ACRONYMS EXPLAINED

Acronym	Definition
ACL	*Access Control List* – rules that define which users or systems may access network resources or objects.
AIR-GAP	Physical network isolation—systems have no wired or wireless link to untrusted networks.
API	*Application Programming Interface* – a defined set of calls and data formats for software components to interact.
APT	*Advanced Persistent Threat* – a stealthy, long-term intrusion by a well-resourced actor.
ARP	*Address Resolution Protocol* – maps IPv4 addresses to MAC addresses on a LAN.
ASR	*Azure Site Recovery* (also "Automated Server Recovery") – cloud-based replication and failover service.
CA	*Certificate Authority* – issues and signs digital certificates in a PKI.
CBR	*Case-Based Reasoning*
CISO	*Chief Information Security Officer* – senior executive responsible for security policy and strategy.
CMDB	*Configuration Management Database* – stores details of IT assets and their configurations.
CRL	*Certificate Revocation List* – list of certificates revoked by the CA.
CSR	*Certificate Signing Request* – data blob sent to a CA to request a certificate.
CVSS	*Common Vulnerability Scoring System* – standard for rating the severity of security vulnerabilities.
CVE	*Common Vulnerabilities and Exposures* – public database of known security flaws.
DaaS	*Desktop as a Service* – cloud-hosted virtual desktops.
DDoS	*Distributed Denial of Service* – flood attack from many sources to overwhelm a target.
DHCP	*Dynamic Host Configuration Protocol* – assigns IP addresses and network settings to hosts.
DNS	*Domain Name System* – translates human-readable names (e.g. www.example.com) into IP addresses.
DMZ	*Demilitarized Zone* – network segment that separates untrusted from internal LANs.
DLP	*Data Loss (or Leak) Prevention* – policies/tools to detect and block unauthorized data exfiltration.
DNSSEC	*DNS Security Extensions* – adds origin authentication and integrity to DNS data.
DRP	*Disaster Recovery Plan* – procedures for restoring IT services after a major outage.

ACRONYMS EXPLAINED

Acronym	Definition
EDR	*Endpoint Detection & Response* – monitors and analyzes endpoint activity for threats.
EAPoL	*Extensible Authentication Protocol over LAN* – carries EAP frames in 802.1X port-based authentication.
FDE	*Full Disk Encryption* – encrypts entire storage volume to protect data at rest.
GRC	*Governance, Risk, and Compliance* – framework aligning IT controls with business objectives.
HIDS	*Host-based Intrusion Detection System* – monitors one host for malicious activity.
HIPS	*Host-based Intrusion Prevention System* – blocks malicious behaviors on a host.
HTTPS	*HTTP Secure* – HTTP over TLS/SSL for encrypted web traffic.
IAM	*Identity and Access Management* – frameworks and tools to manage digital identities and access rights.
ICMP	*Internet Control Message Protocol* – used for network diagnostics (e.g. ping).
IDS	*Intrusion Detection System* – alerts on suspicious network or host activity.
Ie	*Internet Explorer* (legacy browser).
IKE	*Internet Key Exchange* – handles key negotiation in IPsec VPNs.
IoC	*Indicator of Compromise* – artifact (hash, IP, domain) signaling malicious activity.
IP	*Internet Protocol* – routing protocol for addressing and delivering packets.
IPS	*Intrusion Prevention System* – inline device that detects and blocks threats.
IRP	*Incident Response Plan* – documented process for handling security incidents.
ISMS	*Information Security Management System* – comprehensive security framework (e.g. ISO 27001).
IOPS	*Input/Output Operations Per Second* (storage performance metric).
IPv4 / IPv6	*Internet Protocol version 4/6* – two generations of IP addressing.
ISA	*Interconnection Security Agreement* (or Microsoft's old "Internet Security and Acceleration" firewall).
ITIL	*Information Technology Infrastructure Library* – best-practice framework for IT service management.
IV	*Initialization Vector* – random input to cryptographic algorithms to ensure uniqueness.
JWT	*JSON Web Token* – compact URL-safe token format for claims-based authentication.
KA	*Key Agreement* (cryptographic).

