GIAC Security Essentials Certification (GSEC) Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The GIAC Security Essentials Certification (GSEC) training is the definitive entry point for cybersecurity professionals seeking to master foundational information security principles and achieve a globally recognized, DoD-approved credential. This intensive, hands-on course goes far beyond theoretical concepts, diving deep into network security, cloud security, endpoint defense, cryptography, and incident response. We empower participants to build a robust defense-in-depth architecture and apply real-world security controls using industry-standard tools. Graduates gain the technical proficiency to manage and secure critical IT assets, making them immediate contributors to an organization's cyber defense strategy in the face of evolving threat landscapes.

GIAC Security Essentials Certification (GSEC) Training Course is specifically designed to bridge the gap between theoretical knowledge and practical, technical cybersecurity skills. By focusing on active defense, vulnerability management, and the operational aspects of security administration, the training prepares students for the rigorous GSEC certification exam, which includes CyberLive hands-on questions. The curriculum is constantly updated to cover trending areas like Zero Trust architecture, container security, and the integration of AI/ML in security operations. Successful completion not only validates a candidate?ÇÖs expertise in core security domains but also establishes a solid career pathway towards advanced roles in penetration testing, security engineering, and cloud security architecture.

Programme Curriculum

GIAC Security Essentials Certification (GSEC) Training Course

Introduction

The GIAC Security Essentials Certification (GSEC) training is the definitive entry point for cybersecurity professionals seeking to master foundational information security principles and achieve a globally recognized,

DoD-approved credential. This intensive, hands-on course goes far beyond theoretical concepts, diving deep into network security, cloud security, endpoint defense, cryptography, and incident response. We empower participants to build a robust defense-in-depth architecture and apply real-world security controls using industry-standard tools. Graduates gain the technical proficiency to manage and secure critical IT assets, making them immediate contributors to an organization's cyber defense strategy in the face of evolving threat landscapes.

GIAC Security Essentials Certification (GSEC) Training Course is specifically designed to bridge the gap between theoretical knowledge and practical, technical cybersecurity skills. By focusing on active defense, vulnerability management, and the operational aspects of security administration, the training prepares students for the rigorous GSEC certification exam, which includes CyberLive hands-on questions. The curriculum is constantly updated to cover trending areas like Zero Trust architecture, container security, and the integration of AI/ML in security operations. Successful completion not only validates a candidate?ÇÖs expertise in core security domains but also establishes a solid career pathway towards advanced roles in penetration testing, security engineering, and cloud security architecture.

Course Duration

5 days

Course Objectives

1. Master the Defense-in-Depth strategy and its application in modern security architecture.
2. Implement robust Identity and Access Management (IAM) and Multi-Factor Authentication (MFA) policies.
3. Configure and troubleshoot Network Security Devices, including Firewalls, IDS/IPS, and secure VPNs.
4. Apply Cryptography fundamentals to secure data in transit and at rest using PKI and symmetric/asymmetric algorithms.
5. Perform Vulnerability Assessments and execute fundamental Penetration Testing techniques for risk identification.
6. Understand and secure essential operating systems: Windows Security, Linux Hardening, and MacOS Security best practices.
7. Analyze Malicious Code (Malware, Ransomware, Phishing) and implement effective Exploit Mitigation strategies.
8. Formulate and execute a modern Incident Response lifecycle (NIST/SANS frameworks) to manage security breaches.
9. Implement foundational Cloud Security principles for platforms like AWS and Azure (IaaS/SaaS/PaaS).
10. Manage and analyze Security Logs utilizing SIEM (Security Information and Event Management) for real-time threat detection.
11. Secure Web Applications against common threats like SQL Injection and Cross-Site Scripting (XSS).
12. Establish effective Data Loss Prevention (DLP) and implement Mobile Device Security policies.
13. Integrate modern Security Frameworks like CIS Controls and the NIST Cybersecurity Framework into organizational governance.

Target Audience

1. New Information Security Professionals
2. IT Security Managers/Supervisors
3. System Administrators
4. Network Administrators/Engineers
5. Security Analysts

6. IT Operations Personnel
7. Security Auditors and Compliance Staff
8. Penetration Testers and Forensic Analysts

Course Modules

Module 1: Cyber Security and Defense in Depth

- CIA Triad, Risk Management, Defense-in-Depth Architecture.
- Introduction to NIST Cybersecurity Framework and CIS Critical Controls.
- TCP/IP, OSI Model, and common network protocol vulnerabilities.
- Firewalls, IDS/IPS, and secure router configuration.
- Hardening Wi-Fi networks using WPA3 and addressing common attacks.
- Case Study: The Target Data Breach.

Module 2: Access Control, IAM, and Authentication

- Authentication, Authorization, Accounting model, Least Privilege.
- Implementing Role-Based Access Control and user provisioning.
- Hashing, salting, password storage best practices, and auditing.
- Advanced Authentication: Multi-Factor Authentication and Single Sign-On principles.
- Operating System Access Controls.
- Case Study: The Colonial Pipeline Ransomware Incident.

Module 3: Cryptography and Data Security

- Crypto Foundations
- Digital certificates, Certificate Authorities, and the lifecycle of Public Key Infrastructure.
- Configuring SSL/TLS for web and secure VPNs
- Data Protection: Data Loss Prevention strategies and data classification.
- Mobile Device Management and securing mobile data.
- Case Study: The Equifax Breach.

Module 4: Windows Security Infrastructure

- Windows as a Service, security architecture, and system hardening.
- Understanding Active Directory, Group Policy Objects, and NTFS permissions.
- Implementing essential security baselines and configuration management.
- Using PowerShell for auditing and enforcing security policies.
- Basic security concepts for Azure and Microsoft 365.
- Case Study: The SolarWinds Supply Chain Attack.

Module 5: Linux and Container Security

- Essential commands, file system permissions, and services.
- Best practices for securing the operating system, user accounts, and services.
- Configuring system logging and log analysis for security events.
- Introduction to Docker/Kubernetes security and securing images/runtime.
- Key security features and hardening of macOS systems.
- Case Study: The Docker Hub Credential Theft.

Module 6: Vulnerability Management and Penetration Testing

- Using tools like Nessus or OpenVAS for vulnerability identification.
- Establishing a rigorous and timely patching process.
- Scoping, information gathering, scanning, and exploitation phases.
- Common threats like SQL Injection, XSS, and the OWASP Top 10.
- Understanding common attack types and defensive countermeasures.
- Case Study: A Major Retailer's Third-Party Hack.

Module 7: Malicious Code and Endpoint Defense

- Ransomware, Viruses, Worms, Trojans, and Spyware.
- Techniques like Phishing and Pretexting, and awareness training.
- Deployment and management of traditional AV and modern EDR solutions.
- Importance of centralized logging and log parsing techniques.
- Using a SIEM to correlate events and detect anomalies in real-time.
- Case Study: The WannaCry Ransomware Outbreak.

Module 8: Incident Response and Cloud Essentials

- Incident Response Plan.
- Digital Forensics.
- Risk Management.
- Cloud Fundamentals.
- Securing the Cloud
- Case Study: A Cloud-Based Financial Service Breach.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com