SEC504: Hacker Tools, Techniques, and Incident Handling™

GCIH Incident Handler
giac.org/gcih

6 Day Program | 38 CPEs | Laptop Required

You Will Learn

- Respond effectively to incidents to limit damage
- Evaluate breach evidence to determine compromise scope
- Identify shadow cloud systems and other potential threats
- Use attack tools to assess cloud and on-premises exposure
- Apply defenses to enhance security and stop attacks
- Develop threat intelligence by analyzing attacker tactics
- Accelerating analysis tasks using AI systems

Business Takeaways

- Adopt a dynamic and holistic incident response strategy
- Strengthen cloud security posture
- Leverage automation and AI to accelerate response
- Understand and counter advanced attacker tactics
- Protect critical assets with proactive defense strategies
- Enhance threat detection with multi-layered analysis

"Great content! As a developer it is extremely useful to understand exploits and how better coding practices help your security position."

—Alex Colclough, **Clayton Homes**

SEC504 is SANS' flagship incident handling course, equipping you with essential skills to detect, respond to, and neutralize threats across Windows, Linux, and cloud platforms. Through immersive hands-on labs simulating real-world breaches, you'll master the attacker mindset to strengthen your organization's defenses. This course delivers immediately applicable expertise in Cyber Threat Intelligence (CTI), modern threat response, and cutting-edge topics, including API security exploitation and defense, leveraging AI for offensive and defensive operations, and protecting against AI-targeted attacks like prompt injections. Whether analyzing malicious code, hunting threats, or responding to sophisticated attacks, SEC504 prepares you for today's evolving threat landscape.

Inside the Attacker's Mind

You'll learn how to think like an adversary and act as an expert incident responder, using attacker tools and techniques to understand what happened, why it happened, and how to stop it. The course focuses on practical, real-world application—from malware investigation and password cracking to API exploitation and AI threat defense.

SEC504 now includes AI-driven learning experiences, interactive labs, and a gamified challenge (Office Infiltrator) that teaches prompt injection concepts in a fun, realistic environment. Every module has been refreshed with up-to-date tools, vulnerabilities, and use cases that mirror the current cyber threat landscape.

Author Statement

"Attacker tools and techniques have changed, and incident response must evolve to match. Since I took over as SEC504 author in 2019, I've rewritten this course from the ground up to address the realities of modern cybersecurity. You'll master the full threat landscape: Windows and Linux attacks, modern API exploitation, cloud vulnerabilities, and attacks targeting AI systems. By adopting an attacker's mindset and using their tools, from exploitation frameworks to password cracking to web application attacks, you'll understand not just what happened during an incident, but why it happened, and how to stop it.

"I designed SEC504 to meet you where you are in your career. Whether you're new to incident response or a seasoned professional, the course adapts to your learning style: visual, auditory, hands-on, or analytical. With 50% hands-on labs, AI-enhanced workbook features for personalized support, and unlimited practice time, you control the learning pace while building skills you'll use immediately when you return to the office. With your knowledge of hacker tools and techniques combined with effective defense skills, you'll be ready to become the subject-matter expert your organization needs for today's threats and tomorrow's challenges."

—Joshua Wright

"SEC504 is a great class overall that is perfect for pen testers and defenders alike. It has greatly helped me understand how attackers think, how they gather information, and how they maintain and gain control of systems."

—Evan Brunk, **Acuity Insurance**

Section Descriptions

SECTION 1: Incident Response and Cyber Investigations

The first section covers building an incident response process using the Dynamic Approach to Incident Response (DAIR) to verify, scope, contain, and remediate threats. Through hands-on labs and real-world examples, you'll apply this method with tools like PowerShell and learn to accelerate analysis while using generative AI without compromising accuracy.

TOPICS: Incident Response; Live Examination; Network Investigations; Malware Investigations; Accelerating Incident Response with AI

SECTION 2: Scanning and Enumeration Attacks

This section explores attacker reconnaissance techniques, including network scanning, and target enumeration to identify security gaps. You'll apply these tactics on Windows, Linux, Azure, and AWS targets, then analyze logs and evidence to detect attacks in real time.

TOPICS: Network and Host Scanning with Nmap; Cloud Spotlight: Cloud Scanning; Server Message Block (SMB) Security; Defense Spotlight: Hayabusa and Sigma Rules; Attacker Network Access Manipulation

SECTION 3: Password Attacks and Exploit Frameworks

This section covers key techniques for password compromises against on-premises and cloud systems, using tools like Legba, Hashcat, and Metasploit to simulate attacks and strengthen defenses. The insights gained help enhance practical defenses and inform incident response strategies.

TOPICS: Password Attacks; Microsoft 365 Attacks; Understanding Password Hashes; Password Cracking; Metasploit Framework

SECTION 4: Web Application Attacks

In this course section we'll focus on exploiting the many vulnerabilities in web applications including internal and public-facing systems, from on-premises targets to cloud and Software as a Service (SaaS) platforms.

TOPICS: Forced Browsing and IDOR; Command Injection; Cross-Site Scripting (XSS); SQL Injection; Exploiting API Systems

SECTION 5: Post-Exploitation and AI Attacks

This section covers advanced post-exploitation and AI attacks, teaching how attackers bypass protections, establish persistence, exploit AI vulnerabilities, and exfiltrate data from internal networks and vulnerable cloud deployments. You'll build analysis skills to detect and respond to these threats and apply them in real-world scenarios.

TOPICS: Endpoint Security Bypass; Pivoting and Lateral Movement; Hijacking Attacks; Establishing Persistence; Attacking AI Systems

SECTION 6: Capture-the-Flag Event

Our Capture-the-Flag event is a full day of hands-on activity that has you working as a consultant for ISS Playlist, a fictitious company that has recently been compromised.

"SEC504 has been the single best course I have ever taken. It leaves the student prepared and able to understand a broad scope of content in security."

—Joshua Nielson, **Microsoft**

GCIH

Incident Handler
giac.org/gcih

GIAC Certified Incident Handler

The GIAC Incident Handler certification validates a practitioner's ability to detect, respond, and resolve computer security incidents using a wide range of essential security skills. GCIH certification holders have the knowledge needed to manage security incidents by understanding common attack techniques, vectors and tools, as well as defend against and respond to such attacks when they occur.

- Incident Handling and Computer Crime Investigation
- Computer and Network Hacker Exploits
- Hacker Tools (Nmap, Metasploit and Netcat)

Who Should Attend

SEC504 training is recommended for a diverse range of individuals, including:

- Incident handlers
- Leaders of incident response teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack
- General security practitioners and security architects who want to design, build, and operate their systems to prevent, detect, and respond to attacks

NICE Framework Work Roles

- Technical Support Specialist (OPM 411)
- Systems Security Analyst (OPM 461)
- Privacy Officer/Privacy Compliance
- Manager (OPM 732)
- Cyber Instructional Curriculum
- Developer (OPM 711)
- Cyber Instructor (OP 712)
- Security Awareness & Communications Manager (OP 712)
- Information Systems Security Manager (OPM 722)
- IT Investment/Portfolio Manager (OPM 804)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Incident Responder (OPM 531)
- Adversary Emulation Specialist/Red Teamer (OPM 541)
- Threat/Warning Analyst (OPM 141)
- All-Source Analyst (OPM 111)
- Mission Assessment Specialist (OPM 112)
- Target Network Analyst (OPM 132)
- Cyber Intel Planner (OPM 331)