Cyber Security Acronyms Cheat Sheet

#	Acronym	Stands for	Definition
1	APT	Advanced Persistent Threat	A cyber attack that continuously uses advanced techniques to conduct cyber espionage or crime
2	APWG	Anti-Phishing Working Group	An international consortium that brings together businesses affected by phishing attacks with security companies, law enforcement, government , trade associations, and others.
3	AV	Antivirus	A computer program used to prevent, detect, and remove malware.
4	AVIEN	Anti-Virus Information Exchange Network	A group of Antivirus and security specialists who share information regarding AV companies, products, malware and other threats.
5	CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart	A response test used in computing, especially on websites, to confirm that a user is human instead of a bot.
6	CARO	Computer Antivirus Research Organization	An organization established in 1990 to study malware.
7	CAVP	Cryptographic Algorithm Validation Program	This program provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and individual components. Cryptographic algorithm validation is a necessary precursor to cryptographic module validation.
8	CBC	Cipher Block Chaining	Operation for a block cipher using an initialization vector and a chaining mechanism. This will cause the decryption of a block of cipher text to depend on preceding cipher text blocks.
9	CBC-MAC	Cipher Block Chaining Message Authentication Code	This constructs a message authentication code from a block cipher. The message is encrypted with some block cipher algorithm in CBC mode. This creates a chain of blocks with each block depending on the correct encryption of the previous block.
10	CERIAS	Center for Education and Research in Information Assurance and Security	A part of Purdue University dedicated to research and education in information security.
11	CERT	Computer Emergency Response Team	In this case, an expert group that handles computer security incidents and alerts organizations about them.
12	CHAP	Challenge-Handshake Authentication Protocol	A protocol for authentication that provides protection against replay attacks through the use of a changing identifier and a variable challenge-value.
13	CIRT	Computer Incident Response Team	A group that handles events involving computer security and data breaches.
14	CIS	Center for Internet Security	A 501 nonprofit organization with a mission to "Identify, develop, validate, promote, and sustain best practice solutions for cyber defense and build and lead communities to enable an environment of trust in cyberspace."
15	CISA	Certified Information Systems Auditor	Professionals who monitor, audit, control and assess information systems.
16	CISM	Certified Information Systems Security Manager	A certification offered by ISACA which "Demonstrates your understanding of the relationship between an information security program and broader business goals and objectives."
17	CISO	Chief Information Security Officer	The CISO is the executive responsible for an organization's information and data security. Increasingly, this person aligns security goals with business enablement or digital transformation. CISOs are also increasingly in a "coaching role" helping the business manage cyber risk. This is according to Ponemon Institute research.
18	CISSP	Certified Information Systems Security Professional	The CISSP is a security certification for security analysts, offered by ISC(2). It was designed to indicate a person has learned certain standardized knowledge in cybersecurity.
19	CNAP	Cybersecurity National Action Plan	A U.S. plan to enhance cybersecurity awareness and protections, protect privacy, maintain public safety, and economic and national security.
20	CNCI	Comprehensive National Cybersecurity Initiative	A U.S. government initiative designed to establish a front line of defense against network intrusion, defend the U.S. against the threats through counterintelligence, and strengthen the cybersecurity environment.
21	CND	Computer Network Defense	CND is defined by the U.S. military as defined by the US Department of Defense (DoD) as, “Actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks.” This style of defense applies to the private sector as well.

22	COBIT	Control Objectives for Information and Related Technologies	An IT management including practices, tools and models for risk management and compliance.
23	CSEC	Cyber Security Education Consortium	The CSEC, also known as the CEC, partners with educators and the broader cybersecurity community to ensure students are prepared to lead and be changemakers in the cybersecurity workforce.
24	CSA	Cloud Security Alliance	The Cloud Security Alliance is the world's leading organization for defining best practices in cloud cybersecurity. It also provides a cloud security provider certification program, among other things.

