CompTIA CySA+¬ Certification Training

Course: **00066**
Filter: **Beginner**
Duration: **2 days**
Category:: **Gouvernance, Risk and Compliance**
Price: **2800,00 €**

About Course

Join our CompTIA CySA+ Certification Training and gain the knowledge and skills to prepare for and pass the Cybersecurity Analyst (CySA+) exam. In this course, you'll learn how to manage threats and vulnerabilities effectively, implement software and systems security solutions, monitor security operations, perform incident response procedures, and execute compliance and assessment measures. With a focus on hands-on experience, this training requires IT security professionals with at least 3-4 years of experience at the level of CompTIA Network+ or CompTIA Security+. Plus, your course tuition includes a voucher to take the CS0-002 exam at any Pearson VUE Test Center location. Don't miss this opportunity to enhance your expertise and advance your career in IT security. Passing the CompTIA CySA+ Certification Exam meets U.S. DoD Directive 8140/8570.01 Technical (IAT) Level-II, CSSP Analyst, CSSP Infrastructure Support, CSSP Incident Responder, and CSSP Auditor requirements.

What you'll learn

- Prepare for and pass the Cybersecurity Analyst (CySA+) exam.
- Manage Threats and Vulnerabilities
- Secure and Monitor Software and Systems
- Perform an Incident Response.
- Execute Compliance and Assessment.

Pre-requisites

- IT (Information Technology) Security Professionals must have 3-4 years of hands-on information security or related experience at the level of Network+ or Security+.

Curriculum

Module 1: Threat and Vulnerability Management

- Explain the importance of threat data and intelligence.
- Intelligence sources
- Indicator management
- Threat actors
- Intelligence cycle
- Information sharing and analysis communities
- Given a scenario, utilize threat intelligence to support organizational security.
- Attack frameworks
- Threat research
- Threat modeling methodologies
- Threat intelligence sharing with supported functions
- Given a scenario, perform vulnerability management activities.
- Vulnerability identification
- Validation
- Remediation/mitigation
- Scanning parameters and criteria
- Inhibitors to remediation
- Web application scanner
- Infrastructure vulnerability scanner
- Software assessment tools and techniques
- Enumeration
- Wireless assessment tools
- Cloud Infrastructure assessment tools
- Explain the threats and vulnerabilities associated with specialized technology
- Explain the threats and vulnerabilities associated with operating in the cloud.
- Given a scenario, implement controls to mitigate attacks and software vulnerabilities.

- Vulnerabilities

Module 2: Software and Systems Security

- Given a scenario, apply security solutions for infrastructure management
- Explain software assurance best practices.
- Explain hardware assurance best practices.

Module 3: Security Operations and Monitoring

- Given a scenario, analyze data as part of security monitoring activities.
- Given a scenario, implement configuration changes to existing controls to improve security.
- Explain the importance of proactive threat hunting
- Compare and contrast automation concepts and technologies.

Module 4: Incident Response

- Explain the importance of the incident response process.
- Given a scenario, apply the appropriate incident response procedure.
- Given an incident, analyze potential indicators of compromise.
- Given a scenario, utilize basic digital forensics techniques.

Module 5: Compliance and Assessment

- Understand the importance of data privacy and protection.
- Given a scenario, apply security concepts to support organizational risk mitigation.
- Explain the importance of frameworks, policies, procedures, and controls.