**AAA (Authentication, Authorization, and Accounting)** - a security framework that ensures only authorized individuals are able to access resources.

**ABAC (Attribute Based Access Control)** - evaluates attributes to determine the access.

**ACL (Access Control List)** - list of rules that specifies which users or systems are granted or denied access to a particular object or system resource.

**AES (Advanced Encryption Standard)** - a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

**AIS (Automated Indicator Sharing)** - service provided by CISA that enables real-time exchange of machine-readable cyber threat indicators and defensive measures between public and private sector organizations.

**APT (Advanced Persistent Threat)** - a type of cyber attack in which an unauthorized user gains access to a system or network and remains undetected for an extended period of time.

**ARP (Address Resolution Protocol)** - a protocol used to map an IP address to a physical MAC address.

**ASLR (Address Space Layout Randomization)** - a technique used to prevent attackers from exploiting vulnerabilities in software by randomizing the location of key data areas in memory.

**BCP (Business Continuity Planning)** - detailed strategy and set of systems for ensuring an organization’s ability to prevent or rapidly recover from a significant disruption to its operations. The plan is essentially a playbook for how any type of organization—such as a private-sector company, a government agency or a school will continue its day-to-day business during a disaster scenario or otherwise abnormal conditions.

**BDPU Guard (Bridge Protocol Data Units)** - BDPU guard is a feature that defends the layer 2 STP topology against BDPU-related threats.

**BIA (Business Impact Analysis)** - the BIA should identify the operational and financial impacts resulting from the disruption of business functions and processes.

**BIOS (Basic Input/Output System)** - BIOS, or Basic Input/Output System, is software stored on a small memory chip, also known as firmware. BIOS is found on the motherboard. BIOS instructs the computer on how to perform basic functions like booting and keyboard control; it is also used to identify and configure the hardware in a computer such as the hard drive, CPU, memory, and related equipment. Finally, it manages data flow between the computer's operating system (OS) and attached devices.

**BLOB (Binary Large Object Storage)** - used by cloud providers as a database for large amounts of text or binary data.

**BPA (Business Partnership Agreement)** - agreement between 2 companies that are doing business together in which it is confirmed how much each company should contribute as well as their responsibility and how the profit will be split.

**BYOD (Bring Your Own Device)** - a policy that allows employees to use their personal devices, such as smartphones or laptops, to access company resources.

**CA (Certificate Authority)** - trusted entity that issues digital certificates used to verify the identities of individuals, organizations, websites or devices.

**CAC (Common Access Card)** - smart card about the size of a credit card. It is the standard identification for Active Duty United States Defense personnel.

**CASB (Cloud Access Security Broker)** - software/hardware that sits between users and their cloud service to enforce security policies.

**CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)** - a challenge-response test used to distinguish between human and automated users.

**CBC (Cipher Block Chaining)** - a mode of operation for a block cipher -- one in which a sequence of bits are encrypted as a single unit, or block, with a cipher key applied to the entire block. Cipher block chaining uses what is known as an initialization vector (IV) of a certain length. By using this along with a single encryption key, organizations and individuals can safely encrypt and decrypt large amounts of plaintext.

**CER (Certificate)** - security files provided and generated by an Certificate Authority. These files help a browser to verify if a website is secure and save to enter, verifying its authenticity. These CER security certificates are usually installed on a web server.

**CER (Crossover Error Rate)** - point where FAR and FRR are equal.

**CHAP (Challenge Handshake Authentication Protocol)** - challenge-response identity authentication protocol. It depends on a combination of CHAP security credentials and a “shared secret” between the requestor (client) and the authenticator (server), and it does not expose a password.

**CIA (Confidentiality, Integrity, and Availability)** - the three core principles of information security.

**CIRT (Computer Incident Response Team)** - a team responsible for responding to and mitigating cyber security incidents.

**COPE (Corporate-Owned, Personally-Enabled)** - a policy that allows employees to use company-owned devices for personal use.

**CRC (Cyclic Redundancy Check)** - a mathematical algorithm used to detect errors in data transmission.

**CRL (Certificate Revocation List)** - first phase of checking if certificate is valid.

**CSA (Cloud Security Alliance)** - non-profit organization that provides different resources to help Cloud Security Providers (CSPs).

**CSRF (Cross-Site Request Forgery)** - is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform.

**CSO (Chief Security Officer)** - a senior-level executive responsible for overseeing an organization's security program.

