+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 30/04/2024

S'inscrire

Formation Adversary emulation avec MITRE ATT&CK

3 jours (21 heures)

Présentation

Notre formation Adversary emulation avec MITRE ATT&CK vous apprendra à comprendre l'importance de l'émulation d'adversaire pour la sécurité des systèmes d'information. Vous serez donc en mesure de comprendre réellement le scénario d'une cyber attaque et ainsi vous préparer pour y répondre et pour les prévenir.

Notre programme vous permettra de comprendre tous les principes clés liés à la simulation d'adversaires ainsi qu'aux menaces persistantes avancées (APT) et leur impact sur la sécurité. Vous apprendrez aussi l'importance de la visualisation dans la compréhension des attaques

Notre formation vous apprendra à émuler des adversaires au plus proche de la réalité : recherche sur les méthodes des hackeurs et planification des opérations seront au programme afin de créer les scénarios les plus réalistes possibles.

Comme toutes nos formations, celle-ci se déroule sur la dernière version de l'outil : Att&ck V15

Objectifs

- Comprendre l'importance de la simulation d'adversaire
- Simuler efficacement des cyberattaques
- Analyser le résultat des simulations

Public visé

- Ethical Hacker
- Experts en Cybersécurité
- Pentester

Pré-requis

- Expérience en Cybersécurité/pentesting
- Connaissance de base en IT

Programme de notre formation Adversary emulation avec MITRE ATT&CK

INTRODUCTION À L'ÉMULATION D'ADVERSAIRE AVEC MITRE ATT&CK

- Comprendre l'importance de l'émulation d'adversaire pour renforcer la sécurité
- Présentation du framework MITRE ATT&CK
- Distinction entre émulation d'adversaire et simulation de menace
- Vue d'ensemble des menaces persistantes avancées (APT) et de leur impact
- Introduction aux TTPs (Tactics, Techniques, and Procedures)

COMPRÉHENSION DU MODUS OPERANDI DES ADVERSAIRES

- Analyse des frameworks et stratégies utilisés par les adversaires
- Approfondissement des connaissances sur les groupes d'adversaires notoires
- Étude des cas réels d'utilisation des TTPs du framework ATT&CK
- L'importance de la visualisation dans l'analyse des attaques
- Introduction au renseignement sur les menaces cybernétiques (Cyber Threat Intelligence)

PLANIFICATION ET RECHERCHE POUR L'ÉMULATION D'ADVERSAIRE

- Définition des objectifs spécifiques de l'émulation
- Techniques de recherche sur les méthodes opératoires des adversaires
- Planification détaillée des engagements d'émulation d'adversaire
- Sélection des outils et ressources nécessaires pour l'émulation
- Discussion sur l'éthique et la légalité dans les opérations d'émulation

MISE EN ŒUVRE DES TTPs AVEC MITRE ATT&CK

- Construction d'un environnement de test pour l'émulation
- Implémentation pratique des TTPs basée sur des cas d'étude
- Techniques pour simuler les attaques de manière réaliste
- Mesure de l'efficacité des contrôles de sécurité en place
- Retour d'expérience et ajustement des stratégies d'émulation

EXERCICES PRATIQUES D'ÉMULATION D'ADVERSAIRE

- Élaboration d'un plan d'émulation

- Création d'un scénario d'émulation
- Simulation d'une attaque
- Analyse des résultats et identification des lacunes de sécurité
- Techniques pour documenter et rapporter les résultats de l'émulation

STRATÉGIES DÉFENSIVES ET AMÉLIORATION CONTINUE

- Utilisation des résultats d'émulation pour renforcer la posture de sécurité
- Développement de recommandations défensives basées sur les données d'émulation
- Importance de l'intégration de l'émulation dans le cycle de vie de la sécurité
- Planification des mises à jour et de l'évolution du programme d'émulation
- Engagement avec la communauté ATT&CK et partage des connaissances

CONCLUSION ET ÉVALUATION DE LA FORMATION

- Récapitulatif des points clés de la formation
- Évaluation des compétences acquises par des tests pratiques
- Discussion sur les prochaines étapes et les opportunités d'apprentissage

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte

des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.