Cycle Sécurité Systèmes et Réseaux

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

DURÉE	RÉFÉRENCE	CATÉGORIE
10 jours (70h)	**RST40**	**Sécurité Du Réseau**

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

Innov Systems

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 / 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

3 / 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

4 / La sécurité des systèmes, le "Hardening"

- Insuffisance des installations par défaut

Innov Systems

- 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

5 / La sécurité des applications

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

6 / 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

7 / Sécurité des échanges

- Sécurité WiFi
- Présentation des risques inhérents aux réseaux sans fil

Innov Systems

- Les limites du WEP, WPA, WPA2
- Panorama des types d'attaques
- Protocole SSL (Secure Sockets Layer)
- Le protocole SSH/SSL
- Protocole TLS (Transport Layer Security)
- Protocole HTTPS (HyperText Transfer Protocol Secure)
- Les VPNs site à site et nomade

8 / 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

9 / Outils de détection d'une intrusion

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

10 / Vérification de l'intégrité d'un système

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

Innov Systems

- Politique de sécurité

11 / Gestion des événements de sécurité

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

12 / 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

13 / 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

14 / 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

Inov Systems

- 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

15 au 26 Fév. 2027	Présentiel - Casablanca
12 au 23 Avr. 2027	Présentiel - Casablanca
07 au 18 Juin 2027	Présentiel - Casablanca
02 au 13 Août 2027	Présentiel - Casablanca
27 Sep. au 08 Oct. 2027	Présentiel - Casablanca

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

Innov Systems

Innov Systems — Tous droits réservés