Course: **Security+**

Contact Hours: **30**

Pre-requisite: **A+ & Network+ / Equivalent**

Abstract

This course covers knowledge of security concepts, tools and procedures to react to security incidents, anticipating security risks and guarding against them

Target Audience

- Security Architect
- Security Engineer
- Security Consultant/Specialist
- Information Assurance Technician
- Security Administrator
- Systems Administrator
- Network Administrator

Learning outcomes

On completion of this course, learners will be able to:

1. Identify fundamental concepts of computer security.
2. Identify security threats and vulnerabilities
3. Describe network security
4. Implement managing application, data, and host security
5. Describe access control, authentication, and account management
6. Describe compliance & operational security
7. Perform basic risk management
8. Manage security incidents
9. Describe business continuity and disaster recovery planning

Course Content

1. General Security Concepts

- Categories of security controls (technical, managerial, operational, physical) and control types (preventive, detective, corrective, etc.)
- Core principles: CIA triad, AAA framework, non-repudiation, gap analysis, Zero Trust architecture
- Physical security measures (fencing, surveillance, sensors) and deception technologies (honeypots, honeytokens)
- Change management processes, cryptographic solutions (PKI, encryption, hashing, digital signatures), and threat actor motivations and vectors

2. Threats, Vulnerabilities, and Mitigations

- Common vulnerability types (buffer overflows, injection, misconfigurations, zero-days)
- Indicators of malicious activity (malware families, DDoS, phishing, credential replay)
- Mitigation techniques: segmentation, access control lists, patching, hardening, least privilege

3. Security Architecture

- Security considerations for architecture models: cloud (IaaS, serverless, microservices), virtualization, containers, air-gapping
- Data protection strategies: classification, encryption/hashing, tokenization, data sovereignty
- Resilience and recovery: high availability, backup strategies, disaster recovery sites, testing exercises

4. Security Operations

- Vulnerability management lifecycle: identification, analysis, remediation, and validation
- Monitoring and alerting: SIEM, antivirus, DLP, log aggregation, incident response workflows
- Identity and Access Management (IAM): provisioning, SSO, federation, multifactor authentication, privileged access management
- Automation and orchestration benefits and risks, incident response phases, forensic data sources

5. Security Program Management and Oversight

- Governance: policies, standards, procedures, and roles for systems/data owners, custodians, and controllers
- Risk management: identification, assessment (qualitative/quantitative), treatment strategies, and business impact analysis
- Third-party risk: vendor assessments, agreements (SLA, NDA, SOW), and ongoing monitoring
- Compliance and audits: internal/external reporting, privacy considerations, and security awareness training

Assessment Criteria

In order to achieve Learning Outcome…	The Learner must…
1. Identify fundamental concepts of computer security	Describe what is security Identify Security concepts
2. Identify security threats and vulnerabilities	Differentiate Threats vs Vulnerability Identify major threats Identify major Vulnerability Explain the impact of vulnerabilities
3. Describe network security	Identify components of a secure networks Identify methodology of securing a network Identify and contrast security tools (hardware and software) and protocols
4. Implement managing application, data, and host security	Define cryptography Define IDS, IPS and DMZ Define methods to harden a Host Summarize Virtualization Explain resiliency and automation
5. Describe access control, authentication, and account management	Identify physical access control Identify network access control Identify Remote Access and authentication Explain concepts of account management
6. Describe compliance & operational security	Define physical security Identify major compliance laws
7. Perform basic risk management	Define risk Outline vulnerability testing Explain and Outline the use of policies, procedures and plans Outline Business Impact Analysis
8. Manage security incidents	Identify incident response methodology Summarize Forensic concepts
9. Describe business continuity and disaster recovery planning	Define cold, warm and hot sites Define backups, cloud and network Identify concepts for creating a disaster recovery plan

Websites
http://www.comptia.org