TechyEdz Solutions

Training | Consulting | Developement | Outsourcing

Cyber Security Master Program

9032803832

contact@techyedz.com

9032803832

www.techyedz.com

Cyber Security Training Program

- **Learning Path**

1. CompTIA Security+ 501
2. Certified Ethical Hacker
3. CISM
4. CISSP
5. CCSP

CompTIA Security+ 501

- **Course Overview:**

There are many career opportunities for IT and cybersecurity professionals. If you're wondering where to start to help fill this gap, start with the CompTIA Security+ SY0-501 certification. This certification course helps you prove your competency in topics such as threats, vulnerabilities, and attacks, system security, network infrastructure, access control, cryptography, risk management, and organizational security.

If you're wondering where to start in cybersecurity to help fill this gap, start with Security+. The CompTIA Security+ SY0-501 exam is an internationally recognized validation of foundation-level security skills and knowledge and is used by organizations and security professionals around the globe. The CompTIA Security+ certification proves an IT security professional's competency in topics such as threats, vulnerabilities, and attacks, system security, network infrastructure, access control, cryptography, risk management, and organizational security. This course covers those topics to prepare students for the CompTIA SY0-501 certification exam. The fundamentals taught in this class will prepare you for a career as a cybersecurity analyst.

- **Course Outline:**

1. Introduction

- Who Should Read This Book?
- CompTIA Security+ Exam Topics

2. Introduction to Security

- Security 101
- Think Like a Hacker
- Threat Actor Types and Attributes
- Review Key Topics

3. Computer Systems Security Part I

- Malicious Software Types
- Delivery of Malware
- Preventing and Troubleshooting Malware
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

4: Computer Systems Security Part II

- Implementing Security Applications
- Securing Computer Hardware and Peripherals
- Securing Mobile Devices
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

5. OS Hardening and Virtualization

- Hardening Operating Systems
- Virtualization Technology
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

6. Application Security

- Securing the Browser
- Securing Other Applications
- Secure Programming
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

7. Network Design Elements

- Network Design
- Cloud Security and Server Defense
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

8. Networking Protocols and Threats

- Ports and Protocols
- Malicious Attacks
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

9. Network Perimeter Security

- Firewalls and Network Security
- NIDS Versus NIPS
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

10. Securing Network Media and Devices

- Securing Wired Networks and Devices
- Securing Wireless Networks
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

11. Physical Security and Authentication Models

- Physical Security
- Authentication Models and Components
- Lesson Summary
- Review Key Topics

- Complete the Real-World Scenarios

12. Access Control Methods and Models

- Access Control Models Defined
- Rights, Permissions, and Policies
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

13. Vulnerability and Risk Assessment

- Conducting Risk Assessments
- Assessing Vulnerability with Security Tools
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

14. Monitoring and Auditing

- Monitoring Methodologies
- Using Tools to Monitor Systems and Networks
- Conducting Audits
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

15. Encryption and Hashing Concepts

- Cryptography Concepts
- Encryption Algorithms
- Hashing Basics
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

16. PKI and Encryption Protocols

- Public Key Infrastructure

- Security Protocols
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

17. Redundancy and Disaster Recovery

- Redundancy Planning
- Disaster Recovery Planning and Procedures
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

18. Social Engineering, User Education, and Facilities Security

- Social Engineering
- User Education
- Facilities Security
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

19. Policies and Procedures

- Legislative and Organizational Policies
- Incident Response Procedures
- IT Security Frameworks
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

Prerequisites:

- One or two years of experience in networking support and IT administration
- Able to use Windows to create and manage files and use basic administrative features (Explorer, Control Panel and Management Consoles).
- Know basic network terminology and functions (such as OSI Model, topology, Ethernet, TCP/IP, switches and routers).
- Understand TCP/IP addressing, core protocols and troubleshooting tools.

- **Who can Attend:**
- The CompTIA Security+ course is ideal for professionals who are working in the roles of system administrators, network administrators, security administrators, and IT auditors.
- **Certification: CompTIA Security+ SY0-501**
- **Number of Hours: 50hrs**

Certified Ethical Hacker (CEH)

- **Course Overview:**

Certified Ethical Hacker (CEH) Certification is the most comprehensive course for network security professionals. This globally acceptable certification authenticates the applied knowledge of the network administrators, auditors and professionals from a security perspective. Since this course contents are vendor-neutral, it covers a wide range of network-security concepts. This training will help you to think from the malicious hackers viewpoint but try to penetrate the network, ethically and list out the loopholes and vulnerabilities.

