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

Mis à jour le 11/08/2025

S'inscrire

Formation certification Red Team Ops 2

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

4 jours (28 heures)

Présentation

Red Team Ops 2 (RTO) est un programme avancé de cybersécurité offensive qui vous plonge dans des scénarios réalistes d'adversary emulation, du déploiement d'une infrastructure Command & Control à l'évasion des défenses (EDR, WDAC, ASR) et au développement d'outils sur mesure.

Vous apprendrez à opérer avec une OPSEC rigoureuse, à manipuler les Windows API, à réaliser des injections de processus furtives et à produire des rapports exploitables par les décideurs.

À l'issue, vous serez prêt à conduire une campagne Red Team de bout en bout et à viser la certification RTO II, sur la dernière version stable disponible.

Comme toutes nos formation, celle-ci utilise les derniers outils et techniques de Zero-Point Security.

Objectifs

- Maîtriser les tactiques avancées de cybersécurité offensive
- Déployer et sécuriser une infrastructure C2
- Concevoir et utiliser des outils offensifs personnalisés
- Contourner des défenses modernes (EDR, WDAC, ASR)
- Conduire une simulation alignée sur MITRE ATT&CK
- Se préparer à la certification RTO II

Public visé

- Consultants en cybersécurité offensive
- Analystes Red Team
- Pentesters expérimentés
- Professionnels SOC / Blue Team
- Experts sécurité

Pré?requis

- Pratique préalable du Red Teaming / pentest
- Connaissances opérationnelles Windows & Active Directory

Programme de notre formation certification Red Team Ops 2

Fondations avancées & infrastructure

- Objectifs et périmètre de RTO II ; posture OPSEC avancée
- Rappels ciblés : adversary emulation, MITRE ATT&CK, kill chain
- Panorama des outils : Cobalt Strike, redirecteurs, profils malleables
- Choix d’architecture C2 (on?prem / cloud) et modèles de résilience
- Atelier : mise en place d’une infra C2 de base (listener, profil, redirecteur)

Infrastructure C2 durcie et camouflage réseau

- Configuration d’Apache/Nginx redirectors et certificats TLS
- Camouflage par URI, User?Agent, cookies, hôtes frontaux
- Gestion du trafic (staging/beacon) et rotation des IOCs
- Journalisation minimale et hygiène OPSEC
- Atelier : déployer un redirecteur HTTPS avec règles de filtrage

Windows APIs & développement offensif

- Interop C# / C++ ; appels Windows API, D/Invoke, ordinals
- Modèles d’injection (CreateRemoteThread, APC, MapViewOfFile)
- PPID spoofing, masquage de commande, gestion des handles
- Nettoyage mémoire et réduction de surface de détection
- Atelier : coder un loader simple s’appuyant sur WinAPI

Évasion des défenses

- Fonctionnement des EDR/AV (ETW, hooks user/kernel)
- Offuscation en mémoire, syscalls directs/indirects
- Bypass d’AMSI et durcissement du beacon
- Tests contrôlés et mesure du bruit
- Atelier : évaluer un payload face à un EDR de labo

ASR & WDAC : comprendre et contourner

- Politiques Attack Surface Reduction (ASR) : logique, règles, télémétrie
- Windows Defender Application Control (WDAC) : catalogues, signatures
- Abus de LOLBAS, détournements signés et chargements permissifs
- Scénarios d’évasion responsables et limites éthiques
- Atelier : contourner une politique WDAC en environnement simulé

Processus protégés & durcissements Windows

- Modèle des Protected Processes et implications offensives
- Contrainte code signing, certificats et chaînes de confiance
- Techniques d’accès contrôlé et exécution conditionnelle
- Stratégies de rollback & désengagement propre
- Atelier : analyse guidée d’un cas de processus protégé

Chaîne d’attaque intégrée

- Orchestration bout?en?bout : infra, chargement, pivot, actions
- Gestion des artefacts et log minimalistes
- Adaptation tactique en temps réel
- Préparation d’un playbook d’équipe
- Atelier : exercice fil rouge d’intrusion contrôlée

Adversary emulation & threat intel

- Modéliser un adversaire avec ATT&CK (tactiques/techniques)
- Cartographie des contrôles défensifs et hypothèses
- Renseigner des objectifs, préconditions et sorties attendues
- Mesurer l’impact et la couverture
- Atelier : mapping d’un scénario RTO II sur ATT&CK

Reporting Red Team exécutif & technique

- Structure : résumé exécutif, narration, preuves, recommandations
- Traceabilité : timelines, captures, indicateurs, IOCs
- Qualité rédactionnelle et actionnabilité
- Préparer la soutenance et le debrief multi?parties
- Atelier : rédaction d’un mini?rapport structuré

Préparation certification

- Mise en condition & contraintes de l’épreuve RTO II
- Révision ciblée : C2, injections, évasion, rapport
- Stratégie de gestion du temps et des flags
- Check?list d’avant?examen
- Atelier : simulation type examen

Analyse post?simulation & plan d’ancrage

- Revue des réussites et axes d’amélioration
- Consolidation des acquis techniques
- Plan de progression (labs, lectures, drill)
- Préparer la montée vers des cursus connexes
- Atelier : rétro sur preuves & amélioration continue

Clôture & certification

- Valorisation des compétences & livrables attendus
- Rappels éthiques et conformité
- Projection métier et veille
- Feuille de route post?certification
- Atelier : simulation d’entretien & pitch de mission

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.