Ref. SEC-REDTEAM

Opérations Red Team et émulation d'adversaires

3 jours (21 heures) | Expertise | Présentiel ou classe à distance

à partir de
2 625 € HT par personne (TVA en vigueur)

Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 06/10/2026.

Objectifs

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

- Construire un Adversary Emulation Plan aligné sur MITRE ATT&CK ICS / Enterprise
- Déployer et orchestrer une infrastructure d'attaque automatisée (Caldera) et modulaire
- Simuler les phases clés d'une cyber-attaque (reconnaissance, accès initial, post-exploitation, déplacement latéral)
- Exploiter des techniques avancées sur Active Directory et Cloud (Kerberoasting, Golden Ticket, Azure AD)
- Etablir des métriques de détection (IoCs) et rédiger un rapport opérationnel de recommandations.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Opérateurs Red Team et pentesters, consultants en Threat Intelligence, membres d'équipes IR / SOC souhaitant comprendre les scénarios attaquants, ingénieurs DevSecOps intégrants des tests d'intrusion automatisés.

Prérequis

Avoir une expérience de base en tests d'intrusion, une familiarité avec un shell Linux / Windows et un framework C2 (Metasploit, Covenant) ainsi qu'une connaissance des concepts MITRE ATT&CK.

Programme

1 Pendant votre formation

Opérations Red Team et émulation d'adversaires

Jour 1 - Matin

Planification et accès initial automatisé

- Présentation de l'émulation d'adversaires et du processus Red Team
- Elaboration d'un Adversary Emulation Plan (scénarios, objectifs, TTPs MITRE)

Exemple de travaux pratiques (à titre indicatif)

- *Définition et priorisation des scénarios d'attaque*

Jour 1 - Après-midi

Planification et accès initial automatisé - Suite

- Installation et configuration de Caldera (plugins, sandboxes)
- Exécution automatisée de modules reconnaissance (Network Discovery, Credential Access)

Exemple de travaux pratiques (à titre indicatif)

- *Création et test d'un plugin Caldera personnalisé*

Jour 2 – Matin

Post-exploitation et déplacement latéral

- Maintien de l'accès :
  - Payloads furtifs
  - Tunnels chiffrés
  - Persistence scripts
- Utilisation de Atomic Red Team pour tests ciblés (Evasion, Credential Access)

Exemple de travaux pratiques (à titre indicatif)

- *Génération d'exemples adversariaux et validation des détections SOC*

Jour 2 - Après-midi

Post-exploitation et déplacement latéral - Suite

- Déplacement latéral sur Windows et Linux :
  - Pass-the-Hash / Ticket
  - SSH pivot
  - Impacket
- Attaques avancées sur Active Directory et Azure AD (Kerberoasting, Golden Ticket)

Exemple de travaux pratiques (à titre indicatif)

- Chaining de modules Caldera pour un scénario latéral "on-prem / Cloud"

Jour 3 - Matin

Objectifs finaux et reporting opérationnel

- Actions sur objectifs :
  - Exfiltration de données sensibles
  - Déni de service ciblé
- Automatisation de l'exfiltration et camouflage des traces

Exemple de travaux pratiques (à titre indicatif)

- *Orchestration Caldera d'un scénario complet*

Jour 3 - Après-midi

Objectifs finaux et reporting opérationnel - Suite

- Analyse des logs et collecte des IoCs générés
- Rédaction du rapport d'émulation :
  - Méthodologie
  - Findings
  - Recommandations opérationnelles
- Présentation synthétique du plan et des metrics de succès (TTP couverts, IoCs détectés)

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.
Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

Nous contacter pour en savoir plus →

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 7 octobre 2026 au 9 octobre 2026 (3 jours / 21 heures)

Lyon

Du 7 octobre 2026 au 9 octobre 2026 Lyon

- 7 octobre 2026 ---------- 9h00 - 16h00
- 8 octobre 2026 ---------- 9h00 - 16h00
- 9 octobre 2026 ---------- 9h00 - 16h00