Course duration

- 5 days

Course Benefits

- Identify the fundamental components of information security.
- Analyze risk.
- Identify various threats to information security.
- Conduct security assessments to detect vulnerabilities.
- Implement security for hosts and software.
- Implement security for networks.
- Manage identity and access.
- Implement cryptographic solutions in the organization.
- Implement security at the operational level.
- Address security incidents.
- Ensure the continuity of business operations in the event of an incident.

Course Outline

1. Comparing Security Roles and Security Controls
2. Explaining Threat Actors and Threat Intelligence
3. Performing Security Assessments
4. Identifying Social Engineering and Malware
5. Summarizing Basic Cryptographic Concepts
6. Implementing Public Key Infrastructure
7. Implementing Authentication Controls
8. Implementing Identity and Account Management Controls
9. Implementing Secure Network Designs
10. Implementing Network Security Appliances
11. Implementing Secure Network Protocols
12. Implementing Host Security Solutions
13. Implementing Secure Mobile Solutions
14. Summarizing Secure Application Concepts
15. Implementing Secure Cloud Solutions
16. Explaining Data Privacy and Protection Concepts
17. Performing Incident Response
18. Explaining Digital Forensics
19. Summarizing Risk Management Concepts
20. Implementing Cybersecurity Resilience
21. Explaining Physical Security

Class Materials

Each student will receive a comprehensive set of materials, including course notes and all the class examples.

Class Prerequisites

Experience in the following *is required* for this CompTIA class:

- Basic Windows skills
- Fundamental understanding of computer and networking concepts.