The CEH Certification Course will teach the students about hacking from an entirely practical stand-point following the principle of 'Learning by Doing'. In this course you will be performing all the steps right from scanning and identifying vulnerable targets and gaining access to those systems and suggesting the remedies. The practical approach gives the student an in-depth knowledge about the hacking tools and techniques. The simulated lab environment will demonstrate how actual hackers penetrate through the multi-level defenses of the organization. This course additionally teaches you about the virus creation, DDoS attacks, Intrusion Detection techniques and Social Engineering, apart from the steps of hacking.

- **Course Outline:**

1. Background

Network and Communication Technologies

- Networking technologies (e.g., hardware, infrastructure)
- Web technologies (e.g., web 2.0, skype)
- Systems technologies
- Communication protocols
- Telecommunication technologies
- Mobile technologies (e.g., smartphones)
- Wireless terminologies
- Cloud computing
- Cloud deployment models

Information Security Threats and Attack Vectors

- Malware (e.g., Trojan, virus, backdoor, worms)
- Malware operations
- Information security threats and attack vectors
- Attacks on a system (e.g., DoS, DDoS, session hijacking, webserver and web application attacks, SQL injection, wireless threats)
- Botnet
- Cloud computing threats and attacks
- Mobile platform attack vectors
- Cryptography attacks

Information Security Technologies

- Information security elements
- Information security management (e.g. IA, Defense-in-Depth, incident management)
- Security trends
- Hacking and ethical hacking
- Vulnerability assessment and penetration testing
- Cryptography
- Encryption algorithms
- Wireless encryption
- Bring Your Own Device (BYOD)
- Backups and archiving (e.g., local, network)
- IDS, firewalls, and honeypots

2. Analysis / Assessment

Information Security Assessment and Analysis

- Data analysis
- Systems analysis
- Risk assessments
- Vulnerability assessment and penetration testing
- Technical assessment methods
- Network sniffing
- Malware analysis

Information Security Assessment Process

- Footprinting
- Scanning (e.g., Port scanning, banner grabbing, vulnerability scanning, network discovery, proxy chaining, IP spoofing)
- Enumeration
- System hacking (e.g., password cracking, privilege escalation, executing applications, hiding files, covering tracks)

3. Security

Information Security Controls

- Systems security controls
- Application/file server
- IDS
- Firewalls
- Cryptography
- Disk Encryption
- Network security
- Physical security
- Threat modeling
- Biometrics
- Wireless access technology (e.g., networking, RFID, Bluetooth)
- Trusted networks
- Privacy/confidentiality (with regard to engagement)

Information Security Attack Detection

- Security policy implications

- Vulnerability detection
- IP Spoofing detection
- Verification procedures (e.g., false positive/negative validation)
- Social engineering (human factors manipulation)
- Vulnerability scanning
- Malware detection
- Sniffer detection
- DoS and DDoS detection
- Detect and block rogue AP
- Evading IDS (e.g., evasion, fragmentation)
- Evading Firewall (e.g., firewalking, tunneling)
- Honeypot detection
- Steganalysis

Information Security Attack Prevention

- Defend against webserver attacks
- Patch management
- Encoding schemes for web application
- Defend against web application attacks
- Defend against SQL injection attacks
- Defend against wireless and Bluetooth attacks
- Mobile platforms security
- Mobile Device Management (MDM)
- BYOD Security
- Cloud computing security

4. Tools / Systems / Programs

Information Security Systems

- Network/host based intrusion
- Boundary protection appliances
- Access control mechanisms (e.g., smart cards)
- Cryptography techniques (e.g., IPSec, SSL, PGP)
- Domain name system (DNS)
- Network topologies
- Subnetting

- Routers / modems / switches
- Security models
- Database structures

Information Security Programs

- Operating environments (e.g., Linux, Windows, Mac)
- Anti-malware systems and programs (e.g., anti-keylogger, anti-spyware, anti-rootkit, anti-trojan, anti-virus)
- Wireless IPS deployment
- Programming languages (e.g. C++, Java, C#, C)
- Scripting languages (e.g., PHP, Javascript)

