



RED TEAM CYBERSECURITY ENGINEER

Specialized Engineering Course + Certified Professional License Pathway

Learn to plan, engineer, execute, and validate authorized, threat-informed adversary emulation by governing scope, modeling attack paths, testing controls, evaluating detection and response, and turning evidence into defensible defensive improvements.

COURSE IN ONE VIEW

Field: Red Team Engineering / Adversary Emulation

Course Type: Specialized Engineering / Core

Level: Professional

Delivery: 100% online, self-paced

Pace: 5 days / 1 week

Modules: 5

Applied Practice: Cyber Simulations

Assessment: Applied Cyber Capstone

Credential Pathway: Red Team Engineer CPL

Tuition: \$2,495 Pro Bundle=Course + CPL included. Payment options available

WHY THIS COURSE

- Develop professional red-team engineering capability grounded in authorization, Rules of Engagement, safety, and evidence discipline.
- Learn to turn threat-informed adversary behavior into controlled multi-step attack paths that challenge real defenses.
- Validate preventive, detective, and responsive controls through realistic simulation, telemetry review, and retest logic.
- Produce decision-ready findings, remediation priorities, and executive reporting rather than isolated exploit output.

WHAT YOU WILL LEARN

- Define engagement boundaries, sponsor authority, scope, ROE, deconfliction, and stop conditions.
- Model systems, trust relationships, attack surfaces, and credible adversary objectives across enterprise, cloud, identity, application, and supporting infrastructure.
- Engineer controlled offensive tests with clear objectives, prerequisites, success criteria, expected controls and detections, and evidence requirements.
- Execute authorized adversary emulation and preserve packet, endpoint, identity, application, firewall, IDS, and SIEM evidence.
- Evaluate prevention, telemetry, detection, escalation, containment, and response outcomes.
- Convert validated results into remediation, retest criteria, and defensible technical and executive reporting.

WHO THIS COURSE IS FOR

- Working cybersecurity professionals.
- Red team or offensive security practitioners.
- Security engineers, architects, or technical leads involved in defensive validation.
- Blue team, detection, SOC, or response professionals expanding into adversary-emulation understanding. Practitioners preparing for the Red Team Engineer CPL pathway.

FIVE-MODULE LEARNING PATH

The course progresses from engagement governance and target understanding through defensive expectations, controlled test engineering, simulation-based validation, and evidence-driven improvement. Each module builds toward practical Red Team Engineering capability.

01	Scope, System Dissection, and Technical Adversarial & Defensible Analysis (TADA) Govern the engagement and understand the target. Define sponsor authority, scope, ROE, prohibited actions, testing windows, evidence rules, stop conditions, and deconfliction. Map endpoints, servers, identity services, applications, monitoring paths, trust boundaries, remote access, threat vectors, and credible multi-step attack paths.
02	Defensible 10 Architecture (D10A) & Structural Controls Define what the defenses should do. Use D10A and D10S to identify micro-perimeters, segmentation, identity and management boundaries, control dependencies, and expected preventive, telemetry, detection, escalation, containment, and response behavior, with primary emphasis on D07 and D08.
03	Advanced TADA Defensive Engineering & Protocol Security Engineer the adversary-emulation test. Translate threat hypotheses into controlled test sequences with objectives, prerequisites, expected controls and detections, success and failure criteria, protocol and authorization boundaries, evidence requirements, fallback logic, abort conditions, tool provenance, and cleanup expectations.
04	Applied Simulation & Telemetry Verification Execute and prove what happened. Run an authorized Cyber Simulation under the approved ROE. Capture packet, endpoint, identity, application, firewall, IDS, and SIEM evidence. Classify material actions as prevented, observed, detected, escalated, contained, missed, or indeterminate.
05	Operational Resilience & System Defense Synthesis Turn evidence into defensive improvement. Reconstruct the validated attack path, distinguish controls that worked from those that failed, identify root causes, define remediation and detection improvements, establish measurable retest criteria, and prepare the Domain Defense Specification and executive improvement brief.

APPLIED RED TEAM PRACTICE ACROSS THE COURSE

01 GOVERN	Establish sponsor intent, scope, ROE, safety controls, evidence rules, and stop conditions.
02 MODEL	Map systems, identities, trust relationships, exposure, and credible adversary behaviors.
03 ENGINEER	Design controlled test paths, define expected controls and detections, and prepare evidence logic.
04 VALIDATE	Execute the simulation, collect telemetry, and measure prevention, detection, and response outcomes.
05 IMPROVE	Turn evidence into remediation, retest criteria, executive findings, and defensible improvement.

OFFICIAL COURSE MATERIAL

- Digital Book
- Videos
- Templates
- Cyber Simulations

LEARNING EXPERIENCE

- 100% online and self-paced
- Hands-on Cyber Simulations
- Evidence-driven capstone preparation
- Professional reporting and defensive-improvement focus

COMPLETE THE COURSE. PROVE THE CAPABILITY.

The course culminates in an Applied Cyber Capstone. Learners receive an authorized red-team scenario and demonstrate evidence-based planning, controlled execution, defensive validation, and reporting. Course completion and CPL award are separate outcomes.

APPLIED CYBER CAPSTONE - FIVE REQUIRED ARTIFACTS

1 Engagement Charter & Rules of Engagement

Define mission context, authorization, scope, allowed and prohibited activity, safety controls, evidence handling, stop conditions, and cleanup.

2 Threat-Informed Adversary Emulation Plan

Document threat rationale, objectives, attack-surface model, attack paths, assumptions, success criteria, expected controls and detections, and fallback logic.

3 Attack Path & Operational Evidence Package

Capture execution timeline, tested actions, system context, successful and blocked steps, evidence provenance, defensive signals, constraints, and cleanup confirmation.

4 Control, Detection & Response Validation Report

Assess preventive outcomes, telemetry, analytic and detection coverage, alert quality, escalation, investigation, containment, response timing, gaps, limitations, and retest opportunities.

5 Red Team Findings & Executive Defensive Improvement Brief

Present attack-path findings, impact, root causes, D10S traceability, remediation priorities, owner needs, retest criteria, residual exposure, and executive summary.

HOW YOU ARE EVALUATED

Part 1 - Technical Artifact Evaluation checks completeness, correctness, traceability, safety, and defensibility across the submitted work.

Part 2 - SKA Capability Profile evaluates disciplined engineering practice, reasoning, judgment, and professional communication using evidence from the portfolio.

COURSE OUTCOME & CPL PATHWAY

- Certified Professional License (CPL) and Number
- Digital certification + verifiable License ID and issue date
- Public registry entry after successful evaluation
- License term: 3 years
- Renewal requirement: 20 CPE credits.

READY TO REGISTER?

1 CHECK FIT

Cybersecurity Essentials is required. Review the program, schedule, tuition, and certification pathway before registering.

2 REVIEW DETAILS

Have your contact details, LinkedIn profile, and resume/CV ready for the Cyber Academy registration form.

3 REGISTER

Select the course program, identify your enrollment goal, submit the form, and follow the Academy onboarding instructions.

TAKE THE NEXT STEP

Register: isaunited.org/isaunited-school-of-engineering-cyber-defense-form

Tuition & Plans: isaunited.org/isaunited-membership-pricing-and-plans

Questions: info@isaunited.org

Workforce-Informed | Evidence-Governed | Publicly Verifiable

Tuition, course sequence, eligibility, and program details may change. Confirm current information on [ISAUnited.org](https://isaunited.org) before enrollment.