+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 Advanced Red Team Operations Certification

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

Advanced Red Team Operations Certification (ARTOC) est une formation avancée qui marie Red Teaming et pratiques DevOps, vous y intégrez des tactiques offensives aux pipelines CI/CD et aux infrastructures automatisées.

Vous apprendrez à déployer des infrastructures C2 furtives, à développer des outils offensifs, à contourner EDR/ASR/WDAC et à exploiter des chaînes CI/CD, y compris sur Kubernetes et OpenShift.

À l'issue, vous saurez conduire des opérations Red Team complexes et préparer l'examen ARTOC.

Comme toutes nos formations, celle-ci utilise la dernière version à jour pour ARTOC de White Knight Labs.

Objectifs

- Maîtriser le Red Teaming dans un contexte DevOps
- Automatiser des infrastructures C2 sécurisées
- Intégrer des outils offensifs aux pipelines CI/CD
- Contourner des défenses modernes (EDR, ASR, WDAC)
- Simuler des adversaires alignés MITRE ATT&CK
- Se préparer efficacement à la certification ARTOC

Public visé

- Ingénieurs DevOps
- Pentesters expérimentés
- Professionnels sécurité CI/CD
- Architectes systèmes

Pré?requis

- Connaissances solides en DevOps
- Expérience en sécurité offensive / pentest
- Maîtrise des environnements Linux et Windows
- Familiarité avec les outils C2

Programme de notre formation Advanced Red Team Operations Certification

Fondations avancées & cadre opérationnel

- Objectifs de l’ARTOC et livrables attendus
- Rôles Red Team dans un contexte DevOps
- Règles d’engagement, éthique et périmètre
- Organisation d’une mission et gestion des risques
- Atelier : cadrer une mission Red Team intégrée au CI/CD

Infrastructure offensive dans un contexte CI/CD

- Déployer une infra C2 hautement disponible
- Intégration Cloud & pipelines CI/CD
- Déploiements via Infrastructure as Code
- Résilience et rotation des IOCs
- Atelier : C2 automatisé avec Terraform

OPSEC & camouflage réseau

- Bonnes pratiques OPSEC pour DevOps offensif
- Reverse proxies & redirecteurs
- Profilage C2 (URIs, User?Agent, cookies)
- Réduction de la télémétrie et du bruit
- Atelier : redirecteur furtif en environnement cloud

Techniques offensives avancées

- Scripts offensifs intégrés aux workflows
- Langages : Python, Go, C#
- Gestion des secrets & code signing

- Tests & QA sur outils offensifs
- Atelier : outil offensif branché sur un pipeline CI

Contournement des défenses

- Évasion EDR, ASR et WDAC
- Injections & exécutions furtives
- Abus de LOLBAS et binaires signés
- Mesurer l’empreinte et adapter les TTPs
- Atelier : évaluer un payload face à un EDR de labo

Exploitation & escalade dans la chaîne CI/CD

- Cibles et points d’attaque du pipeline
- Registres de conteneurs & dépendances
- Secrets exposés, rôles et permissions
- Attaques orchestrateurs Kubernetes / OpenShift
- Atelier : exploitation d’une faille CI/CD simulée

Post?exploitation & pivoting

- Scripts de maintien d’accès furtifs
- Persistance sur environnements éphémères
- Gestion multi?env. (DEV/QA/PROD)
- Nettoyage & désengagement propre
- Atelier : persistance multi?stage

Pivoting inter?environnements

- Cartographier les passerelles & trusts
- Mouvement latéral via API & orchestrateurs
- Tunnels chiffrés & jump hosts
- Détection/évasion durant le pivot
- Atelier : pivot automatisé Dev ? Prod

Exfiltration furtive & data staging

- Canaux légitimes & encapsulation
- Chiffrement, encodage, fragmentation
- Opsec d’exfiltration et timings
- Validation & preuve des objectifs
- Atelier : pipeline d’exfiltration simulé

Emulation d’adversaire & rapport

- Threat intel & ciblage TTPs
- Alignement MITRE ATT&CK
- Mesurer l’efficacité défensive
- Itérations & adaptation des scénarios
- Atelier : scénario ATT&CK complet

Reporting Red Team pour DevSecOps

- Structure : exécutif + technique
- Preuves actionnables pour DevSecOps
- Traçabilité : timelines, IOCs
- Communication multi?parties prenantes
- Atelier : mini?rapport ARTOC

Debriefing & recommandations

- Analyse des résultats & écarts
- Évaluation de maturité DevSecOps
- Plan d’amélioration continue
- Roadmap post?mission
- Atelier : restitution orale simulée

Préparation à la certification ARTOC

- Format d’examen et critères de succès
- Gestion du temps & priorisation
- Check?list de révision
- Pièges classiques & remédiations
- Atelier : session blanche ARTOC

Révision technique complète

- Récap outils & techniques clés
- Revue OPSEC et profils C2
- Orchestrateurs & CI/CD
- Évasion EDR/ASR/WDAC
- Atelier : résolution d’un scénario multi?TTPs

Passage simulé & validation finale

- Mise en condition type examen
- Validation des livrables
- Feedback personnalisé
- Plan d’action jusqu’au jour J
- 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.