**CSP (cloud service provider)** - is a third-party company that provides scalable computing resources that businesses can access on demand over a network, including cloud-based compute, storage, platform, and application services.

**CSR (Certificate Signing Request)** - a request made by a user or device to a certificate authority for a digital certificate.

**CSRF (Cross Site Request Forgery)** - attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated.

**CSV (Comma Separated Values)** - a file format used to store data in a table-like format, with each row separated by a comma.

**CVE (Common Vulnerabilities and Exposure)** - list of vulnerabilities created by MITRE.

**CVSS (Common Vulnerabilities Scoring System)** - ranking of vulnerabilities and their severity.

**CYOD (Choose Your Own Device)** - company has set of devices that employees can choose to use for work.

**DAC (Discretionary Access Control)** - restricting access to objects based on the identity of subject.

**DDoS (Distributed Denial of Service)** - a type of cyber attack in which multiple systems are used to flood a target server or network with traffic, causing it to become unavailable.

**DES (Data Encryption Standard)** - is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) that was widely used in the past but is now considered insecure.

**DHCP (Dynamic Host Configuration Protocol)** - a protocol used to automatically assign IP addresses and other network settings to devices on a network.

**DMZ (Demilitarized Zone)** - a network segment that is isolated from the internal network and is used to provide public-facing services, such as web servers or email servers.

**DNS (Domain Name System)** - a system that translates domain names into IP addresses.

**DoS (Denial of Service)** - a type of cyber attack in which a server or network is overwhelmed with traffic, causing it to become unavailable.

**DPO (Data Protection Officer)** - DPO makes sure that the organization is correctly protecting individuals personal data according to current legislation.

**DRP (Disaster Recovery Plan)** - preparing for any type of disaster that could occur.

**EAP (Extensible Authentication Protocol)** - architectural framework that provides extensibility for authentication methods for commonly used protected network access technologies such as IEEE 802.1X-based wireless access, IEEE 802.1X-based wired access and Point-to-Point Protocol (PPP).

**EFS (Encrypting File System)** - a feature in Windows that allows files and folders to be encrypted using a user's public key. Windows' EFS feature allows you to easily encrypt and decrypt files on your Windows NTFS drives. Once you’ve encrypted files with this tool, other people won’t be able to access them unless they have your password.

**EMI (Electromagnetic Interference)** - interference caused by electromagnetic waves, which can disrupt the functioning of electronic devices.

**EMP (Electromagnetic Pulse)** - a burst of electromagnetic radiation that can cause damage to electronic devices.

**ESP (Encapsulating Security Payload)** - is security payload is an individual protocol in IPSec. ESP is responsible for the CIA triad of security (Confidentiality, Integrity, Availability), which is considered significant only when encryption is carried along with them. Securing all payload/ packets/ content in IPv4 and IPv6 is the responsibility of ESP.

**FAR (False Acceptance Rate)** - metric used to measure the likelihood of granting access to an unauthorized user.

**FDE (Full Disk Encryption)** - security technique that encrypts all data stored on a disk or storage device, including the operating system, applications, and user data.

**FISMA (Federal Information Security Management Act)** - FISMA requires federal agencies to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

**FRR (False Rejection Rate)** - metric used to measure the likelihood of denying access to an authorized user.

**FTP (File Transfer Protocol)** - a protocol used to transfer files between computers over a network. Port 21.

**GDPR (General Data Protection Regulation)** - regulation in European Union (EU) law on data protection and privacy for individuals within the EU and the European Economic Area (EEA). It came into effect on May 25, 2018 and is enforced by the EU Data Protection Authorities.

**GPS (Global Positioning System)** - a system of satellites used to determine the location of a device.

**GRE (Generic Routing Encapsulation)** - a protocol used to encapsulate one type of packet within another.

**GBAC (Group Based Access Control)** - gives access to a group of individuals to the resources that they need.

**HMAC (Hash-based Message Authentication Code)** - is a cryptographic authentication technique that uses a hash function and a secret key. With HMAC, you can achieve authentication and verify that data is correct and authentic with shared secrets, as opposed to approaches that use signatures and asymmetric cryptography.

**HIDS (Host Intrusion Detection System)** - HIDS stands for host-based intrusion detection system and represents an application that is monitoring a computer or network for suspicious activities.

**HIPAA (Health Insurance Portability And Accountability Act)** - federal law that was enacted in 1996 to protect the privacy and security of patients' personal health information (PHI).

**HOTP (HMAC-based One-Time Password)** - algorithm used to generate one-time passwords that are used for authentication purposes.

