Training: OffSec

OffSec SEC-100 CyberCore - Security Essentials

OffSec | Learning Partner

TRAINING GOALS:

SEC-100 CyberCore - Security Essentials is the fundamental course for cybersecurity. Providing learners with the basic understanding of the world of cybersecurity, from an understanding of the terminology and programming skills required, to a broad overview of the offensive, defensive, build, and personal capabilities that an individual should have to launch a career in this growing industry. It creates a foundation for those who know they want a role in cybersecurity but aren't sure where to start. Learners will explore topics such as:

- Understanding the anatomy of cybersecurity and the CIA Triad (Confidentiality, Integrity, Availability), a foundational model that defines core security objectives
- Integrating industry-recognized frameworks like NIST and ISO 27001 to implement effective security practices
- Addressing the risks and vulnerabilities associated with cloud computing as organizations migrate applications and infrastructure to the cloud
- Examining AI's influence in cybersecurity, both as a threat and as a tool to enhance offensive and defensive capabilities
- Exploring what a Penetration Test (Pentest) is, how they are performed, and what their objectives are
- Completing a self-assessment to review skills, and learning how to create a resume or CV that aligns with cybersecurity career opportunities

After completing the course and the labs within them, learners can expect to be prepared to complete the OSCC-SEC exam certification, showcasing their ability to take on information security positions.

Each participant in an authorized OffSec SEC-100 training held at Compendium CE receives a “OffSec CyberCore” license, which includes, among other benefits, a free OSCC-SEC exam voucher.

Objectives

After completing this course, learners will be able to:

- Explain the core concepts of cybersecurity and its evolving landscape
- Describe key cybersecurity frameworks, standards, and roles within organizations
- Develop foundational technical skills in Linux, Windows, and scripting languages like Python and

PowerShell
- Analyze enterprise networking fundamentals, including network firewalls and cloud computing
- Outline the penetration testing process, including information gathering and web attack techniques
- Identify defensive cybersecurity strategies, including SOC management and vulnerability management
- Evaluate methods for mitigating social engineering, phishing, and ransomware threats
- Integrate risk management principles into a comprehensive cybersecurity strategy

Who is this course for?

The course is designed for individuals who are at the beginning of their journey into the cybersecurity field. It's perfect for recent graduates or anyone looking to change careers and enter the world of cybersecurity.

This course is ideal for those who are familiar with computing but not yet experts. If you can navigate a computer, use a web browser, and operate standard applications but feel overwhelmed by the breadth of cybersecurity options and jargon, this course is for you. Whether you're interested in offense, defense or building, intrigued by networking, or curious about scripting and programming, SEC-100 provides a structured and accessible path into the field.

CONSPECT:

- Anatomy of Cybersecurity
  - Understand the fundamental principles of cybersecurity, including common threats, vulnerabilities, and the importance of proactive defense
- Cybersecurity Frameworks and Standards
  - Learn about industry-recognized frameworks like NIST and ISO 27001, which provide guidance for implementing effective security practices
- Cybersecurity Roles
  - Discover the diverse career paths available in cybersecurity, from penetration testers and information security analysts to incident responders and security architects
- Introduction to General Cybersecurity Skills
  - Explore the general skills that apply to roles throughout the cybersecurity industry
- Linux Basics
  - Master the fundamentals of the Linux operating system, a critical skill for cybersecurity professionals due to its prevalence in server environments
- Windows Basics
  - Gain familiarity with the Windows operating system, its security features, and common vulnerabilities exploited by attackers

