CompTIA
SecurityX
CERTIFICATION
Xpert Series

CompTIA SecurityX Certification Exam Objectives

EXAM NUMBER: CAS-005 V5

CompTIA SecurityX CAS-005 V5 Certification Exam
Exam Objectives Document Version 6.0

Copyright © 2023 CompTIA, Inc. All rights reserved.

CompTIA

About the Exam

The CompTIA SecurityX (formerly CASP+) certification exam 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.

EXAM ACCREDITATION

The CompTIA SecurityX exam is accredited by the ANSI National Accreditation Board (ANAB) to show compliance with the International Organization for Standardization (ISO) 17024 standard and, as such, undergoes regular reviews and updates to the exam objectives.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

COMPTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse, or condone utilizing any content provided by unauthorized third-party training sites (aka “brain dumps”). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA’s exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka “brain dumps”), they should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam, although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

Copyright © 2023 CompTIA, Inc. All rights reserved.

TEST DETAILS

Required exam	CAS-005
Number of questions	Maximum of 90
Types of questions	Multiple-choice, performance-based
Length of test	165 minutes
Recommended experience	Minimum of 10 years of general, hands-on IT experience that includes at least 5 years of broad, hands-on IT security experience.
Passing Score	Pass/fail only; no scaled score

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN		PERCENTAGE OF EXAMINATION
1.0	Governance, Risk, and Compliance	20%
2.0	Security Architecture	27%
3.0	Security Engineering	31%
4.0	Security Operations	22%
Total		**100%**

Copyright © 2023 CompTIA, Inc. All rights reserved.

1.0 Governance, Risk, and Compliance

1.1 Given a set of organizational security requirements, implement the appropriate governance components.

- **Security program documentation**
  - Policies
  - Procedures
  - Standards
  - Guidelines
- **Security program management**
  - Awareness and training
    - Phishing
    - Security
    - Social engineering
    - Privacy
    - Operational security
    - Situational awareness
  - Communication
  - Reporting
  - Management commitment
  - Responsible, accountable, consulted, and informed (RACI) matrix
- **Governance frameworks**
  - Control Objectives for Information and Related Technologies (COBIT)
  - Information Technology Infrastructure Library (ITIL)
- **Change/configuration management**
  - Asset management life cycle
  - Configuration management database (CMDB)
  - Inventory
- **Governance risk and compliance (GRC) tools**
  - Mapping
  - Automation
  - Compliance tracking
  - Documentation
  - Continuous monitoring
- **Data governance in staging environments**
  - Production
  - Development
  - Testing
  - Quality assurance (QA)
  - Data life cycle management

1.2 Given a set of organizational security requirements, perform risk management activities.

- **Impact analysis**
  - Extreme but plausible scenarios
- **Risk assessment and management**
  - Quantitative vs. qualitative analysis
  - Risk assessment frameworks
  - Appetite/tolerance
  - Risk prioritization
  - Severity impact
  - Remediation
  - Validation
- **Third-party risk management**
  - Supply chain risk
  - Vendor risk
  - Subprocessor risk
- **Availability risk considerations**
  - Business continuity/disaster recovery
    - Testing
  - Backups
    - Connected
    - Disconnected
- **Confidentiality risk considerations**
  - Data leak response
  - Sensitive/privileged data breach
  - Incident response testing
  - Reporting
  - Encryption
- **Integrity risk considerations**
  - Remote journaling
  - Hashing
  - Interference
  - Antitampering
- **Privacy risk considerations**
  - Data subject rights
  - Data sovereignty
  - Biometrics
- **Crisis management**
- **Breach response**

Copyright © 2023 CompTIA, Inc. All rights reserved.

1.3 Explain how compliance affects information security strategies.

- **Awareness of industry-specific compliance**
  - Healthcare
  - Financial
  - Government
  - Utilities
- **Industry standards**
  - Payment Card Industry Data Security Standard (PCI DSS)
  - International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 series
  - Digital Markets Act (DMA)
- **Security and reporting frameworks**
  - Benchmarks
  - Foundational best practices
  - System and Organization Controls 2 (SOC 2)
  - National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
  - Center for Internet Security (CIS)
  - Cloud Security Alliance (CSA)
- **Audits vs. assessments vs. certifications**
  - External
  - Internal
- **Privacy regulations**
  - General Data Protection Regulation (GDPR)
  - California Consumer Privacy Act (CCPA)
  - General Data Protection Law (LGPD)
  - Children's Online Privacy Act (COPPA)
- **Awareness of cross-jurisdictional compliance requirements**
  - e-discovery
  - Legal holds
  - Due diligence
  - Due care
  - Export controls
  - Contractual obligations