25	CSO	Chief Security Officer	In some cases, the Chief Security Officer is in charge of an organization's entire security posture or strategy. This includes both physical security and cybersecurity. In other cases, this title belongs to the senior most role in charge of cybersecurity.
26	CSSIA	Center for Systems Security and Information Assurance	The CSSIA is a U.S. leader in training cybersecurity educators. It provides these teachers and professors with real-world learning experiences in information assurance and network security.
27	CVSS	Common Vulnerability Scoring System	An inudstry standard for rating the severity of security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat.
28	DDoS	Distributed Denial of Service	A distributed denial-of-service (DDoS) attack attempts to disrupt normal traffic of a targeted server, service or network to make a service such as a website unusable by “flooding” it with malicious traffic or data from multiple sources (often botnets).
29	DLP	Data Loss Prevention	An information security strategy to protect corporate data. DLP is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users, either inside or outside of an organization.
30	DNS attack	Domain Name Server	DNS stands for “domain name server,” which uses the name of a website to redirect traffic to its owned IP address. Amazon.com should take you to Amazon's website, for example. During this type of attack, which is complex and appears in several ways, cybercriminals can redirect you to another site for their own purposes. This attack takes advantage of the communication back and forth between clients and servers.
31	EDR	Endpoint Detection & Response	Endpoint Detection & Response (EDR) solutions are designed to detect and respond to endpoint anomalies. EDR solutions are not designed to replace IDPS solutions or firewalls but extend their functionality by providing in-depth endpoint visibility and analysis. EDR uses different datasets, which facilitates advanced correlations and detection.
32	FISMA	Federal Information Security Management Act	FISMA is United States legislation which requires each federal agency to develop, document, and implement an agency-wide program to provide information security for its information systems and data. The act recognized the importance of information security to the economic and national security interests of the United States.
33	FISMA	Federal Information Security *Modernization* Act (2014)	Laws that assigns responsibilities within the U.S. federal government for setting and complying with policies to secure agencies’ information systems. For example, Department of Homeland Security administers cybersecurity policies and the Office of Management and Budget provides oversight.
34	FISSEA	Federal Information Systems Security Educators' Association	An organization run by and for information systems security professionals to assist federal agencies in meeting their information systems security awareness, training, and education responsibilities.
35	GRC	Governance, Risk Management, and Compliance	Three parts of a strategy for managing an organization's overall governance, enterprise risk management and compliance with regulations. Cybersecurity people, practices and tools play a key part in GRC for many organizations.
36	HTTPS	Secure Hypertext Transfer Protocol	An extension of the Hypertext Transfer Protocol. It is used for secure communication over a computer network by encrypting the information you send from your computer to another website, for example. It is a means of ensuring privacy, security and also a way of authenticating that the site you’re on is the one you intended to visit.
37	IA	Information Assurance	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.
38	IAM	Identity and access management	IAM is a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources. This helps organizations maintain “least privileged” or "zero trust" account access, where employees only have access to the minimum amount of data needed for their roles.
39	IBE	Identity-Based Encryption	A type of public-key encryption in which the public key of a user is some unique information about the identity of the user, like a user's email address, for example.
40	IDS/IDP	Intrusion Detection/Intrusion Detection and Prevention	Intrusion Detection Systems (IDS) analyze network traffic for signatures that match known cyberattacks. Intrusion Prevention Systems (IPS) analyze packets as well, but can also stop the packet from being delivered based on what kind of attacks it detects, helping to stop the attack.
41	ISACA	Information Systems Audit and Control Association	ISACA provides certifications for IT security, audit and risk management professionals. ISACA also maintains the COBIT framework for IT management and governance. ISACA was incorporated in 1969 by a small group of individuals who recognized a need for a centralized source of information and guidance in the growing field of auditing controls for computer systems. Today, ISACA serves professionals in 180 countries.

