Training: CompTIA
CompTIA Security+ Prep Course

TRAINING GOALS:

CompTIA's Security+ certification is a global certification that validates the foundational cybersecurity skills necessary to perform core security functions and pursue an IT security career.

This course can benefit you in two ways. If you intend to pass the CompTIA Security+ (Exam SY0-701) certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of IT security. Today's job market demands individuals with demonstrable skills, and the information and activities in this course can help you build your cybersecurity skill set so that you can confidently perform your duties in any entry-level security role.

On course completion, you will be able to achieve the following:

- Summarize fundamental security concepts.
- Compare threat types.
- Explain appropriate cryptographic solutions.
- Implement identity and access management.
- Secure enterprise network architecture.
- Secure cloud network architecture.
- Explain resiliency and site security concepts.
- Explain vulnerability management.
- Evaluate network security capabilities.
- Assess endpoint security capabilities.
- Enhance application security capabilities.
- Explain incident response and monitoring concepts.
- Analyze indicators of malicious activity.
- Summarize security governance concepts.
- Explain risk management processes.
- Summarize data protection and compliance concepts.

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

Job roles that benefit from Security+ skills

- Cybersecurity Analyst (SOC Analyst)
- Security Administrator
- Systems Administrator
- Network Administrator
- Junior IT Auditor
- Security Consultant
- Technical Support Engineer
- Security Specialist

Each participant in an authorized training CompTIA Security+ Prep Course held in Exclusive Networks will receive a free SY0-701 CompTIA Security+ Certification Exam vouchers.

CONSPECT:

- Summarize Fundamental Security Concepts
  - Security Concepts
    - Information Security
    - Cybersecurity Framework
    - Gap Analysis
    - Access Control
    - Assisted Live Lab: Exploring The Lab Environment
    - Assisted Live Lab: Perform System Configuration Gap Analysis
  - Security Controls
    - Security Control Categories
    - Security Control Functional Types
    - Information Security Roles and Responsibilities
    - Information Security Competencies
    - Information Security Business Units
    - PBQ: Compare and Contrast Security Control and Framework Types
    - Assisted Live Lab: Configuring Examples Of Security Control Types
- Compare Threat Types
  - Threat Actors
    - Vulnerability, Threat, and Risk

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

        - Attributes of Threat Actors
        - Motivations of Threat Actors
        - Hackers and Hacktivists
        - Nation-State Actors
        - Organized Crime and Competitors
        - Internal Threat Actors
    - Attack Surfaces
        - Attack Surface and Threat Vectors
        - Vulnerable Software Vectors
        - Network Vectors
        - Lure-Based Vectors
        - Message-Based Vectors
        - Supply Chain Attack Surface
        - Assisted Live Lab: Finding Open Service Ports
    - Social Engineering
        - Human Vectors
        - Impersonation and Pretexting
        - Phishing and Pharming
        - Typosquatting
        - Business Email Compromise
        - PBQ: Compare and Contrast Social Engineering Techniques
        - Assisted Live Lab: Using Set To Perform Social Engineering
- Explain Cryptographic Solutions
    - Cryptographic Algorithms
        - Cryptographic Concepts
        - Symmetric Encryption
        - Key Length
        - Asymmetric Encryption
        - Hashing
        - Digital Signatures
        - PBQ: Identify Cryptographic Modes of Operations
        - Applied Live Lab: Using Storage Encryption
    - Public Key Infrastructure
        - Certificate Authorities
        - Digital Certificates
        - Root of Trust

