SEC401: **Security Essentials™**

GSEC
Security Essentials
giac.org/gsec

6	46	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Analyze network traffic at the packet level—identifying protocols and recognizing indicators of compromise—using tools including tcpdump and Wireshark
- Design and evaluate network architecture for defensibility: VLANs, NAC, 802.1x, and Zero Trust principles applied to real organizational environments
- Implement and assess Identity and Access Management strategies, including multi-factor authentication, in both on-premises and cloud environments
- Build a network visibility map that defines your organization's attack surface and informs a systematic approach to hardening and configuration management
- Apply a vulnerability management program that prioritizes by organizational risk—identifying, assessing, and addressing vulnerabilities before they are exploited
- Recognize and respond to the full attack lifecycle—from initial compromise through lateral movement, persistence, and exfiltration—including ransomware-specific defense strategies
- Use Windows and Linux command-line tools to identify high-risk indicators of compromise and automate continuous monitoring through scripting
- Evaluate the security posture of cloud environments across major providers, understanding the distinctions between shared responsibility models and the security implications
- Construct an incident response plan that is built, tested, and operational before it is needed—not assembled under pressure after a compromise has occurred
- Return to work on the first day after class and apply what you learned—that is the standard this course is built to meet

GSEC
Security Essentials
giac.org/gsec

GIAC Security Essentials

The GIAC Security Essentials (GSEC) certification validates that a practitioner's security knowledge extends beyond terminology into application. GSEC holders have demonstrated the ability to perform hands-on security tasks—a distinction that matters to employers evaluating whether a credential reflects competence or simply familiarity.

Organizations are under constant threat—and not all of those threats will be stopped. The more important question is not whether an adversary will find a way in. It is how quickly you will find them once they do. The longer an adversary remains in your environment undetected, the greater the damage becomes. Timely detection and response are not aspirational goals. They are operational requirements.

SEC401 is built around that reality. Across more than 30 information security topic areas—network security, cloud environments, identity management, cryptography, vulnerability management, endpoint hardening, and more—the course establishes the foundational knowledge that makes every subsequent security decision more informed, more defensible, and more effective. This is not specifically entry-level content. These are the load-bearing concepts of the discipline: the ones that, when missing, no amount of specialization fully compensates for.

Offense informs defense. That principle runs throughout SEC401—in the attack methodologies examined, in the real-world compromise scenarios worked through in the labs, and in the direct connection drawn between what adversaries do and what defenders must understand to stop them. What you learn here will be applicable when you return to work. That is the **SANS Promise**.

Enhanced Labs Overview

SEC401 features 20 hands-on labs spanning the full breadth of the course—from network traffic analysis and cryptographic validation to intrusion detection, container security, and Windows and Linux security. Select labs now incorporate AI assistance, reflecting the reality that AI tools are already part of the modern security practitioner's workflow. The lab environment is built around real tools, real scenarios, and real decisions—because proficiency developed in an artificial environment does not transfer.

Business Takeaways

- Establish a security program built on defensible architecture principles—one that can be explained, justified, and measured at the organizational level
- Develop a vulnerability management approach that prioritizes by actual organizational risk
- Reduce organizational risk through systematic hardening and configuration management across every major platform: Windows, Linux, and macOS
- Articulate the connection between foundational security controls and the adversarial tactics they are designed to defeat—a capability that directly improves security investment decisions
- Return to work on day one with skills, frameworks, and tools that are immediately applicable to your organization's specific security challenges

Hands-On Cybersecurity Training

The hands-on labs in SEC401 follow the security team at Alpha Incorporated—a fictitious global organization working through four real-world compromise scenarios: An AWS server compromise, a USB device containing sensitive documents, a phishing attack, and a development environment pushed prematurely to production. Each scenario is drawn from the types of incidents organizations actually face, and each requires applying the course concepts directly. This is how SEC401 fulfills the **SANS promise: what you learn in this course will be immediately applicable when you return to work.**

Section Descriptions

SECTION 1: Network Security and Cloud Essentials

Within any organization, not all data holds equal value. Some information is routine; other data is so sensitive that its loss causes irreparable damage. That distinction directly determines where your defenses are focused and where the consequences of a gap are most severe—and it begins with understanding how modern network communication protocols behave and where they are vulnerable. Cloud computing is not a separate conversation from network security. It is a continuation of it. Artificial intelligence enters here as well—not as a standalone topic, but because AI-driven solutions increasingly operate within cloud environments, and the gap between what AI actually is and what most people assume it to be has direct security implications. Adversaries rely on our networks as much as we do. They move laterally, pivot relentlessly, and exploit the infrastructure we built for our own purposes. Understanding how your network functions is what makes adversarial movement visible. You cannot see what you do not understand. Wireless networking compounds this reality—it is simultaneously the most pervasive and least understood component of most organizations' network infrastructure.

TOPICS: Defensible Network Architecture; Protocols and Packet Analysis; Virtualization, Cloud, and AI Essentials; Securing Wireless Networks

SECTION 2: Defense in Depth

No single control stops every threat. That is not a failure of security—it is the reality that defense-in-depth is designed to address. This section builds the layered defensive strategy every organization needs: from information assurance and its foundational commitment to confidentiality, integrity, and availability, through identity and access management—increasingly the security perimeter for cloud-based systems—to modern authentication, password security, and passkeys. From there, the section turns to the frameworks that structure defensive decision-making: the CIS Controls, the NIST Cybersecurity Framework, and the MITRE ATT&CK knowledge base. These are not compliance checkboxes. They are the organized intelligence of the security community, distilled into actionable guidance—and the difference between a reactive security program and a deliberate one.

