+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 03/09/2024

Sign up

OSCC™ Certification Training: SEC-100 CYBERCORE

ALL-IN-ONE: EXAM INCLUDED IN PRICE WITH SEC-100 COURSE

3 days (21 hours)

PRESENTATION

The all-new OffSec CyberCore Certified (OSCC SEC-100) certification, released on June 25, 2024, attests to your fundamental skills in cybersecurity and offensive operations.

With our training and curriculum, you'll develop essential practical and theoretical skills, aimed at strengthening your expertise in offensive and defensive techniques, as well as cloud security.

Our training covers crucial aspects such as networking, defensive best practices, cloud security and cryptography. With a perfect balance of in-depth theory and practical lab work, this course offers you comprehensive preparation in the essential disciplines of cybersecurity.

Each module tests your knowledge and skills in specific areas of cybersecurity and offensive exploitation.

OSCC™ training is constantly updated to reflect the latest trends and developments in OffSec IT security.

OBJECTIVES

- Understand the basic concepts of networking and security
- Learn offensive techniques and best defensive practices
- Getting to grips with cloud security architectures
- Study cryptography, operating systems and penetration testing processes
- Acquire an overview of offensive techniques and defensive tactics

TARGET AUDIENCE

- **System administrators**
- Network technicians
- Security Consultants
- Safety researchers
- SOC Analyst

Prerequisites

- Basic computer skills
- Familiarity with Windows and Linux operating systems

Technical requirements

- **Kali Linux** --> Download here
- A computer capable of running three virtual machines with ease
- VMware Workstation 15 or higher
- 64-bit processor with a minimum of 2 cores and support for NX, SMEP, VT-d/IOMMU and VT-x/EPT
- At least 100 GB of available hard disk space
- At least 8 GB RAM
- The only host operating system supported is Windows 10 / 11

Note: Ambient IT does not own OSCC™, this certification belongs to OffSec ® Services LLC.

OUR OSCC™ CERTIFICATION TRAINING PROGRAM

Introduction to CyberSecurity

- General introduction to the course
- The importance of cybersecurity today
- Understanding threats and vulnerabilities
- Cybersecurity roles
- Summary of prerequisite skills
- Training program presentation
- Learning objectives
- Training methodology

Fundamental techniques

- Basic concepts and introduction to AWS
- Introduction to Linux operating systems
- Basic commands and file management
- Introduction to Windows operating systems
- User and file management

Scripts and network

- Introduction to Python programming
- Basic scripts for task automation
- Introduction to PowerShell for Windows administration
- Basic system management scripts
- Basic network concepts
- OSI model and common protocols

Network and Cryptography

- Enterprise network design and management
- Firewall introduction and configuration
- Cryptography principles
- Common algorithms and their use

Penetration testing and attacks

- Intrusion testing steps and methodologies
- Information gathering techniques
- Using Nmap for network reconnaissance
- Common types of web attack
- Prevention and detection techniques
- Attack methods on terminals
- Defense strategies

Privileges and Defense

- Privilege elevation techniques
- Countermeasures
- Techniques for bypassing defense systems
- Best practices for detection
- Attacks specific to cloud environments
- Cloud defense strategies

Management and Analysis

- Managing a Security Operations Center
- Roles and responsibilities
- Identifying and managing vulnerabilities

- Tools and techniques
- Malware analysis techniques
- Prevention and response

Social engineering and Wi-Fi security

- Understanding and detecting social engineering attacks
- Prevention methods
- Types of attack and their impact
- Defense strategies
- Threats and countermeasures for wireless networks

Systems security and career management

- Safety of embedded and industrial control systems
- Fundamental concepts of input validation
- Reliable system design
- Basic concepts and best practices
- Introduction to quality assurance testing
- Risk identification and assessment
- Safe decision-making for the company

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.