Training: CompTIA
# CompTIA SecurityX Prep Course

## TRAINING GOALS:

The SecurityX Certification (formerly CASP+) is an advanced skill level cybersecurity certification designed for professionals with 10 years of general hands-on IT experience, with at least five of those years being broad hands-on IT security experience.

This course can benefit you in two ways. If you intend to pass the CompTIA SecurityX (Exam CAS-005) certification examination, this course can be a significant part of your preparation. However, certification is not the only key to professional success in the field of cybersecurity. Today's job market demands individuals have demonstrable skills, and the information and activities in this course can help you build your information security skill set so that you can confidently perform your duties as an advanced security practitioner.

Upon course completion, you will be able to:

- Summarize governance, risk, and compliance.
- Implement architecture and design.
- Understand security engineering.
- Apply security operations and incident response.

Skills you'll learn

- Design, implement, and integrate secure solutions across complex environments to support a resilient enterprise in security architecture and engineering.
- Use automation, monitoring, detection, and incident response to proactively support ongoing security operations.
- Apply security practices to cloud, on-premises, and hybrid environments to ensure enterprise-wide protection.
- Utilize cryptographic technologies and techniques while evaluating the impact of emerging trends, such as artificial intelligence, on information security.
- Implement governance, compliance, risk management, and threat modeling strategies across the enterprise.



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

- Validate advanced, hands-on skills in security architecture and senior security engineering within live environments.

Job roles that benefit from SecurityX skills

- Security Architect
- Senior Cybersecurity Engineer
- Security Consultant (Senior level)
- Technical Lead Analyst
- Security Manager / Director
- Cloud Security Architect
- Application Security Engineer
- Cybersecurity Risk Manager

This course is for "defense architects." It's ideal for those with years of experience who want to validate their competencies in designing systems resistant to advanced attacks (APTs), integrating cloud security, and managing risk at a strategic level.

*Each participant in an authorized training CompTIA SecurityX Prep Course held in Exclusive Networks will receive a free CAS-005 CompTIA SecurityX Certification Exam vouchers.*

## CONSPECT:

- Summarizing Governance, Risk, and Compliance
  - Implement Appropriate Governance Components
    - Security Program Documentation
    - Security Program Management
    - Governance Frameworks
    - Change / Configuration Management
    - Governance Risk and Compliance (GRC) Tools
    - Data Governance in Staging Environments
    - Legal and Privacy Implications of AI Use
  - Explain Legal Compliance
    - Awareness of Industry-Specific Compliance
    - Industry Standards



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

        - Security and Reporting Frameworks
        - Audits vs. Assessments vs. Certifications
        - Privacy Regulations
        - Awareness of Cross-Jurisdictional Compliance Requirements
    - Apply Risk Management Strategies
        - Impact Analysis
        - Risk Assessment and Management
        - Applying the Appropriate Risk Strategies
        - Third-Party Risk Management
        - Availability Risk Considerations
        - Confidentiality Risk Considerations
        - Integrity Risk Considerations
        - Privacy Risk Considerations
        - Risks of AI Usage
        - Crisis Management
        - Breach Response
- Implementing Architecture and Design
    - Apply Software Development
        - Security Requirements Definition
        - Software Assurance
        - Securely Integrating Software Applications
        - Continuous Integration/Continuous Deployment (CI/CD)
        - Supply Chain Risk Management
        - Hardware Assurance
        - End-of-Life (EOL) Considerations
    - Integrate Software Architecture
        - Attack Surface Management and Reduction
        - Detection and Threat-Hunting Enablers
        - Detection and Threat-Hunting Enablers Part 1
        - Detection and Threat-Hunting Enablers Part 2
        - Information and Data Security Design
        - Information and Data Security Design
        - Data Loss Prevention (DLP)
        - Implementing Data Security Techniques
        - Hybrid Infrastructures
        - Third-Party Integrations



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

    - Control Effectiveness
- Support Operational Resilience
    - Availability and Integrity Design Considerations
    - Network Traffic Inspection
    - Network Access Control & VPN
    - Proxies
    - Specialized Components
- Implement Cloud Infrastructure
    - Cloud Access Security Broker (CASB)
    - Shadow IT Detection
    - Shared Responsibility Model
    - CI/CD Pipeline
    - Continuous Integration/Continuous Deployment
    - Terraform
    - Ansible
    - Package Monitoring
    - Container Security
    - Container Orchestration
    - Serverless
    - API Security
    - Cloud vs. Customer-Managed
    - Cloud Data Security Considerations
    - Cloud Data Security Considerations
    - Cloud Control Strategies
    - Cloud Control Strategies
    - Customer-to-Cloud Connectivity
    - Cloud Service Integration
    - Cloud Service Adoption
- Integrate Zero Trust Concepts
    - Continuous Authorization
    - Context-Based Reauthentication
    - Network Architecture
    - Analyzing Security Requirements to Ensure Secure Network Architecture
    - API Integration and Validation
    - Asset Identification, Management, and Attestation
    - Security Boundaries