TOPICS: Defense-in-Depth; IAM, Authentication, and Password Security; Security Frameworks; Data Loss Prevention; Mobile Device Security

SECTION 3: Vulnerability Management & Response

Every compromise begins somewhere. Section 3 addresses the full arc of that reality—from the vulnerabilities that give adversaries their initial foothold, through the attack methodologies they use to exploit them, to the detection capabilities that make post-compromise activity visible, and finally to the incident response discipline that determines how effectively an organization recovers. The adversary understands every stage. So should you. Vulnerability management opens the section—not as an abstract concept, but as a measurable condition that exists in every environment. Without a systematic program to identify and prioritize vulnerabilities, security investment is reactive at best and misdirected at worst. Because vulnerabilities are what adversaries exploit, understanding them requires understanding how adversaries actually use them—including web applications, which consistently represent some of the greatest organizational risk and receive an entire dedicated module. Logging capabilities built into hardware and software are not compliance artifacts. They are detection infrastructure. The section closes with incident response—because detection without a structured response plan is incomplete. That plan is built, tested, and maintained long before it is needed.

TOPICS: Vulnerability Assessments; Penetration Testing; Attacks and Malicious Software; Web Application Security; Security Operations and Log Management; Digital Forensics and Incident Response

SECTION 4: Data Security Technologies

Section 4 addresses the technologies that form the operational core of a defensive security program—beginning with the one most frequently misapplied: cryptography. Powerful when deployed correctly, cryptography produces something considerably more dangerous than weak security when deployed incorrectly—it produces the illusion of security. The section examines cryptographic concepts practically: what they protect, how they work, where they fail, and what the quantum computing threat means for the cryptographic standards organizations rely on today. From there, the section turns to prevention and detection technologies—firewalls, intrusion prevention systems, and intrusion detection systems—deployed at both the network and endpoint levels. Knowing these technologies exist is not sufficient. Understanding how they work, where they fail, and how they complement each other is what makes them defensible choices rather than assumed ones.

TOPICS: Cryptography; Cryptography Algorithms and Deployment; Applying Cryptography; Network Security Devices; Endpoint Security

SECTION 5: Windows and Azure Security

Windows remains the most widely used and most targeted desktop operating system in the world—and those two facts are not unrelated. Section 5 addresses Windows security in the context of what the Windows ecosystem actually looks like today: Active Directory, Azure, PowerShell, PKI, BitLocker, Microsoft 365, Hyper-V, and more. The Windows of small workgroups and simple desktops is not the Windows most organizations are defending. This section is built around the Windows that is. What was once a contained environment is now a complex, hybrid infrastructure. Each expansion of that ecosystem introduced new capabilities—and new attack surface that the previous generation of Windows administration was never designed to address. Windows security in this context is the intersection of identity management, access control, endpoint hardening, automation, and cloud security. This section works through all of it—on-premises and Azure—with automation and auditing treated as operational necessities, not optional enhancements.

TOPICS: Windows Security Infrastructure; Windows as a Service; Windows Access Controls; Enforcing Security Configurations; Microsoft Cloud Computing; Automation, Logging, and Auditing

SECTION 6: Containers, Linux, and Mac Security

The final section of SEC401 addresses the operating systems and deployment models that complete the modern enterprise environment—Linux and macOS. Each presents its own security model, its own strengths, and its own commonly misunderstood limitations. Linux systems are often fewer in number than Windows systems—but they are frequently the most critical. Database servers, web servers, and cloud infrastructure disproportionately run on Linux, which means the consequences of a Linux compromise are disproportionately severe. This section addresses Linux security practically and deliberately: foundational concepts for those newer to the platform, and advanced guidance for administrators who manage it daily. Both audiences will find content that challenges what they think they already know. Containers enter the discussion here because Linux is where they were born. Built on the principle of minimization, containers offer deployment flexibility central to modern cloud computing. That same principle aligns naturally with defense-in-depth—but containers introduce security considerations that organizations adopting them primarily for operational convenience frequently overlook. macOS closes the course for a specific reason. Its security reputation is partly deserved and partly myth. This section separates the reality from the reputation—giving security professionals an accurate basis for the decisions they make about macOS in their environments.

TOPICS: Linux Fundamentals: Containerized Security; Linux Security Enhancements and Infrastructure; macOS Security

Who Should Attend

SEC401 is designed for security professionals at every stage of their career—not because the content is adjusted for different audiences, but because the foundational gaps this course addresses are not exclusive to any single experience level or job title.

You should attend if:

- You work in InfoSec—**as a practitioner, engineer, administrator, or analyst**—and want a comprehensive, current understanding of the concepts your daily work depends on
- **You manage security teams or security budgets** and need the technical grounding to make defensible decisions, not just informed ones
- You specialize in a specific security discipline—**forensics, penetration testing, cloud security, incident response**—and recognize that specialization built without foundational grounding has limits
- You are **new to InfoSec** and want to build the foundation that every subsequent course, certification, and career decision will rest upon
- You are an IT professional—**engineer, administrator, or supervisor**—whose responsibilities increasingly intersect with security and who needs a structured, rigorous path into the discipline

NICE Framework Work Roles

- Security Control Assessor (OPM 612)
- Database Administrator (OPM 421)
- Data Analyst (OPM 422)
- Technical Support Specialist (OPM 411)
- Network Operations Specialist (OPM 441)
- System Administrator (OPM 451)
- Systems Security Analyst (OPM 461)
- Cyber Instructional Curriculum Developer (OPM 711)
- IT Investment/Portfolio Manager (OPM 804)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Infrastructure Support Specialist (OPM 521)