Training: CompTIA
CompTIA CySA+ Prep Course

TRAINING GOALS:

CompTIA Cybersecurity Analyst (CySA+) is a cybersecurity certification that validates your ability to detect, analyze, and respond to threats in security operations and vulnerability management roles. It focuses on incident detection, response, and continuous monitoring in modern environments, while managing vulnerabilities and effectively communicating critical risks.

This course can benefit you in two ways. If you intend to pass the CompTIA CySA+ (Exam CS0-004) 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 security analyst. Today's job market demands individuals with demonstrable skills, and the information and activities in this course can help you build your security analyst skill set so that you can confidently perform your duties in any security analyst role.

Skills you'll learn

- Identify and investigate suspicious activity across networks, endpoints, and cloud environments to uncover potential security threats.
- Monitor and analyze data using industry-standard tools such as SIEM and EDR platforms.
- Identify, prioritize, and mitigate vulnerabilities using risk-based approaches.
- Investigate and respond to security incidents using structured processes and real-world techniques.
- Clearly communicate security findings and risks to stakeholders through reports and dashboards.
- Apply security practices across cloud and hybrid environments while supporting efficient and effective operations.

Job roles that benefit from CySA+ skills

- Application Security Analyst
- Threat Hunter
- Threat Intelligence Analyst

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

- Vulnerability Analyst
- Security Operations Center (SOC) Analyst
- Security Architect
- Cybersecurity Engineer

Each participant in an authorized training CompTIA CySA+ Prep Course held in Exclusive Networks will receive a free CS0-004 CompTIA CySA+ Certification Exam voucher.

CONSPECT:

- Identifying Security Operations Fundamentals
  - Cybersecurity Foundations
    - What is Cybersecurity
    - Role of the Security Operations Center
    - Job Roles in the SOC
    - Job Roles Using CySA+
    - Incident Lifecycle
  - Governance, Policies, and Controls
    - The Role of Governance
    - Policy Concepts
    - Policies
    - Service Level Objectives
    - Control Types
    - Control Functions
  - Introduction to Incident Response in the SOC
    - Incident Response and Roles
    - Escalation Paths
    - Incident Response Lifecycle
- Applying Risk Management Strategies
  - Risk Concepts
    - Risk Mindset
    - Risk States
    - Applying the Appropriate Risk Strategies
    - Risk Management Response
  - Threat Modeling Frameworks
    - Threat Modeling

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

        - Threat Modeling Analysis
        - The STRIDE Framework
- Managing System Security and Configurations
    - Attack Surface Management
        - Attack Surfaces
        - Indicators of Malicious Activity
        - Scan for Open Ports with Netstat
        - Discovery Scanning
        - Network Scanning Tools
        - Track Port Usage with TCPView
        - Active Threats
        - Detect Malicious Network Traffic with a Honeypot
        - Prioritize Threats
        - Mitigation Strategies
        - Disable IIS Banner Broadcasting
        - Disable DNS Zone Transfers
    - System Hardening
        - Hardening Steps
        - File Systems
        - The Windows File System
        - View Windows Services
        - The Linux File System
        - View Linux Services
        - System Processes
        - Patch Management
        - Configuration Management
- Comparing System Architectures
    - Infrastructure and System Architecture
        - Infrastructure and System Architecture Fundamentals
        - Cloud-Native Technologies
        - Virtualization
        - Containerization
        - Application Programming Interfaces (APIs)
    - Modern Network Architectures
        - Zero Trust Network Architecture
        - Network Segmentation

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

        - Zero Trust Implementation
        - Applying System and Network Architecture Concepts in Security Operations
        - Secure Access Service Edge
        - Hybrid Cloud
        - Hybrid Cloud Configuration
        - Hybrid Cloud Security
        - Cloud Access Security Broker
    - Critical Infrastructure and Industrial Controls
        - Operational Technology (OT)
        - Scan for IoT with Nmap
        - Industrial Control Systems (ICS)
        - Supervisory Control and Data Acquisition (SCADA) Systems
        - Industrial Control Systems Security
- Applying Access Management
    - Identity and Access Management
        - Identity Concepts
        - Explore Privilege Creep
        - Authentication Methods
        - Configure Password Policies
        - Configure User Account Control
        - Federated Identity Management
        - Authorization
        - Escalate Privileges with Curl
        - Privileged Access Management
        - Change File Permissions with icacls
        - Secrets Management
    - Device and Endpoint Management
        - Mobile Device Management
        - Mobile Device Controls
        - Securing Mobile Devices
        - Mobile Device Security
        - Recover Deleted Files with Recuva
        - Endpoint Management
        - Encrypt a Hard Disk
        - Wipe Disk Space
    - Data Protection and Cryptography

