

CRTO — Certified Red Team Operator Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

ADVANCED

At a glance

COURSE	CRTO — Certified Red Team Operator	WHAT IS INCLUDED ✓ Instructor-led delivery by practitioners who also work our SOC ✓ Hands-on lab access for the duration of the course ✓ Course materials and lab guides ✓ Hacky Security certificate of completion ✓ Post-course support by email
TRACK	Zero-Point Security	
DOMAIN	Cyber Security	
LEVEL	Advanced	
DURATION	On request	
DELIVERY	Classroom · Online live · On-site at your office	
LANGUAGE	English	
CLASS SIZE	Small cohorts — everyone gets lab time	

Who this is for

This is an advanced course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

CRTO — Certified Red Team Operator — is Zero-Point Security's course, and it is the one that teaches red teaming as an operation rather than a penetration test. The difference matters. A penetration test finds vulnerabilities; a red team tests whether a defended organisation can detect and respond to a realistic adversary. CRTO is built around a command-and-control framework, and its whole emphasis is on operating quietly against a monitored environment with a modern EDR watching.

It has become one of the most respected practical red-team certifications precisely because it is honest about the modern defensive stack. You do not just get a shell; you get a shell past defences that are designed to catch shells, and you keep it while blending into the noise. The tradecraft — sleep, jitter, in-memory execution, avoiding the telemetry EDR watches — is the actual subject.

The exam is a practical against a defended Active Directory lab, where reaching the objective means doing so without being trivially caught.

Module 01 — Red-team operations and infrastructure

The frame and the plumbing before the attack.

- Red teaming versus penetration testing: goals, rules, and what success means
- Command-and-control concepts: listeners, beacons, and how an operator works
- Setting up resilient C2 infrastructure with redirectors
- Operational security for the operator, not just the payload

Module 02 — Initial access and payload delivery

Getting the first beacon into a defended environment.

- Crafting payloads that survive antivirus and initial inspection
- Delivery pretexts and the client-side execution path
- The first callback, and keeping it quiet from the start
- Sleep, jitter and beacon hygiene

Module 03 — Host reconnaissance and defence awareness

Learning the environment without alerting it.

- Enumerating a host while minimising telemetry
- Identifying the EDR and security tooling present
- Deciding which techniques are safe here and which are not
- Situational awareness before any loud action

Module 04 — Evading endpoint detection

The core skill: doing what you need while EDR watches.

- How modern EDR builds its picture from process, memory and network signal
- In-memory execution and avoiding on-disk artefacts
- Bypassing AMSI and script-block logging
- Choosing quiet techniques over the textbook loud ones

Module 05 — Privilege escalation and credential access

Escalating without tripping the sensors that watch for exactly this.

- Local escalation with an eye on what each method logs
- Credential theft that avoids the obvious LSASS access patterns
- Token manipulation and its telemetry

Module 06 — Active Directory attack and lateral movement

Moving through the domain as an operator, quietly.

- Domain enumeration under monitoring
- Kerberos attacks: Kerberoasting, delegation abuse, ticket attacks
- Lateral movement techniques ranked by noise
- Reaching the objective while staying under the detection threshold

Module 07 — Persistence and acting on objectives

Staying in, and completing the mission.

- Persistence that survives without being obvious
- Data location and the objective the exercise is built around
- Withdrawing cleanly

Module 08 — Operating as a team

Red teaming is rarely solo — the operational discipline of it.

- Logging your own actions for the eventual debrief and blue-team replay
- Deconfliction with the defenders when required
- The report: what the client learns about their own detection gaps

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 · info@hackysecurity.com

<https://hackysecurity.com/courses/crto/>

CHANDIGARH · SHIMLA · DELHI · DUBAI · LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 19 September 2026.