SEC565:™ Red Team Operations and Adversary Emulation™

GRTP Red Team Professional
giac.org/grtp

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Plan and execute Red Team engagements
- Leverage cyber threat intelligence in Red Teaming
- Accelerate CTI analysis and TTP extraction using AI
- Emulate adversary TTPs using MITRE ATT&CK
- Modernize and patch open-source tooling with AI
- Develop custom evasion frameworks using AI
- Create MCP servers for AI-driven C2 operations

Business Takeaways

- Strengthen Blue Team defenses through simulations
- Enhance detection and response with attack emulation
- Provide actionable insights to address security gaps
- Measure and optimize defense systems for effectiveness
- Identify weaknesses in people, processes, and technology
- Leverage AI to increase Red Team efficiency

Authors' Statement

"Organizations are maturing their security testing programs to include Red Team engagements and adversary emulations. These engagements provide a holistic view of an organization's security posture by emulating a realistic adversary to test security assumptions, measure the effectiveness of people, processes, and technology, and improve detection and prevention controls. This course will teach you how to plan Red Team engagements, leverage threat intelligence to map against adversary tactics, techniques, and procedures, build a Red Team program and plan, execute a Red Team engagement with a strong emphasis on operational security and tradecraft, and report and analyze the results. Direct application of the lessons in this course will give Red Team operators the skills necessary to improve the overall security posture of an organization."
—Barrett Darnell

"With this course we provide students with a blueprint they can use to set up a realistic Red Team operation against a client environment. Students will be able to consume threat intelligence, formulate a plan of attack, execute it, and ultimately create a debrief package that will provide maximum value for their organization. This course truly brings together a wide variety of knowledge and aims to equip the students with state-of-the-art tradecraft, keeping up to date with the latest and greatest TTPs. No other course brings together such a wide variety of knowledge of all things Red Team."
—Jean-Françis Maes

The SEC565 Red Team course equips participants with the skills to plan and execute Red Team engagements through adversary emulation. Leveraging cyber threat intelligence, the MITRE® ATT&CK framework, and cutting-edge AI capabilities, students learn to build resilient attack infrastructure, bypass modern defenses, and exploit Active Directory.

Red Team Training – Real-World Skills for Emerging Threats

Penetration testing is effective at enumerating vulnerabilities, but less effective in addressing personnel and processes on the defense side. This can leave Blue Teams or defenders without sufficient knowledge of what offensive input to improve, in turn leaving organizations stuck in a cyclical process of just focusing on vulnerabilities in systems rather than on maturing defenders to effectively detect and respond to attacks.

In SEC565, students will learn how to plan and execute end-to-end Red Teaming engagements that leverage adversary emulation, gaining the skills to organize a Red Team, consume threat intelligence to map against adversary tactics, techniques, and procedures (TTPs), emulate those TTPs, report and analyze the results of the Red Team engagement, and ultimately improve the overall security posture of the organization. As part of the course, students will perform an adversary emulation against a target organization modeled on an enterprise environment, including Active Directory, intelligence-rich emails, file servers, and endpoints running in Windows.

SEC565 features six intensive course sections. We will start by consuming cyber threat intelligence to identify and document an adversary that has the intent, opportunity, and capability to attack the target organization. Students will learn to accelerate this process by using AI to extract TTPs from CTI reports and generate highly convincing social engineering pretexts. Using this strong threat intelligence and proper planning, students will follow the Unified Kill Chain and multiple TTPs mapped to MITRE ATT&CK during execution.

Students will be immersed in deeply technical Red Team tradecraft ranging from establishing resilient and advanced attack infrastructure to abusing Active Directory. Students will harness AI coding assistants to modernize legacy open-source tooling, build custom evasion frameworks using "vibe coding," and create Model Context Protocol (MCP) servers to drive Command and Control (C2) operations via natural language. After gaining initial access, students will thoroughly analyze each system, pilfer technical data and target intelligence, and then move laterally, escalating privileges, laying down persistence, and collecting and exfiltrating critically impactful sensitive data. The course concludes with an exercise analyzing the Blue Team response, reporting, and remediation planning and retesting.

In SEC565, you will learn how to show the value that Red Teaming and adversary emulations bring to an organization. The main job of a Red Team is to make a Blue Team better. Offense informs defense and defense informs offense.

"Course content is great. Very informative and up-to-date attack vectors."
—Hunter Vaughan, **Northrop Grumman**

Section Descriptions

SECTION 1: Planning Adversary Emulation and Threat Intelligence

This initial section establishes foundational concepts in adversary tactics, Red Team operations, and threat intelligence frameworks. Focus areas include engagement planning, threat actor analysis, and initial attack execution—all critical for emulating sophisticated adversaries in controlled environments.

