Wissenhive

CompTIA Security+ Training Certification

Table of Contents

About the Program

CompTIA Security+ Certification is a trusted training course globally that validates vendor-neutral and foundational IT security skills and knowledge. As a benchmark for being the best practices in IT security, this certification covers the baseline skills, network security, and risk management principles to pursue a career in IT security and perform core security functions.

Cybersecurity attacks are continuously growing day by day with modern technology, which leads to rising job roles that are tasked with security baseline readiness and effective strategies to address and respond to today's threats. This program focuses on risk management, authentication & authorization, cryptography, and security on host, application, LAN, mobile, wireless, and cloud.

Key Training Features

- Accredited Training Partner
- Lifetime Training Access
- Access to Labs
- Study Guides
- Assessments
- Exam Voucher Included
- 24/7 support
- Flexible Scheduling

Why CompTIA Security+

CompTIA Security+ creates new opportunities in the field of cyber security boosting an individual's employability.

Why is it different?

- More choose Security+ – chosen by more corporations and defense organizations than any other certification on the market to validate core security skills and for fulfilling DoD 8570 compliance.
- Security+ proves hands-on skills – the only baseline cybersecurity certification emphasizing vendor-neutral, hands-on practical skills, ensuring the security professional is better prepared to problem solve a wider variety of today's complex issues.
- More job roles turn to Security+ to supplement skills – baseline cybersecurity skills are applicable across more of today's job roles to secure systems, software and hardware.
- Security+ is aligned to the latest trends and techniques – covering the most core technical skills in risk assessment and management, incident response, forensics, enterprise networks, hybrid/cloud operations, and security controls, ensuring high-performance on the job.

What's in this Version?

New updates to the Security+ exam domains:

1. Attacks, Threats and Vulnerabilities 24%

- Compare and contrast different types of social engineering techniques
- Analyze potential indicators to determine the type of attack
- Explain different threat actors, vectors, and intelligence sources
- Explain security concerns associated with various types of vulnerabilities
- Summarize techniques used in security assessments
- Explain techniques used in penetration testing

2. Architecture and Design 21%

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

3. Implementation 25%

- Given a scenario, implement secure protocols, host or application security solutions, and secure network designs
- Comprehend how to install and configure wireless security settings and how to apply cybersecurity solutions to the cloud
- Given a scenario, implement authentication and authorization solutions and identity and account management controls
- Understand implementing public key infrastructure (PKI)

4. Operations and Incident Response 16%

- Given a scenario, use appropriate tool to assess organizational security
- Summarize importance of policies, processes, and procedures for incident response
- Given an incident, utilize appropriate data sources to support investigations
- Given an incident, apply mitigation techniques or controls to secure an environment
- Explain key aspects of digital forensics

