Master Network, Endpoint & Cloud Security | SEC410 Training

12 – 16 October 2026
San Diego

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Master Network, Endpoint & Cloud Security | SEC410 Training

Ref: 72_86976 **Date:** 12 – 16 October 2026 **Location:** San Diego **Fees:** 14000 Euro

Course Overview:

This course provides foundational knowledge and hands-on skills essential for defending systems and networks. Covering the full scope of modern cybersecurity, SEC410 focuses on security across network, endpoint, and cloud environments. Participants will develop practical expertise in cryptography, OS hardening, access control, security operations, and incident response. The course is mapped directly to the GIAC Security Essentials Certification GSEC.

Target Audience:

- InfoSec professionals
- System and Network Administrators
- IT Support and Helpdesk Staff
- Junior SOC Analysts
- Security Engineers and Technicians

Targeted Departments:

- IT & Cybersecurity
- Security Operations Centers SOC
- Cloud and Network Teams
- Risk Management and Audit
- Compliance and Infrastructure

Course Offerings:

By the end of this course, participants will be able to:

- Understand and apply core cybersecurity principles and defense strategies
- Secure communication using cryptographic methods and tools
- Implement endpoint hardening and user access controls
- Analyze network traffic and secure common protocols
- Respond to incidents using SIEM tools and detection methods
- Securely manage cloud platforms AWS/Azure using best practices
- Prepare for and pass the GIAC GSEC certification exam

Training Methodology:

- Instructor-led sessions
- Hands-on labs and simulations
- Group-based threat modeling and review
- Real-world case studies and cyber hygiene exercises
- Practice quizzes and exam walkthroughs

Course Toolbox:

- Wireshark, PowerShell, Linux CLI
- Sample GSEC practice test
- Secure configuration templates
- SIEM event analysis scenarios
- Cryptographic tools demo

Course Agenda:

Day 1: Cybersecurity Foundations and Cryptography

- **Topic 1:** Introduction to Cybersecurity and GIAC GSEC Overview
- **Topic 2:** Core Security Concepts: Threats, CIA Triad, and Controls
- **Topic 3:** Cryptographic Terminology, Symmetric & Asymmetric Encryption
- **Topic 4:** Hashing, HMAC, and Digital Certificates
- **Topic 5:** Authentication Models and Access Control Mechanisms
- **Topic 6:** Managing Identity and Password Security
- **Reflection & Review:** Crypto tools lab and access control scenarios

Day 2: Network Security and Protocol Defense

- **Topic 1:** Networking Basics: IP, TCP/UDP, and Common Attacks
- **Topic 2:** Network Defense Models: Firewalls, IDS, and Zero Trust
- **Topic 3:** Secure Protocols: SSH, SSL/TLS, VPN, and DNSSEC
- **Topic 4:** Web and Email Security: HTTPS, Certificates, SPF, DKIM
- **Topic 5:** Packet Capture and Protocol Analysis Wireshark Lab
- **Topic 6:** Network Segmentation and Secure Architecture
- **Reflection & Review:** Traffic inspection and protocol hardening

Day 3: Endpoint and OS Security Windows & Linux

- **Topic 1:** Windows Security Fundamentals: GPOs and User Rights
- **Topic 2:** Linux Security Principles: Permissions, sudo, and Logs
- **Topic 3:** Secure Configuration and Hardening Techniques
- **Topic 4:** Endpoint Detection & Response EDR Concepts
- **Topic 5:** PowerShell and Bash for Security Tasks
- **Topic 6:** Mobile and Device Security Basics MDM, BYOD
- **Reflection & Review:** OS hardening exercises and access audit

Day 4: Security Operations and Cloud Fundamentals

- **Topic 1:** Introduction to SIEM and Log Analysis Techniques
- **Topic 2:** Cloud Security Principles Shared Responsibility, IAM
- **Topic 3:** Monitoring and Incident Response Procedures
- **Topic 4:** Vulnerability Management and Patch Strategy
- **Topic 5:** Penetration Testing Basics and Exploit Prevention
- **Topic 6:** Securing Virtual Environments and Cloud Workloads
- **Reflection & Review:** SIEM lab and cloud misconfiguration demo

Day 5: GSEC Preparation and Career Readiness

- **Topic 1:** GSEC Exam Strategy and Practice Questions Review
- **Topic 2:** Mapping Learning to Job Roles and Cybersecurity Tracks
- **Topic 3:** Developing Enterprise Security Policies and Controls
- **Topic 4:** Final Hands-on Lab: Network & Endpoint Defense Scenario
- **Topic 5:** Career Planning: Analyst, SOC, Cloud Security Roles
- **Topic 6:** Review Checklist, FAQs, and Certification Readiness
- **Reflection & Review:** Q&A, Exam Simulation, and Course Wrap-up

FAQ:

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

No formal prerequisites are required. However, basic familiarity with IT systems, operating systems, or networking concepts is helpful. This course is designed as a practical entry point into cybersecurity.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session is generally structured to last around 4–5 hours, including breaks. The total course duration spans five days, totaling approximately 20–25 hours of guided instruction.

Why is understanding the shared responsibility model critical in cloud security?

In cloud environments such as AWS or Azure, security responsibilities are divided between the cloud provider and the customer. Misunderstanding this model can lead to critical misconfigurations, such as unprotected data storage or insecure IAM roles, making it vital for learners to grasp this concept early in their cloud security journey.

How This Course is Different from Other Security Essentials Courses:

Unlike generic cybersecurity foundations courses, SEC410: Security Essentials – Network, Endpoint, and Cloud offers a deeply practical, real-world approach to security fundamentals. What makes this course unique is its balanced focus across network security, endpoint protection, and cloud-based defenses, ensuring participants build a truly well-rounded skillset. Rather than relying solely on theoretical concepts, SEC410 incorporates live demonstrations and guided tool-based exercises using real security utilities like Wireshark, PowerShell, and cloud IAM configurations.

Additionally, this course is designed in full alignment with the GIAC GSEC certification framework, helping participants not only understand security concepts but also apply them in exam scenarios and job-related challenges. It also distinguishes itself by bridging the gap between traditional IT security and modern cloud environments, offering up-to-date content on AWS, Azure, and virtualization risks.