Cycle Cybercriminalité

Lien : https://innov-systems.com/formation/cycle-cybercriminalite

DURÉE
10 jours (70h)

RÉFÉRENCE
SEC326

CATÉGORIE
Fondamentaux Sécurité Informatique

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les différentes formes de cybercriminalité et leurs mécanismes
- Maîtriser les bases juridiques encadrant la cybersécurité
- Apprendre à identifier et prévenir les cyberattaques
- Développer les compétences en sécurité des systèmes et des réseaux
- Renforcer la capacité d’analyse et d’enquête numérique
- Sensibiliser aux enjeux de protection des données personnelles
- Appliquer les principes de cryptographie dans un contexte professionnel
- Acquérir une approche méthodique de la gestion des incidents
- Intégrer une gouvernance efficace de la cybersécurité dans son organisation
- Former les équipes et utilisateurs à adopter des comportements sûrs
- Évaluer les risques et mettre en place des stratégies de mitigation
- Distinguer les différents types de menaces (cybercrime, cyberespionnage, etc.)
- Se préparer à la conformité réglementaire en matière de cybersécurité
- Comprendre les enjeux géopolitiques de la cybersécurité
- Mettre en place une veille stratégique sur les menaces émergentes

POUR QUI ?

- Responsables des systèmes d’information (RSI / DSI)
- Responsables de la sécurité informatique (RSSI)
- Agents des forces de l’ordre et magistrats
- Juristes spécialisés en droit du numérique
- Responsables conformité et protection des données
- Responsables métiers (RH, Finance, etc.) impliqués dans la sécurité
- Membres des équipes de gestion des risques
- Responsables d’infrastructures critiques (transport, énergie, santé)

Innov Systems

Programme détaillé

1 / Introduction à la cybercriminalité

- Définition et typologies de la cybercriminalité
- Acteurs principaux : hackers, groupes organisés, insiders
- Tendances actuelles et menaces émergentes

2 / Cadres juridiques nationaux et internationaux

- Lois marocaines et africaines sur la cybercriminalité
- Conventions internationales (Budapest, Malabo, etc.)
- Coopération judiciaire et entraide entre États

3 / Cyberattaques : classification et fonctionnement

- Attaques par phishing, ransomware, DDoS, etc.
- Exemples de cyberattaques réelles
- Analyse des vecteurs d'attaque

4 / Sécurité des systèmes d'information

- Notions de sécurité logique, physique et organisationnelle
- Outils et techniques de sécurisation des SI
- Politique de sécurité et plan de continuité

5 / Investigation numérique et forensic

- Principes et cadre légal de l'investigation numérique
- Méthodologies d'analyse forensique
- Collecte, conservation et analyse de la preuve numérique

Innov Systems

6 / Protection des données personnelles

- Notions de RGPD et lois locales
- Mesures de conformité et d’audit
- Responsabilités des acteurs publics et privés

7 / Ingénierie sociale et manipulation psychologique

- Techniques de manipulation et hameçonnage
- Détection et prévention des arnaques sociales
- Études de cas et scénarios simulés

8 / Sécurité des réseaux et protocoles

- Failles des protocoles TCP/IP, DNS, etc.
- Analyse de paquets et détection d’intrusion
- Mise en place de pare-feux et VPN

9 / Cryptographie et protection de l’information

- Principes de la cryptographie : symétrique, asymétrique
- Signature électronique et certificats
- Applications concrètes : emails, communications, documents

10 / Cyberespionnage, cyberterrorisme et cyberguerre

- Différences conceptuelles entre les trois
- Acteurs étatiques et non-étatiques
- Menaces pour la souveraineté nationale

11 / Sécurité des applications et développement sécurisé

- Failles courantes : XSS, SQLi, CSRF
- Méthodes de test d’intrusion (pentest)

Inov Systems

- Bonnes pratiques de codage sécurisé

12 / Usurpation d’identité numérique

- Techniques et outils utilisés par les cybercriminels
- Impacts sur les victimes : réputation, finances
- Moyens de prévention et recours juridiques

13 / Gestion des incidents de sécurité

- Détection, réponse et communication de crise
- Rédaction d’un plan de réponse aux incidents
- Outils de monitoring et de gestion centralisée

14 / Gouvernance de la cybersécurité

- Rôles et responsabilités des parties prenantes
- Mise en œuvre d’un système de management de la sécurité
- Évaluation des risques et audits réguliers

15 / Stratégies de sensibilisation et formation continue

- Campagnes de sensibilisation des utilisateurs
- Intégration dans les programmes de formation RH
- Évaluation de la maturité en cybersécurité
- Responsables des systèmes d’information (RSI / DSI)
- Responsables de la sécurité informatique (RSSI)
- Agents des forces de l’ordre et magistrats
- Juristes spécialisés en droit du numérique
- Responsables conformité et protection des données
- Responsables métiers (RH, Finance, etc.) impliqués dans la sécurité
- Membres des équipes de gestion des risques
- Responsables d’infrastructures critiques (transport, énergie, santé)

Inov 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

18 au 29 Jan. 2027	Présentiel - Casablanca
15 au 26 Mars 2027	Présentiel - Casablanca
10 au 21 Mai 2027	Présentiel - Casablanca
05 au 16 Juil. 2027	Présentiel - Casablanca
30 Août au 10 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