Sécurité Systèmes et Réseaux, niveau 2

Lien : https://innov-systems.com/formation/securite-systemes-et-reseaux-niveau-2

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SEC20**	**Sécurité du SI**

OBJECTIFS DE LA FORMATION

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

- Connaitre les solutions pour maintenir la protection de l'entreprise
- Etre capable de mettre en oeuvre une architecture de sécurité répondant aux exigences de l'entreprise

POUR QUI ?

- Architectes sécurité
- Techniciens et administrateurs systèmes et réseaux
- Toute personne en charge de la sécurité d'un système d'information

Programme détaillé

1 / Rappels

- Rappels sur le protocole TCP/IP
- L'architecture des réseaux
- Différents types de réseaux : VPN SSL, VPN IPsec, MPLS, VLANs, Wifi…
- Panorama des équipements : NAT, firewall, proxy, UTM…
- DMZ

2 / Les outils d'attaque

- Classification des attaques
- Les méthodes des attaquants : spoofing, flooding, injection, capture, etc
- Librairies : Libnet, Libpcap, Winpcap, Libbpf, Nasl, lua
- Panorama des outils

3 / Application de la cryptographie

- Les services de sécurité
- Principes et algorithmes cryptographique
- Certificats et PKIs
- Protocole IPSEC
- Réseaux privés virtuels (VPN)
- Protocole SSL (Secure Sockets Layer)
- Protocole TLS (Transport Layer Security)
- Protocole HTTPS (HyperText Transfer Protocol Secure)

4 / Architectures "3A" : Authentication, Autorization, Accounting

- Le réseau AAA

- One Time Password
- Positionnement de LDAP dans les solutions d'authentification
- Les module PAM et SASL
- Architecture et protocole Radius
- Se protéger aux attaques

5 / Outils de détection d'une intrusion

- Principes et méthodes de détection
- Panorama des solutions du marché
- Nmap
- Les IDS
- Avantages et limites

6 / Vérification de l'intégrité d'un système

- Principes
- Outils disponibles
- Tripwire ou AIDE
- Audit des vulnérabilités : Principes et méthodes
- Présentation des outils d'audit
- Politique de sécurité

7 / Gestion des événements de sécurité

- Traitement des informations
- La consolidation et la corrélation
- Security Information Management (SIM) : présentation
- Solution de sécurité de SNMP

8 / La sécurité des réseaux WiFi

- Rappels sur les technologies WiFi

- Menaces et attaques sur les réseaux sans fils
- Les faiblesses intrinsèques des réseaux WiFi
- Les protocoles de sécurité
- Architecture Wi-Fi sécurisée

9 / La sécurité de la téléphonie sur IP

- Concepts VoIP
- L'architecture d'un système VoIP
- Présentation du protocole SIP. Faiblesses
- Les problématiques du NAT
- Menaces et attaques sur la téléphonie sur IP
- Les moyens de protection

10 / La sécurité de la messagerie

- Architecture et fonctionnement
- Présentation des protocoles
- Menaces et attaques sur la messagerie
- Présentation des acteurs de lutte contre le SPAM
- Solutions de lutte contre le SPAM
- Panorama des outils de collecte des emails
- Moyens de protection contre le SPAM

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

20 au 24 Juil. 2026	Présentiel - Casablanca
14 au 18 Sep. 2026	Distanciel
09 au 13 Nov. 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-systems.com
Web : https//www.innov-systems.com