GLOSSARY

.cer The file extension for an X.509 certificate that is stored in a binary file.

.P12 The file extension for a Personal Information Exchange Syntax Standard based on PKCS#12 that defines the file format for storing and transporting a user's private keys with a public key certificate.

.P7B The file extension for a Cryptographic Message Syntax Standard based on PKCS#7 that defines a generic syntax for defining digital signature and encryption.

5G The fifth-generation cellular wireless standard.

A

acceptable use policy (AUP) A policy that defines the actions users may perform while accessing systems and networking equipment.

acceptance Acknowledging a risk but taking no steps to address it.

access control list (ACL) A set of permissions or rules attached to an object that administer its availability by granting or denying access.

access control scheme A framework embedded in hardware and software that can be used for controlling access.

access policy A policy that allows a network administrator to create the privileges that the user is given based on a role-based access control scheme.

Account Audits An account setting that audits user connections and events.

account permissions The privileges that a user is given.

accounting A record that is preserved of who accessed the network, what resources they accessed, and when they disconnected from the network.

active-active A configuration in which all load balancers are always active.

active-passive A configuration in which the primary load balancer distributes the network traffic to the most suitable server while the secondary load balancer operates in a "listening mode."

ad hoc mode A WLAN functioning without an AP.

Address Resolution Protocol (ARP) Part of the TCP/IP protocol for determining the MAC address based on the IP address.

admissibility Evidence that can hold up to judicial scrutiny and can be entered as evidence.

advanced persistent threat (APT) A class of attacks that use innovative attack tools to infect and silently extract data over an extended period of time.

adversarial artificial intelligence Exploiting the risks associated with using AI and ML in cybersecurity.

adversary tactics, techniques, and procedures (TTP) A database of the behavior of threat actors and how they orchestrate and manage attacks.

agentless A NAC system that does not require additional software to be installed on endpoints.

agents Software that is installed on endpoints to gather information for a NAC.

aggregators Network devices that combine multiple network connections into a single link.

air gap An area that separates threat actors from defenders.

alarm An audible warning of an unexpected or unusual action.

algorithm Consists of procedures based on a mathematical formula used to encrypt and decrypt the data. Also called a *cipher*.

always-on VPN A VPN that allows the user to stay connected at all times instead of connecting and disconnecting from it.

Annualized Loss Expectancy (ALE) The expected monetary loss for an asset due to a risk over a one-year period.

Annualized Rate of Occurrence (ARO) A calculation for determining the likelihood of a risk occurring within a year.

anomaly monitoring A monitoring technique used by an intrusion detection system (IDS) that creates a baseline of normal activities and compares actions against the baseline. Whenever there is a significant deviation from the baseline, an alarm is raised.

antimalware A suite of software intended to provide protections against multiple types of malware, such as ransomware, cryptomalware, Trojans, and other malware.

antivirus (AV) Software that can examine a computer for file-based virus infections as well as monitor computer activity and scan new documents that might contain a virus.

Anything as a Service (XaaS) A broad category of subscription services related to cloud computing.

API inspection and integration A service for authentication, authorization, encryption, availability, and policy compliance of APIs.

appliance firewall A separate hardware device designed to protect an entire network.

application program interface (API) attack An attack that targets vulnerabilities in an API.

application security Protecting cloud-based applications.

application whitelisting/blacklisting Requiring preapproval for an application to run or not run.

Arduino A controller for other devices.

ARP poisoning An attack that corrupts the ARP cache.

artifacts Technology devices that may contain evidence in a forensics investigation.

asset management policy A policy that provides the guidelines and practices that govern decisions about how assets should be acquired, maintained, and disposed.

asset value The relative worth of an asset.

asymmetric cryptographic algorithm Cryptography that uses two mathematically related keys.

attack vector A pathway or avenue used by a threat actor to penetrate a system.

attestation A key pair that is "burned" into a security key during manufacturing and is specific to a device model that can verify authentication.

Attribute-Based Access Control (ABAC) An access control scheme that uses flexible policies that can combine attributes.

attributes Characteristic features of the different groups of threat actors.

authentication app A smartphone application that can be used to verify a user's login attempt.

Authentication Header (AH) An IPsec protocol that authenticates that packets received were sent from the source.

authentication mode of operation An information service that provides credentialing by a block cipher mode of operation.

authentication Proving that a user is genuine and not an imposter.

authentication servers Servers that facilitate authentication of an entity to access a network.

authority A social engineering principle that involves directing others by impersonating an authority figure or falsely citing their authority.

authorization Granting permission to take an action.

automated courses of action Developing code as quickly and securely as possible.

Automated Indicator Sharing (AIS) A technology that enables the exchange of cyberthreat indicators between parties through computer-to-computer communication.

Autopsy A digital forensics platform.

auto-update The automatic download and installation of patches as they become available.

availability loss The loss that results from making systems inaccessible.

avoidance Identifying a risk but making the decision to not engage in the activity.

B

backdoor Malware that gives access to a computer, program, or service that circumvents any normal security protections.

background checks Examining the history of a job candidate.

backup copy A copy of the original data backup.

badge A token that indicates the wearer has been approved.

barricade Objects generally designed to block the passage of traffic.

baseband The original frequency range of a transmission signal before it is converted to a different frequency range.

baseline configuration A set of security settings that are the initial starting point and the minimum settings.

Bash The command language interpreter for the Linux/UNIX OS.

behavioral monitoring A monitoring technique that uses the normal processes and actions as the standard and compares actions against it.

benchmark/secure configuration guides Guidelines for configuring a device

or software usually distributed by hardware manufacturers and software developers.

binary Machine code.

birthday attack A statistical phenomenon that makes finding collisions easier.

Black box A penetration testing level in which the testers have no knowledge of the network and no special privileges.

black hat hackers Threat actors who violate computer security for personal gain or to inflict malicious damage.

blacklisting Creating a list of unapproved software so that any item not on the list of blacklisted applications can run.

block cipher A cipher that manipulates an entire block of plaintext at one time.

block cipher mode of operation How block ciphers handle blocks of ciphertext by using a symmetric key block cipher algorithm to provide an information service.

blockchain A shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.

Blue Team A penetration testing team that monitors for Red Team attacks and shores up defenses as necessary.

bluejacking An attack that sends unsolicited messages to Bluetooth-enabled devices.

bluesnarfing An attack that accesses unauthorized information from a wireless device through a Bluetooth connection.

Bluetooth A wireless technology that uses short-range radio frequency (RF) transmissions and provides rapid ad hoc device pairings.

bollard A short but sturdy vertical post used as a vehicular traffic barricade to prevent a car from ramming into a secured area.

boot attestation The process of determining that the boot process is valid.

bot An infected computer placed under the remote control of an attacker for the purpose of launching attacks.

BPDU guard A feature on a switch that creates an alert when a BPDU is received from an endpoint.

bring your own device (BYOD) Allows users to use their own personal mobile devices for business purposes.

broadcast storm prevention Steps that can be taken to avert a broadcast storm.

brute force attack An attack in which every possible combination of letters, numbers, and characters is combined to attempt to determine the user's password.

buffer overflow attack An attack that occurs when a process attempts to store data in RAM beyond the boundaries of a fixed-length storage buffer.

bug bounty A monetary reward given for uncovering a software vulnerability.

burning Lighting paper on fire to destroy the data on it.

business continuity plan (BCP) A strategic document that provides alternative modes of operation for business activities that, if interrupted, could result in a significant loss to the enterprise.

business impact analysis (BIA) A process that identifies the business functions and quantifies the impact a loss of these functions may have on business operations.

business partners Commercial entities with whom an organization has an alliance.

business partnership agreement (BPA) A contract between two or more business partners that is used to establish the rules and responsibilities of each partner.

C

cable lock A device inserted into the security slot of a portable device to prevent its theft.

cache A type of high-speed memory that stores recently used information so that it can be quickly accessed again at a later time.

call manager A platform used to provide telephony, video, and web conferences.

Canonical Encoding Rules (CER) An X.509 encoding format.

captive portal AP An infrastructure on public access WLANs that uses a standard web browser to provide information, and gives the wireless user the opportunity to agree to a policy or present valid login credentials to provide a higher degree of security.

capture the flag (CTF) An exercise in which a series of challenges is planted as a competition between participants.

card cloning Unauthorized duplication of smart cards.

carrier unlocking Uncoupling a phone from a specific wireless provider.

cat A Linux text file manipulation tool for displaying an entire file.

cellular telephony A communications network in which the coverage area is divided into hexagon-shaped cells.

Center for Internet Security (CIS) A nonprofit community-driven organization.

certificate attributes Fields in an X.509 digital certificate that are used when parties negotiate a secure connection.

certificate authority (CA) The entity that is responsible for digital certificates.

certificate chaining Linking several certificates together to establish trust between all the certificates involved.

Certificate Revocation List (CRL) A list of certificate serial numbers that have been revoked.

Certificate Signing Request (CSR) A user request for a digital certificate.

chain of custody A process that shows evidence was always under strict control and no unauthorized person was given the opportunity to corrupt the evidence.

