Clemson University - Center for Corporate Learning
1 North Main Street, 7th Floor,
Greenville, SC 29601
http://www.clemson.edu/online/
Contact: Juanita Durham | 864.656.3984 | jdrhm@clemson.edu

IT Cyber Security Professional with CompTIA Security+

Format:	Self-Pace Online / eLearning
Program Duration:	6 Months
Course Contact Hours:	375

The IT Cyber Security Professional with CompTIA Security+

Computer Technology Industry Association (CompTIA) Security+ training designates knowledgeable professionals in the field of IT security. As an international, vendor-neutral credential, CompTIA Security+ certification ensures successful students gain competency in network security, compliance and operational security, common/possible threats and vulnerabilities, application, data and host security, access control and identity management, as well as cryptography. Earning CompTIA Security+ Certification signifies to employers that candidates will apply their knowledge of security concepts, tools and procedures to prevent security breaches, react accordingly to any security incidents, and anticipate further security risks in order to effectively guard against them.

The IT Cyber Security Professional with CompTIA Security+ Program

The CompTIA Security+ program offers an in-depth understanding of each objectives mastered by CompTIA Security+ professionals as well as a deeper understanding of security foundations and principles. This CompTIA Security+ program covers every objective in the newly updated CompTIA Security+ SY0-501 exam and includes screencast teaching, whiteboard explanations, deep dives on security theory and everyday practices, and live demos/labs showing how to complete tasks in real time. Most lessons end with a "Security in Action" segment, which takes the security knowledge you've learned to the next level.

Education and National Certifications

- Students should have or be pursuing a high school diploma or GED.
- There are no state approval and/or state requirements associated with this program.
- National Certification:
  - **CompTIA Security+ (SY0-501) Certification Exam**
    - NOTE: CompTIA® recommends candidates for the CompTIA A+ Exam have a minimum of two years of experience in IT administration with a focus on security

Program Objectives

At the conclusion of this program, students will be able to:

- Detect various types of compromise and have an understanding of penetration testing and vulnerability scanning concepts
- Install, configure, and deploy network components while assessing and troubleshooting issues to support organizational security
- Implement secure network architecture concepts and systems design
- Install and configure identity and access services, as well as management controls
- Implement and summarize risk management best practices and the business impact
- Install and configure wireless security settings and implement public key infrastructure
- Be familiar with every objective on the CompTIA Security+ Exam
- Employ tips to prepare for and pass the exam

IT Cyber Security Professional with CompTIA Security+ Detailed Student Objectives:

THREATS, ATTACKS AND VULNERABILITIES

COMPROMISE INDICATORS AND MALWARE

- Identify types of Malware
- Understand a identify indicators of compromise
- Understand Malware IOC

CYBER ATTACKS

- Understand how to anticipate cyber attacks
- Understand social engineering
- Understand and identify application and service attacks
- Identify wireless attacks
- Implement a plan around Typo Squatting

THREAT ACTORS AND ATTRIBUTES

- Identify actor types and attributes
- Understand Open Source Threat Intelligence (OSINT)
- Implement OSINT measures

PENETRATION TESTING

- Understand Pen Testing Concepts
- Employ Pen Testing Techniques
- Work through Passive Recon events

VULNERABILITY SCANNING

- Distinguish between penetration and vulnerability testing
- Explore passive and active scanning techniques
- Understand and identify common findings
- Employ passive scanning techniques

VULNERABILITY IMPACT

- Understand various scanning techniques
- Understand common findings
- Employ Port Scanning techniques

TOOLS AND TECHNOLOGIES

NETWORK COMPONENTS

- Install and configure perimeter and networking components from both an operational and security perspective including:
    - Firewalls
    - Filters and Proxies
    - IDS and IPS
    - Virtual Private Networks (VPNs)
    - Layer 1 and 2 Devices
    - Routers and Load Balancers
    - Access Points
    - NACs, DPPs, and Mail Gateways
    - SIEM
    - Create Firewall Rules

SECURITY POSTURE

- Understand the importance of using security scanners and analyzers in assessing and devising security posture
- Understand the importance of using command line tools for security posture assessment
- Understand one of the most versatile security tools: Nmap

COMMON SECURITY ISSUES

- Identify and address configuration issues and solutions
- Identify and address operational issues and solutions
- Identify and address personnel issues and solutions
- Perform a "5 Whys" root cause analysis

ACTIVITY AND ERROR OUTPUT REPORTING

- Survey the type of activity and error reporting and output we can expect from network devices including:
    - Firewalls
    - HIDS/HIPS
    - Antivirus
    - Patch Management Tools
    - Unified Threat management
    - Data Loss Prevention (DLP)
    - Data Execution Prevention (DEP)
    - File Integrity Check
- Local Host Reporting

SECURE MOBILE DEVICE DEPLOYMENT

- Understand and select mobile device connection methods
- Design and implement mobile device management strategies
- Understand and mitigate mobile device concerns including attack factors
- Design and deploy a mobile device ownership decision tree

SECURE PROTOCOLS

- Understand the practical application and use cases for secure communication protocols
- Understand the practical application and use cases for secure network and administration protocols
- Use a protocol analyzer to demonstrate the difference between a secure and insecure protocol

ARCHITECTURE AND DESIGN

FRAMEWORKS, CONFIGURATION GUIDES, AND BEST PRACTICES

- Recognize a variety of global, government, sector-specific and industry security resources
- Understand the use cases and purposes of different security resources available
- Apply existing security frameworks, configuration guides and best practices in implementing and maintaining security controls
- Use a configuration tool

