS2...).
  - Acteurs impliqués (IT, RH, sécurité, métiers).
- **Module 2 : Cycle de vie des identités : création, modification, retrait**
  - Étapes : onboarding, mobilité interne, offboarding.
  - Gestion des comptes dans les SI (Active Directory, applications SaaS...).
  - Processus automatisés vs manuels.
  - Notion de « Just Enough Access » et « Just In Time Access ».
  - Points de contrôle sécurité (revue des droits, SoD).
- **Module 3 : Modèles de gouvernance des accès : RBAC, ABAC, Zero Trust**
  - RBAC (Role Based Access Control) : principes, construction, risques.
  - ABAC (Attribute Based Access Control) : flexibilité, contexte.
  - PBAC / UBAC / SoD (Séparation des responsabilités).
  - Introduction au modèle Zero Trust appliqué à l'IAM.
  - Comment documenter et auditer une politique d'accès.
- **Module 4 : Panorama des outils IAM : Azure AD, Okta, CyberArk, etc.**
  - Présentation des grands éditeurs IAM : Microsoft Entra (ex-Azure AD), Okta, CyberArk.
  - IAM intégré vs solutions spécialisées.
  - Principales fonctionnalités : annuaires, SSO, MFA, synchronisation, reporting.
  - Intégration avec les annuaires d'entreprise (LDAP, AD...).
- **Cas pratique guidé : cartographie des droits dans un SI fictif**
- **QCM + échanges autour des projets IAM en entreprise**