ETHICAL TECH COLAB · REFERENCE EDITION

THE CYBER DICTIONARY AND DATABASE LIBRARY

1,020 TERMS IN PLAIN ENGLISH, AND 105 PLACES TO GET THE DATA

Ethical Tech CoLab
September 2026

Compiled from the live dictionary at ethical-tech-colab.github.io/cyber-dictionary

> A dictionary is a machine for the moment you looked something up. This edition keeps that moment intact on paper: the terms run A to Z with the range printed at the head of every page, and the database library is a catalogue you walk shelf by shelf rather than a search box you have to already know the answer for.

Front matter

HOW TO USE THIS BOOK

The book has two rooms. **The Dictionary** defines 1,020 technology and cybersecurity terms across 15 domains, each in a sentence or two of the plain English you wanted at the moment you actually looked the term up. **The Database Library** catalogues 105 open data sources and open-source technologies across 11 shelves, each with what it gives you, how to reach it, and what it costs.

Entries in the Dictionary are filed by headword, ignoring case, spaces and hyphens, so *air-gap* and *airgap* sit together. Where a term is normally met as an abbreviation, the expansion follows the headword in italics; where it is normally met expanded, the abbreviation does. The small capitals at the end of a definition name the domain the term belongs to, which is the answer to the second question a reader usually has: not only what it means, but which part of the field is talking.

The Database Library is arranged by shelf rather than alphabetically, because nobody arrives at a library knowing the name of the thing they need. Each catalogue card gives the operator, the address, what the source actually holds, how to connect a program to it, and the cost line — which is the field most likely to have changed since printing, and the one worth checking against the live entry before you build on it.

A note on currency. Definitions age slowly; endpoints, licences and free tiers age fast. The live edition is the authority on the Database Library. Treat a cost line here as a description of what the source offered when this edition was compiled, not as a promise about today.

The collection in numbers

WHAT IS IN HERE

1,020

terms defined, across 15 domains

105

sources catalogued, across 11 shelves

29

alphabetical sections, # to Z

103

sources free to use at the tier described

TERMS BY DOMAIN

Networking & Protocols	192
Endpoints & Systems	77
Identity & Access	75
Governance, Risk & Compliance	74
Attacks & Exploitation	71
Defense & Operations	71
Cryptography	70
Intelligence & Investigations	70
Dev & Delivery	65
Malware & Threat Actors	56
Compute & Hardware	54
Application Security	41
Cloud & Infrastructure	38
AI & Emerging Tech	38
Classification & Personal Data	28

SOURCES BY SHELF

Satellite & Earth Observation	12
Maps & Geospatial	15
Climate & Weather	10
Population & Development	9
Conflict, Rights & Humanitarian	9
Environment & Biodiversity	8
Health	5
Economy, Trade & Corporate	7
Security & Threat Data	10
Geospatial Tooling	10
Communities & Programmes	10

Part one

THE DICTIONARY

1,020 terms, A to Z. The head of each page carries the range of terms on it.

# #

2 ENTRIES

1999 Brooklyn credit card case
An early US case where stolen card details were used at scale — investigated as identity theft rather than as hacking. An illustration of how cyber cases get charged under whatever law already exists. INTELLIGENCE & INVESTIGATIONS

3-2-1 rule
Three copies of data, on two media types, with one off-site. Modern versions add one offline or immutable copy. CLOUD & INFRASTRUCTURE

A

53 ENTRIES

ABAC *Attribute-Based Access Control*
Access decided by attributes — department, device posture, location, time — evaluated as policy. More expressive than roles, and harder to reason about. IDENTITY & ACCESS

Access control
Deciding who may reach which resource, and enforcing it. Everything else in identity — accounts, roles, permissions — exists to make this decision reliably. NETWORKING & PROTOCOLS

Access control list *ACL*
A list attached to a resource naming who may use it and how. Simple, explicit, and still the model behind file permissions and router rules. NETWORKING & PROTOCOLS

Access control service
A service whose job is to keep unauthorised users away from system resources, usually through lists of permitted identities or issued tickets. IDENTITY & ACCESS

Access management
The everyday work of keeping access information correct: creating accounts, maintaining them, watching them, and revoking them when they should end. IDENTITY & ACCESS

Access matrix
A grid of subjects against objects, with the permitted actions in each cell. Mostly a teaching model, but it is the mental picture behind every permissions system. NETWORKING & PROTOCOLS

Access review *Recertification / attestation*
A periodic check where owners confirm who still needs access. The main defence against privilege creep — and often rubber-stamped. IDENTITY & ACCESS

Account harvesting
Collecting the valid account names on a system. Half of a password attack is knowing who exists. ATTACKS & EXPLOITATION

Account takeover *ATO*
An attacker gaining full control of a legitimate account, then using its normal permissions. Hard to spot precisely because nothing technically breaks. IDENTITY & ACCESS

ACK piggybacking
Sending an acknowledgement inside another packet already headed the same way, rather than on its own. ATTACKS & EXPLOITATION

Active content
Code embedded in a web page that runs on the visitor's machine when the page loads. The reason a page you merely opened can attack you. ENDPOINTS & SYSTEMS

Activity monitor
A defence that watches for malicious behaviour on a system and blocks it as it happens, rather than matching known files. DEFENSE & OPERATIONS

Adversarial example
Input perturbed slightly so a model misclassifies it while a person sees nothing unusual. The classic attack on vision systems. AI & EMERGING TECH

Adversary-in-the-middle *AiTM / MitM*
Sitting between the user and the real site, relaying traffic and capturing the session cookie after login. It defeats codes and push, but not hardware-bound factors. ATTACKS & EXPLOITATION

Adware
Software that injects ads or hijacks searches. Mostly a nuisance, sometimes a delivery route for worse. MALWARE & THREAT ACTORS

AES *Advanced Encryption Standard*
The default symmetric cipher, normally with 128- or 256-bit keys. Unbroken in practice — failures around it are nearly always key management or mode-of-operation mistakes. CRYPTOGRAPHY

Agentic AI *AI agent*
A model given tools and the autonomy to take multi-step actions. It converts a text-generation risk into a systems-and-permissions risk. AI & EMERGING TECH

AI red teaming
Deliberately probing a model or AI system for harmful, biased, or unsafe behaviour before users find it. AI & EMERGING TECH

Air gap
Physically isolating a system from other networks. Strong in principle, routinely defeated in practice by USB drives, maintenance laptops, and forgotten management links. NETWORKING & PROTOCOLS

Alert fatigue
Analysts becoming numb to alerts through sheer volume. The mechanism by which a genuine alert is closed unread. DEFENSE & OPERATIONS

Algorithm
A finite set of steps for solving a problem or performing a computation. ENDPOINTS & SYSTEMS

Algorithmic bias
Systematic unfairness in outputs, usually inherited from data or objectives. A safety and legal problem, not only an accuracy one. AI & EMERGING TECH

Amplification attack *Reflection*
Sending small spoofed requests to services that reply with much larger responses, aimed at the victim. DNS and NTP are classic amplifiers. ATTACKS & EXPLOITATION

Anonymisation vs pseudonymisation
Anonymised data cannot be linked back and leaves scope; pseudonymised data can be re-linked with a key and is still personal data. GOVERNANCE, RISK & COMPLIANCE

Antivirus *AV*
Signature and heuristic detection of malicious files. Necessary, insufficient, and blind to fileless and living-off-the-land activity. ENDPOINTS & SYSTEMS

API *Application Programming Interface*
The defined way one piece of software talks to another. Everything in the library section of this site is reached through one. DEV & DELIVERY

API endpoint *Route*
A specific URL an API exposes for one operation. Each one needs its own authorisation check — this is where broken access control usually lives. DEV & DELIVERY

API gateway
A single front door for APIs handling authentication, rate limits, routing, and logging, so services do not each reimplement them. CLOUD & INFRASTRUCTURE

Applet
A small program delivered to run inside a browser, historically in Java. The model is gone; the lesson about running untrusted code is not. ENDPOINTS & SYSTEMS

Application allow-listing *Whitelisting*
Only approved executables may run. Extremely strong, operationally demanding, and impractical for developer machines. ENDPOINTS & SYSTEMS

APT *Advanced Persistent Threat*
A well-resourced group, usually state-linked, that gets in and stays quietly for a long time. Persistence and patience matter more than sophistication. MALWARE & THREAT ACTORS

ARP *Address Resolution Protocol*
Maps IP addresses to hardware MAC addresses on a local network. It has no authentication at all, which is why ARP spoofing is trivial on a flat network. NETWORKING & PROTOCOLS

ARPANET *Advanced Research Projects Agency Network*
The 1970s packet-switched research network, funded by the US government, that the internet grew out of. Decommissioned in 1990. NETWORKING & PROTOCOLS

Artifact
The output of a build: a binary, a container image, a zipped bundle. What actually gets deployed, as opposed to the source. DEV & DELIVERY

ASIC / FPGA *Application-Specific Integrated Circuit / Field-Programmable Gate Array*
An ASIC is a chip hard-wired for one job — fast, cheap at volume, unchangeable. An FPGA is reconfigurable hardware: slower, but you can rewrite what it is. COMPUTE & HARDWARE

Asymmetric encryption *Public-key cryptography*
A key pair: the public key encrypts or verifies, the private key decrypts or signs. Slower, but it lets strangers exchange secrets without meeting first. CRYPTOGRAPHY

Asymmetric warfare
Conflict where a small investment, well aimed, produces effects out of all proportion to its cost. The standing description of offensive cyber. ATTACKS & EXPLOITATION

Attack chain *Kill chain*
The ordered stages of an intrusion, from reconnaissance through to impact. Useful because breaking any single link stops the whole chain. ATTACKS & EXPLOITATION

Attack surface
Everything an attacker could touch — exposed services, endpoints, APIs, staff, suppliers. Reducing it is usually cheaper than defending it. ATTACKS & EXPLOITATION

Attack surface management *ASM / EASM*
Continuously discovering what of yours is exposed to the internet, including assets nobody remembered owning. DEFENSE & OPERATIONS

Attorney-client privileged material
Legal advice and communications with counsel, protected from disclosure. Incident investigations are often run under privilege, which changes who may see the findings and how they are written. CLASSIFICATION & PERSONAL DATA

Attribution
Assigning an attack to a specific actor. Genuinely hard, often political, and rarely changes what a defender should do next. MALWARE & THREAT ACTORS

Attribution threshold
Establishing who was behind an intrusion, to a standard someone will act on. Technical indicators rarely get there alone; attribution usually needs intelligence, finance and human sources too. INTELLIGENCE & INVESTIGATIONS

Auditing
Gathering and examining evidence about systems to check they comply with policy and are not exposed. The routine, unglamorous half of assurance. DEFENSE & OPERATIONS

Audit trail
A tamper-evident record of who did what and when. Required by most frameworks and indispensable during an investigation. GOVERNANCE, RISK & COMPLIANCE

Australian Federal Police *AFP*
Australia's national police force, handling cybercrime with national or international reach. INTELLIGENCE & INVESTIGATIONS

Authentication *AuthN*
Proving who you are. Distinct from authorisation, and confusing the two is the root of a surprising number of vulnerabilities. IDENTITY & ACCESS

Authenticity
That information is genuine and unaltered — that it really is what it claims to be. IDENTITY & ACCESS

Authorisation *AuthZ*
Deciding what an already-identified user is allowed to do. A logged-in user reaching another user's record is an authorisation failure, not an authentication one. IDENTITY & ACCESS

Authoritative name server
The server that holds the real, official records for a domain. Everything else is a cached copy of what it said. NETWORKING & PROTOCOLS

Autonomous system *AS*
A network, or set of networks, under one organisation's routing control, identified by an AS number. BGP is the language autonomous systems use to talk to each other. NETWORKING & PROTOCOLS

Autonomous system number *ASN*
The globally unique number identifying a network in the routing system. Useful in attribution: it says which network an address belongs to. NETWORKING & PROTOCOLS

Availability
That the system can actually do its job for the people who need it. The leg of the triad security controls most often damage. GOVERNANCE, RISK & COMPLIANCE

B

45 ENTRIES

Backdoor
A hidden way back into a system that bypasses normal authentication. Left by attackers, and occasionally by developers who meant it as a debug feature. MALWARE & THREAT ACTORS

Backup
A separate copy of data that can be restored. Untested backups are a plan, not a control — and ransomware crews delete the ones they can reach. CLOUD & INFRASTRUCTURE

Bandwidth
How much data a link can carry in a given time, usually in bits per second. Not the same as latency — a fat pipe can still be slow to respond. NETWORKING & PROTOCOLS

Banner
The text a service announces when you connect to it, often naming the software and version. Free reconnaissance for an attacker, which is why banners get trimmed. NETWORKING & PROTOCOLS

Bare metal vs virtualised
A whole physical machine versus a share of one. Bare metal gives predictable performance and no noisy neighbours, at the cost of flexibility. COMPUTE & HARDWARE

Baseline / anomaly detection
Learning what normal looks like and alerting on deviation. Catches novel attacks and generates plenty of noise doing it. DEFENSE & OPERATIONS

Baseline / benchmark *CIS Benchmarks*
A published, agreed secure configuration for a platform. Gives you something concrete to measure drift against. ENDPOINTS & SYSTEMS

Basic authentication
The simplest web authentication: the username and password are sent with every request, barely encoded. Safe only inside TLS, and not really then. CRYPTOGRAPHY

Bastion host *Jump box*
A single hardened, monitored entry point for administrative access to a private network, so nothing else needs exposing. CLOUD & INFRASTRUCTURE

Batch size
How many inputs are processed together. Larger batches use hardware more efficiently and need more memory. COMPUTE & HARDWARE

Beaconing
An implant checking in with its controller at regular intervals. The rhythm of those check-ins is one of the most reliable detections available. ATTACKS & EXPLOITATION

Bearer token
A credential where possession alone grants access, with no further proof required. Which is exactly why leaked tokens in logs or repos are so damaging. IDENTITY & ACCESS

BEC *Business Email Compromise*
Impersonating or hijacking a trusted business mailbox to redirect a payment or an invoice. Consistently causes larger financial losses than ransomware. ATTACKS & EXPLOITATION

BGP *Border Gateway Protocol*
How the internet's large networks tell each other which address ranges they can reach. Built on trust, so a bad or malicious announcement can hijack traffic globally. NETWORKING & PROTOCOLS

BGP hijacking *Route hijacking*
Announcing routes for address space you do not own, pulling other people's traffic through your network. The internet's routing still runs largely on trust. NETWORKING & PROTOCOLS

BIND *Berkeley Internet Name Domain*
The long-running reference implementation of DNS. Much of the internet's name resolution has run on it, so its vulnerabilities matter widely. NETWORKING & PROTOCOLS

Biometrics
Authenticating people by physical characteristics — fingerprint, face, iris. Convenient, and impossible to reissue once copied. IDENTITY & ACCESS

Bit
The smallest unit of storage: a single 0 or 1. ENDPOINTS & SYSTEMS

Blockchain *Distributed ledger*
An append-only ledger replicated across many parties. Strong integrity guarantees; no confidentiality, and no help if the data entered was wrong. AI & EMERGING TECH

Blockchain analysis *Chain analysis*
Following cryptocurrency through the public ledger, clustering addresses and linking them to real identities at the points where coins meet a regulated exchange. The reason a public ledger is worse for criminals than cash. INTELLIGENCE & INVESTIGATIONS

Block cipher
A cipher that encrypts fixed-size blocks of data at a time. AES is the one in use nearly everywhere. CRYPTOGRAPHY

Blue-green / canary deploy
Two ways to release safely: run two full environments and switch traffic, or send the new version to a small slice of users first and watch. DEV & DELIVERY

Bootkit
A rootkit that loads before the operating system, surviving reinstalls. Secure Boot and measured boot exist mainly to stop this. MALWARE & THREAT ACTORS

Boot record infector
Malware that writes itself into the boot sector so it runs before the operating system does. The predecessor of the modern bootkit. MALWARE & THREAT ACTORS

Botnet
A fleet of compromised machines under one controller, rented out for denial of service, spam, proxying, or credential stuffing. ATTACKS & EXPLOITATION

Branch
A named line of work running alongside the main one. It lets you build or break something without affecting what everyone else is using. DEV & DELIVERY

Breach and attack simulation *BAS*
Automated, continuous safe replay of attack techniques to validate that controls and detections still work after changes. DEFENSE & OPERATIONS

Breach notification
The legal duty to report certain breaches within a deadline — 72 hours to a regulator under GDPR, and to affected people if the risk is high. GOVERNANCE, RISK & COMPLIANCE

Breaking change
A change that stops existing users' code or configuration working. It needs a major version bump and a note, not a quiet release. DEV & DELIVERY

Bridge
A device that joins two network segments using the same protocol, passing frames between them. A switch is essentially a bridge with many ports. NETWORKING & PROTOCOLS

British Standard 7799 *BS 7799*
The British code of practice for information security management that became ISO/IEC 17799 and then ISO/IEC 27002. GOVERNANCE, RISK & COMPLIANCE

Broadcast
Sending one message to every host on a network at once. Useful for discovery, and abusable — the Smurf attack is broadcast turned into a weapon. NETWORKING & PROTOCOLS

Broadcast address
The address that reaches every host on a network segment. Traffic sent to it multiplies, which is why routers do not forward it across networks. NETWORKING & PROTOCOLS

Broken access control
Authorisation not enforced consistently on the server. Persistently the number one web risk, because it cannot be found by scanners alone. APPLICATION SECURITY

Browser
The client program that fetches and renders web content. Now the operating system most work actually happens in, and the most attacked software on any endpoint. ENDPOINTS & SYSTEMS

Brute force
Trying every possibility until something works. Defeated by rate limiting, lockouts, and enough entropy to make the search space impractical. ATTACKS & EXPLOITATION

Budapest Convention *Convention on Cybercrime*
The Council of Europe treaty that harmonises cybercrime offences and cooperation procedures across its parties. The closest thing to a common international framework. INTELLIGENCE & INVESTIGATIONS

Buffer overflow
Writing past the end of a memory buffer, corrupting adjacent data and often enabling code execution. Mostly a C and C++ problem. APPLICATION SECURITY

Bug bounty
Paying external researchers for valid vulnerability reports. Continuous and broad, but no substitute for internal testing. APPLICATION SECURITY

Build
Turning source code into something runnable — compiled, bundled, containerised. A build that only works on one machine is a bug. DEV & DELIVERY

Business continuity *BCP*
How the organisation keeps operating during disruption, including manual fallbacks. Broader than technical disaster recovery. DEFENSE & OPERATIONS

Business impact analysis *BIA*
Working out how much disruption to each system the organisation can actually tolerate. It is what turns recovery targets from guesses into decisions. DEFENSE & OPERATIONS

BYOD *Bring Your Own Device*
Staff using personal devices for work. Convenient, and it puts corporate data on hardware you do not control or get to inspect. ENDPOINTS & SYSTEMS

BYOVD *Bring Your Own Vulnerable Driver*
Installing a legitimately signed but flawed driver in order to abuse it for kernel access. A standard technique for disabling security tooling. COMPUTE & HARDWARE

Byte
The smallest individually addressable unit of storage, in practice eight bits. ENDPOINTS & SYSTEMS

C

96 ENTRIES

Cache *L1 / L2 / L3*
Tiny, very fast memory close to the processor holding recently used data. Its timing behaviour leaks information, which is what Spectre-class attacks exploit. COMPUTE & HARDWARE

Cache cramming
Tricking a browser into running cached code from local disk, where it is granted more permission than code from the internet would get. ATTACKS & EXPLOITATION

Cache poisoning *DNS poisoning*
Getting a name server to store and serve a false answer, so everyone it serves is quietly sent to the wrong place. NETWORKING & PROTOCOLS

Cash-out *Off-ramp*
The point where criminal proceeds are converted into usable money. Cryptocurrency is traceable on the chain, so the exchange where it is cashed out is where investigations most often land. INTELLIGENCE & INVESTIGATIONS

CD *Continuous Delivery / Deployment*
Delivery keeps every change releasable at a button press; deployment ships it automatically once checks pass. The two are often written as one and mean different things. DEV & DELIVERY

CDN *Content Delivery Network*
Distributed edge servers caching content close to users. Also a practical place to absorb denial-of-service traffic and enforce WAF rules. CLOUD & INFRASTRUCTURE

Cell
A fixed-length unit of data in ATM networks. Fixed size made switching fast in hardware, a design later overtaken by packet-based Ethernet. NETWORKING & PROTOCOLS

Certificate *X.509 certificate*
A signed statement binding a public key to an identity such as a domain name. Trust rests entirely on trusting whoever signed it. CRYPTOGRAPHY

Certificate authority *CA*
An organisation that issues and vouches for certificates. Its root certificate ships in browsers and operating systems, so a compromised CA breaks trust everywhere. CRYPTOGRAPHY

Certificate-based authentication
Proving identity with a certificate and its private key instead of a password. Phishing-resistant, and only as good as the issuing process. CRYPTOGRAPHY

Certificate pinning
Hard-coding which certificate or key an app will accept, so a rogue CA cannot impersonate the server. Powerful, and easy to brick your own app with. CRYPTOGRAPHY

CGI *Common Gateway Interface*
The old mechanism for a web server to pass a request to an executable script and return its output. The first generation of dynamic web vulnerabilities lived here. ENDPOINTS & SYSTEMS

Chain of custody
Documented handling of evidence from collection onwards. Break it and the evidence may be worthless in a legal proceeding. DEFENSE & OPERATIONS

CHAP *Challenge-Handshake Authentication Protocol*
Authentication by responding to a fresh challenge each time, so a captured response cannot be replayed. IDENTITY & ACCESS

Chatham House Rule
A meeting convention: you may use what was said, but never say who said it. Standard for intelligence and industry threat-sharing sessions. GOVERNANCE, RISK & COMPLIANCE

Checksum
A short value computed from data and stored with it, to detect whether the data changed. It catches accidents, not attackers. CRYPTOGRAPHY

Cherry-pick
Copying one specific commit onto another branch. How an urgent fix reaches a release branch without dragging everything else with it. DEV & DELIVERY

Chip supply chain *Fab, foundry*
The concentrated global pipeline that designs and manufactures processors. A geopolitical dependency as much as a technical one. COMPUTE & HARDWARE

CI *Continuous Integration*
Automatically building and testing every change as it is pushed, so problems surface in minutes rather than at release. DEV & DELIVERY

CIA *Central Intelligence Agency*
The US foreign intelligence service, collecting abroad through its own operations and through partners. It has no domestic law-enforcement role. INTELLIGENCE & INVESTIGATIONS

CIA triad *Confidentiality, Integrity, Availability*
The three properties security exists to protect. Most controls trade one against another, and naming which one you are protecting sharpens the argument. GOVERNANCE, RISK & COMPLIANCE

CIDR *Classless Inter-Domain Routing*
The /24-style notation for writing a block of IP addresses. The number after the slash says how many leading bits are fixed — the bigger the number, the smaller the block. NETWORKING & PROTOCOLS

CIEM *Cloud Infrastructure Entitlement Management*
Finding and trimming excessive cloud permissions. Most cloud identities hold far more rights than they ever use. CLOUD & INFRASTRUCTURE

Cipher
An algorithm for turning readable text into unreadable text and back. The cipher is public; the key is what must stay secret. CRYPTOGRAPHY

Circuit *Tor circuit*
The path of relays Tor picks for your traffic — normally three, rebuilt every few minutes. No single relay in it knows both who you are and where you are going. NETWORKING & PROTOCOLS

Circuit-switched network
A network that reserves one continuous path for the whole conversation, as the old telephone system did. Reliable and wasteful; the internet chose packets instead. NETWORKING & PROTOCOLS

CISA *Cybersecurity and Infrastructure Security Agency*
The US civilian agency responsible for defending federal networks and helping critical infrastructure defend itself. It advises and coordinates; it does not investigate crimes. INTELLIGENCE & INVESTIGATIONS

Classification levels (government)
The US government scheme: Unclassified, then Confidential, Secret and Top Secret, according to the damage disclosure would cause. Compartments and handling caveats sit on top of the level. CLASSIFICATION & PERSONAL DATA

Classification scheme
Sorting information into levels according to the harm its disclosure would cause, so protection can follow the label rather than being argued case by case. CLASSIFICATION & PERSONAL DATA

Client
The system that asks for a service. A machine can be a client and a server at once — a proxy is both. NETWORKING & PROTOCOLS

Clock speed *GHz*
How many cycles a processor runs per second. A poor way to compare modern chips — architecture, cores and memory bandwidth matter more. COMPUTE & HARDWARE

Clone
Copying a remote repository, including its full history, onto your own machine. The first command of most working days. DEV & DELIVERY

Cluster / node
A cluster is many machines working as one system; a node is a single machine in it. The unit of scale for both HPC and cloud training runs. COMPUTE & HARDWARE

Code review
Another engineer reading a change before it lands. The cheapest place to catch both bugs and security mistakes. DEV & DELIVERY

Cold boot attack
Chilling memory chips so their contents survive a reboot long enough to be read, recovering encryption keys. Why locking a laptop is weaker than shutting it down. COMPUTE & HARDWARE

Cold, warm and hot sites *Recovery sites*
The three grades of standby facility. A hot site can take over in minutes and costs accordingly; a warm site takes hours to days; a cold site is space and power waiting for hardware to arrive. DEFENSE & OPERATIONS

Collision
Two different inputs producing the same hash. Once collisions are practical — as with MD5 and SHA-1 — the hash can no longer prove a file is unmodified. CRYPTOGRAPHY

Command and control *C2 / C&C*
The channel an attacker uses to issue instructions to compromised hosts. Increasingly hidden inside normal cloud and messaging traffic. ATTACKS & EXPLOITATION

Command injection
User input reaching a shell command, letting an attacker run arbitrary system commands as the application's user. APPLICATION SECURITY