1.4 Given a scenario, perform threat-modeling activities.

- **Actor characteristics**
  - Motivation
    - Financial
    - Geopolitical
    - Activism
    - Notoriety
    - Espionage
  - Resources
    - Time
    - Money
  - Capabilities
    - Supply chain access
    - Vulnerability creation
    - Knowledge
    - Exploit creation
- **Attack patterns**
- **Frameworks**
  - MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)
  - Common Attack Pattern Enumeration and Classification (CAPEC)
  - Cyber Kill Chain
  - Diamond Model of Intrusion Analysis
  - Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE)
  - Open Web Application Security Project (OWASP)
- **Attack surface determination**
  - Architecture reviews
  - Data flows
  - Trust boundaries
  - Code reviews
  - User factors
  - Organizational change
    - Mergers
    - Acquisitions
    - Divestitures
    - Staffing changes
  - Enumeration/discovery
    - Internally and externally facing assets
    - Third-party connections
    - Unsanctioned assets/accounts
    - Cloud services discovery
    - Public digital presence
- **Methods**
  - Abuse cases
  - Antipatterns
  - Attack trees/graphs
- **Modeling applicability of threats to the organization/environment**
  - With an existing system in place
    - Selection of appropriate controls
  - Without an existing system in place

Copyright © 2023 CompTIA, Inc. All rights reserved.

1.5 Summarize the information security challenges associated with artificial intelligence (AI) adoption.

- **Legal and privacy implications**
  - Potential misuse
  - Explainable vs. non-explainable models
  - Organizational policies on the use of AI
  - Ethical governance
- **Threats to the model**
  - Prompt injection
  - Insecure output handling
  - Training data poisoning
  - Model denial of service (DoS)
  - Supply chain vulnerabilities
  - Model theft
  - Model inversion
- **AI-enabled attacks**
  - Insecure plug-in design
  - Deepfake
    - Digital media
    - Interactivity
  - AI pipeline injections
  - Social engineering
  - Automated exploit generation
- **Risks of AI usage**
  - Overreliance
  - Sensitive information disclosure
    - To the model
    - From the model
  - Excessive agency of the AI
- **AI-enabled assistants/digital workers**
  - Access/permissions
  - Guardrails
  - Data loss prevention (DLP)
  - Disclosure of AI usage

Copyright © 2023 CompTIA, Inc. All rights reserved.

2.0 Security Architecture

2.1 Given a scenario, analyze requirements to design resilient systems.

- **Component placement and configuration**
  - Firewall
  - Intrusion prevention system (IPS)
  - Intrusion detection system (IDS)
  - Vulnerability scanner
  - Virtual private network (VPN)
  - Network access control (NAC)
  - Web application firewall (WAF)
  - Proxy
  - Reverse proxy
  - Application programming interface (API) gateway
  - Taps
  - Collectors
  - Content delivery network (CDN)
- **Availability and integrity design considerations**
  - Load balancing
  - Recoverability
  - Interoperability
  - Geographical considerations
  - Vertical vs. horizontal scaling
  - Persistence vs. non-persistence

2.2 Given a scenario, implement security in the early stages of the systems life cycle and throughout subsequent stages.

- **Security requirements definition**
  - Functional requirements
  - Non-functional requirements
  - Security vs. usability trade-off
- **Software assurance**
  - Static application security testing (SAST)
  - Dynamic application security testing (DAST)
  - Interactive application security testing (IAST)
  - Runtime application self-protection (RASP)
  - Vulnerability analysis
  - Software composition analysis (SCA)
  - Software bill of materials (SBoM)
  - Formal methods
- **Continuous integration/ continuous deployment (CI/CD)**
  - Coding standards and linting
  - Branch protection
  - Continuous improvement
  - Testing activities
    - Canary
    - Regression
    - Integration
    - Automated test and retest
    - Unit
- **Supply chain risk management**
  - Software
  - Hardware
- **Hardware assurance**
  - Certification and validation process
- **End-of-life (EOL) considerations**