Challenge-Handshake Authentication Protocol (CHAP) A weak authentication framework protocol that has been replaced by more secure versions.

change control policy A policy that stipulates the processes to be followed for implementing system changes.

change management policy A written document that defines the types of changes that can be made and under what circumstances.

channel overlays Conflicting frequency channels in a Wi-Fi network.

chmod A Linux text file manipulation tool for changing file permissions.

choose your own device (CYOD) Employees choose from a limited selection of approved devices, but the employee pays the upfront cost of the device while the business owns the contract.

Cipher Block Chaining Message Authentication Code (CBC-MAC) A component of CCMP that provides data integrity and authentication.

cipher suite A named combination of the encryption, authentication, and message authentication code (MAC) algorithms that are used with TLS and SSL.

clean desk space A policy designed to ensure that all confidential or sensitive materials, either in paper form or electronic, are removed from a user's workspace and secured.

cleanup Returning all systems back to normal following a penetration test.

client-side execution and validation Input validation that is performed by the user's web browser.

client-side request forgery An attack that takes advantage of an authentication "token" that a website sends to a user's web browser to imitate the identity and privileges of the victim.

closed circuit television (CCTV) Activity captured by video surveillance cameras that transmit a signal to a specific and limited set of receivers.

closed source Proprietary information owned by an entity that has an exclusive right to it.

cloud A remote facility for computing.

cloud access security broker (CASB) A set of software tools or services that resides between an enterprise's on-prem infrastructure and the cloud provider's infrastructure.

cloud computing An on-demand infrastructure to a shared pool of configurable computing resources that can be rapidly provisioned and released.

Cloud Controls Matrix A specialized framework of cloud-specific security controls.

cloud native controls A cloud security control that is inherent to the cloud computing platforms and offered by the cloud computing providers to their customers.

cloud platforms A pay-per-use computing model in which customers pay only for the online computing resources they need.

Cloud Security Alliance (CSA) An organization whose goal is to define and raise awareness of best practices to help secure cloud computing environments.

cloud security audit An independent examination of cloud service controls.

cloud service providers Entities that offer cloud computing resources.

code reuse of third-party libraries and SDKs Using existing software or software development kits (SDKs) in a new application.

code signing digital certificate Certificate used by software developers to digitally sign a program to prove that the software comes from the entity that signed it and that no unauthorized third party has altered it.

code signing Digitally signing applications.

cold site A remote site that provides office space; the customer must provide and install all the equipment needed to continue operations.

collectors Network devices that gather traffic.

collision When two files have the same hash.

command and control (C&C) A structure that sends instructions to infected bot computers.

common name (CN) The name of the device protected by the digital certificate.

Common Vulnerabilities and Exposures (CVE) A tool that identifies vulnerabilities in operating systems and application software.

Common Vulnerability Scoring System (CVSS) A numeric rating system of the impact of a vulnerability.

communication plan A formalized plan that outlines the internal and external constituents who need to be informed of an incident, how they should be informed, and when it should take place.

community cloud A type of cloud that is open only to specific organizations that have common concerns.

compensating controls Controls that provide an alternative to normal controls that for some reason cannot be used.

competitors Threat actors who launch attacks against an opponent's system to steal classified information.

compilers Programs that create binary machine code from human source code.

computer-based training (CBT) Using a computer to deliver instruction.

conditional access Dynamically assigning roles to subjects based on a set of rules.

confidential The highest level of data sensitivity.

configuration review An examination of the software settings for a vulnerability scan.

consensus A social engineering principle that involves being influenced by what others do.

constraints Limitations that make security a challenge for embedded systems and specialized devices.

container A more reduced instance of virtualization.

container security Protecting containers from attacks.

containerization Separating storage into separate business and personal "containers."

containment An incident response plan step for limiting the damage of the incident and isolating those systems that are impacted to prevent further damage.

content management Tools used to support the creation and subsequent editing and modification of digital content by multiple employees.

content/URL filtering A process used by a firewall to monitor websites accessed through HTTP to create custom filtering profiles.

context-aware authentication Using a contextual setting to validate a user.

continuity of operation planning (COOP) A federal initiative that is intended to encourage organizations to address how critical operations will continue under a broad range of negative circumstances.

continuous delivery Moving the code to each stage as it is completed.

continuous deployment Continual code implementation.

continuous integration Ensuring that security features are incorporated at each stage.

continuous monitoring Examining the processes in real-time instead of at the end of a stage.

continuous validation Ongoing approvals of code.

control risk The probability that financial statements are materially misstated because of failures in the system of controls used by an organization.

controller AP An AP that is managed through a dedicated wireless LAN controller (WLC).

corporate owned A mobile device that is purchased and owned by the enterprise.

corporate owned, personally enabled (COPE) Employees choose from a selection of company approved devices.

corrective controls Controls that are intended to mitigate or lessen the damage caused by an incident.

counter (CTR) A block cipher mode of operation that both the message sender and receiver access a counter, which computes a new value each time a ciphertext block is exchanged.

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) The encryption protocol used for WPA2 that specifies the use of a general-purpose cipher mode algorithm providing data privacy with AES.

credential harvesting Using the Internet and social media searches to perform reconnaissance.

credential policies Policies that address requirements for authentication credentials, such as the length and complexity of passwords.

credentialed scan A scan in which valid authentication credentials, such as usernames and passwords, are supplied to the vulnerability scanner to mimic the work of a threat actor who possesses these credentials.

criminal syndicates Threat actors who have moved from traditional criminal activities to more rewarding and less risky online attacks.

critical Data classified according to availability needs so that the function and mission would be severely impacted if compromised.

crossover error rate (CER) The biometric error rate in which the FAR and FRR are equal over the size of the population.

cross-site request forgery (CSRF) An attack that takes advantage of an authentication "token" that a website sends to a user's web browser to imitate the identity and privileges of the victim.

cross-site scripting (XSS) An attack that takes advantage of a website that accepts user input without validating it.

cryptography The practice of transforming information so that it is secure and cannot be understood by unauthorized persons.

cryptomalware Malware that encrypts all the files on the device so that none of them can be opened until a ransom is paid.

Cuckoo An automated malware analysis system.

curl A Linux command-line utility used to transfer data to or from a server.

custom firmware Firmware that is written by users to run on their own mobile devices.

Cyber Kill Chain An exploitation framework that outlines the steps of an attack in an integrated and end-to-end process like a "chain."

cybersecurity insurance Insurance that protects an organization by monetary compensation in the event of a successful attack.

D

dark web Part of the web is beyond the reach of a normal search engine and is the domain of threat actors.

data anonymization Changing data so that there is not a means to reverse the process to restore the data back to its original state.

data at rest Data that is stored on electronic media.

data backup Copying information to a different medium and storing it so that it can be used in the event of a disaster.

data breach notification law A law that requires user notification of a data breach.

data breach Stealing data to disclose it in an unauthorized fashion.

data classification policy A policy that outlines how to assign data type labels to data.

data controller The principal party for collecting data.

data custodian/steward An individual to whom day-to-day actions have been assigned by the owner.

data exfiltration Stealing data to distribute it to other parties.

data exposure Disclosing sensitive data to attackers.

data governance policy A policy that defines who is responsible for the data, how it can be accessed, how it should be used, and how its integrity can be maintained.

data in processing Data actions being performed by "endpoint devices," such as printing a report from a desktop computer.

data in transit Actions that transmit the data across a network.

data loss prevention (DLP) A system of security tools used to recognize and identify data that is critical to the organization and ensure it is protected.

data loss The destruction of data so that it cannot be recovered.

data masking Creating a copy of the original data but obfuscating any sensitive elements.

data minimization Limiting the collection of personal information to that which is directly relevant and necessary to accomplish a specific task.

data owner The person responsible for the data.

data privacy officer (DPO) A manager who oversees data privacy compliance and manages data risk.

data processor A proxy who acts on behalf of data controller.

data retention policy A policy that specifies how long data should retained after it has fulfilled its initial purpose.

data sanitization The process of cleaning data to provide privacy.

data sovereignty Country-specific requirements that apply to data.

data storage Third-party facilities used for storing important data.

dd An imaging utility used for generating a physical copy.

dead code A section of an application that executes but performs no meaningful function.

decryption The process of changing encrypted text into the original text.

default settings Settings that are predetermined by the vendor for usability and ease of use (but not security) so the user can immediately begin using the product.

degaussing Permanently destroying an entire hard drive by reducing or eliminating its magnetic field.

demilitarized zone (DMZ) An area that separates threat actors from defenders.

deprovisioning Removing a resource that is no longer needed.

detective controls Controls designed to identify any threat that has reached the system.

deterrent controls Controls that attempt to discourage security violations before they occur.

development stage A stage of application development in which the requirements for the application are established and it is confirmed that the application meets the intended business needs before the actual coding begins.

device driver manipulation An attack that alters a device driver from its normal function.

DHCP snooping A security technology in a switch that drops unacceptable DHCP traffic.

diagram A visual mapping of security appliances.