Commit
A saved, described snapshot of your changes, recorded permanently in the history. The unit of work everything else — review, revert, blame — operates on. DEV & DELIVERY

Commit message
The note explaining what changed and why. The why is the part future-you cannot reconstruct from the diff. DEV & DELIVERY

Compartmentalisation
Splitting classified information into compartments so that access to one grants nothing in another. It limits the damage a single insider can do. CLASSIFICATION & PERSONAL DATA

Compensating control
An alternative measure when the required control is not feasible. Must genuinely meet the intent, not merely be documented as if it does. GOVERNANCE, RISK & COMPLIANCE

Competitive intelligence
Gathering information about competitors by means that are legal, or at least not obviously illegal. The boundary with espionage is thinner than the phrase suggests. ATTACKS & EXPLOITATION

Computer forensics
Recovering and analysing data from computers to a standard that will stand up in court. Method and documentation matter as much as findings. INTELLIGENCE & INVESTIGATIONS

Confidential (classification)
Information whose disclosure would harm the organisation or a person: contracts, salaries, customer lists, unreleased results. Access is granted by need, not by seniority. CLASSIFICATION & PERSONAL DATA

Confidential computing *TEE / enclave*
Processing data inside a hardware-protected enclave so even the host operating system cannot read it. Closes the in-use gap left by encryption at rest and in transit. AI & EMERGING TECH

Confidential (government)
The lowest US classification level, for information whose disclosure would cause damage to national security. Not the same thing as commercial confidential. CLASSIFICATION & PERSONAL DATA

Confidentiality
That information is seen only by those authorised to see it. The first leg of the CIA triad. GOVERNANCE, RISK & COMPLIANCE

Configuration drift
Live systems gradually diverging from their defined state through manual fixes. The reason a system that passed audit fails six months later. CLOUD & INFRASTRUCTURE

Configuration management
Establishing a known-good baseline and keeping systems to it. Most incidents start with something that drifted. DEFENSE & OPERATIONS

Constant-time comparison
Comparing secrets in a way that always takes the same time, so an attacker cannot learn the value one character at a time from response timing. CRYPTOGRAPHY

Container *Docker*
An application packaged with its dependencies, sharing the host kernel. Fast and portable, but isolation is weaker than a VM's. CLOUD & INFRASTRUCTURE

Container escape
Breaking out of a container to the host. Usually the result of privileged mode, a mounted socket, or an unpatched kernel. CLOUD & INFRASTRUCTURE

Container image
The read-only template a container starts from. Base images carry their own vulnerabilities, so scanning and rebuilding matter as much as your code. CLOUD & INFRASTRUCTURE

Containment
Stopping an incident spreading — isolating hosts, disabling accounts, blocking traffic — before removing the attacker. DEFENSE & OPERATIONS

Content provenance *C2PA*
Cryptographically signed metadata recording how a piece of media was made and edited. An attempt to make authenticity checkable rather than assumed. AI & EMERGING TECH

Context window
How much text a model can consider at once. Anything beyond it is dropped or summarised, which quietly changes behaviour. AI & EMERGING TECH

Contingency plan *User contingency plan*
How the business keeps working while the systems are down. Written for the people doing the work, not for the IT department. DEFENSE & OPERATIONS

Control
A safeguard reducing risk. Categorised as preventive, detective, or corrective, and as technical, administrative, or physical. GOVERNANCE, RISK & COMPLIANCE

Controlled unclassified information *CUI*
US government information that is unclassified but still restricted in how it is handled, covering categories such as export-controlled, law enforcement and privacy data. NIST SP 800-171 sets what contractors must do to protect it. CLASSIFICATION & PERSONAL DATA

Cookie
A small piece of data a server asks a browser to store and send back, so it can recognise the same client later. Session cookies are credentials in all but name. ENDPOINTS & SYSTEMS

Core / thread
A core is an independent processing unit; a thread is one stream of instructions running on it. More cores means more genuinely simultaneous work. COMPUTE & HARDWARE

Corruption
A threat action that changes system functions or data so the system works wrongly rather than not at all. ATTACKS & EXPLOITATION

CORS *Cross-Origin Resource Sharing*
Rules for when one origin may read another's responses. Loosening it to a wildcard with credentials is a routine and serious misconfiguration. APPLICATION SECURITY

Cost benefit analysis
Weighing what a control costs against the risk it removes. The argument that gets security funded, or does not. GOVERNANCE, RISK & COMPLIANCE

Countermeasure
An action taken to stop a detected threat from succeeding — a patch, a block rule, a filter. DEFENSE & OPERATIONS

Court order
An intermediate legal instrument between a subpoena and a warrant, reaching records a subpoena cannot but stopping short of content. INTELLIGENCE & INVESTIGATIONS

Covert channel
A way to move information using system behaviour never meant to carry it — free disk space, timing, packet sizes. Hard to see and harder to stop. ATTACKS & EXPLOITATION

CPU *Central Processing Unit*
The general-purpose processor that runs the operating system and most software. Very fast at doing one complicated thing after another. COMPUTE & HARDWARE

CPU vs GPU
A CPU is a few very fast generalists; a GPU is thousands of narrow specialists working in step. If your problem is the same maths repeated across a big array, the GPU wins by orders of magnitude. COMPUTE & HARDWARE

Credential stuffing
Replaying username and password pairs from earlier breaches against other sites, betting on reuse. Cheap, automated, and depressingly effective. IDENTITY & ACCESS

Crime of opportunity
An offence committed because the chance appeared, not because it was planned. Most low-level cybercrime, and the reason basic hygiene removes so much of it. INTELLIGENCE & INVESTIGATIONS

Crimeware
Malware built to make its operator money — stealing keystrokes, draining accounts, renting out infected machines. MALWARE & THREAT ACTORS

CRINK *China, Russia, Iran, North Korea*
Shorthand for the four states most often named as the strategic cyber adversaries of the United States and its allies. Convenient, and it flattens four very different actors. MALWARE & THREAT ACTORS

Crisis communications
Deciding in advance who says what to staff, customers, regulators, and press. Prepared badly, it turns an incident into a reputational event. DEFENSE & OPERATIONS

Critical infrastructure
The sectors a country cannot function without — power, water, health, finance, transport, communications. Mostly privately owned, which is why defending it needs public-private arrangements. DEFENSE & OPERATIONS

Criticality
How much a given failure actually matters — which is judged very differently by a government protecting a country and a company protecting a balance sheet. It is why the same vulnerability gets very different responses. INTELLIGENCE & INVESTIGATIONS

CRL / OCSP *Certificate Revocation List / Online Certificate Status Protocol*
The two ways to check whether a certificate has been revoked early. Both are patchy in practice, which is why short-lived certificates are now preferred. CRYPTOGRAPHY

Cross-border investigation
An investigation where evidence, suspects and victims sit in different jurisdictions. The technical work is usually the easy part. INTELLIGENCE & INVESTIGATIONS

Crossover cable
A cable wired to swap transmit and receive pairs so two devices can be connected directly. Modern hardware auto-detects, so it is mostly history. NETWORKING & PROTOCOLS

Cryptanalysis
The science of breaking cryptography — recovering plaintext or keys without being given them. What a cipher has to survive to be trusted. CRYPTOGRAPHY

Cryptominer *Cryptojacking*
Malware that quietly uses your compute to mine cryptocurrency. Low drama, but it signals that something else could have run instead. MALWARE & THREAT ACTORS

CSP *Content Security Policy*
A header telling the browser which sources of script, style, and frames are allowed. A strong second line of defence when XSS slips through. APPLICATION SECURITY

CSPM *Cloud Security Posture Management*
Continuously checking cloud configuration against policy — public buckets, open groups, missing encryption, over-broad roles. CLOUD & INFRASTRUCTURE

CSPRNG *Cryptographically Secure Pseudo-Random Number Generator*
A random source safe for keys and tokens. Ordinary language random() functions are not, and using one for a session token is a classic bug. CRYPTOGRAPHY

CSRF *Cross-Site Request Forgery*
Tricking a logged-in browser into sending a state-changing request the user never intended. Blocked with anti-CSRF tokens and SameSite cookies. APPLICATION SECURITY

Cut-through
Switching that starts forwarding as soon as the header is read, before the whole packet arrives. Lower latency, at the cost of passing on damaged frames. NETWORKING & PROTOCOLS

CVE / CVSS *Common Vulnerabilities and Exposures / Scoring System*
CVE is the unique identifier for a known flaw; CVSS scores its severity out of ten. CVSS ignores your context, so it is an input, not a decision. GOVERNANCE, RISK & COMPLIANCE

CWPP / CNAPP *Cloud Workload / Native Application Protection Platform*
Runtime protection for cloud workloads, and the bundled platforms that combine posture, workload, and identity checks. CLOUD & INFRASTRUCTURE

Cybercrime
Crime committed using a computer, or against one. The distinction matters in law: cyber as the means of an ordinary crime is charged differently from cyber as the target. INTELLIGENCE & INVESTIGATIONS

Cyber-enabled vs cyber-dependent crime
Cyber-enabled crime is an old crime committed with new tools — fraud, extortion, harassment. Cyber-dependent crime could not exist without computers — intrusion, malware, denial of service. INTELLIGENCE & INVESTIGATIONS

Cyber intelligence
Collecting and analysing information about adversaries in cyberspace to inform decisions, rather than to prosecute. Different standard of proof, different consumers, different timelines from an investigation. INTELLIGENCE & INVESTIGATIONS

Cyber investigation
Establishing what happened on a system, who did it and what can be proved about it. Distinct from incident response, which is about stopping it: an investigation has to survive scrutiny afterwards. INTELLIGENCE & INVESTIGATIONS

Cyber warfare
The use of cyber operations as an instrument of armed conflict. High impact for low cost, which is precisely what makes proportional response so contested. INTELLIGENCE & INVESTIGATIONS

Cyclic redundancy check *CRC*
A checksum designed to catch transmission errors. Fast, standard, and trivially forged — never use it as a security control. CRYPTOGRAPHY

D

87 ENTRIES

Daemon
A program that starts at boot and runs continuously in the background, serving requests. Windows calls the equivalent a service. ENDPOINTS & SYSTEMS

Dark web
Sites reachable only through anonymising networks like Tor. It hosts marketplaces and leak sites, and also censorship-resistant journalism. NETWORKING & PROTOCOLS

Dark web archive *Marketplace archive*
Preserved copies of seized or defunct hidden services — page captures, listings, vendor profiles and forum threads — held by researchers and law enforcement. The Silk Road archives are the worked example: the site is gone, and years of its listings, PGP keys and forum posts remain searchable evidence. INTELLIGENCE & INVESTIGATIONS

Dark web marketplace
A hidden service selling illicit goods, run with escrow, vendor ratings and dispute handling like any other marketplace. They are seized regularly and reconstitute under new names within weeks. INTELLIGENCE & INVESTIGATIONS

DAST *Dynamic Application Security Testing*
Testing a running application from the outside. Fewer false positives, but it only finds what it can reach. APPLICATION SECURITY

Data aggregation
Combining several kinds of record to build a fuller picture than any of them gives alone. It is why individually harmless datasets can become sensitive together. GOVERNANCE, RISK & COMPLIANCE

Datacentre *Rack, colocation*
The building full of racked servers behind every cloud service. Physical security, power and cooling are as much a part of availability as any software control. COMPUTE & HARDWARE

Data classification
Labelling data by sensitivity so handling rules can follow the label. Three or four tiers work; ten do not. GOVERNANCE, RISK & COMPLIANCE

Data custodian
Whoever is currently holding or processing the data and is responsible for protecting it while they do. The database team is a custodian, not an owner. GOVERNANCE, RISK & COMPLIANCE

Datagram
A self-contained packet that carries everything needed to be routed, without relying on any earlier exchange. The basis of connectionless protocols like UDP. NETWORKING & PROTOCOLS

Data handling rules
What each classification actually requires in practice — who may access it, how it is stored and transmitted, whether it may leave the country or the device, how it is disposed of. A classification without handling rules is decoration. CLASSIFICATION & PERSONAL DATA

Data minimisation
Collect only what you need and keep it only as long as you need it. The control that shrinks breach impact more than any tool. GOVERNANCE, RISK & COMPLIANCE

Data mining
Analysing existing data to find patterns worth acting on. The same technique serves fraud detection and intrusive profiling. GOVERNANCE, RISK & COMPLIANCE

Data owner
The person accountable for a set of data — what it is for, who may see it, how long it is kept. Accountability, not custody. GOVERNANCE, RISK & COMPLIANCE

Data poisoning
Corrupting training or retrieval data so the model learns something the attacker chose. Very hard to detect after the fact. AI & EMERGING TECH

Data residency *Data sovereignty*
Legal requirements about where data physically lives and which government can compel access to it. A cloud region choice with legal consequences. CLOUD & INFRASTRUCTURE

Data subject rights *DSAR*
Individuals' rights to access, correct, delete, or port their data, with statutory response deadlines. GOVERNANCE, RISK & COMPLIANCE

Data warehousing
Consolidating separate databases into one place for analysis. It also concentrates the consequences of one breach. GOVERNANCE, RISK & COMPLIANCE

Decapsulation
Stripping a layer's header off a packet and handing the rest up the stack. The receiving half of what encapsulation does on the way out. NETWORKING & PROTOCOLS

Deception technology *Honeypot, canary token*
Fake systems, files, or credentials that nothing legitimate should ever touch. Very low false-positive rate when they trigger. DEFENSE & OPERATIONS

Deception technology (honeytoken)
Planting credentials, files or hosts that have no legitimate use, so any touch is a high-confidence alert. DEFENSE & OPERATIONS

Deepfake *Synthetic media*
AI-generated audio, image, or video imitating a real person. Already routine in payment fraud and executive impersonation. AI & EMERGING TECH

Deep web
Everything on the web that a search engine has not indexed — anything behind a login, a paywall or a form. Vastly bigger than the dark web, and routinely confused with it: your bank statements are deep web, not dark web. NETWORKING & PROTOCOLS

Defacement
Altering a website's content to embarrass or make a point. Loud by design, and often a cover for something quieter. ATTACKS & EXPLOITATION

Defence in depth
Layering independent controls so no single failure is fatal. Assumes each layer will eventually fail, because it will. GOVERNANCE, RISK & COMPLIANCE

De-identification
Removing identifiers so data no longer points to a person. It is a spectrum, not a switch: weakly de-identified data is routinely re-identified by linking it to something else. CLASSIFICATION & PERSONAL DATA

Denial of service *DoS (concept)*
Preventing legitimate access to a system, or delaying it enough to matter. It does not require breaking in. ATTACKS & EXPLOITATION

Department of Defense intelligence *DoD*
The military side of US intelligence, including the service intelligence organisations such as naval intelligence. The US intelligence community runs to some eighteen to twenty separate organisations. INTELLIGENCE & INVESTIGATIONS

Department of Homeland Security *DHS*
The US department that CISA and the Secret Service sit under, covering domestic protective security across borders, infrastructure and emergencies. INTELLIGENCE & INVESTIGATIONS

Department of Justice *DOJ*
The US department that prosecutes federal crime, including computer crime, and supervises the FBI. Its independence from political direction is a norm rather than a mechanism. INTELLIGENCE & INVESTIGATIONS

Dependency *Package, library*
Third-party code your project relies on. Most of a modern application is dependencies, which is why supply chain security is a real concern. DEV & DELIVERY

Dependency confusion
Publishing a public package with the same name as a company's internal one so build tools fetch the attacker's version by mistake. ATTACKS & EXPLOITATION

Deploy *Ship, release to production*
Putting a built version onto the servers where real users reach it. Small, frequent deploys are safer than big rare ones, because there is less to unpick when one goes wrong. DEV & DELIVERY

Deprecation *EOL notice*
Formal warning that something will be removed, with a date. The window in which to migrate calmly rather than in an incident. DEV & DELIVERY

DES *Data Encryption Standard*
The 1970s US encryption standard, retired because its 56-bit key can be brute-forced. Its successor is AES. CRYPTOGRAPHY

Deserialisation vulnerability
Rebuilding objects from untrusted serialised data, which in many languages can trigger code execution during reconstruction. APPLICATION SECURITY

Detection as code
Managing detection rules in a repository with review and CI, so changes are traceable and testable like any other software. DEFENSE & OPERATIONS

Detection engineering
Treating detections as code: written, tested, version-controlled, and measured. The shift from buying alerts to building them. DEFENSE & OPERATIONS

DHCP *Dynamic Host Configuration Protocol*
Hands out IP addresses and network settings to devices as they join. A rogue DHCP server can quietly point every new device at an attacker's gateway and DNS. NETWORKING & PROTOCOLS

Dictionary attack
Trying words and phrases from a prepared list rather than every possible combination. Faster than brute force, because people pick words. IDENTITY & ACCESS

Diff
The line-by-line difference between two versions — what was added, removed and changed. What you actually review, rather than the whole file. DEV & DELIVERY

Differential privacy
Adding calibrated statistical noise so aggregate results are useful while no individual's presence can be inferred. GOVERNANCE, RISK & COMPLIANCE

Diffie–Hellman *DH / ECDH*
A method for two parties to agree a shared secret over a channel anyone can watch, without ever sending the secret itself. CRYPTOGRAPHY

Digest authentication
A web authentication scheme where the client proves it knows the password by hashing a challenge, rather than sending the password itself. CRYPTOGRAPHY

Digital envelope
A message encrypted with a session key, packaged together with that session key encrypted to the recipient. The classic hybrid construction. CRYPTOGRAPHY

Digital evidence
Data used to prove or disprove something in a proceeding. It must be collected in a way that keeps it authentic, complete and demonstrably unaltered. INTELLIGENCE & INVESTIGATIONS

Digital forensics *DFIR*
Recovering and analysing digital evidence to establish what happened. Paired with incident response as one discipline. DEFENSE & OPERATIONS

Digital signature
A hash of a message encrypted with the sender's private key. Anyone with the public key can confirm authorship and that nothing changed — and the signer cannot credibly deny it. CRYPTOGRAPHY

Digital Signature Algorithm *DSA*
An asymmetric algorithm that produces signatures as a pair of large numbers. Verifies both who signed and that nothing changed. CRYPTOGRAPHY

Directory
The catalogue of users, groups, machines and their attributes that an organisation authenticates against. IDENTITY & ACCESS

Directory service *Active Directory, LDAP*
The central store of users, groups, and computers. In most enterprises, compromising Active Directory is functionally the same as compromising everything. IDENTITY & ACCESS

Disassembly
Turning a compiled binary back into assembly to see what it actually does. The starting point of most malware analysis. ATTACKS & EXPLOITATION

Disaster recovery *DR*
Restoring technology after a major failure. Distinct from business continuity, which covers how the organisation keeps operating meanwhile. CLOUD & INFRASTRUCTURE

Discretionary access control *DAC*
Access decided by the owner of the resource, who can hand out permissions at will. Flexible, and it drifts. IDENTITY & ACCESS

Disruption
An event that interrupts or prevents correct operation of a service. It need not be an attack — a cut cable counts. ATTACKS & EXPLOITATION

Distance vector
A routing approach that picks paths by their cost in hops. Simple to run and slow to react to change; RIP is the classic example. NETWORKING & PROTOCOLS

Distillation
Training a small model to imitate a large one, trading a little quality for a lot of speed and cost. How capable models reach modest hardware. COMPUTE & HARDWARE

Distributed scan
Scanning from many source addresses at once so no single one looks busy enough to alarm anyone. Detection has to correlate across sources. NETWORKING & PROTOCOLS

DLL hijacking
Placing a malicious library where a trusted program will load it first. Turns a legitimate signed application into the malware's launcher. ENDPOINTS & SYSTEMS

DLP *Data Loss Prevention*
Tooling that spots and blocks sensitive data leaving. Good at accidents, weak against a determined insider. GOVERNANCE, RISK & COMPLIANCE

DLP monitoring *DLP (practice)*
Tooling that watches documents, mail and endpoints for sensitive information leaving, and blocks or flags it. Effective and intrusive: it means monitoring people's communications, which is a policy question before it is a technical one. DEFENSE & OPERATIONS

DMA *Direct Memory Access*
Devices reading and writing system memory without going through the CPU. Fast, and a real attack path — a malicious Thunderbolt or PCIe device can read memory directly. COMPUTE & HARDWARE

DNS *Domain Name System*
The internet's phone book: it turns names like example.com into IP addresses. Almost every attack chain touches it, which is why DNS logs are gold for investigators. NETWORKING & PROTOCOLS

DNS cache
The store of recent answers a resolver keeps so it need not ask again. It makes DNS fast, and gives poisoning something to aim at. NETWORKING & PROTOCOLS

DNS resolver *Recursive resolver*
The server that does the lookup legwork on your behalf, walking from the root servers down to the authoritative one and caching the answer. NETWORKING & PROTOCOLS

DNSSEC *DNS Security Extensions*
Cryptographic signatures on DNS records so a resolver can tell a genuine answer from a forged one. It proves authenticity, not confidentiality — the query is still visible. NETWORKING & PROTOCOLS

DNS tunnelling
Smuggling data in and out of a network inside DNS queries and responses. Slow, noisy if you look for it, and effective because DNS is rarely blocked. NETWORKING & PROTOCOLS

Documentation *README, docs*
The instructions that let someone else run, use or fix the thing. A project without a README is a project only its author can operate. DEV & DELIVERY

DoH / DoT *DNS over HTTPS / DNS over TLS*
Encrypted DNS lookups. Good for user privacy, awkward for defenders, because it hides the query from the network monitoring that used to see it. NETWORKING & PROTOCOLS

Domain *Windows domain*
A set of network resources and accounts managed together, where users log in once to reach everything in it. IDENTITY & ACCESS

Domain hijacking
Taking control of someone's domain — through the registrar, the DNS servers, or an expired registration. Everything that trusts the name follows the attacker. NETWORKING & PROTOCOLS

Domain name
The name that locates an organisation on the internet, read right to left from the top-level domain inward. NETWORKING & PROTOCOLS

DOM-based XSS
XSS caused entirely by client-side JavaScript writing untrusted data into the page. The server may never see the payload at all. APPLICATION SECURITY

DoS / DDoS *(Distributed) Denial of Service*
Overwhelming a service so real users cannot reach it. Distributed versions use many hosts at once, often a botnet or reflected traffic. ATTACKS & EXPLOITATION

Double extortion
Encrypting data and also threatening to publish it. Backups solve the outage but not the leak, which is why they are no longer a complete answer. MALWARE & THREAT ACTORS

DPIA *Data Protection Impact Assessment*
A required assessment before high-risk processing, documenting risks to people and how they are mitigated. Best done at design, not sign-off. GOVERNANCE, RISK & COMPLIANCE

DPRK IT worker scheme *North Korean remote workers*
North Korean operatives hired as remote IT staff under bought or stolen identities, routing pay back to the state and leaving remote access behind. Detected through identity, payroll and geolocation anomalies as much as through malware. MALWARE & THREAT ACTORS

Drive-by download
Malware installed simply by loading a page, exploiting the browser or a plugin without any click. ATTACKS & EXPLOITATION

Driver
Software letting the operating system talk to hardware. Drivers run with kernel privileges, so a vulnerable or signed-but-malicious driver is a direct route to full control. COMPUTE & HARDWARE

Drone forensics
Recovering flight logs, telemetry, imagery and controller pairings from unmanned aircraft. Increasingly routine in both criminal and security investigations. INTELLIGENCE & INVESTIGATIONS

Due care
Putting a reasonable level of protection in place, in line with what the industry considers normal practice. GOVERNANCE, RISK & COMPLIANCE

Due diligence
Assessing a supplier's security before signing. Questionnaires are the norm; evidence and audit rights are what actually matter. GOVERNANCE, RISK & COMPLIANCE

DumpSec
An old Windows auditing tool that dumped users, permissions, policies and services. Equally useful to an administrator and to an intruder. ENDPOINTS & SYSTEMS

Dumpster diving
Finding passwords, directories and documents in what an organisation threw away. Shredding is a security control. ATTACKS & EXPLOITATION

Dwell time
How long an intruder is inside before being detected. The metric that best reflects whether detection actually works. MALWARE & THREAT ACTORS

Dynamic link library *DLL*
A shared library that a program loads at runtime rather than containing itself. Which one gets loaded, and from where, is a whole class of vulnerability. ENDPOINTS & SYSTEMS

Dynamic routing protocol
A protocol that lets routers learn paths by talking to their neighbours. Convenient, and a target — routing announcements can be forged. NETWORKING & PROTOCOLS

E

45 ENTRIES

EAP *Extensible Authentication Protocol*
A framework that lets a link negotiate which authentication method to use, from passwords to certificates. The basis of enterprise Wi-Fi authentication. IDENTITY & ACCESS

Eavesdropping
Listening in on a conversation not meant for you. Often the first step, not the whole attack — what is overheard becomes the way in. NETWORKING & PROTOCOLS

ECC *Elliptic Curve Cryptography*
Public-key cryptography over elliptic curves, giving the same strength as RSA with far smaller keys. The default for new TLS and signing work. CRYPTOGRAPHY

Echo request / echo reply *Ping*
The ICMP pair behind ping: a request asking whether a host is alive, and its reply. Blocked on many networks, which is why a silent host is not necessarily a dead one. NETWORKING & PROTOCOLS

Edge computing
Processing data near where it is produced rather than in a central cloud. Cuts latency and bandwidth; multiplies the number of devices to secure. CLOUD & INFRASTRUCTURE

Edge inference *On-device AI*
Running a model on the user's own hardware. No data leaves the device, which is a privacy gain and a hard limit on model size. COMPUTE & HARDWARE

EDR *Endpoint Detection and Response*
An agent recording process, file, and network behaviour on the endpoint, with the ability to alert, hunt, and isolate. The successor to antivirus. ENDPOINTS & SYSTEMS

Egress cost / lock-in
Charges for moving data out of a cloud, and the dependence they create. A commercial concern that becomes a resilience concern. CLOUD & INFRASTRUCTURE

