A QUICK-REFERENCE CYBERSECURITY ACRONYMS CHEAT SHEET

Cybersecurity *Acronyms.*

A quick-reference guide to the acronyms you'll see across exams, vendor documents, and cybersecurity content. Built for cybersecurity students, practitioners, and upskillers.

▸ ALSO AVAILABLE IN THREE OTHER FORMATS

- ✓ **A searchable web table** on thecybersecuritytrail.com — same entries, but filterable and always current.
- ✓ **A desk mat & mouse pad** in the CTRLALTSTUFF — for the acronyms you want at a glance, every day.
- ✓ **An interactive web-based game** NEW thecybersecuritytrail.com/cybersecurity-acronym-challenge — test recall, learn the ones you don't, no signup required.

96	A–Z	9
ACRONYMS COVERED	SORTED ALPHABETICALLY	PAGES OF QUICK REFERENCE

Cybersecurity *Acronyms.*

ACRONYM	STANDS FOR	DESCRIPTION
ACL	**Access Control List**	Specifies which users or systems can access specific resources and what actions they can perform.
AD	**Active Directory**	Microsoft directory service for managing users, computers, and resources.
AES	**Advanced Encryption Standard**	A symmetric encryption algorithm widely used for securing data.
ALE	**Annualized Loss Expectancy**	Estimated financial loss from a risk over a one-year period.
APT	**Advanced Persistent Threat**	A prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected.
AV	**Antivirus**	Software designed to detect, prevent, and remove malware.
BEC	**Business Email Compromise**	Social-engineering scam that tricks staff into sending money or data to attackers via spoofed email threads.
BGP	**Border Gateway Protocol**	Protocol used to exchange routing information across the internet; can be exploited.
BIA	**Business Impact Analysis**	Identifies critical operations and the impact of disruptions to them.
C2	**Command and Control**	Communication channel an attacker uses to issue commands to, and receive data from, compromised systems.
CA	**Certificate Authority**	Entity that issues digital certificates used to verify identities online.
CAB	**Change Advisory Board**	A group that evaluates and approves IT change requests.

Cybersecurity *Acronyms.*

ACRONYM	STANDS FOR	DESCRIPTION
CBC	**Cipher Block Chaining**	A mode of operation for block ciphers to enhance encryption strength.
CERT	**Computer Emergency Response Team**	A group that handles cybersecurity incidents and responses.
CI/CD	**Continuous Integration / Continuous Deployment**	Automated software development practice that can introduce security risks if not managed properly.
CIO	**Chief Information Officer**	Senior executive responsible for managing and implementing IT strategy.
CISA	**Cybersecurity and Infrastructure Security Agency**	U.S. government agency responsible for protecting critical infrastructure.
CISO	**Chief Information Security Officer**	Executive responsible for an organization's information and data security.
CSP	**Content Security Policy**	A security standard that helps prevent cross-site scripting and other attacks.
CSPM	**Cloud Security Posture Management**	Tools that help manage cloud security misconfigurations and risks.
CSRF	**Cross-Site Request Forgery**	A web exploit where a user is tricked into performing actions without consent.
CTR	**Click-Through Rate**	Used in phishing analysis to evaluate the effectiveness of email lures.
CVE	**Common Vulnerabilities and Exposures**	Public catalog that assigns IDs to disclosed security flaws so they can be tracked consistently.
CVSS	**Common Vulnerability Scoring System**	Standardized formula (0–10) for gauging the severity of a CVE.

Cybersecurity *Acronyms.*

ACRONYM	STANDS FOR	DESCRIPTION
CWE	**Common Weakness Enumeration**	Community-curated list of software and hardware weakness types (e.g., buffer overflow, XSS).
DAC	**Discretionary Access Control**	Access control method where owners decide permissions for resources.
DDoS	**Distributed Denial of Service**	A type of cyberattack where multiple systems overwhelm a target, disrupting service.
DLP	**Data Loss Prevention**	Tools and strategies to prevent sensitive data from leaving the organization.
DMZ	**Demilitarized Zone**	A physical or logical subnetwork that separates an internal network from untrusted external networks.
DNS	**Domain Name System**	Translates domain names into IP addresses. DNS can be exploited for attacks like DNS spoofing.
DSA	**Digital Signature Algorithm**	NIST-approved algorithm for generating/verifying digital signatures.
EASM	**External Attack Surface Management**	Identifies and manages assets exposed to the internet.
ECC	**Elliptic Curve Cryptography**	Public-key crypto that offers strong security with smaller key sizes than RSA.
EDR	**Endpoint Detection and Response**	Security technology that monitors endpoint devices to detect and respond to cyber threats.
EPP	**Endpoint Protection Platform**	Security solution to protect endpoints such as PCs and servers.
FIDO	**Fast Identity Online**	Open standard for secure, passwordless authentication.

