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
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 Database Management
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
DAST	Dynamic Application Security Testing

ACRONYM	DEFINITION
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
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
MDM	Mobile Device Management
MFA	Multifactor Authentication

ACRONYM	DEFINITION
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
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
SDLC	Software Development Life Cycle
SDN	Software-defined Network
SDR	Software-defined Radio

ACRONYM	DEFINITION
SD-WAN	Software-defined Wide Area Network
SED	Self-encrypting Drive
SIEM	Security Information Event Management
SLA	Service-level Agreement
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
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
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
TTPs	Tactics, Techniques, and Procedures
UBA	User Behavior Analytics
UDP	User Datagram Protocol
UEBA	User & Entity Behavior Analytics
UEFI	Unified Extensible Firmware Interface
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