Training: CompTIA
# CompTIA SecurityX Prep Course

## TRAINING GOALS:

CompTIA SecurityX (formerly CASP+ CompTIA Advanced Security Practitioner) is an advanced-level cybersecurity certification for security architects and senior security engineers charged with leading and improving an enterprise's cybersecurity readiness.

CompTIA SecurityX will certify the successful candidate has the knowledge and skills required to:

- Architect, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise.
- Use automation, monitoring, detection, and incident response to proactively support ongoing security operations in an enterprise environment.
- Apply security practices to cloud, on-premises, and hybrid environments.
- Consider cryptographic technologies and techniques, as well as the impact of emerging trends (e.g., artificial intelligence) on information security.
- Use the appropriate governance, compliance, risk management, and threat-modeling strategies throughout the enterprise.

SecurityX (formerly CASP+) is compliant with ISO 17024 standards and approved by the U.S. DoD to meet Directive 8140.03M requirements.

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

Jobs You Can Land With CompTIA Security+

- Security Architect
- Cybersecurity Engineer
- SOC Manager
- Cyber Risk Analyst
- Chief Information Security Officer (CISO)

## CONSPECT:

- Governance, Risk, and Compliance
    - Given a set of organizational security requirements, implement the appropriate



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

governance components
    - Security program documentation
    - Security program management
    - Governance frameworks
    - Change/configuration management
    - Governance risk and compliance (GRC) tools
    - Data governance in staging environments
- Given a set of organizational security requirements, perform risk management activities
    - Impact analysis
    - Risk assessment and management
    - Third-party risk management
    - Availability risk considerations
    - Confidentiality risk considerations
    - Integrity risk considerations
    - Privacy risk considerations
    - Crisis management
    - Breach response
- Explain how compliance affects information security strategies
    - Awareness of industry-specific compliance
    - Industry standards
    - Security and reporting frameworks
    - Audits vs. assessments vs. certifications
    - Privacy regulations
    - Awareness of cross-jurisdictional compliance requirements
- Given a scenario, perform threat-modeling activities
    - Actor characteristics
    - Attack patterns
    - Frameworks
    - Attack surface determination
    - Methods
    - Modeling applicability of threats to the organization/environment
- Summarize the information security challenges associated with artificial intelligence (AI) adoption
    - Legal and privacy implications
    - Threats to the model
    - AI-enabled attacks
    - Risks of AI usage



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- AI-enabled assistants/digital workers

- Security Architecture
  - Given a scenario, analyze requirements to design resilient systems
    - Component placement and configuration
    - Availability and integrity design Considerations
  - Given a scenario, implement security in the early stages of the systems life cycle and throughout subsequent stages
    - Security requirements definition
    - Software assurance
    - Continuous integration/continuous deployment (CI/CD)
    - Supply chain risk management
    - Hardware assurance
    - End-of-life (EOL) considerations
  - Given a scenario, integrate appropriate controls in the design of a secure architecture
    - Attack surface management and reduction
    - Detection and threat-hunting enablers
    - Information and data security design
    - DLP
    - Hybrid infrastructures
    - Third-party integrations
    - Control effectiveness
  - Given a scenario, apply security concepts to the design of access, authentication, and authorization systems
    - Provisioning/deprovisioning
    - Federation
    - Single sign-on (SSO)
    - Conditional access
    - Identity provider
    - Service provider
    - Attestations
    - Policy decision and enforcement points
    - Access control models
    - Logging and auditing
    - Public key infrastructure (PKI) architecture
    - Access control systems
  - Given a scenario, securely implement cloud capabilities in an enterprise environment
    - Cloud access security broker (CASB)



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Shadow IT detection
- Shared responsibility model
- CI/CD pipeline
- Terraform
- Ansible
- Package monitoring
- Container security
- Container orchestration
- Serverless
- API security
- Cloud vs. customer-managed
- Cloud data security considerations
- Cloud control strategies
- Customer-to-cloud connectivity
- Cloud service integration
- Cloud service adoption

- Given a scenario, integrate Zero Trust concepts into system architecture design
  - Continuous authorization
  - Context-based reauthentication
  - Network architecture
  - API integration and validation
  - Asset identification, management, and attestation
  - Security boundaries
  - Deperimeterization
  - Defining subject-object relationships