Information Security Tools

- Network/wireless sniffers (e.g., Wireshark, Airsnort)
- Port scanning tools (e.g., Nmap, Hping)
- Vulnerability scanner (e.g., Nessus, Qualys, Retina)
- Vulnerability management and protection systems (e.g., Founds tone, Ecora)
- Log analysis tools
- Exploitation tools
- Footprinting tools (e.g., Maltego, FOCA, Recon-ng)
- Network discovery tools (e.g., Network Topology Mapper)
- Enumeration tools (e.g., SuperScan, Hyena, NetScanTools Pro)
- Steganography detection tools
- Malware detection tools
- DoS/DDoS protection tools
- Patch management tool (e.g., MBSA)
- Webserver security tools
- Web application security tools (e.g., Acunetix WVS)
- Web application firewall (e.g., dotDefender)
- SQL injection detection tools (e.g., IBM Security AppScan)
- Wireless and Bluetooth security tools
- Android, iOS, Windows Phone OS, and BlackBerry device security tools
- MDM Solutions
- Mobile Protection Tools
- Intrusion Detection Tools (e.g., Snort)
- Hardware and software firewalls (e.g., Comodo Firewall)
- Honeypot tools (e.g., KFSenser)

- IDS/Firewall evasion tools (e.g., Traffic IQ Professional)
- Packet fragment generators
- Honeypot Detection Tools
- Cloud security tools (e.g., Core CloudInspect)
- Cryptography tools (e.g., Advanced Encryption Package)
- Cryptography toolkit (e.g., OpenSSL)
- Disk encryption tools
- Cryptanalysis tool (e.g., CrypTool)

5. Procedures / Methodology

Information Security Procedures

- Cryptography
- Public key infrastructure (PKI)
- Digital signature and Pretty Good Privacy (PGP)
- Security Architecture (SA)
- Service oriented architecture
- Information security incident
- N-tier application design
- TCP/IP networking (e.g., network routing)
- Security testing methodology

Information Security Assessment Methodologies

- Web server attack methodology
- Web application hacking methodology
- SQL injection methodology and evasion techniques
- SQL injection evasion techniques
- Wireless and Bluetooth hacking methodology
- Mobile platform (Android, iOS, Windows Phone OS, and BlackBerry) hacking methodology
- Mobile Rooting and Jailbreaking

6. Regulation / Policy

Information Security Policies/ Laws/Acts

- Security policies
- Compliance regulations (e.g., PCI-DSS, SOX)

Ethics of Information Security

- Professional code of conduct
- Appropriateness of hacking

- **Prerequisites:**

- Participants should have good knowledge and understanding of OS, TCP/IP and Network
- Networking Basics will be an additional advantage to understand the concepts easily

- **Who can attend:**

- Information Security Analyst / Administrator
- Information Assurance (IA) Security Officer
- Information Security Manager / Specialist
- Information Systems Security Engineer / Manager
- Information Security Professionals / Officers
- Information Security / IT Auditors
- Risk / Threat/Vulnerability Analyst
- System Administrators
- Network Administrators and Engineers

- **Number of hours: 50hrs**
- **Certification: CEH 312-50**

CISM (Certified Information Security Manager)

- **Course Overview:**

The CISM certification program was developed by ISACA for experienced information security management professionals who have experience developing and managing information security programs and who understand the programs relationship to the overall business goals. The CISM exam consists of 200 multiple-choice questions that cover the four CISM domains.

The CISM course is designed to teach professionals international security practices and expertise to manage designs, administer and assess IT security for organizations of every size and scale. Here you learn to build core competencies in maintaining and completely owning the security aspect of your organization's IT. Students develop critical thinking skills and sound judgment to perform tasks required to achieve CISM certification. It is one of the most lucrative internationally acclaimed certifications with organizations offering high paying jobs to candidates who possess this credential.

- **Course Outline:**

1. Information Security Governance

- Develop an information security strategy, aligned with business goals and directives.
- Establish and maintain an information security governance framework.
- Integrate information security governance into corporate governance.
- Develop and maintain information security policies.
- Develop business cases to support investments in information security.
- Identify internal and external influences to the organization.
- Gain ongoing commitment from senior leadership and other stakeholders.
- Define, communicate and monitor information security responsibilities
- Establish internal and external reporting and communication channels.

2. Information Risk Management

- Establish and/or maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value.
- Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.
- Ensure that risk assessments, vulnerability assessments and threat analyses are conducted consistently, and at appropriate times, to identify and assess risk to the organization’s information.
- Identify, recommend or implement appropriate risk treatment/response options to manage risk to acceptable levels based on organizational risk appetite.

