SEC665: **Advanced Red Team Operations™**

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Design covert, automated red team infrastructure built to resist attribution and detection
- Execute advanced phishing, including AiTM and device code techniques to bypass MFA
- Evade modern EDR/NDR through unhooking, direct syscalls, and kernel callback bypasses
- Perform stealthy privilege escalation, lateral movement, and cloud/on-prem pivoting
- Exploit AD CS, CI/CD pipelines, and Entra ID for persistent, high-privilege access
- Develop custom BOFs, obfuscated .NET tools, and novel persistence mechanisms
- Apply all skills in a realistic full-day CTF against a hardened multi-domain environment

Business Takeaways

- Build red teams capable of operating effectively against hardened, modern environments
- Reduce organizational blind spots by emulating advanced, real-world adversary behavior
- Improve detection and response by stress-testing EDR, NDR, and identity controls
- Strengthen cloud and hybrid security by validating identity and access assumptions
- Increase red team ROI by developing sustainable, research-driven tradecraft

Hands-On Advanced Read Team Operations Training

SEC665 goes far beyond foundational red team techniques, immersing students in the real-world tradecraft required to operate against modern, hardened enterprise and government environments. This advanced Red Team course is designed for experienced operators who already understand the basics and are ready to evolve their skills to match today's adversaries and defenders.

The course begins with covert infrastructure and advanced initial access. Students learn to design and automate red team infrastructure that blends into internet background noise, minimizes attribution, and resists scanning and threat intelligence collection. The course then explores modern initial access vectors, including abuse of file formats, DLL sideloading, signed payload delivery, advanced phishing, and adversary-in-the-middle techniques that bypass MFA by targeting sessions rather than credentials, with a strong emphasis on OPSEC and detection tradeoffs.

Privilege escalation, lateral movement, and persistence form the next major pillar. Students perform reconnaissance while avoiding common EDR detections, adapt tooling for stealth, and leverage Windows internals such as tokens, COM, WMI, and the Windows loader. The course addresses modern enterprise defenses like LSASS protections, Credential Guard, and UAC, showing how attackers adapt to hardened environments. Persistence is treated as an operational problem, focusing on methods that blend into normal enterprise workflows.

SEC665 places significant emphasis on cloud and identity-based attacks. Students explore Entra ID, OAuth, and OpenID Connect, learning how token abuse enables lateral movement in cloud environments and pivots back on-prem. The course also covers NDR evasion, stealthy impacket modifications, Active Directory Certificate Services exploitation, and attacks against CI/CD and DevOps infrastructure.

A defining feature of SEC665 is red team research and development. Students analyze endpoint and network defenses, understand EDR telemetry, and develop custom tooling to evade controls. Advanced .NET tradecraft is covered in depth, including AMSI and ETW bypasses, runtime patching, automated obfuscation, and Beacon Object Files (BOFs).

The course culminates with Windows kernel tradecraft, giving students hands-on experience with kernel debugging, EDR kernel components, callbacks, minifilters, and driver exploitation. On the final day, students apply everything in a realistic capture-the-flag exercise, operating against a hardened environment while minimizing detection.

SEC665 is built for red teamers in DoD, intelligence, and enterprise environments who must stay ahead of modern defenses and simulate advanced adversaries with precision and discipline.

Section Descriptions

SECTION 1: Introduction and Initial Access

Section 1 covers various topics required to build a successful initial access campaign for covert red team operations. From creating the infrastructure to building evasive payloads and delivery techniques, students will learn how to properly weaponize payloads for initial access. Focus then lies on creating convincing social engineering and phishing campaigns, bringing home the sought-after access. The module is concluded with a deep dive into reconnaissance techniques to avoid losing that well-deserved access.

TOPICS: Introduction to the Course, Havoc C2, and Elastic Security; Designing Resilient Infrastructure and Automating Infrastructure Deployments; Engineering Evasive Payloads; Modern Payload Delivery Techniques; Phishing, Social Engineering, and Creating Convincing Pretexts; Covert Enumeration and Reconnaissance

SECTION 2: Privilege Escalation and Lateral Movement

Section 2 covers advanced lateral movement techniques in modern environments as a follow-on from topics covered in intermediate red team operations courses. Focus areas include credential attacks against hardened systems, Windows authentication protocols, relays over C2, OPSEC-focused stealth lateral movement, EDR architecture, telemetry, and evasion.

TOPICS: Credential Attacks and Relaying in Hardened Windows Environments; Authentication Protocols and Ticketing Attacks in Modern Windows Over C2; Advanced Lateral Movement Techniques with OPSEC Awareness; Windows Access Tokens and UAC; EDR Architecture, Telemetry Sources, and Evasion

SECTION 3: Entra ID and Advanced Lateral Movement

Section 3 introduces lesser-known techniques to achieve persistence on a compromised endpoint, cloud initial access, and lateral movement and attacks on AD CS and Configuration Manager (formerly known as SCCM). Students will understand how to leverage CI/CD pipelines to reach their objectives.

TOPICS: Advanced Persistence; Entra ID Initial Access; Entra ID Lateral Movement; Attacking Configuration Manager; Certificate Services Abuse; Compromising CI/CD Pipelines

SECTION 4: Red Team Engineering

Section 4 focuses on advanced red team engineering and R&D, teaching operators to research defenses, master .NET tradecraft, obfuscation, develop BOFs, and discover novel persistence mechanisms.

TOPICS: Researching Endpoint/Network Defenses like WDAC and Defender; Advanced .NET Tradecraft and Obfuscation; Beacon Object File (BOF) Development and Testing; Discovering Novel Windows Persistence via ProcMon and COM Hijacking

SECTION 5: The Windows Kernel

Explore Windows kernel internals from a red team perspective, including EDR drivers, kernel callbacks, minifilters, and driver exploitation, to understand how modern defenses operate below user mode and where blind spots and evasion opportunities exist.

TOPICS: Windows Kernel Fundamentals and Kernel Debugging for Red Team Operations; How EDR Drivers, Callbacks, and Minifilters Monitor System Activity; Enumerating and Analyzing EDR Kernel Components and Communications; Identify Potential EDR Blind Spots Through Reverse Engineering; Risks, Tradeoffs, and Methods of Kernel Driver Exploitation

SECTION 6: Capture the Flag

During Section 6, students compete in the ranges.io platform, a powered web application penetration testing tournament. This capture-the-flag exercise lets them wield new or sharpened skills to answer questions, complete missions, exfiltrate data, and tackle progressive challenges with hints that support all skill levels and reinforce learning.

Who Should Attend

SEC665 training is recommended for a diverse range of individuals, including:

- Students of SEC565, SEC599, and SEC699
- Red Team operators
- Penetration testers
- Purple Team operators
- Red Team developers