Diamond Model of Intrusion Analysis A framework for examining network intrusion events that uses four core interconnected elements that comprise any event.

dictionary attack A password attack that creates encrypted versions of common dictionary words and compares them against those in a stolen password file.

differential backup A backup that copies any data that has changed since last full backup.

dig A Linux command-line utility used for DNS diagnostics.

digital certificate A technology used to associate a user's identity to a public key and that has been "digitally signed" by a trusted third party.

direct access An attack vector in which a threat actor can gain direct physical access to the computer.

directory service A database stored on the network itself that contains information about users and network devices.

directory traversal An attack that takes advantage of vulnerability so that a user can move from the root directory to other restricted directories.

disablement An action by an administration to suspend an account.

disabling unnecessary open ports and services Turning off any service that is not being used and closing any unnecessary TCP ports to enhance security.

disassociation attack A wireless attack in which false deauthentication or disassociation frames are sent to an AP that appear to come from another client device, causing the client to disconnect.

disaster recovery plan (DRP) A written document that details the process for restoring IT resources following an event that causes a significant disruption in service.

Discretionary Access Control (DAC) An access control scheme that is the least restrictive, giving an owner total control over objects.

distance considerations The process of making location selections of where backups should be stored.

Distinguished Encoding Rules (DER) An X.509 encoding format.

distributed denial of service (DDoS) An attack that uses many computers to perform a DoS attack.

diversity The ability to include different technologies, third-party vendors, controls, and cryptographic solutions in a BCP.

DLL injection An attack that inserts code into a running process through a DLL to cause a program to function in a different way than intended.

DNS hijacking An attack that infects an external DNS server with IP addresses pointing to malicious sites.

DNS poisoning An attack that substitutes DNS addresses in a local lookup table so that the computer is automatically redirected to an attacker's device.

DNS sinkhole A technique that changes a normal DNS request to a preconfigured IP address pointing to a device that will drop all received packets.

dnsenum A Kali Linux utility that lists DNS information of a domain.

domain name resolution Mapping computer and device names to IP addresses.

Domain Name System Security Extensions (DNSSEC) A protocol that adds additional resource records and message header information for improved security.

domain reputation An attack in which the status of a site is manipulated to earn a low domain reputation score.

domain validation digital certificate Certificate that verifies the identity of the entity that has control over the domain name.

downgrade attack An attack in which the system is forced to abandon the current higher security mode of operation and "fall back" to implementing an older and less secure mode.

drone An unmanned aerial vehicle (UAV) without a human pilot on board to control its flight.

dual power supply A specialized computer power supply that can provide redundancy.

dump file A snapshot of the process that was executing and any modules that were loaded for an app at a specific point in time.

dumpster diving Digging through trash receptacles to find information that can be useful in an attack.

dynamic code analysis Examining code after the source code is compiled and when all components are integrated and running.

dynamic resource allocation Deprovision computing resources when they are no longer needed.

E

EAP-FAST An Extensible Authentication Protocol that securely tunnels any credential form for authentication (such as a password or a token) using TLS.

EAP-TLS An Extensible Authentication Protocol that uses digital certificates for authentication.

EAP-TTLS An Extensible Authentication Protocol that securely tunnels client password authentication within Transport Layer Security (TLS) records.

east-west traffic The movement of data from one server to another server within a data center.

Echo Request packets used by the TCP/IP Internet Control Message Protocol.

edge Computing that is performed at or very near to the source of data instead of relying on the cloud or on-prem for processing.

e-discovery Identifying, collecting, and producing electronically stored information (ESI) in response to a request in an investigation or lawsuit.

efficacy rate The benefit achieved of a biometric identifier.

elasticity Flexibility or resilience in code development.

electronic lock A type of lock that uses buttons that must be pushed in the proper sequence for opening.

eliciting information Gathering data.

elliptic curve cryptography (ECC) An algorithm that uses elliptic curves instead of prime numbers to compute keys.

email digital certificate A certificate that allows a user to digitally sign and encrypt mail messages.

embedded system Computer hardware and software contained within a larger system that is designed for a specific function.

Encapsulating Security Payload (ESP) An IPsec protocol that encrypts packets.

encryption The process of changing plaintext into ciphertext.

end of life (EOL) A statement that a product has reached the end of its "useful life" and the manufacturer will no longer market, sell, or update it after a specified date.

end of service (EOS) A statement that the end of support has been reached and no maintenance services or updates are provided.

endpoint detection and response (EDR) Robust tools that monitor endpoint events and take immediate action.

enterprise method Authentication for the WPA2 Enterprise model.

entropy The measure of randomness of a data-generating function.

environmental disasters Disasters such as floods, hurricanes, and tornados that can impact an enterprise.

ephemeral key A temporary key that is used only once before it is discarded.

eradication An incident response plan step for finding the cause of the incident and temporarily removing any systems that may be causing damage.

error handling A programming error that does not properly trap an error condition.

errors Human mistakes in selecting one setting over another without considering the security implications.

escalation Adding steps as the result of a data breach being classified as a "major incident."

European Union General Data Protection Directive (GDPR) A regulation regarding data protection and privacy in the European Union and the European Economic Area (EEA).

evil twin An AP set up by an attacker to mimic an authorized AP and capture transmissions, so a user's device will unknowingly connect to the evil twin instead of the authorized AP.

exercises Simulated activities used to test an incident response plan.

expiration The date of a digital certificate when it ceases to function.

exploitation frameworks A series of documented processes that serve as models of the thinking and actions of threat actors.

Extended Validation (EV) certificate Certificate that requires more extensive verification of the legitimacy of the business than does a domain validation digital certificate.

Extensible Authentication Protocol (EAP) A framework for transporting authentication protocols that defines the format of the messages.

eXtensible Markup Language (XML) A markup language designed to store information.

external disasters Disasters such as environmental disasters that are outside the organization.

external media access A device with a USB connection that can function as a host (to which other devices may be connected such as a USB flash drive) for access to media.

external risk A risk from outside an organization.

external Threat actors who work outside the enterprise.

extranet A private network that can also be accessed by authorized external customers, vendors, and partners.

F

facial recognition A biometric authentication that views the user's face and is becoming increasingly popular on smartphones.

fake telemetry Fictitious data on a honeypot of how certain software features are used, application crashes, and general usage statistics and behavior.

false acceptance rate (FAR) The frequency at which imposters are accepted as genuine when using biometric authentication.

false negative Failure to raise an alarm when there is a problem.

false positive Raising an alarm when there is no problem.

false rejection rate (FRR) The frequency that legitimate users are rejected when using biometric authentication.

familiarity A social engineering principle that portrays the victim as well known and well received.

Faraday cage A metallic enclosure that prevents the entry or escape of an electromagnetic field.

federation Single sign-on for networks owned by different organizations, also called *federated identity management (FIM)*.

fencing A tall, permanent structure to keep out unauthorized personnel.

field-programmable gate array (FPGA) A hardware integrated circuit (IC) that can be programmed by the user.

file and code repositories A storage area in which victims of an attack can upload malicious files and software code that can then be examined by others to learn more about these attacks and craft their defenses.

file integrity monitors A system that detects any changes within the files that may indicate a cyberattack.

File Transfer Protocol (FTP) An unsecure TCP/IP protocol for transferring files.

fileless virus A type of malware that takes advantage of native services and processes that are part of the OS to avoid detection and carry out its attacks.

filesystem permissions A method for protecting files managed by the OS.

financial loss The monetary loss as a result of lost productivity.

fine A financial penalty assessed against an organization as the result of a data breach.

fingerprint A physiological biometric identifier that has become the most common type of authentication.

fire suppression Attempts to reduce the impact of a fire.

firewall Hardware or software that is designed to limit the spread of malware.

firmware OTA updates Mobile operating system patches and updates that are distributed as an over-the-air (OTA) update.

firmware Software that is embedded into hardware to provide low-level controls and instructions.

fog A decentralized computing infrastructure in which data, compute capabilities, storage, and applications are located between the data source and the cloud.

footprinting Gathering information from outside the organization.

forensics The application of science to questions that are of interest to the legal profession.

forward proxy A computer or an application program that intercepts user requests from the internal secure network and then processes those requests on behalf of the users.

framework A series of documented processes used to define policies and procedures for implementation and management of security controls in an enterprise environment.

FTK Imager A package of multiple forensics tools combined into a single suite that has a common user interface and can more easily exchange information among the different tools.

FTP Secure (FTPS) Using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to encrypt commands sent over the control port in an FTP session.

full backup The starting point for all backups; it copies the entire set of data.

full disk encryption The encryption of all user data on a mobile device.

full tunnel A VPN technology in which all traffic is sent to the VPN concentrator and is protected.

functional recovery plan A plan that addresses the steps to be taken to restore processes if necessary.

fusion center A formal repository of information from enterprises and the government used to share information on the latest attacks.

fuzzing Providing random input to a program in an attempt to trigger exceptions, such as memory corruption, program crashes, or security breaches.

