SECURITY+ ACRONYM GUIDE

September 10, 2025

A

- **ACL – Access Control List**
  - **Definition:** A list of permissions associated with a system resource.
  - **Use:** It specifies which users or system processes are granted access to an object, as well as what operations are allowed on that object (e.g., read, write, execute).
- **ALE – Annualized Loss Expectancy**
  - **Definition:** The single loss expectancy (SLE) multiplied by the annualized rate of occurrence (ARO).
  - **Use:** A risk management formula used to determine the expected monetary loss from a specific risk or threat over a one-year period.
- **ARO – Annualized Rate of Occurrence**
  - **Definition:** The number of times a threat is expected to occur in one year.
  - **Use:** A metric used in risk analysis to calculate the probability of a specific threat occurring annually, which is a component of the ALE formula.
- **AUP – Acceptable Use Policy**
  - **Definition:** A policy that outlines the proper use of an organization's resources, such as computers, networks, and internet services.
  - **Use:** Communicates to users what is considered acceptable behavior and what is prohibited, reducing legal liability and protecting corporate assets.

B

- **BCP – Business Continuity Plan**
  - **Definition:** A plan that outlines procedures and instructions an organization must follow in the face of a disaster to continue operating mission-critical functions.
  - **Use:** Ensures a business can continue to function with minimal disruption after a disaster or significant disruption.
- **BPA – Business Process Automation**
  - **Definition:** A technology-enabled strategy for automating complex business processes and functions.
  - **Use:** In security, it can automate tasks like patch management, log analysis, and incident response workflows, improving efficiency and reducing human error.
- **BIA – Business Impact Analysis**
  - **Definition:** A component of the business continuity plan that identifies the critical business functions and the impact a disruption would have on them.
  - **Use:** It helps an organization prioritize which functions to restore first and determines the necessary resources and recovery time objectives (RTOs).
- **BYOD – Bring Your Own Device**
  - **Definition:** An IT policy that allows employees to use their personal mobile devices, such as smartphones and laptops, for work purposes.
  - **Use:** While it can increase employee productivity and satisfaction, it also introduces significant security risks that must be managed.

C

- **CASB – Cloud Access Security Broker**
  - **Definition:** A security policy enforcement point placed between cloud service consumers and cloud service providers.
  - **Use:** It provides visibility into an organization's cloud usage, enforces security policies, and protects sensitive data from being shared or transferred inappropriately.
- **CCTV – Closed-Circuit Television**
  - **Definition:** A television system in which signals are not publicly broadcast but are monitored, primarily for surveillance and security purposes.
  - **Use:** Used for physical security to monitor and record activity in and around a building or sensitive area.
- **COBO – Corporate-Owned, Business-Only**
  - **Definition:** An enterprise mobility policy where the organization provides the device, and the device is used exclusively for business purposes.
  - **Use:** Provides a high level of control and security for the organization, as there is no personal data on the device.
- **COPE – Corporate-Owned, Personally-Enabled**
  - **Definition:** An enterprise mobility policy where the organization provides the device, but employees can use it for personal activities as well.
  - **Use:** Offers a balance of corporate control and employee convenience, but requires robust security measures to separate business and personal data.
- **CRL – Certificate Revocation List**
  - **Definition:** A list of digital certificates that the issuing certificate authority has revoked before their expiration date.
  - **Use:** Allows systems to check if a certificate is still valid and has not been compromised or revoked.
- **CSL – Critical Security Controls**
  - **Definition:** A prioritized list of security controls designed to stop the most prevalent and dangerous cyberattacks.
  - **Use:** Provides a foundational framework for an organization's security program, focusing on high-impact, actionable measures.
- **CVE – Common Vulnerabilities & Exposures**
  - **Definition:** A dictionary of publicly known information security vulnerabilities and exposures.
  - **Use:** Provides a common identifier for each vulnerability, allowing security professionals to share and discuss them more easily.
- **CVSS – Common Vulnerability Scoring System**
  - **Definition:** A standardized framework for rating the severity of software vulnerabilities.
  - **Use:** Provides a method for assigning a numerical score to a vulnerability, enabling organizations to prioritize and manage their vulnerability response efforts effectively.

