1000+ Cybersecurity Words

Every term with a plain-word twin and a one-line meaning

Grouped by topic • Easy English • Made for learners and creators

How to read each row

TERM	ALSO CALLED	SIMPLE MEANING
the real word	an easy twin word	one plain line

Note: most security words have no true synonym. So the middle column is not a fake synonym — it is the everyday phrase people actually use, or the full form of the short name. That teaches the right idea, not a wrong one.

CORE CONCEPTS

#	TERM	ALSO CALLED	SIMPLE MEANING
1	**Cybersecurity**	*Information security, InfoSec*	Protecting computers, networks and data from theft or damage.
2	**CIA Triad**	*Security triangle*	The 3 core goals: keep data secret, correct, and available.
3	**Confidentiality**	*Secrecy*	Only allowed people can see the data.
4	**Integrity**	*Trustworthiness*	Data is correct and not secretly changed.
5	**Availability**	*Uptime*	Systems and data work when needed.
6	**Authentication**	*Identity check*	Proving you are who you claim to be.
7	**Authorization**	*Permission check*	Deciding what an identified user is allowed to do.
8	**Accounting**	*Auditing*	Recording what each user did.
9	**Non-repudiation**	*Undeniable proof*	You can't deny you did an action.
10	**Vulnerability**	*Weakness, hole*	A flaw an attacker can misuse.
11	**Threat**	*Danger*	Anything that could cause harm.
12	**Risk**	*Exposure*	Chance of harm = threat meeting a weakness.
13	**Exploit**	*Attack code*	A trick or code that uses a weakness.
14	**Attack**	*Intrusion attempt*	An action meant to break security.
15	**Attack surface**	*Exposed area*	All the ways an attacker could get in.
16	**Attack vector**	*Entry path*	The specific route an attacker uses.
17	**Payload**	*Harmful part*	The part of an attack that does the damage.
18	**Threat actor**	*Attacker, adversary*	The person or group behind an attack.
19	**Asset**	*Valuable item*	Anything worth protecting (data, servers, people).
20	**Countermeasure**	*Control, safeguard*	Something that reduces risk.
21	**Security control**	*Protection measure*	A rule or tool that lowers risk.
22	**Mitigation**	*Reduction*	Steps that lessen the impact of a threat.
23	**Remediation**	*Fix*	Fully removing or repairing a weakness.
24	**Hardening**	*Locking down*	Removing weak settings to make a system tougher.
25	**Baseline**	*Standard config*	The known-good settings to compare against.
26	**Defense in depth**	*Layered security*	Many layers of protection, not just one.
27	**Least privilege**	*Minimum access*	Give only the access truly needed.
28	**Zero trust**	*Never trust, always verify*	Trust nothing by default; check every request.
29	**Separation of duties**	*Split control*	No single person controls a whole risky task.
30	**Fail-safe**	*Safe default*	On failure, the system locks instead of opening.
31	**Air gap**	*Physical isolation*	A machine with no network connection at all.
32	**Blast radius**	*Damage spread*	How far harm reaches if one part is breached.
33	**Security posture**	*Overall strength*	How well protected an organization is right now.
34	**Threat landscape**	*Danger map*	The full picture of current threats.
35	**Exposure**	*Openness*	A weakness that is reachable by attackers.
36	**Compromise**	*Breach*	When a system falls under attacker control.
37	**Breach**	*Data leak*	Unauthorized access to protected data.
38	**Incident**	*Security event*	Any event that harms or threatens security.
39	**Event**	*Log entry*	Any recorded system activity.
40	**Indicator of Compromise**	*IOC, clue*	Evidence that a breach happened (e.g. bad IP).
41	**Indicator of Attack**	*IOA*	Signs an attack is in progress.
42	**Kill chain**	*Attack stages*	The step-by-step path of a full attack.
43	**MITRE ATT&CK;**	*Attack playbook*	A public library of attacker techniques.
44	**TTP**	*Attacker behavior*	Tactics, Techniques and Procedures of attackers.
45	**Root cause**	*Origin*	The true underlying reason a problem happened.

#	TERM	ALSO CALLED	SIMPLE MEANING
46	**Residual risk**	*Leftover risk*	Risk that remains after controls are applied.
47	**Acceptable risk**	*Tolerated risk*	Risk small enough to live with.
48	**Security by design**	*Built-in security*	Adding security from the start, not later.
49	**Security by obscurity**	*Hiding as defense*	Relying on secrecy alone (weak, discouraged).
50	**Threat model**	*Risk map*	A plan of what could go wrong and how.

ATTACKS & THREATS

#	TERM	ALSO CALLED	SIMPLE MEANING
51	**Phishing**	*Bait email*	Fake messages that trick you into giving secrets.
52	**Spear phishing**	*Targeted phishing*	Phishing aimed at one specific person.
53	**Whaling**	*Executive phishing*	Phishing aimed at bosses or VIPs.
54	**Vishing**	*Voice phishing*	Phishing done over phone calls.
55	**Smishing**	*SMS phishing*	Phishing done through text messages.
56	**Pharming**	*Redirect attack*	Sending users to fake sites secretly.
57	**Social engineering**	*Human hacking*	Fooling people instead of machines.
58	**Pretexting**	*Fake story*	Inventing a lie to gain trust and info.
59	**Baiting**	*Lure trap*	Leaving tempting bait like a USB stick.
60	**Quid pro quo**	*Fake help*	Offering a favor to steal access.
61	**Tailgating**	*Piggybacking*	Sneaking through a door behind someone.
62	**Impersonation**	*Pretending*	Acting as someone you are not.
63	**Business Email Compromise**	*BEC, CEO fraud*	Faking a boss's email to steal money.
64	**Brute force**	*Guess-all*	Trying every password until one works.
65	**Dictionary attack**	*Wordlist attack*	Trying common words as passwords.
66	**Credential stuffing**	*Reused-password attack*	Using leaked passwords on other sites.
67	**Password spraying**	*Slow guessing*	Trying one common password on many accounts.
68	**Rainbow table**	*Precomputed hashes*	A lookup table to crack hashed passwords fast.
69	**Man-in-the-Middle**	*MITM, eavesdropper*	Secretly sitting between two parties.
70	**On-path attack**	*MITM*	Newer name for man-in-the-middle.
71	**Replay attack**	*Repeat trick*	Reusing captured data to fool a system.
72	**Session hijacking**	*Session theft*	Stealing a logged-in session token.
73	**Session fixation**	*Forced session*	Tricking a user into a known session ID.
74	**Denial of Service**	*DoS*	Flooding a system so it stops working.
75	**DDoS**	*Distributed flood*	A DoS from many machines at once.
76	**Amplification attack**	*Reflection flood*	Small requests that trigger huge replies.
77	**Botnet**	*Zombie army*	A network of hijacked machines.
78	**Zero-day**	*Unknown flaw*	A weakness no fix exists for yet.
79	**Supply chain attack**	*Vendor attack*	Hacking a trusted supplier to reach victims.
80	**Watering hole**	*Trap site*	Infecting a site the target often visits.
81	**Drive-by download**	*Silent infection*	Getting malware just by visiting a page.
82	**Clickjacking**	*UI trick*	Hiding buttons so clicks do hidden actions.
83	**Typosquatting**	*Fake-domain trap*	Registering misspelled domains to catch typos.
84	**Domain hijacking**	*Domain theft*	Stealing control of a domain name.
85	**DNS spoofing**	*DNS poisoning*	Feeding fake DNS answers to redirect users.
86	**ARP spoofing**	*ARP poisoning*	Faking network addresses to intercept traffic.
87	**IP spoofing**	*Fake source IP*	Forging the sender address of packets.
88	**MAC spoofing**	*Fake hardware ID*	Faking a device's hardware address.
89	**Eavesdropping**	*Sniffing, snooping*	Secretly listening to network traffic.
90	**Packet sniffing**	*Traffic capture*	Reading data packets on a network.

#	TERM	ALSO CALLED	SIMPLE MEANING
91	**Keylogging**	*Keystroke capture*	Recording everything typed on a keyboard.
92	**Privilege escalation**	*Level-up attack*	Gaining higher access than allowed.
93	**Lateral movement**	*Sideways spread*	Hopping from one machine to another inside.
94	**Pivoting**	*Jump point*	Using one hacked host to reach others.
95	**Data exfiltration**	*Data theft*	Sneaking stolen data out of a network.
96	**Living off the land**	*LOLBins*	Abusing built-in tools to avoid detection.
97	**Fileless attack**	*Memory attack*	Malware that runs in RAM, not on disk.
98	**Injection**	*Code insertion*	Slipping malicious commands into input.
99	**SQL injection**	*SQLi*	Injecting database commands via input fields.
100	**Command injection**	*OS injection*	Running system commands through an app.
101	**Cross-Site Scripting**	*XSS*	Injecting scripts that run in others' browsers.
102	**Cross-Site Request Forgery**	*CSRF*	Tricking a browser into unwanted actions.
103	**Server-Side Request Forgery**	*SSRF*	Making a server fetch attacker-chosen URLs.
104	**Directory traversal**	*Path attack*	Escaping a folder to read other files.
105	**Buffer overflow**	*Memory overflow*	Writing past memory limits to run code.
106	**Race condition**	*Timing bug*	Exploiting the gap between check and use.
107	**Insider threat**	*Rogue employee*	A trusted person who causes harm.
108	**Shoulder surfing**	*Peeking*	Watching a screen or keypad over a shoulder.
109	**Dumpster diving**	*Trash search*	Finding secrets in discarded papers or drives.
110	**Evil twin**	*Fake Wi-Fi*	A rogue Wi-Fi that mimics a real one.
111	**Rogue access point**	*Unauthorized AP*	A hidden Wi-Fi added without permission.
112	**Deauth attack**	*Kick-off attack*	Forcing devices off a Wi-Fi network.
113	**Bluejacking**	*BT spam*	Sending unwanted messages over Bluetooth.
114	**Bluesnarfing**	*BT theft*	Stealing data over a Bluetooth link.
115	**Wardriving**	*Wi-Fi hunting*	Driving around to find open networks.
116	**Deepfake**	*AI fake*	AI-made fake video, image or voice.
117	**Prompt injection**	*AI manipulation*	Tricking an AI with hidden instructions.
118	**Cryptojacking**	*Coin mining hijack*	Secretly using your device to mine crypto.
119	**Ransomware attack**	*Extortion attack*	Locking data and demanding payment.
120	**Double extortion**	*Leak + lock*	Steal data, then also encrypt and threaten to leak.
121	**Wiper attack**	*Data destroyer*	Malware built only to delete data.
122	**Logic bomb trigger**	*Time bomb*	Hidden code that fires on a condition.
123	**Watering the target**	*Recon*	Studying a victim before attacking.
124	**Enumeration**	*Info gathering*	Listing users, shares or services of a target.
125	**Fingerprinting**	*ID scanning*	Identifying software and versions in use.
126	**Spoofing**	*Faking identity*	Pretending to be a trusted source.
127	**Poisoning**	*Data corruption*	Feeding bad data to mislead a system.