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

        - Certificate Signing Requests
        - Subject Name Attributes
        - Certificate Revocation
        - Key Management
        - Cryptoprocessors and Secure Enclaves
        - Key Escrow
        - PBQ: Implement Certificates and Certificate Authorities
    - Cryptographic Solutions
        - Encryption Supporting Confidentiality
        - Disk and File Encryption
        - Database Encryption
        - Transport Encryption and Key Exchange
        - Perfect Forward Secrecy
        - Salting and Key Stretching
        - Blockchain
        - Obfuscation
        - Assisted Live Lab: Using Hashing And Salting
- Implement Identity and Access Management
    - Authentication
        - Authentication Design
        - Password Concepts
        - Password Managers
        - Multifactor Authentication
        - Biometric Authentication
        - Hard Authentication Tokens
        - Soft Authentication Tokens
        - Passwordless Authentication
        - Assisted Live Lab: Managing Password Security
    - Authorization
        - Discretionary and Mandatory Access Control
        - Role- and Attribute-Based Access Control
        - Rule-Based Access Control
        - Least Privilege Permission Assignments
        - User Account Provisioning
        - Account Attributes and Access Policies
        - Account Restrictions

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

        - Privileged Access Management
        - PBQ: Implement an Access Control Model
        - Assisted Live Lab: Managing Permissions
    - Identity Management
        - Local, Network, and Remote Authentication
        - Directory Services
        - Single Sign-on Authentication
        - Single Sign-on Authorization
        - Federation
        - Security Assertion Markup Language
        - Open Authorization
- Secure Enterprise Network Architecture
    - Enterprise Network Architecture
        - Architecture and Infrastructure Concepts
        - Network Infrastructure
        - Switching Infrastructure Considerations
        - Routing Infrastructure Considerations
        - Security Zones
        - Attack Surface
        - Port Security
        - Physical Isolation
        - Architecture Considerations
    - Network Security Appliances
        - Device Placement
        - Device Attributes
        - Firewalls
        - Layer 4 and Layer 7 Firewalls
        - Proxy Servers
        - Intrusion Detection Systems
        - Next-Generation Firewalls and Unified Threat Management
        - Load Balancers
        - Web Application Firewalls
    - Secure Communications
        - Remote Access Architecture
        - Transport Layer Security Tunneling
        - Internet Protocol Security Tunneling

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

        - Internet Key Exchange
        - Remote Desktop
        - Secure Shell
        - Out-of-Band Management and Jump Servers
        - PBQ: Implement Secure Remote Access Protocols
        - Assisted Live Lab: Setting Up Remote Access
        - Assisted Live Lab: Using Ipsec Tunneling
- Secure Cloud Network Architecture
    - Cloud Infrastructure
        - Cloud Deployment Models
        - Cloud Service Models
        - Responsibility Matrix
        - Centralized and Decentralized Computing
        - Resilient Architecture Concepts
        - Application Virtualization and Container Virtualization
        - Cloud Architecture
        - Cloud Automation Technologies
        - Software Defined Networking
        - Cloud Architecture Features
        - Cloud Security Considerations
        - PBQ: Analyze Infrastructure Types and Functions
        - Assisted Live Lab: Using Containers
        - Assisted Live Lab: Using Virtualization
    - Embedded Systems and Zero Trust Architecture
        - Embedded Systems
        - Industrial Control Systems
        - Internet of Things
        - Deperimeterization and Zero Trust
        - Zero Trust Security Concepts
- Explain Resiliency and Site Security Concepts
    - Asset Management
        - Asset Tracking
        - Asset Protection Concepts
        - Data Backups
        - Advanced Data Protection
        - Secure Data Destruction

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

        - Applied live Lab: Implement Backups
        - Assisted Live Lab: Performing Drive Sanitization
    - Redundancy Strategies
        - Continuity of Operations
        - Capacity Planning Risks
        - High Availability
        - Clustering
        - Power Redundancy
        - Diversity and Defense in Depth
        - Deception Technologies
        - Testing Resiliency
        - PBQ: Incorporate Redundancy Strategies
    - Physical Security
        - Physical Security Controls
        - Site Layout, Fencing, and Lighting
        - Gateways and Locks
        - Security Guards and Cameras
        - Alarm Systems and Sensors
- Explain Vulnerability Management
    - Device and OS Vulnerabilities
        - Operating System Vulnerabilities
        - Vulnerability Types
        - Zero-Day Vulnerabilities
        - Misconfiguration Vulnerabilities
        - Cryptographic Vulnerabilities
        - Sideloading, Rooting, and Jailbreaking
        - PBQ: Identify Types of Vulnerabilities
    - Application and Cloud Vulnerabilities
        - Application Vulnerabilities
        - Evaluation Scope
        - Web Application Attacks
        - Cloud-based Application Attacks
        - Supply Chain
        - Assisted Live Lab: Exploiting And Detecting Sqli
    - Vulnerability Identification Methods
        - Vulnerability Scanning

