SEC401: SANS Security Essentials: Network, Endpoint and Cloud

GSEC Security Essentials giac.org/gsec

6 Day Program	46 CPEs	Laptop Required

You Will Be Able To

- Understand the core areas of cybersecurity and how to create a security program that is built on a foundation of Detection, Response, and Prevention
- Apply practical tips and tricks that focus on addressing high-priority security problems within your organization and doing the right things that lead to security solutions that work
- Understand how adversaries adapt tactics and techniques, and importantly how to adapt your defense accordingly
- Know what ransomware is and how to better defend against it
- Leverage a defensible network architecture (VLANs, NAC, and 802.1x) based on advanced persistent threat indicators of compromise
- Understand the Identity and Access Management (IAM) methodology, including aspects of strong authentication (Multi-Factor Authentication)
- Leverage the strengths and differences among the top three cloud providers (Amazon, Microsoft, and Google), including the concepts of multi-cloud
- Identify visible weaknesses of a system using various tools and, once vulnerabilities are discovered, configure the system to be more secure (realistic and practical application 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 the attack surface and determine the best methodology to reduce the attack surface through hardening and configuration management
- Know why some organizations win and some lose when it comes to security, and most importantly, how to be on the winning side

This course will show you the most effective steps to prevent attacks and detect adversaries with actionable techniques that can be used as soon as you get back to work. You'll learn tips and tricks designed to help you win the battle against the wide range of cyber adversaries that want to harm your environment.

Organizations are going to be targeted, so they must be prepared for eventual compromise. Today more than ever before, TIMELY detection and response is critical. The longer an adversary is present in your environment, the more devastating and damaging the impact becomes. The most important question in information security may well be, "How quickly can we detect, respond, and REMEDIATE an adversary?"

Information security is all about making sure you focus on the right areas of defense, especially as applied to the uniqueness of YOUR organization. In SEC401 you will learn the language and underlying workings of computer and information security, and how best to apply them to your unique needs. You will gain the essential and effective security knowledge you will need if you are given the responsibility to secure systems and/or organizations.

Whether you are new to information security or a seasoned practitioner with a specialized focus, SEC401 will provide the essential information security skills and techniques you need to protect and secure your organization's critical information and technology assets, whether on-premise or in the cloud. SEC401 will also show you how to directly apply the concepts learned into a winning defensive strategy, all in the terms of the modern adversary. This is how we fight; this is how we win!

Is SEC401: Security Essentials: Network, Endpoint, and Cloud the right course for you?

Ask yourself the following questions:

- Do you fully understand why some organizations become compromised and others do not?
- If there were compromised systems on your network, are you confident that you would be able to find them?
- Do you understand the effectiveness of each security control and are you certain that they are all configured correctly?
- Are the proper security metrics set up and communicated to your executives to help drive the best security decisions?

SEC401 provides the information security knowledge necessary to help you answer these questions, delivered in a bootcamp-style format and reinforced with hands-on labs.

"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**

Section Descriptions

SECTION 1: Network Security & Cloud Essentials

A typical way attackers gain access to a company's resources is through a network connected to the Internet. Organizations try to prevent as many attacks as possible, but since not all attacks will ultimately be prevented, they must be detected in a timely manner. Therefore, an understanding of and ability to create and identify the goals of building a defensible network architecture are critical. A defensible network would not be complete without an in-depth understanding of what the cloud is and, more importantly, the security abilities (and related concerns) of the cloud that must also be taken into account. It is just as important to know and understand the architecture of the system, types of designs, communication flow and how to protect against attacks using devices such as routers and firewalls. These essentials, and more, will be covered in this first section in order to provide a firm foundation for the consecutive sections of training.

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

SECTION 3: Vulnerability Management and Response

Vulnerabilities represent weaknesses that adversaries exploit. In this section you will discover various areas where vulnerabilities arise. The section begins with vulnerability assessments and penetration testing, then move into attack methodologies and conclude with how to create a proper response plan.

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

SECTION 5: Windows and Azure Security

Remember when Windows was simple? Windows XP desktops in a little workgroup...what could be easier? A lot has changed over time. Now, we have Windows tablets, Azure, Active Directory, PowerShell, Office 365, Hyper-V, Virtual Desktop Infrastructure (VDI), and so on. Microsoft is battling Google, Apple, Amazon.com, and other cloud giants for supremacy. The trick is to do it securely, of course. Windows is the most widely-used and targeted operating system on the planet. At the same time, the complexities of Active Directory, Public Key Infrastructure, BitLocker, AppLocker, and User Account Control represent both challenges and opportunities. This section will help you quickly master the world of Windows security while showing you the tools that can simplify and automate your work. You will complete the section with a solid grounding in Windows security by looking at automation, auditing and forensics.

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

SECTION 2: Defense-in-Depth

This course section looks at the "big picture" threats to our systems and how to defend against them. You will learn that protections need to be layered, leveraging a principle called defense-in-depth. Starting with information assurance foundations, we will move into identity and access management (IAM), then progress to modern security controls that work in the presence of an adversary and conclude with the benefits (and security risks) of mobile devices ranging from Bring Your Own Device (BYOD) to Mobile Device Management (MDM).

TOPICS: Defense-in-Depth; Identity and Access Management (IAM); Critical Controls; Authentication and Password Security; Security Frameworks; Data Loss Prevention; Mobile Device Security

SECTION 4: Data Security Technologies

There is no silver bullet when it comes to security. However, there is one technology that would help solve a lot of security issues, though few companies deploy it correctly. This technology is cryptography. Concealing the meaning of a message can prevent unauthorized parties from reading sensitive information. This course section looks at various aspects of encryption and how it can be used to secure a company's assets. A related area called steganography, or information hiding, is also covered.

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

SECTION 6: Linux, Mac and Smartphone Security

While organizations do not have as many Linux systems, those that they do have are often some of the most critical systems that need to be protected. This final section focuses on the practical guidance necessary to improve the security of any Linux system. The day combines practical "how to" instructions with background information for Linux beginners, as well as security advice and best practices for administrators with various levels of expertise. You will learn what containers are, what they do and best practices for their management. Next you will learn about Linux and UNIX concepts, discuss AWS in relation to Microsoft Azure and end the course with a through review of Apple's MacOS.

TOPICS: Linux Fundamentals: Linux Security Enhancements and Infrastructure; Containerized Security; AWS Fundamentals; AWS Security Controls, AWS Hardening; macOS Security

"Excellent material for security professionals wanting a deeper level of knowledge on how to implement security policies, procedures, and defensive mechanisms in an organization."

— Brandon Smit, **Dynetics**

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

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.

- Active defense, defense in depth, access control and password management
- Cryptography: basic concepts, algorithms and deployment, and application
- Defensible network architecture, networking and protocols, and network security
- Incident handling and response, vulnerability scanning and penetration testing
- Linux security: structure, permissions, and access; hardening nd securing; monitoring and attack detection; and security utilities
- Security policy, contingency plans, critical controls and IT risk management
- Web communication security, virtualization and cloud security, and endpoint security
- Windows: access controls, automation, auditing, forensics, security infrastructure, and securing network services