- Data Transformation Fundamentals
    - Learn how to manipulate and transform data using various techniques, a valuable skill for analyzing security logs and identifying patterns
- Python Scripting Fundamentals
    - Master the basics of Python, a versatile programming language used for automation, scripting security tools, and developing exploits
- PowerShell Scripting Fundamentals
    - Learn the essentials of PowerShell, a powerful scripting language used for automating tasks in Windows environments
- Networking Fundamentals
    - Understand the basics of networking, including protocols, topologies, and how data flows across networks, crucial for understanding how attacks propagate
- Enterprise Network Fundamentals
    - Learn to identify potential vulnerabilities and the ways that breaches can occur
- Introduction to Network Firewalls
    - Explore the basics of firewalls, a key component of every network on the internet
- Cloud Computing Fundamentals
    - Learn about the essential characteristics of cloud computing and the models for deploying and providing cloud resources
- Background to Contemporary Generative AI
    - Explore AI’s potential for malicious use, its defensive applications, and how it’s becoming an increasingly critical attack surface
- Cryptography Fundamentals
    - Dive into the key concepts of cryptography and encryption, and learn about the crucial role they play in modern technology
- Introduction to Offensive Cybersecurity Skills
    - Introduction to the most foundational skills needed for a career in cybersecurity
- Penetration Testing Process
    - Learn what a penetration test is, how it's performed, and what it’s for
- Information Gathering and Enumeration
    - Use Kali Linux for passive and active information gathering
- Understanding Web Attacks
    - Discover how web applications and servers work, and how to assess and defend them
- Attacking Endpoints
    - Outline the most common ways attackers can compromise endpoint systems, elevate privileges, and gather sensitive information from their targets
- Defense Evasion
    - Review the fundamentals of network security and antivirus software

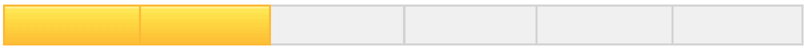
- Offensive Cloud Fundamentals
    - Apply the penetration testing process to cloud environments
- Introduction to Defensive Cybersecurity Skills
    - Explore defensive skills for offensive and defensive security practitioners
- SOC Management Processes
    - Learn about enterprise Security Operations Centers, how they’re organized, and what they do
- Defensive Security Processes
    - Learn about the application of threat hunting and incident response processes
- Vulnerability Management
    - Learn about the lifecycle of software vulnerabilities, how to communicate about vulnerabilities, and how to manage them
- Malware Analysis
    - Learn how to investigate suspected and confirmed malware samples
- Social Engineering and Phishing
    - Explore the different types of social engineering, how to detect it, and why it works
- Ransomware, DDoS, and Availability
    - Learn what ransomware and DDoS attacks are and how to defend against them
- WiFi Security
    - An introduction to wireless terminology and configurations, and how to troubleshoot and defend wireless networks
- Security of Embedded Systems
    - Gain a strong understanding of the basic elements in different kinds of embedded systems
- Industrial Control Systems and OT
    - Learn about Industrial Control Systems, Operational Technology, ICS/OT Security, and the ways they tend to intertwine
- Risk Management in Cybersecurity
    - Understand, analyze, and mitigate risks in cybersecurity
- Introduction to Building Skills for Cybersecurity
    - Highlight the importance of the security mindset in software development and system administration roles
- Software Engineering Security
    - Discover the importance of security in software development and how to incorporate it throughout development
- Foundational Input Validation Concepts
    - Learn how to safely handle user input to avoid errors and prevent vulnerabilities in web applications

- Cloud Architecture Fundamentals
    - Learn foundational cloud computing and cloud-native application architecture concepts and apply them in an AWS lab environment
- Introduction to Assurance Testing
    - Learn assurance testing techniques to mitigate risks in IT systems and how to demonstrate compliance with security standards
- Starting and Developing a Career in Cybersecurity
    - Get prepared to start the search for your first role in cybersecurity. Learn how to find roles that fit your experience, build a strong resume, and prepare for different styles of interviews

REQUIREMENTS:

No prior cybersecurity experience is required. While some IT background can be beneficial, the learning path is designed to introduce fundamental cybersecurity concepts, making it accessible to all.

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Compendium CE (course completion).

The OffSec SEC-100 CyberCore - Security Essentials course and online lab prepares you for the OSCC-SEC certification. Learn more about the OSCC-SEC exam https://help.offsec.com/hc/en-us/articles/27296764876052-OSCC-SEC-Exam-Guide

Each participant in an authorized OffSec SEC-100 training held at Compendium CE receives a "OffSec CyberCore" license, which includes, among other benefits, a free OSCC-SEC exam voucher.

TRAINER:

Authorized OffSec Trainer

ADDITIONAL INFORMATION:

The course includes a license "OffSec CyberCore".

The license includes:

- 1 year of unlimited access to a single 100-level CyberCore course
- 1 year of lab access to associated labs
- Two exam attempts
- 50+ Proving Grounds Play labs
- Bonus access to PEN-103