G

gait A person's manner of walking that can be used as a physiological biometric identifier.

gamification Using game-based scenarios for instruction.

generator A device powered by diesel, natural gas, or propane gas to generate electricity.

generic account An account not tied to a specific person.

geofencing Using the mobile device's GPS to define geographical boundaries where an app can be used.

geographic dispersal Spreading sites across a larger area to mitigate the impact of an environmental disaster.

geographical consideration Firewall rules that are in effect depending on the location of an endpoint.

geolocation The process of identifying the geographical location of a device.

Global Positioning System (GPS) A satellite-based navigation system that provides information to a GPS receiver anywhere on (or near) the earth where there is an unobstructed line of sight to four or more GPS satellites.

GPS tagging (geo-tagging) Adding geographical identification data to media such as digital photos taken on a mobile device.

Gray box A penetration testing level in which the testers are given limited knowledge of the network and some elevated privileges.

gray hat hackers Attackers who attempt to break into a computer system without the organization's permission to publicly disclose the attack and shame the organization into taking action.

grep A Linux text file manipulation tool used for searching for keyword.

guest account An account given to a temporary user.

H

hacker A person who uses advanced computer skills to attack computers.

hacktivists A group of attackers that is strongly motivated by ideology.

hardware firewall A firewall that runs on a separate device.

hardware root of trust Security checks that begin with hardware checks.

Hardware Security Module (HSM) A removable external cryptographic device.

hash An algorithm that creates a unique digital fingerprint.

hashing The process of creating a digital fingerprint.

head A Linux text file manipulation tool for displaying the first 10 lines of a file.

heat map A software tool that provides a visual representation of the wireless signal coverage and strength.

heating, ventilation, and air conditioning (HVAC) Environmental systems that provide and regulate heating and cooling.

heuristic monitoring A monitoring technique that uses an algorithm to determine if a threat exists.

high availability across zones Using multiple geographical cloud zones and regions to provide reliability and resiliency.

high availability The ability to withstand all outages while providing continuous processing for critical applications.

high resiliency The ability to quickly recover from resource vs. security constraints.

HMAC-based one-time password (HOTP) A one-time password that changes when a specific event occurs.

hoax A false warning often contained in an email message claiming to come from the IT department.

honeyfiles Software and data files on a honeypot that appear to be authentic but are actually imitations of real data files.

honeynet A network set up with intentional vulnerabilities.

honeypot A computer located in an area with limited security that serves as "bait" to threat actors and is intentionally configured with security vulnerabilities.

host intrusion detection system (HIDS) A software-based application that runs on an endpoint computer and can detect that an attack has occurred.

host intrusion prevention system (HIPS) Software that monitors endpoint activity to immediately block a malicious attack by following specific rules.

host-based firewall A software firewall that runs as a program on the local device to block or filter traffic coming into and out of the computer.

hot aisle/cold aisle A layout used to reduce the heat in a data center by managing air flow.

hot site A duplicate of the production site that has all the equipment needed for an organization to continue running, including office space and furniture, telephone jacks, computer equipment, and a live telecommunications link.

hotspot A location where users can access the Internet with a wireless signal.

hping A Linux command-line utility that sends custom TCP/IP packets.

HTML 5 The current version of HTML that can be used as a "clientless" VPN on an endpoint so that no additional software must be installed.

HTTP Response Header A header that can inform the browser how to function while communicating with the website.

hybrid cloud A combination of public and private clouds.

hybrid warfare influence campaign Influence campaigns used on social media and other sources.

Hypertext Transport Protocol Secure (HTTPS) HTTP sent over TLS (Transport Layer Security) or SSL (Secure Sockets Layer).

I

identification An incident response plan step for determining whether an event is actually a security incident.

identification of critical systems Recognizing processes that aid the mission-essential function.

identity fraud (also called *impersonation*) Masquerading as a real or fictitious character and then playing out the role of that person with a victim.

identity theft Taking personally identifiable information to impersonate someone.

IEEE 802.1x A standard, originally developed for wired networks, that provides a greater degree of security by implementing port-based authentication.

ifconfig A Linux command-line utility that displays network configuration information such as the IP address, network mask, and gateway for all physical and virtual network adapters.

image backup A backup that captures the entire contents of the disk to enable an entire restoration of the contents of the disk to a new hard disk or computer.

IMAP (Internet Mail Access Protocol) A more recent and advanced electronic email system for managing incoming email; the current version is IMAP4.

impact assessment A means for measuring the effectiveness of the organization's activities.

impersonation (also called *identity fraud*) Masquerading as a real or fictitious character and then playing out the role of that person with a victim.

Impossible Travel Analyzing and denying a second user login attempt based on the time and distance of the prior attempt.

improper input handling A programming error that does not filter or validate user input to prevent a malicious action.

incident response plan A set of written instructions for reacting to a security incident.

incident response process Action steps to be taken when a cyber incident occurs; also serve as the elements of an incident response plan.

incident response team A group that is responsible for responding to security incidents.

incremental backup A backup that copies any data that has changed since last full backup or last incremental backup.

indicator of compromise (IOC) An indicator that malicious activity is occurring but is still in the early stages.

industrial camouflage An attempt to make the physical presence of a building as nondescript as possible so that to a casual viewer, the building does not look like it houses anything important.

industrial control systems (ICS) Systems that control locally or at remote locations by collecting, monitoring, and processing real-time data to control machines.

influence campaigns Using social engineering to sway attention and sympathy in a particular direction.

information life cycle The flow of an information system's data (and metadata) from data creation to the time when it becomes obsolete.

infrared Light that is next to visible light on the light spectrum and was once used for data communications.

Infrastructure as a Service (IaaS) A cloud computing model that provides unlimited computing, storage, and network resources that the enterprise can use to build its own virtual infrastructure in the cloud.

inherent risk The current risk level given the existing set of controls.

initialization vector (IV) A 24-bit value that changes each time a packet is encrypted.

injections Attacks that introduce new input to exploit a vulnerability.

inline A system that is connected directly to the network and monitors the flow of data as it occurs.

insider threat Attackers who manipulate data from the position of a trusted employee.

instance awareness The ability for security appliances to differentiate between different instances of cloud apps.

integer overflow attack An attack that changes the value of a variable to something outside the range that the programmer had intended by using an integer overflow.

integrity measurement An "attestation mechanism" designed to ensure that an application is running only known and approved executables.

intent/motivation Reasons for an attack by threat actors.

intermediate certificate authority (CA) An entity that processes the CSR and verifies the authenticity of the user on behalf of a certificate authority (CA).

internal disasters Disasters such as a fire in a data center that are inside the organization.

internal risk A risk that comes from within an organization.

internal Threat actors who work inside the enterprise.

Internet of Things (IoT) Connecting any device to the Internet for the purpose of sending and receiving data to be acted upon.

Internet Protocol schema A standard guide for assigning IP addresses to devices.

Internet Protocol Security (IPsec) A protocol suite for securing Internet Protocol (IP) communications.

Internet Protocol version 6 (IPv6) The next generation of the IP protocol that addresses the weaknesses of IPv4 and also provides several other significant improvements.

intimidation To frighten and coerce by threat.

intranet A private network that belongs to an organization and can only be accessed by approved internal users.

intrusive scan A vulnerability scan that attempts to employ any vulnerabilities which it finds, much like a threat actor would.

invoice scam A fictitious overdue invoice that demands immediate payment.

IP theft Stealing intellectual property such as an invention or a work that the organization or its customers may own.

ipconfig A Windows command-line utility that displays network configuration information such as the IP address, network mask, and gateway for all physical and virtual network adapters.

IPFIX (IP Flow Information Export) A session sample protocol similar to NetFlow but with additional capabilities.

iris A thin circular structure in the eye that can be used for authentication.

ISO 27001 A standard that provides requirements for an information security management system (ISMS).

ISO 27002 A "code of practice" for information security management within an organization and contains 114 different control recommendations.

ISO 27701 An extension to ISO 27001 and is a framework for managing privacy controls to reduce the risk of privacy breach to the privacy of individuals.

ISO 31000 A standard that contains controls for managing and controlling risk.

isolation Segregating both the attacker and the infected systems from reaching other devices.

J

jailbreaking Circumventing the installed built-in limitations on Apple iOS devices.

jamming Intentionally flooding the radio frequency (RF) spectrum with extraneous RF signal "noise" that creates interference and prevents communications from occurring.

job rotation The act of moving individuals from one job responsibility to another.

journalctl A Linux utility for querying and displaying log files.

jump box A minimally configured administrator server (either physical or virtual) within the DMZ that is used to connect two dissimilar security zones while providing tightly restricted access between them.

K

Kerberos An authentication system developed by the Massachusetts Institute of Technology (MIT) and used to verify the identity of networked users.

key escrow A process in which keys are managed by a third party, such as a trusted CA.

key exchange The process of sending and receiving secure cryptographic keys.

key length The number of bits in a key.

key management The administration by PKI of all the elements involved in digital certificates for digital certificate management of public keys and digital certificates.

key stretching A password hashing algorithm that requires significantly more time than standard hashing algorithms to create the digest.

keylogger Hardware or software that silently captures and stores each keystroke that a user types on the computer's keyboard.

knowledge-based authentication Using perception, thought processes, and understanding for a biometric identifier.