**HSM (Hardware Security Module)** - type of specialized hardware device designed to securely store and manage digital keys and perform cryptographic operations. It can be used to store encryption keys, digital certificates, and other sensitive data.

**HSTS (HTTP Strict Transport Security)** - web security policy mechanism used to protect against protocol downgrade attacks and cookie hijacking.

**HTML (Hypertext Markup Language)** - is the standard markup language for creating Web pages.

**HTTP (Hypertext Transfer Protocol)** - HTTP is the foundation of the World Wide Web, and is used to load webpages using hypertext links. HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack. A typical flow over HTTP involves a client machine making a request to a server, which then sends a response message. HTTP uses port 80.

**HTTPS (Hypertext Transfer Protocol Secure)** - a secure version of HTTP that uses encryption to protect data in transit. HTTPS uses port 443.

**IaaS (Infrastructure as a Service)** - a cloud computing model in which infrastructure resources, such as servers and storage, are provided by a third-party provider.

**IAM (Identity and Access Management)** - a cybersecurity practice that enables IT administrators to restrict access to organizational resources so that only the people who need access have access.

**ICMP (Internet Control Message Protocol)** - a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner.

**IDS (Intrusion Detection System)** - a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, a security operations center (SOC) analyst or incident responder can investigate the issue and take the appropriate actions to remediate the threat.

**IPS (Intrusion Prevention System)** - a network security technology that goes beyond the capabilities of an IDS (Intrusion Detection System) by actively preventing identified threats from being carried out. An IPS monitors network traffic, just like an IDS, but it can also take action to prevent attacks.

**IEEE (Institute of Electrical and Electronics Engineers)** - The IEEE describes itself as the world's largest technical professional society -- promoting the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of our members.

**IKE (Internet Key Exchange)** - a standard protocol used to set up a secure and authenticated communication channel between two parties via a virtual private network (VPN).

**IMAP (Internet Message Access Protocol)** - an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection. IMAP uses port 143.

**IoT (Internet Of Things Devices)** - physical devices that are connected to the internet and that can exchange data with each other.

**IP (Internet Protocol)** - a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.

**IPv4 (Internet Protocol version 4)** - an IPv4 address is a 32-bit address that is usually represented in dotted decimal notation, with a decimal value representing each of the four octets (bytes) that make up the address.

**IPv6 (Internet Protocol version 6)** - a network protocol that serves as the successor to IPv4. The purpose of IPv6 is to provide a larger address space for the internet as the number of connected devices continues to grow. One of the main differences between IPv6 and IPv4 is the size of the address space. IPv4 uses 32-bit addresses, allowing for approximately 4.3 billion unique addresses. In contrast, IPv6 uses 128-bit addresses, which allows for an almost unlimited number of unique addresses.

**ISA (Interconnection Security Agreement)** - a document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities.

**ISO (International Organization for Standardization)** - an international standard-setting organization.

**ISP (Internet Service Provider)** - a company that provides Internet access to customers.

**JSON (JavaScript Object Notation)** - a lightweight data interchange format.

**LDAP (Lightweight Directory Access Protocol)** - is a software protocol for enabling anyone to locate data about organizations, individuals and other resources such as files and devices in a network -- whether on the public internet or a corporate intranet. LDAP is a "lightweight" version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network. LDAP is considered lightweight because it uses a smaller amount of code than other protocols.

**MAC (Media Access Control)** - a unique identifier assigned to a network interface controller (NIC).

**MAC (Mandatory Access Control)** - limiting access to resources based on the sensitivity of information.

**MCSP (Managed Cloud Service Provider)** - provides managed cloud services to customers. Managed cloud services are a type of cloud computing service in which a third-party provider manages and delivers cloud computing resources and services to customers over the internet.

**MFA (Multi-Factor Authentication)** - a security feature that requires multiple forms of authentication to access a resource.

**MITB (Man In The Browser)** - an MITB attack injects malicious software (malware) into a victim's web browser. The malware typically exploits vulnerabilities in the browser or its plugins to intercept and manipulate data exchanged between the browser and the websites the user visits.

**MITM (Man-in-the-Middle)** - a type of cyber attack in which an attacker intercepts communications between two parties in order to either steal or change the data in transit.

**MSSP (Managed Security Service Provider)** - provides managed security services to customers, typically on a subscription basis.

**MTBF (Mean Time Between Failures)** - average amount of time between system failure which shows how reliable a system is.

