Date de publication : 21/05/2025

Formation : Cybersécurité, la simulation d'adversaires (Adversary Emulation)

émulation l'adversaire pour simuler des attaques avancées

Formation pratique - 2j - 14h00 - Réf. RTA

Prix : 1630 CHF H.T.

NEW

L'émulation de l'adversaire est une méthode d'évaluation de la cybersécurité qui reproduit les tactiques, techniques et procédures (TTP) des acteurs de la menace du monde réel afin d'évaluer et d'améliorer les défenses de sécurité d'une organisation. Cette formation vous permettra de simuler des attaques réelles, comprendre les techniques adverses, et tester vos capacités de détection et de réponse dans un environnement contrôlé.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Comprendre l'intérêt stratégique de l'adversary emulation
- Utiliser Atomic Red Team dans une démarche MITRE ATT&CK
- Déployer un scénario réaliste avec Caldera et/ou Atomic Red Team
- Interpréter les résultats, détecter et renforcer la posture défensive

Public concerné

Analystes SOC, blue teamers, pentesters, red teamers, responsables sécurité, administrateurs sécurité.

Prérequis

Bonnes connaissances en sécurité SI, réseaux, systèmes.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

PARTICIPANTS

Analystes SOC, blue teamers, pentesters, red teamers, responsables sécurité, administrateurs sécurité.

PRÉREQUIS

Bonnes connaissances en sécurité SI, réseaux, systèmes.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

1 Adversary Emulation 101

- Définitions et concepts clés.
- Émulation, simulation et pentest : comparatif et pourquoi émuler ?
- Posture défensive proactive, alignement avec les vraies menaces.

2 Découverte de MITRE ATT&CK

- Présentation des matrices MITRE ATT&CK et D3FEND.
- Les outils d'émulation de tactiques, techniques et procédures (TTP).

Travaux pratiques
Identifier les TTP d'un groupe APT.

3 Atomic Red Team

- Présentation d'Atomic Red Team, Atomic CLI, Invoke-Atomic.
- Comment utiliser un test, l'adapter, et en créer un.

Travaux pratiques
Test de TTP simples (ex : exfiltration, persistence, reconnaissance).

4 Création d'une mini-campagne d'attaque émulée avec Atomic Red Team

- Construire une mini-campagne d'attaque.
- Lancer les tests avec Atomic CLI ou Invoke-Atomic.
- Observation des logs et impacts sur la machine cible.

Travaux pratiques
Construction d'une campagne d'attaque et observation des traces et impacts sur la machine cible.

5 Détection et corrélation des TTP d'Atomic Red Team

- Quels logs, quelles règles Sigma, YARA, ou détections EDR ?
- Mise en œuvre d'outils de collecte, de corrélation et d'investigation pour traquer les activités malveillantes.

Travaux pratiques
Détection des TTPs généré par Atomic RedTeam.

6 Caldera

- Plateforme d'émulation d'adversaire : Caldera.
- Présentation et différence avec ART : agents, enchaînements automatiques.
- Démonstration et mise en place d'un scénario automatisé.

Travaux pratiques
Mise en place des agents et exécution d'un scénario Caldera.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

7 IA et cybercriminels

- Utilisation de l'IA par les attaquants (scripts polymorphes, GPT dans l'attaque).
- Menaces émergentes (LLM poisoning, AI jailbreak, social engineering 2.0).
- Adaptation de l'adversary emulation face aux menaces augmentées.

8 Purple Team Challenge

- Comment intégrer Atomic Red Team dans un pipeline de sécurité.
- Bonnes pratiques pour enrichir les use cases SOC.
- Ressources, projets communautaires, scénarios prêts à l'emploi.

Travaux pratiques
Simulation offensive/défensive : une équipe attaque, l'autre détecte, revue des résultats, scoring basé sur MITRE.

Dates et lieux

CLASSE À DISTANCE
2026 : 9 juin, 24 sep., 17 déc.