5. Governance, Risk and Compliance 14%

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

Top Security+ Job Roles

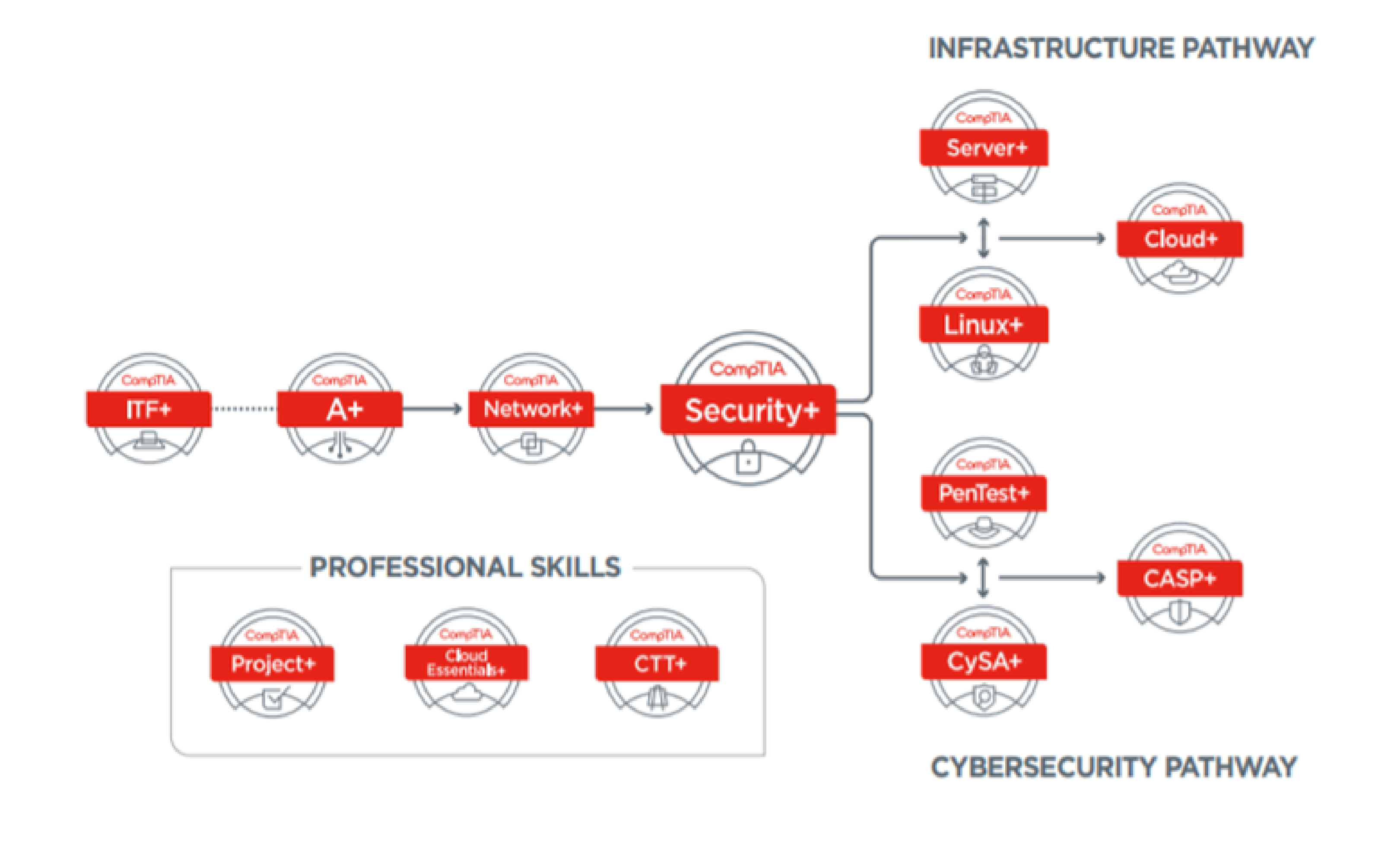
- Security Administrator
- Systems Administrator
- Helpdesk Manager / Analyst
- Security Analyst
- Network / Cloud Engineer
- IT Auditors
- Security Engineer
- IT Project Manager
- Security Officer
- Information Security Manager
- DevOps / Software Developer
- Security Architect

Target Audience

- Network Administrators
- Security Engineers
- Support Analysts
- Security Administrator
- Security Consultant
- IT Managers

CompTIA Certification Pathway

CompTIA certifications align with the skillsets needed to support and manage cybersecurity. Enter where appropriate for you. Consider your experience and existing certifications or course of study.



Course Curriculum

Module 1: Comparing Security Roles and Security Controls

Topic 1A: Compare and Contrast Information Security Roles
Topic 1B: Compare and Contrast Security Control and Framework Types

Module 2: Explaining Threat Actors and Threat Intelligence

Topic 2A: Explain Threat Actor Types and Attack Vectors
Topic 2B: Explain Threat Intelligence Sources

Module 3: Performing Security Assessments

Topic 3A: Assess Organizational Security with Network Reconnaissance Tools
Topic 3B: Explain Security Concerns with General Vulnerability Types
Topic 3C: Summarize Vulnerability Scanning Techniques
Topic 3D: Explain Penetration Testing Concepts

Module 4: Identifying Social Engineering and Malware

Topic 4A: Compare and Contrast Social Engineering Techniques
Topic 4B: Analyze Indicators of Malware-Based Attacks

Module 5: Summarizing Basic Cryptographic Concepts

Topic 5A: Compare and Contrast Cryptographic Ciphers
Topic 5B: Summarize Cryptographic Modes of Operation
Topic 5C: Summarize Cryptographic Use Cases and Weaknesses
Topic 5D: Summarize Other Cryptographic Technologies

