+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 CASP+© training

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

5 days (35 hours)

Presentation

Our Comptia CASP+© (Advanced Security Practitioner) training course will demonstrate your mastery of IT security principles, particularly in threat detection and incident response.

At Ambient IT, you'll benefit from a comprehensive program to prepare you for the exam. We'll start by teaching you the essential concepts for protecting your infrastructure, such as resilience, distributed allocation and virtualization.

In the same vein, we'll introduce you to essential IT security tools such as SIEM and IDS/IPS. We'll remind you of the technologies used to protect your systems, from cryptography to authentication.

We'll teach you about the various standards that regulate this field, and how these laws apply to your organization and your suppliers. Finally, our CASP+© training will cover areas such as impact analysis and forensics.

Objectives

- Structuring, designing, integrating and implementing secure solutions in complex environments to ensure the smooth running of a resilient enterprise
- Use monitoring, detection, incident response and automation to manage a wide range of proactively monitor ongoing safety operations in a professional environment
- Apply security practices in the cloud, on-premises, at the endpoint and to mobile devices, while taking cryptographic technologies into account
- Take into account the challenges of risk management, governance and compliance by company

Target audience

- System administrator
- Safety engineer
- Cybersecurity Analyst
- Network administrator

Prerequisites

- At least 10 years' experience in IT and 5 years in cybersecurity
- Fluency in technical English

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

OUR CASP+ TRAINING PROGRAM

SECURITY ARCHITECTURE

- Analysis of safety requirements
- Objectives for a secure network architecture
- Secure application integration
- Secure infrastructure design
- Evaluating cloud deployment models

RESILIENCE AND SCALABILITY

- High availability
- Action orchestration
- Distributed allocation and redundancy
- Clustering
- Replication
- Auto-scaling and automation

PERFORMANCE AND VIRTUALIZATION

- Containerization and virtualization
- Content delivery network
- Caching
- Secure storage models
- Secure coding standards

THREAT MANAGEMENT

- Types of information
  - Tactics
  - Strategic,
  - Operational
- Types of players
  - APT
  - Internal threat
  - Hacktivists
- Information gathering methods
- Threat management frameworks (MITRE ATT&CK, Cyber Kill Chain)

ANALYSIS OF INDICATORS OF COMPROMISE

- Packet capture (PCAP)
- Network logs
- Notifications and alerts
  - SIEM
  - DLP
  - IDS/IPS
- Unusual activities
- Firewall rules

VULNERABILITIES

- Vulnerability scans (credentialed vs non-credentialed)
- Assessing and analyzing vulnerabilities
- Proactive mitigation techniques
- Incident response

SAFETY CHECKS

- Application and password controls
- MFA configuration and token-based access
- Patch and firmware repositories
- Certificate management and full device encryption
- Hardening techniques (NX bit, ASLR)

TECHNOLOGIES AND OPERATING SECTORS

- IoT and embedded systems
- SCADA and industrial systems
- Specific protocols (CAN bus, Modbus)
- Automation and orchestration methods

PKI AND CRYPTOGRAPHY

- PKI hierarchy and certificate types
- Common uses of PKI (web services, email, code signing)
- Cryptographic protocols
  - SSL/TLS
  - IPSec
  - SSH
- Symmetric and asymmetric algorithms
- Configuration problems

RISK MANAGEMENT

- Risk assessment (probability factor, impact)
- Risk management techniques (transfer, acceptance, avoidance)
- Risk management life cycle
- Risk monitoring and key performance indicators

SUPPLIER MANAGEMENT

- Shared responsibility model
- Supplier viability (financial risk, mergers/acquisitions)
- Customer requirements (legal, change management)
- Geographical considerations and supply chain visibility
- Third-party dependencies (code, hardware, modules)

COMPLIANCE FRAMEWORKS

- Integration of various industries
- Regulatory frameworks for data
  - Sovereignty
  - Classification
  - Retention
- Third-party certifications of conformity
- Regulations and standards
  - PCI
  - DSS
  - RGPD
  - ISO

IMPACT ASSESSMENT

- Recovery point objective (RPO)
- Recovery time objective (RTO)
- Essential mission analysis
- Privacy Impact Assessment
- Disaster recovery plan (DRP)
- Business Continuity Plan (BCP)

- Types of trade-in sites
  - Cold
  - Warm
  - Hot
- Incident response plans

FORENSIC

- The importance of forensics
- Response process
  - Preparation
  - Detection
  - Analysis
- Collecting and preserving evidence
- Forensic analysis tools (ExifTool, Nmap, Wireshark)
- Integrity preservation techniques

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 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.