**MTTD (Mean Time To Detect)** - average time it takes for an organization to detect a security incident or breach after it occurs.

**MTTR (Mean Time To Repair)** - average time that it takes to fix a system.

**NAC (Network Access Control)** - a system used to control access to a network based on the identity of the user or device.

**NAT (Network Address Translation)** - a technique used to map private IP addresses to public IP addresses.

**NDA (Non Disclosure Agreement)** - contract that prevents any side of the business to give away the secrets to others.

**NFC (Near Field Communication)** - short-range wireless communication technology that enables data exchange between devices that are within close proximity to each other, typically within a few centimeters.

**NIDS (Network Intrusion Detection System)** - a system used to detect unauthorized activity on a network.

**NIPS (Network Intrusion Prevention System)** - type of security system that is used to detect and prevent unauthorized access, attacks, and other malicious activity on a network.

**NIST (National Institute of Standards and Technology)** - a U.S. government agency that develops standards for technology and engineering.

**NTFS (New Technology File System)** - a file system used in Windows operating systems.

**OAuth (Open Authorization)** - open standard protocol that is used for authorization and authentication between applications or services. It allows users to grant access to their private resources stored on one website to another website or application, without sharing their credentials, such as passwords.

**OCSP (Online Certificate Status Protocol)** - a protocol used to check the validity of a digital certificate.

**OSI (Open Systems Interconnection)** - conceptual framework that is used to standardize and describe the communication functions of a telecommunication or computing system. The OSI model is divided into seven layers, each with a specific function, that define the communication process between two devices in a network.

**PaaS (Platform as a Service)** - a cloud computing model in which a third-party provider offers a platform for developing and deploying applications.

**PAM (Privileged Access Management)** - type of security solution that helps organizations manage and control access to privileged accounts and systems.

**PCI DSS (Payment Card Industry Data Security Standard)** - a set of security standards for protecting credit card data.

**PGP (Pretty Good Privacy)** - an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

**PMF (Protected Management Frames)** - security feature used in Wi-Fi networks to protect against certain types of attacks that can be carried out against wireless management frames.

**POP3 (Post Office Protocol version 3)** - a protocol used to retrieve email messages from a mail server.

**PPP (Point-to-Point Protocol)** - a protocol used to establish a direct connection between two devices.

**RAID (Redundant Array of Inexpensive Disks)** - a technique used to increase the reliability and performance of data storage.

**RADIUS (Remote Authentication Dial-In User Service)** - networking protocol that is used to provide centralized authentication, authorization, and accounting (AAA) management for users who connect and use network services. RADIUS is commonly used in enterprise and service provider environments, such as Wi-Fi networks, virtual private networks (VPNs), and dial-up services.

**RAM (Random Access Memory)** - computer's short-term memory, where the data that the processor is currently using is stored. Your computer can access RAM memory much faster than data on a hard disk, SSD, or other long-term storage device, which is why RAM capacity is critical for system performance.

**RAT (Remote Access Trojan)** - a type of malware that allows an attacker to remotely control a victim's computer.

**RDP (Remote Desktop Protocol)** - a protocol used to remotely access and control a desktop computer.

**REST (Representational State Transfer)** - software architectural style that describes the architecture of the web.

**RFID (Radio Frequency Identification)** - a technology used for tracking and identifying objects using radio waves.

**RIPEMD (RACE Integrity Primitives Evaluation Message Digest)** - a cryptographic hash function.

**RTO (Recovery Time Objective)** - the maximum amount of time it takes to recover data after a disaster.

**RTOS (Real Time Operating System)** - an operating system commonly found in Internet of Things Devices.

**RBAC (Rule Based Access Control)** - high level rules that determine how, where and when employees can access spaces or resources.

**S/MIME (Secure/Multipurpose Internet Mail Extensions)** - standard for secure email messaging that provides encryption and digital signing capabilities.

**SAN (Storage Area Network)** - specialized, high-speed network that provides network access to storage devices. SANs are typically composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols.

**SaaS (Software as a Service)** - a cloud computing model in which a third-party provider offers software applications.

**SAE (Simultaneous Authentication of Equals)** - key exchange protocol that provides stronger security and that replaced PSK in WPA2.

**SATCOM (Secure Satellite Communications)** - refers to the use of satellite technology for communication purposes, including voice, data, and video transmission.