Egress filtering
Filtering traffic leaving your network. Ignored for years, and one of the most effective ways to break command and control. DEFENSE & OPERATIONS

Emanations analysis *TEMPEST*
Reading data from the unintentional signals a device gives off — electromagnetic leakage, sound, power draw. Defended by shielding, not software. CRYPTOGRAPHY

Embedded forensics
Forensics on devices that are not general-purpose computers — vehicles, controllers, medical devices, IoT. The data is there; the tooling to get at it usually is not. INTELLIGENCE & INVESTIGATIONS

Embedding
A numeric representation capturing meaning, so similar things sit close together. Not anonymised — original text can often be approximately recovered. AI & EMERGING TECH

Embodied carbon
The emissions from manufacturing hardware, before it is ever switched on. For short-lived devices it can outweigh the energy used running them. COMPUTE & HARDWARE

Encapsulation
Wrapping one protocol's data inside another's, so it can travel over a network that would not otherwise carry it. How tunnels and VPNs work. NETWORKING & PROTOCOLS

Encryption at rest
Data encrypted while stored on disk, so stolen hardware or a copied volume is useless. It does not protect data while the system is running and the key is loaded. CRYPTOGRAPHY

Encryption in transit
Data encrypted while moving over a network. The pair to encryption at rest — most compliance regimes ask for both. CRYPTOGRAPHY

End-of-life *EOL / unsupported*
Software the vendor no longer patches. Every future vulnerability in it stays open permanently, so EOL is a security deadline, not an IT one. ENDPOINTS & SYSTEMS

Endpoint
Any device a person uses to reach the network — laptop, phone, tablet, server. Where most intrusions begin and where most detection now lives. ENDPOINTS & SYSTEMS

End-to-end encryption *E2EE*
Only the sender and recipient hold the keys; the service carrying the message cannot read it. The distinction that matters when a provider is subpoenaed or breached. CRYPTOGRAPHY

ENISA *European Union Agency for Cybersecurity*
The EU's cybersecurity agency, which produces guidance, threat analysis and certification schemes rather than investigating incidents. INTELLIGENCE & INVESTIGATIONS

Enterprise risk management *ERM*
Looking at all of an organisation's risks together — cyber, financial, legal, physical — rather than in separate columns. Cyber stops being a special case. DEFENSE & OPERATIONS

Entropy
Genuine unpredictability. Keys and tokens generated from weak entropy are guessable no matter how strong the algorithm. CRYPTOGRAPHY

Environment *dev / staging / production*
Separate copies of the system for building, testing and real use. Staging should resemble production closely enough that passing there means something. DEV & DELIVERY

Environment variable *env var, .env*
Configuration passed to a program at runtime instead of written into the code. Where secrets belong in development — and `.env` belongs in `.gitignore`. DEV & DELIVERY

Ephemeral port
A short-lived high-numbered port assigned to a client for one connection and released when it closes. Firewall rules that assume fixed ports break on these. NETWORKING & PROTOCOLS

EPSS *Exploit Prediction Scoring System*
A probability that a vulnerability will be exploited in the next 30 days. Pairs well with CVSS to cut patch backlogs to something achievable. GOVERNANCE, RISK & COMPLIANCE

Eradication
Removing the attacker's access completely: malware, backdoors, added accounts, altered configuration, rogue tokens. DEFENSE & OPERATIONS

Escrow passwords
Passwords written down and locked away so emergency staff can get in when the usual people are unavailable. A control that has to be audited, not forgotten. IDENTITY & ACCESS

Ethernet *IEEE 802.3*
The dominant LAN technology — the wiring, framing and access rules under nearly every wired network. NETWORKING & PROTOCOLS

EU AI Act
The EU's risk-tiered regulation of AI systems, with outright bans at the top and obligations scaling with risk. Extraterritorial, like GDPR. AI & EMERGING TECH

Europol
The European Union's law enforcement agency, supporting member states on transnational crime and running the European Cybercrime Centre. INTELLIGENCE & INVESTIGATIONS

Event
Any observable occurrence on a system or network. Most events are nothing; an incident is an event that turns out to matter. DEFENSE & OPERATIONS

Event log
The operating system's record of what happened. Default retention is short, so shipping logs off-host is essential before an attacker clears them. ENDPOINTS & SYSTEMS

Evil maid attack
Physical tampering with an unattended device — a modified bootloader, a hardware keylogger. Full-disk encryption alone does not stop it. COMPUTE & HARDWARE

E-waste
Discarded electronics, much of it exported and dismantled unsafely. Extending device life is both an environmental and a procurement decision. COMPUTE & HARDWARE

Executive order
A directive from the US President binding on the executive branch. Much US cybersecurity policy — incident reporting, software supply chain requirements, critical infrastructure duties — arrives this way rather than through legislation. GOVERNANCE, RISK & COMPLIANCE

Exfiltration
Getting stolen data out, often in small encrypted chunks over allowed channels like HTTPS or a sanctioned file-sharing service. ATTACKS & EXPLOITATION

Exit scam
A marketplace operator shutting down and keeping whatever is held in escrow. It ends more dark web markets than police action does. INTELLIGENCE & INVESTIGATIONS

Explainability *XAI*
Being able to say why a model produced a given output. Increasingly a legal requirement for decisions affecting people. AI & EMERGING TECH

Exploit
Working code or a technique that turns a vulnerability into actual unauthorised behaviour. A vulnerability is theoretical until an exploit exists. ATTACKS & EXPLOITATION

Exponential backoff
Waiting progressively longer between retries after a failure, so a struggling system is not hammered by everything retrying at once. NETWORKING & PROTOCOLS

Exposure
A threat action where sensitive data is released directly to someone not entitled to it. ATTACKS & EXPLOITATION

Extended ACL *Cisco*
A router filter that can also match destination, protocol, ports and whether a session is already established. NETWORKING & PROTOCOLS

Exterior gateway protocol *EGP*
A protocol that carries routing between separately administered networks rather than inside one. BGP is the one that survived. NETWORKING & PROTOCOLS

Extradition
Handing a suspect over to another country to be prosecuted. It requires a treaty and a matching offence, which is why suspects in some countries are effectively unreachable. INTELLIGENCE & INVESTIGATIONS

F

37 ENTRIES

False rejects
When an authentication system turns away a legitimate user. Tuning a system to reduce false accepts almost always raises these. IDENTITY & ACCESS

Fast file system *FFS*
The first major redesign of the Unix file system, using inodes and better on-disk layout for speed. The ancestor of the file systems in use now. ENDPOINTS & SYSTEMS

Fast flux
Rapidly rotating the addresses a domain resolves to, across a botnet, so the infrastructure behind it cannot be taken down by blocking an IP. MALWARE & THREAT ACTORS

Fault line attack
Exploiting the gaps between systems, where each side assumes the other is checking. Integration points are where coverage runs out. ATTACKS & EXPLOITATION

FBI *Federal Bureau of Investigation*
The lead US federal agency for investigating cybercrime, and simultaneously a domestic intelligence service. It works cases for prosecution and collects intelligence, which is an unusual combination. INTELLIGENCE & INVESTIGATIONS

Feature flag *Toggle*
A switch that turns functionality on or off without a deploy. Separates releasing code from releasing the feature — and stale flags become their own mess. DEV & DELIVERY

Federation
Trusting another organisation's identity provider so their users can access your systems without separate accounts. Convenient, and it exports your trust decision. IDENTITY & ACCESS

Fetch
Downloading remote changes without applying them to your working copy. The cautious half of a pull, when you want to look before you merge. DEV & DELIVERY

FIDO2 / WebAuthn
The open standards behind hardware keys and passkeys. The browser signs a challenge with a key tied to the exact origin, so a lookalike site gets nothing. IDENTITY & ACCESS

Fileless attack
Malicious activity running in memory or scripting engines without writing to disk. Invisible to file-scanning antivirus by design. ATTACKS & EXPLOITATION

Filter
A rule deciding which packets are kept, shown or blocked — in a capture tool, in a firewall, or in a detection pipeline. DEFENSE & OPERATIONS

Filtering router
A router that also decides whether a packet should be forwarded at all, according to policy. The simplest form of firewall. NETWORKING & PROTOCOLS

Fine-tuning
Further training a base model on specific data to specialise it. Anything in that data is baked into the weights and cannot be selectively deleted. AI & EMERGING TECH

Fine-tuning vs LoRA *Low-Rank Adaptation*
Full fine-tuning updates every weight and needs serious hardware; LoRA trains a small adapter alongside the frozen model and runs on a single consumer GPU. COMPUTE & HARDWARE

Finger
An old protocol that returned information about a user on a host. Helpful, informative and long since disabled for exactly that reason. ENDPOINTS & SYSTEMS

Fingerprinting *OS fingerprinting*
Sending unusual packets and reading the replies to work out what operating system a host runs. Different stacks answer malformed input in different, recognisable ways. NETWORKING & PROTOCOLS

Firewall
A control that allows or blocks traffic by rule — usually address, port, and protocol. The traditional perimeter device, now also a per-host and per-cloud-resource control. NETWORKING & PROTOCOLS

Firmware update
Replacing the low-level software on a device. Often manual, sometimes unsigned, and the reason many devices stay vulnerable for years. ENDPOINTS & SYSTEMS

Five Eyes *FVEY*
The intelligence-sharing arrangement between the United States, United Kingdom, Canada, Australia and New Zealand. The deepest such arrangement that exists between states. INTELLIGENCE & INVESTIGATIONS

Flooding
Overwhelming a system with more input than it can process. The mechanism under most denial of service. NETWORKING & PROTOCOLS

FLOPS *Floating point operations per second*
The standard measure of raw compute, quoted in teraflops or petaflops. Peak FLOPS is a ceiling, not a promise — real workloads rarely approach it. COMPUTE & HARDWARE

Forest
A set of Active Directory domains that replicate with each other. The boundary that matters when working out how far a compromise can reach. IDENTITY & ACCESS

Fork
Your own server-side copy of someone else's repository, so you can change it without write access to the original and propose the change back. DEV & DELIVERY

Fork bomb
A process that repeatedly copies itself until no process slots remain and the machine stops. Four characters of shell, and a hard lesson in resource limits. ATTACKS & EXPLOITATION

Form-based authentication
Logging in through a web page form rather than a browser or protocol mechanism. What almost every web application does, with all the session handling that implies. IDENTITY & ACCESS

Forward lookup
Using a domain name to find its IP address. The ordinary DNS query. NETWORKING & PROTOCOLS

Forward proxy
A proxy that clients send their outbound requests through. The point where an organisation can inspect and control what leaves. NETWORKING & PROTOCOLS

Forward secrecy *PFS*
Using fresh, throwaway keys per session so that stealing the long-term private key later does not decrypt traffic captured earlier. CRYPTOGRAPHY

Fragmentation
Splitting a packet into smaller pieces to fit a link's maximum size. A reliable source of security bugs, because reassembly is easy to get wrong. NETWORKING & PROTOCOLS

Fragment offset
The field that says where a fragment belongs in the original packet. Forged offsets are how fragmentation attacks overwrite headers. NETWORKING & PROTOCOLS

Fragment overlap attack
An attack that sends fragments with deliberately wrong offsets so reassembly overwrites part of the original header — for example, the destination port. NETWORKING & PROTOCOLS

Frame
The unit of data on a local network segment, wrapping a packet in link-layer addressing. Frames carry packets the way envelopes carry letters. NETWORKING & PROTOCOLS

FTP *File Transfer Protocol*
An old file transfer protocol that authenticates in the clear and needs awkward extra connections. Superseded by SFTP and HTTPS. NETWORKING & PROTOCOLS

Full-disk encryption *BitLocker, FileVault, LUKS*
Encrypting the whole drive so a lost or stolen device gives up nothing. Protects data at rest, not a running unlocked machine. ENDPOINTS & SYSTEMS

Full duplex
A link that carries traffic in both directions at the same time. Half duplex takes turns; collisions are a half-duplex problem. NETWORKING & PROTOCOLS

Fully-qualified domain name *FQDN*
A hostname written out in full, all the way to the top-level domain — host plus complete domain, with nothing implied. NETWORKING & PROTOCOLS

Fuzzing
Throwing malformed and random input at a program to find crashes. Extremely effective at finding memory-safety and parser bugs. APPLICATION SECURITY

G

6 ENTRIES

Gateway
A network point that leads into another network. Your default gateway is the router you send everything you cannot reach directly to. NETWORKING & PROTOCOLS

GCHQ *Government Communications Headquarters*
The UK signals intelligence agency, and the parent of the National Cyber Security Centre. INTELLIGENCE & INVESTIGATIONS

GDPR *General Data Protection Regulation*
The EU regulation governing personal data. Extraterritorial, principles-based, and backed by fines up to four percent of global turnover. GOVERNANCE, RISK & COMPLIANCE

GDPR special categories *Sensitive personal data*
Under GDPR: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used to identify someone, health data, and data about sex life or sexual orientation. Processing it needs a specific additional condition, not just a lawful basis. CLASSIFICATION & PERSONAL DATA

Geoblocking
Allowing or refusing access based on the country an IP address maps to. Trivially bypassed with a VPN, which is why it filters noise rather than adversaries. NETWORKING & PROTOCOLS

gethostbyname / gethostbyaddr
The classic pair of lookup calls: name to address, and address to name. The programming face of forward and reverse DNS. NETWORKING & PROTOCOLS

#

1 ENTRY

.gitignore
A list of paths Git should never track — build output, local config, secrets. The first line of defence against committing a key by accident. DEV & DELIVERY

G

9 ENTRIES

GNU *GNU's Not Unix*
The free software project started in 1983 to build a complete Unix-like system, whose tools sit under most Linux distributions. ENDPOINTS & SYSTEMS

Gnutella
An early peer-to-peer file sharing network where every client was also a server. An object lesson in how hard decentralised networks are to police. ENDPOINTS & SYSTEMS

Golden image
A standard, pre-hardened system image every machine is built from, so security settings are the default rather than a follow-up task. ENDPOINTS & SYSTEMS

Golden Ticket
Forging Kerberos tickets using the domain's krbtgt key, granting an attacker persistent, self-issued access to anything in the domain. IDENTITY & ACCESS

GPU *Graphics Processing Unit*
A processor with thousands of simple cores built to do the same operation on huge amounts of data at once. Made for graphics, now the engine of machine learning. COMPUTE & HARDWARE

GPU cloud *Accelerator rental*
Renting accelerators by the hour rather than buying them. Cheaper to start, expensive to leave running — idle GPUs bill the same as busy ones. COMPUTE & HARDWARE

GPU passthrough *vGPU*
Giving a virtual machine direct or partitioned access to a physical GPU. Necessary for accelerated workloads in virtualised environments, and it weakens isolation. COMPUTE & HARDWARE

Group Policy *GPO*
Windows' central mechanism for pushing configuration to domain machines. Also a superb attacker tool once domain admin is obtained. ENDPOINTS & SYSTEMS

Guardrails
Filters and policies around a model's inputs and outputs. Necessary, probabilistic, and not a substitute for real authorisation checks. AI & EMERGING TECH

H

36 ENTRIES

Hacktivist
An attacker motivated by a political or social cause rather than money. Typically defacement, leaks, or denial of service. MALWARE & THREAT ACTORS

Hallucination *Confabulation*
A confident, fluent, wrong output. Not a bug to be patched out but a property of prediction, which is why verification has to be designed in. AI & EMERGING TECH

Hard-coded credentials
Passwords or keys written directly into source. They spread through forks, logs, and backups, and cannot be rotated without a code change. APPLICATION SECURITY

Hardening
Removing unnecessary services, accounts, and features and tightening what remains. Cheap, unglamorous, and highly effective. ENDPOINTS & SYSTEMS

Hardware implant
A malicious component added during manufacture or shipping. Rare, extremely hard to detect, and the reason high-assurance procurement tracks provenance. COMPUTE & HARDWARE

Hardware root of trust
An immutable component in silicon that everything else's trust chains back to. If it is compromised, no software check above it means anything. COMPUTE & HARDWARE

Harvest now, decrypt later
Recording encrypted traffic today in the expectation of breaking it with future technology. The reason long-lived secrets need post-quantum protection now, not eventually. CRYPTOGRAPHY

Hash function
A one-way function turning any input into a fixed-length fingerprint. Same input always gives the same digest; the digest cannot be reversed back to the input. CRYPTOGRAPHY

HBM *High Bandwidth Memory*
Memory stacked next to the processor for enormous bandwidth. The scarce component in AI accelerators, and often the real bottleneck rather than compute. COMPUTE & HARDWARE

HEAD *Git HEAD pointer*
A pointer to the commit you currently have checked out. `HEAD~1` is the one before it. DEV & DELIVERY

Header
The extra information at the front of a packet that lets the protocol stack handle it — addresses, lengths, flags. Everything an inspection tool reads first. NETWORKING & PROTOCOLS

Hidden service *.onion address*
A server reachable only inside Tor, addressed by a cryptographic name ending in .onion rather than a domain. Neither side of the connection learns the other's IP, which is why takedowns target operators rather than addresses. NETWORKING & PROTOCOLS

High availability *HA*
Design that survives component failure without downtime, through redundancy and failover. Availability is a security property too. CLOUD & INFRASTRUCTURE

Hijack attack
Seizing control of an already-established connection, so the attacker inherits an authenticated session. ATTACKS & EXPLOITATION

HIPAA identifiers *Safe harbour list*
The eighteen identifiers that must be stripped for health data to count as de-identified: names, geography finer than a state, all dates tied to an individual, phone and fax numbers, email, Social Security, medical record, health plan, account, licence and vehicle numbers, device identifiers, URLs, IP addresses, biometrics, full-face photographs, and any other unique code. CLASSIFICATION & PERSONAL DATA

HMAC *Hash-based Message Authentication Code*
A hash keyed with a shared secret, proving both that a message is unaltered and that it came from someone holding the key. CRYPTOGRAPHY

Homomorphic encryption
Computing directly on encrypted data without decrypting it. Real, but still slow enough that it is used narrowly rather than by default. CRYPTOGRAPHY

Honeymonkey *Honey client*
An automated system that browses the web pretending to be a user, to find sites that attack visitors. MALWARE & THREAT ACTORS

Honey pot
A system that exists only to be attacked, so defenders can watch how it is attacked. Anything touching it is suspicious by definition. MALWARE & THREAT ACTORS

Hop
One handoff between routers on a packet's journey. Hop counts limit how far a packet can travel before being dropped. NETWORKING & PROTOCOLS

Host-based intrusion detection *HIDS*
Detection that works from a single machine's own records — audit logs, file changes, process activity. Deep visibility on one host, blind to the rest. DEFENSE & OPERATIONS

Hotfix
An urgent fix taken straight to production outside the normal cycle. Legitimate, and worth logging, because it skipped the usual checks. DEV & DELIVERY

HPC *High Performance Computing*
Supercomputing for scientific workloads — climate models, genomics, simulation. Usually accessed through a batch scheduler rather than interactively. COMPUTE & HARDWARE

HSM *Hardware Security Module*
A tamper-resistant device that generates and uses keys without ever exporting them. The key can be used but not copied, even by an administrator. CRYPTOGRAPHY

HSTS *HTTP Strict Transport Security*
A header telling browsers to only ever use HTTPS for a domain, removing the downgrade window on first navigation. APPLICATION SECURITY

HTML *Hypertext Markup Language*
The markup that describes a web page's structure and content. ENDPOINTS & SYSTEMS

HTTP *Hypertext Transfer Protocol*
The request-and-response protocol the web runs on. Plain HTTP is unencrypted, so anything sent over it can be read or altered in transit. NETWORKING & PROTOCOLS

HTTP proxy
A proxy specifically for web traffic, sitting between browsers and servers. Also the standard tool for intercepting and modifying requests during testing. NETWORKING & PROTOCOLS

HTTPS *HTTP over TLS*
HTTP wrapped in TLS encryption. It proves you are talking to the site named in the certificate and stops anyone in the middle reading or editing the traffic. NETWORKING & PROTOCOLS

Hub
An obsolete device that repeated every incoming signal out of every port. Convenient for sniffing, which is exactly why switches replaced it. NETWORKING & PROTOCOLS

Human in the loop *HITL*
Requiring a person to approve consequential AI-driven actions. Only meaningful if the reviewer has the time and information to genuinely disagree. AI & EMERGING TECH

Hybrid attack
A dictionary attack that also tries the predictable variations people add — numbers, symbols, capital first letters. IDENTITY & ACCESS

Hybrid encryption
Using asymmetric cryptography to agree a key and symmetric cryptography to encrypt the data. Every TLS connection works this way. CRYPTOGRAPHY

Hybrid warfare
Combining cyber operations, information operations, economic pressure and conventional force. The Sandworm attacks on Ukraine are the standing example. INTELLIGENCE & INVESTIGATIONS

Hyperlink
A pointer in a document to something located elsewhere. The unit of the web, and the delivery mechanism for most phishing. ENDPOINTS & SYSTEMS

Hypervisor
The layer that runs and isolates virtual machines. Escaping it is the most valuable cloud vulnerability class, and correspondingly rare. CLOUD & INFRASTRUCTURE

59 ENTRIES

IaaS / PaaS / SaaS
Three levels of cloud service — raw machines, a managed platform, or finished software. The level decides how much security is yours and how much is the provider's. CLOUD & INFRASTRUCTURE

IAM policy
The rules defining which identity may perform which action on which cloud resource. Wildcards in these are the most common cloud misconfiguration. CLOUD & INFRASTRUCTURE

ICMP *Internet Control Message Protocol*
The protocol networks use to report errors and test reachability. It carries no user data, but it leaks a great deal about network shape. NETWORKING & PROTOCOLS

Idempotent
An operation that gives the same result whether you run it once or five times. What makes safe retries possible. DEV & DELIVERY

Identity
Who someone or what something is — the name by which a system knows them. Everything an access decision rests on. IDENTITY & ACCESS

Identity lifecycle *Joiner–Mover–Leaver*
Provisioning access on hire, adjusting it on transfer, and removing it on exit. Leaver failures — dormant accounts with live access — are a recurring audit finding. IDENTITY & ACCESS

IDOR *Insecure Direct Object Reference*
Changing an identifier in a URL or request and getting someone else's data because the server never checked ownership. APPLICATION SECURITY

IdP *Identity Provider*
The system that authenticates users and vouches for them to applications — Entra ID, Okta, Google Workspace. Compromise it and every downstream app follows. IDENTITY & ACCESS

IDS / IPS *Intrusion Detection / Prevention System*
Sensors that watch traffic for known-bad patterns. An IDS alerts; an IPS sits inline and drops the traffic, which is more useful and more dangerous. NETWORKING & PROTOCOLS

IETF *Internet Engineering Task Force*
The body that defines the internet's operating protocols, through open working groups and RFCs. NETWORKING & PROTOCOLS

IMAP *Internet Message Access Protocol*
A mail protocol that keeps messages on the server and syncs state across devices. What most mail clients speak today. NETWORKING & PROTOCOLS

Immutable backup *WORM*
Backups that cannot be altered or deleted for a set period, even by an administrator. The specific answer to ransomware deleting backups. CLOUD & INFRASTRUCTURE

Immutable infrastructure
Replacing servers instead of patching them in place. Removes configuration drift and quietly destroys most attacker persistence. CLOUD & INFRASTRUCTURE

Incident
An adverse event affecting a system or network, or a credible threat that one is about to happen. DEFENSE & OPERATIONS

Incident handling
The plan for dealing with an incident, conventionally in six steps: preparation, identification, containment, eradication, recovery and lessons learned. DEFENSE & OPERATIONS

Incident response *IR*
The structured process of handling a confirmed security incident. Usually framed as prepare, detect, contain, eradicate, recover, learn. DEFENSE & OPERATIONS

Incremental backup
A backup covering only what changed since the last one. Cheap to take, slower to restore, and useless if any link in the chain is missing. DEFENSE & OPERATIONS

Indirect prompt injection
Injection delivered through a document, web page, or email the model retrieves, so the attacker never talks to the system directly. AI & EMERGING TECH

Inetd *xinetd*
The old Unix service that listened on many ports and started the right program when a connection arrived. ENDPOINTS & SYSTEMS

Inference
Running a trained model to get an output. Where cost, latency, and most data-exposure questions actually live. AI & EMERGING TECH

Inference attack
Deriving something sensitive by connecting pieces of information that are individually harmless. The problem statistical disclosure control exists to solve. ATTACKS & EXPLOITATION

Information warfare
The contest between attackers and defenders over information itself: taking it, corrupting it, denying it, or shaping what people believe. GOVERNANCE, RISK & COMPLIANCE

Infostealer *Stealer*
Malware that grabs saved passwords, cookies, and session tokens, then leaves. Its output feeds credential markets and skips MFA via stolen sessions. MALWARE & THREAT ACTORS

InfraGard
The FBI's partnership programme with the private sector, sharing threat information with the operators of critical infrastructure across financial, energy, health and other sectors. INTELLIGENCE & INVESTIGATIONS

Infrastructure as code *IaC — Terraform, CloudFormation*
Defining infrastructure in version-controlled files. Makes environments reviewable and repeatable — and replicates a mistake everywhere instantly. CLOUD & INFRASTRUCTURE

Ingress filtering
Filtering traffic entering your network, including dropping packets whose source addresses could not legitimately come from outside. DEFENSE & OPERATIONS

Inherent vs residual risk
Risk before controls versus what remains after them. Residual risk is the number leadership should actually be shown. GOVERNANCE, RISK & COMPLIANCE

Initial access broker *IAB*
A criminal specialising in breaking in and selling that foothold on. The reason ransomware crews can skip the intrusion step entirely. ATTACKS & EXPLOITATION

Injection
Untrusted input being interpreted as code or commands. The root cause behind SQL injection, command injection, and most template attacks. APPLICATION SECURITY

Input validation
Checking that input matches an expected shape before use. Allow-lists work; deny-lists of bad characters eventually fail. APPLICATION SECURITY

