Cybersécurité

Authentifications et autorisations, architectures et solutions

Vous allez apprendre à

- Comprendre les fondamentaux du modèle AAA (Authentication, Authorization, Accounting) et leur rôle dans la sécurisation des accès.
- Maîtriser les mécanismes d'authentification modernes : MFA, protocoles d'authentification, certificats, PKI et TLS.
- Comprendre les modèles de contrôle d'accès et d'autorisation : RBAC, ABAC, PBAC et leurs cas d'usage en entreprise.
- Concevoir des architectures d'accès sécurisées intégrant VPN, bastion, ZTNA et Zero Trust.
- Mettre en œuvre une journalisation exploitable et auditable (Accounting, SIEM, traçabilité, supervision des accès).
- Comprendre la gestion des identités et le cycle de vie IAM : provisioning, gouvernance et centralisation AAA.
- Comparer et sélectionner les solutions AAA du marché (open source vs commerciales) selon des critères techniques, sécurité et conformité.

Public visé

- Architectes cybersécurité et architectes IAM
- RSSI, responsables sécurité et gouvernance IAM
- Responsables infrastructure, systèmes et réseaux
- Administrateurs IAM, systèmes, Active Directory et Linux
- Chefs de projet techniques et décideurs IT
- Consultants cybersécurité, auditeurs et intégrateurs

Les objectifs de la formation

- Comprendre les fondamentaux du modèle AAA : Authentication, Authorization, Accounting, ainsi que leur rôle dans les architectures de sécurité modernes.
- Maîtriser les mécanismes d'authentification et de gestion des identités : MFA, protocoles d'authentification, cycle de vie IAM, Microsoft Identity et Linux PAM.
- Comprendre et appliquer les modèles de contrôle d'accès : RBAC, ABAC, PBAC, Zero Trust et architectures d'accès entreprise (VPN, bastion, ZTNA).
- Appréhender les principes de journalisation, de supervision et d'auditabilité (Accounting) dans une architecture AAA.
- Comprendre les mécanismes cryptographiques appliqués à l'IAM : PKI, certificats, TLS/HTTPS, chiffrement et confiance numérique. Concevoir une architecture AAA centralisée et moderne intégrant RADIUS, TACACS+, LDAP, IAM et MFA moderne.
- Comparer et sélectionner les solutions AAA du marché (open source et commerciales) selon des critères techniques, métiers et de gouvernance.
- Intégrer les exigences réglementaires et de conformité (NIS2, DORA, eIDAS2, UE 2026) dans la conception des architectures AAA.
- Développer une vision architecturale et décisionnelle pour sécuriser les accès, les identités et la traçabilité dans un SI d'entreprise.

Les prérequis de la formation

- Connaissances de base des architectures techniques.

Programme de la formation

Jour 1 - Identification et Authentification

- Fondamentaux AAA & Gouvernance de l'identité, Les mécanismes d'authentification
- Écosystème Microsoft & Gestion des identités, Linux & Authentification modulaire
- les protocoles d'authentification, l'implémentation de la gestion de l'identité, Cycle de vie IAM

Jour 2 - Autorisation, Traçabilité, Architecture, Gouvernance et Conformité.

- Contrôle d'accès & modèles d'autorisation
- Accounting, Cryptographie
- Accès entreprise
- Zero Trust
- MFA modern
- Centralisation AAA
- Solutions open source et commerciales
- Méthode de sélection et conformité UE 2026.