**SCADA (Supervisory Control and Data Acquisition)** - a system used to control and monitor industrial processes.

**SCP (Secure Copy Protocol)** - a protocol used to securely transfer files between two devices.

**SFTP (Secure File Transfer Protocol)** - a protocol used to securely transfer files between two devices.

**SHA (Secure Hash Algorithm)** - SHA stands for secure hashing algorithm. SHA is a modified version of MD5 and used for hashing data and certificates. A hashing algorithm shortens the input data into a smaller form that cannot be understood by using bitwise operations, modular additions, and compression functions.

**SID (Security Identifier)** - a unique identifier used to identify a user or group in Windows operating systems.

**SIEM (Security Information and Event Management)** - type of security solution that provides real-time analysis of security alerts and events generated by network hardware and applications.

**SMTP (Simple Mail Transfer Protocol)** - a protocol used to send email messages between servers.

**SNMP (Simple Network Management Protocol)** - a protocol used to manage and monitor network devices.

**SOAR (Security Orchestration, Automation and Response)** - security technology that helps organizations automate and streamline their security operations and incident response processes.

**SoC (System on Chip)** - integrated circuit (IC) that combines various components of a computer or electronic system into a single chip.

**SQL (Structured Query Language)** - a programming language used for managing and manipulating data in relational databases.

**SSH (Secure Shell)** - a protocol used for secure remote access to a device. Uses Port 22.

**SSL (Secure Sockets Layer)** - SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol. It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern TLS encryption used today. A website that implements SSL/TLS has "HTTPS" in its URL instead of "HTTP".

**STP (Spanning Tree Protocol)** - a protocol used to prevent loops in a network topology.

**STIX (Structured Threat Information Exchange)** - designed to support the sharing of cybersecurity threat intelligence between different organizations and cybersecurity technologies.

**TACACS+ (Terminal Access Controller Access Control System Plus)** - protocol used for providing centralized authentication, authorization, and accounting (AAA) services for network devices such as routers, switches, and firewalls.

**TAXII (Trusted Automated Exchange of Indicator Information)** - application protocol for exchanging Cyber Threat Intelligence over HTTPS. It works with STIX.

**TCP (Transmission Control Protocol)** - a protocol used to establish a reliable connection between two devices. Uses three way handshake.

**TOTP (Time Based One Time Password)** - TOTP uses a timestamp and a time-based factor to generate the password. Specifically, TOTP calculates the message authentication code based on the current time and a time interval (usually 30 seconds).

**TPM (Trusted Platform Module)** - chip on motherboard that can be used to store critical information such as encryption keys. TPM can be used for FDE (Full Disk Encryption).

**UBA (User Behaviour Analysis)** - checks whether user activity sticks out from their usual activity.

**UDP (User Datagram Protocol)** - a protocol used for sending datagrams over a network. Connectionless.

**UEFI (Unified Extensible Firmware Interface)** - modern version of BIOS. UEFI can be used for securely starting a device.

**URL (Uniform Resource Locator)** - a unique identifier used to locate a resource on the Internet. It is also referred to as a web address.

**VLAN (Virtual Local Area Network)** - a logical grouping of devices on a network that are grouped together based on factors such as function, department, or location, rather than physical location.

**VM (Virtual Machine)** - a software environment that emulates a physical computer.

**VPN (Virtual Private Network)** - a virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

**VTP (VLAN Trunking Protocol)** - proprietary protocol used by Cisco switches to exchange VLAN information. With VTP, you can synchronize VLAN information (such as VLAN ID or VLAN name) with switches inside the same VTP domain.

**WAF (Web Application Firewall)** - firewall used to protect web applications.

**WAP (Wireless Access Point)** - network device that receives and transmits data over WLAN.

**WEP (Wired Equivalent Privacy)** - wired equivalent privacy is meant to protect Wi-Fi transmissions by encrypting the data so outsiders who are not inside the encrypted network will not be able to read the messages or data contained within. WEP is better than no security at all, and it is still used on older devices that do not support WPA or WPA2.

**WIDS (Wireless Intrusion Detection System)** - a system used to detect unauthorized access to a wireless network.

**WPA (Wi-Fi Protected Access)** - a security protocol used for wireless networks. There is WPA, WPA2, WPA3.

**X.509** - a standard for public key certificates used for authentication in network communication.

**XML (Extensible Markup Language)** - a markup language used for encoding documents in a format that is both human-readable and machine-readable.

**XSS (Cross-Site Scripting)** - a type of attack in which an attacker injects malicious code into a web page viewed by other users. Usually this code is javascript code. There are 3 main versions of XSS: DOM Based, Stored and Reflected XSS.