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Threat Feeds
- Deep and Dark Web
- Other Vulnerability Assessment Methods
- Assisted Live Lab: Working With Threat Feeds

- Vulnerability Analysis and Remediation
  - Common Vulnerabilities and Exposures
  - False Positives, False Negatives, and Log Review
  - Vulnerability Analysis
  - Vulnerability Response and Remediation
  - Assisted Live Lab: Performing Vulnerability Scans

- Evaluate Network Security Capabilities
  - Network Security Baselines
    - Benchmarks and Secure Configuration Guides
    - Wireless Network Installation Considerations
    - Wireless Encryption
    - Wi-Fi Authentication Methods
    - Network Access Control
    - PBQ: Implement Secure Wireless Infrastructure
    - Assisted Live Lab: Understanding Security Baselines
  - Network Security Capability Enhancement
    - Access Control Lists
    - Intrusion Detection and Prevention Systems
    - IDS and IPS Detection Methods
    - Web Filtering
    - Applied Live Lab: Implementing A Firewall

- Assess Endpoint Security Capabilities
  - Implement Endpoint Security
    - Endpoint Hardening
    - Endpoint Protection
    - Advanced Endpoint Protection
    - Endpoint Configuration
    - Hardening Techniques
    - Hardening Specialized Devices
    - Assisted Live Lab: Using Group Policy
    - Applied Live Lab: Hardening
  - Mobile Device Hardening

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

        - Mobile Hardening Techniques
        - Full Device Encryption and External Media
        - Location Services
        - Cellular and GPS Connection Methods
        - Wi-Fi and Tethering Connection Methods
        - Bluetooth Connection Methods
        - Near-Field Communications and Mobile Payment Services
        - PBQ: Implement Mobile Device Management
- Enhance Application Security Capabilities
    - Application Protocol Security Baselines
        - Secure Protocols
        - Transport Layer Security
        - Secure Directory Services
        - Simple Network Management Protocol Security
        - File Transfer Services
        - Email Services
        - Email Security
        - Email Data Loss Prevention
        - DNS Filtering
        - PBQ: Modify Enterprise Capabilities to Enhance Securtiy
        - Assisted Live Lab: Performing Dns Filtering
    - Cloud and Web Application Security Concepts
        - Secure Coding Techniques
        - Application Protections
        - Software Sandboxing
        - Assisted Live Lab: Configuring System Monitoring
- Explain Incident Response and Monitoring Concepts
    - Incident Response
        - Incident Response Processes
        - Preparation
        - Detection
        - Analysis
        - Containment
        - Eradication and Recovery
        - Lessons Learned
        - Testing and Training

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

        - Threat Hunting
        - PBQ: Summarize Incident Response Procedures
        - Applied Live Lab: Incident Response Detection
    - Digital Forensics
        - Due Process and Legal Hold
        - Acquisition
        - System Memory Acquisition
        - Disk Image Acquisition
        - Preservation
        - Reporting
        - Applied Live Lab: Performing Digital Forensics
    - Data Sources
        - Data Sources, Dashboards, and Reports
        - Log Data
        - Host Operating System Logs
        - Application and Endpoint Logs
        - Network Data Sources
        - Packet Captures
        - Metadata
        - Applied Live Lab: Using Network Sniffers
    - Alerting and Monitoring Tools
        - Security Information and Event Management
        - Alerting and Monitoring Activities
        - Alert Tuning
        - Monitoring Infrastructure
        - Monitoring Systems and Applications
        - Benchmarks
        - Assisted Live Lab: Performing Root Cause Analysis
- Analyze Indicators of Malicious Activity
    - Malware Attack Indicators
        - Malware Classification
        - Computer Viruses
        - Computer Worms and Fileless Malware
        - Spyware and Keyloggers
        - Backdoors and Remote Access Trojans
        - Rootkits