2.3 Given a scenario, integrate appropriate controls in the design of a secure architecture.

- **Attack surface management and reduction**
  - Vulnerability management
  - Hardening
  - Defense-in-depth
  - Legacy components within an architecture
- **Detection and threat-hunting enablers**
  - Centralized logging
  - Continuous monitoring
  - Alerting
  - Sensor placement
- **Information and data security design**
  - Classification models
  - Data labeling
  - Tagging strategies
- **DLP**
  - At rest
  - In transit
  - Data discovery
- **Hybrid infrastructures**
- **Third-party integrations**
- **Control effectiveness**
  - Assessments
  - Scanning
  - Metrics

Copyright © 2023 CompTIA, Inc. All rights reserved.

2.4 Given a scenario, apply security concepts to the design of access, authentication, and authorization systems.

- Provisioning/deprovisioning
  - Credential issuance
  - Self-provisioning
- Federation
- Single sign-on (SSO)
- Conditional access
- Identity provider
- Service provider
- Attestations
- Policy decision and enforcement points
- Access control models
  - Role-based access control
  - Rule-based access control
  - Attribute-based access control (ABAC)
  - Mandatory access control (MAC)
  - Discretionary access control (DAC)
- Logging and auditing
- Public key infrastructure (PKI) architecture
  - Certificate extensions
  - Certificate types
  - Online Certificate Status Protocol (OCSP) stapling
  - Certificate authority/registration authority (CA/RA)
  - Templates
  - Deployment/integration approach
- Access control systems
  - Physical
  - Logical

2.5 Given a scenario, securely implement cloud capabilities in an enterprise environment.

- Cloud access security broker (CASB)
  - API-based
  - Proxy-based
- Shadow IT detection
- Shared responsibility model
- CI/CD pipeline
- Terraform
- Ansible
- Package monitoring
- Container security
- Container orchestration
- Serverless
  - Workloads
  - Functions
  - Resources
- API security
  - Authorization
  - Logging
  - Rate limiting
- Cloud vs. customer-managed
  - Encryption keys
  - Licenses
- Cloud data security considerations
  - Data exposure
  - Data leakage
  - Data remanence
  - Insecure storage resources
- Cloud control strategies
  - Proactive
  - Detective
  - Preventative
- Customer-to-cloud connectivity
- Cloud service integration
- Cloud service adoption

2.6 Given a scenario, integrate Zero Trust concepts into system architecture design.

- Continuous authorization
- Context-based reauthentication
- Network architecture
  - Segmentation
  - Microsegmentation
  - VPN
  - Always-on VPN
- API integration and validation
- Asset identification, management, and attestation
- Security boundaries
  - Data perimeters
  - Secure zone
  - System components
- Deperimeterization
  - Secure access service edge (SASE)
  - Software-defined wide area network (SD-WAN)
  - Software-defined networking
- Defining subject-object relationships

Copyright © 2023 CompTIA, Inc. All rights reserved.

3.0 Security Engineering

3.1 Given a scenario, troubleshoot common issues with identity and access management (IAM) components in an enterprise environment.

- **Subject access control**
  - User
  - Process
  - Device
  - Service
- **Biometrics**
- **Secrets management**
  - Tokens
  - Certificates
  - Passwords
  - Keys
  - Rotation
  - Deletion
- **Conditional access**
  - User-to-device binding
  - Geographic location
  - Time-based
  - Configuration
- **Attestation**
- **Cloud IAM access and trust policies**
- **Logging and monitoring**
- **Privilege identity management**
- **Authentication and authorization**
  - Security Assertions Markup Language (SAML)
  - OpenID
  - Multifactor authentication (MFA)
  - SSO
  - Kerberos
  - Simultaneous authentication of equals (SAE)
  - Privileged access management (PAM)
  - Open Authorization (OAuth)
  - Extensible Authentication Protocol (EAP)
  - Identity proofing
  - Institute for Electrical and Electronics Engineers (IEEE) 802.1X
  - Federation

3.2 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)**
  - Injections
  - Privilege escalation
  - Credential dumping
  - Unauthorized execution
  - Lateral movement
  - Defensive evasion

Copyright © 2023 CompTIA, Inc. All rights reserved.

