CASP+ Course Glossary

This glossary corresponds to the key definitions that are introduced in each lesson. You can reference all of the definitions here in one place as a supplementary study guide.

Numbers

2-Step Verification

An authentication method that uses out-of-band mechanisms and generates a token serverside that is sent to the user to provide for verification. This might be an SMS message with a code, a phone call, a push notification to a mobile phone, or an email.

3D Printing

An emerging technology that uses special-purpose printers that build 3D objects rather than printing on paper. Printing is done by adding layers on top of layers according to a model using computer-aided design (CAD) software. It allows for rapid design and the creation of just about anything.

802.1x

An authentication protocol that uses EAP for wireless, ethernet, or VPN gateway to provide authentication.

A

Access Control List (ACL)

A broad term that outlines how objects are allowed to interact with each other on a network or system. In networking, devices like switches or routers may grant or deny access based on their own ACLs. Similar to a firewall, it helps filter and route traffic.

Access Space Layout Randomization (ASLR)

A buffer overflow prevention control that makes it difficult to guess the memory locations of executables stored in memory.

Accreditation (of a system)

The system owner's agreement and acceptance of the claim that the system is certified.

Advanced Persistent Threat (APT)

A type of adversary group that is typically a nation-state threat actor with extensive resources and sophisticated tools and personnel.

Adversary Emulation
A discipline in cybersecurity that involves using known TTPs (tactics, techniques, and procedures) of a specific threat actor in a realistic way to test current defenses.

Agile Model
In this approach to software development, an iterative process is used to release well-tested code in smaller blocks. Development is continuous. It is adaptive to allow for changes throughout the process. It focuses on rapid development, sometimes at the expense of security.

Air Gap
A host that is physically disconnected from any network so as to protect that network by being segmented from it. (This is a form of segmentation.)

Aircrack-ng
A suite of tools for assessing and analyzing Wi-Fi networks. It is used to monitor, attack, test, and crack WiFi networks.

Analytical Zone
A form of cloud-based data zone where data is used for practical purposes.

Annual Loss Expectancy (ALE)
The total cost of all the single loss events that happen over the course of a year - added together. ALE = SLE X ARO.

Annual Rate of Occurrence (ARO)
The number of times in a year that a single loss event occurs.

Anonymization
A process that removes data that could be used to uniquely identify a person. It is a common requirement in compliance laws.

Antivirus Software
Software that detects and identifies malicious software on an endpoint. Originally, antivirus programs were signature-based file scans that would detect viruses, but now they monitor when processes are launched, intercept them, and look for signature matches.

API CASB Configuration
A configuration of CASB (Cloud Access Security Broker) where an API brokers connections between the cloud provider and the customer.

Application Virtualization
A client accesses an application hosted on a server. This usually occurs through a browser. It allows for specific apps to be shared from a single server through a user's browser. Examples: App-V, XenApp, ThinApp.

Artificial Intelligence
The science of creating computing systems that can simulate or demonstrate intelligence levels similar to humans. Machine learning uses algorithms to parse data then develops strategies for using that data. Machine learning can modify the algorithms and make gradual improvements in its ability to make decisions.

Asset Reporting Format (ARF)
A SCAP language that correlates reporting formats to device information.

Asset Value
Within Quantitative Risk Analysis, this is the value that a given asset is worth.

Attestation of Compliance
The set of policies, contracts, and standards between two entities that have been designated as essential. It will identify how the relationship will be governed, including how incidents will be reported and addressed, the use of independent auditors, data protection requirements, and violation agreements.

Attribute-Based Access Control (ABAC)
An access control method that is fine-grained, as it can utilize a combination of any attributes to determine a user's access level. Uses eXtensible Access Control Markup Language (XACML).

Authentication Bypass
An attack that exploits how logins are received and processed by web applications. An example would be sending an SQL string rather than the login credentials the app is expecting.

Autoscaling
A method of automation in a cloud deployment that dynamically adjusts the allocated resources based on the current need.

AWS CloudTrail
An audit logging service for AWS apps.

AWS CloudWatch
A graphical reporting and analytics service that provides monitoring and alerting in AWS.

B

BGP/Route Hijacking

An attack that involves hijacking BGP routing. BGP is the routing protocol of the Internet. It was designed when security wasn't a consideration, so it depends on interconnected networks to truthfully and accurately maintain the routing tables.

Big Data
Data collections that are too big for traditional database tools to utilize. Ideally suited to AI as the larger the dataset for AI to study, the more effective it will be.

Binwalk
A tool that can be used to inspect binary firmware image files to better understand what is inside the file itself.

BIOS
Basic Input/Output System - this is the program that starts a computer system after it is turned on.

Blob Storage
A cloud-based storage model that supports the storage of large amounts of unstructured data. It is used to store archives and backups.

Block Cipher
An encryption where plaintext is separated into equal-sized blocks, usually 128 bits in size. If there isn't enough data to fill a block, it is padded to make up the rest of the space. Each block is then encrypted based on the mode of operation being used.

Block Storage
A cloud-based storage model that supports high-performance, transactional apps like databases.

Blockchain
An expanding list of transnational records secured by cryptography. Each record is known as a block and the blocks are connected in a chain. Each block is hashed and the hash value of the previous block is included with it. In this way, each block validates the next block in the chain. It is a public ledger that is distributed across a P2P network.

Bluetooth
A short-range wireless communication technology. It can be used to create wireless personal networks (WPANs). It is most often used to connect keyboards, mice, headsets, etc. It is vulnerable to several attacks, but the most dangerous is the BlueBorne attack, which allows for complete control of the device by the attacker and does not require the attacker to be connected to the victim device.

Bootstrapping
A method of automation in a cloud deployment that involves automatically deploying instances.

Bring Your Own Device (BYOD)
A mobile device policy where the employee owns the device, but the device must meet certain corporate specifications and allow auditing. With this type of policy, it is not as easy to fully secure devices as when they are corporately owned and issued by the company to the employee.

Broken Authentication
When an app doesn't protect authentication mechanisms, it allows an attacker to compromise user sessions or passwords.

Browser Extensions
Additional functionality that can be added to a browser. They are not accessible by the code launched by the browser. Plugins can be called by website code.

Buffer Overflow
The process of filling temporary memory space. A well-designed attack can access other parts of the system memory for code insertion and execution.

Business Continuity and Disaster Recovery (BCDR)
This is typically a plan that organizations put in place to deal with unexpected situations that occur and can threaten an organization's operations and/or data and other resources. Cloud technology has become a critical part of BCDR plans due to the capability it provides to expand resources elastically when needed (scaling) and back up resources in case of failure.

Business Continuity Plan (BCP)
A plan for how a business will continue delivering products and services at an acceptable level following an incident. Includes conducting response plans, evaluation activities, and plan maintenance.

Business Impact Analysis
A process of defining the types of risk an organization will likely face and how it will likely impact the business.

Business Impact Assessment (BIA)
An assessment that is performed to determine whether and how cloud resources should be used in an organization.

Bytecode
A type of software code that represents an intermediary state of source code created by a high-level language (when compiled) and is designed to be processed by an interpreter on the target system. The interpreter translates the bytecode into machine code.

C

Caching
A form of scaling that involves making copies of data that either doesn't change or doesn't change often. This improves performance with load times.

Capability Maturity Model Integration (CMMI)
Five levels of maturity in the operational or software capabilities of an organization. Most commonly used for federal contracts. The levels are: Level 1 - Initial; Level 2 - Managed; Level 3 - Defined; Level 4 - Quantitatively Managed; and Level 5 - Optimizing.

Certificate Authority
An entity that is responsible for issuing and then guaranteeing certificates. They provide certificate services to a community of users. They ensure that certificates are valid and that the identity of those applying for certificates is also valid. They perform key and certificate life cycle management, including revoking invalid certificates.

Certificate Errors
A class of vulnerability involving improperly configured certificates. Certificates are a necessary part of SSL encryption. If improperly configured certificates can cause browser viewable errors. This can train users to simply click past the error.

Certificate Pinning
A technique to ensure that when a client inspects a certificate, it is inspecting the proper certificate. Due to chains, there could be many certificates and if one of these were swapped out with a malicious certificate, it could compromise traffic.