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

        - Ransomware, Crypto-Malware, and Logic Bombs
        - TTPs and IoCs
        - Malicious Activity Indicators
        - PBQ: Analyze Indicators of Malware-Based Attacks
        - Assisted Live Lab: Detecting And Responding To Malware
    - Physical and Network Attack Indicators
        - Physical Attacks
        - Network Attacks
        - Distributed Denial of Service Attacks
        - On-Path Attacks
        - Domain Name System Attacks
        - Wireless Attacks
        - Password Attacks
        - Credential Replay Attacks
        - Cryptographic Attacks
        - Malicious Code Indicators
        - Assisted Live Lab: Understanding Onpath Attacks
    - Application Attack Indicators
        - Application Attacks
        - Replay Attacks
        - Forgery Attacks
        - Injection Attacks
        - Directory Traversal and Command Injection Attacks
        - URL Analysis
        - Web Server Logs
- Summarize Security Governance Concepts
    - Policies, Standards, and Procedures
        - Policies
        - Procedures
        - Standards
        - Legal Environment
        - Governance and Accountability
        - PBQ: Apply Appropriate Policies and Regulations
        - Adaptive Live Lab: Using A Playbook
    - Change Management
        - Change Management Programs

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

        - Allowed and Blocked Changes
        - Restarts, Dependencies, and Downtime
        - Documentation and Version Control
        - Assisted Live Lab: Implementing Allow Lists And Deny Lists
    - Automation and Orchestration
        - Automation and Scripting
        - Automation and Orchestration Implementation
        - Assisted Live Lab: Use Cases Of Automation And Scripting
- Explain Risk Management Processes
    - Risk Management Processes and Concepts
        - Risk Identification and Assessment
        - Risk Management Strategies
        - Risk Management Processes
        - Business Impact Analysis
    - Vendor Management Concepts
        - Vendor Selection
        - Vendor Assessment Methods
        - Legal Agreements
    - Audits and Assessments
        - Attestation and Assessments
        - Penetration Testing
        - Exercise Types
        - Assisted Live Lab: Performing Reconnaissance
        - Assisted Live Lab: Performing Penetration Testing
- Summarize Data Protection and Compliance Concepts
    - Data Classification and Compliance
        - Data Types
        - Data Classifications
        - Data Sovereignty and Geographical Considerations
        - Privacy Data
        - Privacy Breaches and Data Breaches
        - Compliance
        - Monitoring and Reporting
        - Data Protection
        - Data Loss Prevention
        - PBQ: Explain Privacy and Data Sensitivity Concepts

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- PBQ: Apply Appropriate Techniques to Secure Data
- Personnel Policies
  - Conduct Policies
  - User and Role-Based Training
  - Training Topics and Techniques
  - Security Awareness Training Lifecycle
  - Assisted Live Lab: Training And Awareness Through Simulation
  - Challenge Live Lab: Network Incident Investigation And Remediation

REQUIREMENTS:

Recommended experience: CompTIA Network+ and two years of experience working in a security/ systems administrator job role.

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by CompTIA (course completion). This course will help prepare you for the CompTIA Security+ certification exam, which is available through the Pearson VUE test centers.

Each participant in an authorized training CompTIA Security+ Prep Course held in Exclusive Networks will receive a free SY0-701 CompTIA Security+ Certification Exam vouchers.

TRAINER:

Authorized CompTIA Trainer.

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310