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

Updated 02/02/2024

Sign up

Cisco CyberOps Professional™ Training: Certification Preparation

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

2 days (14 hours)

Presentation

Acquiring Cisco CyberOps Professional™ certification demonstrates your advanced expertise as a senior analyst within a security operations center (SOC).
Intervening in incident situations, cloud security, and other responsibilities related to active defensive security.

Our Cisco CyberOps Professional™ training will give you a better understanding of cybersecurity operations.

The exam is made up of several modules, including automating security tasks using scripts, and managing data in common formats. It also covers the use of APIs to automate security operations.

You'll learn to recommend analytical techniques, assess asset security posture and perform malware analysis.

During our exam preparation course, we'll cover all the points and give you all the tips you need.

This training program will also give you an in-depth perspective on incident management, monitoring and user behavior analysis.

Objectives

- Understanding how to use playbooks and the necessary tools

- Applying playbooks to common cybersecurity scenarios
- Mastering industrial compliance standards and risk management
- Use data analysis techniques and improve security controls
- Automate operational safety tasks with advanced concepts

Target audience

- Senior cybersecurity analyst
- SOC Analyst

Prerequisites

- CCNA certification or knowledge of basic networking principles and local network construction
- Understanding how Ethernet and TCP/IP networks work
- Proficiency in Windows & Linux operating systems
- 3 to 5 years' experience in implementing network solutions is recommended

Note: Ambient IT does not own Cisco Certifications™, this certification belongs to Cisco, Inc.

Cisco CyberOps Professional™ training program

Cyber Security Fundamentals

- Understanding playbooks and the tools they require
- Applying playbooks to common scenarios
- Knowledge of industrial compliance standards
- Risk management and cyber-insurance
- Security analysis in cloud environments

Operational safety techniques

- Recommendations for data analysis techniques
- Evaluating and improving safety controls
- System security recommendations
- Using threat and analysis to prevent data loss

Investigation and analysis process

- Threat model analysis
- Survey of common types of cases and attacks
- Complete malware analysis process

- Intrusion and data loss investigations
- Vulnerability screening and risk analysis

Automation and orchestration

- Orchestration and automation concepts and mechanisms
- Script interpretation and modification (Python)
- Automating operational safety tasks
- Data format recognition and automation opportunities
- Use of Bash, CI/CD, and Infrastructure as Code principles

Advanced safety practices

- Implementation of advanced detection and response techniques
- Assessment of operational safety metrics
- Advanced analysis of user and entity behavior
- Use of network analysis and intrusion detection tools
- Exploring the implications of SecDevOps and advanced security practices

Strategy and methods for exam success Mock

exam

Companies concerned

This training 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 inputs from the trainer supported by examples and

brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire is used to check that skills have been correctly acquired.

Sanction

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