Certificate Revocation List (CRL)
From time to time, certificates will need to be revoked. Reasons include the certificate being compromised, the user is no longer with an organization, a domain name change, or others. CAs maintain a list of certificates that have been revoked or suspended. This is sent throughout the organization so that the revoked certificates are no longer accepted.

Certificate Signing Requests (CSRs)
CSRs are created on any device that is requesting a certificate from a CA. Contains the information that the CA will need to generate the certificate.

Certificate Stapling
Web servers will periodically obtain OCSP responses that are time-stamped. When clients submit an OCSP request, the web server sends the time-stamped response.

Certification (of a system)

A formal process is used to assure a system owner that a complicated technology solution is configured in a secure manner.

Chain of Custody
In forensics, this is the record of evidence handling from collection through presentation in court.

Children's Online Privacy Protection Act (COPPA)
US federal law that is designed to protect the privacy of children under the age of 13 in and out of the US. It requires notice of when consent is needed and protection of the children's data from marketing.

Choose Your Own Device (CYOD)
A mobile device policy that is similar to COPE, but the employee is allowed to choose the type of device from an approved list.

Cipher Block Chaining (CBC)
A cipher mode of operation that is very simple and shouldn't be used.

Client Authentication
Digital certificates can be used to validate that a client is authorized to connect to a server.

Cloud Access Security Broker (CASB)
An enterprise management tool to mediate access to cloud services by users of all types of devices. Examples: Blue Coat, SkyHigh Networks, Microsoft Cloud App Security. CASBs provide visibility into how clients and nodes are using cloud resources.

Cloud Native Key Management System
This is a situation where the Key Management System (KMS) for encryption keys is operated by the same company that provides the cloud services.

Cloud Security Alliance (CSA) Security Trust and Risk (STAR) certification
This is a third-party assessment of the ability of a Cloud Service Provider (CSP) to adhere to key principles of transparency, auditing, and best practices for security. It measures the security capabilities and privacy controls of a cloud service provider against the CSA Cloud Controls Matrix (CCM).

Cloud Service Provider (CSP)
A company that provides cloud services with varying levels of management and resources available. Examples are AWS, Microsoft Azure, and Google Cloud.

Cloud Service Using External KMS
In this case, the Key Management System (KMS) hardware may be used by the customer and is exclusively used by the customer, but the KMS is not operated by the cloud provider being used.

Clustering
A type of resiliency that involves grouping servers together to distribute workload and allow for failover.

Code Signing
Executables, drivers, applications can all be signed with a certificate (key) issued by a trusted certificate authority (CA). Code signing certificates are issued to software developers so that software can be proven to come from a trusted source.

Command Injection
An attack that takes advantage of web apps that bypass operating system APIs and instead will spawn command shells.

Committee of Sponsoring Organizations of the Treadway Commission (COSO)
A group of five private sector organizations that developed a framework called the Enterprise Risk Management - Integrated Framework.

Common Configuration Enumeration (CCE)
Similar to CVE, but it focuses on configuration issues that may lead to a vulnerability.

Common Platform Enumeration (CPE)
A standardized naming format to identify systems and software.

Common Vulnerabilities and Exposures (CVE)
A list and reference system for all the known, publicly disclosed information security vulnerabilities and exposures. Each item in the list is given a CVE identifier. This list is maintained by the MITRE Corporation.

Common Vulnerability Scoring System (CVSS)
A rating system for the severity of a vulnerability. It uses a scale from 0-10 where 0 is Informational and 10 is Critical.

Community Cloud
A cloud deployment model where several organizations share the cost of a hosted private or totally private cloud.

Configuration Management Database (CMDB)
A database that contains information on the assets and components of the enterprise's IT infrastructure.

Conntrack
A tool that allows for interactions with connection tracking systems and can read data from IPTables.

Containerization
Also known as operating system-level virtualization, this is a virtualization method that uses a system's kernel instead of a hypervisor. It creates a virtual environment with the bare minimum needed parts for an app to run. There are performance benefits to this method due to not needing a hypervisor. Example: Docker.

Containerization of Mobile Devices
Divides the device into profiles. One container profile can be for work purposes while the other can be for personal needs. These containers are isolated from each other and apps on one cannot access the other. Data Loss Prevention can also make sure that tagged data cannot be moved to non-approved containers on the device.

Content Delivery Network (CDN)
An architecture of geographically distributed servers that serve the same content. It allows for content consumers to receive web content sooner, based on the fact that servers are located closer to them. This represents a horizontal form of scaling that allows additional servers to deliver the same content.

Content Management System (CMS)
A system that enables non-technical users to create and publish content to a website. Examples: WordPress, Sharepoint.

Continuous Delivery
This software delivery practice calls for delivering software in short cycles and testing the infrastructure that supports the app, networks, databases, client software, and security as part of delivery.

Continuous Deployment
This software delivery practice utilizes configuration management tools to make changes to a production environment through automated deployments.

Continuous Integration
This software delivery practice requires that DevOps automates the integration of code changes and commits and tests updates often.

Continuous Validation
This software delivery practice involves monitoring and evaluating feedback from delivery and development to ensure goals are meeting user needs.

Control Objectives for Information and Related Technologies (COBIT)
A framework created by ISACA that frames risk according to the leadership of a business organization. The five components are framework, process descriptions, control objectives, management guidelines, and maturity models.

Control Plane
A type of SDN plane that decides on traffic priority, security, and where switching occurs.

Controller Area Network (CAN)
A vehicle bus standard that allows microcontrollers and devices to communicate with each other's applications. Cars and unmanned aerial vehicles rely on this type of electronics to control engine and power systems, braking and landing, suspension, and stability of the vehicles. Each of these subsystems is included in an electronic control unit (ECU) connected to one or more CAN serial communications buses.

Corporate Owned Device
A mobile device policy where the employer owns and issues the mobile device to the employee, who can only use it for corporate matters.

Corporate Owned, Personally Enabled (COPE)
A mobile device management policy where the device is owned and supplied by the corporation but the employee has personal access to email and social media within acceptable use policies.

Counter (CTR)
A cipher mode of operation that applies an Initialization Vector (IV) and an incrementing counter value to the key to create a keystream. It does not require padding, and the left-over space is removed.

Course of Action Orchestration
A type of resiliency that involves automated responses to specific events.

Cross-Site Request Forgery (CSRF)
This attack causes a victim to unintentionally make changes to their account in a web app, thereby giving the attacker access to their account.

Cross-Site Scripting (XSS)
Similar to directory traversal, XSS is a vulnerability that manipulates the file paths to control how a web app operates.

Cryptanalysis
The art of breaking encryption. In certain forensics situations, this may be a requirement if collected data is encrypted.

Crypto Erase
A method of data sanitization that involves removing the key necessary to decrypt the data.

Custom DNS
Since DNS (domain name service) is unencrypted, this type of DNS uses third-party servers to filter malicious DNS requests.

Customer Relationship Management (CRM)
An application and service that contains customer information, sales, communications, and many other sensitive items (example: Salesforce).

Cyber Kill Chain
A model developed by Lockheed Martin that describes the steps an adversary typically takes to achive their goals. It includes: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives.

Cybersecurity Maturity Model Certification (CMMC)
A certification developed by the U.S. Department of Defense to ensure DoD suppliers prove they have mature cybersecurity capabilities and practices.

D

Dark Web Scanning
A practice of looking through the Dark Web for signs of data loss as part of data loss prevention (DLP).

Data at Rest
The state of data when it is stored in databases and other areas.

Data Dispersion
Intentionally spreading data across multiple storage locations and/or cloud providers to ensure that data is safe and available.

Data Distribution Service (DDS)
A machine-to-machine standard that enables the interoperability of networks for machines for the purposes of scalability, performance, and Quality of Service (QoS). It supports cloud and on-premises scenarios, automated orchestration for all connected components.

Data in Transit
The state of data when it is in motion, moving from one place to another.

Data in Use
The state of data when it is in volatile memory (system RAM, CPU registers, cache). Example: Fields in a database while the data is being updated.

Data Integrity Management
Ensures that data is in its proper state and that any changes that occur can be identified. This ensures data reliability.

Data Life Cycle
The life cycle of a given piece of data's existence, including the phases Creating, Storing, Using, Archiving, and Destroying data.

