Forensics réseau : maîtrisez l’investigation et l’analyse des incidents cybersécurité

Lien : https://innov-systems.com/formation/forensics-reseau-maitrisez-linvestigation-et-lanalyse-des-incidents-cybersecurite

DURÉE
5 jours (35h)

RÉFÉRENCE
SI17

CATÉGORIE
Analyse Apres Incident : Analyse Forensique, Investigation Numérique et Plan de Continuité

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes du forensic réseau
- Savoir collecter et analyser le trafic réseau
- Maîtriser les outils d’analyse de paquets et de logs
- Identifier les comportements réseau suspects
- Reconstituer des incidents de cybersécurité
- Analyser les attaques réseau courantes
- Mettre en œuvre une méthodologie d’investigation numérique
- Réagir efficacement aux incidents de sécurité
- Exploiter les données réseau pour l’analyse forensique
- Développer une expertise en investigation cybersécurité

POUR QUI ?

- Analystes SOC
- Experts en cybersécurité
- Administrateurs réseaux
- Ingénieurs sécurité IT
- Pentesters et forensic analysts
- Responsables sécurité des systèmes d’information (RSSI)
- Toute personne impliquée dans la détection et l’analyse d’incidents réseau

Innov Systems

Programme détaillé

1 / Introduction au forensic réseau

- Définition de la forensic et de l’investigation réseau
- Rôle dans la cybersécurité et la réponse aux incidents
- Types d’incidents analysés

2 / Fondamentaux des réseaux informatiques

- Modèle OSI et TCP/IP
- Protocoles réseau essentiels
- Flux de communication et architecture réseau

3 / Collecte des données réseau

- Capture de paquets (Packet capture)
- Sources de logs réseau
- Outils de collecte et d’analyse

4 / Analyse du trafic réseau

- Analyse des flux (NetFlow, IPFIX)
- Identification des comportements suspects
- Détection des anomalies réseau

5 / Outils de forensic réseau

- Wireshark et analyse de paquets
- Tcpdump et outils en ligne de commande
- Solutions SIEM et monitoring

Innov Systems

6 / Analyse des attaques réseau

- Détection des intrusions (IDS/IPS)
- Attaques DDoS et scan réseau
- Analyse des malwares en réseau

7 / Investigation des incidents de sécurité

- Méthodologie d’enquête numérique
- Reconstitution des événements
- Identification des sources d’attaque

8 / Corrélation et analyse des logs

- Centralisation des journaux
- Corrélation multi-sources
- Chronologie des événements

9 / Réponse aux incidents réseau

- Gestion des incidents de sécurité
- Containment et remédiation
- Documentation et reporting

10 / Études de cas et exercices pratiques

- Analyse de scénarios réels
- Investigation complète d’un incident
- Bonnes pratiques de forensic réseau

Innov Systems

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

01 au 05 Fév. 2027	Présentiel - Casablanca
29 Mars au 02 Avr. 2027	Présentiel - Casablanca
24 au 28 Mai 2027	Présentiel - Casablanca
19 au 23 Juil. 2027	Présentiel - Casablanca
13 au 17 Sep. 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 — Tous droits réservés