- Determine whether information security controls are appropriate and effectively manage risk to an acceptable level.
- Facilitate the integration of information risk management into business and IT processes to enable a consistent and comprehensive information risk management program across the organization.
- Monitor for internal and external factors (e.g., threat landscape, cybersecurity, geopolitical, regulatory change) that may require reassessment of risk to ensure that changes to existing or new risk scenarios are identified and managed appropriately.
- Report noncompliance and other changes in information risk to facilitate the risk management decision-making process.
- Ensure that information security risk is reported to senior management to support an understanding of potential impact on the organizational goals and objectives.

3. Information Security Program Development & Management

- Develop a security program, aligned with information security strategy
- Ensure alignment between the information security program and other business functions
- Establish and maintain requirements for all resources to execute the IS program
- Establish and maintain IS architectures to execute the IS program
- Develop documentation that ensures compliance with policies
- Develop a program for information security awareness and training
- Integrate information security requirements into organizational processes
- Integrate information security requirements into contracts and activities of third parties
- Develop procedures (metrics) to evaluate the effectiveness and efficiency of the IS program
- Compile reports to key stakeholders on overall effectiveness of the IS program and the underlying business processes in order to communicate security performance.

4. Information Security Incident Management

- Define (types of) information security incidents

- Establish an incident response plan
- Develop processes for timely identification of information security incidents
- Develop processes to investigate and document information security incidents
- Develop incident escalation and communication processes
- Establish teams that effectively respond to information security incidents
- Test and review the incident response plan
- Establish communication plans and processes
- Determine the root cause of IS incidents
- Align incident response plan with DRP and BCP.

Prerequisites:

- Five years of information security work experience, with a minimum of three years of information security management work experience in three or more of the job practice analysis areas.

Who can Attend:

- Experienced information security managers and those who have information security management responsibilities, including IT consultants, auditors, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, and security engineers.

Certification: CISM

Number of Hours: 30hrs

Certified Information Systems Security Professional (CISSP)

Course Overview:

The CISSP Certification Training Course consists of overall 8 Domains which in turn gain knowledge in the Information Security Field along with a detailed knowledge of the current industry standards and best practices a Security Practitioner needs to implement in their respective organization to keep it in a secure way.

- **Course Outline:**

1: Security and Risk Management

- A Brief Introduction about Confidentiality, Integrity, and Availability.
- How to Apply Security Governance Principles?
- Compliance
- Legal and Regulatory issues related to Cyber Security.
- Understanding the difference between Security Policy, Standards, Procedures, and Guidelines.
- Understand the concept about Business Continuity Planning.
- Understand and Apply Risk Management Concepts
- Understand and Apply Threat Modeling
- Acquisition Strategy and Practice
- Security Awareness and Training.

2: Asset Security

- Classification of Assets
- Least Privilege and Need to Know bases Models.
- Privacy Protection.
- Data Retention Techniques and Security Controls associated with it.
- Secure Handling of Data.

3: Security Architecture and Engineering

- Security Design Principles
- Understanding Security Models

- How to Implement Controls and Countermeasures adhering to the Information Security Standards.
- Assess and Mitigate the Vulnerabilities of Security Architectures Designs, Web-based Systems, Mobile Systems, OT Systems.
- Understanding the Concepts and applying Cryptography.
- Implementation of Physical Security in various sites and data centers.

4: Communication and Network Security

- How to Securely design your Network Architecture?
- Securing Network Components with appropriate hardening standards.
- Secure Communication Channels
- Mitigate Network Attacks.

5: Identity and Access Management (IAM)

- Physical and Logical Access Control.
- Understanding about Identification, Authentication and Authorization
- Integrate Identity as a Service (IDaaS)
- Integrate Third-Party Identity Services

6: Security Assessment and Testing

- Design and Validate Assessment and Test Strategies.
- Conduct Security Control Testing.
- Collection of Security Process Data.
- Enhance Knowledge on how to conduct Internal and about Third-Party Audits.

7: Security Operations

- Day to Day Security Monitoring Methodologies.
- Perform Forensic Investigations and Root Cause Analysis.

- Preventive and Detective Controls.
- Physical and Personnel Security.
- Handling of Incident Response.
- Implement Vulnerability Management.
- Understanding the Change Management Processes.
- Disaster Recovery Strategies

8: Software Development Security

- Applying Security in the Software Development Life Cycle
- Enforce Security Controls and Secure Coding Techniques in the Development Environment.
- Database Security
- Through Assessment in Software Security.