D

- **DDoS – Distributed Denial of Service**
  - **Definition:** A cyberattack in which multiple compromised computer systems attack a target, such as a server, website, or other network resource, causing a denial of service for users of the targeted resource.
  - **Use:** An attack vector; its use is to overwhelm and take down a target's network or service.
- **DMARC – Domain-based Message Authentication, Reporting & Conformance**
  - **Definition:** An email authentication protocol that builds on SPF and DKIM to prevent email spoofing and phishing.
  - **Use:** Allows a domain owner to specify how a recipient's email server should handle emails that fail SPF or DKIM checks.
- **DLP – Data Loss Prevention**
  - **Definition:** A set of technologies and policies used to prevent the loss or theft of sensitive data.
  - **Use:** Monitors and controls data in use, in motion, and at rest to ensure that it is not misused or leaked.
- **DNS – Domain Name System**
  - **Definition:** A hierarchical and decentralized naming system for computers, services, or any resource connected to the Internet or a private network.
  - **Use:** Translates human-readable domain names (e.g., www.example.com) into IP addresses (e.g., 192.0.2.1) that computers use to locate each other.
- **DRP – Disaster Recovery Plan**
  - **Definition:** A documented, structured approach that describes how an organization can quickly resume its business operations after a disaster.
  - **Use:** Focuses on the IT systems and data needed to support business continuity, outlining steps to restore technology infrastructure.

E

- **EAP – Extensible Authentication Protocol**
  - **Definition:** An authentication framework frequently used in wireless networks and Point-to-Point Protocol (PPP) connections.
  - **Use:** Provides a framework for different authentication methods (e.g., passwords, certificates, tokens) to be used with a network access device.
- **ECC – Elliptic Curve Cryptography**
  - **Definition:** A public key encryption method based on the algebraic structure of elliptic curves over finite fields.
  - **Use:** Provides a level of security equivalent to or better than RSA but with smaller key sizes, making it more efficient for devices with limited processing power.

- **EULA – End User License Agreement**
  - **Definition:** A legal contract between a software manufacturer and the user of the software.
  - **Use:** Outlines the terms and conditions under which a user can use the software, including restrictions and liabilities.
- **EDR – Endpoint Detection & Response**
  - **Definition:** A security technology that continuously monitors and responds to threats on endpoints like laptops, desktops, and servers.
  - **Use:** Provides real-time visibility and automates the detection and remediation of suspicious activities on a device.

F

- **FDE – Full Disk Encryption**
  - **Definition:** A security method that encrypts all the data on a hard drive at the hardware level.
  - **Use:** Protects data at rest, ensuring that if a device is lost or stolen, the data on the drive is unreadable without the correct decryption key.
- **FIM – File Integrity Monitoring**
  - **Definition:** A technology that monitors and alerts on changes to critical system files.
  - **Use:** Detects potential malicious activity, such as malware or unauthorized changes to system configurations, by comparing files to a known baseline.
- **FTP – File Transfer Protocol**
  - **Definition:** A standard network protocol used for the transfer of computer files from a server to a client on a computer network.
  - **Use:** Used to transfer files between computers, though it lacks built-in security and is often replaced by more secure alternatives like SFTP.

G

- **GRE – Generic Routing Encapsulation**
  - **Definition:** A tunneling protocol that encapsulates a wide variety of network layer protocols inside virtual point-to-point links over an IP network.
  - **Use:** Used to create a secure tunnel for data transfer, often as a component of a VPN.
- **GPO – Group Policy Object**
  - **Definition:** A collection of settings that define what a system will look like and how it will behave for a defined group of users.
  - **Use:** In Windows environments, it's used to centrally manage and configure security settings, software, and user permissions across a network.

H

- **HSM – Hardware Security Module**
  - **Definition:** A physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing.
  - **Use:** Provides a secure, tamper-resistant environment for generating, storing, and using cryptographic keys.

I

- **IAM – Identity and Access Management**
  - **Definition:** A framework of policies and technologies for ensuring that the right users have the appropriate access to technology resources.
  - **Use:** Manages user identities and their permissions to corporate resources, improving security and reducing the risk of unauthorized access.
- **IdP – Identity Provider**
  - **Definition:** A service that creates, maintains, and manages identity information for principals and provides authentication services to relying applications.
  - **Use:** Authenticates users and provides identity information to other services, often using standards like SAML or OAuth.
- **ICS – Industrial Control System**
  - **Definition:** A system used to monitor and control industrial processes, such as manufacturing, power generation, and water treatment.
  - **Use:** These systems are critical infrastructure and are a target for cyberattacks, requiring specialized security measures.
- **IoT – Internet of Things**
  - **Definition:** A network of physical objects ("things") embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.
  - **Use:** The security of IoT devices is a major concern due to their limited resources and potential for use in botnets.
- **IPS – Intrusion Prevention System**
  - **Definition:** A network security device that monitors network and/or system activities for malicious activity or policy violations.
  - **Use:** It can actively block or prevent detected threats in real-time.
- **IRP – Incident Response Plan**
  - **Definition:** A documented set of procedures for how an organization will respond to a security incident or cyberattack.
  - **Use:** Provides a step-by-step guide for detection, containment, eradication, and recovery, minimizing damage and recovery time.

