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

Mis à jour le 12/08/2025

S'inscrire

Formation Offensive Development Practitioner Certification

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

Offensive Development Practitioner Certification (ODPC) est une formation avancée de développement offensif destinée aux professionnels souhaitant concevoir des outils et payloads sur mesure pour des opérations Red Team réalistes.

Au cours de ce programme, vous apprendrez à manipuler les Windows API, à mettre en œuvre des techniques d'injection furtive et à contourner des défenses modernes comme EDR, AMSI et ETW. Vous verrez également la mise en place de communications C2 chiffrées et discrètes.

La formation couvre l'exploitation mémoire, la persistance avancée, l'exfiltration et l'optimisation de vos outils pour la furtivité et la performance, avec un fort accent sur la pratique en environnement contrôlé.

À l'issue, vous serez capable de développer, tester et documenter des outils offensifs opérationnels et de vous préparer efficacement au passage de la certification ODPC (ateliers quotidiens et examen blanc inclus).

Comme toutes nos formations, celle-ci utilise les dernières ressources à jour de White Knight Labs.

Objectifs

- Concevoir des payloads et loaders sur mesure
- Maîtriser WinAPI, injections et bypass EDR/AMSI/ETW
- Déployer des canaux C2 chiffrés et furtifs
- Automatiser la post-exploitation et l'exfiltration

- Produire un rapport professionnel actionnable
- Se préparer efficacement à la certification ODPC

Public visé

- Développeurs sécurité offensive
- Pentesters expérimentés
- Analystes Red Team
- Professionnels sécurité orientés automatisation

Pré-requis

- Bases en C/C++, C#, Python
- Connaissances en pentest / sécurité offensive
- Maîtrise des environnements Windows et Linux

Programme de notre formation Offensive Development Practitioner Certification

Fondations du développement offensif

- Rôle du développeur offensif, règles d’engagement, périmètre
- Hygiène OPSEC appliquée au code
- Environnements et outillage
- CI local et organisation
- Atelier : préparation de l’environnement

Langages & Windows API

- C/C++, C#, Python, Go
- Appels Windows API, interop
- Gestion mémoire, pointeurs
- I/O, registre, services
- Atelier : utilitaire WinAPI

Payloads & exécutions discrètes

- Exécutables furtifs
- Encodage de shellcode, empaquetage
- Persistance simple
- Signature, trust
- Atelier : payload basique

Injection & évasion

- CreateRemoteThread, APC, hollowing
- PPID spoofing, handles
- Élévation contrôlée
- Nettoyage post-exec
- Atelier : injection

Bypass EDR/AMSI/ETW

- Télémétrie EDR
- Bypass AMSI / ETW
- Anti-sandbox/debug
- Mesure & ajustements
- Atelier : loader chiffré

Canaux C2 & communications

- Canal HTTP/HTTPS
- Chiffrement applicatif
- Profils réseau & OPSEC
- Rotation d’IOCs
- Atelier : beacon minimaliste

Automatisation & exploitation

- Scripts PowerShell / Python
- Modularité, build
- Génération dynamique
- QA offensifs
- Atelier : orchestrateur scripté

Exploitation & hooks

- Buffer overflow
- Hooks et interception d’API
- DLL injection
- Stabilité & perfs
- Atelier : exploitation guidée

Multi-plateforme

- Cross-compil Windows/Linux
- Libs portables
- Packaging & distribution
- Compatibilité/tests
- Atelier : port sur 2 OS

Post-exploitation & furtivité

- Persistance (tâches, services, registre)
- Approches fileless
- Rollback propre
- Journalisation minimale
- Atelier : persistance furtive

Exfiltration & staging

- Canaux discrets
- Chiffrement, fragmentation
- Détournement de protocoles
- Preuves & horodatage
- Atelier : pipeline d’exfiltration

Amélioration & qualité

- Tests en lab
- Optimisations furtivité
- Durcissements
- Bonnes pratiques de release
- Atelier : audit d’outil

Préparation certification

- Format & critères ODPC
- Gestion du temps
- Checklist OPSEC
- Livrables
- Atelier : session blanche

Révision ciblée

- WinAPI, injections, EDR bypass
- C2 & exfiltration
- Pièges & remédiations
- Plan individuel
- Atelier : challenge multi-TTPs

Passage simulé & validation finale

- Conditions type examen
- Objectifs techniques

- Rapport professionnel
- Feedback & plan d’action
- Atelier : examen blanc noté

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.