Prerequisites:

To apply for the CISSP Certification Training , you need to:

- Have a minimum 5 years of cumulative paid full-time work experience in two or more of the 8 domains of the (ISC)² CISSP Common Body of Knowledge (CBK)
- One-year experience waiver can be earned with a 4-year college degree, or regional equivalent or additional credential from the (ISC)² approved list

Who can Attend:

The CISSP course is recommended for the following profiles -

- Security Consultant
- Security Manager
- IT Director/Manager
- Security Auditor
- Security Architect

- Security Analyst
- Security Systems Engineer
- Chief Information Security Officer
- Director of Security
- Network Architect

- **Number Of Hours:** 40hrs
- **Certification: CISSP**

Certified Cloud Security Professional (CCSP)

- **Course Overview:**

The **Cloud Security Professional (CCSP)** training course applies information security expertise to a cloud computing environment and demonstrates competence in cloud security architecture, design, operations, and service orchestration. This professional competence is measured against a globally recognized body of knowledge. This program is comprised of a total of six (6) domains. The modular format is designed to organize and chunk information in order to assist with learning retention as participants are guided through the CCSP course materials.

- **Course Outline:**

1. Cloud Concepts, Architecture, and Design

- Understand Cloud Computing Concepts
- Describe Cloud Reference Architecture
- Understand Security Concepts Relevant to Cloud Computing
- Understand the Design Principles of Secure Cloud Computing
- Evaluate Cloud Service Providers

2. Cloud Data Security

- Understand Cloud Data Lifecycle
- Design and Implement Cloud Data Storage Architectures
- Design and Apply Data Security Strategies

- Understand and Implement Data Discovery and Classification Technologies
- Design and Implement Relevant Jurisdictional Data Protections for Personally Identifiable Information
- Design and Implement Data Rights Management
- Plan and Implement Data Retention, Deletion, and Archiving Policies
- Design and Implement Auditability, Traceability and Accountability of Data Events

3. Cloud Platform and Infrastructure Security

- Comprehend Cloud Infrastructure Components
- Analyse Risks Associated to Cloud Infrastructure
- Design and Plan Security Controls
- Plan Disaster Recovery and Business Continuity Management

4. Cloud Application Security

- Training and Awareness in Application Security
- Understand Cloud Software Assurance and Validation
- Use Verified Secure Software
- Software Development Lifecycle (SDLC) Process
- Secure Software Development Lifecycle
- Cloud Application Architecture
- Identity and Access Management (IAM) Solutions

5. Cloud Security Operations

- Support the Planning Process of the Data Centre Design
- Implement and Build Physical Infrastructure on Cloud Environment
- Run Physical Infrastructure for Cloud Environment
- Manage Physical Infrastructure for Cloud Environment
- Build Logical Infrastructure for Cloud Environment
- Run Logical Infrastructure for Cloud Environment
- Manage Logical Infrastructure for Cloud Environment
- Ensure Compliance with Regulations and Controls
- Conduct Risk Assessment for Logical and Physical Infrastructure
- Understand the Collection and Preservation of Digital Evidence
- Manage Communications with Relevant Parties

6. Legal, Risk, and Compliance

- Legal Requirements and Unique Risks

- Privacy Issues Including Jurisdictional Variances
- Audit Process, Methodologies, and Required Adaptions
- Implications of Cloud to Enterprise Risk Management
- Outsourcing and Cloud Contract Design
- Execute Vendor Management

Prerequisites:

- Information security professionals with at least five years of full-time IT experience, including three years of information security and at least one year of cloud security experience.

Who can attend:

- This CCSP training is suitable for experienced IT personnel who are involved with information security, risk and compliance, security engineering, governance, IT auditing or IT architecture.
- The course is intended for delegates who have at least five years of recent full-time security professional work experience in information technology, of which three of those years must be in security and one year in cloud computing. The course builds on and brings together the holistic view of the topics covered in the everyday environment of an information assurance professional.

Number of Hours: 40

Certification: CCSP

Key Features:

- One to One Training
- Online Training
- Fastrack & Normal Track
- Resume Modification
- Mock Interviews
- Video Tutorials
- Materials
- Real Time Projects
- Virtual Live Experience
- Preparing for Certification