PROGRAMMA CompTIA CySA + (CS0-002)

40 ore

Parts I: Threat and Vulnerability Management

- Explain the importance of threat data and intelligence
- Given a scenario, utilize threat intelligence to support organizationalsecurity
- Given a scenario, perform vulnerability management activities
- Given a scenario, analyze the output from common vulnerability assessment tools
- Explain the threats and vulnerabilities associated with specialized technology
- Explain the threats and vulnerabilities associated with operating in thecloud
- Given a scenario, implement controls to mitigate attacks and softwarevulnerabilities

Parts II: Software and Systems Security

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

Parts III: **Security Operations and Monitoring**

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

Parts IV: **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

Parts V: **Compliance and Assessment**

- Understand the importance of data privacy and protection
- Given a scenario, apply security concepts in support of organizationalrisk mitigation
- Explain the importance of frameworks, policies, procedures, and controls