Input validation attack
Deliberately sending unexpected input to see what breaks. The parent class of injection, overflow and traversal bugs. ATTACKS & EXPLOITATION

Insider threat
Harm caused by someone with legitimate access — malicious, negligent, or coerced. Technical controls help least here; process and monitoring matter most. ATTACKS & EXPLOITATION

Insider threat programme
The formal function for spotting and handling harm caused by people with legitimate access. It sits across HR, legal and security, which is why it is hard to run. DEFENSE & OPERATIONS

Insider threat vs cyber
Harm from someone with legitimate access. Whether it counts as cyber or physical depends on how they took the data, not on the harm — which is why insider programmes sit across both. INTELLIGENCE & INVESTIGATIONS

Instance metadata service *IMDS*
A local endpoint that hands running instances their cloud credentials. Reachable via SSRF unless the hardened version is enforced. CLOUD & INFRASTRUCTURE

Instruction set *ISA — x86, ARM, RISC-V*
The vocabulary of operations a processor understands. x86 dominates servers and older PCs, ARM dominates mobile and now Apple and cloud silicon, RISC-V is the open alternative. COMPUTE & HARDWARE

Integrity
That information has not been changed, by accident or design, and is complete and accurate. GOVERNANCE, RISK & COMPLIANCE

Integrity star property *No read down*
In the Biba integrity model, a user may not read data of lower integrity than their own, which would contaminate their work. IDENTITY & ACCESS

Internal (classification)
Information meant to stay inside the organisation but not damaging if it leaked — internal directories, process documents, ordinary email. The default class most data falls into. CLASSIFICATION & PERSONAL DATA

International warrant
A request through international channels for the arrest or search of someone abroad. Its force depends entirely on the receiving country's cooperation. INTELLIGENCE & INVESTIGATIONS

Internet
Strictly, the practice of connecting separate networks together; in general use, the global network that resulted. NETWORKING & PROTOCOLS

Internet Standard
A specification the IETF has blessed as stable, well understood and proven by working implementations. NETWORKING & PROTOCOLS

INTERPOL *International Criminal Police Organization*
The body that lets police forces in nearly two hundred countries pass information and requests to each other. It coordinates and notifies; it has no officers who make arrests. INTELLIGENCE & INVESTIGATIONS

Interrupt
A signal telling the operating system that something has happened and needs attention now. ENDPOINTS & SYSTEMS

Intranet
An organisation's own internal network built on internet technology, closed to outsiders. NETWORKING & PROTOCOLS

Intrusion detection *IDS (concept)*
Gathering and analysing activity across a system or network to spot security breaches, whether from outside or from insiders. DEFENSE & OPERATIONS

IOC *Indicator of Compromise*
An observable sign of intrusion — a hash, a domain, an IP. Easy to share, easy for attackers to change, so it dates quickly. MALWARE & THREAT ACTORS

IoT *Internet of Things*
Networked physical devices — cameras, sensors, meters. Weak defaults, rare updates, and long deployments make them ideal botnet recruits. ENDPOINTS & SYSTEMS

IP address *Internet Protocol address*
The number that identifies a device on a network so traffic can be routed to it. IPv4 looks like 192.0.2.10; IPv6 is longer and hexadecimal. NETWORKING & PROTOCOLS

IP flood
A denial of service that buries a host in more ping traffic than it can answer. Crude, loud, and still effective against small links. NETWORKING & PROTOCOLS

IP forwarding
The operating system setting that lets a host pass traffic between its network interfaces — that is, act as a router. Enabled accidentally, it bridges networks you meant to keep apart. NETWORKING & PROTOCOLS

IP lookup
Finding out what is known about an address — who holds it, which network and country it sits in. The first step of most attributions, and the least conclusive. INTELLIGENCE & INVESTIGATIONS

IPsec *Internet Protocol Security*
A suite for encrypting and authenticating traffic at the IP layer, used for site-to-site VPNs. Works below the application, so apps need no changes. NETWORKING & PROTOCOLS

IP spoofing
Sending packets with a forged source address. It hides the sender, breaks address-based trust, and makes amplification attacks possible. NETWORKING & PROTOCOLS

Island hopping
Attacking an organisation by first compromising a smaller partner, supplier or subsidiary that is trusted by it. The way into the bank is often through the firm that cleans its offices' laptops. ATTACKS & EXPLOITATION

ISO *International Organization for Standardization*
The international standards body whose members are national standards organisations. Its 27000 series covers information security management. GOVERNANCE, RISK & COMPLIANCE

ISO/IEC 27001 *International Organization for Standardization / International Electrotechnical Commission 27001*
The international standard for an information security management system, and certifiable. It assesses the management system, not the technical strength. GOVERNANCE, RISK & COMPLIANCE

Issue-specific policy
A policy covering one particular subject, such as passwords or acceptable use. GOVERNANCE, RISK & COMPLIANCE

ITU-T *International Telecommunication Union, Telecommunication Standardization Sector*
The United Nations telecommunications standards body, whose specifications are published as Recommendations. X.509 certificates come from here. GOVERNANCE, RISK & COMPLIANCE

J

9 ENTRIES

Jailbreak
Framing that persuades a model past its safety training. Distinct from prompt injection, which targets the application's instructions. AI & EMERGING TECH

Jitter (data)
Perturbing values in a database while preserving its aggregate statistics, so individuals cannot be picked out of published data. GOVERNANCE, RISK & COMPLIANCE

Job scheduler *Slurm, PBS*
Software that queues and allocates cluster jobs across users. On shared research clusters, you submit a job and wait rather than running things directly. COMPUTE & HARDWARE

Joint investigation
An investigation run by more than one agency, often across borders. It multiplies reach and multiplies the questions of who charges, where, and under whose rules. INTELLIGENCE & INVESTIGATIONS

JSON / YAML *JavaScript Object Notation / YAML Ain't Markup Language*
The two everyday data formats: JSON for APIs, YAML for configuration. YAML's indentation and loose typing cause more outages than they should. DEV & DELIVERY

Jump bag *Go bag*
The kit an incident responder can pick up and leave with — write blockers, drives, cables, notebooks, contact lists. Assembled before it is needed, not during. DEFENSE & OPERATIONS

Jumping *Hopping*
Moving a connection through a chain of intermediate machines so the far end never sees where it started. It is what Tor does deliberately with relays, and what an attacker does through compromised hosts — each hop is one more party who would have to be asked, in one more jurisdiction, to trace the traffic back. NETWORKING & PROTOCOLS

Just-in-time access *JIT*
Granting elevated rights only for a defined window, then removing them automatically. Replaces standing admin access, which is what attackers actually hunt for. IDENTITY & ACCESS

JWT *JSON Web Token*
A signed, self-describing token carrying claims about a user. Readable by anyone holding it — signed, not secret — so never put anything confidential inside. IDENTITY & ACCESS

K

9 ENTRIES

Kerberoasting
Requesting service tickets for accounts with weak passwords and cracking them offline. Quiet, effective, and needs only an ordinary domain account to start. IDENTITY & ACCESS

Kerberos
The ticket-based authentication protocol underneath Windows domains. Its ticket mechanics give rise to Kerberoasting, Golden Ticket, and Silver Ticket attacks. IDENTITY & ACCESS

Kernel
The core of the operating system, running with full hardware access. Code running here can hide from everything above it. ENDPOINTS & SYSTEMS

KEV *Known Exploited Vulnerabilities catalogue*
CISA's list of vulnerabilities confirmed exploited in the wild. A far better patching priority than CVSS score alone. GOVERNANCE, RISK & COMPLIANCE

Key derivation function *KDF — bcrypt, scrypt, Argon2, PBKDF2*
A deliberately slow, memory-hungry hash for passwords. Slowness is the feature: it makes brute-force guessing expensive. CRYPTOGRAPHY

Keylogger
Records keystrokes to capture passwords and messages. Exists as software and as small hardware devices inline with a keyboard. MALWARE & THREAT ACTORS

Key management *KMS*
Generating, storing, rotating, and retiring keys. Almost every real-world crypto failure is a key management failure, not a broken algorithm. CRYPTOGRAPHY

Kubernetes *K8s*
The dominant container orchestrator. Powerful, and insecure by default in ways that need deliberate configuration to fix. CLOUD & INFRASTRUCTURE

KV cache
Stored intermediate values that let a language model generate each new token without recomputing the whole context. It grows with context length and eats VRAM. COMPUTE & HARDWARE

L

25 ENTRIES

L2TP *Layer 2 Tunneling Protocol*
A tunnelling protocol used to build VPNs, normally paired with IPsec because it provides no encryption of its own. NETWORKING & PROTOCOLS

Labelling *Marking*
Recording the classification on the document, file or message itself so the handling rules travel with it. Automated labelling is what makes DLP enforceable. CLASSIFICATION & PERSONAL DATA

Large language model *LLM*
A model trained on vast text to predict likely continuations. Fluent by construction, and fluency is not the same as being correct. AI & EMERGING TECH

Lateral movement
Moving from the first compromised host to more valuable ones inside the network. Usually done with stolen valid credentials, not new exploits. ATTACKS & EXPLOITATION

Lattice techniques
Access decided by ordered security labels, where information may move in one direction through the ordering but not the other. IDENTITY & ACCESS

Lawful basis
The legal justification for processing personal data — consent, contract, legal obligation, vital interests, public task, legitimate interests. GOVERNANCE, RISK & COMPLIANCE

LDAP *Lightweight Directory Access Protocol*
The protocol for querying a directory of users, groups and resources. Directory queries are also how attackers map an organisation from the inside. IDENTITY & ACCESS

Least privilege
Give each account only the access its job requires, and no more. The principle nearly every access review is trying to enforce. IDENTITY & ACCESS

Left of boom / right of boom
Military shorthand adopted by security: everything before the incident is left of boom, everything after is right of boom. Prevention against response, on one timeline. DEFENSE & OPERATIONS

Legion
An old tool for finding unprotected network shares. The technique long outlived the tool. ENDPOINTS & SYSTEMS

Let's Encrypt / ACME *Automatic Certificate Management Environment*
A free CA and the protocol that automates issuing and renewing certificates. It made HTTPS the default rather than an upgrade. CRYPTOGRAPHY

Link state
A routing approach where every router keeps a map of the whole area and calculates its own best paths. Faster to converge than distance vector; OSPF is the example. NETWORKING & PROTOCOLS

Linter / formatter
Tools that flag likely mistakes and enforce consistent style automatically. They end style arguments and catch a surprising number of bugs. DEV & DELIVERY

List based access control
Access defined by attaching a list of users and privileges to each object. IDENTITY & ACCESS

Living off the land *LOLBins*
Using tools already installed — PowerShell, certutil, curl, WMI — instead of dropping malware. Nothing to detect as a bad file, so behaviour is the only signal. ATTACKS & EXPLOITATION

Loadable kernel module *LKM*
Code that adds functionality to a running kernel without a reboot. A useful facility, and how kernel-level rootkits get in. ENDPOINTS & SYSTEMS

Load balancer
Spreads incoming traffic across several backend servers, and takes unhealthy ones out of rotation. Also a single point to enforce TLS and rate limits. NETWORKING & PROTOCOLS

Loader / dropper
Small first-stage malware whose only job is to fetch and run the real payload. Kept simple so it stays undetected. MALWARE & THREAT ACTORS

Local admin rights
Full control of one machine. Removing standing local admin from ordinary users blocks a large share of malware outright. ENDPOINTS & SYSTEMS

Lockfile *package-lock.json, requirements.txt*
A record of the exact dependency versions installed, so every machine and every build gets the same ones. Commit it. DEV & DELIVERY

Log clipping
Selectively deleting entries from a log to hide a compromise. Why logs are shipped off the host as they are written. DEFENSE & OPERATIONS

Logic bomb
Malicious code that triggers on a condition, such as a date or a name disappearing from payroll. Usually an insider's tool. MALWARE & THREAT ACTORS

Logic gate
The elementary building block of a digital circuit, taking binary inputs to a binary output. Everything above it is built from these. ENDPOINTS & SYSTEMS

Log retention
How long logs are kept. Intrusions are often found months later, so short retention quietly makes investigation impossible. DEFENSE & OPERATIONS

Loopback address *127.0.0.1*
The pseudo-address that always means this machine. Traffic to it never leaves the host, which is why services bound to it are not exposed. NETWORKING & PROTOCOLS

M

39 ENTRIES

MAC address *Media Access Control address*
The hardware identifier burned into a network interface. Useful for local identification, useless as an authenticator — it can be changed in one command. NETWORKING & PROTOCOLS

Machine learning *ML*
Systems that derive rules from data rather than being programmed with them. The behaviour reflects the training data, including its errors and bias. AI & EMERGING TECH

main / master *Default branch*
The branch treated as the source of truth. Most projects protect it so nothing lands without review. DEV & DELIVERY

Malicious code
Software that looks useful but takes unauthorised access, or tricks the user into running something worse. The umbrella over viruses, Trojans and the rest. MALWARE & THREAT ACTORS

Malvertising
Malicious code delivered through legitimate ad networks, so a trusted site serves it unknowingly. ATTACKS & EXPLOITATION

Malware
Any software written to do harm or gain unauthorised access. An umbrella term covering everything below it. MALWARE & THREAT ACTORS

Malware family
A cluster of related samples sharing code and behaviour. Naming is inconsistent across vendors, which is why the same thing has five names. MALWARE & THREAT ACTORS

Mandatory access control *MAC*
Access decided by the system from classification labels on both users and data, which users cannot override. The model behind government classification. IDENTITY & ACCESS

Masquerade attack
One entity illegitimately posing as another to gain what that identity is trusted with. ATTACKS & EXPLOITATION

MCP *Model Context Protocol*
An open standard for connecting models to tools and data sources. Each connected server is a new trust relationship to review. AI & EMERGING TECH

MD5 *Message Digest 5*
An old cryptographic hash, now broken: attackers can produce two inputs with the same digest. Still seen as a file identifier, never as a security control. CRYPTOGRAPHY

MDM *Mobile Device Management*
Central enrolment and policy for phones and laptops — encryption, passcodes, app control, remote wipe. ENDPOINTS & SYSTEMS

Measures of effectiveness *MOE*
An attempt to estimate what effect a given action will actually have, rather than whether it was carried out. GOVERNANCE, RISK & COMPLIANCE

Memory bandwidth
How fast data moves between memory and the processor. For large models, feeding the chip is harder than the arithmetic itself. COMPUTE & HARDWARE

Memory forensics
Analysing RAM for injected code, decrypted secrets, and running processes that never touched disk. Often the only place fileless malware exists. DEFENSE & OPERATIONS

Memory safety
Preventing whole classes of memory bugs by design. The main argument for Rust, Go, and similar languages in new systems code. APPLICATION SECURITY

Merge
Combining one branch's changes into another. Git does it automatically unless both sides edited the same lines. DEV & DELIVERY

Merge conflict
Two branches changed the same lines and Git refuses to guess. You pick what the file should say, then commit the resolution. DEV & DELIVERY

Metadata vs content
Metadata is the record about a communication — who, when, from where, how long. Content is what was said. They are protected differently in law, and metadata is very often enough on its own. INTELLIGENCE & INVESTIGATIONS

MFA fatigue *Push bombing*
Spamming approval prompts until a tired user taps accept. Countered with number matching or by dropping push approval altogether. ATTACKS & EXPLOITATION

MI5 *Security Service*
The United Kingdom's domestic security service, responsible for threats inside the UK — terrorism, espionage, subversion. INTELLIGENCE & INVESTIGATIONS

MI6 *Secret Intelligence Service, SIS*
The United Kingdom's foreign intelligence service, collecting abroad. The James Bond half of the pair; MI5 is the domestic half. INTELLIGENCE & INVESTIGATIONS

Microsegmentation
Segmentation taken down to the individual workload, with policy attached to the service rather than the subnet. Usually enforced by agents or a service mesh. NETWORKING & PROTOCOLS

MITRE ATT&CK *Adversarial Tactics, Techniques and Common Knowledge*
A public catalogue of real-world attacker techniques, organised by tactic. The common vocabulary for describing and mapping detection coverage. MALWARE & THREAT ACTORS

Model card
Documentation of a model's intended use, training data, evaluation, and limitations. The AI equivalent of a datasheet. AI & EMERGING TECH

Model extraction *Model stealing*
Reconstructing a proprietary model by querying it enough times to train a copy of its behaviour. AI & EMERGING TECH

Model inversion / membership inference
Extracting training data, or proving a specific record was in the training set, by probing the model. A privacy problem for models trained on personal data. AI & EMERGING TECH

Model weights *Parameters*
The learned numbers that are the model. Their count and precision together decide how much VRAM you need — roughly two bytes per parameter at 16-bit. COMPUTE & HARDWARE

Monoculture
Everyone running the same software, so one vulnerability reaches everyone. A resilience argument, not a technical one. MALWARE & THREAT ACTORS

Monorepo
Many projects in one repository, sharing tooling and history. Simpler coordination, heavier tooling; the alternative is many small repos. DEV & DELIVERY

Morris Worm
The 1988 worm that spread across the ARPANET and forced thousands of hosts offline. The event that produced the first CERT. MALWARE & THREAT ACTORS

mTLS *Mutual TLS*
TLS where both sides present certificates, not just the server. Common between internal services because it authenticates the client without passwords. NETWORKING & PROTOCOLS

MTTD / MTTR *Mean Time to Detect / Respond*
How long detection and response take on average. The two operational metrics that most reflect real-world damage. DEFENSE & OPERATIONS

Multicast
Traffic from one host to a defined group of hosts. Efficient for streaming, and awkward to filter. NETWORKING & PROTOCOLS

Multi-cloud
Using more than one cloud provider. Reduces lock-in, multiplies the number of identity and policy models you must get right. CLOUD & INFRASTRUCTURE

Multi-factor authentication *MFA / 2FA*
Requiring two or more different kinds of proof — something you know, have, or are. The single highest-value control against stolen passwords. IDENTITY & ACCESS

Multi-homed
Connected to more than one upstream provider. It buys resilience, and it complicates routing and filtering. NETWORKING & PROTOCOLS

Multiplexing
Combining several signals onto one path so they can share a link. Every backbone circuit depends on it. NETWORKING & PROTOCOLS

Mutual legal assistance treaty *MLAT*
The formal channel by which one country asks another for evidence. Slow enough — often months — that investigators plan around it rather than through it. INTELLIGENCE & INVESTIGATIONS

N

26 ENTRIES

NAT *Network Address Translation*
A router rewriting private internal addresses into one public address on the way out. It is why a whole office can share a single IP, and why inbound connections need explicit port forwarding. NETWORKING & PROTOCOLS

National Crime Agency *NCA*
The UK's national law enforcement agency for serious and organised crime, including its National Cyber Crime Unit. INTELLIGENCE & INVESTIGATIONS

NATO *North Atlantic Treaty Organization*
The intergovernmental military alliance of North American and European states. It has said that a cyber attack can trigger the collective defence commitment, without saying which one would. INTELLIGENCE & INVESTIGATIONS

NATO CCDCOE *Cooperative Cyber Defence Centre of Excellence*
NATO's cyber defence research and training centre in Tallinn, best known for the Tallinn Manual on how international law applies to cyber operations. INTELLIGENCE & INVESTIGATIONS

Natural disaster
Fire, flood, earthquake, storm — the causes of outage that no amount of patching prevents. They belong in the same plan as attacks. DEFENSE & OPERATIONS

N-day *One-day*
A known, patched vulnerability that is still exploitable because the target has not applied the fix. The overwhelming majority of real intrusions. ATTACKS & EXPLOITATION

Need to know
The rule that clearance permits access only to the specific information required for your role. It is what stops a Top Secret clearance from being a key to everything. CLASSIFICATION & PERSONAL DATA

NetFlow *Flow data*
Summary records of who talked to whom, for how long, and how much — without the contents. Cheap to keep for a long time, which makes it the backbone of retrospective hunting. NETWORKING & PROTOCOLS

Netmask *Subnet mask*
The 32-bit value that separates the network part of an address from the host part. It decides what counts as local and what has to go through a router. NETWORKING & PROTOCOLS

Network-based intrusion detection *NIDS*
Detection that watches traffic passing a sensor on the network. It sees breadth, and only what crosses its own segment. DEFENSE & OPERATIONS

Network mapping
Building an inventory of the hosts and services on a network. The same exercise for a defender protecting an estate and an attacker planning a route through it. NETWORKING & PROTOCOLS

Network segmentation
Splitting a network into zones with controlled paths between them so a foothold in one zone does not reach everything. The single most effective limit on lateral movement. NETWORKING & PROTOCOLS

Network tap
A hardware device spliced into a cable that copies passing traffic to a monitoring system. Unlike a mirrored port, it cannot silently drop traffic under load. NETWORKING & PROTOCOLS

NGFW *Next-Generation Firewall*
A firewall that also identifies the application and user behind the traffic, not just ports and IPs, and can inspect decrypted sessions. NETWORKING & PROTOCOLS

NIST *National Institute of Standards and Technology*
The US standards agency whose publications — the Cybersecurity Framework, the 800 series — function as default security guidance far beyond the US government. GOVERNANCE, RISK & COMPLIANCE

NIST CSF *NIST Cybersecurity Framework*
A voluntary framework organised around Govern, Identify, Protect, Detect, Respond, Recover. Widely used as a common structure for maturity conversations. GOVERNANCE, RISK & COMPLIANCE

NIST SP 800-53 / 800-171
Detailed US federal control catalogues — 800-53 for federal systems, 800-171 for contractors handling controlled unclassified information. GOVERNANCE, RISK & COMPLIANCE

Node (Tor) *Relay*
One of the volunteer machines a Tor circuit is built from. Each relay knows only the hop before and the hop after, which is what breaks the link between sender and destination. INTELLIGENCE & INVESTIGATIONS

No expectation of privacy
The doctrine that where a person had no reasonable expectation of privacy, evidence can be gathered without a warrant. Corporate banners and acceptable use policies exist largely to establish it. INTELLIGENCE & INVESTIGATIONS

Nonce / IV *Number used once / Initialisation Vector*
A unique value per encryption operation so identical plaintexts do not produce identical ciphertexts. Reusing one can collapse the security of the whole scheme. CRYPTOGRAPHY

Non-printable character
A byte with no visible character, like a linefeed or a null. Filters that only think about visible text are routinely bypassed with these. NETWORKING & PROTOCOLS

Non-repudiation
Being able to prove someone took an action so they cannot credibly deny it. What signatures and tamper-evident logs provide. GOVERNANCE, RISK & COMPLIANCE

Notification letter *Breach notice*
The letter sent to people whose personal data was exposed, saying what happened and what is being offered. In most US states and under GDPR it is a legal duty with a clock attached. CLASSIFICATION & PERSONAL DATA

NSA *National Security Agency*
The US signals intelligence agency — interception, cryptanalysis, satellites — and also the source of much defensive cryptographic guidance. Long nicknamed 'no such agency' for how little it acknowledged itself. INTELLIGENCE & INVESTIGATIONS

Null session *Anonymous logon*
A Windows connection made without credentials that could still enumerate users and shares. A classic reconnaissance foothold. IDENTITY & ACCESS

NVLink / InfiniBand *Interconnect*
High-speed links between GPUs and between servers. Training a large model across many chips is limited by interconnect as much as by the chips. COMPUTE & HARDWARE

O

21 ENTRIES

OAuth 2.0
A delegation framework: it lets an app act on your behalf against another service without ever seeing your password. It is about access, not identity. IDENTITY & ACCESS

Obfuscation
Deliberately making code hard to read or analyse. Used by malware authors and, legitimately, by software vendors protecting their products. MALWARE & THREAT ACTORS

Object storage *S3, Blob, GCS*
Cloud file storage addressed by key rather than path. Publicly-readable buckets remain one of the most common data exposures. CLOUD & INFRASTRUCTURE

Observability *Logs, metrics, traces*
Being able to tell what a running system is doing from the outside. Logs say what happened, metrics count it, traces follow one request across services. DEV & DELIVERY

Octet
Eight bits. Used instead of 'byte' in networking, where a byte has not always meant eight bits. NETWORKING & PROTOCOLS

OIDC *OpenID Connect*
An identity layer built on top of OAuth 2.0. OAuth grants access; OIDC actually tells the app who you are, in a signed ID token. IDENTITY & ACCESS

On-call / escalation
Defined rotas and paths for raising an incident out of hours. An unclear escalation path costs more time than any tool saves. DEFENSE & OPERATIONS

One-way encryption
An irreversible transformation, where the original cannot be recovered from the output even knowing the key. Hashing, not encryption, despite the name. CRYPTOGRAPHY

One-way function
A function easy to compute forwards and infeasible to reverse. The foundation of hashing and of public-key cryptography. CRYPTOGRAPHY

Onion Router *Tor*
The full name of Tor, filed here so it can be found under O as well as T. Traffic is wrapped in a layer of encryption for each relay it will cross, and each relay peels off one — hence the onion. NETWORKING & PROTOCOLS

Onion routing
The layered-encryption technique behind Tor: each relay peels off one layer, learning only enough to pass the traffic on. NETWORKING & PROTOCOLS

Operating system *OS*
The software managing hardware, memory, and processes. Its permission model is the boundary attackers are usually trying to cross. ENDPOINTS & SYSTEMS

Operational security failure *OPSEC failure*
The mistake that undoes an otherwise anonymous operation — a reused username, an early forum post, a personal email in a code commit, a package addressed to a real name. Silk Road's operator was found through his own early advertising posts, not through breaking Tor. INTELLIGENCE & INVESTIGATIONS

Order of volatility
Collect the most perishable evidence first — memory, then network state, then disk. Pulling the plug destroys the most useful data. DEFENSE & OPERATIONS

OSI model *Open Systems Interconnection*
The seven-layer reference model for network communication, from physical wiring up to the application. Nothing implements it exactly; everyone uses it to describe where a problem sits. NETWORKING & PROTOCOLS