L

lack of vendor support A lack of expertise to handle system integration.

last known good configuration A Microsoft Windows option for earlier versions in which the OS can be rolled back to the last time that the device properly booted.

lateral movement Moving through a network looking for additional systems threat actors can access from their elevated position.

Layer 2 Tunneling Protocol (L2TP) A VPN protocol that does not offer any encryption or protection so it is usually paired with IPsec.

LDAP injection attacks Attacks, similar to SQL injection attacks, that can occur when user input is not properly filtered in an LDAP session.

least privilege A policy that ensures only the minimum amount of privileges necessary to perform a job or function should be allocated.

legacy platform A platform that is no longer in widespread use, often because it has been supplanted or replaced by an updated version of that earlier technology.

legal hold A judicial act that mandates data in an investigation cannot be modified, deleted, erased, or otherwise edited.

lessons learned An incident response plan step for completing incident documentation, performing detailed analysis to increase security and improve future response efforts.

level of capability/sophistication Power and complexity capabilities of threat actors.

lighting Illumination of a secured area so that it can be viewed after dark.

lightweight cryptography A category of cryptography that has fewer features and is less robust than normal cryptography.

Lightweight Directory Access Protocol (LDAP) A directory service that is a simpler subset of the Directory Access Protocol (DAP).

likelihood of occurrence A determination of how realistic the chance is that a given threat will compromise an asset.

live boot media A bootable OS on an external device such as a USB device that contains a complete OS that may be used in recovery.

load balancing A technology that can help to evenly distribute work across a network.

lockout An automatic action that prevents access to an account until a security administrator reviews the incident and removes the lockout.

log A record of events that occur.

log reviews An analysis of log data.

logger A Linux text file manipulation tool for adding content to syslog file.

logic bomb Computer code that is typically added to a legitimate program but lies dormant and evades detection until a specific logical event triggers it.

longevity The useful lifetime of service of a cipher.

loop prevention A technology that uses the IEEE 802.1d standard spanning-tree protocol (STP) to avert a network loop.

low latency A small amount of time that occurs between when a byte is input into a cryptographic algorithm and the time the output is obtained.

low-power devices Small electronic devices that consume very small amounts of power.

MAC cloning attack An attack that spoofs a MAC address on a device so that the switch changes its MAC address table to reflect the new association of that MAC address with the port to which the attacker's device is connected.

M

MAC flooding attack An attack in which the memory of a switch is flooded with spoofed packets to force it to function like a network hub and broadcast frames to all ports.

machine/computer digital certificate Certificate used to verify the identity of a device in a network transaction.

macro A series of instructions that can be grouped together as a single command.

malicious flash drive A USB flash drive infected with malware.

malicious USB cable A USB cable embedded with a Wi-Fi controller that can receive commands from a nearby device to send malicious commands to the connected mobile device.

malware Malicious software that enters a computer system without the user's knowledge or consent and then performs an unwanted and harmful action.

managed security service provider (MSSP) A specialized type of managed service provider (MSP) that can assist with or fully assume the cybersecurity defenses of an organization.

managed service provider (MSP) An entity that delivers services—such as network, application, infrastructure, and security—through ongoing and regular support as well as active administration of those resources.

managerial controls Controls that use administrative methods.

Mandatory Access Control (MAC) An access control scheme that is the most restrictive by assigning users' access controls strictly according to the custodian's desires.

mandatory vacations Requirement that all employees take vacations.

maneuvering Conducting unusual behavior when threat hunting.

man-in-the-browser (MITB) An attack that intercepts communication between a browser and the underlying computer.

man-in-the-middle (MITM) An attack that intercepts legitimate communication to eavesdrop on the conversation or impersonate one of the parties.

man-made disasters Disasters such as industrial accidents, oil spills, terrorist attacks, and transportation accidents that can impact an enterprise.

mantrap An area designed as an air gap to separate a nonsecure area from a secured area.

manual peer reviews Reviews performed by software engineers and developers paired together or grouped in larger teams to laboriously examine each line of source code looking for vulnerabilities.

masking Creating a copy of the original data but making unintelligible any sensitive elements.

mean time between failures (MTBF) A statistical value that is the average time until a component fails, cannot be repaired, and must be replaced.

mean time to recovery (MTTR) The average time for a device to recover from a failure that is not a terminal failure.

Measured Boot A boot attestation procedure in which the computer's firmware logs the boot process so it can be sent to a trusted server to assess the security.

measurement system analysis (MSA) Using scientific tools to determine the amount of variation that is added to a process by a measurement system.

Media Access Control (MAC) address filtering A method for controlling access to a WLAN based on the device's MAC address.

memdump A Linux utility that "dumps" system memory.

memorandum of understanding (MOU) A document that describes an agreement between two or more parties that is not legally enforceable.

memory leak A situation that occurs when, due to a programming error, memory is not freed when the program has finished using it.

memory management Failure of programmers to create secure code, which allows vulnerabilities that manipulate computer RAM.

metadata Data that describes information about other data.

MicroSD HSM A hardware security module in a small consumer-oriented form factor.

microservices APIs Specialized APIs based on a microservices architecture.

microservices architecture Smaller and more specialized elements, each of which manages its own database, generates its own logs, and handles user authentication.

mission-essential function The activity that serves as the core purpose of the enterprise.

mitigation Addressing a risk by making the risk less serious.

MITRE ATT&CK A knowledge base of attacker techniques that have been broken down and classified in detail.

mobile application management (MAM) Tools that are used for distributing and controlling access to apps on mobile devices.

mobile content management (MCM) A system that is tuned to provide content management to mobile devices used by employees in an enterprise.

mobile device management (MDM) Tools that allow a device to be managed remotely by an organization.

moisture detection A sensor that can detect water leaks, dampness, or increased moisture levels.

monitoring service An external third-party service that can provide additional resources to assist an organization in their cybersecurity defenses.

motion detection A sensor that can determine an object's change in position in relation to its surroundings.

motion recognition Using high-end video surveillance cameras that record when they detect movement.

MS-CHAP The Microsoft version of CHAP.

multifactor authentication (MFA) Using more than one type of authentication credential.

multifunctional printer (MFP) A device that combines the functions of a printer, copier, scanner, and fax machine.

multimedia messaging service (MMS) Text messages in which pictures, video, or audio can be included.

multiparty Risks that impact multiple organizations.

multipath A technique for creating more than one physical path between devices and a SAN.

N

Narrowband Internet of Things (NB-IoT) A low-power wide area network (LPWAN) radio technology standard.

near field communication (NFC) A set of standards used to establish communication between devices in very close proximity

Nessus A vulnerability assessment tool.

NetFlow A session sampling protocol feature on Cisco routers that collects IP network traffic as it enters or exits an interface.

netstat A Windows and Linux command-line utility that provides detailed information about current network connections as well as network connections for the Transmission Control Protocol (TCP) network interfaces and routing tables.

network access control (NAC) A technique that examines the current state of a system or network device before it is allowed to connect to the network.

network address translation gateway A cloud-based technology that performs NAT translations for cloud services.

network hardware security module A special trusted network computer that performs cryptographic operations.

network intrusion detection system (NIDS) A technology that watches for attacks on the network and reports back to a central device.

network intrusion prevention system (NIPS) A technology that monitors network traffic to immediately react to block a malicious attack.

Network Location A setting that designates the network type (Not Configured, Public, or Private).

network sensors Sensing devices used to monitor traffic.

network-attached storage (NAS) A single storage device that serves files over the network.

next generation firewall (NGFW) A firewall that has additional functionality beyond a traditional firewall such as the ability to filter packets based on applications.

next generation secure web gateway (SWG) A virtual cloud device that combines several features into a single product.

NIC teaming Configuring multiple network interface card (NIC) adapters into one or more software-based virtual network adapters for redundancy and speed.

NIST Cybersecurity Framework (CSF) A measuring stick against which companies can compare their cybersecurity practices relative to the threats they face.

NIST Risk Management Framework (RMF) A guidance document designed to help organizations assess and manage risks to their information and systems.

nmap A tool for network discovery and security auditing.

noise detection A sensor that can detect a suspicious noise through microphones.

non-credentialed scan A vulnerability scan that provides no authentication information to the tester.

nondisclosure agreement (NDA) A legal contract between parties that specifies how confidential material will be shared but not disclosed to others without permission.

nonintrusive scan A vulnerability scan that does not attempt to exploit the vulnerability but only records that it was discovered.

nonpersistent A characteristic of a system so that any changes or additions are not saved when the system returns to its original state.

nonrepudiation The process of proving that a user performed an action.

normalization Organizing data within a database to minimize redundancy.

nslookup A Windows command-line utility used as a DNS diagnostic utility.

nxlog A multi-platform log management tool that supports various platforms, log sources, and formats.

O

OAuth (Open Authorization) An open source federation framework.

obfuscation Making something obscure or unclear.

obfuscation/camouflaged code Writing an application in such a way that its inner functionality is difficult for an outsider to understand.

object detection Using high-end video surveillance cameras that can identify a suspicious objective and sound an alert.

offboarding Actions to be taken when an employee leaves an enterprise.

offline brute force attack An attack in which a stolen digest file is loaded onto a computer to be cracked using password cracking software.

offline CA A certificate authority that is not directly connected to a network.

off-premises A computing resource hosted and supported by a third party.

onboarding The tasks associated with hiring a new employee.

online brute force attack An attack in which the same account is continuously attacked by entering different passwords.

online CA A certificate authority that is directly connected to a network.