MALWARE TYPES

#	TERM	ALSO CALLED	SIMPLE MEANING
128	**Malware**	*Malicious software*	Any software built to harm or steal.
129	**Virus**	*Infector*	Malware that attaches to files and spreads.
130	**Worm**	*Self-spreader*	Malware that copies itself across networks.
131	**Trojan**	*Trojan horse*	Malware hidden inside a useful-looking app.
132	**Ransomware**	*Lockware*	Malware that encrypts data for ransom.
133	**Spyware**	*Snoopware*	Software that secretly watches you.
134	**Adware**	*Ad malware*	Software that forces unwanted ads.

#	TERM	ALSO CALLED	SIMPLE MEANING
135	**Rootkit**	*Deep hider*	Malware that hides itself deep in the system.
136	**Bootkit**	*Boot malware*	A rootkit that infects the startup process.
137	**Keylogger**	*Key recorder*	Tool that records keystrokes.
138	**Backdoor**	*Secret entrance*	A hidden way back into a system.
139	**Bot**	*Zombie*	An infected machine an attacker controls.
140	**Rat**	*Remote Access Trojan*	Malware giving full remote control.
141	**Logic bomb**	*Time bomb*	Code that harms when a condition is met.
142	**Dropper**	*Loader*	Small malware that installs bigger malware.
143	**Downloader**	*Fetcher*	Malware that pulls in more malware.
144	**Loader**	*Stager*	First-stage code that loads the real payload.
145	**Stealer**	*Info-stealer*	Malware that grabs passwords and data.
146	**Wiper**	*Destroyer*	Malware that erases data permanently.
147	**Cryptominer**	*Coinminer*	Malware that mines crypto on your device.
148	**Fileless malware**	*Memory malware*	Malware living only in memory.
149	**Polymorphic malware**	*Shape-shifter*	Malware that changes its code to hide.
150	**Metamorphic malware**	*Rewriter*	Malware that fully rewrites itself each time.
151	**Scareware**	*Fear malware*	Fake alerts that scare you into paying.
152	**Grayware**	*Nuisance software*	Annoying but not clearly malicious apps.
153	**PUP**	*Unwanted program*	Potentially Unwanted Program bundled in installs.
154	**Macro virus**	*Document malware*	Malware inside document macros.
155	**Ransomware-as-a-Service**	*RaaS*	Rented ransomware kits for criminals.
156	**Malware-as-a-Service**	*MaaS*	Malware sold as a paid service.
157	**Command and Control**	*C2, C&C;*	The server that controls infected machines.
158	**Beacon**	*Check-in signal*	Regular calls from malware to its C2.
159	**Payload dropper**	*Installer*	Component that plants the harmful payload.
160	**Exploit kit**	*Attack toolkit*	A packaged set of ready-made exploits.
161	**Malvertising**	*Bad ads*	Ads that deliver malware.
162	**Spyware toolkit**	*Surveillance kit*	A bundle of spying tools.
163	**Trojan downloader**	*Hidden fetcher*	A trojan whose job is fetching malware.
164	**Banking trojan**	*Bank stealer*	Malware that steals banking logins.
165	**Mobile malware**	*Phone malware*	Malware targeting phones and tablets.
166	**Firmware malware**	*Chip malware*	Malware living in device firmware.

NETWORK SECURITY

#	TERM	ALSO CALLED	SIMPLE MEANING
167	**Network**	*Connected systems*	Devices linked to share data.
168	**Firewall**	*Traffic gate*	Filters network traffic by rules.
169	**Next-gen firewall**	*NGFW*	A firewall that also inspects apps and threats.
170	**Packet filter**	*Basic firewall*	Allows or blocks packets by simple rules.
171	**Stateful firewall**	*Connection-aware filter*	Tracks whole connections, not single packets.
172	**Proxy**	*Middleman server*	A server that forwards requests for you.
173	**Reverse proxy**	*Front server*	A proxy that sits in front of servers.
174	**Web proxy**	*Web gateway*	A proxy that filters web browsing.
175	**NAT**	*Address translation*	Shares one public IP among many devices.
176	**VPN**	*Secure tunnel*	An encrypted link over the internet.
177	**Tunnel**	*Wrapped path*	A protected channel inside another network.
178	**VLAN**	*Virtual LAN*	A logical split of one physical network.

#	TERM	ALSO CALLED	SIMPLE MEANING
179	**Segmentation**	*Network splitting*	Dividing a network to limit spread.
180	**Microsegmentation**	*Fine splitting*	Very small, tight network zones.
181	**DMZ**	*Buffer zone*	A semi-open zone between inside and outside.
182	**IDS**	*Intrusion Detection System*	Watches traffic and alerts on attacks.
183	**IPS**	*Intrusion Prevention System*	Detects and blocks attacks live.
184	**NIDS**	*Network IDS*	An IDS watching network traffic.
185	**HIDS**	*Host IDS*	An IDS watching a single machine.
186	**Honeypot**	*Decoy trap*	A fake target set to catch attackers.
187	**Honeynet**	*Decoy network*	A whole fake network to trap attackers.
188	**Sinkhole**	*Traffic trap*	Redirecting bad traffic to a dead end.
189	**Port**	*Connection door*	A numbered channel for a network service.
190	**Port scanning**	*Door knocking*	Checking which ports are open.
191	**Packet**	*Data chunk*	A small unit of network data.
192	**Protocol**	*Rules of talk*	Agreed rules for devices to communicate.
193	**TCP**	*Reliable transport*	A protocol that guarantees delivery order.
194	**UDP**	*Fast transport*	A quick protocol with no delivery promise.
195	**IP address**	*Network address*	A number identifying a device on a network.
196	**MAC address**	*Hardware address*	A device's built-in network ID.
197	**DNS**	*Name lookup*	Turns names like site.com into IP addresses.
198	**DHCP**	*Auto-address*	Hands out IP addresses automatically.
199	**Gateway**	*Exit door*	The device that leads to other networks.
200	**Router**	*Traffic director*	Sends data between networks.
201	**Switch**	*Traffic connector*	Links devices inside one network.
202	**Access point**	*Wi-Fi hub*	A device giving wireless access.
203	**Load balancer**	*Traffic spreader*	Splits work across many servers.
204	**Bandwidth**	*Data capacity*	How much data a link can carry.
205	**Latency**	*Delay*	Time for data to travel across a network.
206	**Packet loss**	*Dropped data*	Packets that never reach their target.
207	**Traffic analysis**	*Flow study*	Studying traffic patterns for clues.
208	**Deep packet inspection**	*DPI*	Looking inside packets, not just headers.
209	**Network tap**	*Traffic mirror*	A device that copies traffic for monitoring.
210	**SPAN port**	*Mirror port*	A switch port that copies traffic.
211	**Egress filtering**	*Outbound control*	Controlling what leaves the network.
212	**Ingress filtering**	*Inbound control*	Controlling what enters the network.
213	**Allowlist**	*Whitelist*	A list of only what is permitted.
214	**Blocklist**	*Blacklist*	A list of what is forbidden.
215	**Geofencing**	*Location blocking*	Blocking access by geographic area.
216	**Rate limiting**	*Speed cap*	Limiting how many requests are allowed.
217	**Network access control**	*NAC*	Checks devices before letting them on.
218	**802.1X**	*Port auth*	A standard to authenticate devices at ports.
219	**SSID**	*Wi-Fi name*	The public name of a wireless network.
220	**WPA2**	*Wi-Fi security*	A common Wi-Fi encryption standard.
221	**WPA3**	*Newer Wi-Fi security*	The latest Wi-Fi encryption standard.
222	**WEP**	*Old Wi-Fi security*	An outdated, broken Wi-Fi encryption.
223	**SSL stripping**	*Downgrade attack*	Forcing a secure link back to insecure.
224	**Split tunneling**	*Partial VPN*	Sending some traffic outside the VPN.

#	TERM	ALSO CALLED	SIMPLE MEANING
225	**Jump box**	*Bastion host*	A hardened gateway to access sensitive systems.
226	**Bastion host**	*Guarded gateway*	A locked-down entry server.