OSPF *Open Shortest Path First*
A link-state routing protocol used inside an organisation's own network. Routers share a map of links and costs rather than just hop counts. NETWORKING & PROTOCOLS

OT / ICS *Operational Technology / Industrial Control Systems*
Computers that run physical processes — plants, grids, pipelines. Long lifespans, no patch windows, and safety outranks confidentiality. ENDPOINTS & SYSTEMS

Output encoding
Escaping data for the context it lands in — HTML, attribute, JavaScript, SQL. The correct fix for XSS, applied at the point of output. APPLICATION SECURITY

Overload
Degrading a system by loading it beyond what its components can handle. The result may be denial of service without any exploit at all. NETWORKING & PROTOCOLS

OWASP *Open Worldwide Application Security Project*
A nonprofit producing free application security guidance, tools, and the widely-cited Top 10 lists. APPLICATION SECURITY

OWASP Top 10
A periodically-updated list of the most critical web application risks. An awareness document, not a checklist to certify against. APPLICATION SECURITY

P

97 ENTRIES

Package manager *npm, pip, cargo, apt*
The tool that installs and updates dependencies. Also the channel a typosquatted or hijacked package arrives through. DEV & DELIVERY

Packer / crypter
Tools that compress or encrypt malware so its file signature changes. Cheap evasion, which is why signature-only detection fails. MALWARE & THREAT ACTORS

Packet
A chunk of a message with a destination address attached, routed independently across the network. In IP networks packets are also called datagrams. NETWORKING & PROTOCOLS

Packet capture *PCAP*
A raw recording of network traffic, read with tools like Wireshark or tcpdump. The ground truth when logs disagree about what actually crossed the wire. NETWORKING & PROTOCOLS

Packet-switched network
A network where each packet finds its own route to the destination and the pieces are reassembled on arrival. Resilient because there is no single fixed path to break. NETWORKING & PROTOCOLS

PAM *Privileged Access Management*
Controls specifically for admin accounts — vaulted credentials, checkout with approval, session recording, and automatic rotation. IDENTITY & ACCESS

PAP *Password Authentication Protocol*
A weak authentication scheme that sends the password across the network, usually unprotected. Superseded by CHAP and everything after. IDENTITY & ACCESS

Parallelism *Data / model / pipeline parallel*
Splitting work across chips — by data batch, by slicing the model itself, or by staging layers. How anything too large for one accelerator gets trained. COMPUTE & HARDWARE

Parameterised query *Prepared statement*
Sending SQL structure and data separately so input can never become code. The definitive SQL injection fix. APPLICATION SECURITY

Partition
A major division of a physical disk, treated as a separate volume by the operating system. ENDPOINTS & SYSTEMS

Passkey
A WebAuthn credential stored on a device or synced through a platform account, replacing the password entirely. Unlocked with a fingerprint, face, or PIN. IDENTITY & ACCESS

Pass-the-hash *PtH*
Authenticating with a stolen password hash without ever cracking it, because the protocol accepts the hash as proof. IDENTITY & ACCESS

Password cracking
Working out passwords from stolen hashes by guessing and hashing candidates until one matches. IDENTITY & ACCESS

Password sniffing
Capturing credentials off the wire, usually on a local network, from protocols that send them in the clear. IDENTITY & ACCESS

Password spraying
Trying one or two common passwords across many accounts, staying under lockout thresholds. Slower than brute force and far less likely to trip alarms. IDENTITY & ACCESS

Patch
A vendor fix for a bug or vulnerability. Applying them promptly prevents more breaches than any tool you can buy. ENDPOINTS & SYSTEMS

Patch Tuesday
Microsoft's monthly release of security fixes, on the second Tuesday. Exploit development against those fixes typically follows within days. ENDPOINTS & SYSTEMS

Path traversal *Directory traversal*
Using ../ sequences to read files outside the intended directory, such as configuration or key material. APPLICATION SECURITY

Payload
The part of an attack that does the intended damage or gives access, as opposed to the delivery mechanism that gets it there. ATTACKS & EXPLOITATION

Payment card data *CHD*
The cardholder data PCI DSS governs — the card number, cardholder name, expiry and service code — plus the authentication data that may never be stored at all: the full magnetic stripe, the CVV, and the PIN. CLASSIFICATION & PERSONAL DATA

PCI DSS *Payment Card Industry Data Security Standard*
Mandatory rules for anyone handling payment card data. Contractual rather than statutory, and enforced by fines and lost processing rights. GOVERNANCE, RISK & COMPLIANCE

PCIe *Peripheral Component Interconnect Express*
The bus connecting GPUs, drives and network cards to the processor. Its generation and lane count cap how fast data reaches an accelerator. COMPUTE & HARDWARE

Penetration
Getting unauthorised access to sensitive data by getting around a system's protections. ATTACKS & EXPLOITATION

Penetration test *Pentest*
An authorised, time-boxed attempt to break in and prove impact. Deeper than a scan, narrower than a red team engagement. APPLICATION SECURITY

Pepper
A secret value mixed into password hashing and stored separately from the database, so a database dump alone is not enough to start cracking. CRYPTOGRAPHY

Perl
A scripting language with strong text-processing roots, long the default for system administration and CGI scripts. ENDPOINTS & SYSTEMS

Permutation
Rearranging the positions of characters or bits rather than replacing them. One of the two classical building blocks of ciphers, with substitution. CRYPTOGRAPHY

Persistence
Making access survive reboots, password resets, and cleanup — scheduled tasks, services, registry keys, rogue OAuth grants, extra SSH keys. ATTACKS & EXPLOITATION

Personal data / PII *Personally Identifiable Information*
Data relating to an identifiable person. GDPR's definition is deliberately broad and includes IP addresses and device identifiers. GOVERNANCE, RISK & COMPLIANCE

Personal firewall
A firewall running on an individual machine rather than at the network boundary. The last control still standing once an attacker is already inside. DEFENSE & OPERATIONS

Personal information *PI*
The broader legal category used in privacy law — anything relating to an identified or identifiable person, including data that never names them: IP addresses, cookie and advertising identifiers, location traces, browsing history, inferences drawn about them. Wider than PII by design. CLASSIFICATION & PERSONAL DATA

Personally identifiable information *PII*
Information that identifies a specific person, alone or combined with other data. Direct identifiers: name, Social Security number, passport or driving licence number, email address, phone number, home address, account numbers, biometric templates, face photograph, device or vehicle identifiers. Indirect ones become identifying in combination — date of birth with postcode with gender is famously enough to single out most people. CLASSIFICATION & PERSONAL DATA

PGP *Pretty Good Privacy*
Long-standing software for encrypting and signing mail and files with public keys. Powerful, awkward, and still the standard in some communities. CRYPTOGRAPHY

Pharming
Redirecting users to a fake site by corrupting name resolution, so the address they typed is correct and the destination is not. ATTACKS & EXPLOITATION

Phishing
A fraudulent message designed to make someone hand over credentials or run something. Still the most common way intrusions begin. ATTACKS & EXPLOITATION

Phishing-resistant MFA
Factors bound to the real domain so they cannot be relayed to a fake one — hardware security keys and passkeys. Codes and push prompts are not phishing-resistant. IDENTITY & ACCESS

Ping of death
An old attack that sent an oversized ping packet to crash the receiving machine's input buffers. Long fixed, but the template — malformed input crashes a parser — never went away. NETWORKING & PROTOCOLS

Ping scan
A check for which machines answer ICMP echo requests. The cheapest form of host discovery, and the easiest to spot in logs. NETWORKING & PROTOCOLS

Ping sweep
Pinging a whole range of addresses to find out which hosts exist. Usually the first step of mapping a network before probing it. NETWORKING & PROTOCOLS

Pipeline *Workflow, GitHub Actions*
The scripted sequence that runs on a push — install, lint, test, build, scan, deploy. It holds real credentials, which makes it a genuine attack surface. DEV & DELIVERY

Pivoting
Using a machine you have already compromised as the launch point for reaching further into a network. The second host is attacked from inside, where the firewall is not looking. ATTACKS & EXPLOITATION

PKI *Public Key Infrastructure*
The whole apparatus of issuing, distributing, renewing, and revoking certificates and keys. Most PKI incidents are expiries and misissuance, not cryptographic breaks. CRYPTOGRAPHY

Plaintext / ciphertext
Plaintext is the readable data; ciphertext is what it looks like after encryption. Encryption turns one into the other, decryption turns it back. CRYPTOGRAPHY

Playbook / runbook
Written steps for a specific scenario. Their real value is that they work at three in the morning when nobody is thinking clearly. DEFENSE & OPERATIONS

Pod
Kubernetes' smallest deployable unit — one or more containers sharing a network identity and storage. CLOUD & INFRASTRUCTURE

Poison reverse
A stronger form of split horizon: the route is advertised back, but marked as unreachable. The unreachable claim is what kills the loop. NETWORKING & PROTOCOLS

Policy / standard / procedure
Policy states intent, standards set specific requirements, procedures give the steps. Collapsing them into one document is why nobody follows any of them. GOVERNANCE, RISK & COMPLIANCE

Polyinstantiation
Letting a database hold several records with the same key at different classification levels, so users at a lower level cannot infer that a higher-level record exists. GOVERNANCE, RISK & COMPLIANCE

Polymorphic malware
Malware that rewrites its own code each time it spreads, so no two copies look alike to a scanner. MALWARE & THREAT ACTORS

Polymorphism
Malware that rewrites its own code as it spreads, so no two copies look alike to a signature scanner. MALWARE & THREAT ACTORS

POP3 *Post Office Protocol*
A mail protocol where the client downloads messages from the server, traditionally removing them. Largely displaced by IMAP. NETWORKING & PROTOCOLS

Port
A numbered door on a host. The IP gets you to the machine; the port gets you to the specific service — 22 for SSH, 443 for HTTPS. NETWORKING & PROTOCOLS

Port scan
Knocking on each port of a host in turn to see which services answer. The responses tell an attacker where to look for weaknesses. NETWORKING & PROTOCOLS

Possession
Holding and controlling information, whether or not you can read it. A stolen encrypted laptop is a loss of possession even if confidentiality holds. GOVERNANCE, RISK & COMPLIANCE

Post-incident review *Lessons learned, blameless postmortem*
Examining what happened and why, without hunting individuals. Blame guarantees the next incident is reported late or not at all. DEFENSE & OPERATIONS

Post-quantum cryptography *PQC*
Algorithms designed to survive quantum computers, now standardised as ML-KEM and ML-DSA. Being adopted early because encrypted traffic stolen today could be decrypted later. CRYPTOGRAPHY

PowerShell
Windows' scripting and administration shell. Enormously useful to admins and attackers alike, which is why script block logging matters. ENDPOINTS & SYSTEMS

PPP *Point-to-Point Protocol*
A protocol for carrying IP over a direct link between two machines, historically a dial-up line. NETWORKING & PROTOCOLS

PPTP *Point-to-Point Tunneling Protocol*
An early VPN protocol, now considered broken. Its presence in a configuration is a finding, not a feature. NETWORKING & PROTOCOLS

Preamble
The pattern of bits at the start of a transmission that lets receivers lock on to the timing. Below the level most people ever look at, and essential. NETWORKING & PROTOCOLS

Precision *FP32 / FP16 / BF16 / INT8*
How many bits represent each number. Lower precision means less memory and more speed, at some cost in accuracy — the central trade in running models cheaply. COMPUTE & HARDWARE

Preservation request
An order telling a provider to freeze an account's data while legal process is prepared. Without it, logs age out before the warrant arrives. INTELLIGENCE & INVESTIGATIONS

Pretexting
Inventing a plausible scenario and identity to justify an unusual request. The setup that makes the eventual ask feel routine. ATTACKS & EXPLOITATION

Privacy by design
Building privacy protections into a system from the start, with privacy-protective defaults. A GDPR obligation, not a philosophy. GOVERNANCE, RISK & COMPLIANCE

Private addressing *RFC 1918*
The address ranges reserved for internal networks — 10/8, 172.16/12 and 192.168/16 — which routers on the public internet will not carry. NETWORKING & PROTOCOLS

Privilege escalation
Gaining rights beyond those granted. Vertical means user to admin; horizontal means reaching another user's data at the same level. IDENTITY & ACCESS

Privilege separation
Running each component with only the rights it needs, so a compromise in one part does not hand over the whole system. ENDPOINTS & SYSTEMS

Process injection
Running malicious code inside another, trusted process so it inherits that process's identity and looks normal. ENDPOINTS & SYSTEMS

Production *Prod*
The live system real people depend on. Every rule about review, backups and change control exists because of what happens here. DEV & DELIVERY

Program infector
Malware that attaches itself to existing executables, so running an ordinary program runs it too. MALWARE & THREAT ACTORS

Program policy
The high-level policy that sets the organisation's overall security posture and tone. GOVERNANCE, RISK & COMPLIANCE

Promiscuous mode
A network interface configured to accept every packet it sees, not just its own. Necessary for packet capture, and a hallmark of a sniffer. NETWORKING & PROTOCOLS

Prompt
The instruction and context given to a model. In most current systems it is also, unhelpfully, the security boundary. AI & EMERGING TECH

Prompt injection
Hostile instructions hidden in content a model reads, hijacking its behaviour. The defining security problem of LLM applications. AI & EMERGING TECH

Proof of concept *PoC*
Minimal code demonstrating that a vulnerability is genuinely exploitable. Public PoC release usually marks the start of mass scanning. ATTACKS & EXPLOITATION

Proportional response
The principle that retaliation should match the force used against you. Applied to cyber operations it is genuinely unsettled: what a proportional answer to a destructive intrusion looks like is still argued over. INTELLIGENCE & INVESTIGATIONS

Proprietary information
Information unique to a company and central to its ability to compete — customer lists, costs, designs, trade secrets. GOVERNANCE, RISK & COMPLIANCE

Protected health information *PHI*
Health information tied to an identifiable person and handled by a covered organisation — diagnoses, treatment records, prescriptions, test results, insurance and billing detail, appointment records, provider notes. Under HIPAA it is the identifiers plus the health context that make it PHI. CLASSIFICATION & PERSONAL DATA

Protocol
An agreed set of rules for how two endpoints communicate. Protocols exist at every layer of a connection. NETWORKING & PROTOCOLS

Protocol stack
The set of protocol layers that work together to move data, each handing off to the one below. NETWORKING & PROTOCOLS

Proxy
A middleman that makes requests on your behalf. A forward proxy fronts clients, a reverse proxy fronts servers, and both are natural places to inspect or filter traffic. NETWORKING & PROTOCOLS

Proxy chain *Chained proxies*
Stringing several proxies together so each one only knows its neighbours. Cheap to set up, and only as private as the least trustworthy link, which keeps logs. NETWORKING & PROTOCOLS

Proxy (investigative view)
An intermediate server that stands between the user and the destination, so the destination sees the proxy's address. It moves the question of identity one hop back. INTELLIGENCE & INVESTIGATIONS

Proxy server
A server that sits between users and the internet, fetching things on their behalf. It can filter, cache, log — and it hides the real client from the far end. NETWORKING & PROTOCOLS

Public (classification)
Information intended for anyone — published material, marketing, public filings. The only class that needs no protection against disclosure, though it still needs integrity. CLASSIFICATION & PERSONAL DATA

Public key
The half of a key pair you can publish. Others encrypt to it or verify signatures with it; only the private half can reverse that. CRYPTOGRAPHY

Public key encryption *Asymmetric cryptography*
Encryption with a key pair, where what one key does only the other can undo. It solves key distribution at the cost of speed. CRYPTOGRAPHY

Public-key forward secrecy *PFS*
The property that recording today's traffic gains nothing if a long-term private key leaks later, because session keys are derived fresh. CRYPTOGRAPHY

Public / private / hybrid cloud
Shared provider infrastructure, dedicated infrastructure, or a mix. Hybrid is the common reality, and the seams between the two are where control gaps live. CLOUD & INFRASTRUCTURE

Public vs private sector response
Government investigates to enforce law and protect the state; a company investigates to stop the bleeding, meet its obligations and protect its business. The same incident produces two different investigations with different definitions of success. INTELLIGENCE & INVESTIGATIONS

PUE *Power Usage Effectiveness*
Total facility power divided by the power actually reaching the computers. A PUE of 1.1 is efficient; anything near 2 means half the energy is going on cooling and losses. COMPUTE & HARDWARE

Pull
Fetching changes from the remote and merging them into your branch. Pull before you start work, or you will be resolving conflicts later. DEV & DELIVERY

Pull request *PR / merge request / MR*
A proposal to merge one branch into another, with a place to discuss and review it first. Where code review, CI checks and approvals happen. DEV & DELIVERY

Purple teaming
Red and blue working together, running known techniques to check whether detection actually fires. Improvement rather than scorekeeping. DEFENSE & OPERATIONS

Purpose limitation
Data collected for one stated purpose may not be quietly reused for another. The principle most often broken by analytics and AI training. GOVERNANCE, RISK & COMPLIANCE

Push
Sending your local commits up to the remote repository so others — and any deployment pipeline — can see them. Nothing you have not pushed exists to anyone else. DEV & DELIVERY

Pyramid of Pain
A model ranking indicators by how much it costs an attacker when you block them. Hashes are trivial to change; behaviours are not. MALWARE & THREAT ACTORS

Q

3 ENTRIES

QAZ *QAZ network worm*
A network worm from around 2000, notable mainly as an early case of a backdoor spreading through file shares. MALWARE & THREAT ACTORS

Quantisation
Converting model weights to lower precision so they fit in less memory and run faster. It is how large models end up running on a laptop or a phone. COMPUTE & HARDWARE

Quantum computing
Computation using quantum states, able in principle to break RSA and elliptic-curve cryptography. The reason post-quantum migration is starting now. AI & EMERGING TECH

R

59 ENTRIES

Race condition *TOCTOU*
A bug where the outcome depends on timing between a check and its use. Exploited by firing simultaneous requests — a common cause of duplicate refunds and coupon abuse. APPLICATION SECURITY

Radiation monitoring
Capturing images, data or audio by listening to the radiation an unshielded device emits. CRYPTOGRAPHY

RAG *Retrieval-Augmented Generation*
Fetching relevant documents and giving them to a model as context. It grounds answers — and makes every retrievable document an injection surface. AI & EMERGING TECH

Rainbow table
A precomputed lookup from hashes back to passwords. Defeated entirely by per-user salting, which is why unsalted hashes are treated as plaintext. CRYPTOGRAPHY

RAM *Random Access Memory*
Fast working memory holding what a program is actively using. Volatile — it empties on power loss, which is why memory forensics is time-critical. COMPUTE & HARDWARE

Ransomware
Malware that encrypts data and demands payment for the key. Modern operations steal the data first, so paying does not undo the breach. MALWARE & THREAT ACTORS

Ransomware-as-a-service *RaaS*
A criminal business model where developers rent their malware and infrastructure to affiliates for a cut. It industrialised ransomware. MALWARE & THREAT ACTORS

RAT *Remote Access Trojan*
Malware giving an attacker interactive control of a machine — files, screen, camera, shell — as if sitting at it. MALWARE & THREAT ACTORS

Rate limit *Quota*
How many API calls you are allowed in a window. Read it before writing the loop, cache the responses, and handle the 429 rather than retrying blindly. DEV & DELIVERY

Rate limiting
Capping how many requests a client can make in a window. The simplest defence against brute force, scraping, and abuse. CLOUD & INFRASTRUCTURE

RBAC *Role-Based Access Control*
Permissions attached to roles, and roles attached to people. Simple and auditable, until the roles multiply and everyone ends up in several. IDENTITY & ACCESS

RDP *Remote Desktop Protocol*
Windows remote graphical access. Exposed to the internet, it is one of the most-attacked services in existence. ENDPOINTS & SYSTEMS

Rebase
Replaying your commits on top of an updated branch to give a straight history instead of a merge. Never rebase a branch other people have already pulled. DEV & DELIVERY

Reconnaissance *Recon*
The stage of an attack spent finding systems, mapping networks and looking for a way in — before anything is exploited. NETWORKING & PROTOCOLS

Recovery
Bringing systems back into service safely and confirming the environment is clean. Restoring too early reinfects everything. DEFENSE & OPERATIONS

Red team / blue team
Red attacks to test defences, blue defends and detects. Purple team is the practice of running both together so findings actually improve detection. MALWARE & THREAT ACTORS

Refactor
Restructuring code without changing what it does. If behaviour changed, it was not a refactor, and it needs reviewing as a real change. DEV & DELIVERY

Reflexive ACL *Cisco*
A router filter that only allows return traffic belonging to connections started from inside. A step toward stateful firewalling. NETWORKING & PROTOCOLS

Region / availability zone
A geographic location and an isolated datacentre within it. Regions matter for data residency law; zones matter for surviving hardware failure. CLOUD & INFRASTRUCTURE

Registry *Windows Registry*
Windows' central configuration database. A common place for malware to persist, since certain keys run automatically at boot or login. ENDPOINTS & SYSTEMS

Registry (Windows)
The central store of Windows settings and configuration. Persistence, configuration and evidence all live here. ENDPOINTS & SYSTEMS

Regression
Something that used to work and now does not. Regression tests exist so the same bug cannot come back twice unnoticed. DEV & DELIVERY

Regression testing
Running a fixed set of tests before each release to check that what worked still works. Fuzzing is its adversarial cousin. APPLICATION SECURITY

Re-identification
Reconnecting supposedly anonymous records to people, usually by combining datasets. The reason true anonymisation is much harder than it sounds. GOVERNANCE, RISK & COMPLIANCE

Release
A tagged, packaged version handed to users, usually with notes and built artifacts attached. DEV & DELIVERY

Remote *origin, upstream*
A named repository your local copy talks to. `origin` is normally your own copy; `upstream` is the original you forked from. DEV & DELIVERY

Remote work scam
Fraud built on remote employment — fake workers, bought identities, remote access software installed on company machines. The employment process becomes the intrusion vector. INTELLIGENCE & INVESTIGATIONS

Repository *Repo*
The project folder plus its entire history of changes. Everything else in version control is an operation on a repository. DEV & DELIVERY

Reset
Moving your branch pointer backwards, optionally throwing away work. Powerful locally, destructive if you force-push the result. DEV & DELIVERY

Resource exhaustion
Tying up something finite — memory, connections, file handles, disk — until there is none left for legitimate use. NETWORKING & PROTOCOLS

Responsible disclosure *Coordinated disclosure*
Reporting a flaw privately and agreeing a window before publication, so a fix exists before the details do. APPLICATION SECURITY

REST / GraphQL
Two API styles: REST exposes resources at URLs and you take what each returns; GraphQL exposes one endpoint and you ask for exactly the fields you want. DEV & DELIVERY

Restricted (classification) *Highly confidential*
The most sensitive commercial class: credentials, encryption keys, merger plans, source code, regulated personal data. Small named access lists and logged access. CLASSIFICATION & PERSONAL DATA

Retention schedule
How long each category of data is kept before deletion. Data you deleted on schedule cannot be breached or subpoenaed. GOVERNANCE, RISK & COMPLIANCE

Reverse engineering
Working out how a system or component functions by taking it apart. Used to find vulnerabilities, to analyse malware, and to steal designs. ATTACKS & EXPLOITATION

Reverse lookup *Reverse DNS, PTR lookup*
Running a lookup backwards: you have the IP address and you want the name behind it, rather than the other way round. It is a standard first move in an investigation — take the address out of a log and ask who it belongs to — and the answer is often stale, generic or missing entirely, because nobody is obliged to publish one. NETWORKING & PROTOCOLS

Reverse proxy
A server that sits in front of your applications, terminating TLS and passing requests inward. Where load balancing, caching, and web application firewalls usually live. NETWORKING & PROTOCOLS

Revert
Creating a new commit that undoes an earlier one, leaving the history intact. The safe way to back out a change that is already public. DEV & DELIVERY

RFC *Request for Comments*
The numbered document series in which internet protocols are proposed and defined. Anyone can submit one; the IETF decides what becomes a standard. NETWORKING & PROTOCOLS

Right to repair
Being able to fix and upgrade hardware you own — parts, tools and documentation. Directly affects how long a device stays secure and usable. COMPUTE & HARDWARE

RIP *Routing Information Protocol*
An old distance-vector protocol that judges routes by hop count alone. Easy to configure and easy to fool. NETWORKING & PROTOCOLS

Risk appetite / tolerance
How much risk leadership is willing to accept. Without it stated, every risk decision becomes an argument. GOVERNANCE, RISK & COMPLIANCE

Risk assessment
Identifying what could go wrong and how much it would cost you. The input to every decision about what to spend. GOVERNANCE, RISK & COMPLIANCE

Risk averse
Avoiding risk even at the price of the opportunity. A defensible position, and an expensive one when it becomes the default answer. GOVERNANCE, RISK & COMPLIANCE

Risk register
The recorded list of known risks with owners, ratings, and treatment. Useful when actively reviewed, decorative when not. GOVERNANCE, RISK & COMPLIANCE

Risk treatment *Accept, mitigate, transfer, avoid*
The four things you can do about a risk. Accepting is legitimate — provided someone with authority signs it. GOVERNANCE, RISK & COMPLIANCE

Role-based access control *RBAC (concept)*
Access granted through roles that match job functions, rather than to individuals one at a time. IDENTITY & ACCESS

Rollback
Returning to the previous working version after a bad deploy. Knowing you can roll back in one step is what makes frequent deploys reasonable. DEV & DELIVERY

Root
The all-powerful administrative account on Unix systems. Gaining it is usually the attacker's objective, not their entry point. IDENTITY & ACCESS

Rootkit
Malware that hides itself deep in the operating system or below it, altering what the system reports about itself. Often only detectable from outside the host. MALWARE & THREAT ACTORS

Router
A device that forwards traffic between networks based on IP addresses. It decides where a packet goes next, hop by hop. NETWORKING & PROTOCOLS

