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

GIAC CERTIFICATIONS

SEC401:™ Security Essentials – Network, Endpoint, and Cloud™

GSEC
Security Essentials
giac.org/gsec

6	46	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Create a security program that is built on a foundation of detection, response, and prevention
- Know practical tips and tricks that focus on addressing high-priority security concerns within one's organization and doing the right things that lead to effective security solutions
- Understand how adversaries adapt their tactics, techniques, and procedures and how to adapt your defense accordingly
- Know what ransomware is and how to better defend against it
- Leverage a defensible network architecture (VLANs, NAC, 802.1x, Zero Trust) based on indicators of compromise
- Understand the Identity and Access Management (IAM) methodology and related aspects of strong authentication (MFA)
- Leverage the security strengths and differences among various cloud providers (including multicloud)
- Know realistic and practical applications of a capable vulnerability management program
- Sniff network communication protocols to determine the content of network communication (including access credentials) using tools such as tcpdump and Wireshark
- Use Windows, Linux, and macOS command line tools to analyze a system looking for high-risk indicators of compromise, as well as the concepts of basic scripting for the automation of continuous monitoring
- Build a network visibility map that can be used to validate attack surfaces and determine the best methodology to effectively reduce risk through hardening and configuration management
- Understand why some organizations win and why some lose when it comes to cybersecurity

GSEC
Security Essentials
giac.org/gsec

GIAC Security Essentials

The GIAC Security Essentials (GSEC) certification validates a practitioner's knowledge of information security beyond simple terminology and concepts. GSEC certification holders are demonstrating that they are qualified for hands-on IT systems roles with respect to security tasks.

Organizations are under constant threat, and it is critical to be prepared for eventual compromise. Now, more than ever, timely detection and response are essential. The longer an adversary remains in your environment, the greater the damage becomes. Perhaps the most vital question in information security today is: "How quickly can we detect, respond to, and remediate an adversary?"

Information security is about focusing your defenses on the areas that matter most, particularly as they relate to the unique needs of your organization. In SEC401, you will learn the foundational language and inner workings of computer and information security, and how to apply them effectively to your specific challenges. You'll acquire the critical knowledge needed to secure systems and organizations with confidence.

SEC401 teaches you the most effective steps to prevent attacks and detect adversaries, equipping you with actionable techniques you can immediately apply in your workplace. Through practical tips and insights, you'll be better prepared to win the ongoing battle against a broad range of cyber adversaries who seek to infiltrate your environment.

New and Enhanced Labs Overview

Unlock the critical skills needed to defend systems and networks with the latest additions to SEC401, now featuring 20 state-of-the-art labs. These labs have been carefully designed to offer hands-on experience, providing practical skills essential for addressing today's complex cybersecurity challenges.

Each lab is crafted to build proficiency in using real-world tools and techniques, preparing you to effectively respond to a variety of security incidents. Whether you are new to cybersecurity or seeking to update your skills, these labs offer a practical, immersive learning experience in the critical aspects of security fundamentals.

Business Takeaways

- How to address high-priority security concerns
- Leverage security strengths and differences among the top cloud providers
- Build a network visibility map to help validate attack surface
- Reduce an organization's attack surface through hardening and configuration management

Hands-On Cybersecurity Training

The lab-based hands-on portion of the course allows students to apply and master course concepts. The labs follow the adventures of the security team at Alpha Incorporated, a fictitious organization that has suffered from a series of compromises. With the labs based upon four real-world scenarios that many organizations face in today's modern world, students walk away with a keen understanding of the real-world challenges they will face throughout their career. Mastering the course concepts by way of hands-on exercise facilitates the spirit of fulfilling the SANS promise: what is learned in the course is immediately applicable at work.

> **"SEC401 gives you a fantastic knowledge base to build on, and I would say it's essential for anyone working in cybersecurity."**
>
> —Thomas Wilson, **Agile Systems**

sans.org/sec401

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

Section Descriptions

SECTION 1: Network Security and Cloud Essentials

In the first section, we explore the reality that while organizations strive to prevent as many attacks as possible, not all threats will be stopped. Therefore, timely detection becomes critical. Understanding how to construct a defensible network architecture—along with the various network designs and communication flows—is essential to responding effectively. Next, we examine how, within any organization, not all data holds equal value. Some information may be routine, while other data is highly sensitive and critical, with its loss potentially causing irreparable damage. Cloud computing naturally comes into focus as part of modern public and private network discussions. No conversation about defensible networking would be complete without addressing the cloud—its security features, capabilities, and associated concerns. Additionally, we explore artificial intelligence (AI) in this context, discussing its fundamentals and what AI truly means versus common misconceptions. By the end of this section, you will have a solid understanding of defensible network architecture, protocols and packet analysis, virtualization and cloud fundamentals (including AI), and wireless network security.

