Updated on 11/08/2025

Sign up

Advanced Red Team Operations Certification

ALL-IN-ONE: EXAM INCLUDED IN PRICE

5 days (35 hours)

Overview

Advanced Red Team Operations Certification (ARTOC) is an advanced training program that combines Red Teaming and DevOps practices, integrating offensive tactics with CI/CD pipelines and automated infrastructures.

You'll learn how to deploy stealth C2 infrastructures, develop offensive tools, bypass EDR/ASR/WDAC and leverage CI/CD chains, including on Kubernetes and OpenShift.

At the end of the course, you'll be able to conduct complex Red Team operations and prepare for the ARTOC exam.

As with all our training courses, this one uses the latest, up-to-date version for ARTOC from White Knight Labs.

Objectives

- Red Teaming in a DevOps context
- Automate secure C2 infrastructures
- Integrate offensive tools into CI/CD pipelines
- Bypass modern defenses (EDR, ASR, WDAC)
- Simulate MITRE ATT&CK aligned adversaries
- Prepare effectively for ARTOC certification

Target audience

- DevOps engineers
- Experienced Pentesters
- CI/CD security professionals
- Systems architects

Prerequisites

- Solid knowledge of DevOps
- Experience in offensive security / pentesting
- Proficiency in Linux and Windows environments
- Familiarity with C2 tools

Our Advanced Red Team Operations Certification training program

Advanced foundations & operational framework

- ARTOC objectives and deliverables
- Red Team roles in a DevOps context
- Rules of engagement, ethics and scope
- Mission organization and risk management
- Workshop: framing a Red Team mission integrated with CI/CD

Offensive infrastructure in a CI/CD context

- Deploying a highly available C2 infrastructure
- Cloud integration & CI/CD pipelines
- Deployments via Infrastructure as Code
- Resilience and IOC rotation
- Workshop: Automated C2 with Terraform

OPSEC & network camouflage

- OPSEC best practices for offensive DevOps
- Reverse proxies & redirectors
- C2 profiling (URIs, User Agents, cookies)
- Telemetry and noise reduction
- Workshop: stealth redirector in a cloud environment

Advanced offensive techniques

- Offensive scripts integrated into workflows
- Languages: Python, Go, C#
- Secret management & code signing

- Tests & QA on offensive tools
- Workshop: offensive tool connected to a CI pipeline

Bypassing defenses

- EDR, ASR and WDAC evasion
- Injections & stealth executions
- Abuse of LOLBAS and signed binaries
- Measuring footprints and adapting TTPs
- Workshop: evaluating a payload against a lab EDR

Exploitation & escalation in the CI/CD chain

- Pipeline targets and attack points
- Container registers & dependencies
- Exposed secrets, roles and permissions
- Kubernetes / OpenShift orchestrator attacks
- Workshop: exploiting a simulated CI/CD flaw

Post-operation & pivoting

- Stealth access maintenance scripts
- Persistence on ephemeral environments
- Multi-environment management (DEV/QA/PROD)
- Cleanup & disengagement
- Workshop: multi-stage persistence

Pivoting between environments

- Mapping gateways & trusts
- Lateral movement via API & orchestrators
- Encrypted tunnels & jump hosts
- Detection/evasion during pivot
- Workshop: automated Dev? Prod

Stealth exfiltration & data staging

- Legitimate channels & encapsulation
- Encryption, encoding, fragmentation
- Opsec exfiltration and timings
- Validation & proof of objectives
- Workshop: simulated exfiltration pipeline

Adversary emulation & reporting

- Threat intel & targeting TTPs
- MITRE ATT&CK alignment
- Measuring defensive effectiveness
- Iterations & scenario adaptation
- Workshop: complete ATT&CK scenario

Red Team reporting for DevSecOps

- Structure: executive + technical
- Actionable evidence for DevSecOps
- Traceability: timelines, IOCs
- Multi-stakeholder communication
- Workshop: ARTOC mini-report

Debriefing & recommendations

- Results & gap analysis
- DevSecOps maturity assessment
- Continuous improvement plan
- Post-mission roadmap
- Workshop: simulated oral presentation

ARTOC certification preparation

- Exam format and success criteria
- Time management & prioritization
- Review checklist
- Classic pitfalls & remedies
- Workshop: ARTOC white session

Complete technical review

- Recap of key tools & techniques
- OPSEC review & C2 profiles
- Orchestrators & CI/CD
- EDR/ASR/WDAC evasion
- Workshop: solving a multi-TTP scenario

Simulated test & final validation

- Exam preparation
- Validation of deliverables
- Personalized feedback
- Action plan up to D-day
- Workshop: graded mock exam

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire enabling us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire is used to check that skills have been correctly acquired.

Certification

A certificate will be awarded to each trainee who completes the training course.