Global Horizon
TRAINING CENTER

Training Course:
SEC501: Advanced Security Essentials – Enterprise Defender

26 - 30 April 2026
Beirut (Lebanon)

Training Course:
SEC501: Advanced Security Essentials Enterprise Defender

Training Course code: IT236415 From: 26 - 30 April 2026 Venue: Beirut (Lebanon) - Training Course Fees: Euro

Introduction

It costs enterprises worldwide billions of dollars annually to respond to malware and ransomware attacks. The rapid evolution of threat actors, sophisticated intrusion techniques, and enterprise-wide attack surfaces demand advanced defensive capabilities beyond traditional security controls.

The SEC501: Advanced Security Essentials - Enterprise Defender program, designed and delivered by Global Horizon Training Center, provides cybersecurity professionals with advanced knowledge and practical methodologies to design defensible enterprise architectures, detect sophisticated attacks, conduct penetration testing, perform digital forensics, and execute comprehensive malware analysis.

This expanded 6-day version enhances depth in malware reversing, enterprise remediation strategies, and real-world enterprise attack simulation.

You Will Learn

- Core components of building defensible enterprise network infrastructures
- Formal methodologies for vulnerability assessment and penetration testing
- Advanced attack detection and indicators of compromise IOCs
- Digital forensics and incident response using the six-step IR model
- Malware analysis from automated techniques to manual reverse engineering
- Enterprise-wide containment, remediation, and recovery strategies

Course Objectives

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

- Identify and mitigate advanced network security threats
- Architect resilient enterprise security frameworks
- Perform penetration testing and vulnerability exploitation safely
- Analyze network packets and logs to detect anomalies
- Conduct digital forensic investigations
- Reverse-engineer malware and ransomware samples

- Implement enterprise-wide remediation and security hardening strategies

Target Audience

This program is designed for professionals who are responsible for securing enterprise environments and responding to advanced cyber threats, including:

- Cybersecurity Professionals and Security Engineers
- Network and System Administrators
- Security Operations Center SOC Analysts
- Penetration Testers and Ethical Hackers
- Digital Forensics and Incident Response DFIR Specialists
- IT Security Managers and Team Leaders
- Risk, Compliance, and Governance Professionals
- Cloud Security Engineers and Infrastructure Specialists
- Threat Intelligence Analysts
- IT Professionals seeking to advance into cybersecurity roles

Outlines

Day 1: Network Security Architecture & Infrastructure Protection

- Defensible Network Architecture & Infrastructure Security
- Security Standards & Compliance Frameworks
- Authentication, Authorization & Accounting AAA
- Network Segmentation & Zero Trust Principles
- Securing Routers, Switches & Infrastructure
- Intrusion Prevention Systems & Firewalls
- DNS & Name Resolution Attacks and Defense
- Securing Hybrid & Cloud Infrastructure

Day 2: Penetration Testing & Ethical Hacking Essentials

- Penetration Testing Methodology
- Rules of Engagement & Legal Scope
- Reconnaissance Passive & Active
- Social Engineering Tactics
- Network Mapping & Scanning
- Vulnerability Assessment Tools
- Exploitation Frameworks
- Web Application Exploitation
- Post-Exploitation & Lateral Movement

Day 3: Security Operations & Threat Monitoring

- Security Operations Center SOC Foundations
- Network Security Monitoring
- Advanced Packet Analysis
- Intrusion Detection & Prevention Systems
- Signature Development for Threat Detection

- Event Logging & Correlation
- SIEM Architecture & Analytics
- Continuous Monitoring & Threat Hunting

Day 4: Digital Forensics & Incident Response

- Active Defense Strategies
- Digital Forensics Fundamentals
- Evidence Collection & Chain of Custody
- Incident Response Lifecycle 6-Step Model
- Modern DFIR Techniques
- Scaling Incident Response in Enterprises
- Enterprise Threat Containment Strategies

Day 5: Malware Analysis & Capstone Simulation

- Malware Threat Landscape
- Malware Analysis Methodologies
- Automated & Static Analysis Techniques
- Behavioral & Interactive Analysis
- Sandboxing & Monitoring
- Introduction to Reverse Engineering
- Manual Code Reversing
- Memory Forensics & Volatility
- Ransomware Dissection Techniques
- IOC Creation & Threat Intelligence Integration
- Enterprise-Wide Malware Containment
- Recovery & Security Hardening Roadmap
- Capstone Simulation: Enterprise Attack Scenario

Registration form on the Training Course:
SEC501: Advanced Security Essentials Enterprise Defender

Training Course code: IT236415 From: 26 - 30 April 2026 Venue: Beirut (Lebanon) - Training Course Fees: Euro

Complete & Mail or fax to Global Horizon Training Center (GHTC) at the address given below

Delegate Information

Full Name (Mr / Ms / Dr / Eng): .....
Position: .....
Telephone / Mobile: .....
Personal E-Mail: .....
Official E-Mail: .....

Company Information

Company Name: .....
Address: .....
City / Country: .....

Person Responsible for Training and Development

Full Name (Mr / Ms / Dr / Eng): .....
Position: .....
Telephone / Mobile: .....
Personal E-Mail: .....
Official E-Mail: .....

Payment Method

- ☐ Please find enclosed a cheque made payable to Global Horizon
- ☐ Please invoice me
- ☐ Please invoice my company

Easy Ways To Register

Telephone: +201095004484 to provisionally reserve your place.	Fax your completed registration form to: +20233379764	E-mail to us : info@gh4t.com or training@gh4t.com	Complete & return the booking form with cheque to:Global Horizon 3 Oudai street, Aldouki, Giza, Giza Governorate, Egypt.