3.3 Given a scenario, troubleshoot complex network infrastructure security issues.

- **Network misconfigurations**
  - Configuration drift
  - Routing errors
  - Switching errors
  - Insecure routing
  - VPN/tunnel errors
- **IPS/IDS issues**
  - Rule misconfigurations
  - Lack of rules
  - False positives/false negatives
  - Placement
- **Observability**
- **Domain Name System (DNS) security**
  - Domain Name System Security Extensions (DNSSEC)
  - DNS poisoning
  - Sinkholing
  - Zone transfers
- **Email security**
  - Domain Keys Identified Mail (DKIM)
  - Sender Policy Framework (SPF)
  - Domain-based Message Authentication Reporting & Conformance (DMARC)
  - Secure/Multipurpose Internet Mail Extension (S/MIME)
- **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**

3.4 Given a scenario, implement hardware security technologies and techniques.

- **Roots of trust**
  - Trusted Platform Module (TPM)
  - Hardware Security Module (HSM)
  - Virtual Trusted Platform Module (vTPM)
- **Security coprocessors**
  - Central processing unit (CPU) security extensions
  - Secure enclave
- **Virtual hardware**
- **Host-based encryption**
- **Self-encrypting drive (SED)**
- **Secure Boot**
- **Measured boot**
- **Self-healing hardware**
- **Tamper detection and countermeasures**
- **Threat-actor TTPs**
  - Firmware tampering
  - Shimming
  - Universal Serial Bus (USB)-based attacks
  - Basic input/output system/Unified Extensible Firmware Interface
  - (BIOS/UEFI)
  - Memory
  - Electromagnetic interference (EMI)
  - Electromagnetic pulse (EMP)

3.5 Given a set of requirements, secure specialized and legacy systems against threats.

- **Operational technology (OT)**
  - Supervisory control and data acquisition (SCADA)
  - Industrial control system (ICS)
  - Heating ventilation and air conditioning (HVAC)/environmental
- **Internet of Things (IoT)**
- **System-on-chip (SoC)**
- **Embedded systems**
- **Wireless technologies/ radio frequency (RF)**
- **Security and privacy considerations**
  - Segmentation
  - Monitoring
  - Aggregation
  - Hardening
  - Data analytics
  - Environmental
  - Regulatory
  - Safety
- **Industry-specific challenges**
  - Utilities
  - Transportation
  - Healthcare
  - Manufacturing
  - Financial
  - Government/defense
- **Characteristics of specialized/ legacy systems**
  - Unable to secure
  - Obsolete
  - Unsupported
  - Highly constrained

Copyright © 2023 CompTIA, Inc. All rights reserved.

3.6 Given a scenario, use automation to secure the enterprise.

- Scripting
  - PowerShell
  - Bash
  - Python
- Cron/scheduled tasks
- Event-based triggers
- Infrastructure as code (IaC)
- Configuration files
  - Yet Another Markup Language (YAML)
  - Extensible Markup Language (XML)
  - JavaScript Object Notation (JSON)
  - Tom's Obvious, Minimal Language (TOML)
- Cloud APIs/software development kits (SDKs)
  - Web hooks
- Generative AI
  - Code assist
  - Documentation
- Containerization
- Automated patching
- Auto-containment
- Security orchestration, automation, and response (SOAR)
  - Runbooks
  - Playbooks
- Vulnerability scanning and reporting
- Security Content Automation Protocol (SCAP)
  - Open Vulnerability Assessment Language (OVAL)
  - Extensible Configuration Checklist Description Format (XCCDF)
  - Common Platform Enumeration (CPE)
  - Common vulnerabilities and exposures (CVE)
  - Common Vulnerability Scoring System (CVSS)
- Workflow automation

3.7 Explain the importance of advanced cryptographic concepts.

- Post-quantum cryptography (PQC)
  - Post-quantum vs. Diffie-Hellman and elliptic curve cryptography (ECC)
  - Resistance to quantum computing decryption attack
  - Emerging implementations
- Key stretching
- Key splitting
- Homomorphic encryption
- Forward secrecy
- Hardware acceleration
- Envelope encryption
- Performance vs. security
- Secure multiparty computation
- Authenticated encryption with associated data (AEAD)
- Mutual authentication

