Cybercriminalité et Cyberguerre : enjeux et défis

Lien : https://innov-maroc.com/formation/cybercriminalite-et-cyberguerre-enjeux-et-defis

DURÉE
3 jours (21h)

RÉFÉRENCE
SEC10

CATÉGORIE
Fondamentaux Sécurité Informatique

OBJECTIFS DE LA FORMATION

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

- Prendre connaissance des risques et identifier les sources de menaces
- Etre capable de préparer, de détecter, d'anticiper et de gérer les cybercrises
- Acquérir les bonnes pratiques pour maîtriser la sécurité d'un SI

POUR QUI ?

- RSSI
- Professionnels IT
- DSI

Programme détaillé

1 / Introduction à la cybercriminalité

- L'évolution de la cybercriminalité. Son impact
- Les types d'attaquants (White hat...)
- Qu'est-ce que le hacking ?
- Les principaux groupes de hackers
- Les types d'attaques (Malware, MITM, SE...)
- Les différentes phases d'une attaque (Cyber Kill Chain)
- Sophistication des techniques d'attaques
- La 5G et L'IoT : ses enjeux en cybersécurité
- Les différentes lois et référentiels

2 / Les attaques

- Les attaques contre les individus
- Les acteurs contre les acteurs économiques
- Les attaques contre les infrastructures critiques (OIV)
- Les attaques contre la collectivité

3 / Comprendre les cyberattaques

- Les principales vulnérabilités et attaques sur les ordinateurs (PC et Mac), tablettes et smartphones
- Les programmes de type « Bug Bounty »
- Les Botnets

- Les vulnérabilités de la domotique : caméras de surveillance, alarmes, TV, serrures connectées...
- Les objets connectés : les risques
- Les vulnérabilités et attaques sur les réseaux domestiques
- Les attaques basées sur le « Social Engineering » : Spear Phishing, Watering Hole, réseaux sociaux...
- Les attaques avancées de type APT (Advanced Persistent Threat)
- Les attaques techniques
- Les logiciels malveillants

4 / Détection des intrusions

- Gestion des traces, preuves, enregistrements
- Gestion des logs : une mine d'or pour les organismes
- Détection d'une activité anormale. Processus de gestion des incidents
- Analyse et corrélation d'évènements de sécurité
- Pertinence du SOC (Security Operation Center)
- Automatisation de la gestion des incidents
- Les plans de continuité d'activité
- Tests d'intrusion, mesure d'anticipation incontournable
- Les exercices Red, Blue et Purple Teaming
- Recourir à une société spécialisée de détection des incidents
- Le modèle Security as a Service

5 / Organisation de la riposte

- La notion de preuve dans le monde informatique
- Recherche et collecte de preuves
- Méthodologie de gestion d'incidents
- Les CERT (Computer Emergency Response Team) : Rôle
- Le cadre juridique des ripostes à une cyberattaque
- Organisation et gestion d'une cellule de crise
- Importance de la veille en cybersécurité

- Gestion des vulnérabilités et patch management

6 / Recommandations pour maîtriser la sécurité d'un SI

- Politique de gestion des vulnérabilités, traitement
- Modèle de sécurité en "château-fort"
- Prestataires certifiés obligatoires (PDIS, PRIS)
- Audit de sécurité
- Auditeurs certifiés

7 / Protéger le citoyen internaute face aux cybercriminels

- Protéger sa vie privée sur Internet et lutter contre la cybersurveillance
- Eviter les attaques par ingénierie sociale
- Assurer la sécurité de l’ordinateur. Pourquoi l’antivirus n’est-il plus suffisant ?
- Effectuer des transactions financières (achats, ventes, virements…) sur Internet en toute sécurité
- Détecter une opération de Phishing et vérifier la sécurité d’une connexion https
- Utiliser un mot de passe robuste et différent pour chaque service en ligne

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 17 Juil. 2026	Présentiel - Casablanca
09 au 11 Sep. 2026	Distanciel
11 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-maroc.com
Web : https//www.innov-maroc.com