SEC599:™ Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses™

GDAT
Defending Advanced Threats
giac.org/gdat

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Leverage MITRE ATT&CK for threat-informed defense
- Deploy custom security controls and sandboxing
- Implement advanced Windows hardening and detection
- Build logging and monitoring with Elastic and Sysmon
- Design threat detection using intel and traffic analysis
- Practice purple teaming with real-world attack scenarios

Business Takeaways

- Faster threat detection and response
- Stronger red and blue team collaboration
- Defense based on real attacker behaviors
- Better use of existing security tools
- Clear metrics for measuring improvements

Hands-On Training

SEC599 leverages SANS OnDemand systems, allowing attendees to complete the 20+ labs in the course within a full-fledged browser environment. This setup eliminates potential issues with student laptops and maximizes learning time focused on security topics rather than configuring virtual machines. Student virtual machines are provided to facilitate continued learning at home.

Examples of the practical labs and exercises you will complete in this course will enable you to:

- Use MITRE ATT&CK Navigator to assess different techniques
- Leverage MITRE ATT&CK as a "common language" in the organization
- Harden domain environments using Security Compliance Toolkit (SCT) and Security Technical Implementation Guide (STIG)
- Perform atomic TTP testing using Caldera
- Map attack surfaces with BBOT
- Stop NTLMv2 sniffing and relay attacks in Windows
- Block typical phishing payload execution
- Restrict binary and PowerShell execution
- Detect threats using Sysmon and SIGMA
- Utilize online sandboxes and YARA for analysis
- Implement exploit mitigation using compile-time controls and ExploitGuard

Building Enterprise Cyber Defense: From Threat Analysis to Purple Team Implementation

You just got hired to help our virtual organization "SYNCTECHLABS" build out a cyber security capability. On your first day, your manager tells you: "We looked at some recent cyber security trend reports and we feel like we've lost the plot. Advanced persistent threats, ransomware, denial of service... We're not even sure where to start!"

Cyber threats are on the rise: ransomware tactics are affecting small, medium, and large enterprises alike, while state-sponsored adversaries are attempting to obtain access to your most precious crown jewels. SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses™ will arm you with the knowledge and expertise you need to overcome today's threats. Recognizing that a prevent-only strategy is not sufficient, we will introduce security controls aimed at stopping, detecting, and responding to your adversaries. This course is also a key resource for preparing for the GDAT certification, which validates your ability to build a defense-in-depth strategy against sophisticated threats.

Course authors Stephen Sims and Erik Van Buggenhout (both certified as GIAC Security Experts) are hands-on practitioners who have built a deep understanding of how cyber-attacks work through penetration testing and incident response. While teaching penetration testing courses, they were often asked the question: "How do I prevent or detect this type of attack?" Well, this is it! SEC599™ gives students real-world examples of how to prevent attacks. The course features more than 20 labs plus a final capture-the-flag exercise where students can showcase their new technical skills and compete for the coveted SEC599 challenge coin.

Our six-part journey will start off with an analysis of recent attacks through in-depth case studies. We will explain what types of attacks are occurring and introduce formal descriptions of adversary behavior such as the Cyber Kill Chain and the MITRE ATT&CK framework. In order to understand how attacks work, you will also compromise our virtual organization "SYNCTECHLABS" in Section 1 exercises.

In Sections 2, 3, 4 and 5 we will discuss how effective security controls can be implemented to prevent, detect, and respond to cyber attacks. After the full 5-day course you will compete in a capture-the-flag challenge where you can apply your newly learned skills against real-world inspired cases. Your network has been compromised, so the faster you can figure out what's going on, the higher you will score!

"The different topics covered in this course can bring eye-opening layers of defense to any organization."

— Mike Marx, **Carbon Black**

Section Descriptions

SECTION 1: Introduction and Attack Surface Management

Begin your journey with real-world attack analysis and hands-on experience compromising the SYNCTECHLABS virtual environment. Learn to leverage the Cyber Kill Chain and MITRE ATT&CK framework while understanding purple team methodologies and essential defensive tools.