3.8 Given a scenario, apply the appropriate cryptographic use case and/or technique.

- Use cases
  - Data at rest
  - Data in transit
    - Encrypted tunnels
  - Data in use/processing
  - Secure email
  - Immutable databases/blockchain
  - Non-repudiation
  - Privacy applications
  - Legal/regulatory considerations
  - Resource considerations
  - Data sanitization
  - Data anonymization
  - Certificate-based authentication
  - Passwordless authentication
  - Software provenance
  - Software/code integrity
  - Centralized vs. decentralized key management
- Techniques
  - Tokenization
  - Code signing
  - Cryptographic erase/obfuscation
  - Digital signatures
  - Obfuscation
  - Serialization
  - Hashing
  - One-time pad
  - Symmetric cryptography
  - Asymmetric cryptography
  - Lightweight cryptography

4.0 Security Operations

4.1 Given a scenario, analyze data to enable monitoring and response activities.

- **Security information event management (SIEM)**
  - Event parsing
  - Event duplication
  - Non-reporting devices
  - Retention
  - Event false positives/false negatives
- **Aggregate data analysis**
  - Correlation
  - Audit log reduction
  - Prioritization
  - Trends
- **Behavior baselines and analytics**
  - Network
  - Systems
  - Users
  - Applications/services
- **Incorporating diverse data sources**
  - Third-party reports and logs
  - Threat intelligence feeds
  - Vulnerability scans
  - CVE details
  - Bounty programs
  - DLP data
  - Endpoint logs
  - Infrastructure device logs
  - Application logs
  - Cloud security posture management (CSPM) data
- **Alerting**
  - False positives/false negatives
  - Alert failures
  - Prioritization factors
    - Criticality
    - Impact
    - Asset type
    - Residual risk
    - Data classification
  - Malware
  - Vulnerabilities
- **Reporting and metrics**
  - Visualization
  - Dashboards

4.2 Given a scenario, analyze vulnerabilities and attacks, and recommend solutions to reduce the attack surface.

- **Vulnerabilities and attacks**
  - Injection
  - Cross-site scripting (XSS)
  - Unsafe memory utilization
  - Race conditions
  - Cross-site request forgery
  - Server-side request forgery
  - Insecure configuration
  - Embedded secrets
  - Outdated/unpatched software and libraries
  - End-of-life software
  - Poisoning
  - Directory service misconfiguration
  - Overflows
  - Deprecated functions
  - Vulnerable third parties
  - Time of check, time of use (TOCTOU)
  - Deserialization
  - Weak ciphers
  - Confused deputy
  - Implants
- **Mitigations**
  - Input validation
  - Output encoding
  - Safe functions
    - Atomic functions
    - Memory-safe functions
    - Thread-safe functions
  - Security design patterns
  - Updating/patching
    - Operating system (OS)
    - Software
    - Hypervisor
    - Firmware
    - System images
  - Least privilege
  - Fail secure/fail safe
  - Secrets management
    - Key rotation
  - Least function/functionality
  - Defense-in-depth
  - Dependency management
  - Code signing
  - Encryption
  - Indexing
  - Allow listing

4.3 Given a scenario, apply threat-hunting and threat intelligence concepts.

- **Internal intelligence sources**
  - Adversary emulation engagements
  - Internal reconnaissance
  - Hypothesis-based searches
  - Honeypots
  - Honeynets
  - User behavior analytics (UBA)
- **External intelligence sources**
  - Open-source intelligence (OSINT)
  - Dark web monitoring
  - Information sharing and analysis centers (ISACs)
  - Reliability factors
- **Counterintelligence and operational security**
- **Threat intelligence platforms (TIPs)**
  - Third-party vendors
- **Indicator of compromise (IoC) sharing**
  - Structured Threat Information eXchange (STIX)
  - Trusted automated exchange of indicator information (TAXII)
- **Rule-based languages**
  - Sigma
  - Yet Another Recursive Acronym (YARA)
  - Rita
  - Snort
- **Indicators of attack**
  - TTPs

4.4 Given a scenario, analyze data and artifacts in support of incident response activities.

- **Malware analysis**
  - Detonation
  - IoC extractions
  - Sandboxing
  - Code stylometry
    - Variant matching
    - Code similarity
    - Malware attribution
- **Reverse engineering**
  - Disassembly and decompilation
  - Binary
  - Byte code
- **Volatile/non-volatile storage analysis**
- **Network analysis**
- **Host analysis**
- **Metadata analysis**
  - Email header
  - Images
  - Audio/video
  - Files/filesystem
- **Hardware analysis**
  - Joint test action group (JTAG)
- **Data recovery and extraction**
- **Threat response**
- **Preparedness exercises**
- **Timeline reconstruction**
- **Root cause analysis**
- **Cloud workload protection platform (CWPP)**
- **Insider threat**

Copyright © 2023 CompTIA, Inc. All rights reserved.