Data Loss Prevention (DLP)
Software that works to prevent sensitive data from being copied, used, or transmitted improperly. It helps protect against insider threats. It can be configured to block printing of sensitive information. DLP also automates the discovery and classification of data and then enforces rules to ensure the data is not viewed or released improperly.

Data Ownership
The data owner is the entity that is responsible for protecting the data under their control. They are responsible for ensuring the data has been protected in appropriate ways.

Data Plane
A type of SDN plane that handles switching and routing of traffic, as well as ACLs.

Data Sanitization
Removing data from media using the methods of clear, purge, or doing damage to the hardware. It includes removing all labels, markings, and logs. The clear method involves multiple block-level over-writing of data that protects against recovery except in clean rooms. The purge method involves protecting against all recovery methods including clean rooms. The damage method involves physically breaking the storage medium to make it useless.

Data Sovereignty
The laws in the country where the data is stored that govern data collection and its use in the global economy. Regulations vary widely and these can impact how data is stored, transmitted to another country, and what type of encryption must be used to protect it.

Data Zones
A form of cloud-based network segmentation that describes the state and location of data to isolate and protect it.

dd
A Command line tool for making forensic copies of block-level storage. Copies at the block level rather than file level.

Decoy Files
Files that would be appealing to an attacker but are monitored for signs of access: honeytokens.

Deep Learning
A type of machine learning that takes apart knowledge and breaks it into smaller parts. Complex topics can be broken down into parts that are easier to interpret. A deep learning system can decide which parts are applicable to a given problem and make decisions based upon them. IBM's Watson is a good example of this in action.

Deep Packet Inspection
A practice of looking into data traffic for specific content that could be sensitive as part of data loss prevention (DLP).

Deep Web
The parts of the web that are not indexed and are generally hidden. It includes the Dark Web.

Denial-of-Service/Distributed Denial of Service (DOS/DDoS)
Attacks that affect a site's or service's availability by sending too much data for a device to process.

Dependency Management
Evaluating vulnerabilities in third-party libraries and components of software and hardware.

Deperimeterization
Until recently, networks were like castles, and their defenses were set up to trust anything inside the perimeter and nothing outside of it. However, with the advent of remote work, cloud adoption, and the need for 24/7 access to data, the concept of just protecting the perimeter is eroding.

Development Environment
In software development, this is the environment that is used in the early stages of development by individual developers. Like the developer's personal sandbox.

DevOps Pipeline
A set of automated processes and tools that allows developers and operations professionals to collaborate on building and deploying code to a production environment.

Diameter
An authentication protocol that improves upon RADIUS. It is TCP-based, requires IPSec and TLS for confidentiality. Diameter is considered "twice" as good as RADIUS.

Diamond Model of Intrusion Analysis
Under this model, an adversary achieves goals by using capabilities over infrastructure against a victim.

Digital Certificate
Public assertion of identity validated by a Certificate Authority (CA). Can be used for signing messages, encrypting web server communications. Often used to prove and guarantee the identity of a website, assuming that the certificate provider is trustworthy

Digital Rights Management (DRM)
A method for controlling how digital content is used after being published so as to prevent copying.

Directory Services
A directory of all the resources within a network. Example: Active Directory.

Directory Traversal
Also known as file path traversal, is a web server vulnerability that allows access to files outside of the web document directory.

Disaster Recovery Plan
A part of the overall business continuity plan that focuses on the immediate needs of a specific event and how to recover critical systems.

Discretionary Access Control (DAC)
An access control method where the resource owner determines who has access. It is the most flexible method and is used by default in Unix/Linux and Windows. It is also the weakest model because it requires centralized administration that is difficult to enforce. It is vulnerable to insider threats and compromised account abuse.

Distributed Allocation
A type of resiliency that involves spreading workloads across multiple units that work together.

Distributed Consensus
An emerging technology that is a distributed/decentralized system where all systems come to an agreement for a specific computation to maintain the overall integrity fo a distributed

system. It includes the possibility that some systems are malicious so it takes a vote from all included systems on the data. The value with the most votes is accepted.

DNS over HTTPS
To secure DNS requests, they are tunneled over an HTTPS connection using TLS to encrypt the DNS requests. However, this can cause issues because organizations can no longer see requests leaving their network, and malware can use this situation to hide itself.

Domain Name System (DNS)
A system that associates each domain to a host IP address.

Due Care
What is considered to be the reasonable and expected protections of an asset. this is a baseline and will vary widely based on what is being protected. Also called the "prudent man rule."

Due Diligence
The ongoing and documented processes to continuously evaluate and improve the ways we protect data.

Dynamic Analysis
A type of vulnerability analysis that involves an evaluation of software or a system while it is running.

Dynamic Application Security Testing (DAST)
Reviewing code while it is running and used as a final product.

Dynamic Network Configurations
Network configurations that can be redeployed after an attack is noticed so as to contain the threat.

E

e-Discovery
Identifying, collecting, and providing the Electronically Stored Information (ESI) that is identified in a Legal Hold.

Electronic Codebook (ECB)
A cipher mode of operation that is simple and shouldn't be used.

Enable No Execute (NX)/Execute Never (XN bit)
A setting in CPUs to keep areas of memory separated, designated for instructions or data.

Endpoint Detection and Response (EDR)
A centralized managed solution, usually from a cloud portal, that monitors many systems at once looking for malicious activity across them all. It uses artificial intelligence (AI) and machine learning to monitor user and system behaviors. By watching all devices in context, a more realistic assessment can be performed. Responses are automated.

Enterprise Resource Planning (ERP)
Monitors the day-to-day operations of an enterprise and can provide reports on resources and activities.

Enterprise Risk Management Integrated Framework
A risk management framework developed by COSO that defines a risk management approach for strategic leadership.

Enterprise Service Bus (ESB)
A middleware app that integrates communications between apps in an enterprise.

ExifTool
A tool to read/write file metadata for many file formats.

Exploit Framework
A collection of tools for exploiting systems and software. Examples: Metasploit, PowerShell Empire.

Exposure Factor
Within Quantitative Risk Analysis, this is the portion of an asset that would be lost given a certain bad thing happening; in other words, the percentage of the asset lost. For example: how much of an office building would be damaged if a hurricane hit it. That would be its exposure factor.

Extensible Authentication Protocol (EAP)
A framework for deploying different kinds of authentication protocols and systems. It mostly uses digital certificates rather than passwords to establish trust.

Extensible Configuration Checklist Description Format (XCCDF)
A SCAP language that is written in XML and provides a consistent way to define benchmarks and checks performed during assessments.

External Key Origination
This is a situation where the Key Management System (KMS) for encryption keys is not operated by the cloud provider being used.

F

False Negative
Something not identified as an issue, but it is an issue.

False Positive
Something that is not an issue but was identified as one.

Federation
Trusting accounts made and used by other organizations. This allows these organizations to connect across each other. Examples: using your Google ID to log into other sites/applications.

Field Programmable Gate Array (FPGA)
A controller that can have its program logic configured to run specific applications.

File-based storage
A cloud-based storage model that consists of a hierarchical file system that stores files by path and includes attributes like owner and access permissions.

File Integrity Monitoring (FIM)
A type of activity monitoring that ensures key files have not been altered.

foremost
A Linux utility used to extract deleted or corrupted data from a partition. Even if there is no file system in place, data can be recovered.

Forged Code Signing
This is a cyber-attack where forged digital certificates are used in order to bypass malware detection. The Stuxnet breach involved forged code signing.

Forward Proxy
A configuration of CASB where the appliance is at the network edge of the customer and traffic is directed to the cloud network if policies allow.

Fuzzing
Purposely injecting malformed data into an application to see if the application will reveal sensitive data.

G

Galois/Counter Mode (GCM)
A cipher mode of operation that has high performance and provides authenticated encryption. This is widely adopted.

Gap Analysis
A measure of the difference between the current state and the desired state. By creating metrics such as ALE, MTTR, MTBF, and TCO, an organization can evaluate where they stand and make improvements.

General Data Protection Regulation (GDPR)
A regulation that enforces privacy rules for organizations that offer services to entities within the European Union (EU) or that collect/analyze data on subjects in the EU. It doesn't matter where the requesting organization is located or where the data is stored. If the data is on subjects in the EU, then it is covered by this regulation.

Ghidra
A free and open-source tool developed by the NSA, written in Java, that is used for reverse engineering.

