SEC401: SANS Security Essentials: Network, Endpoint and Cloud

Course Overview

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.

Job Roles

- Security Professionals
- Security Managers
- Operations Personnel
- Forensic Analysts
- Penetration Testers
- It Engineers And Supervisors
- Security Administrators
- Auditors

Intended Audience

- 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

Duration

6 Days

Certifications

GIAC Security Essentials (GSEC)

Contact Us

800.674.3550

2151 W. Hillsboro Blvd.
Suite 210
Deerfield Beach, FL 33442

Connect with us

APPLIED TECHNOLOGY ACADEMY

Sign Up Today!

SEC401: SANS Security Essentials: Network, Endpoint and Cloud

APPLIED TECHNOLOGY ACADEMY

Course Outline

SECTION 1: Network Security & Cloud Essentials

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

SECTION 2: Defense-in-Depth

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

SECTION 3: Vulnerability Management and Response

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

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

SECTION 5: Windows and Azure Security

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

SECTION 6: Linux, Mac and Smartphone Security

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

Course Objectives

- 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

GIAC Security Essentials (GSEC)

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 and 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