SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

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

GDAT
Defending Advanced Threats
giac.org/gdat

6 Day Program | 46 CPEs | Laptop Required

You Will Be Able To

- Understand how recent high-profile attacks were delivered and how they could have been stopped
- Implement security controls throughout the different phases of the Cyber Kill Chain and the MITRE ATT&CK framework to prevent, detect, and respond to attacks

Topics To Be Addressed

- Leveraging MITRE ATT&CK as a "common language" in the organization
- Building your own Cuckoo sandbox solution to analyze payloads
- Developing effective group policies to improve script execution (including PowerShell, Windows Script Host, VBA, HTA, etc.)
- Highlighting key bypass strategies for script controls (unmanaged Powershell, AMSI bypasses, etc.)
- Stopping 0-day exploits using ExploitGuard and application whitelisting
- Highlighting key bypass strategies in application whitelisting (focus on AppLocker)
- Detecting and preventing malware persistence
- Leveraging the Elastic stack as a central log analysis solution
- Detecting and preventing lateral movement through Sysmon, Windows event monitoring, and group policies
- Blocking and detecting command and control through network traffic analysis
- Leveraging threat intelligence to improve your security posture

You just got hired to help our virtual organization "SYNCTECHLABS" build out a cybersecurity capability. On your first day, your manager tells you: "We looked at some recent cybersecurity 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, mid-size, 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.

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 full-day Defend-the-Flag exercise during which students attempt to defend our virtual organization from different waves of attacks against its environment.

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 one exercises.

In sections two through five, we will discuss how effective security controls can be implemented to prevent, detect, and respond to cyber attacks.

SEC599 will finish with a bang. During the Defend-the-Flag Challenge on the final course day, you will be pitted against advanced adversaries in an attempt to keep your network secure. Can you protect the environment against the different waves of attacks? The adversaries aren't slowing down, so what are you waiting for?

> **"The different topics covered in this course can bring eye-opening layers of defense to any organization."**
>
> — Mike Marx, **Carbon Black**

sans.org/sec599

- **Watch a preview of this course**
- **Discover how to take this course: Online, In-Person**

Section Descriptions

SECTION 1: Introduction and Reconnaissance

Our six-part journey starts with an analysis of recent attacks through in-depth case studies. We will explain what's happening in real situations and introduce the Cyber Kill Chain and MITRE ATT&CK framework as a structured approach to describing adversary tactics and techniques. We will also explain what purple teaming is, typical tools associated with it, and how it can be best organized in your organization. In order to understand how attacks work, students will also compromise our virtual organization "SYNCTECHLABS" during section one exercises.

TOPICS: Course Outline and Lab Setup; Adversary Emulation and the Purple Team; Reconnaissance

SECTION 2: Payload Delivery and Execution

Section 2 will cover how the attacker attempts to deliver and execute payloads in the organization. We will first cover adversary techniques (e.g., creation of malicious executables and scripts), then focus on how both payload delivery (e.g., phishing mails) and execution (e.g., double-clicking of the attachment) can be hindered. We will also introduce YARA as a common payload description language and SIGMA as a vendor-agnostic use-case description language.

TOPICS: Common Delivery Mechanisms; Hindering Payload Delivery; Preventing Payload Execution

SECTION 3: Exploitation, Persistence, and Command and Control

Section 3 will first explain how exploitation can be prevented or detected. We will show how security should be an integral part of the software development lifecycle and how this can help prevent the creation of vulnerable software. We will also explain how patch management fits in the overall picture. Next, we will zoom in on exploit mitigation techniques, both at compile-time (e.g., ControlFlowGuard) and at run-time (ExploitGuard). We will provide an in-depth explanation of what the different exploit mitigation techniques (attempt to) cover and how effective they are. We'll then turn to a discussion of typical persistence strategies and how they can be detected using Autoruns and OSQuery. Finally, we will illustrate how command and control channels are being set up and what controls are available to the defender for detection and prevention.

TOPICS: Protecting Applications from Exploitation; Avoiding Installation; Foiling Command and Control

SECTION 4: Lateral Movement

Section 4 will focus on how adversaries move laterally throughout an environment. A key focus will be on Active Directory (AD) structures and protocols (local credential stealing, NTLMv2, Kerberosm, etc.). We will discuss common attack strategies, including Windows privilege escalation, UAC bypasses, (Over-) Pass-the-Hash, Kerberoasting, Silver Tickets, and others. We'll also cover how BloodHound can be used to develop attack paths through the AD environment. Finally, we will discuss how lateral movement can be identified in the environment and how cyber deception can be used to catch intruders red-handed!

TOPICS: Protecting Administrative Access; Key Attack Strategies against AD; How Can We Detect Lateral Movement?

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

Section 5 focuses on stopping the adversary during the final stages of the attack:

- How does the adversary obtain "domain dominance" status? This includes the use of Golden Tickets, Skeleton Keys, and directory replication attacks such as DCSync and DCShadow.
- How can data exfiltration be detected and stopped?
- How can threat intelligence aid defenders in the Cyber Kill Chain?
- How can defenders perform effective incident response?

As always, theoretical concepts will be illustrated during the different exercises performed throughout the day.

TOPICS: Domain Dominance; Data Exfiltration; Leveraging Threat Intelligence; Threat Hunting and Incident Response

SECTION 6: APT Defender Capstone

The course culminates in a team-based Defend-the-Flag competition. Section 6 is a full day of hands-on work applying the principles taught throughout the course. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cybersecurity controls promoted all week long. This challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge. Note that OnDemand students will enjoy this exercise on an individual basis. As always, SANS subject-matter experts are available to support every OnDemand student's experience.

TOPICS: Applying Previously Covered Security Controls In-depth; Reconnaissance; Weaponization; Delivery; Exploitation; Installation; Command and Control; Action on Objectives

Who Should Attend

- Security architects and security engineers
- Red teamers and penetration testers
- Technical security managers
- Security Operations Center analysts, engineers, and managers
- 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.

GDAT
Defending Advanced Threats
giac.org/gdat

GIAC Defending Advanced Threats

"The GDAT certification is unique in how it covers both offensive and defensive security topics in-depth. Holders of the GDAT certification have demonstrated advanced knowledge of how adversaries are penetrating networks, but also what security controls are effective to stop them. Next to knowing what controls are instrumental to prevent recent attacks, certified GDAT professionals know that prevent-only is not feasible and thus know how to detect and respond to attacks. Combining all these skills, they have the ability to prevent, detect, and respond to both traditional and APT-style attacks!"

— Erik Van Buggenhout, SEC599 Course Author

- 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