GNU Project Debugger
A tool used to identify what is occurring in an application while it is running.

Graph Cloud Storage Database
Supports millions of relationships between highly connected datasets (social media, for example)

Guest Environment
A guest network that is completely isolated from the main network.

H

Hacktivists
Hackers who use cyber attacks to support a political agenda. They may target corporations for their actions or social stances. Example: Anonymous.

Hardening
The process to remove unnecessary elements from a system and make configuration changes to make a system less vulnerable.

Hardware Root of Trust (RoT)
Trust anchor, a secure subsystem that can provide attestation. Established using a trust platform module (TPM) which is a hardware module to store encryption keys or other forms of identification.

Hardware Security Module (HSM)
A network appliance that offers centralized PKI (public key infrastructure) management for the network.

Hashing
A mathematical function that inputs data and transforms it into a fixed-length hexadecimal output. The same input will always produce the same output. There is no way to use the output to recreate the input. It is irreversible. The output is also called a "digest."

Health Insurance Portability and Accountability Act (HIPAA)
A federal law created to protect personal health information (PHI). Sensitive data like this must have special security controls in place to ensure its protection.

hexdump
A utility that can extract data from a binary file and present it in hex, decimal, octal, and ASCII

HMAC
A hash-based Message Authentication Code where both the source and the message content can be verified without needing anything else. HMACs have two parameters: the message and a secret key that is known by the sender and receiver. They both use the MAC hashing algorithm, and the receiver can check the hash of the message to confirm its integrity.

HMAC-Based One-Time Password (HTOP)
An algorithm for token-based authentication, client and server both use the same shared secret. It's stored as an 8-byte value generated by a random number generator.

Homomorphic Encryption
Encryption that is primarily used to share privacy-sensitive data. It allows for statistical analysis of data without decrypting it.

Honeynet
Several honeypots together that pretend to be an entire network with monitoring to see if attackers try to access it.

Honeypot
A fake computer system that is monitored for activity and set up to see if attackers try to access it.

Host-Based Firewalls
A firewall running on a host that will protect it only. It uses packet filtering ACLs to allow/block traffic.

Host-Based IDS (HIDS)
Similar to an IDS but on a single system. It monitors OS logs, files, and processes. It may utilize file integrity monitoring (FIM).

Host-based IPS (HIPS)
On a single system, it not only detects but has the ability to respond to anomalies by stopping processes or blocking traffic.

Hosted Private Cloud
A cloud deployment model that is hosted with a third party but for exclusive use by one company. It offers security benefits over a public cloud.

HTTP Interceptor
A tool that captures HTTP/S traffic between hosts to inspect or modify the data. Example: Burp Suite.

HTTP Strict Transport Security (HSTS)
This is a mechanism for protecting web traffic that is configured as a response header on a web server. It notifies browsers to use HTTPS instead of HTTP. This protects against downgrade attacks or SSL stripping.

Human-Machine Interfaces (HMIs)
Workers configure Programmable Logic Controllers (PLCs) in Industrial Control Systems using human-machine interfaces (HMIs). They may be in the form of control panels or software on a computer.

HUMINT
Human Intelligence - collecting intelligence by interacting with people.

Hybrid SDN
A type of SDN that involves traditional networks and SDNs working together.

I

Identity Proofing
Verifies that a user's various characteristics and credentials are accurate and unique to the individual.

Immutable Systems
A system that is unchangeable, often referred to as frozen.

Improper Headers
A class of vulnerability that involves improper HTTP headers. HTTP response headers control how web servers operate to increase overall security. Properly configured headers can prevent CSRF, XSS, downgrade attacks, cookie hijacking, user impersonation, clickjacking, and other attacks.

Indicators of Compromise (IOCs)
Indicators of Compromise are signs that an intrusion has taken place in some way. Examples: many accounts being locked out at once, an abnormal amount of exiting network traffic, and privileged accounts being created and used in abnormal ways.

Industrial Control Systems (ICS)
Industrial Control Systems provide mechanisms for workflow and process automation. They control machinery used in critical infrastructures, such as power utilities, water utilities, telecoms, healthcare, and national defense.

Information Sharing and Analysis Centers (ISACs)
Information Sharing and Analysis Centers - are non-profit groups that specialize in sharing vulnerability advisories for specific sectors.

Infrastructure as a Service (IaaS)
With this cloud service model, the customer is responsible for most of the major components, and the CSP is only responsible for the infrastructure, utilities, and physical security of the data centers where the cloud servers are located.

Infrastructure as Code (IaC)
A required element of SecDevOps that uses configuration management tools to control code changes. Examples: Puppet Ansible.

Inherent Risk
This is risk that is built-in. Everything in life carries some level of risk, and mitigating controls lower the risk.

Initialization Vector (IV)
A starting variable that is an arbitrary number (random or pseudorandom) that can be used along with a secret key for data encryption.

Insecure References
A class of vulnerability related to weak access controls. An app takes user-supplied input and uses it to give access to areas that normally shouldn't be accessible

Insider Threat
An employee or contractor who is already on the inside and poses a threat either intentionally (through malicious acts) or unintentionally (through poor security practices).

Integration Testing
In software development, this type of testing ensures individual components are tested together to ensure they all work together as expected.

Intellectual Property (IP)
The intangible products created by human thought and ingenuity. It can be protected by trademarks, copyrights, patents, and trade secrets.

Interactive Application Security Testing (IAST)
Analyzes code while running for security issues; looks for problems when functions are triggered.

Interception Attacks
Any unauthorized access to network traffic. Defenses include access controls and traffic encryption

Interconnection Security Agreement (ISA)
An agreement used when two parties need to share data via an interface. It describes the expectations, roles, and operating parameters of the connection.

International Organization for Standardization (ISO)
An international standard-setting body that publishes many technical, commercial, and industrial standards, including, among other things, the cybersecurity framework ISO 27000 series (ISO 27k) of standards.

Internet of Things (IoT)
A global network of appliances and personal devices that contain sensors, network connectivity, and software. They collect information and pass it between themselves, which is referred to as machine to machine (M2M).

Intrusion Detection System (IDS)
A system that monitors for signs of an attack on the network/system. Only reports if it finds something. A NIDS (Network IDS) must be placed in-line to monitor traffic.

Intrusion Prevention System (IPS)
A system that goes a step beyond an IDS because it reacts to events that it sees. Resets connections or blocks traffic.

ISO 31000
A comprehensive risk management framework that considers risks in cyber, financial, legal, and other areas.

J

Jailbreaking
A type of exploit that enables a user to become root on an iOS device. It allows the user to install apps, change carriers, and customize the system in ways that a normal user wouldn't normally be able to do.

JSON Web Token (JWT)
A JavaScript Object Notation (JSON) Web Token - is a subset of JavaScript used in the REST style of web application architecture. A JWT provides a method to transfer claims between two parties. JWTs have a header, payload, and signature separated by dots and expressed in Base64.

Jump Box
A hardened and monitored system used to perform administrative functions. This is a form of segmentation to protect the wider network/system.

K

Kerberos
An authentication protocol that is single sign-on network authentication. It is used in Active Directory. Clients request services from a server. Clients and servers both rely on a Key Distribution Center (KDC) for authentication. The KDC has two parts: Authentication Service and Ticket Granting Service. KDC runs on port 88 TCP or UDP.

Key Performance Indicators (KPIs)
A measurement of the performance of a program compared to the desired goals. Determines effectiveness based on current measurements against the goals.

Key Risk Indicators (KRI)
When analyzing KPIs, new risks may appear in trends. These risks, or key risk indicators, should be analyzed and addressed proactively.

L

Ladder Logic
A sequential control language that dictates out Programmable Logic Controllers (PLCs) operate in Industrial Control Systems (ICSs). Ladder Logic uses a graphical flow-chart-like interface.

LDAP Injection
An attack that manipulates LDAP strings to perform malicious actions.

ldd
A command-line utility that displays a program's dependencies.

Ledger Cloud Storage Database
Enables trusted and verifiable authority for banking transactions and systems of records

Legal Hold
Also called a litigation hold, this is a notification received by an entity that requires the preservation of electronically stored information (ESI) and paper records that may be relevant to a pending legal proceeding. It is handled by legal teams, but cybersecurity teams are involved to place holds on the data.

