ITPro Today™ Cybersecurity Acronyms Cheat Sheet

This reference guide details essential cybersecurity acronyms and terminology to help you speak like a seasoned security expert.

Term	Short for …	Meaning
AES	Advanced Encryption Standard	An encryption method widely used to secure data today.
APT	Advanced Persistent Threat	A threat actor with sophisticated expertise and extensive resources who is capable of carrying out advanced attacks. The opposite of a "script kiddie," meaning an inexperienced attacker who relies primarily on tools developed by others to exploit vulnerabilities.
AV	Antivirus	A type of software that helps detect and mitigate malware on computer systems. AV is an old term, but it remains a core element of cybersecurity.
CISO	Chief Information Security Officer	This is the title of the executive who oversees all aspects of cybersecurity at most organizations.
CSO	Chief Security Officer	Some businesses maintain a CSO role in addition to a CISO role. The differences between each position can vary, but in general, a CSO focuses on tasks like physical security and employee education, while the CISO oversees cybersecurity initiatives as a whole.
CVE	Common Vulnerabilities and Exposures	A system for tracking publicly known security vulnerabilities. Following CVE data helps you know if any of the software your business uses is vulnerable to attack.
IAM	Identity and Access Management	A type of framework for managing access rights. It covers PAM (which focuses on access for privileged users), as well as permissions for non-privileged users.
IDS	Intrusion Detection System	A category of security software whose main purpose is to identify signs of a breach, typically by using cybersecurity analytics to detect anomalous activity on networks or within applications.
MDR	Managed Detection and Response	An outsourced alternative to an in-house security operations center (SOC). A team of experts continuously monitor your systems, often using advanced tools to stop cyberattacks and improve your security posture.
MFA	Multi-factor Authentication	A type of authentication process that requires users to enter multiple credentials — such as a password and a numeric one-time login code sent by email — to access a resource.
MSSP	Managed Security Service Provider	A type of business that specializes in providing security services to other companies on an outsourced basis. MSSPs are valuable for organizations with limited in-house security capabilities.
PAM	Privileged Access Management	The process of managing access rights and permissions for privileged users inside a software system, such as system administrators. PAM is one component of IAM.
SASE	Secure Access Service Edge	An approach to network design that integrates security capabilities, such as traffic filtering, into the network architecture.
SBOM	Software Bill of Materials	An inventory of all the software resources included in a codebase or system. SBOMs help organizations track the software they use so they'll know if they're vulnerable to threats against that software. They're particularly important for tracking risks associated with software components sourced externally, such as open source code or libraries that developers borrow when creating an app.
SIEM	Security Information and Event Management	A type of software tool that ingests and analyzes data from a variety of sources to discover potential security risks.
SOAR	Security Orchestration, Automation and Response	A type of software tool that can identify threats, as well as help manage automated responses to them. There's some debate about exactly how SOARs are different from SIEMs, but the general consensus is that SOARs extend SIEM functionality by adding automated response and incident management capabilities to cybersecurity analytics.
SOC	Security Operations Center	The set of people and tools responsible for managing cybersecurity within a business. Some organizations have physical SOC spaces that serve as a center for security operations, but SOC can also refer to cybersecurity as a business function, even if it's not a physical resource.
XDR	Extended Detection and Response (or Cross-Layered Detection and Response, by some definitions)	A category of cybersecurity tool that analyzes data from across the business to detect risks. XDR is arguably just a new buzzword to refer to what used to be called SIEM, although XDR advocates typically contend that XDR tools include more advanced analytics capabilities and can work with a broader range of data types.
ZTNA	Zero Trust Network Access	An approach to network security in which devices must be explicitly determined to be secure before they can access network resources.