CRYPTOGRAPHY

#	TERM	ALSO CALLED	SIMPLE MEANING
227	**Cryptography**	*Secret writing*	The science of protecting data with math.
228	**Encryption**	*Scrambling*	Turning readable data into secret code.
229	**Decryption**	*Unscrambling*	Turning secret code back to readable data.
230	**Plaintext**	*Clear data*	Readable, unencrypted data.
231	**Ciphertext**	*Scrambled data*	Encrypted, unreadable data.
232	**Cipher**	*Code method*	The rule used to scramble data.
233	**Key**	*Secret code*	The value that locks or unlocks data.
234	**Symmetric encryption**	*Shared-key*	Same key locks and unlocks.
235	**Asymmetric encryption**	*Public-key*	One key locks, a different key unlocks.
236	**Public key**	*Shareable key*	A key you can give to anyone.
237	**Private key**	*Secret key*	A key you must keep hidden.
238	**Key pair**	*Matched keys*	A linked public and private key set.
239	**AES**	*Strong cipher*	A widely used symmetric encryption standard.
240	**RSA**	*Public-key cipher*	A common asymmetric encryption method.
241	**ECC**	*Elliptic curve*	Strong encryption using smaller keys.
242	**DES**	*Old cipher*	An outdated, weak symmetric cipher.
243	**3DES**	*Triple DES*	DES run three times; now retired.
244	**Hashing**	*Fingerprinting*	Turning data into a fixed unique code.
245	**Hash**	*Digest*	The fixed output of a hash function.
246	**MD5**	*Weak hash*	An old, broken hashing method.
247	**SHA-256**	*Strong hash*	A common secure hashing method.
248	**Salt**	*Random extra*	Random data added before hashing passwords.
249	**Pepper**	*Secret extra*	A hidden site-wide value added to hashes.
250	**Collision**	*Hash clash*	Two inputs giving the same hash.
251	**Digital signature**	*E-signature*	Proof that data came from a signer unaltered.
252	**Certificate**	*Digital ID*	A file proving a site or user's identity.
253	**Certificate Authority**	*CA*	A trusted body that issues certificates.
254	**PKI**	*Trust system*	The system managing keys and certificates.
255	**Root certificate**	*Trust anchor*	The top certificate everything trusts.
256	**Chain of trust**	*Trust path*	The linked certificates back to a root.
257	**Self-signed cert**	*Own certificate*	A certificate you signed yourself.
258	**TLS**	*Transport security*	Encrypts data moving over networks.
259	**SSL**	*Old TLS*	The older, retired version of TLS.
260	**HTTPS**	*Secure web*	HTTP protected with TLS encryption.
261	**Handshake**	*Setup chat*	The opening exchange to agree on encryption.
262	**Session key**	*Temporary key*	A short-lived key for one session.
263	**Key exchange**	*Key sharing*	Safely agreeing on a shared secret.
264	**Diffie-Hellman**	*DH key swap*	A method to share a key over open lines.
265	**Perfect forward secrecy**	*PFS*	Old sessions stay safe if a key leaks later.
266	**Nonce**	*One-time number*	A random value used only once.
267	**Initialization vector**	*IV*	Random start value for encryption.
268	**Block cipher**	*Chunk encryptor*	Encrypts data in fixed-size blocks.

#	TERM	ALSO CALLED	SIMPLE MEANING
269	**Stream cipher**	*Flow encryptor*	Encrypts data one bit at a time.
270	**Key rotation**	*Key refresh*	Regularly replacing keys.
271	**Key escrow**	*Key backup*	Storing a key copy with a trusted party.
272	**HSM**	*Hardware Security Module*	A hardware device that guards keys.
273	**Entropy**	*Randomness*	The amount of true unpredictability.
274	**End-to-end encryption**	*E2EE*	Only sender and receiver can read it.
275	**At-rest encryption**	*Stored encryption*	Encrypting saved data.
276	**In-transit encryption**	*Moving encryption*	Encrypting data while it travels.
277	**Steganography**	*Hidden data*	Hiding a message inside another file.
278	**Obfuscation**	*Confusion*	Making code or data hard to read.
279	**Quantum cryptography**	*Post-quantum*	Encryption meant to resist quantum computers.
280	**Cryptanalysis**	*Code-breaking*	The study of breaking encryption.
281	**Message Authentication Code**	*MAC*	A tag proving a message wasn't changed.
282	**HMAC**	*Keyed MAC*	A MAC built using a hash and a key.

IDENTITY & ACCESS MANAGEMENT

#	TERM	ALSO CALLED	SIMPLE MEANING
283	**Identity**	*Digital self*	Who a user or system is online.
284	**IAM**	*Identity management*	Managing who can access what.
285	**Credential**	*Login proof*	Something used to log in (password, key).
286	**Password**	*Secret phrase*	A private string used to log in.
287	**Passphrase**	*Long password*	A longer, sentence-like password.
288	**Passwordless**	*No-password login*	Logging in without a typed password.
289	**Multi-Factor Authentication**	*MFA*	Needing two or more proofs to log in.
290	**Two-Factor Authentication**	*2FA*	Needing exactly two proofs to log in.
291	**One-Time Password**	*OTP*	A code that works only once.
292	**TOTP**	*Time-based OTP*	A code that changes every 30 seconds.
293	**Token**	*Access pass*	A small item proving identity or access.
294	**Hardware token**	*Security key*	A physical device for login.
295	**Soft token**	*App token*	A login code from an app.
296	**Biometrics**	*Body login*	Using fingerprints or faces to log in.
297	**Single Sign-On**	*SSO*	One login for many apps.
298	**Federation**	*Trust sharing*	Letting one system trust another's logins.
299	**OAuth**	*Access delegation*	Letting apps access data without your password.
300	**OpenID Connect**	*OIDC*	An identity layer built on OAuth.
301	**SAML**	*Login exchange*	A standard for sharing login info between sites.
302	**Kerberos**	*Ticket auth*	A ticket-based network login system.
303	**LDAP**	*Directory protocol*	A way to look up users and groups.
304	**Active Directory**	*AD*	Microsoft's user and computer directory.
305	**Directory service**	*User database*	A central store of identities.
306	**Role-Based Access Control**	*RBAC*	Access based on your job role.
307	**Attribute-Based Access Control**	*ABAC*	Access based on many attributes.
308	**Access Control List**	*ACL*	A list of who can do what.

#	TERM	ALSO CALLED	SIMPLE MEANING
309	**Privileged access**	*Admin access*	High-power accounts and rights.
310	**PAM**	*Privileged Access Management*	Controlling powerful admin accounts.
311	**Just-in-time access**	*JIT*	Granting access only when needed, briefly.
312	**Provisioning**	*Account setup*	Creating and setting up user access.
313	**Deprovisioning**	*Account removal*	Removing access when no longer needed.
314	**Identity provider**	*IdP*	The system that verifies who you are.
315	**Service provider**	*SP*	The app that trusts the IdP's login.
316	**Claim**	*Identity fact*	A stated fact about a user (e.g. email).
317	**Assertion**	*Signed statement*	A trusted statement about a login.
318	**Session**	*Login period*	The time you stay logged in.
319	**Cookie**	*Session token*	Small data a site stores in your browser.
320	**Token expiry**	*Timeout*	When a login token stops working.
321	**Refresh token**	*Renewal token*	A token used to get new access tokens.
322	**Access token**	*Entry token*	A token proving current access rights.
323	**Credential theft**	*Login theft*	Stealing usernames and passwords.
324	**Account takeover**	*ATO*	An attacker seizing someone's account.
325	**Password manager**	*Vault app*	An app that stores your passwords safely.
326	**Password vault**	*Secret store*	A protected store for credentials.
327	**Identity governance**	*IGA*	Overseeing who has access and why.
328	**Step-up authentication**	*Extra check*	Asking for more proof for risky actions.
329	**Adaptive authentication**	*Smart login*	Login checks that adjust to risk.
330	**Continuous authentication**	*Ongoing check*	Constantly re-verifying the user.

WEB & APPLICATION SECURITY

#	TERM	ALSO CALLED	SIMPLE MEANING
331	**Application security**	*AppSec*	Protecting software from attacks.
332	**Web application firewall**	*WAF*	A firewall that filters web app traffic.
333	**Input validation**	*Input checking*	Making sure user input is safe.
334	**Output encoding**	*Safe output*	Escaping data so it can't run as code.
335	**Sanitization**	*Input cleaning*	Removing dangerous parts from input.
336	**Parameterized query**	*Prepared statement*	Safe database calls that block injection.
337	**Same-origin policy**	*SOP*	Rule keeping sites from reading each other.
338	**CORS**	*Cross-origin sharing*	Rules allowing safe cross-site requests.
339	**Content Security Policy**	*CSP*	Rules limiting what a page can load.
340	**Secure cookie**	*Protected cookie*	A cookie sent only over HTTPS.
341	**HttpOnly cookie**	*Script-blocked cookie*	A cookie JavaScript can't read.
342	**SameSite cookie**	*Cross-site guard*	A cookie rule that blocks CSRF.
343	**CSRF token**	*Anti-forgery token*	A secret proving a request is genuine.
344	**Session management**	*Login control*	Handling user sessions safely.
345	**Broken authentication**	*Weak login*	Flaws letting attackers bypass login.
346	**Broken access control**	*Weak permissions*	Users reaching things they shouldn't.
347	**IDOR**	*Object reference flaw*	Changing an ID to see others' data.
348	**Security misconfiguration**	*Bad setup*	Weak or default settings left in place.

#	TERM	ALSO CALLED	SIMPLE MEANING
349	**Sensitive data exposure**	*Data leak*	Secrets shown due to weak protection.
350	**Insecure deserialization**	*Object attack*	Abusing how apps rebuild saved objects.
351	**XML External Entity**	*XXE*	Abusing XML parsers to read files.
352	**Server-side template injection**	*SSTI*	Injecting code into page templates.
353	**API security**	*Interface security*	Protecting app-to-app connections.
354	**API key**	*Access key*	A secret string identifying an app caller.
355	**Rate limit bypass**	*Throttle evasion*	Getting around request limits.
356	**Web shell**	*Backdoor page*	A malicious script giving server control.
357	**Cookie theft**	*Session steal*	Stealing cookies to hijack a session.
358	**Session token**	*Login ID*	A secret that keeps you logged in.
359	**OWASP Top 10**	*Risk list*	The top 10 common web app risks.
360	**Secure coding**	*Safe coding*	Writing code that resists attacks.
361	**Code review**	*Peer check*	Reading code to find flaws.
362	**SAST**	*Static analysis*	Scanning source code for flaws.
363	**DAST**	*Dynamic analysis*	Testing a running app for flaws.
364	**IAST**	*Interactive analysis*	Testing from inside a running app.
365	**SCA**	*Dependency scan*	Checking third-party libraries for flaws.
366	**Dependency**	*Library*	Outside code your app relies on.
367	**Software composition**	*Component list*	All the parts making up an app.
368	**SBOM**	*Software bill of materials*	A full list of software components.
369	**Secrets management**	*Key handling*	Safely storing app passwords and keys.
370	**Hardcoded secret**	*Embedded key*	A password left inside source code.
371	**Fuzzing**	*Random testing*	Feeding junk input to find crashes.
372	**Penetration test**	*Pentest*	A hired hacker test of your defenses.
373	**Bug bounty**	*Reward program*	Paying outsiders to report flaws.
374	**Responsible disclosure**	*Coordinated disclosure*	Reporting flaws privately before public.
375	**Threat modeling**	*Risk mapping*	Planning what could attack an app.
376	**Clickjack protection**	*Frame guard*	Stopping hidden-click attacks.
377	**Web scraping**	*Data harvesting*	Auto-collecting data from websites.