Lightweight Directory Access Protocol (LDAP)
A directory service protocol that runs over TCP/IP. LDAP service uses a directory database to determine who can and cannot access something.

Local Drive Encryption
Protects data when the system isn't running. Examples: BitLocker, TrueCrypt, cryptsetup.

Location Services
The capability on a mobile device to provide geographical positioning of the device using several methods. GPS is the most common method, but cellular tower triangulation, Wi-Fi signals, and Bluetooth can also be used. Geofencing is a capability to trigger a response if a mobile device enters a pre-defined geographical area. Geotagging is a capability to add location metadata to files or devices, usually for the purposes of asset management.

lsof
A command-line utility that displays the list of open files and their associated processes.

M

Machine Code
The lowest level of source code; devices can understand it.

Management plane
A type of SDN plane that monitors traffic conditions and overall network status.

Mandatory Access Control (MAC)
An access control method that is based on security clearance levels. It involves labels, and objects and subjects are each granted a clearance level. Labeling is performed using pre-established rules. Rules cannot be changed by subject accounts. It is non-discretionary.

Master Service Agreement (MSA)
An umbrella contract that establishes an agreement between parties to conduct business during a specified period of time. It is defined by scopes of work and expectations/deliverables.

Mean Time Between Failure (MTBF)
The lifespan of a device but also the amount of time until a service goes down.

Mean Time to Recovery (MTTR)
The measure of the amount of time a device or service is down (i.e., how long from the time that it goes down to when it comes back up.)

Measured Boot
During the boot process, this mechanism uses platform configuration registers (PCRs) in the TPM at every stage of the process. It validates that hashes of the key boot firmware, boot loader, kernel, and drivers haven't been altered.

Memorandum of Understanding (MOU)
A non-binding document that formally defines the roles and expectations of two parties who want to work together.

Message Authentication Code (MAC)
Message authentication codes can be used to confirm the authenticity of a message. A more secure version is a hash-based MAC, called an HMAC. HMACs have two parameters: the message and a secret key that is known by the sender and receiver.

Message Digest Algorithm (MD5)
An algorithm that creates a 128-bit output. This is easily brute-forced and has a high chance of collisions.

Microcontrollers
Perform sequential operations from a vendor-determined dedicated instruction set. Embedded systems often only need to perform the same basic task over and over, so hardware controllers can be programmed with these instructions at creation.

Microsegmentation
A cloud-based network segmentation that isolates workloads from each other and protects them individually.

Microsoft Monitor Logs
Logs that are collected and organized in Azure and can be visualized in Azure Portal.

Middleware
Software applications that are designed to integrate two systems together.

MITRE ATT&CK
The MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) is a knowledge base of real-world information about adversary TTPs. It describes in detail how adversaries perform their attacks and breaks them down into logical groupings. See attack.mitre.org.

Mobile Device Management (MDM)
Compliance with an organization's security policies related to mobile device usage in the enterprise.

Modbus
The protocol used on OT networks which allows control servers and SCADA devices to query and change configurations of PLCs. Originally, Modbus was a serial protocol (Modbus RTU), but it has been modified to run on Ethernet and TCP/IP now.

Multi-Cloud KMS (MCKMS)
The Key Management System (KMS) can be used for multiple clouds and multiple clouds can use many KMSs.

Multi-factor Authentication (MFA)
An authentication process that requires more than one of the following to authenticate a user: Something the user knows (like a password), something the user has (like a token or similar device), and/or something the user is (biometrics).

N

NAC Lists
Pronounced "nackles" - these are used to control inbound and outbound traffic between VPCs as a form of cloud-based network segmentation.

Nation-State Threat Actors
These are truly skilled groups with sophisticated tools and resources that are supported by government agencies. They are also known as APTs - Advanced Persistent Threats.

National Institute of Standards (NIST)
A non-regulatory agency of the U.S. government that creates best practices and standards across all technology and science fields. Included are the SP 800 series for cybersecurity, the Risk Management Framework, and the Cybersecurity Framework.

Near Field Communication (NFC)
A technology in modern smartphones that enables contactless payments (like with Google Pay, Apple Pay, and Samsung Pay). It is based on a specific type of Radio Frequency ID (RFID). It is not encrypted and is vulnerable to many types of attacks, like MIM and skimming.

Netcat
A tool for reading and writing from network connections using TCP or UDP.

Netflow
Netflow and sFlow are network protocols for capturing network traffic for analysis.

netstat
A command-line utility that displays current network connections and their state.

Network Access Control
Limits network access to only trusted devices and creates a security baseline that trusted devices must adhere to. It can require that a device wanting to connect present the proper credentials or authorized digital certificates.

Network Access Control (NAC)
Requires a device to provide a valid token to gain access to network resources.

Network Intrusion Prevention System (NIPS)
Network Intrusion Prevention System - a wireless NIPS can block unknown devices.

Network Segmentation
Dividing a network into smaller parts. Other related terms: subnetting, VLAN, screened subnet.

Network Traffic Analyzer
A tool that analyzes data captured by a sensor. Example: Zeek.

NIST Risk Management Framework
A cybersecurity risk framework adopted by the US government. It has five core functions: Identify, Protect, Detect, Respond, and Recover.

NMap
An open-source IP scanner for host and network discovery.

Non-Disclosure Agreement (NDA)
An agreement that defines how an entity can use data it has access to while working with another party and what must be kept confidential. It also contains the legal ramifications to be faced in the event of disclosure to serve as a deterrent to disclosure.

O

OAuth
Open Authorization - an authentication protocol that is often used for authentication and authorization for RESTful APIs. The user account is hosted by one or more resource servers. Authorization requests are processed by authorization servers. It uses JavaScript object notation (JSON) web token (JWT) format. It can be passed in URLs and HTTP headers and can be digitally signed for authentication and integrity.

Obfuscating and Masking
Mechanisms for hiding data. These do not always involve encryption. Sometimes data can be encoded in different formats, such as Base64. The goal is to have data in a format that isn't easily recognizable.

Objdump
A tool that, similar to readelf, is used to analyze object files, also includes a disassembler.

Object storage
A cloud storage model that supports cloud-based applications needing access to documents, videos, and image files.

OllyDbg
A debugger that performs binary code analysis. It has a GUI and is focused on Microsoft Windows.

Online Certificate Status Protocol (OCSP)
Rather than having to send the entire CRL, OCSP can be used. This allows end-users to query the status of a single certificate. This is kept up-to-date and easier to distribute than the CRL.

Open SDN
A type of SDN that is open source and used to reduce vendor lock-in.

Open Vulnerability and Assessment Language (OVAL)
A SCAP language that provides a consistent way to collect and assess 3 main aspects of evaluated systems: system information, machine state, reporting.

OpenID
Allows for a single ID to be used by anyone in participating Open ID sites. OpenID adds authentication to OAuth 2.0.

Operation Technology (OT)
This is the type of technology used in Industrial Control Systems. It differs quite a bit from client/server networks and has its own set of security concerns to be considered.

Operational Level Agreement
Internal documents that define the essential operational needs so that an entity can maintain an SLA.

OSINT
Open-source Intelligence - publicly available information, social media, DNS records, and websites, from which threat intelligence may be obtained.

Output Feedback (OFB)
A cipher mode of operation that uses initial chaining vector (ICV) for the first round and combines the output of all previous rounds as input for the next round.

Over-the-Air (OTA)
Over-the-air updates are delivered to mobile devices via cellular or Wi-Fi connections. These can be firmware updates to the radio modem that is used for cellular, Wi-Fi, Bluetooth, NFC, and GPS operations.

OWASP
Open Web Application Security Project - produces free and open-source resources to promote secure coding, including the OWASP Top 10 list of software security vulnerabilities and attack vectors

P

Packet Capture
Capturing network traffic for the purposes of analyzing the packets. It requires a sniffing tool or protocol analyzer. Examples: Wireshark and TCPDump.

Password Cracker
A utility designed to crack passwords from a variety of sources using several methods such as brute force and dictionary attacks. Example: John the Ripper.

Payment Card Industry Data Security Standard (PCI-DSS)
A global data protection standard created by the credit card industry. It identifies controls that must be used to help prevent fraud and to protect credit and debit card data.