CompTIA SecurityX Acronym List

The following is a list of acronyms that appears on the CompTIA SecurityX CAS-005 exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

ACRONYM	DEFINITION
ABAC	Attribute-based Access Control
ACL	Access Control List
ACME	Automated Certificate Management Environment
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
AQL	Ariel Query Language
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BEAST	Browser Exploit against SSL/TLS
BIOS	Basic Input/Output System
BYOD	Bring Your Own Device
C2	Command and Control
CA	Certificate Authority
CAPEC	Common Attack Pattern Enumeration and Classification
CA/RA	Certificate Authority/Registration Authority
CASB	Cloud Access Security Broker
CBC	Cipher Block Chaining
CCPA	California Consumer Privacy Act
CDN	Content Delivery Network
CI/CD	Continuous Integration/Continuous Deployment
CIS	Center for Internet Security
CMDB	Configuration Management Database
CNAME	Canonical Name
COBIT	Control Objectives for Information and Related Technologies
COPPA	Children's Online Privacy Act
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPE	Common Platform Enumeration
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRM	Customer Relationship Manager
CSA	Cloud Security Alliance
CSPM	Cloud Security Posture Management
CSR	Certificate Signing Request
CSRF	Cross-site Request Forgery
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWPP	Cloud Workload Protection Platform
D3FEND	Detection, Denial, and Disruption Framework Empowering Network Defense
DAC	Discretionary Access Control

Copyright © 2023 CompTIA, Inc. All rights reserved.

ACRONYM	DEFINITION
DAST	Dynamic Application Security Testing
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DKIM	Domain Keys Identified Mail
DLP	Data Loss Prevention
DMA	Digital Markets Act
DMARC	Domain-based Message Authentication Reporting and Conformance
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DORA	Digital Operational Resilience Act
DoS	Denial of Service
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
EDR	Endpoint Detection Response
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EOL	End-of-life
FAST	Flexible Authentication via Secure Tunneling
FDE	Full Disk Encryption
FIDO	Fast Identity Online
GDPR	General Data Protection Regulation
GPO	Group Policy Objects
GRC	Governance, Risk, and Compliance
HIPS/HIDS	Host-based Intrusion Protection System/Host-based Detection System
HKLM	Hkey_Local_Machine
HSM	Hardware Security Module
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating Ventilation and Air Conditioning
IaC	Infrastructure as Code
IAM	Identity and Access Management
IAST	Interactive Application Security Testing
ICS	Industrial Control System
IDS	Intrusion Detection System
IDE	Integrated Development Environment
IEEE	Institute for Electrical and Electronics Engineers
IIS	Internet Information Services
IKE	Internet Key Exchange
IoC	Indicator of Compromise
IoT	Internet of Things
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Centers
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
ISP	Internet Service Provider
ITIL	Information Technology Infrastructure Library
JSON	JavaScript Object Notation
JTAG	Joint Test Action Group
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LGPD	General Data Protection Law
LLM	Large Language Model
MAC	Mandatory Access Control

Copyright © 2023 CompTIA, Inc. All rights reserved.

