Cybersécurité Réseaux/Internet

DURÉE
4 jours (28h)

RÉFÉRENCE
MSI91

CATÉGORIE
Sécurité Du Réseau

OBJECTIFS DE LA FORMATION

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

- Etre capable d'assurer et superviser la sécurité du système d'Information
- Mettre en œuvre les meilleures techniques pour répondre aux intrusions et aux menaces qui pèsent sur le SI

POUR QUI ?

- Administrateurs
- Architectes
- Développeurs
- DSI
- Responsable sécurité

Programme détaillé

1/ Les principes et concepts fondamentaux de la sécurité informatique

- Vue globale sur la sécurité du Système d'Information
- Défense en profondeur et politique de sécurité
- Principales méthodes et normes pour l'analyse des risques
- Présentation des normes ISO 2700x
- La cybercriminalité : Définition, évolution
- Les nouvelles menaces
- Les failles de sécurité dans les applications
- Cyberattaque (Kill Chain)
- Les failles 0day, 0day Exploit et kit d'exploitation

2/ Sécurité des postes clients

- Comprendre les menaces orientées postes clients
- Les logiciels anti-virus/anti-spyware
- Gestion des correctifs de sécurité sur les postes clients ?
- Ransomware : mesures préventives et correctives
- Comment sécuriser les périphériques amovibles ?
- Les vulnérabilités des navigateurs et des plug-ins
- L'attaque Drive-by download
- Les menaces via les clés USB

3/ Eléments de cryptographie

- Cryptographie : Objectifs et fonctions de base
- Chiffrements symétrique
- Chiffrements asymétriques
- Les algorithmes de hashing

- Certificats et PKIs

4/ Authentification et habilitation des utilisateurs

- L'authentification biométrique et les aspects juridiques
- L'authentification par challenge/response
- Les différentes techniques d’attaque
- L’authentification forte à facteurs multiples (MFA)
- Authentification carte à puce et certificat client X509
- Les standards HOTP et TOTP de l’OATH
- Les standards UAF et U2F de l’alliance FIDO

5/ La sécurité dans le nuage

- Plan d’infrastructure technique pour les centres de données
- DMZ, quartiers techniques, VLANs et appliances next génération
- Plan de Continuité d’Activité (PCA) et Plan de Reprise d’Activité (PRA)
- Etablir une stratégie de la sauvegarde et de l'archivage des données
- Virtualiser serveurs, réseaux et applications
- Les solutions de la sécurité du Cloud : VPC, CASB, VPN…
- Analyse de risque avec la Cloud Control Matrix
- Contrats et certifications d’hébergement

6/ Sécurité du réseau

- Le protocole TCP/IP : Rappels
- Typologie de réseaux : VPN SSL, VPN IPsec, MPLS, VLANs, Wifi…
- Equipements : NAT, Firewall, proxy, UTM…
- Systèmes de détection et de prévention des intrusions
- Méthodes et outils pour l’identification, l’authentification
- Les contrôles d’opérations (SAML, LDAP, AD, Kerberos…)
- Détection des anomalies, stockage et analyse des logs…

- Les protocoles SSL, TLS et HTTPS
- Supervision du réseau : bonnes pratiques

7/ Sécurité Wi-Fi

- Les technologies WiFi : Rappels
- Le WiFi et ses vulnérabilités
- Détecter les Rogue AP
- Mécanismes de sécurité des bornes
- Description des risques
- IEEE 802.11i
- Attaque KRACK sur WPA et WPA2
- Les apports de WPA3
- Vulnérabilités DragonBlood
- Authentification des utilisateurs et des terminaux
- L’authentification WiFi dans l’entreprise
- Outils d'audit

8/ Sécurité des mobiles

- Présentation des risques et attaques sur la mobilité
- Forces et faiblesses des systèmes iOS et Android
- Virus et codes malveillants
- MDM et EMM pour la gestion de flotte

9/ Sécurité des logiciels et applications

- Application du principe de défense en profondeur
- Différences en matière de sécurité entre une application Web et mobile
- Vue d'ensemble des principaux risques selon l'OWASP
- Vue d'ensemble des attaques XSS, CSRF, SQL injection et session hijacking
- Les bonnes pratiques de développement

- Le pare-feu applicatif ou WAF
- Evaluation du niveau de sécurité d'une application
- Supervision logicielle avec les technologies Big Data

10/ Supervision active de la sécurité

- Audits de la sécurité
- Les tests d’intrusion
- Les plateformes de "bug Bounty"
- Répondre efficacement aux attaques
- Inforensic, pentests et mise en place du SIEM
- Implémenter Security Operation Center (SOC)
- Les technologies du SOC 2.0
- Les labels ANSSI pour l’externalisation
- Les procédures de réponse à incident

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

09 au 12 Juin 2026	Casablanca - Maroc
04 au 07 Août 2026	Casablanca - Maroc
29 Sep. au 02 Oct. 2026	Casablanca - Maroc
24 au 27 Nov. 2026	Casablanca - Maroc

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

Scannez pour accéder à la fiche en ligne