Red Team Testing pour applications simuler des attaques réalistes sur vos systèmes

Lien : https://innov-systems.com/formation/red-team-testing-pour-applications-simuler-des-attaques-realistes-sur-vos-systemes

DURÉE
5 jours (35h)

RÉFÉRENCE
TLA27

CATÉGORIE
Tests de Sécurité Applicative

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes et les méthodologies du Red Team Testing
- Planifier et conduire des simulations d’attaques réalistes sur des applications
- Identifier les vulnérabilités des applications Web, API et architectures Cloud
- Évaluer la robustesse des mécanismes d’authentification, d’autorisation et de gestion des identités
- Mesurer les capacités de détection et de réponse des équipes de sécurité
- Tester la résilience des environnements DevSecOps et Cloud
- Documenter les vulnérabilités et proposer des actions de remédiation efficaces
- Intégrer les exercices Red Team dans une démarche d’amélioration continue
- Renforcer lsa collaboration entre les équipes Red Team, Blue Team et Purple Team
- Améliorer la posture globale de cybersécurité des applications et des systèmes
- Évaluer les risques techniques et organisationnels liés aux cyberattaques
- Réaliser un exercice complet de Red Team Testing conforme aux bonnes pratiques du secteur

POUR QUI ?

- Pentesters
- Red Teamers
- Blue Teamers
- Purple Teamers
- Analystes SOC
- Ingénieurs cybersécurité
- DevSecOps Engineers
- Security Engineers
- Architectes sécurité
- Développeurs d’applications
- Responsables de la sécurité des systèmes d’information (RSSI/CISO)
- Toute personne impliquée dans les tests de sécurité offensive, l’évaluation de la résilience et la protection des applications

Innov Systems

Programme détaillé

1 / Introduction au Red Team Testing

- Principes du Red Teaming et différences avec les tests d'intrusion
- Objectifs, méthodologie et règles d'engagement (Rules of Engagement)
- Référentiels MITRE ATT&CK, OWASP et Cyber Kill Chain

2 / Reconnaissance et collecte d'informations

- OSINT et cartographie de la surface d'attaque
- Découverte des actifs, services et applications exposés
- Identification des technologies, dépendances et vulnérabilités potentielles

3 / Simulation d'attaques sur les applications

- Exploitation des vulnérabilités Web (OWASP Top 10)
- Attaques sur les API REST, GraphQL et gRPC
- Tests sur les applications Cloud, mobiles et microservices

4 / Escalade de privilèges et mouvements latéraux

- Exploitation des faiblesses d'authentification et d'autorisation
- Déplacement latéral dans les environnements applicatifs
- Simulation de compromission de comptes à privilèges

5 / Attaques sur les identités et les accès

- Tests des mécanismes MFA, SSO et IAM
- Simulation de phishing ciblé et d'ingénierie sociale
- Validation de la gestion des sessions et des secrets

Innov Systems

6 / Détection, réponse et collaboration Blue Team

- Mesure des capacités de détection du SOC
- Évaluation des mécanismes EDR, SIEM et XDR
- Analyse des délais de détection et de réponse (MTTD, MTTR)

7 / Sécurité des environnements Cloud et DevSecOps

- Tests des configurations Cloud et conteneurs
- Validation des pipelines CI/CD et de la Supply Chain logicielle
- Simulation d’attaques sur Kubernetes et les plateformes Cloud

8 / Documentation, remédiation et gestion des risques

- Qualification des vulnérabilités selon leur criticité
- Élaboration des rapports techniques et exécutifs
- Recommandations de remédiation et plans d’amélioration

9 / Automatisation et amélioration continue

- Intégration des exercices Red Team dans DevSecOps
- Automatisation des contrôles et validation continue
- Mesure de la maturité de la sécurité applicative

10 / Cas pratiques et exercice Red Team complet

- Préparation et exécution d’une campagne Red Team
- Coordination avec les équipes Blue Team et Purple Team
- Retour d’expérience (Lessons Learned) et amélioration de la posture de 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

12 au 18 Jan. 2027	Présentiel - Casablanca
08 au 12 Mars 2027	Présentiel - Casablanca
03 au 07 Mai 2027	Présentiel - Casablanca
28 Juin au 02 Juil. 2027	Présentiel - Casablanca
23 au 27 Août 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