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

SECTION 2: Defense in Depth

This section of the course explores large-scale threats to our systems and the strategies for defending against them, emphasizing the need for layered protection, known as defense-in-depth. We begin by laying the groundwork for information assurance, examining how security threats impact the confidentiality, integrity, and availability of our systems. Midway through this section, we shift focus to contemporary security controls that are effective against today's adversaries. We do this by examining frameworks such as the Center for Internet Security (CIS) Controls, the NIST Cybersecurity Framework, and the MITRE ATT&CK knowledge base. We conclude this section with a dedicated module on mobile devices, examining both the benefits and the security risks they present.

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

SECTION 3: Vulnerability Management and Response

In this section, we turn our attention to the various areas within our environment where vulnerabilities can emerge. We begin by defining what constitutes a vulnerability and how to establish an effective vulnerability assessment program. Since vulnerabilities represent the weaknesses that adversaries exploit, a discussion on this topic must also include an in-depth examination of modern attack methodologies, with real-world examples of compromises. Among the potential areas for vulnerabilities, web applications pose some of the greatest risks, often leading to the most severe consequences. While vulnerabilities may provide adversaries with easy access to systems, it's important to remember that their actions post-compromise can often be detected. By effectively leveraging the logging capabilities of hardware and software, we can detect adversarial activity more quickly. This capability is covered in our penultimate module, which focuses on Security Operations and Log Management. Finally, it's crucial to have a well-structured response plan for handling any compromises. The methodology for an appropriate incident response is the focus of the final module in this section.

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

There is no single solution that guarantees complete security, but one technology that can address many security challenges--though often improperly deployed—is cryptography. In the first half of this section, we will delve into various cryptographic concepts and explore how they can be effectively used to safeguard an organization's assets. In the second half, our focus shifts to prevention technologies that can stop adversaries from gaining access to your organization. This includes the use of firewalls and intrusion prevention systems. We will also examine detection technologies, such as intrusion detection systems, which can identify the presence of an adversary. These prevention and detection methods can be deployed at both the network and endpoint levels, and we will discuss the similarities and differences in their implementation.

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

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

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)

SECTION 5: Windows and Azure Security

Remember when Windows was simple? Back in the days of Windows XP desktops in small workgroups, things seemed straightforward. But much has changed. Today, we manage Windows tablets, Azure, Active Directory, PowerShell, Microsoft 365 (formerly Office 365), Hyper-V, Virtual Desktop Infrastructure, and more. As Microsoft competes with cloud giants like Google and Amazon, securing the cloud has become a critical challenge. Windows remains the most widely used and targeted desktop operating system globally. At the same time, the complexities of Active Directory, Public Key Infrastructure (PKI), BitLocker, endpoint security, and user access control present both challenges and opportunities. This course section will guide you through mastering the essentials of Windows security while introducing tools that can streamline and automate your work, whether on-premises or in the cloud with Microsoft Azure. By the end of this section, you'll have a solid foundation in Windows security, including automation and auditing within the Windows ecosystem.

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

While organizations may not have a large number of Linux systems, those they do have are often the most critical and require the highest levels of protection. This course section focuses on providing practical guidance to enhance the security of any Linux system. It offers step-by-step instructions with foundational background for Linux beginners, as well as advanced security advice and best practices for administrators of varying expertise levels. Given Linux's reputation as a free and open-source operating system, it's no surprise that many advanced security concepts are first developed for Linux. One notable example is containers, which offer powerful and flexible capabilities for cloud computing deployments. Although containers weren't initially designed for security purposes, they are built on the principle of minimization, which can be leveraged as part of a defense-in-depth security strategy. We will explore what containers represent for information security, what they do not, and best practices for their management. Finally, we conclude this section with a review of Apple's macOS, which is built on a UNIX foundation. Despite its robust hardware and software security features, macOS is often misunderstood regarding what it can and cannot achieve in terms of security.

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