Cybersecurity *Acronyms.*

ACRONYM	STANDS FOR	DESCRIPTION
FIM	**File Integrity Monitoring**	Detects changes to files that could indicate a breach or unauthorized activity.
FIPS	**Federal Information Processing Standards**	U.S. government security standards (e.g., FIPS 140-3 for crypto modules).
FISMA	**Federal Information Security Management Act**	U.S. law to protect government information systems.
FQDN	**Fully Qualified Domain Name**	Complete domain name that specifies exact location within DNS hierarchy.
GA	**General Availability**	Phase when software becomes publicly available — relevant for tracking patch cycles.
GDPR	**General Data Protection Regulation**	EU law that governs personal-data privacy, breach notification, and fines.
GRC	**Governance, Risk, and Compliance**	Framework for managing IT and cybersecurity risks and meeting compliance.
HIDS	**Host-based Intrusion Detection System**	Monitors a specific host or device for suspicious activity.
HMAC	**Hash-based Message Authentication Code**	Combines a cryptographic hash with a secret key to verify data integrity and authenticity.
HSM	**Hardware Security Module**	Physical device that safeguards and manages digital keys.
HSTS	**HTTP Strict Transport Security**	Response header that forces browsers to use HTTPS for a site, mitigating downgrade attacks.
IAM	**Identity and Access Management**	Framework of policies and technologies to ensure proper access to systems.

Cybersecurity *Acronyms.*

ACRONYM	STANDS FOR	DESCRIPTION
IDS	**Intrusion Detection System**	Monitors network traffic for suspicious activity and alerts administrators.
IoC	**Indicator of Compromise**	Evidence on a network or system that indicates a security breach.
IoT	**Internet of Things**	Network of connected devices that can be vulnerable to cyberattacks.
IPS	**Intrusion Prevention System**	Like IDS, but also takes action to block detected threats in real time.
JWT	**JSON Web Token**	Compact, signed JSON object used to convey identity or claims between parties (common in APIs).
KBA	**Knowledge-Based Authentication**	Authentication based on the user's knowledge of personal information.
KMS	**Key Management Service**	Centralized system for creating, rotating, and destroying cryptographic keys (cloud or on-prem).
LAPS	**Local Administrator Password Solution**	Microsoft tool for managing local admin passwords securely.
MAC	**Mandatory Access Control**	Access control where policies are centrally enforced, not at the discretion of users.
MDR	**Managed Detection and Response**	Outsourced service providing threat hunting, monitoring, and response.
MFA	**Multi-Factor Authentication**	A security system that requires more than one method of authentication from independent categories.
MITM	**Man-In-The-Middle**	An attack where the attacker secretly intercepts communication between two parties.

Cybersecurity *Acronyms.*

ACRONYM	STANDS FOR	DESCRIPTION
MTTD	**Mean Time to Detect**	Average time it takes to identify a threat or incident.
MTTR	**Mean Time to Respond / Recover**	Average time to contain and remediate a threat.
NAC	**Network Access Control**	Restricts unauthorized devices from accessing the network.
NIDS	**Network Intrusion Detection System**	Monitors network traffic for malicious patterns and raises alerts.
NIST	**National Institute of Standards and Technology**	U.S. agency that provides cybersecurity frameworks and best practices.
OAUTH	**Open Authorization**	A protocol for secure delegated access (e.g., logging in via Google).
OCSP	**Online Certificate Status Protocol**	Real-time method for checking whether an X.509 certificate has been revoked.
OSINT	**Open Source Intelligence**	Information collected from publicly available sources for threat analysis.
OTP	**One-Time Password**	Password valid for a single login or transaction (often delivered via SMS or app).
PAM	**Privileged Access Management**	Controls and monitors access of privileged users to critical systems.
PFS	**Perfect Forward Secrecy**	Ensures session keys are not compromised even if private key is.
PII	**Personally Identifiable Information**	Data that can uniquely identify an individual (name, SSN, biometric data, etc.).

