Sécuriser les Architectures Réseaux et Infrastructures Modernes

Lien : https://innov-maroc.com/formation/securiser-les-architectures-reseaux-et-infrastructures-modernes

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC303

CATÉGORIE
Fondamentaux Sécurité Informatique

OBJECTIFS DE LA FORMATION

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

- Identifier les vulnérabilités structurelles d’une architecture réseau complexe
- Concevoir des architectures réseau sécurisées et résilientes
- Appliquer les bonnes pratiques de segmentation, d’isolation et de durcissement des environnements
- Évaluer et auditer la sécurité d’une architecture existante
- Élaborer un plan d’évolution et de sécurisation continue des infrastructures IT et Cloud

POUR QUI ?

- Administrateurs systèmes et réseaux confirmés
- Architectes techniques ou responsables d’infrastructure
- Responsables sécurité IT (RSSI, responsables de la conformité)
- Chefs de projets techniques en charge de la sécurisation des SI
- Ingénieurs ou techniciens souhaitant renforcer leurs compétences en architecture sécurisée

Programme détaillé

1 / INTRODUCTION ET CONTEXTE

- Présentation des objectifs et enjeux de la formation
- Panorama des menaces modernes sur les architectures
- Notions de surface d’attaque et d’exposition
- Principes de conception sécurisée (security by design)

2 / PRINCIPES D’ARCHITECTURE ET DE SEGMENTATION

- Modèles de référence (OSI, TCP/IP) appliqués à la sécurité
- Segmentation logique : LAN, VLAN, zones et sous-zones
- Micro-segmentation et isolation des flux
- Notion de zones de confiance et périmètres de sécurité

3 / DÉMARCHE D’ANALYSE DES RISQUES

- Identification et classification des actifs critiques
- Évaluation des menaces et vulnérabilités
- Introduction aux méthodes EBIOS et ISO 27005
- Application sur un cas concret d’architecture d’entreprise

4 / COMPOSANTS ET SERVICES RÉSEAUX SÉCURISÉS

- Routeurs, commutateurs, pare-feu : configuration et durcissement
- Protocoles sécurisés : SSH, HTTPS, IPsec, TLS

- Sécurité des services de base (DNS, DHCP, NTP, etc.)

5 / FLUX ET CONTRÔLE D’ACCÈS

- Filtrage des flux interzones (ACL, firewall, IDS/IPS)
- Authentification et autorisation sur les équipements réseau
- Gestion des accès distants et des VPN
- Chiffrement des communications et segmentation des flux sensibles

6 / ADMINISTRATION SÉCURISÉE

- Bonnes pratiques d’administration des systèmes et réseaux
- Comptes d’administration et séparation des privilèges
- Gestion des journaux et traçabilité des actions
- Sécurisation des postes d’administration et bastions

7 / HAUTE DISPONIBILITÉ ET CONTINUITÉ DE SERVICE

- Concepts de redondance et basculement
- Gestion de la tolérance aux pannes
- Plans de reprise d’activité (PRA) et de continuité (PCA)
- Dépendances circulaires et risques liés aux interconnexions

8 / SÉCURITÉ DES ENVIRONNEMENTS VIRTUALISÉS

- Risques spécifiques à la virtualisation
- Sécurisation des hyperviseurs et des machines virtuelles
- Cloisonnement des réseaux virtuels
- Bonnes pratiques pour VMware, Hyper-V et KVM

9 / CLOUD ET INFRASTRUCTURES HYBRIDES

- Modèles de déploiement (IaaS, PaaS, SaaS)

- Sécurité partagée et responsabilités
- Sécurisation des identités et des accès (IAM)
- Audit et conformité des environnements Cloud

10 / MÉTHODOLOGIE D'AUDIT DE SÉCURITÉ

- Préparation, périmètre et collecte d'informations
- Outils et techniques d'audit d'architecture
- Cartographie des flux et dépendances critiques
- Évaluation de la maturité de la sécurité d'une architecture

11 / CAS PRATIQUE D'AUDIT

- Étude d'un cas réel d'architecture multi-sites
- Identification des vulnérabilités et points faibles
- Proposition de plan de remédiation
- Présentation et justification des recommandations

12 / OUTILS ET RÉFÉRENTIELS

- Référentiels techniques : ANSSI, CIS Benchmarks, NIST
- Outils d'analyse et de supervision de sécurité
- Gestion centralisée des configurations (Ansible, Terraform, etc.)

13 / PLAN D'ÉVOLUTION SÉCURISÉE

- Élaboration d'un plan de sécurisation à moyen terme
- Gouvernance et suivi des évolutions
- Indicateurs de performance et tableaux de bord sécurité

14 / GESTION DES TIERS ET SOUS-TRAITANTS

- Risques liés à la sous-traitance et aux interconnexions externes

- Contrôle et supervision des prestataires
- Clauses contractuelles de sécurité et conformité

15 / ATELIER DE CONCEPTION D'ARCHITECTURE SÉCURISÉE

- Travaux pratiques en groupe : conception d'une architecture sécurisée complète
- Présentation, échanges et validation collective
- Synthèse des acquis et plan d'action individuel

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

31 Août au 04 Sep. 2026	Distanciel
26 au 30 Oct. 2026	Distanciel

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-maroc.com
Web : https//www.innov-maroc.com