TEKTUT

TEKTUT CYBER ACADEMY

60 Cyber Security Terms Explained

Core security, cloud, architecture and compliance — every term you need before your first day in the industry.

APT
Advanced Persistent Threat — a prolonged, targeted cyber attack, often state-sponsored, designed to stay undetected.

Attack Surface
The total number of entry points an attacker could exploit — every system, app, or user is part of it.

Authentication
Verifying who you are — e.g. a password, fingerprint, or security key.

Authorisation
Deciding what you're allowed to do once your identity is confirmed.

Blue Team
The defenders — security professionals who monitor, detect, and respond to attacks.

Brute Force
Trying every possible password combination until the correct one is found.

CIA Triad
Confidentiality, Integrity, Availability — the three core principles of information security.

CISO
Chief Information Security Officer — the senior executive responsible for an organisation's cyber strategy.

Compliance
Meeting the rules, laws, or standards that govern how data and systems must be protected (e.g. GDPR, ISO 27001).

CREST
A professional body that certifies ethical hackers and penetration testers to a recognised standard.

Lateral Movement
When an attacker moves through a network after initial access, escalating privileges and reaching sensitive systems.

Malware
Malicious software — includes viruses, ransomware, spyware, and trojans designed to damage or gain access.

MFA
Multi-Factor Authentication — requiring two or more verification methods to access an account.

MITRE ATT&CK;
A publicly available knowledge base of attacker tactics and techniques used to improve threat detection.

Network+
CompTIA Network+ — a foundational certification covering networking concepts required for most cyber roles.

OSINT
Open Source Intelligence — gathering information about a target from publicly available sources.

Patch Management
The process of regularly updating software to fix known vulnerabilities.

Penetration Test
A simulated, authorised attack on a system to identify security weaknesses before real attackers do.

Phishing
A social engineering attack using fake emails or messages to trick users into revealing credentials or installing malware.

Privilege Escalation
Gaining higher-level permissions than originally granted — a key step in many attacks.

CVE
Common Vulnerabilities and Exposures — a public database of known security flaws in software.

CySA+
CompTIA Cybersecurity Analyst — an industry-recognised certification for security analyst roles.

Dark Web
An encrypted part of the internet not indexed by standard search engines, often used for illegal activity.

Data Breach
An incident where sensitive data is accessed, stolen, or exposed without authorisation.

DDoS
Distributed Denial of Service — flooding a system with traffic to make it unavailable to users.

Defence in Depth
Layering multiple security controls so that if one fails, others still protect the system.

DMZ
Demilitarised Zone — a network segment that sits between an internal network and the internet, hosting public-facing services.

Encryption
Converting data into a coded format so only authorised parties with the correct key can read it.

Endpoint
Any device that connects to a network — laptops, phones, servers, printers.

Ethical Hacker
A security professional hired to attempt to breach systems — legally — to find weaknesses before attackers do.

Exploit
A piece of code or technique that takes advantage of a vulnerability to cause harm or gain access.

Firewall
A security system that monitors and controls incoming and outgoing network traffic based on defined rules.

Forensics
Digital forensics — the investigation of cyber incidents by collecting, preserving and analysing digital evidence.

Ransomware
Malware that encrypts a victim's files and demands payment to restore access.

Red Team
Offensive security professionals who simulate real-world attacks to test an organisation's defences.

Risk Assessment
The process of identifying, analysing, and evaluating security risks to determine appropriate controls.

Security+
CompTIA Security+ — the most widely held entry-level cyber security certification.

SIEM
Security Information and Event Management — a tool that collects and analyses security logs in real time.

Social Engineering
Manipulating people into revealing confidential information — exploiting human nature rather than technology.

SOC
Security Operations Centre — a team or facility that monitors and responds to security incidents around the clock.

Threat Intelligence
Information about current or potential cyber threats used to inform defensive decisions.

Zero-Day
A previously unknown vulnerability that has no patch available — highly prized by attackers.

AWS IAM
Amazon Web Services Identity and Access Management — controls who can access AWS resources and what they can do.

AWS Architect
An Amazon Web Services certified specialist who designs and manages cloud infrastructure — one of the most in-demand and highest-paid roles in tech, with contractor rates from £300+ per day.

Cloud Architect
A specialist who designs secure, scalable cloud infrastructure across any platform — responsible for the overall structure, security, and performance of cloud environments.

Cloud Security
The practice of protecting data, applications, and infrastructure hosted in cloud environments from threats and misuse.

GRC
Governance, Risk and Compliance — the framework organisations use to manage security policies, risk, and regulatory requirements.

Hashing
A one-way function that converts data into a fixed-length string — used to store passwords securely.

IAM
Identity and Access Management — controlling who has access to what systems and data.

Incident Response
The process of detecting, containing, and recovering from a security breach or attack.

IDS / IPS
Intrusion Detection System / Intrusion Prevention System — tools that identify and block suspicious network activity.

ISO 27001
An international standard for managing information security — a widely recognised compliance benchmark.

Keylogger
Malware that records every keystroke on a device, often used to steal passwords.

Container Security
Securing containerised applications (e.g. Docker, Kubernetes) — increasingly critical as modern software moves to microservices.

Hybrid Cloud
An environment that combines on-premises infrastructure with public or private cloud services, connected and managed together.

IaaS / PaaS / SaaS
Three cloud service models: Infrastructure as a Service (raw compute), Platform as a Service (dev environment), Software as a Service (end-user apps).

On-Premises
Infrastructure that is physically hosted and managed within an organisation's own facilities, rather than in the cloud.

S3 Bucket
Amazon's cloud object storage service — commonly misconfigured, making it a frequent target for data exposure incidents.

Shared Responsibility Model
The division of security duties between a cloud provider (infrastructure) and the customer (data, access, configuration).

VPC
Virtual Private Cloud — an isolated network within a public cloud where resources can be deployed with controlled access.