ACRONYM	DEFINITION
MDM	Mobile Device Management
MFA	Multifactor Authentication
MIME	Multipurpose Internet Mail Extensions
MX	Mail Exchange
NAC	Network Access Control
NFS	Network File System
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
NTLM	New Technology LAN Manager
OAuth	Open Authorization
OIDC	OpenID Connect
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OS	Operating System
OSINT	Open-source Intelligence
OT	Operational Technology
OTP	One-time Password
OVAL	Open Vulnerability Assessment Language
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PAM	Privileged Access Management
PCI DSS	Payment Card Industry Data Security Standard
PEAP	Protected Extensible Authentication Protocol
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PQC	Post-quantum Cryptography
PTR	Pointer Record
QA	Quality Assurance
RACI	Responsible, Accountable, Consulted, and Informed
RADIUS	Remote Authentication Dial-in User Service
RASP	Runtime Application Self-protection
RAT	Remote Access Trojan
RCE	Remote Code Execution
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RF	Radio Frequency
RPO	Recovery Point Objective
RSA	Rivest-Shamir-Aldeman Encryption Algorithm
RTO	Recovery Time Objective
SaaS	Software as a Service
SAE	Simultaneous Authentication of Equals
SAML	Security Assertions Markup Language
SAN	Storage Area Network
SASE	Secure Access Service Edge
SAST	Static Application Security Testing
SBoM	Software Bill of Materials
SCA	Software Composition Analysis
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCCM	System Center Configuration Management
SCEP	Simple Certificate Enrollment Protocol
SCHANNEL	Secure Channel
SDK	Software Development Kit

Copyright © 2023 CompTIA, Inc. All rights reserved.

ACRONYM	DEFINITION
SDLC	Software Development Life Cycle
SDN	Software-defined Network
SDR	Software-defined Radio
SD-WAN	Software-defined Wide Area Network
SED	Self-encrypting Drive
SIEM	Security Information Event Management
SLA	Service-level Agreement
SMB	Server Message Block
S/MIME	Secure/Multipurpose Internet Mail Extensions
SOA	Service-oriented Architecture
SOAR	Security Orchestration, Automation, and Response
SoC	System-on-Chip
SOC	Security Operations Center
SOC 2	System and Organization Controls 2
SPF	Sender Policy Framework
SQL	Structured Query Language
SSD	Solid-state Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-on
STIX	Structured Threat Information eXchange
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege
TAXII	Trusted Automated Exchange of Indicator Information
TCP	Transfer Control Protocol
TIP	Threat Intelligence Platforms
TLS	Transport Layer Security
TOCTOU	Time of Check, Time of Use
TOML	Tom’s Obvious, Minimal Language
TPM	Trusted Platform Module
TTLS	Tunneled Transport Layer Security
TTPs	Tactics, Techniques, and Procedures
UBA	User Behavior Analytics
UDP	User Datagram Protocol
UEBA	User & Entity Behavior Analytics
UEFI	Unified Extensible Firmware Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus
VDI	Virtual Desktop Environment
VPN	Virtual Private Network
vTPM	Virtual Trusted Platform Module
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAF	Web Application Firewall
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Newtork
XCCDF	Extensible Configuration Checklist Description Format
XDR	Extended Detection and Response
XML	Extensible Markup Language
XSS	Cross-site Scripting
YAML	Yet Another Markup Language
YARA	Yet Another Recursive Acronym

Copyright © 2023 CompTIA, Inc. All rights reserved.

CompTIA SecurityX Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the SecurityX CAS-005 certification exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

EQUIPMENT

- Computers with a TPM
- Basic server hardware (email server/ Active Directory server, trusted OS)
- Tokens
- Mobile devices (Android and iOS)
- Switches (managed switch)
- Gateway/router (wired/wireless)
- Firewall
- Proxy server
- Load balancer
- Access points
- Biometric devices
- Arduino/Raspberry Pi
- Software-defined radio (SDR)

OTHER

- Sample logs
- Sample network traffic (packet capture)
- Sample organizational structure
- Sample network documentation
- Internet connection
- Cloud services
- Online productivity suite
- Diagramming software connectors

SOFTWARE

- Virtualized appliances (firewall, IPS, SIEM solution)
- Windows
- Linux distributions
- VMware Workstation Player
- Vulnerability assessment tools
- Secure Shell (SSH) and Telnet utilities
- Threat-modeling tool
- IPS/IDS
- HIPS
- Wireless intrusion prevention system (WIPS)
- Forensic tools
- Certificate authority
- Kali and all Kali toolsets
- GNS and associated firmware
- Log analysis tools
- API SDKs
- Python 3+
- Security Onion tools
- Metasploitable
- Large language model platform
- IDE
- Cryptographic library
- Code versioning, integration, and deployment platform

CompTIA.

© 2023 CompTIA, Inc., used under license by CompTIA, Inc. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA, Inc. CompTIA is a registered trademark of CompTIA, Inc. in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA, Inc. or of their respective owners. Reproduction or dissemination prohibited without the written consent of CompTIA, Inc. Printed in the U.S. 10952-Dec2023