CYBERYAAN
TRAINING & CONSULTANCY

CompTIA Security +

CompTIA Security+

CompTia Security +
COURSE BROCHURE

Course Content

Module 01: Threats, Attacks, and Vulnerabilities
- Compare and contrast different types of social engineering techniques
- Given a scenario, analyze potential indicators to determine the type of attack
- Given a scenario, analyze potential indicators associated with application attacks
- Given a scenario, analyze potential indicators associated with network attacks
- Explain threat actors, vectors, intelligence sources
- Explain the security concerns associated with various types of vulnerabilities
- Summarize the techniques used in security assessments
- Explain the techniques used in penetration testing

Module 02: Architecture and Design
- Explain the importance of security concepts in an enterprise environment
- Summarize virtualization and cloud computing concepts
- Summarize secure application development, deployment and automation concepts
- Summarize authentication & authorization design concepts
- Given a scenario, implement cybersecurity resilience
- Explain the security implications of embedded & specialized systems.
- Explain the importance of physical security controls
- Summarize the basics of cryptographic concepts

Module 03: Implementation
- Given a scenario, implement secure protocols.
- Given a scenario, implement host or application security solutions
- Given a scenario, implement secure network designs
- Given a scenario, install and configure wireless security settings
- Given a scenario, implement secure mobile solutions
- Given a scenario, apply cybersecurity solutions to he cloud
- Given a scenario, implement identity and account management controls
- Given a scenario, implement authentication and authorization solutions

- Given a scenario, implement public key infrastructure

Module 04: Operations and Incident Response
- Given a scenario, use the appropriate tool to assess organizational security
- Summarize the importance of policies, processes, and procedures for incident response.
- Given an incident, utilize appropriate data sources to support an investigation
- Given an incident, apply mitigation techniques or controls to secure an environment
- Explain the key aspects of digital forensics

Module 05: Governance, Risk, and Compliance
- Compare and contrast various types of controls
- Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture
- Explain the importance of policies to organizational security.
- Summarize risk management processes and concepts
- Explain privacy and sensitive data concepts in relation to security

For more information call us
+91 7428748576 | 7428748577

Duration
40 Hours

Language
Hindi & English

Certificate
Yes

"Unlock the secrets of cybersecurity with our CompTia Security+ course – where curiosity meets responsibility in the world of digital defense."

Scan for Youtube

Scan for LinkedIn

Scan for Instagram

CONTACT US:
+91-742 874 8576