Peer-to-Peer
A decentralized network that provides services only to those connected. (This is a form of segmentation.)

Perimeter Security Devices
Devices that protect the perimeter of the network. These include things like routers, load balancers, firewalls [signature-based, Unified Threat Management (UTM), Next-Generation Firewall (NGFW), Web Application Firewall (WAF)], and proxies (forward/transparent, reverse proxies).

Persistence
An attacker's ability to maintain access to an environment and stay undetected.

Personally Identifiable Financial Information
Data provided to a financial institution about a consumer. It is generally used to gain access to financial services or products.

Personally Identifiable Information (PII)
Any data that can be used, alone or in combination with other data, to identify a person. Note that some more sensitive PII must be protected at a higher level than other PII.

Pivoting
Once an attacker has exploited one system, they will use it to target others on the same network to gain further access.

Platform as a Service (PaaS)
With this cloud service model, the customer is responsible for the operating system and the applications that are running, but the CSP is responsible for the other major components in the cloud.

Port Scanner
A tool that looks for services running on ports on a specific system. it can also be used for network discovery.

Privacy Impact Assessment
An assessment performed to discover where privacy data is stored, how it is stored, and the impact that would occur if the confidentiality, integrity, and availability of the data were compromised.

Privacy Level Agreement
An agreement that is commonly used when working with a CSP and details how data will be kept private and protected.

Private Cloud
A cloud deployment model where the organization using the cloud completely owns and operates the infrastructure itself and does not rely on a third-party provider.

Private Function Evaluation (PFE)
Describes calculations done by more than one system but the function used is only known by one party.

Private Information Retrieval (PIR)
This protocol allows for retrieval of data without revealing which specific item is being collected

Privileged Access Management
Software or a service that protects against credential theft and credential misuse. Stores credentials in a secure vault that requires additional authentication to be used. Examples: CyberArk, BeyondTrust, Centrify.

Process Injection
Defined within the MITRE ATT&CK Framework as an attack where an attacker injects code into a currently running process.

Production Environment
In software development, this is the live environment where the software is moved for use by its intended users.

Programmable Logic Controllers (PLCs)
These are a type of computer that enables automation in settings such as assembly lines, autonomous field operations, robotics, etc. They are embedded in Industrial Control System equipment and are linked by an OT fieldbus serial network, or with an industrial Ethernet, to actuators. Actuators operate motors, circuit breakers, valves, and sensors, such as for temperature.

Protected Health Information (PHI)
Data that can be used to identify an individual concerning their health, including their past, present, and future health.

Protocol Analyzer
A tool used to capture network traffic for analysis. Example: Wireshark.

ps (process status)
A command-line utility used to display running processes on a Linux system including the PID and user running it.

Public Cloud
Also known as multi-tenant, this cloud deployment model is offered over the Internet by a cloud service provider. Example: AWS, Azure.

Public Key Infrastructure (PKI)
A combination of software, hardware, and services that work together to create digital certificates and the capabilities of public-key encryption. It solves the problem of secure key distribution. Public and private keys are a matched pair. Public keys can be freely given away. Private keys must be kept secure. Keys can be used to digitally sign messages or files, proving authenticity or ownership. PKI also helps to "prove" who a user is since the user has their own unique digital certificate that is issued by a trusted CA.

Q

Qualitative Risk Analysis
Risk is evaluated through words and not numbers. It is very subjective but works well for assets that are intangible like risks to brand and reputation. It also requires a lot of input from other departments like Marketing, Sales, and Corporate Communications.

Quantitative Risk Analysis
A numerical representation of risk, normally in the form of money/dollars that the risk represents.

Quantum Computing
Manipulates data at the atomic level. Qubits (quantum bits) are the base unit in quantum computing. Qubits can have a value/state of 0 or 1 or any value in between. They can also have multiple states at the same time. Qubits can become entangled and the value can only be observed by collapsing the quantum effect. The only way to get measurements is to indirectly entangle two qubits. This allows quantum computers to perform many calculations at once. Because of this, quantum computing is especially useful in breaking RSA and ECC encryption.

R

Race Conditions
Conditions that occur in software when several processes are needed to complete a task at one time and bugs can occur as a result. In addition, applications can be manipulated by altering the assumptions made on the processes and their outcomes.

RACE Integrity Primitives Evaluation Message Digest (RIPEMD)
An algorithm that was developed completely independently from the U.S. government. It has 128, 160, 256, and 320-bit outputs and is used for Bitcoin addresses.

RADIUS
Remote Authentication Dial-In User Service - an authentication protocol that uses UDP and authenticates with a shared secret.

Raw Zone
A form of cloud-based data zone that has data from multiple sources.

readelf
A tool that is able to read the Executable and Linkable Format (ELF) within an object file.

Recovery Point Objective
The amount of data that can be lost before the organization is irreparably harmed.

Recovery Time Objective
The maximum amount of time that it should take to perform the recovery activities and be back up and running.

Regions
A form of cloud-based network segmentation that involves having data centers physically located in a globally distributed cloud.

Registration Authority
Accepts requests for digital certificates and validates that the one requesting the certificate is who they say they are.

Regression Testing
In software development, this type of testing ensures that new changes in code do not break previously existing functionality or features.

Remote Wipe
If a device is lost or stolen, a remote wipe can be performed, and the device will remotely be restored to factory defaults and all sensitive data will be removed. A person can prevent a remote wipe from being possible by using a faraday bag.

Replication
A type of resiliency that involves copying data to where it can be used most effectively.

Residual Risk
The risk that is left over after mitigating controls have been applied.

Resiliency

Enables systems to recover when some of their parts fail. Offers high availability of resources in the event of increased demand or failures. Increases the complexity, costs, and management of the network.

Responsible Disclosure Forms
Allow for the easy reporting of data loss incidents.

REST
Representational State Transfer - an architecture for data exchange based on web technologies.

Return on Investment (ROI)
Compares the cost of an item to the benefits it provides.

Reversible Encryption
Storing passwords in a way that they can be decrypted. This is a massive security risk and should never be used.

Reverse Engineering
A type of vulnerability analysis that involves deconstructing software/hardware to see how it functions.

Reverse Proxy
A configuration of CASB where the appliance is positioned at the cloud network edge, and it directs traffic to cloud services if the traffic complies with the policies.

Risk
A measurement of the impact (or consequence) and likelihood that a threat will exploit a vulnerability.

Risk Appetite
The level of residual risk that is acceptable for an organization.

Risk Register
A visualization of identified risks and corresponding controls. It is the most recognized output of a risk management program, and it is a working document.

Risk Tolerance
The level of risk that is acceptable to achieve a goal.

Role-Based Access Control (RBAC)
An access control method that adds an additional element to DAC based on a subject's role. Users gain rights based on their roles.

Rooting
For Android devices, this is an exploit where a user obtains system-level (or root) access to the device, allowing them to control many aspects that a normal user would not be able to. Systemless root refers to obtaining the same access without modifying system partitions, which is harder to detect.

Rule-Based Access Control
An access control method where policies are determined by system-enforced rules rather than system users.

S

Safety Instrumented System (SIS)
A system composed of sensors, logic solvers, and final control elements (horns, flashing lights, sirens, etc.). It is designed to return an industrial process to a safe state after present conditions have occurred. The goal is to monitor industrial processes for possible dangerous conditions and reduce the impact of an emergency event by taking defined actions.

Sandbox Detonation
A segregated system that can allow for the execution of malware to see what it does without the risk of it infecting production systems.

Sandbox Escape
Often occurs in web browsers when code escapes the safety of the browser sandbox and executes outside of it.

Sandboxing
In software development, this is the process of ensuring each process is segmented from other processes and each part of the development process does not cause changes in other parts. This allows developers to work on their parts of the software without disrupting each other's work.

Scalability
The ability to expand with the growth and changing needs of your organization by adding resources as they are needed. Scalability performs in two ways: vertically (resources like processing, memory, and storage, are added to an individual system) and horizontally (additional servers are added to process the same workload)

SCAP Scanner
A tool that uses SCAP to compare a scanned device against SCAP baselines. Example: DoD SCAP Scanner.

Screened subnet

Has two firewalls placed on each side of a DMZ (demilitarized zone, which is a perimeter network set up to protect your internal network.)