- **IPSec – Internet Protocol Security**
  - **Definition:** A suite of protocols used to secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet.
  - **Use:** Often used to create secure VPN tunnels between networks.

- **IaaS – Infrastructure as a Service**
  - **Definition:** A form of cloud computing that provides virtualized computing resources over the internet.
  - **Use:** Provides the foundational building blocks for cloud services, such as virtual machines, storage, and networks.
- **IaC – Infrastructure as Code**
  - **Definition:** The process of managing and provisioning computer data centers through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools.
  - **Use:** Automates the creation and configuration of infrastructure, improving consistency and reducing the risk of misconfigurations.

L

- **LDAP – Lightweight Directory Access Protocol**
  - **Definition:** An open, vendor-neutral, industry-standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.
  - **Use:** Commonly used to centralize user authentication and authorization, allowing applications to verify a user's identity against a central directory.

M

- **MDM – Mobile Device Management**
  - **Definition:** A type of security software used by an IT department to monitor, manage, and secure employee mobile devices that are deployed across multiple mobile service providers and across the organization.
  - **Use:** Enforces security policies, such as strong passwords, encryption, and remote wiping, on mobile devices.
- **MOA – Memorandum of Agreement**
  - **Definition:** A formal document that outlines a collaborative agreement between two or more parties.
  - **Use:** In security, it can be used to document the understanding and responsibilities between organizations when sharing security-related data or services.

- **MOU – Memorandum of Understanding**
  - **Definition:** A document that expresses a mutual accord between two or more parties without a formal legal commitment.
  - **Use:** Similar to an MOA, it clarifies the terms of a cooperative relationship without creating a legally binding contract.
- **MSA – Measurement Systems Analysis**
  - **Definition:** A formalized process for assessing and quantifying the amount of variation in a measurement system.
  - **Use:** Not directly a security term, but can be relevant in security operations to ensure the accuracy and reliability of security metrics and data.
- **MTTR – Mean Time to Recovery**
  - **Definition:** The average time it takes for a system or component to be restored after a failure or a security incident.
  - **Use:** A key metric used to evaluate the effectiveness of an incident response and disaster recovery plan.

N

- **NAC – Network Access Control**
  - **Definition:** A set of technologies that controls access to a network based on pre-defined policies.
  - **Use:** Can prevent unauthorized devices from connecting to the network and can enforce security policies on devices that are granted access.
- **NIDS – Network Intrusion Detection System**
  - **Definition:** A system that monitors network traffic for suspicious activity and known threats.
  - **Use:** Detects potential intrusions and sends alerts to a security administrator, but does not take automated action to block the traffic.
- **NIPS – Network Intrusion Prevention System**
  - **Definition:** Similar to a NIDS, but it can actively block or prevent detected threats from entering the network.
  - **Use:** A proactive security control that can automatically drop malicious packets and block an attacking IP address.
- **NGFW – Next-Generation Firewall**
  - **Definition:** A firewall that goes beyond basic port and protocol inspection by integrating other security features like application awareness, intrusion prevention, and threat intelligence.
  - **Use:** Provides deeper inspection of network traffic and more granular control than a traditional firewall.

- **NDA – Non-Disclosure Agreement**
  - **Definition:** A legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to.
  - **Use:** Protects sensitive business information from being disclosed to unauthorized third parties.
- **NFC – Near Field Communication**
  - **Definition:** A set of communication protocols for communication between two electronic devices over a distance of 4 cm or less.
  - **Use:** Used in contactless payment systems, keycards, and mobile device pairing. The short range provides a level of security against eavesdropping.

O

- **OAuth – Open Authorization**
  - **Definition:** An open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites without giving them the passwords.
  - **Use:** Enables single sign-on (SSO) and secure access to APIs.
- **OCSP – Online Certificate Status Protocol**
  - **Definition:** A protocol used to determine the revocation status of an X.509 digital certificate in real-time.
  - **Use:** An alternative to the Certificate Revocation List (CRL) that provides faster, real-time checks on a certificate's validity.

P

- **PAM – Privileged Access Management**
  - **Definition:** A comprehensive security strategy and technology for managing and securing privileged accounts and their access to critical systems.
  - **Use:** Controls and monitors the activity of privileged accounts to prevent misuse and reduce the attack surface.
- **PKI – Public Key Infrastructure**
  - **Definition:** A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.
  - **Use:** Provides a framework for secure electronic commerce, communication, and digital signatures.