Course Curriculum

Module 5: Summarizing Basic Cryptographic Concepts

Topic 5A: Compare and Contrast Cryptographic Ciphers
Topic 5B: Summarize Cryptographic Modes of Operation
Topic 5C: Summarize Cryptographic Use Cases and Weaknesses
Topic 5D: Summarize Other Cryptographic Technologies

Module 6: Implementing Public Key Infrastructure

Topic 6A: Implement Certificates and Certificate Authorities
Topic 6B: Implement PKI Management

Module 7: Implementing Authentication Controls

Topic 7A: Summarize Authentication Design Concepts
Topic 7B: Implement Knowledge-Based Authentication
Topic 7C: Implement Authentication Technologies
Topic 7D: Summarize Biometrics Authentication Concepts

Module 8: Implementing Identity and Account Management Controls

Topic 8A: Implement Identity and Account Types
Topic 8B: Implement Account Policies
Topic 8C: Implement Authorization Solutions
Topic 8D: Explain the Importance of Personnel Policies

Course Curriculum

Module 9: Implementing Secure Network Designs

Topic 9A: Implement Secure Network Designs
Topic 9B: Implement Secure Switching and Routing
Topic 9C: Implement Secure Wireless Infrastructure
Topic 9D: Implement Load Balancers

Module 10: Implementing Network Security Appliances

Topic 10A: Implement Firewalls and Proxy Servers
Topic 10B: Implement Network Security Monitoring
Topic 10C: Summarize the Use of SIEM

Module 11: Implementing Secure Network Protocols

Topic 11A: Implement Secure Network Operations Protocols
Topic 11B: Implement Secure Application Protocols
Topic 11C: Implement Secure Remote Access Protocols

Module 12: Implementing Host Security Solutions

Topic 12A: Implement Secure Firmware
Topic 12B: Implement Endpoint Security
Topic 12C: Explain Embedded System Security Implications

Course Curriculum

Module 13: Implementing Secure Mobile Solutions

Topic 13A: Implement Mobile Device Management
Topic 13B: Implement Secure Mobile Device Connections

Module 14: Summarizing Secure Application Concepts

Topic 14A: Analyze Indicators of Application Attacks
Topic 14B: Analyze Indicators of Web Application Attacks
Topic 14C: Summarize Secure Coding Practices
Topic 14D: Implement Secure Script Environments
Topic 14E: Summarize Deployment and Automation Concepts

Module 15: Implementing Secure Cloud Solutions

Topic 15A: Summarize Secure Cloud and Virtualization Services
Topic 15B: Apply Cloud Security Solutions
Topic 15C: Summarize Infrastructure as Code Concepts

Module 16: Explaining Data Privacy and Protection Concepts

Topic 16A: Explain Privacy and Data Sensitivity Concepts
Topic 16B: Explain Privacy and Data Protection Controls

Course Curriculum

Module 17: Performing Incident Response

Topic 17A: Summarize Incident Response Procedures
Topic 17B: Utilize Appropriate Data Sources for Incident Response
Topic 17C: Apply Mitigation Controls

Module 18: Explaining Digital Forensics

Topic 18A: Explain Key Aspects of Digital Forensics Documentation
Topic 18B: Explain Key Aspects of Digital Forensics Evidence Acquisition

Module 19: Summarizing Risk Management Concepts

Topic 19A: Explain Risk Management Processes and Concepts
Topic 19B: Explain Business Impact Analysis Concepts

Module 20: Implementing Cybersecurity Resilience

Topic 20A: Implement Redundancy Strategies
Topic 20B: Implement Backup Strategies
Topic 20C: Implement Cybersecurity Resiliency Strategies

Module 21: Explaining Physical Security

Topic 21A: Explain the Importance of Physical Site Security Controls
Topic 21B: Explain the Importance of Physical Host Security Controls

Contact us

DREAM BIG IT SOLUTION INDIA PVT LTD

Noida

B-115, B Block, Sector 2,
Noida, Uttar Pradesh-201301

If you have any further questions or would like to chat with us, give us a call

IND +91 9368569359 **US** +1 (908)-(952)-(2400)

https://www.facebook.com/Wissenhive

https://www.linkedin.com/company/wissenhive/

https://www.instagram.com/wissenhive/

https://twitter.com/HiveWissen