TOPICS: Advanced Adversary Emulation Methods; Unified Kill Chain and Attack Mapping; AI-Assisted CTI Analysis and TTP Extraction; Multifactor Bypass Techniques; Social Engineering and AI-Generated Pretexts

SECTION 2: Attack Infrastructure and Operational Security

Section 2 is an advanced command-and-control (C2) infrastructure and tooling deep-dive focused on resilient attack frameworks, evasive redirector implementation, and OPSEC hardening. Students learn operational security monitoring, infrastructure protection, and defender evasion through sophisticated C2 architectures and communication channels.

TOPICS: Modern C2 Infrastructure Design; Advanced Redirector Methodologies; Third-Party Hosting Strategies; OPSEC and Infrastructure Hardening; AI-Driven C2 Operations with Model Context Protocol (MCP)

SECTION 3: Getting In and Staying In

Advanced payloads and network infiltration tactics form the core of this section. Students explore stealthy weaponization techniques and learn to establish reliable initial access vectors for target environments. We pay special attention to evasive post-exploitation methodologies, including privilege escalation chains and persistent access methods.

TOPICS: Sophisticated Payload Engineering; Defensive Control Bypass Tactics; Network Infiltration Methodology; AI-Assisted Tool Restoration and Patching; Vibe Coding Custom Evasion Frameworks

SECTION 4: Active Directory Attacks and Lateral Movement

Students explore comprehensive domain enumeration and advanced privilege escalation within Windows environments. Deep technical analysis covers cross-domain attack patterns, trust relationship exploitation, and sophisticated lateral movement tactics. Each concept integrates with practical attack tool implementation for maximum operational impact.

TOPICS: Domain Trust Exploitation Chains; Authentication Bypass Techniques; Certificate Service Manipulation; Advanced Delegation Attacks; Enterprise Network Pivoting

SECTION 5: Obtaining the Objective and Reporting

Students navigate advanced database attacks, sensitive data exfiltration methods, and impact demonstration through targeted system manipulation. We comprehensively cover engagement analysis, strategic reporting methodologies, and automated breach simulation techniques for continuous security validation.

TOPICS: Database Exploitation Techniques; Target System Manipulation; Engagement Analysis Frameworks; Breach Simulation Deployment; Red Team Measurement Protocols

SECTION 6: Immersive Red Team Capture the Flag

Students operate across multiple domains, implementing sophisticated attack chains against Windows and Linux infrastructures. The immersive environment presents authentic user activity patterns, rich intelligence gathering opportunities, and segmented network challenges requiring advanced lateral movement techniques.

TOPICS: Enterprise Adversary Emulation; Cross-Domain Attack Strategies; Credential Theft and Exploitation; Advanced C2 Infrastructure; Comprehensive Impact Analysis

"The course content is absolutely amazing. Even if you already have some knowledge on the topic, there is still a wealth of information that will further enhance your understanding and solidify your procedures!"

—Kemmner L., **NetPlas Neckarsulm**

Who Should Attend

- Security professionals interested in expanding their knowledge of Red Team engagements
- Penetration testers and Red Team members looking to better understand their craft
- Blue Team members, defenders, and forensic specialists looking to integrate AI into their workflows
- Blue Team members, defenders, and forensic specialists
- Auditors who need to build deeper technical skills
- Information security managers

NICE Framework Work Roles

- Adversary Emulation Specialist/Red Teamer (OPM 541)
- Target Developer (OPM 131)
- Cyber Ops Planner (OPM 332)
- Partner Integration Planner (OPM 333)

GRTP
Red Team Professional
giac.org/grtp

GIAC Red Team Professional

The GIAC Red Team Professional certification validates an individual's ability to conduct end-to-end Red Team engagements. GRTP certification holders have demonstrated knowledge of building an adversary emulation plan, establishing an C2 infrastructure, and emulating adversary tactics, techniques, and procedures (TTPs) to assist in improving overall security.

- Building an adversary emulation plan using gathered threat intelligence
- Creating a comprehensive attack infrastructure
- Performing target reconnaissance
- Gaining initial access
- Network and Active Directory enumeration
- Propagate throughout the network
- Active Directory attacks
- Bypassing common defense mechanisms
- Collect and exfiltrate sensitive data
- Producing an engagement report
- Presenting Red Team actions to key personnel
- Performing retesting and replaying of Red Team activities