CLOUD & VIRTUALIZATION

#	TERM	ALSO CALLED	SIMPLE MEANING
378	**Cloud computing**	*Rented servers*	Using computing over the internet.
379	**Cloud security**	*Cloud protection*	Securing data and apps in the cloud.
380	**Shared responsibility**	*Split duty*	Cloud provider and you each secure parts.
381	**IaaS**	*Infrastructure as a Service*	Renting raw servers and storage.
382	**PaaS**	*Platform as a Service*	Renting a ready platform to build on.
383	**SaaS**	*Software as a Service*	Using software over the web.
384	**Public cloud**	*Shared cloud*	Cloud shared by many customers.
385	**Private cloud**	*Dedicated cloud*	Cloud used by one organization.
386	**Hybrid cloud**	*Mixed cloud*	A blend of private and public cloud.
387	**Multi-cloud**	*Many providers*	Using several cloud providers at once.
388	**Virtual machine**	*VM*	A software-based computer.
389	**Hypervisor**	*VM manager*	Software that runs virtual machines.
390	**Container**	*App box*	A lightweight package of an app and its parts.

#	TERM	ALSO CALLED	SIMPLE MEANING
391	**Kubernetes**	*Container orchestrator*	A tool to run many containers.
392	**Orchestration**	*Auto-coordination*	Automating how systems work together.
393	**Serverless**	*Function cloud*	Running code without managing servers.
394	**Function as a Service**	*FaaS*	Running single functions on demand.
395	**Cloud workload**	*Cloud task*	Any app or job running in the cloud.
396	**CSPM**	*Cloud posture management*	Tools finding cloud misconfigurations.
397	**CWPP**	*Workload protection*	Tools protecting cloud workloads.
398	**CASB**	*Cloud access broker*	A gate controlling cloud app use.
399	**CNAPP**	*Cloud-native protection*	An all-in-one cloud security platform.
400	**Cloud misconfiguration**	*Bad cloud setup*	Weak cloud settings attackers exploit.
401	**Bucket**	*Storage box*	A cloud container for files.
402	**Public bucket**	*Open storage*	Cloud storage exposed to everyone.
403	**IAM role**	*Cloud role*	A set of cloud permissions for a task.
404	**Instance**	*Cloud server*	A single running cloud machine.
405	**Snapshot**	*Backup image*	A saved copy of a system's state.
406	**Image**	*Template*	A ready-made system to launch copies from.
407	**Region**	*Data zone*	A geographic cloud location.
408	**Availability zone**	*Data center group*	Isolated sites inside a region.
409	**Elasticity**	*Auto-scaling*	Growing or shrinking resources on demand.
410	**Tenant**	*Cloud customer*	One user of a shared cloud system.
411	**Multi-tenancy**	*Shared hosting*	Many customers on one system.
412	**Ephemeral**	*Short-lived*	Resources that exist only briefly.
413	**Infrastructure as Code**	*IaC*	Building systems from written config files.
414	**Secrets store**	*Cloud vault*	A cloud service holding keys and secrets.
415	**Cloud-native**	*Built-for-cloud*	Designed to run in the cloud from the start.
416	**Edge computing**	*Near-user compute*	Processing data close to where it's made.

ENDPOINT & DEVICE SECURITY

#	TERM	ALSO CALLED	SIMPLE MEANING
417	**Endpoint**	*End device*	Any device that connects to a network.
418	**Endpoint security**	*Device protection*	Securing laptops, phones and servers.
419	**Antivirus**	*AV*	Software that finds and removes malware.
420	**Anti-malware**	*Malware blocker*	Software that stops many malware types.
421	**EDR**	*Endpoint Detection and Response*	Advanced device threat detection tool.
422	**XDR**	*Extended Detection and Response*	Detection across devices, network and cloud.
423	**MDR**	*Managed Detection and Response*	Outsourced threat detection service.
424	**Host firewall**	*Device firewall*	A firewall built into one machine.
425	**Sandbox**	*Test cage*	A safe isolated space to run risky code.
426	**Quarantine**	*Isolation box*	Locking away a suspected malicious file.
427	**Signature**	*Malware fingerprint*	A known pattern used to spot malware.
428	**Heuristics**	*Behavior guess*	Spotting malware by suspicious behavior.
429	**Behavioral analysis**	*Action watching*	Judging software by what it does.
430	**Whitelisting**	*Allow-only*	Running only approved programs.
431	**Application control**	*App gate*	Deciding which apps may run.
432	**Patch**	*Fix update*	Code that repairs a flaw.
433	**Patch management**	*Update control*	Keeping software fixed and current.

#	TERM	ALSO CALLED	SIMPLE MEANING
434	**Hotfix**	*Quick fix*	A fast, small urgent patch.
435	**Update**	*Upgrade*	New software replacing old.
436	**End-of-life**	*EOL*	Software no longer supported or fixed.
437	**BYOD**	*Bring Your Own Device*	Using personal devices for work.
438	**MDM**	*Mobile Device Management*	Tools to control company phones.
439	**UEM**	*Unified Endpoint Management*	One tool to manage all devices.
440	**Disk encryption**	*Drive lock*	Encrypting a whole storage drive.
441	**BitLocker**	*Windows drive lock*	Microsoft's disk encryption tool.
442	**Secure boot**	*Trusted startup*	Ensuring only trusted code boots.
443	**TPM**	*Trusted Platform Module*	A chip that guards keys and boot integrity.
444	**Firmware**	*Chip software*	Low-level code built into hardware.
445	**BIOS**	*Startup firmware*	Basic code that starts a computer.
446	**UEFI**	*Modern BIOS*	The newer startup firmware standard.
447	**Device driver**	*Hardware bridge*	Software letting the OS use hardware.
448	**USB blocking**	*Port lock*	Stopping unknown USB devices.
449	**Data Loss Prevention**	*DLP*	Tools stopping data from leaking out.
450	**Screen lock**	*Auto-lock*	Locking a device after inactivity.
451	**Remote wipe**	*Erase-from-afar*	Deleting a lost device's data remotely.
452	**Endpoint agent**	*Local sensor*	Software on a device that reports to security.

TOOLS & SOFTWARE

#	TERM	ALSO CALLED	SIMPLE MEANING
453	**Nmap**	*Port scanner*	A tool to map networks and open ports.
454	**Wireshark**	*Packet analyzer*	A tool to capture and read network traffic.
455	**Metasploit**	*Exploit framework*	A toolkit to test exploits.
456	**Burp Suite**	*Web test tool*	A tool to test web app security.
457	**Nessus**	*Vuln scanner*	A tool that scans for known weaknesses.
458	**OpenVAS**	*Open vuln scanner*	A free vulnerability scanner.
459	**Nikto**	*Web scanner*	A tool that scans web servers for issues.
460	**Hydra**	*Login cracker*	A tool to brute-force logins.
461	**John the Ripper**	*Password cracker*	A tool to crack password hashes.
462	**Hashcat**	*GPU cracker*	A fast password-cracking tool.
463	**Aircrack-ng**	*Wi-Fi cracker*	A tool to test wireless security.
464	**Kali Linux**	*Hacker OS*	A Linux built for security testing.
465	**Snort**	*IDS engine*	An open intrusion detection tool.
466	**Suricata**	*Traffic IDS*	A high-speed intrusion detection engine.
467	**Zeek**	*Network monitor*	A tool for deep network analysis.
468	**Sqlmap**	*SQLi tool*	A tool that automates SQL injection tests.
469	**Ndmap**	*Recon tool*	A tool for network reconnaissance.
470	**OSINT**	*Open-source intel*	Info gathered from public sources.
471	**Shodan**	*Device search engine*	A search engine for internet devices.
472	**Maltego**	*Link mapper*	A tool to map relationships in data.
473	**theHarvester**	*Email finder*	A tool to gather emails and names.
474	**Recon-ng**	*Recon framework*	A framework for information gathering.
475	**Cobalt Strike**	*Red-team tool*	A commercial attack simulation tool (often abused).
476	**Mimikatz**	*Credential dumper*	A tool that steals Windows passwords.
477	**BloodHound**	*AD mapper*	A tool that maps Active Directory attack paths.

#	TERM	ALSO CALLED	SIMPLE MEANING
478	**Autopsy**	*Forensics tool*	A tool to investigate digital evidence.
479	**Volatility**	*Memory forensics*	A tool to analyze RAM dumps.
480	**YARA**	*Malware rules*	A tool to identify malware by patterns.
481	**Sysmon**	*System monitor*	A Windows tool logging detailed events.
482	**OSquery**	*System query*	A tool to ask a device about its state.
483	**Splunk**	*Log platform*	A tool to search and analyze logs.
484	**ELK Stack**	*Log toolkit*	Elasticsearch, Logstash and Kibana together.
485	**Wazuh**	*Open SIEM*	A free security monitoring platform.
486	**Nuclei**	*Vuln templates*	A fast template-based vulnerability scanner.
487	**Gobuster**	*Path finder*	A tool to brute-force hidden web paths.
488	**Ffuf**	*Web fuzzer*	A fast web fuzzing tool.
489	**Netcat**	*Network tool*	A simple tool to read/write network data.
490	**Tcpdump**	*CLI sniffer*	A command-line packet capture tool.
491	**Frida**	*App hooker*	A tool to inspect running apps.
492	**MobSF**	*Mobile scanner*	A tool to test mobile app security.