Routing loop
Two or more misconfigured routers passing the same packet back and forth. TTL is what eventually ends it. NETWORKING & PROTOCOLS

Rowhammer
Repeatedly accessing memory rows to flip bits in neighbouring ones through electrical interference. A software attack on a physical property of RAM. COMPUTE & HARDWARE

Royal Canadian Mounted Police *RCMP*
Canada's national police force, and its point of contact for cross-border cybercrime investigations. INTELLIGENCE & INVESTIGATIONS

RPC scan
A probe for which remote procedure call services a machine is running. Often the route to an unpatched service nobody knew was exposed. NETWORKING & PROTOCOLS

RSA *Rivest–Shamir–Adleman*
The classic public-key algorithm, based on the difficulty of factoring large numbers. Still common, but large and slow next to elliptic curve, and a prime target for quantum attacks. CRYPTOGRAPHY

RTO / RPO *Recovery Time / Point Objective*
How fast you must be back, and how much data you can afford to lose. Two numbers that decide the entire backup architecture. CLOUD & INFRASTRUCTURE

Rule set based access control *RSBAC*
Access decided by rules about what entities may do to objects, rather than by lists attached to either. IDENTITY & ACCESS

Runbook automation
Turning repeated manual response steps into scripts or workflows. Consistency under pressure, and a free audit trail. DEFENSE & OPERATIONS

S

135 ENTRIES

Safety
That the people involved with an organisation — staff, customers, visitors — come to no harm. In OT and medical systems it outranks every other property. GOVERNANCE, RISK & COMPLIANCE

Salt
Random data added to a password before hashing, unique per user. It stops one precomputed table cracking every account at once. CRYPTOGRAPHY

Same-origin policy *SOP*
The browser rule that keeps one site's scripts from reading another site's data. The foundation everything else in web security sits on. APPLICATION SECURITY

SAML *Security Assertion Markup Language*
The older XML-based standard for federated SSO, still standard in enterprise software. Its signature handling has a long history of bypass bugs. IDENTITY & ACCESS

Sandbox
An isolated environment where untrusted code can run without touching anything that matters — a browser tab, a malware analysis VM, or the boundary an AI agent is meant to stay inside. Only as strong as the boundary itself: escapes are the whole game. MALWARE & THREAT ACTORS

Sandbox escape
Breaking out of the isolation a sandbox is supposed to enforce, so code reaches the host, the network, or credentials it was never meant to see. MALWARE & THREAT ACTORS

Sandbox evasion
Malware checking whether it is being watched — virtual machine artefacts, no mouse movement, too little uptime — and staying dormant if so. MALWARE & THREAT ACTORS

Sandworm
The Russian military intelligence unit behind BlackEnergy, Industroyer, NotPetya and the attacks that cut power in Ukraine. The name comes from Andy Greenberg's book about it — the standard case study in cyber as an instrument of war. MALWARE & THREAT ACTORS

SAST *Static Application Security Testing*
Scanning source code for vulnerable patterns without running it. Broad coverage, high false-positive rate. APPLICATION SECURITY

SBOM *Software Bill of Materials*
A machine-readable inventory of components in a piece of software. Turns a new vulnerability disclosure into a lookup rather than a scramble. GOVERNANCE, RISK & COMPLIANCE

SCA *Software Composition Analysis*
Inventorying third-party dependencies and flagging known-vulnerable versions. Most of a modern codebase is not written in-house. APPLICATION SECURITY

SCADA *Supervisory Control and Data Acquisition*
The monitoring and control layer above industrial equipment. Historically built for isolated networks and now, unhelpfully, often reachable. ENDPOINTS & SYSTEMS

Scareware
Fake alerts claiming infection to push a purchase or a phone call. The on-ramp to tech-support fraud. MALWARE & THREAT ACTORS

Scavenging
Searching through leftover data — deleted files, swap space, freed memory — for something sensitive that was never really erased. ATTACKS & EXPLOITATION

Scheduled task / cron
Built-in job schedulers. Legitimate everywhere, and among the first things to check for attacker persistence. ENDPOINTS & SYSTEMS

SCIM *System for Cross-domain Identity Management*
The standard for pushing user creation, updates, and deprovisioning from an identity provider into applications automatically. IDENTITY & ACCESS

Scotland Yard *Metropolitan Police*
The headquarters of London's police force, and by extension shorthand for British policing. A local force, not a national one — a common source of confusion in cross-border cases. INTELLIGENCE & INVESTIGATIONS

Script kiddie
Someone using others' tools without understanding them. Still capable of real damage against anything left unpatched. MALWARE & THREAT ACTORS

SDK / CLI *Software Development Kit / Command Line Interface*
A library that wraps an API in your language, and a terminal tool that wraps it for humans and scripts. Usually easier and safer than hand-rolling HTTP calls. DEV & DELIVERY

Search warrant
A judicial authorisation to search and seize, granted on probable cause. It is what reaches content: the messages themselves, the files, the contents of an account. INTELLIGENCE & INVESTIGATIONS

Secret
The US classification for information whose disclosure would cause serious damage to national security. CLASSIFICATION & PERSONAL DATA

Secrets management
Keeping credentials out of code and configuration and in a vault with rotation and audit. Hard-coded secrets in repositories remain a top breach cause. APPLICATION SECURITY

Secure Boot
Firmware refusing to load unsigned boot code, blocking bootkits before the operating system starts. ENDPOINTS & SYSTEMS

Secure cookie flags *HttpOnly, Secure, SameSite*
HttpOnly hides a cookie from JavaScript, Secure restricts it to HTTPS, and SameSite limits cross-site sending. Three flags, most cookie attacks covered. APPLICATION SECURITY

Secure SDLC
Building security into every stage of development rather than testing at the end. Threat modelling, review, testing, and monitoring as normal practice. APPLICATION SECURITY

Security awareness training
Teaching staff to recognise and report attacks. Effective when it is short, frequent, and safe to report to; useless as an annual slideshow. GOVERNANCE, RISK & COMPLIANCE

Security clearance
A vetting decision that a person may be trusted with classified information up to a level. Clearance alone is not enough: access also requires need to know. CLASSIFICATION & PERSONAL DATA

Security group *Network ACL*
Cloud firewall rules attached to resources or subnets. An accidentally open management port here is a recurring breach origin. CLOUD & INFRASTRUCTURE

Security key *Hardware token, YubiKey*
A physical device that holds authentication keys and requires a touch to use. The strongest widely-available second factor. IDENTITY & ACCESS

Security log
The record of security-relevant activity on a system — logons, privilege use, policy changes. The first thing an investigator asks for and the first thing an attacker edits. DEFENSE & OPERATIONS

Security policy
The rules that say how an organisation protects its systems and information. Everything else — standards, procedures, controls — hangs off it. GOVERNANCE, RISK & COMPLIANCE

Segment
A TCP packet. Also, confusingly, a physical or logical slice of a network. NETWORKING & PROTOCOLS

Segregation of duties *SoD*
Splitting a sensitive process so no one person can complete it alone. The standard control against both fraud and single-point mistakes. GOVERNANCE, RISK & COMPLIANCE

Semantic versioning *SemVer*
MAJOR.MINOR.PATCH, where major means a breaking change, minor adds features, patch fixes bugs. It tells you how nervous to be about upgrading. DEV & DELIVERY

Sensitive information
Information that is not classified but would still cause harm if it got out. Governments define it formally; most organisations discover the definition after a leak. GOVERNANCE, RISK & COMPLIANCE

Sensitive information (commercial)
The working middle of a private-sector scheme — information that is not secret but should not circulate freely. The label does the work; the definitions vary by organisation. CLASSIFICATION & PERSONAL DATA

Sensitive PII
The subset of personal data whose exposure causes immediate, serious harm: Social Security and national ID numbers, financial account and card numbers, passport and driving licence numbers, biometrics, and credentials. Usually the trigger for breach notification and for encryption requirements. CLASSIFICATION & PERSONAL DATA

Separation of duties
Splitting a sensitive task so no one person can complete it alone. It turns fraud from a decision into a conspiracy. GOVERNANCE, RISK & COMPLIANCE

Server
The system that answers requests from clients. The word covers the software, the machine, or both, depending on who is talking. NETWORKING & PROTOCOLS

Serverless *FaaS, Lambda*
Running functions without managing servers. No host to patch, but function permissions and event sources become the security surface. CLOUD & INFRASTRUCTURE

Service account *Machine identity*
A non-human account used by an application or script. Typically over-permissioned, rarely rotated, never MFA-protected — a standing favourite for attackers. IDENTITY & ACCESS

Service mesh *Istio, Linkerd*
A layer that handles service-to-service traffic, giving mutual TLS, policy, and telemetry without changing application code. CLOUD & INFRASTRUCTURE

Session
A connection between two hosts that lasts long enough to carry a conversation. Stealing one is cheaper for an attacker than stealing a password. NETWORKING & PROTOCOLS

Session hijacking
Stealing a valid session cookie or token to become an already-authenticated user, skipping login and MFA entirely. Infostealer malware's main product. IDENTITY & ACCESS

Session key
A symmetric key used for a single connection or a short period, then discarded. Limits how much traffic one compromised key exposes. CRYPTOGRAPHY

SHA-1 *Secure Hash Algorithm 1*
A superseded hash function with demonstrated collisions. Anything still relying on it for signatures is a finding. CRYPTOGRAPHY

SHA-256 *Secure Hash Algorithm 256*
The workhorse hash for integrity checks, signatures, and blockchains. SHA-1 and MD5 are its broken predecessors and should never be used for security. CRYPTOGRAPHY

Shadow AI
Staff using AI tools without approval, often pasting confidential data into them. The current form of shadow IT, moving faster. AI & EMERGING TECH

Shadow IT
Tools and accounts staff adopt without approval. Not hostile, but invisible to security, unpatched, and outside the incident response plan. ATTACKS & EXPLOITATION

Shadow password file
The separate, restricted file where Unix stores password hashes, so ordinary users cannot read them out of the world-readable account file. IDENTITY & ACCESS

Share
A directory or printer made available to other machines over the network. ENDPOINTS & SYSTEMS

Shared responsibility model
The provider secures the cloud; you secure what you put in it. Nearly every cloud breach lands on the customer's side of that line. CLOUD & INFRASTRUCTURE

Shell
The command interpreter you type into — bash, zsh, PowerShell. Getting one on a target machine is the usual definition of a foothold. ENDPOINTS & SYSTEMS

Shift left
Moving security checks earlier into design and development. Genuinely valuable, and frequently reduced to adding a scanner to the build. APPLICATION SECURITY

Side-channel attack
Recovering secrets from physical or timing leakage rather than breaking the maths — power draw, execution time, cache behaviour, even sound. CRYPTOGRAPHY

SIEM *Security Information and Event Management*
Central log collection, correlation, and alerting. Only as good as the sources feeding it and the rules written on top. DEFENSE & OPERATIONS

Sigma
A vendor-neutral format for writing detection rules that can be converted to run on different SIEMs. The shared language for sharing detections. DEFENSE & OPERATIONS

Signals analysis
Deriving information indirectly from a signal a system emits that was never meant to carry it. CRYPTOGRAPHY

Signature (detection)
A distinctive pattern that identifies a specific tool or exploit in traffic or on disk. Precise, and useless against anything new. DEFENSE & OPERATIONS

Silk Road
The Tor-hosted drug marketplace taken down in 2013. The standing case study in dark web investigation: the site was anonymous, and the operator's early forum posts and cash-out were not. INTELLIGENCE & INVESTIGATIONS

Simple integrity property *No write up*
In the Biba integrity model, a user may not write data to a higher integrity level than their own. IDENTITY & ACCESS

Simple security property *No read up*
In Bell-LaPadula, a user may not read data classified higher than their own clearance. IDENTITY & ACCESS

SIM swapping
Convincing a mobile carrier to move a number to an attacker's SIM, capturing every SMS code. The reason SMS is the weakest second factor. ATTACKS & EXPLOITATION

S/Key
An early one-time password scheme that generates a chain of passwords by repeated hashing. The ancestor of modern OTP. CRYPTOGRAPHY

SLA / SLO *Service Level Agreement / Objective*
The availability you promise contractually, and the internal target you actually manage to. The objective should be stricter than the agreement. DEV & DELIVERY

Smartcard
A card with a chip that holds keys and performs cryptographic operations without releasing them. The basis of most government credentialing. IDENTITY & ACCESS

Smart contract
Code executing automatically on a blockchain. Immutable once deployed, which means bugs are permanent and expensive. AI & EMERGING TECH

Smishing
Phishing over SMS rather than email. Short messages strip away most of the cues people use to spot a fake. ATTACKS & EXPLOITATION

Smishing / vishing
Phishing by SMS and by voice call. Voice versions increasingly use cloned audio, and helpdesk vishing is a proven route past MFA. ATTACKS & EXPLOITATION

Smurf
An old amplification attack: ping a network's broadcast address with the victim's address forged as the source, and every host replies to the victim. NETWORKING & PROTOCOLS

SNI *Server Name Indication*
The field in a TLS handshake that names which site you want, sent before encryption starts. It leaks the hostname to anyone watching, which is what Encrypted Client Hello is meant to fix. NETWORKING & PROTOCOLS

Sniffer
A tool that reads traffic off a network interface. The same tool troubleshoots a network and harvests credentials from it. NETWORKING & PROTOCOLS

Sniffing *Passive wiretapping*
Reading network traffic you were not the intended recipient of. Passive, silent, and the reason unencrypted protocols are indefensible. NETWORKING & PROTOCOLS

SNMP *Simple Network Management Protocol*
The protocol for monitoring and configuring network devices. Old versions used a shared community string as the only password — often left as 'public'. NETWORKING & PROTOCOLS

SOAR *Security Orchestration, Automation and Response*
Automating repetitive response steps through playbooks — enrich, contain, notify — so analysts handle the judgement calls. DEFENSE & OPERATIONS

SOC *Security Operations Centre*
The team and tooling that monitor, triage, and respond to security events. In-house, outsourced, or a mix. DEFENSE & OPERATIONS

SOC 2 *Service Organization Control 2*
An audit report on a service provider's controls against trust criteria. Type I is a point in time; Type II covers a period and is the one to ask for. GOVERNANCE, RISK & COMPLIANCE

Social engineering
Manipulating people rather than systems — urgency, authority, helpfulness. It bypasses technical controls by using someone who already holds legitimate access. ATTACKS & EXPLOITATION

Socket
The combination of an IP address and a port that tells the network stack which application a data stream belongs to. NETWORKING & PROTOCOLS

Socket pair
The four values that uniquely name a connection: source address and port, destination address and port. It is how a host keeps thousands of connections apart. NETWORKING & PROTOCOLS

SOCKS *Socket Secure*
A generic proxy protocol that forwards connections of any kind rather than just web traffic. Widely used to route traffic through somewhere else, legitimately or not. NETWORKING & PROTOCOLS

Software
Programs and their associated data, stored in and executed by hardware, and changeable while running. ENDPOINTS & SYSTEMS

Source port
The temporary port a client picks for its end of a connection, usually a high number chosen at random. It changes with every connection. NETWORKING & PROTOCOLS

Southern District of New York *SDNY*
The federal prosecutorial district that handles a disproportionate share of US financial and white-collar cases, cyber fraud included. Where a case is charged shapes how it is investigated. INTELLIGENCE & INVESTIGATIONS

Spanning port *Port mirroring, SPAN*
A switch port configured to receive a copy of other ports' traffic. How monitoring and intrusion detection get to see the network. NETWORKING & PROTOCOLS

Spear phishing
Phishing tailored to one person using real details about their role, colleagues, or current projects. Much higher success rate, much lower volume. ATTACKS & EXPLOITATION

Special category data *Sensitive personal data*
Health, biometrics, ethnicity, religion, sexuality, politics, union membership. Higher legal protection and higher real-world harm if exposed. GOVERNANCE, RISK & COMPLIANCE

Spectre / Meltdown *Speculative execution attacks*
Flaws in how processors guess ahead, letting one process read memory it should not. Fixes cost real performance and the class keeps producing new variants. COMPUTE & HARDWARE

Split horizon
A routing rule that stops a router advertising a route back to the neighbour it learned it from. It prevents a common class of routing loop. NETWORKING & PROTOCOLS

Split key
A key divided into parts, none of which reveals anything alone. Used where no one person should be able to act by themselves. CRYPTOGRAPHY

Spoof
Posing as someone or something else to gain access — an address, a sender name, a caller ID. The general case behind spoofing of every kind. NETWORKING & PROTOCOLS

Spot / preemptible instance
Discounted cloud capacity that can be taken back at short notice. Fine for checkpointed training, unusable for anything that cannot be interrupted. COMPUTE & HARDWARE

Spyware
Software that covertly monitors activity — messages, location, microphone, camera. Includes commercial surveillance tools sold to states. MALWARE & THREAT ACTORS

SQL injection *SQLi*
Slipping SQL into input so the database runs it. Fixed properly by parameterised queries — never by filtering quotes. APPLICATION SECURITY

SSH *Secure Shell*
Encrypted remote command-line access. Key-based authentication should replace passwords, and unmanaged authorised_keys entries are a persistence route. ENDPOINTS & SYSTEMS

SSO *Single Sign-On*
One login granting access to many applications. It centralises control and logging — and centralises risk, since the identity provider becomes the crown jewel. IDENTITY & ACCESS

SSRF *Server-Side Request Forgery*
Making the server fetch a URL of the attacker's choosing, often reaching internal services or cloud metadata endpoints the internet cannot. APPLICATION SECURITY

Stack mashing
Using a buffer overflow to overwrite the stack so the program returns into attacker-supplied code. ATTACKS & EXPLOITATION

Staging area *Index*
Git's holding pen between your working files and a commit. `git add` puts changes there so you can commit some edits and not others. DEV & DELIVERY

Stalkerware
Consumer spyware marketed for monitoring partners, children, or staff. Legally grey, technically ordinary, and a serious safety issue in domestic abuse. MALWARE & THREAT ACTORS

Standard ACL *Cisco*
A router filter that makes its decision on source IP address alone. Blunt, but cheap to evaluate at line rate. NETWORKING & PROTOCOLS

Star property *No write down*
In Bell-LaPadula, a user may not write data down to a lower classification, which would leak it. IDENTITY & ACCESS

Stash
Parking uncommitted changes temporarily so you can switch context, then bringing them back. DEV & DELIVERY

Stateful inspection *Dynamic packet filtering*
Firewalling that tracks the state of each connection rather than judging every packet alone. It is how a firewall knows a reply is legitimate. NETWORKING & PROTOCOLS

State machine
A system that moves through a defined series of conditions, one at a time. Protocols and parsers are state machines, and their bugs are usually states nobody planned for. ENDPOINTS & SYSTEMS

Static host table *hosts file*
A plain text file mapping names to addresses, consulted before DNS. Editing it is a simple and often overlooked redirection technique. ENDPOINTS & SYSTEMS

Static routing
Routing table entries typed in by hand that never change on their own. Predictable and unforgiving when the network does change. NETWORKING & PROTOCOLS

Stealthing
The techniques malicious code uses to hide the fact that it is present on an infected system. MALWARE & THREAT ACTORS

Steganalysis
Detecting and defeating steganography — finding the hidden message rather than reading an encrypted one. CRYPTOGRAPHY

Steganography
Hiding a message inside something innocuous, such as an image, so nobody knows a message exists. Concealment rather than encryption — often used to smuggle payloads past filters. CRYPTOGRAPHY

Stimulus and response
In traffic analysis, the distinction between packets that start something and packets that answer. Unsolicited responses are a signal worth chasing. DEFENSE & OPERATIONS

Storage *SSD / NVMe / HDD*
Persistent storage. NVMe SSDs are dramatically faster than spinning disks, which matters when loading model weights or replaying logs. COMPUTE & HARDWARE

Store-and-forward
Switching where the whole packet is read and checked before being sent on. Slower than cut-through, and it does not forward corrupted frames. NETWORKING & PROTOCOLS

Stored vs reflected XSS
Stored XSS is saved server-side and hits every viewer; reflected XSS is echoed back from a crafted link and hits whoever clicks it. APPLICATION SECURITY

Straight-through cable
An ordinary patch cable with each pin wired to the same pin at the other end. NETWORKING & PROTOCOLS

Stream cipher
A cipher that encrypts data continuously, a bit or byte at a time, rather than in blocks. Fast, and unforgiving if a keystream is ever reused. CRYPTOGRAPHY

Strong star property
A stricter rule: a user may write only at their own level, neither up nor down. IDENTITY & ACCESS

Subnet
A slice of a larger network, carved out so that traffic inside it stays local and traffic leaving it has to pass a router. Written as a CIDR range like 10.0.1.0/24. NETWORKING & PROTOCOLS

Sub network *Subnet*
A separately identifiable slice of a bigger network, usually a building, a floor or a single LAN. NETWORKING & PROTOCOLS

Subpoena
A legal order compelling someone to produce records or testimony. In practice it gets subscriber and transactional detail — account records, IP addresses, connection logs — not the content of communications. INTELLIGENCE & INVESTIGATIONS

Subresource integrity *SRI*
A hash on a third-party script tag so the browser refuses it if the file changed. Cheap protection against a compromised CDN. APPLICATION SECURITY

Sudo / runas
Mechanisms for running a single command with elevated rights instead of working as an administrator all day. Also a valuable audit trail. ENDPOINTS & SYSTEMS

Supply chain attack
Compromising a supplier, library, or update channel to reach everyone downstream. One breach, many victims — SolarWinds and XZ Utils are the canonical cases. ATTACKS & EXPLOITATION

Switch
A device that learns which MAC address sits on which port and sends frames only where they need to go. It is why a modern LAN does not broadcast everything to everyone. NETWORKING & PROTOCOLS

Symbolic link *Symlink*
A file that points at another file. Where a program follows one without checking, an attacker can redirect it to a file they should not reach. ENDPOINTS & SYSTEMS

Symmetric encryption
One shared key both encrypts and decrypts. Fast, ideal for bulk data, but everyone who needs to read it needs the same secret — which is the hard part. CRYPTOGRAPHY

Symmetric key
One key used for both encryption and decryption. Fast, and it leaves you with the problem of getting the key to the other side. CRYPTOGRAPHY

Sync
Bringing two copies into agreement — usually a pull followed by a push, so local and remote match. In GUIs it is often one button doing both. DEV & DELIVERY

Synchronisation
The distinctive bit pattern network hardware watches for to know a frame is starting. NETWORKING & PROTOCOLS

SYN flood
A denial of service that opens half-finished TCP handshakes faster than the target can clear them, exhausting its connection table. NETWORKING & PROTOCOLS

Syslog
The long-standing Unix logging facility, and the protocol for shipping those logs elsewhere. Still the plumbing under most log pipelines. DEFENSE & OPERATIONS

Sysmon
A free Windows tool producing detailed process, network, and file telemetry. The cheapest meaningful upgrade to endpoint visibility. ENDPOINTS & SYSTEMS

System on a Chip *SoC — not to be confused with a Security Operations Centre*
CPU, GPU, memory controller, and often a neural engine on a single piece of silicon. What phones, Raspberry Pis and Apple laptops are built on. COMPUTE & HARDWARE

System prompt
Standing instructions set by the developer ahead of user input. Treat it as configuration, never as a secret — it leaks. AI & EMERGING TECH

System-specific policy
A policy written for one system or device, where general rules are not specific enough to act on. GOVERNANCE, RISK & COMPLIANCE

T

61 ENTRIES

T1 / T3
Traditional leased digital circuits of fixed capacity. Still a unit of thinking in telecoms, if rarely a purchase. NETWORKING & PROTOCOLS

Tabletop exercise
A discussion-based rehearsal of an incident scenario. Cheap, and reliably exposes decision-making and communication gaps. DEFENSE & OPERATIONS

Tag
A permanent name pinned to a specific commit, normally a release like v2.1.0. Unlike a branch, it does not move. DEV & DELIVERY

Takedown *Seizure notice*
Seizing the infrastructure behind a criminal service and, usually, replacing its front page with a law enforcement banner. Effective as disruption and as messaging; rarely permanent on its own. INTELLIGENCE & INVESTIGATIONS

Tamper
Deliberately altering a system's logic, data or control information so it does something it should not. ATTACKS & EXPLOITATION

TCP *Transmission Control Protocol*
The reliable transport: it sets up a connection, numbers every packet, and re-sends anything lost. Slower to start, but nothing arrives out of order. NETWORKING & PROTOCOLS

TCPDump
The standard command-line packet capture tool on Unix. Windump is the Windows equivalent. DEFENSE & OPERATIONS

TCP fingerprinting
Using odd combinations of TCP header flags to identify a remote operating system by how it responds. NETWORKING & PROTOCOLS

TCP full open scan
A port scan that completes the full three-way handshake on every port. Accurate, noisy, and reliably logged by the target. NETWORKING & PROTOCOLS

TCP half open scan *SYN scan*
A scan that sends a SYN and never finishes the handshake, judging the port by the reply. Faster and quieter than a full open scan. NETWORKING & PROTOCOLS

TCP/IP *Internet Protocol Suite*
The protocol family the internet runs on, named for its two central members. Also usable on a private network. NETWORKING & PROTOCOLS

TCP wrapper
An old but instructive control that decides whether to accept a connection to a service based on where it came from. DEFENSE & OPERATIONS

TDP *Thermal Design Power*
The heat a chip is expected to produce, in watts. It drives cooling, power supply sizing and, at scale, the electricity bill. COMPUTE & HARDWARE

Technical debt
Shortcuts taken to ship faster that cost more later. Sometimes a good trade — but only if someone writes down that it was taken. DEV & DELIVERY

Telemetry
The raw signals systems emit. Detection is limited by telemetry — you cannot alert on something nobody records. DEFENSE & OPERATIONS

Telnet
A remote login protocol that sends everything, passwords included, in the clear. Replaced by SSH, and still found on forgotten devices. NETWORKING & PROTOCOLS