Online Certificate Status Protocol (OCSP) A process that performs a real-time lookup of a certificate's status.

on-premises Computing resources located on the campus of the organization.

on-premises platform Software and technology located within the physical confines of an enterprise, which is usually consolidated in the company's data center.

Opal A set of specifications for SEDs developed by the Trusted Computing Group (TCG).

Open ID A federation technology that provides user authentication information.

open method A wireless network mode in which no authentication is required.

open permissions User access over files that should have been restricted.

open ports and services Devices and services that are often configured to allow the most access so that the user can then close those ports that are specific to that organization.

open source Anything that could be freely used without restrictions.

open source firewall A firewall that is freely available.

open source intelligence (OSINT) Publicly accessible information.

Open Source Interconnection (OSI) seven-layer model A conceptual model that illustrates network functionality.

OpenSSL A cryptography library that offers open source applications of the TLS protocol.

operational controls Controls implemented and executed by people.

Operational Technology (OT) The source of a DDoS attack in which endpoints can be programmed and have an IP address.

order of volatility The specific order in which evidence from an incident should be examined.

organizational policies Policies that relate to the management and functioning of the organization as a whole.

OS event logs Logs produced by an operating system that document incorrect login attempts, system setting modifications, application or system failures, and other events.

out-of-band management Using an independent and dedicated channel to reach a device for management purposes.

outsourced code development Contracting with third parties to assist the organization in the development and writing of a software program or app.

OWASP (Open Web Application Security Project) A group that monitors web attacks.

P

pagefile A file that contains data moved from RAM to the hard drive due to a lack of RAM space.

pass the hash An attack in which the attacker steals the digest of an NTLM password and pretends to be the user by sending that hash to the remote system to be authenticated.

passive A system that is connected to a device that receives a copy of network traffic.

passive reconnaissance Searching online for publicly accessible information.

password A secret combination of letters, numbers, and/or characters that only the user should have knowledge of.

Password Authentication Protocol (PAP) A weak version of Extensible Authentication Protocol (EAP).

password complexity A setting that determines passwords must meet complexity requirements.

password crackers Software designed to break passwords through matching.

password history A setting that determines how many days a new password must be kept before the user can change it.

password keys A hardware-based device to store passwords.

password reuse A setting that determines the number of unique new passwords a user must use before an old password can be reused.

password spraying An attack that uses one or a small number of commonly used passwords when trying to log in to several different user accounts.

password vault A secure repository in which users can store their passwords.

patch An officially released software security update intended to repair a vulnerability.

pathping A Windows command-line utility that tests the connection to each hop.

Payment Card Industry Data Security Standard (PCI DSS) A compliance standard to provide a minimum degree of security for handling customer card information.

payment method An electronic alternative to using cash or a credit card for payments; also called *contactless payment system*.

penetration testing A type of test that attempts to exploit vulnerabilities just as a threat actor would.

perfect forward secrecy Public key systems that generate different random public keys for each session.

persistence A process in which a load balancer creates a link between an endpoint and a specific network server for the duration of a session.

persistence The determination, resolve, and perseverance necessary for performing a successful penetration test.

personal identification number (PIN) A passcode made up of numbers only.

Personal Information Exchange (PFX) An X.509 file format that is the preferred file format for creating certificates to authenticate applications or websites.

Personally Identifiable Information (PII) Data that could potentially identify a specific individual.

pharming Exploiting how a URL is converted into its corresponding IP address to redirect traffic away from its intended target to a fake website instead.

phishing campaign A broad initiative that uses a variety of tools to train users to resist phishing attacks.

phishing Sending an email or displaying a web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information or taking action.

phishing simulations Exercises to help employees recognize phishing emails.

phone call A process to use a smartphone to verify a user's login attempt.

physical controls Controls that implement security in a defined structure and location.

physical locks A type of lock that requires a key for opening.

ping A Windows and Linux command-line utility that tests the ability of the source computer to reach a specified destination computer.

pinning Hard-coding a digital certificate within a program that is using the certificate.

pivot Turning to other systems to be compromised.

Platform as a Service (PaaS) A cloud computing model of a software platform on which the enterprise or users can build their own applications and then host them.

platform/vendor-specific guides Guidelines that only apply to specific products.

playbook A linear-style checklist of required steps and actions needed to successfully respond to specific incident types and threats.

pointer/object dereference A flaw that results in a pointer given a NULL instead of valid value.

point-to-multipoint A network topology in which one device is connected to multiple devices.

point-to-point A network topology in which one device is connected to one other device.

policy A document that outlines specific requirements or rules that must be met.

port mirroring (port spanning) A technology on a managed switch that copies traffic that occurs on some or all ports to a designated monitoring port on the switch.

port TAP (test access point) A device that transmits the send and receive data streams simultaneously on separate dedicated channels so that all data arrives at the monitoring tool in real time.

Post Office Protocol (POP) A TCP/IP protocol for receiving email messages; the current version is POP3.

post-quantum cryptography Cryptographic algorithms that are secure against an attack by a quantum computer.

potentially unwanted programs (PUPs) Software that users do not want on their computer.

power distribution unit (PDU) A device fitted with multiple electrical outputs and designed to distribute electric power, especially to racks of computers and networking equipment located within a data center.

PowerShell A task automation and configuration management framework from Microsoft.

predictive analysis An evaluation used for discovering an attack before it occurs.

preparation An incident response plan step for equipping IT staff, management, and users to handle potential incidents when they arise.

prepending Influencing a subject before an event occurs.

preservation of the evidence Ensuring that important proof is not corrupted or even destroyed.

preshared key (PSK) The authentication model used in WPA that requires a secret key value to be entered into the AP and all approved wireless devices prior to communicating.

pretexting Using impersonation to obtain private information.

preventative controls Controls that prevent the threat from coming in contact with the vulnerability.

Privacy Enhancement Mail (PEM) An X.509 file format that uses DER encoding and can have multiple certificates.

privacy notice A document that outlines how the organization uses personal information it collects.

privacy The state or condition of being free from public attention, observation, or interference to the degree that the person chooses.

private cloud A type of cloud that is created and maintained on a private network.

private information sharing centers Organizations participating in closed source information that restrict both access to data and participation.

private Restricted data with a medium level of confidentiality.

private subnet A VPC for backend servers that are not publicly accessible.

privilege escalation Moving to more advanced resources that are normally protected from an application or user.

privileged access management Technologies and strategies for controlling elevated privilege access.

production stage An application development stage in which the application is released to be used in its actual setting.

proper input validation Accounting for errors such as incorrect user input.

proprietary Data that belongs to the enterprise.

proprietary firewall A firewall that is owned by an entity who has an exclusive right to it.

protected cable distribution A system of cable conduits used to protect classified information transmitted between two secure areas.

Protected EAP (PEAP) An EAP method designed to simplify the deployment of 802.1x by using Microsoft Windows logins and passwords.

Protected Health Information (PHI) Data about a person's health status, provision of health care, or payment for health care.

provenance Evidence in a forensics investigation that can be traced to the very beginning.

provisioning The enterprise-wide configuration, deployment, and management of multiple types of IT system resources.

proximity A sensor that detects the presence of an object when it enters the sensor's field.

pseudo-anonymization Changing data so there is a means to reverse the process to restore the data back to its original state.

public cloud A type of cloud in which the services and infrastructure are offered to all users with access provided remotely through the Internet.

public Data for which there is no risk of release.

public information sharing centers A repository by which open source cybersecurity information is collected and disseminated.

public key infrastructure (PKI) The underlying infrastructure for the management of public keys used in digital certificates.

public notifications and disclosures Contacting relevant stakeholders in the event of a data breach.

public subnet A VPC with a subnet for public-facing web server applications.

pulping Breaking paper into wood cellulose fibers after the ink is removed to destroy the data on it.

pulverizing "Hammering" the paper into dust to destroy the data on it.

Purple Team A penetration testing team that provides real-time feedback between the Red and Blue Teams to enhance the testing.

push notification A message displayed on a smartphone through an authentication app.

push notification services Sending SMS text messages to selected users or groups of users.

Python A popular programming language that can run on several OS platforms.

Q

qualitative risk assessment An approach that uses an "educated guess" based on observation.

quality assurance (QA) The process of the verification of quality.

Quality of Service (QoS) A set of network technologies used to guarantee a network's ability to dependably serve resources and high-priority applications to endpoints.

quantitative risk assessment An approach that attempts to create "hard" numbers associated with the risk of an element in a system by using historical data.

quantum communication A subcategory of quantum cryptography used to secure telecommunications.

quantum computer A computer that relies on quantum physics using atomic-scale units (*qubits*) that can be both 0 and 1 at the same time.

quarantine The process that holds a suspicious document.