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

        - Deperimeterization
        - Defining Subject-Object Relationships
    - Troubleshoot using AAA and IAM
        - Provisioning/Deprovisioning
        - Federation
        - Conditional Access
        - Identity and Service Providers
        - Policy Decision and Enforcement Points
        - Access Control Models
        - Logging and Auditing
        - Public Key Infrastructure (PKI) Architecture
        - Access Control Systems
        - Subject Access Control
        - Biometrics
        - Secrets Management
        - Secrets Management
        - Cloud IAM Access and Trust Policies
        - Logging and Monitoring
        - Privilege Identity Management
        - Authentication and Authorization
- Understanding Security Engineering
    - Enhance Endpoint Security
        - Endpoint Detection Response (EDR)
        - Configure and Implement Endpoint Security Controls
        - Endpoint Privilege Management
        - Attack Surface Monitoring and Reduction
        - Endpoint Protection Tools
        - Mobile Device Management (MDM) Technologies
        - Applying Secure Configurations to Enterprise Mobility
        - Threat-actor tactics, techniques, and procedures (TTPs)
        - Specialized and Embedded Systems
        - Security and Privacy Considerations
        - Industry-Specific Challenges
        - Characteristics of Specialized/Legacy Systems
    - Configure Network Infrastructure
        - Network Misconfigurations



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

        - IPS/IDS Issues
        - Observability
        - Domain Name System (DNS) Security
        - Email Security
        - Cryptography Issues
        - Implementing the Appropriate PKI Solution
        - Resource Exhaustion
    - Initiate Security Automation
        - Hardware Security Technologies
        - Secure Boot
        - Hardware Security Features
        - Host-Based Encryption
        - Threat-Actor TTPs
        - Scripting, Scheduling and Event Triggers
        - Generative AI
        - Security Orchestration, Automation, and Response (SOAR)
        - Workflow Automation
    - Apply Cryptography Concepts
        - Post-Quantum Cryptography (PQC)
        - Key Stretching, Key Splitting, and Envelope Encryption
        - Homomorphic Encryption and Secure Multiparty Computation
        - Forward Secrecy, Mutual Authentication, and AEAD
        - Mutual Authentication
        - Cryptographic Performance vs. Security
        - Data Security States
        - Implementing the Appropriate Cryptographic Protocols and Algorithms
        - Encryption and Authentication Mechanisms
        - Data Protection Techniques
        - Blockchain and Immutable Records
        - Legal and Resource Considerations
        - Software Integrity and Provenance
        - Data Protection and Privacy
        - Data Integrity and Authenticity
        - Encryption Techniques
- Applying Security Operations and Incident Response
    - Perform Threat Modeling



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

        - Understanding and Profiling Threats
        - Structured Threat Assessment
        - Threat Modeling Methods
        - Attack Surface Determination
        - Modeling Applicability of Threats to the Organization/Environment
        - Threats to the Model
        - AI-Enabled Attacks
        - AI-Enabled Assistants/Digital Workers
    - Examine Security Monitoring
        - Data Collection and Integration
        - Data Processing and Behavioral Benchmarking
        - Incorporating Diverse Data Sources
        - Alerting Concepts and Practices
        - Reporting and Metrics
    - Analyze Known Attack Methods and Associated Mitigations
        - Vulnerabilities: Input and Output Manipulation
        - Vulnerabilities: Memory and Execution Vulnerabilities
        - Vulnerabilities: Cryptographic Issues
        - Vulnerabilities: System Configuration and Management
        - Vulnerabilities: Supply Chain and External Dependencies
        - Analyzing Vulnerabilities and Recommending Risk Mitigations
        - Mitigations: Input and Output Security
        - Mitigations: Secure Coding Practices
        - Mitigations: System Maintenance and Management
        - Mitigations: Data Security and Management
    - Apply Threat Hunting Tools and Technologies
        - Internal Intelligence Sources
        - External Intelligence Sources
        - Counterintelligence and Operational Security
        - Threat Intelligence Platforms (TIPs)
        - Indicator of Compromise (IoC) Sharing
        - Analyzing Indicators of Compromise
        - Rule-Based Languages
    - Evaluate Incident Analysis and Response
        - Malware Analysis
        - Malware Analysis



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

- Forensic Analysis
- Detection and Initial Analysis
- Metadata Analysis
- Continuous Improvement
- Preparedness and Prevention

## REQUIREMENTS:

Recommended experience: minimum of 10 years of general hands-on IT experience, including 5 years of hands-on security, with Network+, Security+, CySA+, Cloud+, and PenTest+ or equivalent knowledge.

## Difficulty level



## CERTIFICATE:

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

*Each participant in an authorized training CompTIA SecurityX Prep Course held in Exclusive Networks will receive a free CAS-005 CompTIA SecurityX Certification Exam vouchers.*

## TRAINER:

Authorized CompTIA Trainer.



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