Simulation d'attaques (Red Team Operations) : planification, exécution et reporting

Lien : https://innov-systems.com/formation/simulation-dattaques-red-team-operations-planification-execution-et-reporting

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SI115**	**Ethical Hacking**

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes des opérations Red Team
- Planifier et structurer une simulation d’attaque réaliste
- Identifier les failles de sécurité organisationnelles et techniques
- Évaluer la résilience des systèmes d’information
- Améliorer la détection et la réponse des équipes Blue Team
- Utiliser des frameworks comme MITRE ATT&CK
- Rédiger des rapports d’audit et de vulnérabilités exploitables
- Renforcer la posture de cybersécurité globale
- Simuler des scénarios d’attaque avancés en environnement contrôlé
- Développer une culture de sécurité proactive
- Prioriser les remédiations de sécurité
- Étudier des cas concrets de simulations Red Team

POUR QUI ?

- Pentesters
- Red Team operators
- SOC analysts
- Blue Team engineers
- Cybersecurity engineers
- RSSI / CISO
- Consultants cybersécurité
- Auditeurs sécurité
- Threat hunters
- Security architects
- DevSecOps engineers
- Toute personne impliquée dans la simulation d’attaques et l’amélioration de la posture de cybersécurité

Innov Systems

Programme détaillé

1 / Introduction aux Red Team Operations

- Définition et objectifs des opérations Red Team
- Différence entre Red Team, Blue Team et Purple Team
- Place des simulations d’attaques dans la cybersécurité moderne

2 / Cadre légal et éthique des tests d’intrusion

- Autorisations et règles de conduite (Rules of Engagement)
- Limites légales et responsabilités
- Confidentialité et gestion des données sensibles

3 / Planification d’une opération Red Team

- Définition des objectifs et du périmètre
- Choix des scénarios d’attaque réalistes
- Modélisation des adversaires (Threat Modeling)

4 / Reconnaissance et collecte d’informations (OSINT)

- Techniques de collecte de données publiques
- Analyse de la surface d’attaque organisationnelle
- Identification des vecteurs d’entrée potentiels

5 / Simulation des techniques d’attaque

- Phishing, spear phishing et ingénierie sociale
- Exploitation de vulnérabilités techniques
- Mouvement latéral et élévation de privilèges (conceptuel)

Innov Systems

6 / Outils et frameworks Red Team

- MITRE ATT&CK framework
- Outils de simulation et de test d’intrusion
- Automatisation des scénarios d’attaque

7 / Évasion et furtivité des attaques simulées

- Techniques de contournement des contrôles de sécurité
- Simulation de comportements adverses avancés
- Gestion des traces et logs (dans un cadre contrôlé)

8 / Coordination avec les équipes Blue Team

- Exercices de détection et réponse en temps réel
- Analyse des réactions de défense
- Amélioration continue de la posture de sécurité

9 / Reporting et restitution des résultats

- Documentation des vulnérabilités découvertes
- Cartographie des risques et impacts potentiels
- Recommandations de remédiation

10 / Amélioration de la posture de sécurité

- Plans de correction et priorisation des failles
- Mesure de la maturité cybersécurité
- Intégration des retours dans la stratégie sécurité

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

25 au 29 Jan. 2027	Présentiel - Casablanca
22 au 26 Mars 2027	Présentiel - Casablanca
17 au 21 Mai 2027	Présentiel - Casablanca
12 au 16 Juil. 2027	Présentiel - Casablanca
06 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