Thermal throttling
Hardware slowing itself down to avoid overheating. The usual explanation when performance falls off partway through a long run. COMPUTE & HARDWARE

Third-party risk *TPRM / vendor risk*
Managing the risk suppliers introduce. You can outsource the processing, but not the accountability. GOVERNANCE, RISK & COMPLIANCE

Threat actor
The person or group behind an attack. Grouped by capability and motive rather than by the tools they happen to use. MALWARE & THREAT ACTORS

Threat assessment
Working out which kinds of threat an organisation is actually exposed to, before designing anything to stop them. GOVERNANCE, RISK & COMPLIANCE

Threat hunting
Proactively searching for intrusions that no alert fired on, driven by a hypothesis rather than a queue. DEFENSE & OPERATIONS

Threat intelligence *CTI*
Analysed information about who is attacking, how, and what to look for. Useful only when it changes a decision, not when it is a feed nobody reads. MALWARE & THREAT ACTORS

Threat modelling *STRIDE*
Working out systematically what could go wrong with a design before it is built. Cheapest security work there is, and the most often skipped. APPLICATION SECURITY

Threat vector
The route a threat takes to reach its target — email, a supplier, a remote service, a person. GOVERNANCE, RISK & COMPLIANCE

Threat / vulnerability / risk
A threat is who might hurt you, a vulnerability is the weakness they would use, and risk is the combination weighted by likelihood and impact. Vendors blur these constantly. ATTACKS & EXPLOITATION

Three-way handshake *SYN / SYN-ACK / ACK*
The three packets TCP exchanges to open a connection. Half-finished handshakes left open on purpose are the basis of the SYN flood attack. NETWORKING & PROTOCOLS

Throughput vs latency
Throughput is how much work finishes per second; latency is how long one request takes. Batching raises throughput and worsens latency, and you usually have to choose. COMPUTE & HARDWARE

Timeline analysis
Building an ordered sequence of events across sources to reconstruct an intrusion and find the initial access point. DEFENSE & OPERATIONS

Time to live *TTL*
A counter in a packet that drops by one at every hop and kills the packet at zero. It stops routing loops from running forever, and traceroute exploits it. NETWORKING & PROTOCOLS

Tiny fragment attack
Splitting a packet so small that the fields a filter checks land in the second fragment, letting the first slip past the rule. NETWORKING & PROTOCOLS

Title 18
The part of the US Code covering federal crimes, including the computer fraud and wiretap statutes that most cyber prosecutions are brought under. GOVERNANCE, RISK & COMPLIANCE

TLS *Transport Layer Security*
The protocol that encrypts and authenticates most internet traffic. SSL is its dead predecessor — people still say SSL, but they mean TLS. NETWORKING & PROTOCOLS

TLS handshake
The opening exchange where client and server agree a cipher, verify the certificate, and derive session keys before any real data moves. NETWORKING & PROTOCOLS

Token
The chunk of text a model processes, roughly a word fragment. The unit of both pricing and context limits. AI & EMERGING TECH

Token-based access control
Access defined by attaching a list of objects and privileges to each user — the mirror image of list-based control. IDENTITY & ACCESS

Token-based device *Hardware token*
A device that generates a changing code the user must supply to log in, proving they physically hold it. IDENTITY & ACCESS

Token binding / DPoP
Tying a token to the client that requested it, so a stolen token is useless elsewhere. The countermeasure to plain bearer tokens. IDENTITY & ACCESS

Token ring
A LAN design where a circulating token granted the right to transmit, avoiding collisions by design. Elegant, and beaten by cheap Ethernet. NETWORKING & PROTOCOLS

Tokens per second *tok/s*
The practical speed measure for language model inference. Time to first token matters for how responsive it feels; tokens per second for how fast it finishes. COMPUTE & HARDWARE

Tool use / function calling
Letting a model invoke external functions or APIs. Whatever the tool can do, a successful prompt injection can do. AI & EMERGING TECH

Topology
The shape of a network — bus, star, ring, mesh — physically or logically. Two networks can share a logical topology and look nothing alike in the racks. NETWORKING & PROTOCOLS

Top Secret *TS*
The US classification for information whose disclosure would be expected to cause exceptionally grave damage to national security. CLASSIFICATION & PERSONAL DATA

Tor *The Onion Router*
A network that routes traffic through several volunteer relays, each knowing only the previous and next hop, so no single point sees both who you are and where you are going. NETWORKING & PROTOCOLS

TOTP *Time-based One-Time Password*
The rotating six-digit code from an authenticator app. Far better than SMS, but still phishable, because the user can be tricked into typing it into a fake site. IDENTITY & ACCESS

TPM *Trusted Platform Module*
A small secure chip on a motherboard that stores keys and measures boot integrity. What full-disk encryption and secure boot lean on. CRYPTOGRAPHY

TPU / NPU *Tensor / Neural Processing Unit*
Chips designed specifically for neural network maths. Google's TPUs run in its cloud; NPUs now ship inside phones and laptops for on-device inference. COMPUTE & HARDWARE

Traceroute *tracert*
A tool that shows each hop a packet takes to a destination. It exposes the path, and often the internal structure of the network at the far end. NETWORKING & PROTOCOLS

Trade secret
Commercially valuable information that derives its value from being secret and that the holder takes reasonable steps to keep secret. The reasonable steps are a legal requirement, not just good practice. CLASSIFICATION & PERSONAL DATA

Training data
The corpus a model learns from. Its provenance, licensing, and bias become properties of the finished system. AI & EMERGING TECH

Training vs inference
Training builds the model and is enormously expensive but happens rarely; inference runs it and is cheap per call but happens constantly. Most lifetime cost ends up in inference. COMPUTE & HARDWARE

Triage
Rapidly deciding whether an alert is real and how urgent. The gatekeeping step between monitoring and incident response. DEFENSE & OPERATIONS

Triple DES *3DES*
DES applied three times to compensate for its short key. Slow, deprecated, and still lurking in payment and legacy systems. CRYPTOGRAPHY

Trojan
Malware disguised as something wanted — a cracked app, an installer, a document viewer. It relies on the user choosing to run it. MALWARE & THREAT ACTORS

True / false positive
A real detection versus a false alarm. False positive volume, not detection coverage, is what usually breaks a SOC. DEFENSE & OPERATIONS

Trunking
Carrying traffic for several VLANs over one link between switches. Misconfigured trunks are how attackers hop between VLANs. NETWORKING & PROTOCOLS

Trust
In systems terms, the relationship that decides what one machine or domain will let another's users do. IDENTITY & ACCESS

Trusted ports
Ports below 1024, which on Unix only a privileged account may bind. A weak assurance today, but it still shapes how services are started. NETWORKING & PROTOCOLS

TTPs *Tactics, Techniques, and Procedures*
How a group operates rather than what they used once. Far more durable than indicators, and the basis of ATT&CK-style detection. MALWARE & THREAT ACTORS

Tumbler *Mixer*
A service that pools and re-splits cryptocurrency to break the link between source and destination. Using one is itself a signal, and several operators have been prosecuted. INTELLIGENCE & INVESTIGATIONS

Tunnel
A link built by wrapping one protocol inside another so traffic can cross a network that would not normally carry it. VPNs, IPsec and GRE are all tunnels. NETWORKING & PROTOCOLS

Typosquatting
Registering near-miss domains or package names to catch typos. Used both for phishing and for poisoning software dependencies. ATTACKS & EXPLOITATION

U

19 ENTRIES

UAC *User Account Control*
Windows' prompt before elevated actions. A speed bump rather than a boundary — plenty of documented bypasses exist. ENDPOINTS & SYSTEMS

UDP *User Datagram Protocol*
Fire-and-forget transport with no handshake and no resends. Used where speed beats completeness — DNS, video, games — and popular with attackers for spoofing and amplification. NETWORKING & PROTOCOLS

UDP scan
Probing UDP ports to see which are open. Slow and unreliable, because silence can mean either an open port or a dropped packet. NETWORKING & PROTOCOLS

UEBA *User and Entity Behaviour Analytics*
Behavioural profiling of users and machines to spot compromised accounts and insiders acting out of character. DEFENSE & OPERATIONS

UEFI / BIOS *Firmware*
The low-level code that starts the hardware. Rarely patched, hard to inspect, and highly persistent when compromised. ENDPOINTS & SYSTEMS

Unclassified *U*
Government information with no classification level. It may still be controlled: CUI — controlled unclassified information — is unclassified but restricted. CLASSIFICATION & PERSONAL DATA

Undercover purchase *Test buy*
Buying from a marketplace vendor to establish what is being sold, from whom, and where it ships from. It converts an anonymous listing into physical evidence and a delivery address. INTELLIGENCE & INVESTIGATIONS

Unicast
Traffic from one host to one host. The ordinary case. NETWORKING & PROTOCOLS

United Nations (cyber norms) *UN*
The forum where states negotiate norms for behaviour in cyberspace. It produces recommendations, not enforcement, which is both its limit and the reason states will talk there. INTELLIGENCE & INVESTIGATIONS

Unit / integration test
Unit tests check one piece in isolation; integration tests check the pieces working together. You need both, and integration tests are the ones people skip. DEV & DELIVERY

Unix
The multi-user, multitasking operating system from Bell Labs in the early 1970s whose design underlies Linux, macOS and most servers. ENDPOINTS & SYSTEMS

Unprotected share
A share anyone can connect to. Still one of the most common ways ransomware moves through an organisation. ENDPOINTS & SYSTEMS

Upstream / downstream
Upstream is the project or service you depend on; downstream is whoever depends on you. Vulnerabilities travel downstream, fixes come from upstream. DEV & DELIVERY

URI *Uniform Resource Identifier*
The general term for names and addresses that identify something on the web. A URL is a URI that also says where to get it. ENDPOINTS & SYSTEMS

URL *Uniform Resource Locator*
The address of a resource: the protocol to use, then where the resource lives. The part users are asked to inspect and almost never do. ENDPOINTS & SYSTEMS

US Cyber Command *USCYBERCOM*
The US military command for cyber operations, defensive and offensive. Where CISA protects and the FBI investigates, this is the element that can act against an adversary. INTELLIGENCE & INVESTIGATIONS

Use-after-free
Using memory after it has been released, letting an attacker control what now sits there. A leading source of browser and kernel exploits. APPLICATION SECURITY

User space vs kernel space
The separation between ordinary programs and privileged system code. Crossing from one to the other is the goal of local privilege escalation. ENDPOINTS & SYSTEMS

US Secret Service *USSS*
Originally the investigators of counterfeit currency, now a principal US agency for financial cybercrime — payment card fraud, cryptocurrency laundering, digital financial investigations — alongside its protective mission. INTELLIGENCE & INVESTIGATIONS

V

14 ENTRIES

Vector database *Embedding store*
Storage for numeric representations of text so similar meaning can be found by proximity. The retrieval half of RAG, and it inherits the source's access rules only if you make it. AI & EMERGING TECH

Version control *Git, VCS*
A system that records every change to a codebase, who made it and why, and lets you go back. Git is the near-universal one; GitHub and GitLab are hosts for it. DEV & DELIVERY

Virtualisation
Running multiple isolated systems on one machine. The basis of cloud, and a safe place to detonate suspicious files. ENDPOINTS & SYSTEMS

Virtual machine *VM*
A simulated computer running on shared hardware, with its own operating system. Strong isolation, heavier than a container. CLOUD & INFRASTRUCTURE

Virus
Malicious code that attaches itself to a file or program and spreads when that host is run. Largely historical, but the word stuck to everything. MALWARE & THREAT ACTORS

Vishing *Voice phishing*
Phishing by phone call, including over VoIP. Now routinely paired with cloned voices. ATTACKS & EXPLOITATION

VLAN *Virtual LAN*
A logical network laid over shared switch hardware, so two ports on the same switch can be on separate networks. A control, but a soft one — VLAN hopping is a real attack. NETWORKING & PROTOCOLS

VLAN hopping
Escaping the VLAN you were put on to reach traffic on another, usually by abusing trunk negotiation or double-tagged frames. It is why VLANs are a segmentation convenience, not a security boundary. ATTACKS & EXPLOITATION

Volatile vs non-volatile storage
Volatile memory disappears when power is cut; disks survive. It sets the order of collection: capture memory first, then image the disk. INTELLIGENCE & INVESTIGATIONS

VPN *Virtual Private Network*
An encrypted tunnel that makes a remote device behave as if it were on the internal network. It moves the trust boundary — it does not remove it. NETWORKING & PROTOCOLS

VPN (investigative view)
An encrypted tunnel to a provider that then makes connections on the user's behalf. Whether it defeats an investigation depends entirely on what logs the provider keeps. INTELLIGENCE & INVESTIGATIONS

VRAM *Video / GPU memory*
Memory attached directly to a GPU. It is the hard limit on model size: if the weights do not fit in VRAM, the model will not run, however fast the chip is. COMPUTE & HARDWARE

Vulnerability management
Finding, prioritising, fixing, and verifying vulnerabilities as a continuous cycle. Prioritisation is the hard part, not scanning. DEFENSE & OPERATIONS

Vulnerability scanner
A tool that checks systems against a database of known flaws. Reports what might be vulnerable, not what is exploitable in your context. DEFENSE & OPERATIONS

W

20 ENTRIES

WAF *Web Application Firewall*
Filters HTTP requests against attack patterns. Buys time before a patch; it does not fix the underlying flaw. CLOUD & INFRASTRUCTURE

War chalking
Marking pavements to show where open wireless signals could be picked up. A period detail from the early Wi-Fi years. ATTACKS & EXPLOITATION

War dialing
Dialling ranges of telephone numbers to find modems answering. The ancestor of port scanning. ATTACKS & EXPLOITATION

War driving
Driving around looking for wireless networks that can be reached or joined. ATTACKS & EXPLOITATION

Watering hole
Compromising a site the intended victims already visit and waiting for them to arrive. No message to the target means nothing to flag as suspicious. ATTACKS & EXPLOITATION

Watermarking
Embedding a detectable signal in AI-generated output. Helpful at scale, and generally removable by anyone who wants to remove it. AI & EMERGING TECH

Webhook
A URL you register so another service can push events to you as they happen, instead of you polling. Verify the signature, or anyone can post to it. DEV & DELIVERY

Web of trust
Trust built by people signing each other's keys, rather than granted by a central authority. PGP's alternative to certificate authorities. CRYPTOGRAPHY

Web server
The software that answers HTTP requests for content. Also the process most often running as the entry point to an internal network. ENDPOINTS & SYSTEMS

Whaling
Spear phishing aimed at executives, whose approval authority and access make a single success unusually valuable. ATTACKS & EXPLOITATION

WHOIS *Who is — registration lookup*
The lookup service for who registered a domain or holds a block of addresses. Redaction has hollowed it out, but it is still an early stop in an investigation. NETWORKING & PROTOCOLS

Windowing
A windowing system shares a screen among several running applications, tracking where each window is and what state it is in. NETWORKING & PROTOCOLS

Wiper
Malware built purely to destroy data, sometimes disguised as ransomware. There is no key, because recovery was never the point. MALWARE & THREAT ACTORS

Wired Equivalent Privacy *WEP*
The original Wi-Fi encryption standard, broken since the early 2000s. Finding it in use is finding an open network. ENDPOINTS & SYSTEMS

WireGuard
A modern VPN protocol with a deliberately small codebase and a fixed set of modern ciphers. Faster and easier to audit than IPsec or OpenVPN. NETWORKING & PROTOCOLS

Wireless Application Protocol *WAP*
An early specification for getting internet services onto mobile phones, before phones could simply speak the web. ENDPOINTS & SYSTEMS

Wiretapping
Monitoring and recording data moving between two points in a communication system. Passive wiretapping listens; active wiretapping alters. NETWORKING & PROTOCOLS

Workload identity
Giving a running service a short-lived, automatically issued identity instead of a static key. The modern replacement for hard-coded credentials. IDENTITY & ACCESS

World Wide Web *WWW*
The global collection of hypermedia documents and services reached over HTTP. Not a synonym for the internet, though everyone uses it as one. ENDPOINTS & SYSTEMS

Worm
Malware that spreads by itself across a network with no user action. Why unpatched internet-facing services are treated as emergencies. MALWARE & THREAT ACTORS

X

3 ENTRIES

XDR *Extended Detection and Response*
Correlating endpoint telemetry with identity, email, and cloud signals in one place. Often just a vendor's bundle under a new name. ENDPOINTS & SYSTEMS

XSS *Cross-Site Scripting*
Injecting JavaScript that runs in another user's browser under your site's origin, letting an attacker read cookies or act as that user. APPLICATION SECURITY

XXE *XML External Entity*
Abusing XML parsers that resolve external references, allowing file reads or server-side requests. Fixed by disabling external entities. APPLICATION SECURITY

Y

1 ENTRY

YARA *Yet Another Ridiculous Acronym*
A pattern-matching language for identifying malware families by content. Widely used in threat hunting and malware triage. DEFENSE & OPERATIONS

Z

3 ENTRIES

Zero-day *0-day*
A vulnerability being exploited before a patch exists. Rare and expensive — most breaches still use flaws patched months earlier. ATTACKS & EXPLOITATION

Zero trust
Assume no network location is trusted; verify identity, device, and context on every request. A design principle, not a product, whatever a vendor tells you. IDENTITY & ACCESS

Zombie
A compromised machine taking orders remotely, usually as one of many in a botnet. Its owner almost never knows. MALWARE & THREAT ACTORS

Part two

THE DATABASE LIBRARY

105 open data sources and open-source tools, arranged by shelf.

SATELLITE & EARTH OBSERVATION

12 SOURCES

Copernicus Data Space Ecosystem

ESA / EUROPEAN COMMISSION · FREE

Free, full-archive Sentinel-1 (radar), Sentinel-2 (10 m optical), Sentinel-3 and Sentinel-5P imagery for the whole planet, updated every few days.

HOW TO CONNECT Register for a free account, then use the OData/STAC catalogue APIs to search and the S3-compatible endpoint to download. openEO and Sentinel Hub APIs sit on top for on-the-fly processing.

dataspace.copernicus.eu

NASA Earthdata

NASA · FREE

The front door to NASA's entire Earth science archive — MODIS, VIIRS, Landsat, GRACE, SMAP, atmospheric and ocean products.

HOW TO CONNECT Create a free Earthdata Login, then query the CMR (Common Metadata Repository) API or use the earthaccess Python library, which handles auth and streaming for you.

www.earthdata.nasa.gov

USGS EarthExplorer / Landsat

USGS · FREE

Fifty years of Landsat imagery plus aerial photography, elevation and declassified historical satellite data.

HOW TO CONNECT Free account, then the M2M (machine-to-machine) JSON API for scripted search and bulk download, or pull the same scenes as cloud-optimised GeoTIFFs from AWS Open Data.

earthexplorer.usgs.gov

Sentinel Hub

PLANET / SINERGISE · FREE TIER, PAID ABOVE IT

Processing API that renders satellite imagery on demand — pick a bounding box, date range and band maths, get a PNG or GeoTIFF back.

HOW TO CONNECT OAuth client credentials, then a POST to the Process API with an evalscript. WMS/WMTS endpoints let you drop it straight into Leaflet or QGIS.

www.sentinel-hub.com

Microsoft Planetary Computer

MICROSOFT · FREE

A large STAC catalogue of Earth observation data hosted on Azure, with a hosted JupyterHub for analysis next to the data.

HOW TO CONNECT Query the public STAC API, then sign asset URLs with the free token endpoint (or the planetary-computer Python package) before reading the COGs.

planetarycomputer.microsoft.com

AWS Open Data Registry

AMAZON WEB SERVICES · FREE TO READ

Hundreds of public datasets hosted free in S3 — Sentinel, Landsat, NOAA weather, OpenStreetMap extracts, genomics, census.

HOW TO CONNECT Most buckets are anonymously readable: point the AWS CLI or boto3 at them with --no-sign-request. Many also publish a STAC catalogue.

registry.opendata.aws

Google Earth Engine

GOOGLE · FREE FOR NON-COMMERCIAL

A planetary-scale analysis platform with a petabyte catalogue already ingested and ready to compute over.

HOW TO CONNECT Register a cloud project, then use the JavaScript Code Editor or the Python earthengine-api. Free for research, non-profit and education; commercial use is paid.

earthengine.google.com

Planet

PLANET LABS · FREE UNDER NICFI, OTHERWISE COMMERCIAL

Daily high-resolution commercial imagery. The NICFI programme releases tropical basemaps free for forest and land-use work.

HOW TO CONNECT Apply for NICFI access, then use the Planet Basemaps API or the XYZ tile endpoint directly in a web map.

www.planet.com/nicfi/

Maxar Open Data Program

MAXAR · FREE (NON-COMMERCIAL)

Very high-resolution imagery released free after major disasters and crises, licensed CC BY-NC.

HOW TO CONNECT Browse the event STAC catalogue and pull cloud-optimised GeoTIFFs directly over HTTP — no key required.

www.maxar.com/open-data

UNOSAT

UNITAR · FREE

Satellite-derived damage assessments, flood extents and displacement maps produced for UN operations.

HOW TO CONNECT Download analysis-ready GIS layers and PDF maps per activation; some layers are served as ArcGIS REST feature services you can consume live.

unosat.org

NASA FIRMS

NASA · FREE

Near-real-time active fire and thermal anomaly detections worldwide, within about three hours of satellite overpass.

HOW TO CONNECT Request a free MAP_KEY, then hit the CSV/GeoJSON area API by country or bounding box. WMS layers exist for direct map embedding.

firms.modaps.eosdis.nasa.gov

OpenAerialMap

HUMANITARIAN OPENSTREETMAP TEAM · FREE

Openly licensed drone and aerial imagery, much of it flown after disasters.

HOW TO CONNECT Search the open catalogue API for imagery footprints, then use the returned TMS tile URL straight in Leaflet or MapLibre.

openaerialmap.org

MAPS & GEOSPATIAL

15 SOURCES

OpenStreetMap

OSM FOUNDATION · FREE

The crowd-built map of the world — roads, buildings, rivers, clinics, shops — open-licensed under ODbL.

HOW TO CONNECT For live queries use the Overpass API with its own query language; for bulk use Geofabrik regional extracts. Never scrape the main tile server for production.

www.openstreetmap.org

Overpass Turbo

OSM COMMUNITY · FREE

A browser sandbox for writing and testing Overpass queries against OpenStreetMap before you put them in code.

HOW TO CONNECT Write the query, run it, export GeoJSON. The generated query string drops straight into a fetch() against an Overpass endpoint.

overpass-turbo.eu

Geofabrik Downloads

GEOFABRIK · FREE

Daily OpenStreetMap extracts cut by country and region, in PBF and shapefile.

HOW TO CONNECT Plain HTTP download by URL — trivially scriptable in a build step. Load PBF with osmium or osm2pgsql into PostGIS.

download.geofabrik.de

Overture Maps Foundation

LINUX FOUNDATION / META, MICROSOFT, AMAZON, TOMTOM · FREE

Open, standardised global map layers — places, buildings, transportation, administrative boundaries — released quarterly.

HOW TO CONNECT Data ships as GeoParquet on S3 and Azure. Query it in place with DuckDB's spatial extension, or use the overturemaps Python CLI.

overturemaps.org

Natural Earth

VOLUNTEER / NACIS · FREE

Small-scale cartographic base layers — coastlines, borders, rivers, populated places — in three tidy resolutions, public domain.

HOW TO CONNECT Download shapefiles or GeoJSON directly. Bundled inside most mapping libraries already, so often a one-line import.

www.naturalearthdata.com

GADM

UNIVERSITY OF CALIFORNIA, DAVIS · FREE (NON-COMMERCIAL)

Administrative boundaries for every country, down to district and ward level.

HOW TO CONNECT Download per-country GeoPackage or shapefile by URL. Free for academic and non-commercial use — check the licence for anything else.

gadm.org

geoBoundaries

WILLIAM & MARY GEOLAB · FREE

Open, CC BY licensed administrative boundaries for every country — the permissively-licensed alternative to GADM.

HOW TO CONNECT A simple REST API returns a download link per country and admin level; the GeoJSON is small enough to fetch client-side.

www.geoboundaries.org

MapLibre GL

MAPLIBRE / OPEN SOURCE · FREE / OPEN SOURCE

The open-source fork of Mapbox GL — fast vector map rendering in the browser and on mobile.

HOW TO CONNECT npm install maplibre-gl, point it at a style JSON and a vector tile source. No API key and no vendor account required.

maplibre.org

Leaflet

OPEN SOURCE · FREE / OPEN SOURCE

The small, dependable JavaScript library for raster tile maps and GeoJSON overlays.

HOW TO CONNECT One script tag or npm install, then L.map() and L.tileLayer() with any XYZ tile URL. Huge plugin ecosystem for clustering, heatmaps and drawing.

leafletjs.com

Protomaps

PROTOMAPS · FREE / OPEN SOURCE

A single-file map tile format (PMTiles) that serves an entire basemap from static hosting — no tile server at all.

HOW TO CONNECT Download or build a .pmtiles file, put it on S3 or GitHub Pages, and read it with the pmtiles JS library via HTTP range requests.

protomaps.com

Nominatim

OSM FOUNDATION · FREE (RATE-LIMITED)

Geocoding and reverse geocoding built on OpenStreetMap — address to coordinates and back.

HOW TO CONNECT The public endpoint allows one request per second with a valid User-Agent. For real volume, run the Docker image against your own extract.

nominatim.org

Pelias

OPEN SOURCE · FREE / OPEN SOURCE

A self-hostable geocoder that blends OpenStreetMap, OpenAddresses, Who's on First and Geonames into one search index.

HOW TO CONNECT Run the Docker Compose project for your region, then query its JSON API for search, autocomplete and reverse lookups.

pelias.io

GeoNames

GEONAMES · FREE

Eleven million place names with coordinates, population, elevation and alternate spellings in many languages.