R

race condition A situation in software that occurs when two concurrent threads of execution access a shared resource simultaneously.

radio frequency identification (RFID) A wireless set of standards used to transmit information from paper-based tags to a proximity reader.

RADIUS (Remote Authentication Dial-In User Service) An industry standard authentication service with widespread support across nearly all vendors of networking equipment.

RAID (Redundant Array of Independent Drives or **Redundant Array of Inexpensive Disks)** A technology that uses multiple hard disk drives for increased reliability and performance.

rainbow tables Large pregenerated data sets of encrypted passwords used in password attacks.

ransomware Malware that prevents a user's endpoint device from properly and fully functioning until a fee is paid.

Raspberry Pi A low-cost credit-card-sized computer motherboard.

real-time operating system (RTOS) An operating system that is specifically designed for an SoC in an embedded system.

receptionist A person who staffs a public reception area to provide a level of active security.

reconnaissance Learning as much about a person as possible in order to appear as genuine while acting as an imposter.

recovery An incident response plan step for ensuring no threat remains, permitting affected systems to return to normal operation.

recovery point objective (RPO) The maximum length of time that an organization can tolerate between backups.

recovery time objective (RTO) The length of time it will take to recover data that has been backed up.

Red Team A penetration testing team that scans for vulnerabilities and then exploits them.

redundancy The use of duplicated equipment to improve the availability of the system.

refactoring Changing the design of existing code.

reference architecture An authoritative source of information.

registration authority An entity that is responsible for verifying the credentials of the applicant for a digital certificate.

registry A database that contains low-level settings used by the Windows OS and for those applications that elect to use it.

regulations Standards typically developed by established professional organizations or government agencies using the expertise of seasoned security professionals.

regulations that affect risk posture Controls based upon regulatory requirements that may be required regardless of risk.

regulatory/jurisdiction A law that governs the site in which cloud data resides.

remote access Trojan (RAT) Malware that infects a computer like a Trojan but also gives the threat agent unauthorized remote access to the victim's computer by using specially configured communication protocols.

remote access VPN A user-to-LAN VPN connection for remote users.

remote wipe A technology used to erase sensitive data stored on the mobile device.

replay An attack that copies data and then uses it for an attack.

replication A copy of a virtual machine that is automatically launched.

reputation damage A tarnished reputation to an organization as the result of a data breach.

reputation Public perception.

request for comments (RFC) Documents that are authored by technology bodies employing specialists, engineers, and scientists who are experts in those areas.

residual risk The risk level that remains after additional controls are applied.

resource exhaustion attacks An attack that depletes parts of memory and interferes with the normal operation of the program in RAM to give an attacker access to the underlying OS.

resource policies Written statements that outline who is the responsible party for cloud computing, what are their duties and responsibilities, and how cloud computing can be used.

resource vs. security constraint A limitation in providing strong cryptography due to the "tug-of-war" between the available resources (time and energy) and the security provided by cryptography.

resources and funding Financial capabilities of threat actors.

response and recovery controls Steps that should be taken when responding to an incident in order to recoup from it.

restoration order The sequence in which different systems are reinstated after a disaster.

retention policy Part of an incident response plan that outlines how long the evidence of the incident should be retained.

retina A layer at the back (posterior) portion of the eyeball that contains cells sensitive to light and can be used for biometric authentication.

reverse proxy A proxy that routes requests coming from an external network to the correct internal server.

revert to known state An OS feature to restore it to an earlier point in time prior to a problem.

rich communication services (RCS) Mobile device communication which can convert a texting app into a live chat platform and supports pictures, videos, location, stickers, and emojis.

right to audit clause A part of a cloud contract that gives the customer the legal right to review logs.

rights management The authority of the owner of the data to impose restrictions on its use.

risk A situation that involves exposure to some type of danger.

risk appetite A level of risk that is considered acceptable.

risk awareness Raising of understanding of what risks exist, their potential impacts, and how they are managed.

Risk Control Self-Assessment (RCSA) A methodology by which management and staff at all levels collectively work to identify and evaluate risks.

risk matrix/heatmap A visual color-coded tool that lists the impact and likelihood of risks.

risk register A list of potential threats and associated risks often shown as a table.

Risky IP address Examining the IP address that was used to attempt a login and comparing it against a list of IP addresses involved in malicious activities.

robot sentries Automated devices that patrol and use CCTV with object detection in public areas.

rogue AP An unauthorized AP that allows an attacker to bypass many network security configurations and opens the network and its users to attacks.

Role-Based Access Control An access control scheme that is considered a more "real-world" access control that based on a user's job function within an organization.

role-based awareness training Specialized training that is customized to the specific role that an employee holds in the organization.

root digital certificate A certificate that is created and verified by a CA.

rooting Circumventing the installed built-in limitations on Android devices.

rootkit Malware that can hide its presence and the presence of other malware on the computer.

route A Linux command-line utility that displays and manipulates IP routing tables to create static routes to specific hosts.

route security The trust of packets sent through a router.

rsyslog (rocket-fast system for log processing) An open source utility for forwarding log messages in an IP network on UNIX devices.

Rule-Based Access Control An access control scheme that can dynamically assign roles to subjects based on a set of rules defined by a custodian.

rules of engagement Limitations or parameters in a penetration test.

runbook A series of automated conditional steps that are part of an incident response procedure.

S

safe A ruggedized steel box with a lock.

salt A random string added to a hash algorithm for enhanced security.

sandbox A "container" in which an application can be run so that it does not impact the underlying OS.

scalability Expandability from small projects to very large projects.

scanless A tool for using websites to perform port scan.

scarcity When something is in short supply.

scheduling Protocols that are used in load balancers to distribute the workload among devices.

screen lock A security setting that prevents a mobile device from being accessed until the user enters the correct passcode permitting access.

script kiddies Individuals who want to perform attacks yet lack the technical knowledge to carry them out.

SEAndroid A security-enhanced version of the Android operating system that uses MAC.

secrets management A process that enables strong security and improved management of a microservices-based architecture.

secure areas Areas that separate threat actors from defenders.

secure coding practices and techniques A methodology to create secure software applications.

secure cookie A cookie that is only sent to the server with an encrypted request over the secure HTTPS protocol.

Secure FTP (SFTP) A protocol that encrypts and compresses all FTP data and commands.

Secure Real-time Transport Protocol (SRTP) A protocol for providing protection for Voice over IP (VoIP) communications.

Secure Shell (SSH) An encrypted alternative to the Telnet protocol that is used to access remote computers.

Secure Sockets Layer (SSL) An early and widespread cryptographic transport algorithm that is now considered obsolete.

Secure/Multipurpose Internet Mail Extensions (S/MIME) A protocol for securing email messages.

Security Assertion Markup Language (SAML) An Extensible Markup Language (XML) standard that allows secure web domains to exchange user authentication and authorization data.

security groups Segmented computing resources formed into logical groupings to create network perimeters.

security guards People who patrol and monitor restricted areas.

Security Information and Event Management (SIEM) A tool that consolidates real-time security monitoring and management of security information with analysis and reporting of security events.

security key A hardware device inserted into a computer port that contains all the necessary cryptographic information to authenticate the user.

security of the ML algorithms A risk associated with the vulnerabilities in AI-powered cybersecurity applications and their devices.

Security Orchestration, Automation and Response (SOAR) A tool designed to help security teams manage and respond to the very high number of security warnings and alarms by combining comprehensive data gathering and analytics in order to automate incident response.

self-encrypting drives (SEDs) Drives that can automatically encrypt any data stored on them.

self-signed A signed digital certificate that does not depend upon any higher-level authority for authentication.

sensitive Data that could cause catastrophic harm to the company if disclosed, such as technical specifications for a new product.

sensors Electronic devices that supplement the work of security guards.

sentiment analysis The process of computationally identifying and categorizing opinions, usually expressed in response to textual data, in order to determine the writer's attitude toward a particular topic.

separation of duties The practice of requiring that processes should be divided between two or more individuals.

serverless infrastructure A cloud infrastructure in which the capacity planning, installation, setup, and management are all invisible to the user because they are handled by the cloud provider.

server-side execution and validation Input validation that uses the server to perform the validation.

server-side request forgery (SSRF) An attack that takes advantage of a trusting relationship between web servers.

service account A user account that is created explicitly to provide a security context for services running on a server.

service-level agreement (SLA) A service contract between a vendor and a client that specifies what services will be provided, the responsibilities of each party, and any guarantees of service.

services integration The combined management function of multiple services into a single entity.

Session Initiation Protocol (SIP) A signaling protocol that is used to create "sessions" between multiple participants and is widely found in voice telephony products.

session replay An attack in which an attacker attempts to impersonate the user by using the user's session token.

sFlow A packet sampling protocol that gives a statistical sampling instead of the actual flow of packets.

shadow IT Employees who become frustrated with the slow pace of acquiring technology, so they purchase and install their own equipment or resources in violation of company policies.

shared account An account used by more than one user.

shimming Transparently adding a small coding library that intercepts calls made by a device and changes the parameters passed between the device and the device driver.

short message service (SMS) Text messages of a maximum of 160 characters.

shoulder surfing Watching an individual enter a security code on a keypad.

shredding Cutting paper into small strips or particles to destroy the data on it.

sideloading Downloading unofficial apps.

signage Written information on fencing that explains the area is restricted.

signature-based monitoring A monitoring technique that examines network traffic to look for well-known patterns and compares the activities against a predefined signature.