SECURE NETWORK ARCHITECTURE

- Meet security objectives by using zones including demilitarized zones (DMZs), extra and intranets
- Meet security objectives by using isolation techniques including virtual local area networks (VLAN)s, virtual machines (VMs) and air gapped networks
- Understand the criticality of proper device placement
- Understand and implement isolation techniques

SECURE SYSTEM DESIGN

- Implement hardware security
- Implement firmware security
- Implement operating system security
- Harden operating systems

SECURE STAGING AND DEPLOYMENT

- Describe deployment best practices
- Describe dev, test, stage and prod strategies
- Describe staging and deployment best practices and scheduling for developed or acquired code
- Understand the importance of preserving the integrity of the production environment
- Describe process flow as it relates to deployment and staging

EMBEDDED SECURITY SYSTEMS

- Describe embedded security systems and their function
- Explain why embedded systems are vulnerable to attack
- Describe best practices for evaluating and security embedded systems

- Describe available resources

SECURE APPLICATION DEVELOPMENT AND DEPLOYMENT

- Describe traditional and emerging software development techniques
- Describe secure coding techniques
- Explain the importance of code quality and code testing
- Understand and identify 3 types of code attacks:
    - Sequel injection
    - Persistent cross-site scripting, and
    - Reflective cross-site scripting

CLOUD AND VIRTUALIZATION

- Examine the security and performance features of virtualization
- Describe the security and performance features of cloud service models including Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)
- Describe the security and performance features as well as customer impact of cloud deployment models including private, public, community and hybrid cloud models
- Create and configure a virtual machine

RISK REDUCING RESILIENCY AND AUTOMATION

- Describe automation techniques for risk reduction likelihood and/or impact
- Explain Nonpersistence in order to mitigate the permanence of any changes
- Describe scalability by scaling up or scaling out
- Describe elasticity concepts necessary to dynamically cope with workload increases and decreases
- Explain availability as a measure of a system's uptime and how it relates to resiliency
- Describe fault tolerance including Redundant Array of Independent Disks (RAID)
- Distinguish between active and passive redundancy
- Explain RAID level 1 and 5

PHYSICAL SECURITY CONTROLS

- Explain the importance of building and facility security around physical assets including preventative, deterrent and detective access controls and workplace safety
- Explain the effects and consideration necessary around environmental issues such as air flow, heat, humidity, electrostatic discharge, data emanation, fire and power
- Describe Crime Prevention Through Environmental Design (CPTED) philosophy

IDENTITY AND ACCESS MANAGEMENT

IDENTITY AND ACCESS MANAGEMENT STRATEGIES

- Understand Identification and Authentication requirement
- Understand and implement identity management
- Employ Transitive Trust principles

IDENTITY AND ACCESS SERVICES

- Understand network identity and access services
- Understand web identity and access services

- Implement OAuth 2.0 practices

IDENTITY AND ACCESS MANAGEMENT CONTROLS

- Understand and use authentication controls
- Utilize access control models
- DAC Permissions

ACCOUNT MANAGEMENT PRACTICES

- Account Types
- General Concepts
- Account Auditing
- **Security in Action:** Account Policy Enforcement

IDENTITY AND ACCESS MANAGEMENT

POLICIES, PLANS AND PROCEDURES

- Security Policies and Agreements
- Personnel Management
- Security Awareness Training
- **Security in Action:** Policies, Standards and Procedures

BUSINESS IMPACT ANALYSIS

- Business Impact Analysis
- Privacy Impact and Threshold Assessments
- **Security in Action:** BIA Metrics

RISK MANAGEMENT & ASSESSMENT

- Risk Management
- Risk Assessments
- Testing and Change Management
- **Security in Action:** Quantitative Risk Assessment

INCIDENT RESPONSE PROCEDURES

- Incident Response Plans
- Incident Response Process
- **Security in Action:** IR Response Creating a Playbook

FORENSICS

- Forensic Fundamentals
- Data Acquisitions
- **Security in Action:** Forensic Techniques

DISASTER RECOVERY AND CONTINUITY OF OPERATIONS

- Recovery and Restoration
- Continuity of Operations Planning
- **Security in Action:** Site Selection Decision Tree

SECURITY CONTROLS

- Comparing and Contrasting Controls

- **Security in Action:** Technical Control Crossover

DATA SECURITY AND PRIVACY

- Data Protection and Classification
- Data Retention and Destruction
- **Security in Action:** Disk Wiping

CRYPTOGRAPHY AND PKI

CRYPTOGRAPHY CONCEPTS

- Cryptography Basics
- Steganography
- **Security in Action:** Basic Steganography

CRYPTOGRAPHIC ALGORITHMS

- Symmetric Encryption
- Asymmetric Encryption
- Hashing
- Digital Signatures
- **Security in Action:** Hashing

WIRELESS SECURITY STANDARDS

- Wireless Cryptographic Protocols
- **Security in Action:** WPS Issues

PUBLIC KEY INFRASTRUCTURE (PKI)

- Digital Certificates
- Key Lifecycle Management
- Cryptographic Attacks
- **Security in Action:** Crypto Vulnerabilities

EXAM PREPARATION

- Understanding the Security+ Exam Structure
- Test Taking Strategies
- The Week Leading Up to You Exam
- What to Expect at the Testing Center
- Attaining and Maintaining Your Security+ Certification