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

        - Data Protection Fundamentals
        - Data Loss Prevention
        - Cryptography
        - Symmetric Encryption
        - Asymmetric Encryption
        - Hashing
        - Verify MD5 Hash Integrity
- Threat Intelligence and Threat Hunting
    - Threat Actor Concepts
        - Threat Actors
        - Advanced Persistent Threat
        - Tactics, Techniques, and Procedures
        - Pyramid of Pain
        - Heat Maps
    - Threat Intelligence Sources
        - Intelligence Collection Sources
        - Reconnaissance with theHarvester
        - Reconnaissance with Nmap
        - Intelligence Collection Methods
        - Confidence Levels
        - Confidence Level Factors
        - Types of Indicators of Compromise
        - Indicators of Compromise Analysis and Application
    - Threat Hunting
        - Threat Mapping
        - Cyber Deception
        - Breadcrumbs and Deceptive Endpoints
- Assessing Network Vulnerabilities
    - Vulnerability Scanning Foundations
        - Asset Inventory
        - Vulnerability Scan Impact
        - Vulnerability Scan Scheduling
        - Special Cases for Vulnerability Scans
        - Implementing Vulnerability Scanning Methods and Concepts
    - Vulnerability Scan Types
        - Establishing A Baseline

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

    - Internal and External Scans
    - Agent and Agentless Scans
    - Credentialed and Non-Credentialed Scans
    - Passive and Active Scanning
    - Mapping and Fingerprinting Scans
- Select Vulnerability Tools
    - Enumeration Concepts
    - Angry IP Scanner
    - Masscan
    - Nmap and Zenmap
    - Metasploit
    - Enumerate with Metasploit
    - Bypass Windows Firewall with Metasploit
    - Maltego
    - Recon-ng
    - Nessus
    - Configure a Nessus Scan
    - Analyze Scan Results from a Nessus Report
    - Nuclei
    - Open Vulnerability Assessment Scanner (OpenVAS)
    - Atomic Red Team
    - Caldera
- Vulnerability Analysis and Prioritization
    - Vulnerability Evaluation Criteria
    - Analyzing Data to Prioritize Vulnerabilities
    - The Common Vulnerability Scoring System (CVSS)
    - CVSS Metric Groups Overview
    - CVSS Base Metrics
    - CVSS Environmental Metrics
    - CVSS Supplemental Metrics
    - CVSS Threat Metric
    - The Exploitability Prediction Scoring System (EPSS)
    - EPSS Implementation
    - Vulnerabilities in Context
    - Mitigation Strategies
- Vulnerability and Incident Reporting

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

        - Purpose of Reporting and Communication
        - Reporting Concepts
        - Remediation Planning and Tracking
        - Inhibitors to Remediation
        - Metrics and Key Performance Indicators
- Managing Incident Response and Communication
    - Manage Logs
        - Logging Fundamentals
        - Log Configuration
        - Configure Collector-Initiated Subscriptions
        - Configure Source-Initiated Subscriptions
        - Log Ingestion
        - Use pfSense to Log Events
        - Log Security
        - Time Synchronization
        - Log Retention
        - Evaluate Event Logs in pfSense
    - Incident Escalation
        - Incident Declaration and Escalation
        - Communication Plan
        - Execute Incident Response Reporting and Communication
        - Executive Summary
    - Post-Incident Actions
        - Preparing for Post-Incident Activity Phases
        - Post-incident Reporting
        - After-action Reports
        - Lessons Learned Meetings
        - Root Cause Analysis
        - Shift and Turnover Reports
        - Internal Threat Intelligence Reports
    - Incident Response Metrics
        - Key Performance Indicators
        - KPI Challenges
        - Mean Time Metrics
        - Alert Volume
        - True and False Positive Rates

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

        - Phishing Click Rates
- Executing Incident Response Plans
    - Attack Methodology Frameworks
        - Cyber Kill Chain
        - Cyber Kill Chain Stages
        - Cyber Kill Chain Application
        - Diamond Model of Intrusion Analysis
        - Diamond Model Application
        - MITRE ATT&CK Framework
        - MITRE ATT&CK Components
    - The Incident Response Process
        - Incident Response Process Overview
        - Preparation
        - Detection
        - Search Memory Dump for Malware
        - Analysis
        - Containment
        - Eradication
        - Recovery
        - Post-Incident Activities
    - Incident Response Techniques
        - Incident Analysis and Triage
        - Containment Techniques
        - Escalation Techniques
        - Create a Forensic Drive Image with Guymager
        - Evidence Acquisition
        - Examine a Forensic Drive Image with Autopsy
        - Eradication Techniques
        - Continuous Monitoring
- Analyzing Malicious Activity
    - Threat Detection and Analysis Tools
        - Decoding and Parsing
        - Log Analysis Concepts
        - Log Analysis with SIEM Platforms
        - Threat Intelligence Platforms
        - File Formats