ACRONYMS EXPLAINED

Acronym	Definition
LAN / WAN	*Local / Wide Area Network*.
MFA	*Multi-Factor Authentication* – requires two or more credential types (something you know, have, or are).
MITM	*Man-in-the-Middle* – attacker intercepts and possibly alters communication.
MPLS	*Multiprotocol Label Switching* – directs data from one network node to the next based on short path labels.
NAC	*Network Access Control* – enforces policy on devices before granting network access.
NAT	*Network Address Translation* – remaps private IP addresses to a public IP.
NIDS	*Network-based Intrusion Detection System* – monitors network traffic for signatures or anomalies.
NIPS	*Network-based Intrusion Prevention System* – inline NIDS that can block malicious traffic.
OCSP	*Online Certificate Status Protocol* – checks revocation status of digital certificates in real time.
PAM	*Privileged Access Management* – secure handling of high-privilege credentials.
PBX	*Private Branch Exchange* (telephone system).
PDU	*Protocol Data Unit* – packet at a given OSI layer.
PKI	*Public Key Infrastructure* – framework for public/private key management and certificates.
PoLP	*Principle of Least Privilege* – users/processes get only the rights they need.
PPE	*Personal Protective Equipment* (in physical security contexts).
PTZ	*Pan-Tilt-Zoom* (camera).
QA	*Quality Assurance*.
QoS	*Quality of Service* – prioritizes network traffic by type.
RADIUS	*Remote Authentication Dial-In User Service* – AAA protocol for network access.
RBAC	*Role-Based Access Control* – permissions assigned to roles rather than individuals.
RDP	*Remote Desktop Protocol* – Microsoft's remote-access protocol.
RPO / RTO	*Recovery Point Objective* / *Recovery Time Objective* – DR metrics.
RSA	Rivest–Shamir–Adleman public-key algorithm.
SaaS / PaaS / IaaS	*Software / Platform / Infrastructure as a Service* – cloud service models.
SAML	*Security Assertion Markup Language* – XML-based SSO and federated identity standard.
SCADA	*Supervisory Control and Data Acquisition* – industrial control systems.

ACRONYMS EXPLAINED

Acronym	Definition
SDN / SD-WAN	*Software-Defined Networking* / *WAN* – programmable network architectures.
SEIM	(typo; should be SIEM) see below.
SIEM	*Security Information and Event Management* – collects and correlates security logs and alerts.
SIM	*Subscriber Identity Module* (cellular).
SLB	*Server Load Balancer*.
SMTP / POP / IMAP	*Mail transfer / retrieval protocols*.
SNMP	*Simple Network Management Protocol* – monitors and configures network devices.
SOAR	*Security Orchestration, Automation, and Response* – automates and orchestrates incident handling.
SSH	*Secure Shell* – encrypted remote-login protocol.
SSL / TLS	*Secure Sockets Layer* / *Transport Layer Security* – protocols for encrypted communications.
SSO	*Single Sign-On* – one authentication to access multiple systems.
SPF	*Sender Policy Framework* – email spoofing prevention.
SQLi	*SQL Injection* – attack exploiting poorly sanitized database inputs.
SRTP	*Secure Real-time Transport Protocol* – encrypts media streams.
TCP / UDP	*Transmission Control Protocol* / *User Datagram Protocol*.
TDOA	*Time Difference of Arrival* (wireless tracking).
TOE	*Target of Evaluation* (Common Criteria).
TOTP	*Time-based One-Time Password* – dynamic token algorithm for MFA.
TPM	*Trusted Platform Module* – hardware chip for secure key storage.
TTP	*Tactics, Techniques, and Procedures* – attacker behavior patterns (e.g. MITRE ATT&CK).
UDP	*User Datagram Protocol* – connectionless transport.
USB	*Universal Serial Bus*.
UVC	*Unlicensed Visual Communications* (wireless).
VLAN	*Virtual LAN* – isolated broadcast domain on the same switch.
VPN	*Virtual Private Network* – encrypted tunnel over untrusted networks.
VTP	*VLAN Trunking Protocol* (Cisco).
WAF	*Web Application Firewall* – filters/blocks HTTP attacks.
WLAN / WWAN	Wireless Local / Wide Area Network.
WPS	*Wi-Fi Protected Setup* – simplified Wi-Fi pairing protocol (insecure).

ACRONYMS EXPLAINED

Acronym	Definition
XSS	*Cross-Site Scripting* – injection of client-side scripts into web pages.
XSRF / CSRF	*Cross-Site Request Forgery* – forged state-changing requests on authenticated sites.

Additional “specialized” acronyms and initialisms—beyond the core security terms—commonly encountered in development, scripting, and integration contexts:

Acronym	Definition
BASH	*Bourne Again SHell* – the standard GNU Unix shell and scripting language.
CLI	*Command-Line Interface* – text-based user interface for interacting with software.
GUI	*Graphical User Interface* – visual elements (windows, icons) for user interaction.
REST	*Representational State Transfer* – architectural style for designing HTTP-based APIs.
SOAP	*Simple Object Access Protocol* – XML-based messaging protocol for web services.
JSON	*JavaScript Object Notation* – lightweight, text-based data-interchange format.
XML	*eXtensible Markup Language* – flexible, text-based format for structured data.
YAML	*YAML Ain’t Markup Language* – human-friendly data-serialization standard.
SDK	*Software Development Kit* – collection of tools and libraries for building applications.
IDE	*Integrated Development Environment* – software suite combining code editor, debugger, and build tools.
CI/CD	*Continuous Integration / Continuous Deployment* – practices for automating build, test, and deploy pipelines.
LDAP	*Lightweight Directory Access Protocol* – protocol for accessing and maintaining directory services.
SQL	*Structured Query Language* – language for managing and querying relational databases.
NoSQL	*Not Only SQL* – umbrella term for non-relational, schema-flexible data stores.

ACRONYMS EXPLAINED

Acronym	Definition
HTTP	*Hypertext Transfer Protocol* – foundational protocol of the Web (often over TLS as HTTPS).
GDPR	*General Data Protection Regulation* – EU regulation (effective May 25, 2018) governing the processing and protection of personal data for EU residents.