PROTOCOLS

#	TERM	ALSO CALLED	SIMPLE MEANING
493	**HTTP**	*Web protocol*	Rules for browsers and web servers.
494	**FTP**	*File transfer*	An old protocol to move files.
495	**SFTP**	*Secure file transfer*	File transfer over SSH.
496	**FTPS**	*FTP with TLS*	FTP protected by TLS.
497	**SSH**	*Secure shell*	Encrypted remote command access.
498	**Telnet**	*Old remote shell*	Unencrypted remote access (unsafe).
499	**SMTP**	*Mail send*	Protocol for sending email.
500	**IMAP**	*Mail read*	Protocol for reading email on a server.
501	**POP3**	*Mail download*	Protocol for downloading email.
502	**DNSSEC**	*Signed DNS*	DNS with tamper protection.
503	**SNMP**	*Device monitor*	Protocol to manage network devices.
504	**ICMP**	*Ping protocol*	Used for network status messages.
505	**ARP**	*Address resolver*	Maps IP to hardware addresses.
506	**NTP**	*Time sync*	Keeps device clocks in sync.
507	**RDP**	*Remote desktop*	Protocol for remote screen control.
508	**SMB**	*File sharing*	Protocol to share files on a network.
509	**IPsec**	*IP security*	Encrypts network traffic at the IP layer.
510	**RADIUS**	*Login server protocol*	Central authentication for network access.
511	**TACACS+**	*Admin auth protocol*	Access control for network devices.
512	**SCIM**	*User sync*	Automates user account provisioning.
513	**Syslog**	*Log protocol*	A standard for sending system logs.
514	**VoIP**	*Internet calls*	Voice calls over the internet.
515	**SIP**	*Call setup*	Protocol that sets up VoIP calls.
516	**MQTT**	*IoT messaging*	A lightweight protocol for IoT devices.
517	**BGP**	*Route protocol*	Directs traffic between big networks.
518	**QUIC**	*Fast transport*	A modern quick, secure transport protocol.
519	**WPA2-Enterprise**	*Business Wi-Fi*	Wi-Fi security using a login server.
520	**EAP**	*Auth framework*	A flexible network authentication method.

COMPLIANCE & GOVERNANCE

#	TERM	ALSO CALLED	SIMPLE MEANING
521	**Compliance**	*Rule-following*	Meeting required security laws and rules.
522	**Governance**	*Oversight*	Directing and controlling security.
523	**GRC**	*Governance Risk Compliance*	Managing rules, risk and oversight together.
524	**Policy**	*Rulebook*	A formal statement of security rules.
525	**Standard**	*Fixed requirement*	A mandatory technical rule.
526	**Procedure**	*Step guide*	Exact steps to do a security task.
527	**Guideline**	*Advice*	Recommended, non-mandatory practices.
528	**Framework**	*Structure*	An organized set of security practices.
529	**NIST CSF**	*NIST framework*	A popular US cybersecurity framework.
530	**ISO 27001**	*Security standard*	A global standard for security management.
531	**SOC 2**	*Trust report*	An audit of a service's security controls.
532	**PCI DSS**	*Card standard*	Rules for handling payment card data.
533	**HIPAA**	*Health privacy law*	US law protecting health data.
534	**GDPR**	*EU privacy law*	EU law protecting personal data.
535	**CCPA**	*California privacy law*	California's data privacy law.
536	**DPDP**	*India privacy law*	India's data protection law.
537	**Audit**	*Formal check*	An independent review of controls.
538	**Assessment**	*Evaluation*	Judging how secure something is.
539	**Gap analysis**	*Shortfall check*	Comparing current state to a target.
540	**Attestation**	*Formal claim*	A signed statement that controls exist.
541	**Risk assessment**	*Risk study*	Finding and rating risks.
542	**Risk register**	*Risk list*	A recorded list of known risks.
543	**Risk appetite**	*Risk comfort*	How much risk an org accepts.
544	**Risk treatment**	*Risk handling*	Deciding how to deal with each risk.
545	**Control objective**	*Control goal*	What a control is meant to achieve.
546	**Compensating control**	*Backup control*	An alternate control when the ideal isn't possible.
547	**Preventive control**	*Blocker*	A control that stops incidents.
548	**Detective control**	*Alarm*	A control that spots incidents.
549	**Corrective control**	*Repairer*	A control that fixes after an incident.
550	**Due diligence**	*Homework*	Careful checking before a decision.
551	**Due care**	*Reasonable effort*	Taking sensible steps to protect assets.
552	**Data classification**	*Data labeling*	Ranking data by sensitivity.
553	**Data retention**	*Keep period*	How long data must be stored.
554	**Chain of custody**	*Evidence trail*	A record of who handled evidence.
555	**Regulatory requirement**	*Legal rule*	A rule set by law or regulators.
556	**Third-party risk**	*Vendor risk*	Risk from outside suppliers.
557	**Vendor assessment**	*Supplier check*	Judging a supplier's security.
558	**Privacy impact assessment**	*PIA*	A study of privacy risks in a project.
559	**Business Impact Analysis**	*BIA*	Judging the effect of losing a system.
560	**Service Level Agreement**	*SLA*	A promised level of service.

INCIDENT RESPONSE & FORENSICS

#	TERM	ALSO CALLED	SIMPLE MEANING
561	**Incident response**	*IR*	The plan to handle a security breach.
562	**Playbook**	*Response guide*	Step-by-step actions for an incident type.

#	TERM	ALSO CALLED	SIMPLE MEANING
563	**Runbook**	*Ops guide*	Detailed steps to run or fix a system.
564	**Triage**	*Sorting*	Ranking incidents by urgency.
565	**Containment**	*Stop-spread*	Limiting an incident's reach.
566	**Eradication**	*Removal*	Getting rid of the threat completely.
567	**Recovery**	*Restore*	Bringing systems back to normal.
568	**Lessons learned**	*Post-mortem*	Reviewing an incident to improve.
569	**Root cause analysis**	*RCA*	Finding the true source of a problem.
570	**SOC**	*Security Operations Center*	A team that watches for threats 24/7.
571	**SIEM**	*Log analyzer*	A tool that collects and correlates logs.
572	**SOAR**	*Auto-response*	A tool that automates security actions.
573	**Alert**	*Warning*	A signal that something may be wrong.
574	**Alert fatigue**	*Warning overload*	Too many alerts to handle well.
575	**False positive**	*False alarm*	An alert with no real threat.
576	**False negative**	*Missed threat*	A real threat that wasn't detected.
577	**True positive**	*Correct alert*	A real threat correctly flagged.
578	**Correlation**	*Linking clues*	Combining events to spot an attack.
579	**Log**	*Record*	A saved list of system events.
580	**Log aggregation**	*Log gathering*	Collecting logs into one place.
581	**Threat hunting**	*Proactive search*	Actively looking for hidden threats.
582	**Threat intelligence**	*Threat intel*	Knowledge about current attackers.
583	**Feed**	*Data stream*	A live source of threat data.
584	**Digital forensics**	*Cyber CSI*	Investigating digital evidence.
585	**Forensic image**	*Bit copy*	An exact copy of a drive for analysis.
586	**Memory dump**	*RAM copy*	A snapshot of a system's memory.
587	**Artifact**	*Digital trace*	A leftover piece of evidence.
588	**Timeline analysis**	*Event ordering*	Reconstructing what happened, when.
589	**Volatile data**	*Fleeting data*	Data lost when power is off (like RAM).
590	**Write blocker**	*Read-only tool*	A device that stops changing evidence.
591	**Anti-forensics**	*Trace hiding*	Techniques to defeat investigators.
592	**Malware analysis**	*Malware study*	Examining malware to understand it.
593	**Static analysis**	*Code-off study*	Studying malware without running it.
594	**Dynamic analysis**	*Run study*	Studying malware while it runs.
595	**Reverse engineering**	*Teardown*	Taking software apart to understand it.
596	**Disaster recovery**	*DR*	Restoring IT after a major failure.
597	**Business continuity**	*BCP*	Keeping the business running through disruption.
598	**Backup**	*Data copy*	A spare copy for restoring data.
599	**Immutable backup**	*Locked backup*	A backup that can't be changed or deleted.
600	**Recovery Time Objective**	*RTO*	Target time to restore a system.
601	**Recovery Point Objective**	*RPO*	How much data loss is acceptable.
602	**Tabletop exercise**	*Practice drill*	A talk-through rehearsal of an incident.
603	**Escalation**	*Hand-up*	Raising an issue to higher responders.

PEOPLE & ROLES

#	TERM	ALSO CALLED	SIMPLE MEANING
604	**Hacker**	*Cyber intruder*	Someone who breaks into systems.
605	**Black hat**	*Criminal hacker*	A malicious, illegal hacker.
606	**White hat**	*Ethical hacker*	A hacker who helps improve security.

#	TERM	ALSO CALLED	SIMPLE MEANING
607	**Gray hat**	*In-between hacker*	A hacker who bends rules without clear malice.
608	**Script kiddie**	*Novice attacker*	An unskilled attacker using others' tools.
609	**Hacktivist**	*Cause hacker*	A hacker driven by a political cause.
610	**Nation-state actor**	*State hacker*	A government-backed attacker.
611	**Advanced Persistent Threat**	*APT*	A skilled, patient, long-term attacker group.
612	**Cybercriminal**	*Online crook*	A person committing crimes online.
613	**Ethical hacker**	*Pentester*	A hired hacker who tests defenses legally.
614	**Red team**	*Attack team*	Testers who simulate real attackers.
615	**Blue team**	*Defense team*	Defenders who protect and respond.
616	**Purple team**	*Blend team*	Red and blue working together.
617	**Security analyst**	*SOC analyst*	A person who watches and investigates alerts.
618	**Threat hunter**	*Proactive defender*	Someone who searches for hidden threats.
619	**Incident responder**	*First responder*	A person who handles active breaches.
620	**Security engineer**	*Builder*	Someone who builds security systems.
621	**Security architect**	*Designer*	Someone who designs secure systems.
622	**CISO**	*Security chief*	The top security executive.
623	**Compliance officer**	*Rule keeper*	Someone ensuring rules are met.
624	**Forensic analyst**	*Cyber investigator*	Someone examining digital evidence.
625	**Malware analyst**	*Malware researcher*	Someone who studies malicious code.
626	**Bug bounty hunter**	*Flaw finder*	Someone paid to report security bugs.
627	**Insider**	*Trusted user*	Someone inside the organization.
628	**Data Protection Officer**	*DPO*	Someone overseeing privacy compliance.
629	**Vulnerability researcher**	*Flaw hunter*	Someone who discovers new weaknesses.