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

- Sandboxing Concepts
- Sandboxing Tools

- Host Indicators of Compromise
  - Indicators of Compromise
  - Anomalous System Behavior
  - Scanning and Terminating Processes
  - System-Related Indicators of Compromise
  - Endpoint Security Tools
  - File Analysis Tools
- Network Indicators of Compromise
  - Anomalous Network Behavior
  - Detect a Rogue Device
  - Packet Analysis Concepts
  - Irregular Peer-to-Peer Communication Intrusions IoCs
  - Detect Promiscuous Mode
  - Wireshark
  - Sniff Network Traffic with Wireshark
  - tcpdump
  - Capture Traffic with TCPDump
  - Launch a DoS and DDoS Attack
  - Snort Concepts
  - Snort Rules
  - Snort Use Cases
  - Intrusion Detection and Prevention with Snort
  - Suricata
  - Zeek
  - Domain and IP Reputation
- Application and Web-based Indicators
  - Anomalous Application Behavior
  - Analyzing Indicators of Compromise
  - Identity-based Indicators
  - Service Disruptions
  - Perform a SYN Flood
  - Email Indicators
  - Social Engineering
  - Use the Social Engineer Toolkit

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

- Automating Data Analysis
  - Scripting Fundamentals
    - The Purpose of Scripts
    - Script Variables and Arrays
    - Special Characters in Scripts
    - Script Functions and Comments
    - Script Execution
    - Loops
    - For Loops
    - While and Until Loops
    - Conditionals
    - Operators
  - Scripting Languages
    - Shell Scripting
    - Shell Variables, Arrays, and Escape Characters
    - Shell Functions, Loops, and Operators
    - PowerShell
    - PowerShell Variables, Arrays, and Escape Characters
    - PowerShell Functions, Loops, and Operators
    - Python
    - Python Components
    - Python Script Construction
    - Perform a Scan with Nmap Scripts
  - Security Analytics and Pattern Recognition
    - Pattern Recognition
    - Regular Expressions
    - Regex Example
    - Suspicious Command Interpretation
    - User and Entity Behavior Analytics (UEBA)
    - Automated Log Analysis
  - Technology and Tool Integration
    - Integrating Tools
    - Security Orchestration, Automation and Response
    - SOAR Workflows
    - Infrastructure as Code (IaC)
- Improving Processes with Automation

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

- Standardization and Team Coordination
  - Role of Efficiency in Security Operations
  - Process Improvement
  - Waste in Security Workflows
  - Process Frameworks
  - Standardization in Security Operations
  - Designing Standard Security Processes
  - Maintaining Processes and Standards
  - Playbooks and Runbooks
  - Playbook Maintenance
- Automation, Orchestration, and Enrichment
  - Streamline Security Operations
  - Data Enrichment
  - Rule and Alert Tuning
  - Dashboards
- AI Risks and Governance
  - Principles of Responsible AI Use
  - AI Principles in Practice
  - Discuss Risks with AI
  - AI Security Risks
  - AI Organizational Risks
  - AI Governance
  - AI Regulation Best Practices
  - Important AI Compliance Frameworks
  - Organizational AI Policies
  - External Compliance Impacts
- AI in Security Operations
  - AI Tools in Security Operations
  - AI Security Use Cases
  - Detection and Analysis
  - Testing and Management
  - AI and Incident Management
  - AI in Security Scripting
  - AI in Security Workflows
  - Automate Security Tasks
- Assessing Application Vulnerabilities

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

- Web and Application Vulnerability Analysis
  - Web Application Attacks
  - Browser Exploitation
  - Scan a Website with Acunetix
  - Burp Suite
  - Test a Web Application with Burp Suite
  - Zed Attack Proxy
  - Nikto
  - Scan a Webserver with Nikto
  - Third-Party Risks
  - Supply Chain Attacks
  - Extract Web Server Information
- Cloud Vulnerability Assessment
  - Cloud-Based Attacks
  - ScoutSuite
  - Use ScoutSuite to Analyze a Cloud Infrastructure
  - Additional Cloud Assessment Tools
  - Cloud-Related Indicators

- Securing Applications
  - Secure Software Development and Testing
    - Analyzing Vulnerabilities and Recommending Risk Mitigation
    - Application Security Testing
    - Software Assurance Maturity Model
    - Software Testing with Python
    - Secure Coding Best Practices
  - Application Attack Identification and Mitigation
    - Packet Analysis
    - Wireshark and Packet Analysis
    - Exploit SQL on a Web Page
    - Web Application Scanners
    - Find SQL Injection Flaws with sqlmap
    - Risk Reduction and Acceptance
    - Hidden Field Manipulation Attacks
    - Third-Party Risk Management

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

REQUIREMENTS:

Recommended experience: Network+, Security+, or equivalent knowledge, with a minimum of 4 years of hands-on experience as an incident response analyst, security operations center (SOC) analyst, or equivalent experience

Difficulty level



CERTIFICATE:

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

Each participant in an authorized training CompTIA CySA+ Prep Course held in Exclusive Networks will receive a free CS0-004 CompTIA CySA+ Certification Exam voucher.

TRAINER:

Authorized CompTIA Trainer.

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