TOPICS: Course Objectives and Lab Environment Setup; Analysis of Current Cyber-Attack Landscapes; Extended Kill Chain Methodology; Purple Team Concepts and Implementation; MITRE ATT&CK Framework Integration

SECTION 2: Payload Delivery and Execution

In Section 2, we will explore attacker techniques for payload delivery and execution, focusing on prevention and detection methods. Learn to implement controls against malicious executables and scripts, while gaining hands-on experience with YARA for payload description and SIGMA for use-case documentation.

TOPICS: Common Delivery Mechanism Analysis; Payload Delivery Prevention Strategies; Network and Removable Media Controls; Mail Security and Web Proxy Implementation

SECTION 3: Exploitation, Persistence, and Command and Control

In Section 3, will will learn to integrate security into the software development lifecycle while implementing effective exploit mitigation techniques. The section focuses on both compile-time and run-time protections, persistence detection strategies, and command and control channel identification.

TOPICS: Software Development Lifecycle Security Integration; Patch Management Strategies; Exploit Mitigation Techniques; Persistence Strategy Analysis

SECTION 4: Lateral Movement

Section 4 will focus on defending against lateral movement. We examine credential protection, Windows privilege escalation, and various attack strategies while implementing effective detection and deception techniques.

TOPICS: Active Directory and Entra ID Security Fundamentals; Principle of Least Privilege and UAC; Privilege Escalation Prevention; Credential Theft Protection; Attack Path Mapping Using BloodHound

SECTION 5: Action on Objectives, Threat Hunting, and Incident Response

In Section 5, we address final attack stages including domain dominance prevention and data exfiltration detection. Learn to leverage threat intelligence effectively and perform incident response, with hands-on practice using advanced forensics tools.

TOPICS: Domain Dominance Prevention Strategies; Data Exfiltration Detection Methods; Threat Intelligence Implementation; Proactive Threat Hunting; Incident Response Procedures

SECTION 6: Capture-The-Flag Challenge

Apply your newly acquired skills in a comprehensive, team-based capture-the-flag competition. Your environment is under attack and it's up to you to identify how they got in, and what they're doing once they obtained access.

TOPICS: Practical Exercises Based on Real-World Cases; Analyze Identified Nalware; Perform Network Analysis to Identify Intrusions; Examine Memory Captures to Identify Artefacts; Find Potential Attack Paths in Your Environment

Author Statement

"After writing and teaching many advanced penetration testing and exploit development courses over the past 10 years, I started to see a trend developing. Often, over half of the students in my classes were not actually penetration testers or those who would be writing zero-days. In fact, they most often worked in a defensive role and were coming to these courses to learn about the techniques used by attackers so that they could better defend their networks. This led to our idea to write a course that focused on teaching just enough of the offense to demonstrate the impact, and then focus the majority of the time on implementing controls to break the techniques used by adversaries and red team testers."

—Erik Van Buggenhout

Who Should Attend

- Security architects and security engineers who want to better understand how the defenses they put in place make an impact on adversary operations
- Red teamers and penetration testers who want to better understand how blue team techniques could stop their attacks
- Technical security managers who want to understand what security controls should be prioritized
- Security Operations Center analysts and engineers who want to better understand how they can detect adversary techniques
- Individuals looking to better understand how persistent cyber adversaries operate and how the IT environment can be improved to better prevent, detect, and respond to incidents

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)

GDAT
Defending Advanced Threats
giac.org/gdat

GIAC Defending Advanced Threats

The GIAC Defending Advanced Threats (GDAT) certification covers both offensive and defensive topics in-depth. GDAT-certified professionals have a thorough understanding of how advanced cyber adversaries operate and how the IT environment can be improved to better prevent, detect, and respond to incidents.

- Advanced persistent threat models and methods
- Detecting and preventing payload deliveries, exploitation, and post-exploitation activities
- Using cyber deception to gain intelligence for threat hunting and incident response
- Adversary emulation