R

- **RAS – Remote Access Service**
  - **Definition:** Any combination of hardware and software that enables a remote computer to connect to a local area network (LAN) by means of a telecommunication line.
  - **Use:** Allows users to connect to a corporate network from a remote location, often via a VPN.
- **RADIUS – Remote Authentication Dial-In User Service**
  - **Definition:** A networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect to and use a network service.
  - **Use:** Commonly used by ISPs and corporations to manage user access to network resources, such as dial-up or wireless networks.
- **RPO – Recovery Point Objective**
  - **Definition:** A metric that defines the maximum amount of data (measured in time) that an organization can afford to lose during a disaster.
  - **Use:** A key parameter in a DRP and BCP that helps determine the frequency of backups.

S

- **SAML – Security Assertion Markup Language**
  - **Definition:** An open standard for exchanging authentication and authorization data between an identity provider and a service provider.
  - **Use:** Used to enable single sign-on (SSO) in web applications.
- **SCADA – Supervisory Control & Data Acquisition**
  - **Definition:** A type of industrial control system (ICS) that monitors and controls processes in a wide range of industries, such as power, oil and gas, and water.
  - **Use:** These systems are critical infrastructure and are a high-value target for cyberattacks.
- **SCAP – Security Content Automation Protocol**
  - **Definition:** A suite of standards and policies developed to automate the management and assessment of system security.
  - **Use:** Provides a standardized way to evaluate and report on the security posture of an organization's systems.
- **SDN – Software-Defined Networking**
  - **Definition:** An architecture that centralizes control of the network, separating the control plane from the data plane.
  - **Use:** Allows network administrators to manage and configure network devices programmatically, improving security and flexibility.

- **SLA – Service Level Agreement**
  - **Definition:** A contract between a service provider and a customer that defines the level of service expected from the provider.
  - **Use:** In a security context, it can define the expected uptime of a security service or the response time for a security incident.
- **SIEM – Security Information & Event Management**
  - **Definition:** A security solution that provides a centralized platform for collecting, analyzing, and correlating security event data from various sources.
  - **Use:** Helps organizations identify potential security threats and manage their security posture.
- **SOAR – Security Orchestration, Automation & Response**
  - **Definition:** A stack of software that allows an organization to collect security alerts from multiple sources and perform automated responses to low-level threats.
  - **Use:** Automates repetitive and low-level security tasks, allowing security analysts to focus on more complex threats.
- **SQLi – SQL Injection**
  - **Definition:** A code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution.
  - **Use:** An attack vector used to bypass authentication, retrieve sensitive data, or modify database information.
- **SSL – Secure Sockets Layer**
  - **Definition:** A deprecated cryptographic protocol designed to provide communication security over a computer network.
  - **Use:** While now replaced by TLS, the term is still commonly used to refer to encrypted web traffic (e.g., "SSL certificate").
- **SLE – Single Loss Expectancy**
  - **Definition:** The expected monetary loss when a single threat or attack occurs.
  - **Use:** A component of the ALE formula that quantifies the financial impact of a single security event.
- **SDLC – Software Development Life Cycle**
  - **Definition:** A framework that defines the stages involved in the creation of software.
  - **Use:** In a security context, it's used to integrate security best practices and testing throughout the development process (secure SDLC).

T

- **TPM – Trusted Platform Module**
  - **Definition:** A dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.
  - **Use:** Provides hardware-based security for cryptographic functions, such as disk encryption and authentication, protecting keys from software-based attacks.

- **TGT – Ticket Granting Ticket**
  - **Definition:** A special kind of Kerberos ticket that a Kerberos authentication server grants to a user.
  - **Use:** It is used to request other Kerberos tickets for access to different services, allowing single sign-on.

U

- **UBA – User Behavior Analytics**
  - **Definition:** A cybersecurity process that uses a set of technologies to analyze the behavior of users within a network.
  - **Use:** Detects anomalous behavior that may indicate an insider threat or a compromised account.
- **UTM – Unified Threat Management**
  - **Definition:** A type of network security device that combines multiple security functions into a single hardware or software platform.
  - **Use:** Simplifies network security by integrating features like firewalls, intrusion prevention, antivirus, and content filtering into a single appliance.

V

- **VPN – Virtual Private Network**
  - **Definition:** A technology that creates an encrypted connection over a less secure network, such as the internet.
  - **Use:** Provides a secure way for users to access a private network from a remote location, ensuring data confidentiality and integrity.

W

- **WAF – Web Application Firewall**
  - **Definition:** A specific type of firewall that monitors, filters, and blocks HTTP traffic to and from a web application.
  - **Use:** Protects web applications from common attacks like SQL injection and cross-site scripting (XSS) by inspecting web traffic for malicious payloads.

X

- **XSS – Cross-Site Scripting**
  - **Definition:** A type of security vulnerability typically found in web applications.
  - **Use:** An attack vector where a malicious actor injects client-side script into web pages viewed by other users.