Sécurité Systèmes et Réseaux, niveau 1

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC19

CATÉGORIE
Sécurité du SI

OBJECTIFS DE LA FORMATION

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

- Connaitre le rôle des divers équipements de sécurité dans la protection des Systèmes et réseaux de l'entreprise
- Etre capable de concevoir et mettre en œuvre une architecture de sécurité

POUR QUI ?

- Responsables de l'informatique
- Administrateurs réseaux
- Techniciens
- Webmasters
- Responsables de la sécurité informatique
- Toute personne en charge de la sécurité d'un système d'information

Programme détaillé

1/ Concepts de base de la sécurité informatique

- Vue d'ensemble de la sécurité informatique
- Panorama des risques actuels
- Les attaques sur les protocoles réseaux
- Principales faiblesses du protocole TCP/IP
- Les faiblesses de l'accès réseau
- Les faiblesses des services : Web, VoIP, Messagerie
- Attaque par injection SQL, Cross Site Scripting
- DNS : attaque Dan Kaminsky

2/ La sécurité des accès, Firewall, WAF, Proxy, NAC

- L’accès des stations aux réseaux d’entreprise, 802.1X, NAC
- Panorama des types de firewalls
- Présentation des règles de filtrage
- Les règles de la translation d'adresse (NAT)
- Le rôle des zones démilitarisées (DMZ)
- Détection des vulnérabilités avec les IDS (Intrusion Detection System)
- Proxy ou firewall
- Intégrer et gérer un firewall
- Gestion et l'analyse des fichiers log

3/ La sécurité des systèmes, le "Hardening"

- Insuffisance des installations par défaut
- Critères d'évaluation (TCSEC, ITSEC et critères communs)
- Le Hardening de Windows
- Gestion de comptes d'accès
- Contrôle des services
- Configuration réseau et audit
- Le Hardening d’Unix/Linux
- Configuration du noyau
- Système de fichiers
- Gestion des services et du réseau
- Le Hardening des nomades : IOS / Android

4/ La sécurité des applications

- Les serveurs et clients Web
- La messagerie électronique
- La VoIP IPbx et téléphones

5/ Sécurité des données, la cryptographie

- Cryptographie : Objectifs et fonctions de base
- Chiffrements symétrique
- Chiffrements asymétriques
- Les algorithmes de hashing
- Authentification de l'utilisateur (pap,chap,Kerberos)
- Le HMAC et la signature électronique
- Les certificats et la PKI
- Virus, Antivirus, Malwares, Ransomwares

6/ Sécurité des échanges

- Sécurité WiFi

- Présentation des risques inhérents aux réseaux sans fil
- Les limites du WEP, WPA, WPA2
- Panorama des types d'attaques
- Le protocole SSH/SSL
- Les VPNs site à site et nomade

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

29 Juin au 03 Juil. 2026	Casablanca
24 au 28 Août 2026	
19 au 23 Oct. 2026	

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

Scannez pour accéder à la fiche en ligne