DATA & PRIVACY

#	TERM	ALSO CALLED	SIMPLE MEANING
630	**Data privacy**	*Info privacy*	Keeping personal data under control.
631	**Personal data**	*PII*	Info identifying a specific person.
632	**PII**	*Personal info*	Personally Identifiable Information.
633	**PHI**	*Health info*	Protected Health Information.
634	**Sensitive data**	*Critical info*	Data that would cause harm if leaked.
635	**Anonymization**	*De-identifying*	Removing identity from data permanently.
636	**Pseudonymization**	*Masking IDs*	Replacing identifiers with fake ones.
637	**Tokenization**	*Value swap*	Replacing sensitive data with safe tokens.
638	**Data masking**	*Data hiding*	Hiding parts of data (e.g. card digits).
639	**Redaction**	*Blacking out*	Permanently removing sensitive text.
640	**Data minimization**	*Collect less*	Keeping only the data truly needed.
641	**Consent**	*Permission*	A user's agreement to use their data.
642	**Data subject**	*Data owner*	The person a piece of data is about.
643	**Data controller**	*Data decider*	Who decides why data is processed.
644	**Data processor**	*Data handler*	Who processes data for a controller.
645	**Right to erasure**	*Right to be forgotten*	A user's right to have data deleted.
646	**Data breach notification**	*Breach alert*	Telling people their data was exposed.
647	**Data sovereignty**	*Local data law*	Data ruled by the laws of its location.
648	**Data residency**	*Data location*	Where data is physically stored.
649	**Data lifecycle**	*Data journey*	Data from creation to deletion.

#	TERM	ALSO CALLED	SIMPLE MEANING
650	**Data at rest**	*Stored data*	Data saved on a disk or database.
651	**Data in transit**	*Moving data*	Data traveling across a network.
652	**Data in use**	*Active data*	Data being processed in memory.
653	**Data leakage**	*Slow leak*	Data slipping out unintentionally.
654	**Exfiltration**	*Data smuggling*	Stealing data out of a system.
655	**Data integrity**	*Data correctness*	Ensuring data isn't secretly changed.
656	**Checksum**	*Integrity check*	A value confirming data is unchanged.
657	**Data governance**	*Data rules*	Managing data quality and access.
658	**Privacy by design**	*Built-in privacy*	Adding privacy from the start.

MOBILE & IOT SECURITY

#	TERM	ALSO CALLED	SIMPLE MEANING
659	**Mobile security**	*Phone security*	Protecting phones and their data.
660	**IoT**	*Internet of Things*	Everyday devices connected online.
661	**IoT security**	*Device security*	Protecting connected smart devices.
662	**Rooting**	*Android unlock*	Gaining full control of an Android phone.
663	**Jailbreaking**	*iOS unlock*	Removing Apple's restrictions on an iPhone.
664	**Sideloading**	*Off-store install*	Installing apps from outside official stores.
665	**App sandbox**	*App cage*	Isolation keeping apps from each other.
666	**App permission**	*Access grant*	What an app is allowed to use.
667	**Overprivileged app**	*Greedy app*	An app asking for more access than needed.
668	**SMS phishing**	*Smishing*	Phishing over text messages.
669	**SIM swapping**	*SIM hijack*	Stealing a phone number to grab codes.
670	**IMSI catcher**	*Fake tower*	A fake cell tower that spies on phones.
671	**Man-in-the-Middle mobile**	*Mobile MITM*	Intercepting a phone's traffic.
672	**Certificate pinning**	*Cert lock*	Forcing an app to trust only set certificates.
673	**Root detection**	*Tamper check*	An app checking if a phone is rooted.
674	**Mobile DLP**	*Phone data guard*	Stopping data leaks from phones.
675	**Wearable security**	*Gadget security*	Protecting smartwatches and bands.
676	**Firmware update**	*Device patch*	Fixing bugs in device firmware.
677	**Default credentials**	*Factory password*	Preset logins left unchanged (risky).
678	**Botnet of things**	*IoT botnet*	Hijacked smart devices used to attack.
679	**OTA update**	*Over-the-air update*	Updating a device wirelessly.
680	**Edge device**	*Field device*	A device at the network's outer edge.
681	**Smart home risk**	*Home IoT risk*	Weaknesses in home smart devices.
682	**Bluetooth attack**	*BT attack*	Exploiting Bluetooth connections.
683	**Pairing**	*Device linking*	Connecting two devices to trust each other.

AI & EMERGING SECURITY

#	TERM	ALSO CALLED	SIMPLE MEANING
684	**AI security**	*Machine security*	Protecting AI systems from misuse and attack.
685	**Adversarial attack**	*AI fooling*	Tricking an AI with crafted input.
686	**Adversarial example**	*Trick input*	Input designed to fool an AI model.
687	**Data poisoning**	*Training poison*	Corrupting an AI's training data.
688	**Model poisoning**	*Model tampering*	Secretly corrupting an AI model.
689	**Jailbreak**	*Guardrail bypass*	Tricking an AI past its safety rules.
690	**Model inversion**	*Data recovery attack*	Extracting training data from a model.
691	**Membership inference**	*Data guess*	Guessing if data was used to train a model.

#	TERM	ALSO CALLED	SIMPLE MEANING
692	**Model extraction**	*Model theft*	Copying a model by probing it.
693	**Hallucination**	*AI making-up*	When an AI states false things confidently.
694	**Guardrails**	*Safety limits*	Rules that keep an AI safe and on-task.
695	**Red teaming AI**	*AI stress test*	Attacking an AI to find its flaws.
696	**Alignment**	*Goal matching*	Making AI act as intended and safely.
697	**Training data**	*Learning data*	The data an AI learns from.
698	**Inference**	*AI prediction*	When a trained AI produces an answer.
699	**LLM**	*Large Language Model*	An AI trained on huge amounts of text.
700	**RAG**	*Retrieval-augmented AI*	AI that looks up facts before answering.
701	**Shadow AI**	*Unapproved AI*	AI tools used without security approval.
702	**Model card**	*AI spec sheet*	A document describing an AI model.
703	**Watermarking AI**	*AI marking*	Hidden marks proving content is AI-made.
704	**Data leakage AI**	*Model leak*	An AI revealing its private training data.
705	**Supply chain AI**	*Model provenance*	Tracking where AI models and data come from.
706	**Deepfake detection**	*Fake spotting*	Tools that detect AI-faked media.
707	**Sensitive output filtering**	*Output guard*	Blocking harmful AI responses.

GENERAL & OPERATIONS

#	TERM	ALSO CALLED	SIMPLE MEANING
708	**Access**	*Entry*	The ability to use a system or data.
709	**Account**	*User profile*	A named identity for using a system.
710	**Admin**	*Administrator*	A high-power user account.
711	**Agent**	*Local software*	A small program that runs on a device.
712	**Alert triage**	*Alert sorting*	Ranking alerts to handle first.
713	**Anomaly**	*Oddity*	Something outside the normal pattern.
714	**Anomaly detection**	*Odd-spotting*	Finding activity that breaks the norm.
715	**Antispam**	*Junk blocker*	Software that blocks unwanted email.
716	**Application**	*App*	A software program for a task.
717	**Approval workflow**	*Sign-off flow*	A required chain of approvals.
718	**Assurance**	*Confidence*	Evidence that controls truly work.
719	**Attribution**	*Blame tracing*	Identifying who did an attack.
720	**Awareness training**	*Security training*	Teaching staff to stay secure.
721	**Backdoor account**	*Hidden account*	A secret account for later access.
722	**Bandwidth throttling**	*Speed limiting*	Slowing traffic on purpose.
723	**Behavioral biometrics**	*Habit login*	Identifying users by their behavior.
724	**Blocklisting**	*Denylisting*	Blocking known-bad items.
725	**Boot sector**	*Startup area*	The disk part that starts a computer.
726	**Bring your own key**	*BYOK*	Using your own encryption keys in the cloud.
727	**Brute-forcing**	*Guess attack*	Trying all combinations to break in.
728	**Certificate revocation**	*Cert cancel*	Marking a certificate as no longer valid.
729	**CRL**	*Revocation list*	A list of canceled certificates.
730	**OCSP**	*Cert status check*	A live check if a certificate is valid.
731	**Cipher suite**	*Encryption set*	The chosen mix of encryption methods.
732	**Cleartext**	*Unencrypted*	Data with no encryption.
733	**Cloud broker**	*Access gate*	A control point for cloud services.
734	**Command injection point**	*Weak input*	A spot where commands can be injected.
735	**Compliance audit**	*Rule check*	A formal review of rule-following.

#	TERM	ALSO CALLED	SIMPLE MEANING
736	**Configuration drift**	*Setting slip*	Settings slowly changing from the baseline.
737	**Container escape**	*Box breakout*	Breaking out of a container to the host.
738	**Credential harvesting**	*Login collecting*	Mass-stealing login details.
739	**Cyber hygiene**	*Basic habits*	Everyday steps that keep you secure.
740	**Cyber insurance**	*Breach insurance*	Insurance covering cyber losses.
741	**Cyber range**	*Practice lab*	A safe arena to practice defense.
742	**Cyber resilience**	*Bounce-back*	Ability to keep going despite attacks.
743	**Dark web**	*Hidden internet*	Hidden sites often used for crime.
744	**Deep web**	*Unindexed web*	Web pages search engines don't list.
745	**Decommissioning**	*Retiring*	Safely shutting down old systems.
746	**Defacement**	*Site vandalism*	Attackers altering a website's look.
747	**Detection rule**	*Alert rule*	Logic that triggers a security alert.
748	**Digital footprint**	*Online trail*	The data trail a person leaves online.
749	**Disaster recovery site**	*Backup site*	A spare location to run systems.
750	**Domain**	*Network group*	A managed group of systems or a web name.
751	**Endpoint hardening**	*Device locking*	Tightening a device's settings.
752	**Enumeration attack**	*Listing attack*	Discovering valid users or resources.
753	**Evasion**	*Detection dodging*	Avoiding security tools.
754	**Exploit chain**	*Combo attack*	Linking several exploits together.
755	**Exposure management**	*Weakness tracking*	Managing all reachable weaknesses.
756	**Federated identity**	*Shared login*	One identity trusted across systems.
757	**File integrity monitoring**	*FIM*	Watching files for unexpected changes.
758	**Firewall rule**	*Traffic rule*	One instruction telling a firewall what to allow.
759	**Golden image**	*Master template*	A trusted base system to clone.
760	**Hardening guide**	*Lockdown guide*	Instructions to secure a system.
761	**Hash function**	*Digest maker*	Math that turns data into a fixed code.
762	**Host**	*Machine*	A single computer on a network.
763	**Identity theft**	*ID theft*	Stealing someone's identity for gain.
764	**Incident ticket**	*Case record*	A tracked record of an incident.
765	**Insider risk**	*Trusted risk*	Danger from people inside the org.
766	**Integrity check**	*Tamper check*	Verifying data hasn't changed.
767	**Intrusion**	*Break-in*	Unauthorized entry into a system.
768	**Isolation**	*Separation*	Keeping a threat away from other systems.
769	**Jump server**	*Access hub*	A controlled server to reach secure zones.
770	**Key management**	*Key control*	Handling encryption keys safely.
771	**Kill switch**	*Emergency stop*	A control to instantly shut something down.
772	**Known-good**	*Trusted state*	A verified safe version to compare to.
773	**Log retention**	*Log keeping*	How long logs are stored.
774	**Log tampering**	*Log editing*	Secretly altering logs to hide tracks.
775	**Malicious insider**	*Rogue staff*	An insider who intends harm.
776	**Managed service provider**	*MSP*	A company running IT for others.
777	**MSSP**	*Managed security provider*	A company running security for others.
778	**Network scanning**	*Network probing*	Checking a network for live hosts.
779	**Obfuscated code**	*Hidden code*	Code deliberately made unreadable.
780	**Offboarding**	*Exit process*	Removing access when someone leaves.
781	**Onboarding**	*Entry process*	Setting up access for new staff.

