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

Updated 06/19/2024

Sign up

Comptia CySA+© training

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

5 days (35 hours)

Presentation

Our CySA+© training course will prepare you for Comptia©'s renowned certification for cybersecurity analysts. This globally recognized qualification will greatly enhance your employability.

Our certification preparation is designed to be comprehensive, covering the essential content of the exam. You'll start with a refresher on threat management, enabling you to effectively detect intrusions and secure access points.

Speaking of threats, you'll learn about best practices for configuring vulnerability scans and analyzing reports. Our training includes a section on incident response: how to categorize threats, the use of forensic tools and communication methods.

You'll learn more about compliance policies, coding practices and IT security tools. Finally, we'll prepare you for the certification exam with case studies.

Objectives

- Know how to use intelligence and threat detection techniques
- Analyze and interpret data
- Identify and correct vulnerabilities
- Suggest preventive measures
- Introduce an effective incident response and recovery process

Target audience

- Cybersecurity Analyst
- Threat Intelligence Analyst
- Cybersecurity Engineer
- Application Security Analyst
- Compliance Analyst
- Threat hunters

Prerequisites

- 3 to 4 years' experience in cybersecurity is recommended
- Fluency in technical English

Note: Ambient IT is not the owner of Comptia Certifications©, this certification belongs to Comptia, Inc.

OUR CYSA© TRAINING PROGRAM

THREAT MANAGEMENT

- Recognition techniques
- Threat detection tools (NMAP, NETSTAT)
- Analysis of network reconnaissance results
- Response and countermeasures to network threats
- Access point and group policy security

VULNERABILITY MANAGEMENT

- Identification of regulatory and policy requirements
- Setting the scan frequency
- Configuring tools for vulnerability scans
- Run and analyze scan reports
- Remedial techniques and ongoing monitoring

INCIDENT RESPONSE

- Threat classification (Zero day, APT)
- Preparing and using forensic kits
- The importance of communication during incident response
- Containment and eradication techniques
- Validation of corrective actions

SECURITY ARCHITECTURE AND TOOL SETS

- Compliance frameworks and safety policies (NIST, ISO)
- Analysis of safety data (trends, history)
- Best practices during the software development life cycle (SDLC)
- Secure coding practices (OWASP, SANS)
- Comparison of cybersecurity tools (IPS, SIEM, IDS)

CASE STUDIES AND EXAMS

- Applying recognition techniques in real-life situations
- Vulnerability scan simulation and results analysis
- Incident response scenarios and real-time management
- Review of security architectures and recommendations for compensatory controls
- Mock exam and final review for certification

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 enabling 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 with regard to 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.