



Cybersécurité avancée : analysez, détectez et neutralisez les codes malveillants

Lien :

<https://innov-systems.com/formation/cybersecurite-avancee-analysez-detectez-et-neutralisez-les-codes-malveillants>

 DURÉE
5 jours (35h)

 RÉFÉRENCE
SI11

 CATÉGORIE
**Sécurité Technique :
Cryptographie,
Protocoles et
Infrastructures**

OBJECTIFS DE LA FORMATION

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

- ✓ Comprendre les différentes menaces informatiques
- ✓ Identifier les types de codes malveillants
- ✓ Analyser le fonctionnement des malwares
- ✓ Maîtriser les techniques d'analyse statique et dynamique
- ✓ Mettre en place des solutions de détection et de prévention
- ✓ Réagir efficacement face à une attaque informatique
- ✓ Sécuriser les systèmes d'information
- ✓ Développer une culture de cybersécurité

POUR QUI ?

- ✓ Administrateurs systèmes et réseaux
- ✓ Analystes en cybersécurité
- ✓ Responsables IT
- ✓ Ingénieurs sécurité informatique
- ✓ Techniciens informatiques
- ✓ Toute personne impliquée dans la sécurité des systèmes d'information

Innov Systems



Programme détaillé

1 / Introduction à la cybersécurité et aux menaces informatiques

- Panorama des cybermenaces actuelles
- Enjeux pour les entreprises et institutions
- Typologie des attaques

2 / Typologie des codes malveillants

- Virus, vers (worms) et chevaux de Troie
- Ransomware, spyware et rootkits
- Botnets et malwares avancés

3 / Modes d'infection et vecteurs d'attaque

- Phishing et ingénierie sociale
- Exploitation des vulnérabilités
- Téléchargements malveillants et supports externes

4 / Fonctionnement des malwares

- Cycle de vie d'un malware
- Techniques d'obfuscation
- Mécanismes de propagation

5 / Analyse statique des codes malveillants

- Étude du code sans exécution
- Identification des signatures
- Outils d'analyse (sandbox, antivirus)

6 / Analyse dynamique des malwares

- Exécution en environnement contrôlé
- Observation des comportements
- Détection des actions malveillantes

7 / Détection et prévention des attaques

- Antivirus, EDR et SIEM
- Systèmes de détection d'intrusion (IDS/IPS)
- Mise en place de politiques de sécurité

8 / Réponse aux incidents et remédiation

- Gestion des incidents de sécurité
- Isolation et suppression des menaces
- Plan de reprise d'activité (PRA)

9 / Bonnes pratiques de cybersécurité

- Sensibilisation des utilisateurs
- Gestion des mises à jour et correctifs
- Sécurisation des accès et des données

10 / Veille et évolution des menaces

- Cybercriminalité et tendances
- Zero-day et attaques avancées
- Importance de la veille en cybersécurité

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

 26 au 30 Oct. 2026

 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>

Document généré le 12/10/2026 — Réf : SI11
Innov Systems — Tous droits réservés