PROGRAMMA CompTIA CASP + (CAS-004)

40 ore

Parts I: Security Architecture

- Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network.
- Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.
- Given a scenario, integrate software applications securely into an enterprise architecture.
- Given a scenario, implement data security techniques for securing enterprise architecture.
- Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.
- Given a set of requirements, implement secure cloud and virtualization solutions.
- Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements.
- Explain the impact of emerging technologies on enterprise security and privacy.

Parts II: Security Operations

- Given a scenario, perform threat management activities.
- Given a scenario, analyze indicators of compromise and formulate an appropriate response.
- Given a scenario, perform vulnerability management activities.
- Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools.
- Given a scenario, analyze vulnerabilities and recommend risk mitigations.
- Given a scenario, use processes to reduce risk.
- Given an incident, implement the appropriate response.
- Explain the importance of forensic concepts.
- Given a scenario, use forensic analysis tools.

Parts III: Security Engineering and Cryptography

- Given a scenario, apply secure configurations to enterprise mobility.
- Given a scenario, configure and implement endpoint security controls.
- Explain security considerations impacting specific sectors and operational technologies.
- Explain how cloud technology adoption impacts organizational security.
- Given a business requirement, implement the appropriate PKI solution.
- Given a business requirement, implement the appropriate cryptographic protocols and algorithms.

- Given a scenario, troubleshoot issues with cryptographic implementations.

Parts IV: Governance, Risk and Compliance

- Given a set of requirements, apply the appropriate risk strategies.
- Explain the importance of managing and mitigating vendor risk.
- Explain compliance frameworks and legal considerations, and their organizational impact.
- Explain the importance of business continuity and disaster recovery concepts.