42	ISAKMP	Internet Security Association and Key Management Protocol	A protocol for establishing Security Associations and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent.
43	ISAP	Information Security Automation Program	The ISAP is a U.S. government agency initiative to enable automation and standardization of technical security operations. Its standards based design may benefit those in the private sector as well.
44	(ISC)²	International Information Systems Security Certification Consortium	A non-profit organization which specializes in training and certification for cybersecurity professionals. Certifications include the CISSP.
45	ISO	International Organization for Standardization	An organization that develops international standards of many types, including two major information security management standards, ISO 27001 and ISO 27002.
46	ISSA	Information Systems Security Association	ISSA is a not-for-profit, international organization of information security professionals and practitioners.
47	ISSO	Information Systems Security Officer	Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.
48	ISSPM	Information Systems Security Program Manager	The ISSPM, sometimes called an IT Security Manager, coordinates and executes security policies and controls, as well as assesses vulnerabilities within a company. They are often responsible for data and network security processing, security systems management, and security violation investigation.
49	JSM	Java Security Manager	To use Java security to protect a Java application from performing potentially unsafe actions, you can enable a security manager for the JVM in which the application runs. The security manager enforces a security policy, which is a set of permissions (system access privileges) that are assigned to code sources.
50	MS-ISAC	Multi-State Information Sharing and Analysis Center	The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.
51	MSSP	Managed Security Services Provider	Provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services.
52	NCS	National Cryptologic School	A school within the National Security Agency. The NCS provides the NSA workforce and its Intelligence Community and Department of Defense partners highly-specialized cryptologic training, as well as courses in leadership, professional development, and over 40 foreign languages.
53	NCSA	National Cyber Security Alliance	A non-profit working with the Department of Homeland Security, private sector sponsors, and nonprofit collaborators to promote cyber security awareness for home users, small and medium size businesses, and primary and secondary education.
54	NCSAM	National Cyber Security Awareness Month	NCSAM is a collaborative effort between government and industry to raise awareness about the importance of cybersecurity and to ensure that all Americans have the resources they need to be safer and more secure online. It occurs each year in October. The security awareness month started with a joint effort by the National Cyber Security Division within the Department of Homeland Security and the nonprofit National Cyber Security Alliance.
55	NCSD	National Cyber Security Division	A division of the Office of Cyber Security & Communications with the mission of collaborating with the private sector, government, military, and intelligence stakeholders to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of the civilian government and private sector critical cyber infrastructures.
56	NICCS	National Initiative for Cybersecurity Careers and Studies	An online resource for cybersecurity training that connects government employees, students, educators, and industry with cybersecurity training providers throughout the United States.
57	NICE	National Initiative for Cybersecurity Education	The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development.
58	NISPOM	National Industrial Security Program Operating Manual	The National Industrial Security Program Operating Manual (NISPOM) establishes the standard procedures and requirements for all government contractors, with regards to classified information. It covers the entire field of government-industrial security related matters.
59	NIST	National Institute of Standards and Technology	In cybersecurity circles, NIST is extremely well known for the NIST Cybersecurity Framework, as well the NIST Risk Management Framework (RMF), NIST 800-53 control guidance, NIST Digital Identity Guidelinesand others. The overall NIST mission is to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." NIST is part of the U.S. Department of Commerce.

60	OPSEC	Operational Security	OPSEC is a term derived from the U.S. military and is an analytical process used to deny an adversary information that could compromise the secrecy and/or the operational security of a mission.Performing OPSEC related techniques can play a significant role in both offensive and defensive cybersecurity strategies
61	SANS	SysAdmin, Audit, Network and Security	SANS Institute (officially the Escal Institute of Advanced Technologies) is a private U.S. for-profit company founded in 1989 that specialises in information security, cybersecurity training, and selling certificates. The SANS Institute sponsors the Internet Storm Center, an internet monitoring system staffed by a community of security practitioners, and the SANS Reading Room, a research archive of information security policy and research documents. SANS is one of the founding organizations of the Center for Internet Security.