- Security Engineering
  - Given a scenario, troubleshoot common issues with identity and access management (IAM) components in an enterprise environment
    - Subject access control
    - Biometrics
    - Secrets management
    - Conditional access
    - Attestation
    - Cloud IAM access and trust policies
    - Logging and monitoring
    - Privilege identity management



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Authentication and authorization
- Given a scenario, analyze requirements to enhance the security of endpoints and servers
  - Application control
  - Endpoint detection response (EDR)
  - Event logging and monitoring
  - Endpoint privilege management
  - Attack surface monitoring and reduction
  - Host-based intrusion protection system/host-based detection system (HIPS/HIDS)
  - Anti-malware
  - SELinux
  - Host-based firewall
  - Browser isolation
  - Configuration management
  - Mobile device management (MDM) technologies
  - Threat-actor tactics, techniques, and procedures (TTPs)
- Given a scenario, troubleshoot complex network infrastructure security issues
  - Network misconfigurations
  - IPS/IDS issues
  - Observability
  - Domain Name System (DNS) security
  - Email security
  - Transport Layer Security (TLS) errors
  - Cipher mismatch
  - PKI issues
  - Issues with cryptographic implementations
  - DoS/distributed denial of service (DDoS)
  - Resource exhaustion
  - Network access control list (ACL) issues
- Given a scenario, implement hardware security technologies and techniques
  - Roots of trust
  - Security coprocessors
  - Virtual hardware
  - Host-based encryption
  - Self-encrypting drive (SED)
  - Secure Boot
  - Measured boot



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Self-healing hardware
- Tamper detection and countermeasures
- Threat-actor TTPs

- Given a set of requirements, secure specialized and legacy systems against threats
  - Operational technology (OT)
  - Internet of Things (IoT)
  - System-on-chip (SoC)
  - Embedded systems
  - Wireless technologies/radio frequency (RF)
  - Security and privacy considerations
  - Industry-specific challenges
  - Characteristics of specialized/legacy systems
- Given a scenario, use automation to secure the enterprise
  - Scripting
  - Cron/scheduled tasks
  - Event-based triggers
  - Infrastructure as code (IaC)
  - Configuration files
  - Cloud APIs/software development kits (SDKs)
  - Generative AI
  - Containerization
  - Automated patching
  - Auto-containment
  - Security orchestration, automation, and response (SOAR)
  - Vulnerability scanning and reporting
  - Security Content Automation Protocol (SCAP)
  - Workflow automation
- Explain the importance of advanced cryptographic concepts
  - Post-quantum cryptography (PQC)
  - Key stretching
  - Key splitting
  - Homomorphic encryption
  - Forward secrecy
  - Hardware acceleration
  - Envelope encryption
  - Performance vs. security



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Secure multiparty computation
- Authenticated encryption with associated data (AEAD)
- Mutual authentication

- Given a scenario, apply the appropriate cryptographic use case and/or technique
  - Use cases
  - Techniques

- Security Operations
  - Given a scenario, analyze data to enable monitoring and response activities
    - Security information event management (SIEM)
    - Aggregate data analysis
    - Behavior baselines and analytics
    - Incorporating diverse data sources
    - Alerting
    - Reporting and metrics
  - Given a scenario, analyze vulnerabilities and attacks, and recommend solutions to reduce the attack surface
    - Vulnerabilities and attacks
    - Mitigations
  - Given a scenario, apply threat-hunting and threat intelligence concepts
    - Internal intelligence sources
    - External intelligence sources
    - Counterintelligence and operational security
    - Threat intelligence platforms (TIPs)
    - Indicator of compromise (IoC) sharing
    - Rule-based languages
    - Indicators of attack
  - Given a scenario, analyze data and artifacts in support of incident response activities
    - Malware analysis
    - Reverse engineering
    - Volatile/non-volatile storage analysis
    - Network analysis
    - Host analysis
    - Metadata analysis
    - Hardware analysis
    - Data recovery and extraction
    - Threat response



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Preparedness exercises
- Timeline reconstruction
- Root cause analysis
- Cloud workload protection platform (CWPP)
- Insider threat

## REQUIREMENTS:

Minimum 10 years general hands on IT experience, 5 years being 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 Compendium CE will receive a free CAS-005 CompTIA SecurityX Certification Exam vouchers.*

## TRAINER:

Authorized CompTIA Trainer.



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007