Cybersecurity *Acronyms.*

ACRONYM	STANDS FOR	DESCRIPTION
PKI	**Public Key Infrastructure**	System for managing encryption keys and digital certificates.
RAT	**Remote Access Trojan**	Malware that allows an attacker to control a system remotely.
RBAC	**Role-Based Access Control**	Grants permissions based on users' job roles to enforce least privilege.
RPO	**Recovery Point Objective**	Maximum acceptable amount of data loss in a disaster scenario.
RTO	**Recovery Time Objective**	Maximum acceptable time to restore operations after an incident.
SAML	**Security Assertion Markup Language**	XML-based standard that transmits authentication and authorization data between identity providers and services.
SAST	**Static Application Security Testing**	Examines source code for vulnerabilities without executing it.
SBOM	**Software Bill of Materials**	A list of components in a software product to manage supply chain risks.
SCADA	**Supervisory Control and Data Acquisition**	Systems for controlling industrial processes, often targeted in cyberattacks.
SHA	**Secure Hash Algorithm**	Family of cryptographic hash functions (SHA-256, SHA-3) used in digital signatures and data integrity checks.
SIEM	**Security Information and Event Management**	Collects and analyzes log data for real-time threat detection and compliance.
SOAR	**Security Orchestration, Automation, and Response**	Tools that help automate and coordinate incident response workflows.

Cybersecurity *Acronyms.*

ACRONYM	STANDS FOR	DESCRIPTION
SOC	**Security Operations Center**	Centralized team and facility that monitors and responds to cybersecurity incidents.
SSL/TLS	**Secure Sockets Layer / Transport Layer Security**	Protocols for encrypting data transmitted over the internet.
SSO	**Single Sign-On**	Authentication process allowing a user to access multiple systems with one login.
STIX	**Structured Threat Information eXpression**	Format for sharing cyber threat intelligence.
TLP	**Traffic Light Protocol**	System for classifying and sharing sensitive cyber threat information.
TOTP	**Time-based One-Time Password**	OTP that changes every fixed interval (usually 30s), generated from a shared secret and the current time.
TTP	**Tactics, Techniques, and Procedures**	Patterns of behavior used by threat actors.
UDT	**User Datagram Protocol**	A connectionless protocol vulnerable to spoofing and DoS attacks.
UEBA	**User and Entity Behavior Analytics**	Uses AI to detect anomalies in user or system behavior.
VLAN	**Virtual Local Area Network**	Network segmentation tool used to isolate traffic and enhance security.
VPN	**Virtual Private Network**	Creates a secure, encrypted connection over a less secure network, such as the internet.
WAF	**Web Application Firewall**	Protects web applications by filtering and monitoring HTTP traffic.

Cybersecurity *Acronyms.*

ACRONYM	STANDS FOR	DESCRIPTION
WPA3	**Wi-Fi Protected Access 3**	Latest Wi-Fi security standard, replacing WPA2, with stronger encryption and individualized data protection.
XDR	**Extended Detection and Response**	Security solution that integrates data across multiple security layers for better detection and response.
XSS	**Cross-Site Scripting**	Injection attack where malicious scripts run in a victim's browser within a trusted site's context.
YARA	**Yet Another Recursive Acronym**	Rule-based toolkit for identifying and classifying malware samples.
ZKP	**Zero-Knowledge Proof**	Cryptographic method that proves possession of secret information without revealing the secret itself.
ZTA	**Zero Trust Architecture**	Security model that assumes no implicit trust — everything must be verified.

▸ FROM CHEAT SHEET TO MUSCLE MEMORY

Don't just *read* them. Drill them.

Reading an acronym is one thing. Recalling it in a Security+ question or a 2 AM SOC ticket is another. The Cybersecurity Trail turns this list into an interactive challenge — timed rounds, randomized order, instant feedback, no signup.

▸ THE ACRONYM CHALLENGE

Test what you actually know.

Pick a domain, race the clock, and learn the ones you missed. Free, browser-based, mobile-friendly.

thecybersecuritytrail.com/cybersecurity-acronym-challenge

▸ THE FULL TRAIL

2,000+ practice questions.

Domain-aligned practice tests for Security+, CEH v13, and Network+, plus branching SOC simulations and long-form guides.

thecybersecuritytrail.com

Spotted a missing acronym, a fresh CVE-class term, or a description that could be sharper? We update this sheet quarterly — write to **contact@thecybersecuritytrail.com**.