62	UCF	Unified Compliance Framework	Unified Compliance Framework is one of the plugins which helps to bring data from UCF Common Controls Hub to servicenow. In Common Controls Hub all the list of authority documents will be getting imported to servicenow in the form of Authority Documents (Also known as global policies).
63	CVE	Common Vulnerabilities and Exposure	Common Vulnerabilities and Exposures (CVE) is a catalog of known security threats.The catalog is sponsored by the United States Department of Homeland Security (DHS), and threats are divided into two categories: vulnerabilities and exposures.According to the CVE website, a vulnerability is a mistake in software code that provides an attacker with direct access to a system or network. For example, the vulnerability may allow an attacker to pose as a superuser or system administrator who has full access privileges. An exposure, on the other hand, is defined as a mistake in software code or configuration that provides an attacker with indirect access to a system or network.
64	CWE	Common Weakness Enumeration	The Common Weakness Enumeration (CWE) is a community-developed register that defines software weakness types and is sponsored by the National Cyber Security Division and US Department of Homeland Security. CWE defines a buffer overflow as a failure to constrain operations within the bounds of a memory buffer (CWE-119).
65	ALE	Annual Loss of Expectancy	Annual Loss of Expectancy is one of the parameters in Risk management module of servicenow which would be calculated in the form of numeric values. Result would be coming with the formula : SLE(Single Lost of Expectancy) * ARO(Annual Rate of Occurrence) = ALE(Annual Loss of Expectancy)
66	ARO	Annual Rate of Occurrence	Annual Rate of Occurrence is one of the parameters in Risk management in servicenow which shows how many times risk occurs in a year
67	SLE	Single Lost of Expectancy	Single Loss of Expectancy is one of the parameters of Risk management in servicenow which helps to get the value of loss or any impact occurred in a year
68	NVD	National Vulnerability Database	The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP).This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references,security-related software flaws, misconfigurations, product names, and impact metrics.For information on how to the cite the NVD, including the database's Digital Object Identifier (DOI),we need to consult NIST's Public Data Repository.
69	CPE	Common Platform Enumeration	Common Platform Enumeration (CPE) is a structured naming scheme for information technology systems, software, and packages.Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.The CPE Product Dictionary provides an agreed upon list of official CPE names. The dictionary is provided in XML format and is available to the general public. The CPE Dictionary is hosted and maintained at NIST, may be used by nongovernmental organizations on a voluntary basis, and is not subject to copyright in the United States.
70	CCE	Common Configuration Enumeration	Common Configuration Enumeration (CCE) provides unique identifiers to system configuration issues in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools.

71	PCI-DSS	Payment Card Industry Data Security Standard	The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.
72	SANS	System Administration, Networking, and Security Institute	A private company that specializes in information security training and security certification.
73	SIEM	Security Information and Event Management	Security Information and Event Management (SIEM) technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual sources.
74	SOC	Security Operations Center	A central location or team within an organization that is responsible for monitoring, assessing and defending security issues.
75	SSO	Single Sign-On	A system which enables users to securely authenticate themselves with multiple applications and websites by logging in with a single set of credentials.
76	UBA/UEBA	User Behaviour Analytics	UBA tracks a system's users, looking for unusual patterns of behavior. In cybersecurity, the process helps detect insider threats, and other targeted attacks including financial fraud. User behavior analytics solutions look at patterns of human behavior, and then apply algorithms and statistical analysis to detect meaningful anomalies from those patterns. This guides efforts to correct unintentional behavior that puts business at risk and risky and intentional deceit.
77	VPN	Virtual Private Network	By connecting through a VPN, all the data you send and receive travels through an encrypted "tunnel" so that no one can see what you are transmitting or decipher it if they do get ahold of it. VPNs also allow you to hide your physical location and IP address, often displaying the IP address of the VPN service, instead.