#	TERM	ALSO CALLED	SIMPLE MEANING
782	**Out-of-band**	*Separate channel*	A different path used for safety.
783	**Patch Tuesday**	*Update day*	Microsoft's monthly patch release day.
784	**Perimeter**	*Boundary*	The outer edge of a protected network.
785	**Persistence**	*Foothold*	How malware survives reboots.
786	**Phishing simulation**	*Fake-phish test*	A safe test phishing email for staff.
787	**Physical security**	*Site security*	Protecting buildings and hardware.
788	**Principle of least privilege**	*Minimal rights*	Give only the access needed.
789	**Privilege creep**	*Access buildup*	Users slowly gaining extra rights.
790	**Proof of concept**	*PoC*	A demo showing an exploit works.
791	**Quarantine network**	*Holding zone*	A restricted area for risky devices.
792	**Recon**	*Scouting*	Gathering info before an attack.
793	**Red flag**	*Warning sign*	A hint that something is wrong.
794	**Remediation plan**	*Fix plan*	Steps to correct found weaknesses.
795	**Replay protection**	*Repeat guard*	Stopping reused data from working.
796	**Rogue device**	*Unknown device*	An unauthorized device on the network.
797	**Sandboxing**	*Caging*	Running code in a safe isolated space.
798	**Scanning**	*Probing*	Automatically checking for issues.
799	**Secure by default**	*Safe out-of-box*	Ships with strong settings enabled.
800	**Secure channel**	*Protected link*	An encrypted communication path.
801	**Secure erase**	*Wipe*	Permanently destroying data.
802	**Security awareness**	*Staff alertness*	How well staff spot threats.
803	**Security champion**	*Team advocate*	A developer who promotes security.
804	**Security gateway**	*Guard point*	A device filtering traffic at a boundary.
805	**Security incident**	*Breach event*	Any event harming security.
806	**Security operations**	*SecOps*	The daily work of defending systems.
807	**Segregation**	*Separation*	Keeping systems or duties apart.
808	**Shadow IT**	*Hidden tech*	Tech used without IT's approval.
809	**Signature-based detection**	*Pattern matching*	Spotting threats by known patterns.
810	**Single point of failure**	*SPOF*	One part whose failure breaks everything.
811	**Smart card**	*Chip card*	A card holding login credentials.
812	**Spoofed email**	*Fake email*	Email forged to look genuine.
813	**Spam**	*Junk mail*	Unwanted bulk messages.
814	**Stateful inspection**	*Connection tracking*	Watching whole connections for safety.
815	**Threat feed**	*Threat stream*	A live source of attacker data.
816	**Time-to-detect**	*Detection speed*	How fast a threat is noticed.
817	**Time-to-respond**	*Response speed*	How fast a threat is handled.
818	**Tokenized data**	*Swapped data*	Data replaced by safe placeholders.
819	**Traffic shaping**	*Flow control*	Managing network traffic priority.
820	**Trust boundary**	*Trust edge*	Where trust level changes in a system.
821	**Two-person rule**	*Dual control*	Two people needed for a risky action.
822	**Unauthorized access**	*Illegal entry*	Getting in without permission.
823	**Uptime**	*Availability time*	How long a system stays running.
824	**Vulnerability disclosure**	*Flaw report*	Reporting a weakness to be fixed.
825	**Vulnerability management**	*Weakness control*	Finding and fixing weaknesses over time.
826	**Vulnerability scan**	*Weakness check*	An automated search for known flaws.
827	**Whitelisted app**	*Approved app*	An app cleared to run.

#	TERM	ALSO CALLED	SIMPLE MEANING
828	**Wiping**	*Erasing*	Destroying data so it can't return.
829	**Zero-day exploit**	*Fresh exploit*	An attack using an unknown, unpatched flaw.
830	**Zombie**	*Bot host*	An infected machine under remote control.
831	**Zone**	*Segment*	A separated part of a network.
832	**Threat surface**	*Exposure area*	All points open to attack.
833	**Security debt**	*Neglect backlog*	Piled-up unfixed security problems.
834	**Canary token**	*Trap token*	A fake secret that alerts if used.
835	**Decoy**	*Bait*	A fake target to lure attackers.
836	**Beaconing**	*Check-in traffic*	Regular signals from malware to its owner.
837	**Data enclave**	*Safe zone*	A tightly controlled data area.
838	**Break-glass account**	*Emergency login*	A sealed account used only in crises.
839	**Session timeout**	*Auto-logout*	Ending idle sessions automatically.
840	**Secure wipe**	*Full erase*	Overwriting data so it's unrecoverable.
841	**Threat actor group**	*Crew*	A named team of attackers.
842	**Watchlist**	*Monitor list*	Items flagged for close watching.
843	**Smurf attack**	*Ping flood*	Flooding a victim using broadcast pings.
844	**Fraggle attack**	*UDP flood*	A Smurf-style flood using UDP packets.
845	**Teardrop attack**	*Fragment attack*	Crashing systems with broken packet fragments.
846	**Ping of death**	*Oversized ping*	Crashing a system with a huge ping packet.
847	**SYN flood**	*Half-open flood*	Overloading a server with fake connection starts.
848	**Slowloris**	*Slow flood*	Holding many connections open to stall a server.
849	**HTTP flood**	*Web flood*	Overwhelming a site with fake requests.
850	**Zip bomb**	*Decompression bomb*	A tiny file that explodes into huge data.
851	**Fork bomb**	*Process bomb*	Code that multiplies to crash a system.
852	**Cache poisoning**	*Cache trick*	Filling a cache with false data.
853	**Cookie poisoning**	*Cookie tampering*	Editing cookies to fool a site.
854	**Parameter tampering**	*Value editing*	Changing hidden values to abuse an app.
855	**HTTP response splitting**	*Header injection*	Injecting fake headers into responses.
856	**Host header injection**	*Header trick*	Abusing the Host header to redirect users.
857	**Open redirect**	*Redirect abuse*	Tricking a site into sending users to a bad link.
858	**Subdomain takeover**	*Orphan hijack*	Claiming an abandoned subdomain.
859	**Credential replay**	*Reused login*	Replaying stolen login data.
860	**Pass-the-hash**	*Hash reuse*	Logging in with a stolen password hash.
861	**Pass-the-ticket**	*Ticket reuse*	Reusing a stolen Kerberos ticket.
862	**Golden ticket**	*Master ticket*	A forged, all-powerful Kerberos ticket.
863	**Silver ticket**	*Service ticket forge*	A forged ticket for one service.
864	**Kerberoasting**	*Ticket cracking*	Cracking service passwords from Kerberos tickets.
865	**DLL injection**	*Code injection*	Forcing a program to load malicious code.
866	**Process hollowing**	*Ghost process*	Hiding malware inside a real process.
867	**Return-oriented programming**	*ROP*	Reusing existing code snippets to run an attack.
868	**Heap spray**	*Memory flooding*	Filling memory to make an exploit reliable.
869	**Use-after-free**	*Freed-memory bug*	Abusing memory that was already released.
870	**Integer overflow**	*Number wrap*	A math error attackers exploit.
871	**Format string attack**	*Printf bug*	Abusing text formatting to read or write memory.
872	**Side-channel attack**	*Leak-by-hint*	Stealing secrets from timing or power clues.
873	**Timing attack**	*Clock leak*	Guessing secrets from how long things take.
874	**Cold boot attack**	*Frozen RAM attack*	Reading memory from a just-powered-off machine.