Script Kiddie
A person who is utilizing hacker tools without having the knowledge of how they work. Usually, this type of threat actor's goals are thrill-seeking or to gain attention or prove their skills.

Scrubbing
A data integrity control designed to find and remove invalid, redundant, or outdated data from a database or data warehouse. If you don't need it, get rid of it.

SDN Overlay
Using existing hardware with software that allows for the creation and management of new virtual networks.

SecDevOps
A discipline of software development and operations that requires security to be included in all decisions, plans, and coding. It also requires developers to have a strong understanding of possible vulnerabilities and to use version control for code changes.

Secure Boot
During the boot process, this mechanism prevents computers from being hijacked by a malicious OS. Configured with a digital certificate from valid OS vendors, and firmware checks the bootloader to ensure the certificate is valid. Requires UEFI but not TPM.

Secure Coding Standards
Templates for a structured approach to software development. The goal is to prevent coding vulnerabilities and reduce costs upfront by preventing vulnerabilities instead of fixing them after a release.

Secure Design Patterns
Templates for solutions to security issues that can be utilized in different situations. They cover a wide range of components such as identity and access management, federated identities, cryptography, public-facing websites, and others.

Secure Encrypted Enclaves/Memory Encapsulation
Protected areas of memory in a database engine that only allow data to be decrypted on the fly in a CPU, SoC, or protected region.

Secure Hash Algorithm (SHA)
This is an algorithm type that has several variants. For example, SHA-1 produces a 160-bit output and has been successfully cracked and should not be used for anything that needs to be secure. SHA-3 has replaced SHA-1 and is fundamentally different in nature than SHA-1 and MD-5.

Secure LDAP
This is LDAP over SSL/TLS.

Secure Multi-Party Computation
An emerging technology that distributes computations across multiple systems. No individual system is able to read the data of the other parties. It allows for problem-solving without compromising privacy. Used for DNA data, research, etc.

Secure Two-Party Computation or Secure Function Evaluation (SFE)
Allows two parties to check input without disclosing the results.

Security as Code (SaC)
A required element of SecDevOps that uses automated methods for static code testing and dynamic application testing.

Security Assertion Markup Language (SAML)
A protocol used for cloud and network federation. Attestations (authorizations) are written in XML. Communications are performed over HTTP/HTTPS and Simple Object Access Protocol (SOAP). Secure tokens are signed using XML signature specifications. Example: Amazon AWS, where customers can access apps and resources on AWS without the need to create AWS accounts.

Security Content Automation Protocol (SCAP)
A suite of interoperable specifications designed to standardize the naming conventions and formatting used to identify and report software flaws.

Security Data Analytics
A set of tools to collect, order, and analyze the vast amount of data available on an enterprise so as to identify security incidents and perform threat detection.

Security Groups
A form of cloud-based network segmentation that involves virtual firewalls limiting inbound and outbound traffic for an instance.

Security Information and Event Management (SIEM)
Security Information and Event Management - a type of activity and traffic sensor that collects data from many sources and creates alerts. Has the ability to correlate different data sets to create more informed alerts.

Security Orchestration, Automation, and Response (SOAR)
Security Orchestration, Automation, and Response - automated response to security incidents. Incident response usually consists of a list of items to be performed in response to an incident. These steps can be automated with playbooks, which are scripts of steps to perform when an

incident is observed. SOAR will scan threat data collected from various sources and automatically respond to it.

Server Authentication
Digital certificates can be used to validate that a server is legitimate. Example: Web server certificates used to validate a website.

Serverless Computing
An architecture where all network architecture is in the cloud. This architecture is designed to replace LANs. Applications are functions and microservices that interact with each other for handling client requests. The cloud will create a container, perform the processing, and then destroy the container. Billing is handled by execution time, rather than hourly rates. Also called Function as a Service (FaaS).

Service Level Agreement (SLA)
An agreement that defines how a service will be provided and contains measurable and repeatable levels of service, as well as penalties for not meeting those requirements.

Service-Oriented Architecture (SOA)
A method of designing apps in the form of interoperable services.

sha256sum
A hashing utility in Linux that generates SHA-2 hashes for files with a digest length of 256 bits.

Shared Responsibility Model
When an organization has a cloud service provider (CSP), there is typically a shared responsibility model in place, where the CSP shares responsibility with the organization to secure the apps, data, workloads, and other resources that are in the cloud. Different areas will be assigned to each, but identifying these responsibilities and ensuring they are being taken care of is critical.

Shell Restrictions
Restrict what a shell is allowed to do.

Shibboleth
A federated trust model that is based on SAML (Security Assertion Markup Language) and is often used by universities and public service organizations. The process flow is that the user contacts the Shibboleth site via SAML. The site redirects to an identity provider that verifies using SAML info. The identity provider responds to the site with authentication information. The site validates and then gives access based on the user's SAML info.

Side-Channel Analysis
A type of vulnerability analysis that involves inspections of a system or software while running by analyzing its data: sniffers.

Sideloading
The installation of apps on a mobile device from any third party. Management suites can be configured not to allow this.

Simple Network Management Protocol (SNMP)
A common protocol for monitoring and managing network infrastructure. Uses ports 161 and 162. Consists of monitors and agents. If it is present and not being used, it should be disabled, as it can be a security risk.

Simple Object Access Protocol (SOAP)
A protocol and communication mechanism. SOAP APIs can be exploited by SQL injection.

Single Loss Expectancy (SLE)
The cost of an event happening one time; a server crash.

Single Sign On (SSO)
An authentication protocol that allows a user to authenticate once to a local server and then be authenticated to other servers without having to enter in credentials again.

Smart Card Authentication
Storing a digital certificate in a chip on a card. This is used to prove identity and authenticate the user. A user will provide his/her pin to activate the card.

Social Engineering
Manipulating users by using emotions (fear, need to be helpful, etc) to gain access or get them to do what that attacker wants.

Software as a Service (SaaS)
With this cloud service model, the customer has the lowest level of responsibility, and the Cloud Service Provider (CSP) takes responsibility for almost everything, including the facilities, utilities, physical security, platform, and applications that are running in the cloud.

Software Composition Analysis
Inspecting source code to identify open-source components that may contain vulnerabilities.

Software Defined Networking (SDN)
Software Defined Networking - software-defined network technology that enables efficient network management.

Software Development Life Cycle (SDLC)
Software Development Life Cycle - consists of the phases Planning, Solution, Coding, Testing, Release.

Software-Defined Networking (SDN)
A capability that allows for fully automated deployment (or provisioning) of network links, appliances, and servers.

Source Code Escrow
A vendor assessment consideration related to whether vendor-developed products have their source code placed at third parties so that it will still be available should they go out of business.

Spiral Method
In this approach to software development, development is modified continually throughout the process based on stakeholder feedback. Risk analysis is performed at each iterative step. It is suited well for large, complex projects.

SQL Injection
An attack that manipulates the SQL language to gain access to data stored in the targeted database.

ssdeep
A hashing utility that is commonly used by antivirus programs to compare files to identity matches. It utilizes context-triggered piecewise hashing (CTPH).

Staging or QA Environment
In software development, this is the environment where work is performed in the final stages to confirm the software is ready for release.

Static Analysis
A type of vulnerability analysis that involves manually reviewing source code or using applications that can look for coding errors.

Static Application Security Testing (SAST)
Reviewing code when it is not running.

Steganalysis
This process is concerned with locating data that may be hidden within other files. This is usually associated with images, but data can be stored in many types of files.

strace
A tool used to identify interactions between processes and the Linux kernel.

Stream Cipher
An encryption where each digit of plaintext data is encrypted one at a time using a keystream (a stream of pseudorandom values). It is useful for encrypting data when the amount or length of the data isn't known, such as with video. Keystreams are generated by an initialization vector

(IV) that is combined with a static key. This creates a unique keystream. The IV is always changing to ensure that unique ciphertext is created from the same plaintext.

strings
A Unix/Linux utility that can recover text strings and discover attributes regarding the internal structure of a program.

Structured/Curated Zone
A form of cloud-based data zone where the data is checked for quality and formatted for later use.

Supervisory Control and Data Acquisition (SCADA)
A large-scale, multi-site ICS will use a SCADA system in place of a control server. SCADA systems are usually software running on computers that gather data from management plant devices and equipment with embedded PLCs. SCADA systems usually have WAN connections such as satellite and cellular connections to link to the field devices.