HOW TO CONNECT Free account gives you a username to pass to the JSON web services; the full database is also downloadable as tab-separated dumps.

www.geonames.org

Copernicus DEM / SRTM

ESA / NASA · FREE

Global elevation models — 30 m Copernicus DEM and the older SRTM — for terrain, slope, viewshed and flood modelling.

HOW TO CONNECT Copernicus DEM tiles are on AWS Open Data as COGs; SRTM comes from NASA Earthdata or OpenTopography's API.

spacedata.copernicus.eu/collections/copernicus-digital-elevation-model

OpenTopography

NSF / UC SAN DIEGO · FREE

High-resolution topography, including lidar point clouds, plus hosted global DEMs.

HOW TO CONNECT Free API key, then the Global DEM REST API returns a GeoTIFF for a bounding box in a single call.

opentopography.org

CLIMATE & WEATHER

10 SOURCES

Copernicus Climate Data Store

ECMWF / EUROPEAN COMMISSION · FREE

ERA5 reanalysis, seasonal forecasts and climate projections — the standard source for historical hourly weather anywhere on Earth since 1940.

HOW TO CONNECT Register, accept the licence, then use the cdsapi Python client with your key in ~/.cdsapirc. Requests are queued, so plan for asynchronous retrieval.

cds.climate.copernicus.eu

Open-Meteo

OPEN-METEO · FREE (NON-COMMERCIAL)

Weather forecast, historical, air quality, marine and climate projection APIs with genuinely simple JSON.

HOW TO CONNECT No key needed for non-commercial use — a single GET with latitude, longitude and the variables you want. Ideal for prototypes and dashboards.

open-meteo.com

NOAA / NWS API

US NATIONAL WEATHER SERVICE · FREE

Official US forecasts, alerts, observations and radar as a public JSON API.

HOW TO CONNECT No key; just set a descriptive User-Agent header. GeoJSON responses drop straight into a map layer.

www.weather.gov/documentation/services-web-api

NOAA Climate Data Online

NOAA NCEI · FREE

Station-level historical temperature, precipitation and extremes going back over a century, worldwide.

HOW TO CONNECT Request a free token by email, then pass it as a header to the CDO v2 REST API. Bulk GHCN files are also on FTP and AWS.

www.ncei.noaa.gov/cdo-web/

IPCC WGI Interactive Atlas

IPCC · FREE

Regional climate change projections from the assessment reports, explorable by region, scenario and variable.

HOW TO CONNECT Explore in the browser and export figures and data; underlying CMIP6 data is downloadable from ESGF for analysis.

interactive-atlas.ipcc.ch

World Bank Climate Change Knowledge Portal

WORLD BANK · FREE

Country-level historical climate and projections packaged for planners rather than climate scientists.

HOW TO CONNECT A documented REST API returns country time series as JSON; the site also exports CSV per indicator.

climateknowledgeportal.worldbank.org

Global Forest Watch

WORLD RESOURCES INSTITUTE · FREE

Near-real-time deforestation alerts, tree cover loss and land use layers, updated weekly.

HOW TO CONNECT The GFW Data API serves query and tile endpoints; free API key via the developer portal. Alerts also come as XYZ raster tiles for direct map use.

www.globalforestwatch.org

Climate TRACE

CLIMATE TRACE COALITION · FREE

Independently estimated greenhouse gas emissions by asset and sector, built from satellite and sensor data rather than self-reporting.

HOW TO CONNECT Bulk CSV downloads per country and sector, plus a public REST API for assets and emissions.

climatetrace.org

Electricity Maps

ELECTRICITY MAPS · FREE TIER, PAID ABOVE

Live carbon intensity and power breakdown of electricity grids by zone.

HOW TO CONNECT Free tier API key covers one zone; commercial plans for more. The historical dataset is also published for download.

www.electricitymaps.com

Our World in Data

GLOBAL CHANGE DATA LAB / OXFORD · FREE

Cleaned, harmonised long-run datasets on climate, energy, health, poverty and more, with the charts to match.

HOW TO CONNECT Every chart has a download button, and the full data catalogue is on GitHub as tidy CSVs — no key, no auth.

ourworldindata.org

POPULATION & DEVELOPMENT

9 SOURCES

World Bank Open Data

WORLD BANK · FREE

Around 16,000 development indicators for every country — GDP, population, access to electricity, schooling, health.

HOW TO CONNECT A clean REST API: /v2/country/{iso}/indicator/{code}?format=json. No key. The wbdata and wbgapi Python packages wrap it.

data.worldbank.org

UN Data / SDG Indicators

UNITED NATIONS · FREE

Official Sustainable Development Goal indicator data by country, target and year.

HOW TO CONNECT The SDG API returns JSON by series and geo area; bulk downloads are available per goal.

unstats.un.org/sdgs/dataportal

WorldPop

UNIVERSITY OF SOUTHAMPTON · FREE

Gridded population estimates at 100 m resolution, plus age and sex structure, births and migration.

HOW TO CONNECT Download GeoTIFFs per country and year, or use the WorldPop REST API to request statistics for your own polygon.

www.worldpop.org

Humanitarian Data Exchange

UN OCHA · FREE

The main open repository for humanitarian data — 20,000+ datasets on displacement, needs, food security, admin boundaries.

HOW TO CONNECT It runs on CKAN, so the full CKAN API works for search and download. The hdx-python-api package handles pagination and resources.

data.humdata.org

IPUMS

UNIVERSITY OF MINNESOTA · FREE (REGISTRATION)

Harmonised census and survey microdata from over 100 countries, made comparable across time and place.

HOW TO CONNECT Free registration, define an extract in the web interface or via the IPUMS API, then download when it is built.

www.ipums.org

DHS Program

USAID · FREE (ACCESS REQUEST)

Demographic and Health Surveys — nationally representative household data on health, nutrition, gender and mortality.

HOW TO CONNECT Request dataset access per country with a stated research purpose; the DHS API serves indicator data as JSON without that step.

dhsprogram.com

GHSL — Global Human Settlement Layer

EUROPEAN COMMISSION JRC · FREE

Global built-up surface, population grids and settlement classification derived from satellite imagery, back to 1975.

HOW TO CONNECT Direct download of GeoTIFF tiles by epoch and resolution; also available as WMS layers for quick map use.

human-settlement.emergency.copernicus.eu

Eurostat

EUROPEAN COMMISSION · FREE

Official statistics for the EU and member states — economy, population, environment, transport, at NUTS region level.

HOW TO CONNECT The Statistics API returns JSON-stat by dataset code; the eurostat Python and R packages make it a one-liner.

ec.europa.eu/eurostat

data.gov / data.europa.eu

US GOVERNMENT / EUROPEAN COMMISSION · FREE

National open data portals aggregating hundreds of thousands of government datasets.

HOW TO CONNECT Both run catalogue APIs (CKAN-style and SPARQL respectively) so you can search programmatically before downloading.

data.europa.eu

CONFLICT, RIGHTS & HUMANITARIAN

9 SOURCES

ACLED

ARMED CONFLICT LOCATION & EVENT DATA PROJECT · FREE FOR RESEARCH

Coded records of political violence and protest events worldwide — date, location, actors, fatalities — updated weekly.

HOW TO CONNECT Register for a free access key, then query the REST API by country, date range and event type. Free for academic and non-profit use.

acleddata.com

UCDP

UPPSALA UNIVERSITY · FREE

The longest-running armed conflict dataset, with georeferenced events back to 1989 and conflict-year data to 1946.

HOW TO CONNECT An open REST API returns JSON per dataset version; full CSV and RData downloads need no registration at all.

ucdp.uu.se

ReliefWeb

UN OCHA · FREE

Situation reports, appeals, maps and job postings across every active humanitarian emergency.

HOW TO CONNECT A well-documented public API supports full-text search and filtering by country, disaster and source. No key; just an appname parameter.

reliefweb.int

IDMC

INTERNAL DISPLACEMENT MONITORING CENTRE · FREE

Global estimates of people internally displaced by conflict and disaster, by country and year.

HOW TO CONNECT The Global Internal Displacement Database offers CSV export and a public API for displacement figures.

www.internal-displacement.org

UNHCR Refugee Data Finder

UNHCR · FREE

Official refugee, asylum seeker and stateless population statistics by country of origin and asylum, back to 1951.

HOW TO CONNECT A public REST API serves population and solutions data as JSON; the refugees R package wraps it.

www.unhcr.org/refugee-statistics/

IOM Displacement Tracking Matrix

INTERNATIONAL ORGANIZATION FOR MIGRATION · FREE

Field-collected data on displaced populations — locations, numbers, needs — at site and admin level.

HOW TO CONNECT A public API serves admin-level datasets by country and round; bulk downloads available per operation.

dtm.iom.int

Bellingcat Online Investigation Toolkit

BELLINGCAT · FREE

A curated, maintained index of open-source investigation tools — geolocation, satellite, archives, transport tracking.

HOW TO CONNECT Browse by category; most entries are free web tools or open-source repos you can run yourself.

bellingcat.gitbook.io/toolkit

OpenSanctions

OPENSANCTIONS · FREE (NON-COMMERCIAL)

Consolidated sanctions lists, politically exposed persons and watchlists from hundreds of sources, as structured entity data.

HOW TO CONNECT Bulk JSON and CSV downloads are free under CC BY-NC; a hosted matching API and commercial licence exist for business use.

www.opensanctions.org

Forensic Architecture

GOLDSMITHS, UNIVERSITY OF LONDON · FREE / OPEN SOURCE

Investigations reconstructing human rights incidents from open sources, plus open-source tooling they build to do it.

HOW TO CONNECT Methods and some tools are published openly on GitHub — notably Timemap for building situated event timelines.

forensic-architecture.org

ENVIRONMENT & BIODIVERSITY

8 SOURCES

GBIF

GLOBAL BIODIVERSITY INFORMATION FACILITY · FREE

Over two billion species occurrence records contributed by museums, researchers and citizen scientists.

HOW TO CONNECT An open REST API for search and a download API for large extracts (free account needed for the latter). pygbif and rgbif wrap both.

www.gbif.org

IUCN Red List

IUCN · FREE (TOKEN)

Extinction risk assessments and range data for over 150,000 species.

HOW TO CONNECT Request a free API token, then query by species, country or category. Spatial range polygons are a separate download request.

www.iucnredlist.org

Protected Planet / WDPA

UNEP-WCMC & IUCN · FREE

The World Database on Protected Areas — boundaries and attributes for every designated protected area on Earth.

HOW TO CONNECT Free API token for the REST API, or download monthly shapefile and GeoDatabase releases by country.

www.protectedplanet.net

OpenAQ

OPENAQ · FREE

Aggregated air quality measurements from government and research monitoring stations worldwide, harmonised into one schema.

HOW TO CONNECT Free API key, then query measurements by location, parameter and date. The full archive is also mirrored on AWS Open Data.

openaq.org

Global Fishing Watch

GLOBAL FISHING WATCH · FREE FOR NON-COMMERCIAL

Vessel activity and apparent fishing effort derived from AIS tracking, plus port visits and encounters at sea.

HOW TO CONNECT Register for an API token, then use the vessels, events and 4Wings tile APIs. Map tiles can be layered directly in MapLibre.

globalfishingwatch.org

Copernicus Marine Service

MERCATOR OCEAN / EU · FREE

Ocean physics and biogeochemistry — sea surface temperature, currents, sea level, chlorophyll — as analysis and forecast products.

HOW TO CONNECT Free account, then the copernicusmarine Python toolbox to subset and download NetCDF, or open datasets lazily over the ARCO/Zarr endpoints.

marine.copernicus.eu

Global Flood Monitor / GloFAS

EUROPEAN COMMISSION JRC · FREE

Global flood forecasting and monitoring, including river discharge forecasts and rapid flood mapping.

HOW TO CONNECT Forecast data is distributed through the Climate Data Store API; flood extent layers come as WMS and downloadable rasters.

global-flood.emergency.copernicus.eu

USGS Earthquake Hazards

USGS · FREE

Real-time global earthquake catalogue, shakemaps and hazard models.

HOW TO CONNECT The FDSN event API returns GeoJSON with no key; there are also live GeoJSON feeds updated every minute for direct map consumption.

earthquake.usgs.gov

HEALTH

5 SOURCES

WHO Global Health Observatory

WORLD HEALTH ORGANIZATION · FREE

Official global health statistics — mortality, disease burden, immunisation, health systems — by country and year.

HOW TO CONNECT The GHO OData API returns JSON by indicator code with no authentication. Athena API serves the same data in XML/CSV.

www.who.int/data/gho

IHME Global Health Data Exchange

INSTITUTE FOR HEALTH METRICS AND EVALUATION · FREE

Global Burden of Disease results — cause-specific mortality and disability for every country, age and sex, over decades.

HOW TO CONNECT Use the GBD Results Tool to build a query and export CSV; a results API is available for registered users.

ghdx.healthdata.org

HealthSites.io

HEALTHSITES / OSM COMMUNITY · FREE

An open, validated global registry of health facility locations built on OpenStreetMap.

HOW TO CONNECT Free API key, then a REST API returns facilities as GeoJSON by country or bounding box.

healthsites.io

OpenFDA

US FOOD AND DRUG ADMINISTRATION · FREE

Drug adverse events, recalls, labelling and device reports as queryable open data.

HOW TO CONNECT Public JSON API with no key for light use; a free key raises the rate limit. Elasticsearch-style query syntax.

open.fda.gov

DHIS2

UNIVERSITY OF OSLO · FREE / OPEN SOURCE

The open-source health information platform used as the national system in over 80 countries.

HOW TO CONNECT Self-host or use the demo server; a comprehensive REST API covers data values, metadata and analytics for integration.

dhis2.org

ECONOMY, TRADE & CORPORATE

7 SOURCES

UN Comtrade

UNITED NATIONS · FREE TIER

Official bilateral trade statistics — who exports what to whom, by commodity code and year.

HOW TO CONNECT Free API key from the developer portal, then query by reporter, partner, period and HS code. Rate limits are tight on the free tier.

comtrade.un.org

OpenCorporates

OPENCORPORATES · FREE TIER, LICENSED ABOVE

The largest open database of companies — legal entities, officers and filings from company registers worldwide.

HOW TO CONNECT REST API with a free key for public-interest and non-commercial use; bulk data under licence for commercial work.

opencorporates.com

GLEIF

GLOBAL LEGAL ENTITY IDENTIFIER FOUNDATION · FREE

The authoritative register of Legal Entity Identifiers, including parent and child ownership relationships.

HOW TO CONNECT A fully open REST API and daily bulk files — no key, no licence fee, CC0 licensed.

www.gleif.org

Open Ownership

OPEN OWNERSHIP · FREE

Beneficial ownership data — who ultimately controls companies — in a standard data format across jurisdictions.

HOW TO CONNECT Bulk downloads in the Beneficial Ownership Data Standard JSON; a register API for programmatic lookup.

www.openownership.org

Open Contracting Data Standard

OPEN CONTRACTING PARTNERSHIP · FREE

A common schema for public procurement data, used by dozens of national and city contracting portals.

HOW TO CONNECT Publishers expose OCDS releases as JSON APIs or bulk files; Kingfisher tooling collects and normalises them for analysis.

standard.open-contracting.org

IMF Data

INTERNATIONAL MONETARY FUND · FREE

Macroeconomic and financial statistics — balance of payments, government finance, exchange rates, WEO projections.

HOW TO CONNECT An SDMX JSON REST API by dataset and series key, no authentication required.

data.imf.org

OECD Data Explorer

OECD · FREE

Comparable statistics across member and partner countries — labour, education, tax, environment, innovation.

HOW TO CONNECT SDMX REST API returning JSON or CSV; the OECD R and Python packages handle the query syntax.

data-explorer.oecd.org

SECURITY & THREAT DATA

10 SOURCES

NVD

NIST · FREE

The US National Vulnerability Database — CVE records enriched with CVSS scores, affected product identifiers and references.

HOW TO CONNECT CVE API 2.0 returns JSON; request a free API key to lift the rate limit substantially. Full JSON feeds are downloadable for offline use.

nvd.nist.gov

CISA KEV Catalog

CISA · FREE

Vulnerabilities confirmed to be exploited in the wild — the single best free patch-prioritisation list.

HOW TO CONNECT One JSON or CSV file at a stable URL, updated as entries are added. No key, trivially automatable.

www.cisa.gov/known-exploited-vulnerabilities-catalog

OSV

GOOGLE / OPEN SOURCE SECURITY FOUNDATION · FREE

Vulnerability data for open-source packages, keyed precisely to affected versions across every major ecosystem.

HOW TO CONNECT A free REST API takes a package name and version and returns matching advisories. osv-scanner scans a lockfile or SBOM directly.

osv.dev

MITRE ATT&CK

MITRE · FREE

The reference catalogue of real-world adversary tactics and techniques, with groups, software and mitigations mapped to each.

HOW TO CONNECT The full knowledge base is published as STIX 2.1 JSON on GitHub; the mitreattack-python library loads and queries it locally.

attack.mitre.org

AlienVault OTX

LEVELBLUE · FREE

A community threat intelligence exchange — indicators grouped into pulses by contributors.

HOW TO CONNECT Free account gives an API key; the DirectConnect API pulls subscribed pulses and indicators as JSON.

otx.alienvault.com

abuse.ch

ABUSE.CH / SPAMHAUS · FREE

Feeds of malware samples, botnet C2 servers, malicious URLs and SSL fingerprints — MalwareBazaar, ThreatFox, URLhaus.

HOW TO CONNECT Free API key per service, then simple POST queries returning JSON. Plain-text and CSV blocklists are also published for direct ingestion.

abuse.ch

Shodan

SHODAN · PAID, ACADEMIC ACCESS AVAILABLE

A search engine for internet-connected devices and exposed services, with banners, certificates and known vulnerabilities.

HOW TO CONNECT API key from a paid or academic account; the shodan Python library covers search, host lookup and streaming.

www.shodan.io

Have I Been Pwned

TROY HUNT · MIXED

Breach exposure lookup for email addresses and domains, plus a password-compromise check.

HOW TO CONNECT The Pwned Passwords range API is free and anonymous via k-anonymity; breach search by email needs a paid key.

haveibeenpwned.com

Censys Search

CENSYS · FREE TIER, PAID ABOVE

Continuously scanned inventory of internet hosts and certificates — useful for attack surface discovery.

HOW TO CONNECT Free tier API credentials allow a modest query volume; the REST API and Python client support structured host and certificate search.

search.censys.io

CIS Benchmarks

CENTER FOR INTERNET SECURITY · FREE (PDFS)

Consensus secure configuration baselines for operating systems, cloud platforms, databases and browsers.

HOW TO CONNECT Free PDF download after registration; automated assessment content and hardened images are membership or paid.

www.cisecurity.org/cis-benchmarks

GEOSPATIAL TOOLING

10 SOURCES

QGIS

OSGEO · FREE / OPEN SOURCE

The full open-source desktop GIS — analysis, cartography, georeferencing, and a large plugin ecosystem.

HOW TO CONNECT Install and open. Connects directly to PostGIS, WMS/WFS services and cloud-optimised GeoTIFFs over HTTP; scriptable in Python via PyQGIS.

qgis.org

GDAL / OGR

OSGEO · FREE / OPEN SOURCE

The translation layer underneath almost every geospatial tool — reads and writes several hundred raster and vector formats.

HOW TO CONNECT Command line (gdal_translate, ogr2ogr) or bindings in Python, R and Node. The /vsicurl/ prefix reads remote files without downloading them.

gdal.org

PostGIS

OSGEO · FREE / OPEN SOURCE

Spatial extension for PostgreSQL — geometry types, spatial indexes and hundreds of analysis functions in SQL.

HOW TO CONNECT CREATE EXTENSION postgis on any Postgres instance, then load data with ogr2ogr or shp2pgsql.

postgis.net

STAC

STAC COMMUNITY · FREE / OPEN STANDARD

SpatioTemporal Asset Catalog — the common JSON standard for describing and searching satellite imagery archives.

HOW TO CONNECT Learning one STAC API means you can query Copernicus, Planetary Computer, Earth Search and dozens more the same way. Use pystac-client.

stacspec.org

Cloud-Optimised GeoTIFF

COG COMMUNITY · FREE / OPEN STANDARD

A GeoTIFF layout that lets clients read just the tiles they need over HTTP range requests, with no server-side software.

HOW TO CONNECT Serve a COG from static hosting and read windows of it with rasterio or GDAL — the key to cheap, serverless imagery pipelines.

www.cogeo.org

Rasterio & Shapely

OPEN SOURCE · FREE / OPEN SOURCE

The Python workhorses for reading raster data and manipulating vector geometry respectively.

HOW TO CONNECT pip install rasterio shapely geopandas. GeoPandas ties them together with a familiar DataFrame interface.

rasterio.readthedocs.io

Titiler

DEVELOPMENT SEED · FREE / OPEN SOURCE

A dynamic tile server that turns any cloud-optimised GeoTIFF or STAC item into XYZ map tiles on the fly.

HOW TO CONNECT Run the Docker image or deploy to Lambda, then request /cog/tiles/{z}/{x}/{y} with a url parameter pointing at your raster.

developmentseed.org/titiler/

Kepler.gl / deck.gl

OPENJS FOUNDATION / UBER · FREE / OPEN SOURCE

WebGL layers for rendering very large geospatial datasets in the browser — millions of points, arcs, hexbins and trips.

HOW TO CONNECT npm install deck.gl and compose layers over a MapLibre basemap. Kepler.gl is the no-code application built on top of it.

deck.gl

DuckDB Spatial

DUCKDB FOUNDATION · FREE / OPEN SOURCE

An in-process analytical database that queries GeoParquet, GeoJSON and shapefiles directly, including files on S3.

HOW TO CONNECT INSTALL spatial; LOAD spatial; then query remote Parquet with SQL. The fastest route into Overture data with no infrastructure.

duckdb.org/docs/extensions/spatial

OpenLayers

OSGEO · FREE / OPEN SOURCE

A mature JavaScript mapping library with unusually strong support for OGC services, projections and raster analysis.

HOW TO CONNECT npm install ol. Better than Leaflet when you need WMTS, WFS, reprojection or non-Mercator coordinate systems.

openlayers.org

COMMUNITIES & PROGRAMMES

10 SOURCES

Development Seed Community

DEVELOPMENT SEED · FREE

The open-source geospatial community around Development Seed — the team behind STAC tooling, Titiler, eoAPI and much NASA and World Bank open data infrastructure.

HOW TO CONNECT Follow their open repositories on GitHub, join the community calls and Slack, and reuse their STAC and tiling stacks directly in your own projects.

developmentseed.org/community/

Humanitarian OpenStreetMap Team

HOT · FREE

Coordinates volunteer mapping of unmapped, vulnerable places, and builds the open tooling to do it.

HOW TO CONNECT Map through the Tasking Manager, or use their open tools — the Export Tool for custom OSM extracts and OpenAerialMap for imagery.

www.hotosm.org

Open Data Kit / KoboToolbox

ODK / KOBO INC. · FREE TIER

Offline-first mobile data collection for field research and humanitarian assessment, used across the aid sector.

HOW TO CONNECT Free hosted server for humanitarian users, or self-host. A REST API exposes submissions as JSON, CSV or GeoJSON for downstream pipelines.

www.kobotoolbox.org

OpenStreetMap Foundation community

OSMF · FREE

The forum where OSM tagging, imports and local mapping conventions are actually decided.

HOW TO CONNECT Read before importing anything at scale — imports without community agreement get reverted.

community.openstreetmap.org

OSGeo

OPEN SOURCE GEOSPATIAL FOUNDATION · FREE

The umbrella foundation behind QGIS, GDAL, PostGIS, GeoServer and much of the open geospatial stack.

HOW TO CONNECT Project directories, the OSGeoLive bootable distribution with everything preinstalled, and local chapters worldwide.

www.osgeo.org

Colophon

Radiant Earth / Source Cooperative

RADIANT EARTH · FREE

A publishing platform for open geospatial data, hosting large public datasets with permanent, citable access.

HOW TO CONNECT Browse repositories and read data directly from S3-compatible endpoints; many are STAC-catalogued.

source.coop

Open Knowledge Foundation

OKFN · FREE

Long-running advocates for open data, and stewards of CKAN, Frictionless Data and the Open Definition.

HOW TO CONNECT CKAN powers many national data portals, so learning its API unlocks a great many catalogues at once.

okfn.org

Datasette

SIMON WILLISON · FREE / OPEN SOURCE

A tool for publishing any SQLite database as a browsable, queryable website with a JSON API for free.

HOW TO CONNECT pip install datasette, point it at a .db file, deploy anywhere. The fastest way to turn a CSV into a public API.

datasette.io

OpenSSF

OPEN SOURCE SECURITY FOUNDATION · FREE

The cross-industry body working on open-source supply chain security — Scorecard, Sigstore, SLSA, OSV.

HOW TO CONNECT Run Scorecard against your own repository for an immediate baseline, and use Sigstore to sign releases without managing keys.

openssf.org

Zenodo

CERN · FREE

Open repository for research data and software, issuing a permanent DOI for anything you deposit.

HOW TO CONNECT A REST API supports programmatic deposit; connect a GitHub repo and every release is archived and given a DOI automatically.

zenodo.org

ABOUT THIS EDITION

Compiled by the Ethical Tech CoLab from the Cyber Dictionary and Library, a searchable web tool published at ethical-tech-colab.github.io/cyber-dictionary. The entries in this book and the entries in that tool come from the same two files in the same repository; this edition is typeset from them rather than rewritten, so the two cannot drift apart in wording.

Definitions are written to be read cold, by someone who does not yet have the surrounding vocabulary. That is a deliberate constraint and it costs precision: where a term has a formal standards definition, this book gives the working one instead, and says what the term is for rather than exactly what it denotes.

Source and citation: github.com/Ethical-Tech-CoLab/cyber-dictionary