#	TERM	ALSO CALLED	SIMPLE MEANING
875	**Rowhammer**	*Bit-flip attack*	Flipping memory bits by hammering nearby cells.
876	**Spectre**	*CPU leak*	A processor flaw leaking memory across programs.
877	**Meltdown**	*CPU boundary leak*	A processor flaw exposing protected memory.
878	**Evil maid attack**	*Tamper attack*	Physically tampering with an unattended device.
879	**Juice jacking**	*USB charge attack*	Malware spread through public charging ports.
880	**BadUSB**	*Rogue USB*	A USB device that acts as a malicious keyboard.
881	**RFID cloning**	*Tag copying*	Copying an access card's wireless chip.
882	**NFC relay**	*Tap relay*	Relaying contactless signals to steal access.
883	**GPS spoofing**	*Location faking*	Sending fake GPS signals.
884	**Jamming**	*Signal blocking*	Drowning out wireless signals.
885	**War dialing**	*Number scanning*	Auto-dialing numbers to find systems.
886	**Banner grabbing**	*Service reading*	Reading service info from responses.
887	**Google dorking**	*Search hacking*	Using clever searches to find exposed data.
888	**Credential dumping**	*Secret extraction*	Pulling stored passwords from a system.
889	**Token theft**	*Session steal*	Stealing access tokens to impersonate users.
890	**Consent phishing**	*OAuth phishing*	Tricking users into granting app access.
891	**Malicious app**	*Rogue app*	An app built to harm or spy.
892	**Fake update**	*Trojan update*	Malware disguised as a software update.
893	**Bastion**	*Guard host*	A hardened access point to secure zones.
894	**Canary**	*Early warning*	A tripwire that signals an intrusion.
895	**Deception technology**	*Trap tech*	Fake assets built to catch intruders.
896	**Moving target defense**	*Shifting defense*	Constantly changing to confuse attackers.
897	**Threat emulation**	*Attack mimicry*	Safely copying real attacks to test defenses.
898	**Breach and attack simulation**	*BAS*	Automated, continuous attack testing.
899	**Attack path**	*Route*	The chain of steps to reach a target.
900	**Attack graph**	*Path map*	A map of possible attack routes.
901	**Security orchestration**	*Coordination*	Linking security tools to act together.
902	**Playbook automation**	*Auto-steps*	Auto-running incident response steps.
903	**Enrichment**	*Context adding*	Adding detail to an alert for clarity.
904	**Dwell time**	*Hidden time*	How long an attacker stays undetected.
905	**Mean time to detect**	*MTTD*	Average time to notice a threat.
906	**Mean time to respond**	*MTTR*	Average time to react to a threat.
907	**Baseline behavior**	*Normal pattern*	The usual activity used for comparison.
908	**User behavior analytics**	*UBA*	Spotting threats by unusual user activity.
909	**UEBA**	*Entity analytics*	Behavior analytics for users and devices.
910	**Risk score**	*Danger rating*	A number showing how risky something is.
911	**Confidence score**	*Certainty rating*	How sure a tool is about a finding.
912	**Severity**	*Seriousness*	How bad an issue or alert is.
913	**CVSS**	*Severity score*	A standard 0-10 score for vulnerabilities.
914	**CVE**	*Flaw ID*	A public ID for a known vulnerability.
915	**CWE**	*Weakness type*	A category label for a kind of flaw.
916	**CPE**	*Product ID*	A standard name for a software product.
917	**Patch gap**	*Fix delay*	Time between a fix release and its install.
918	**Exposure window**	*Risk window*	The time a weakness stays open.
919	**Attack simulation**	*Drill*	A rehearsed fake attack for practice.
920	**Purple teaming**	*Joint testing*	Attackers and defenders improving together.
921	**Tabletop**	*Discussion drill*	A talk-through incident rehearsal.

#	TERM	ALSO CALLED	SIMPLE MEANING
922	**Runtime protection**	*Live defense*	Blocking attacks while software runs.
923	**Memory protection**	*RAM guard*	Stopping code from abusing memory.
924	**Control plane**	*Management layer*	Where a system is configured and controlled.
925	**Data plane**	*Traffic layer*	Where actual data moves through a system.
926	**Trust store**	*Cert store*	Where a system keeps trusted certificates.
927	**Certificate transparency**	*Cert logging*	Public logs of issued certificates.
928	**Mutual TLS**	*mTLS*	Both sides prove identity with certificates.
929	**Federated login**	*Shared sign-in*	Logging in via a trusted outside provider.
930	**Passkey**	*FIDO login*	A phishing-resistant passwordless credential.
931	**FIDO2**	*Strong auth standard*	A standard for passwordless, secure login.
932	**WebAuthn**	*Browser auth*	A web standard for passwordless login.
933	**Attestation key**	*Proof key*	A key proving a device is genuine.
934	**Secure element**	*Chip vault*	A tamper-resistant chip storing secrets.
935	**Enclave**	*Protected zone*	An isolated area for sensitive processing.
936	**Confidential computing**	*In-use encryption*	Protecting data even while it's processed.
937	**Homomorphic encryption**	*Compute-on-cipher*	Doing math on data without decrypting it.
938	**Zero-knowledge proof**	*Secret proof*	Proving something true without revealing it.
939	**Key derivation function**	*KDF*	Turning a password into a strong key.
940	**PBKDF2**	*Slow hash*	A method to make password cracking slow.
941	**bcrypt**	*Password hash*	A slow, salted password hashing method.
942	**Argon2**	*Modern hash*	A strong, memory-hard password hash.
943	**Certificate signing request**	*CSR*	A request asking a CA to issue a certificate.
944	**Wildcard certificate**	*Multi-sub cert*	A certificate covering all subdomains.
945	**Revocation**	*Cancellation*	Marking a key or certificate as invalid.
946	**Trust chain**	*Trust ladder*	The linked certificates proving trust.
947	**Security policy**	*Rule set*	The official rules for staying secure.
948	**Acceptable use policy**	*AUP*	Rules for how staff may use systems.
949	**Change management**	*Change control*	A process for safe system changes.
950	**Configuration management**	*Config control*	Tracking and controlling system settings.
951	**Asset inventory**	*Asset list*	A full list of owned devices and software.
952	**Asset management**	*Asset tracking*	Tracking all valuable systems and data.
953	**CMDB**	*Config database*	A database of all IT assets and links.
954	**Data flow diagram**	*DFD*	A map of how data moves through a system.
955	**Threat register**	*Threat list*	A recorded list of known threats.
956	**Control framework**	*Control set*	An organized list of security controls.
957	**Maturity model**	*Growth scale*	A scale rating how developed security is.
958	**Key performance indicator**	*KPI*	A number tracking security performance.
959	**Key risk indicator**	*KRI*	A number warning that risk is rising.
960	**Security metrics**	*Score tracking*	Numbers measuring security health.
961	**Continuous monitoring**	*Always watching*	Constantly checking systems for issues.
962	**Continuous compliance**	*Always compliant*	Staying rule-compliant at all times.
963	**Segregation of duties**	*Split roles*	Splitting tasks so no one has full power.
964	**Data steward**	*Data caretaker*	A person responsible for data quality.

#	TERM	ALSO CALLED	SIMPLE MEANING
965	**Records management**	*Record keeping*	Controlling how records are stored and kept.
966	**Legal hold**	*Preserve order*	A rule to keep data for a legal case.
967	**eDiscovery**	*Legal search*	Finding electronic data for legal cases.
968	**Whistleblower**	*Reporter*	Someone reporting wrongdoing internally.
969	**Security clearance**	*Access level*	Approved permission to see secret data.
970	**Need to know**	*Info limit*	Access only to info required for a job.
971	**Background check**	*Vetting*	Screening a person before granting trust.
972	**Nondisclosure agreement**	*NDA*	A contract to keep information secret.
973	**Threat vector map**	*Vector list*	All the routes threats can take.
974	**Exploit database**	*Exploit-DB*	A public archive of known exploits.
975	**Vulnerability database**	*Flaw archive*	A public store of known weaknesses.
976	**Patch level**	*Update state*	How up-to-date a system's fixes are.
977	**Golden config**	*Ideal setup*	The approved perfect configuration.
978	**Drift detection**	*Change spotting*	Noticing when settings stray from baseline.
979	**Secure SDLC**	*Safe build cycle*	Building security into every dev stage.
980	**Shift left**	*Early security*	Adding security early in development.
981	**DevSecOps**	*Security in DevOps*	Blending security into fast development.
982	**CI/CD security**	*Pipeline security*	Securing the automated build pipeline.
983	**Artifact signing**	*Build signing*	Proving a build wasn't tampered with.
984	**Provenance**	*Origin proof*	Verified history of where something came from.
985	**Immutable infrastructure**	*Replace-not-patch*	Systems replaced whole instead of edited.
986	**Blue-green deployment**	*Swap deploy*	Switching between two live environments safely.
987	**Chaos engineering**	*Break testing*	Breaking systems on purpose to test resilience.
988	**Observability**	*See-inside*	Being able to understand a system's inner state.
989	**Telemetry**	*Sensor data*	Data streamed from systems for monitoring.
990	**Log source**	*Event origin*	Where a log entry comes from.
991	**Normalization**	*Format matching*	Making logs share one common format.
992	**Parsing**	*Breaking down*	Splitting raw data into usable fields.
993	**Retention policy**	*Keep rule*	How long data or logs are stored.
994	**Data broker**	*Info seller*	A company that buys and sells personal data.
995	**Threat actor profile**	*Attacker dossier*	A summary of an attacker's habits.
996	**Campaign**	*Attack wave*	A coordinated set of related attacks.
997	**Watchtower**	*Monitor*	A system that watches for danger.
998	**Sinkholing**	*Traffic trap*	Redirecting malicious traffic to a dead end.
999	**Takedown**	*Removal*	Shutting down malicious infrastructure.
1000	**Blocklist feed**	*Bad-IP list*	A live list of known malicious addresses.
1001	**Reputation service**	*Trust rating*	A service rating IPs or domains by risk.
1002	**Sandbox detonation**	*Safe explode*	Running a suspect file in isolation to observe.
1003	**Threat scoring**	*Danger rating*	Rating how dangerous something is.
1004	**Attack attribution**	*Blame assignment*	Deciding which actor is responsible.
1005	**Cyber kill chain**	*Attack ladder*	The staged model of a full attack.
1006	**Diamond model**	*Intrusion model*	A model linking attacker, victim, tool, target.
1007	**Pyramid of pain**	*Indicator scale*	How much each clue hurts an attacker to lose.
1008	**Security control test**	*Control check*	Verifying a safeguard actually works.
1009	**Compensating measure**	*Backup safeguard*	A stand-in control when the ideal can't be used.
1010	**Fail-open**	*Open on failure*	Letting traffic through if a control fails.

#	TERM	ALSO CALLED	SIMPLE MEANING
1011	**Fail-closed**	*Block on failure*	Blocking traffic if a control fails.
1012	**Watch window**	*Alert period*	A time frame monitored closely.
1013	**Alert tuning**	*Rule tuning*	Adjusting rules to cut noise.
1014	**Suppression rule**	*Mute rule*	A rule that hides known-harmless alerts.
1015	**Escalation path**	*Hand-up chain*	Who to notify as an issue grows.
1016	**On-call**	*Standby duty*	Being ready to respond outside hours.
1017	**Severity level**	*Priority tier*	A ranked label for how urgent an issue is.
1018	**Postmortem**	*After-review*	A written review after an incident.
1019	**Blameless review**	*Fault-free review*	A review focused on fixing, not blaming.