CA404: Adversary Emulation with MITRE ATT&CK

41 Instructional Hours 51 CPEs 10 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

ADVANCED

This course delivers a comprehensive, hands-on introduction to adversary emulation (AE), focusing on replicating real-world attacker behavior using the MITRE ATT&CK framework. Participants will learn how advanced persistent threats (APTs) operate, how to model their tactics, techniques, and procedures (TTPs), and how to assess organizational defenses against realistic threat scenarios. The course bridges the gap between red and blue teams by integrating cyber threat intelligence (CTI), enabling organizations to evaluate security holistically across people, processes, and technology.

You Will Be Able To

- Conduct adversary emulation engagements based on real-world threat intelligence
- Map cyber threat intelligence to the MITRE ATT&CK framework
- Develop adversary profiles and build TTP-based attack scenarios
- Plan, implement, and execute adversary emulation operations
- Evaluate detection and response capabilities across the attack lifecycle
- Use tools such as ATT&CK Navigator, Caldera, and Atomic Red Team
- Measure defensive effectiveness and identify security gaps
- Produce actionable reports to improve organizational resilience

Who Should Attend

This course is designed for cybersecurity professionals who want to simulate real adversary behavior and improve defensive capabilities, including:

- Red Team Operators
- Blue Team / SOC Analysts
- Threat Hunters
- Cyber Threat Intelligence Analysts
- Penetration Testers transitioning to advanced assessments
- Security Engineers and Architects
- Incident Responders

Relevant Combat Roles

- Red Team Operator
- Purple Team Practitioner
- SOC Analyst (Tier 2–3)
- Threat Intelligence Analyst
- Detection Engineer
- Security Operations Engineer
- Cyber Defense Analyst

Topics Covered

Adversary Emulation Fundamentals and Methodology

Advanced Persistent Threats (APTs) and attacker motivations

MITRE ATT&CK Framework (tactics, techniques, procedures)

Adversary lifecycle: reconnaissance impact

Cyber Threat Intelligence (collection, enrichment, mapping)

ATT&CK-based detection and defense strategies

Visualization using ATT&CK Navigator

Engagement planning and rules of engagement

TTP development, implementation, and execution

Measuring detection, prevention, and response effectiveness

Real-world adversary emulation plans (FIN6, APT3, APT29)

Labs

Adversary Emulation Lab & Environment Operations
(Splunk Attack Range setup, lab deployment, and adversary emulation environments)

Threat Intelligence & MITRE ATT&CK Mapping
(real-world CTI mapping, ATT&CK techniques, and ATT&CK Navigator visualization)

Adversary Profiling & TTP Development
(adversary profiles, threat actor research, and TTP outline creation)

Initial Access & Exploitation Simulations
(phishing simulations, exploitation scenarios, and initial access techniques)

Post-Exploitation & Lateral Movement Operations
(lateral movement, credential access, persistence, and privilege escalation techniques)

Command & Control (C2) & Data Exfiltration Simulations
(C2 communications, data exfiltration, and adversary tradecraft simulations)

Adversary Emulation Automation & Detection Validation
(Atomic Red Team, CALDERA automation, detection analysis, and defensive control validation)

Professional Adversary Emulation Reporting
(emulation findings, remediation recommendations, and security assessment reporting)