Supply Chain Attack
A form of attack that is becoming more common in which threat actors go after a supplier or third-party contractor to gain access to their actual targets. These are often easier to gain access to, like coming in the back door. Example: the retailer Target was attacked this way, through their HVAC vendor.

Supply Chain Visibility
Understanding how all vendor-supplied parts and services are produced and delivered and how they will impact your organization's operations or finished products.

Symmetric Algorithms
Algorithms that are used to encrypt data or messages. They can only be unlocked with a single key. Encryption is not like hashing, as you can view the data once it's decrypted. The weakness is in creating and distributing the keys in a secure way.

System and Organization Controls (SOC)
Audit standards created by the American Institute of Certified Public Accountants (AICPA) for the evaluation of policies, procedures, and processes, to protect technology and financial operations.

System on a Chip (SoC)
Integrates part of a chipset into a single chip. Chipsets can include up to 4 chips that control communications between the CPU, RAM, storage, and peripherals. SoC contains the processor along with a graphics processor (GPU), memory, USB controller, power management, and wireless radios. It uses low power while offering good performance.

T

TACACS+

Terminal Access Controller Access Control System Plus - is a CISCO-developed authentication protocol. It uses TCP port 49, data is encrypted, and AAA functions are all discrete.

Tactics, Techniques, and Procedures (TTPs)

Tactics, Techniques, and Procedures - these are adversary behaviors that various threat actors are known to have exhibited in real-world attacks.

TCG Opal 2.0

TCG is Trusted Computing Group, and it maintains the Opal 2.0 encryption specifications for manufacturers of encrypted storage devices and drives like self-encrypting drives (SEDs).

tcpdump

A command-line packet analysis tool. It captures network data and saves it to a pcap file for analysis.

Test/Integration Environment

In software development, this is the environment that is where code from multiple developers can be merged and tested to ensure that code builds properly and functions correctly.

Third-Party App Stores

Sites other than Apple App Store and Google Play Store where mobile apps may be found.

Third-Party Library Validation

In software development, outside libraries that will be used in the application must be checked for insecurities before deployment. Sometimes third-party libraries themselves have third-party libraries. With the modular nature of modern programming, third-party libraries are easy to include.

Threat Emulation

Using known TTPs (tactics, techniques, and procedures) to emulate how an attacker may operate in a realistic way. Can be used to test current defenses.

Threat Hunting

Using assessment techniques with insight gained from threat intelligence so that threats can be proactively found.

Threat Intelligence

The continual process organizations use to collect and analyze threat information so they can understand the threats that they face. Threat intelligence can be of one of three types: tactical, strategic, and operational.

Time Series Cloud Storage Database
Focused on supporting apps that analyze data and changes over time, best represented using time intervals

Time-Based One-Time Password (TOTP)
A refined version of HMAC that adds a value taken from the timestamp of the client and server. This allows each token to have a short usage time (30-60 seconds). Example: Google Authenticator

Tokenization
A security mechanism used in credit card processing; data is replaced with a token that cannot be reversed.

Total Cost of Ownership (TCO)
All costs associated with an asset including the costs to operate it and maintain it over its entire lifetime.

Traffic Mirroring
A critical part of NIDS devices. Other terms are port mirroring and SPAN ports. Sniffs the network data in real-time to see the traffic packets. Traffic frames are copied to the port for analysis.

Transitive Trust
A trust mechanism that assumes if resource A trusts B, and B trusts C, then A trusts C. Example: Active Directory.

True Negative
Something correctly identified as not an issue.

True Positive
Something identified as an issue that is an issue.

Trusted Platform Module (TPM)
A specification for hardware-based storage of encryption keys, hashed passwords, and other identification data.

Type 1 Hypervisor
A type of virtualization that consists of bare metal, doesn't need a host OS, interacts with hardware directly. Examples: Hyper-V, XEN, Proxmox, VMWare, ESXI

Type 2 Hypervisor
A type of virtualization that requires a host OS. Examples: Virtual Box, VMWare Workstation, Parallels Workstation

U

UEFI (Unified Extensible Firmware Interface)
A program that runs when a computer system is first booted up and connects the computer's firmware with its operating system.

Unit Testing
In software development, this type of testing is done on individual blocks of code to make sure it performs the exact function it was intended to perform.

User and Entity Behavior Analytics (UEBA)
Scan indicators from IDS and logging systems to spot anomalies. Often integrated with SIEMs.

V

Vendor Lock-in
A vendor assessment consideration related to whether the customer could become completely dependent on the vendor because changing to another vendor would be either too expensive or impossible.

Vendor Lock-out
A vendor assessment consideration where the vendor's product will not work with other vendors' products.

Vendor Viability
A vendor assessment consideration where the customer needs to assess whether the vendor will stay in business in the future and/or grow and expand in their field.

Virtual Desktop Infrastructure
Desktops are virtualized and run from servers. This separates the user from a physical machine. There are three deployment models: hosted (provided by a third party); centralized (hosted within the enterprise itself); and synchronized (allows for work to continue in a disconnected state, but requires more local resources.

Virtual Local Area Network (VLAN)
A network that has software-defined, usually on switches. Allows a single device to separate network traffic.

Virtual Private Cloud (VPC)
A cloud-based network segmentation that allows for creating cloud resources within a private network.

Virtual Private Network (VPN)
A network that creates a tunnel and protects the data within that tunnel. Types of VPNs include OpenVPN, L2TP/IPSec, IKEA/IPSec, WireGuard, SSTP, IPSec, PPTP.

Virtual/Augmented Reality
Extended concept of AI. Emulates a real-life environment with computer-generated sights and sounds. It has numerous applications and can be used for training or providing information to a user on people or objects that are within view.

Virtualization
Creating a simulated or virtual environment that is not limited by the physical one. It allows for multiple operating systems to be run at the same time on the same computer. It requires three components: host hardware, a hypervisor (virtualization software), and the guest operating system, virtual machines, or instances.

VLAN Hopping
An attack that allows attackers to move between otherwise isolated networks. It usually occurs by spoofing a switched network.

VM Hopping and Escape
An attack against a hypervisor of virtualization software so as to allow an attacker to move from one VM to another.

vmstat
A command-line tool used to display real-time information on system memory, running processes, interrupts, paging, and I/O stats.

Volatility
A command-line tool used to perform memory analysis. It can be used to view the contents of a memory dump.

Vulnerability
Any area of the enterprise where you are not fully protected and could be exploited by attackers. This does not only relate to software bugs or weak patches but can also be things like insufficient security training for staff or the lack of an alarm system to protect your premises.

Vulnerability Scanner
A tool that scans devices on your network to see what areas might be vulnerable. They may test known exploits against your systems, look for missing patches and misconfigured system settings or default settings that need to be changed. Example: Nessus.

W

Wassenaar Agreement

An agreement that was established in 1996 to define export controls for "conventional arms and dual-use goods and technologies." It was agreed to by 42 participating states that work to prevent sensitive technology from getting to terrorist groups and rogue nations.

Waterfall

In this approach to software development, each phase cascades downward when all tasks in the previous phase have been completed. Code check is performed at the end of each phase. It is very rigid and you cannot skip a phase.

Watermarking

Marking data so that it clearly displays important details about the data, such as ownership, classification, usage, etc.

Wi-Fi Protected Access 3 (WPA3)

The latest generation of security for wireless networks. Neither WEP nor WPA is considered safe for use, and while WPA2 uses AES encryption with 128-bit keys, making it stronger, it is still vulnerable due to how it was implemented. As such, WPA3 was introduced to address the weaknesses in WPA2.

Wireless Intrusion Detection System (WIDS)

Wireless Intrusion Detection System - monitors for rogue access points and evil twins. Monitors unauthorized client devices. Identifies wireless denial of service attacks. Looks for MAC address spoofing.

Wireshark

A GUI-based packet analysis tool.

X

XML External Entity (XXE) Injection

XML is read and processed and can lead to many types of attacks such as directory traversal, code execution attacks, etc.

Z

Zero Trust

The concept of never trusting anything, always verifying and assuming something could be a breach. This means that every connection and request on the network must be explicitly evaluated and validated. It focuses on resources. The NIST SP 800-207 covers the Zero Trust Architecture.