Simple Mail Transfer Protocol (SMTP) A TCP/IP protocol for sending email messages.

Simple Network Management Protocol (SNMP) A popular protocol used to manage network equipment that is supported by most network equipment manufacturers.

simulation A hands-on exercise using a realistic scenario to thoroughly test each step of an incident response plan.

Simultaneous Authentication of Equals (SAE) A component of WPA3 that is designed to increase security at the time of the handshake when the key is being exchanged.

Single Loss Expectancy (SLE) The expected monetary loss every time a risk occurs.

single point of failure A component or entity in a system that, if it no longer functions, will disable the entire system.

single sign-on (SSO) Using one authentication credential to access multiple accounts or applications.

site risk assessment A detailed evaluation of the processes performed at a site and how they can be impacted.

site survey An in-depth examination and analysis of a WLAN site.

site-to-site VPN A VPN connection in which multiple sites can connect to other sites over the Internet.

skimming A process in which a threat actor attaches a small device that fits inside a card reader to capture information.

smart card A card that contains information used as part of the authentication process.

smart meters Digital meters that measure the amount of utilities consumed.

smishing Using short message service (SMS) text messages to perform phishing.

sn1per A penetration testing tool.

snapshot The current state of all settings and data used for forensics and data backups.

SNMPv3 The current version of the Simple Network Management Protocol used to manage network equipment that supports authentication and encryption.

social engineering Gathering data by relying on the weaknesses of individuals.

social media analysis Viewing social media posts of potential candidates to look for important insights.

social media influence campaign An influence campaign exclusively used on social media.

Software as a Service (SaaS) A cloud computing model of hosted software environment.

software compliance and licensing Risks associated with violating software license agreements.

software diversity Software development technique in which two or more functionally identical variants of a program are developed from the same specification but by different programmers or programming teams.

software firewall A firewall that runs as a program or service on a device, such as a computer or router.

software-defined network (SDN) A network that virtualizes parts of the physical network so that it can be more quickly and easily reconfigured.

software-defined visibility (SDV) A framework that allows users to create programs in which critical security functions that previously required manual intervention can now be automated.

someone you know Authentication based on being validated by another person.

something you are Authentication based on the features and characteristics of the individual.

something you can do Authentication based on actions that the user can uniquely perform.

something you exhibit Authentication based on a genetically determined characteristic.

something you have Authentication based on the approved user having a specific item in his or her possession.

something you know Authentication based on something the user knows but no one else knows.

somewhere you are Authentication based on where the user is located.

spam Unsolicited email that is sent to a large number of recipients.

spear phishing Targeting specific users.

spim Spam delivered through instant messaging (IM) instead of email.

split tunneling A VPN technology in which only some traffic is sent to the VPN concentrator and is protected, while other traffic directly accesses the Internet.

spyware Tracking software that is deployed without the consent or control of the user.

SQL injection An attack that inserts statements to manipulate a database server using Structured Query Language commands.

SSAE SOC 2 Type II A standard for reports on internal controls report that reviews how a company safeguards customer data and how well those controls are operating.

SSAE SOC 2 Type III A standard for reports on internal controls that can be freely distributed.

SSL stripping An attack that manipulates SSL functions by intercepting an HTTP connection.

staging stage A stage in application development that tests to verify that the code functions as intended.

stakeholder management Identifying the relevant stakeholders within the organization who need to be initially informed of an incident and then kept up to date.

standard A document approved through consensus by a recognized standardization body.

standard naming conventions Using the same conventions for assigning names to appliances.

stapling A process for verifying the status of a certificate by sending queries at regular intervals to receive a signed time-stamped response.

state actors Government-sponsored attackers who launch cyberattacks against the foes of the state.

stateful packet filtering A firewall that keeps a record of the state of a connection between an internal computer and an external device and then makes decisions based on the connection as well as the conditions.

stateless packet filtering A firewall that looks at the incoming packet and permits or denies it based on specific conditions.

static code A value that never changes.

static code analysis Analyzing and testing software from a security perspective before the source code is compiled.

steganography Hiding the existence of data within another type of file, such as an image file.

storage area network (SAN) A dedicated network storage facility that provides access to data storage over a high-speed network.

storage segmentation Separating business data from personal data on a mobile device.

stored procedure A subroutine available to applications that access a relational database.

strategic counterintelligence Gaining information about the attacker's intelligence collection capabilities.

strategic intelligence The collection, processing, analysis, and dissemination of intelligence for forming policy changes.

stream cipher An algorithm that takes one character and replaces it with one character.

Structured Query Language (SQL) A language used to view and manipulate data that is stored in a relational database.

Structured Threat Information Expression (STIX) A language and format used to exchange cyberthreat intelligence.

Subject Alternative Name (SAN) Also known as a *Unified Communications Certificate* (*UCC*), certificate primarily used for Microsoft Exchange servers or unified communications.

subscriber identity module (SIM) card An integrated circuit that securely stores information used to identify and authenticate the IoT device on a cellular network.

supervisory control and data acquisition (SCADA) A system that controls multiple industrial control systems (ICS).

supply chain A network that moves a product from the supplier to the customer and is made up of vendors that supply raw material, manufacturers who convert the material into products, warehouses that store products, distribution centers that deliver them to the retailers, and retailers who bring the product to the consumer.

swap file A file that contains data moved from RAM to the hard drive due to a lack of RAM space.

symmetric cryptographic algorithm Encryption that uses a single key to encrypt and decrypt a message.

syslog (system logging protocol) A standard to send system log or event messages to a server.

syslog-ng An open source utility for UNIX devices that includes content filtering.

system integration Connectivity between the systems of an organization and its third parties.

system on a chip (SoC) A single microprocessor chip on which all the necessary hardware components are contained.

T

tabletop A monthly 30-minute discussion of a scenario conducted in an informal and stress-free environment.

TACACS+ The current version of the Terminal Access Control Access Control System (TACACS) authentication service.

tags Identifying labels for evidence bags that have a description of the item, a numeric identifier, date, collection location, and other relevant data.

tail A Linux text file manipulation tool for displaying the last 10 lines of a file.

tailgating Following an authorized user through a door.

tainted training data for machine learning A risk associated with attackers can attempt to alter the training data that is used by ML.

Tcpdump A command-line packet analyzer.

Tcpreplay A tool for editing packets and then replaying the packets back onto the network to observe their behavior.

technical controls Controls that are incorporated as part of hardware, software, or firmware.

temperature detection A sensor that can detect a sudden increase or decrease in temperature or the temperature of an object in relation to its surroundings.

terms of agreement A document that defines what is expected from both the organization and its users.

testing stage A stage in which an application is tested for any errors that could result in a security vulnerability.

tethering Using a mobile device with an active Internet connection to share that connection with other mobile devices through Bluetooth or Wi-Fi.

theHarvester A Kali Linux utility that provides information about email accounts, user names, and hostnames/subdomains from public sources.

thin client A computer that runs from resources stored on a central cloud server instead of a localized hard drive.

third parties External entities outside of the organization.

third-party app store A site from which unofficial apps can be downloaded.

third-party solution A data destruction technique that requires specialized equipment from an outside source.

third-party solutions Cloud security controls that are available from external sources.

third-party updates Patch updates for application and utility software.

threat actor Individuals or entities who are responsible for cyber incidents against the technology equipment of enterprises and users.

threat feeds Cybersecurity data feeds that provide information on the latest threats.

threat hunting Proactively searching for cyber threats that thus far have gone undetected in a network.

threat map An illustration of cyberthreats overlaid on a diagrammatic representation of a geographical area.

time of check/time of use A software check of the state of a resource before using that resource.

time of day Restrictions regarding limiting when a user can log in to their account to access resources.

time offset The amount of time added to or subtracted from Coordinated Universal Time (UTC) to arrive at the current "actual" (called *civil*) time.

time stamp The recorded time that an event took place irrespective of the location of the endpoint.

time-based login A user account login that is based on a specific day and time.

time-based one-time password (TOTP) A one-time password that changes after a set period of time.

token A small device with a window display.

token key A hardware device inserted into a computer port that contains all the necessary cryptographic information to authenticate the user.

tokenization Obfuscating sensitive data elements into a random string of characters and then stores them in a database for retrieval as needed.

traceroute A Linux command-line utility that shows the details about the path a packet takes from a computer or device to a destination.

tracert A Windows command-line utility that shows the details about the path a packet takes from a computer or device to a destination.

transference Transferring the responsibility of a risk to a third party.

transit gateway An Amazon Web Services (AWS) technology that allows organizations to connect all existing virtual private clouds (VPC), physical data centers, remote offices, and remote gateways into a single managed source.

Transport Layer Security (TLS) A widespread cryptographic transport algorithm that replaces SSL.

Transport mode An IPsec mode that encrypts only the data portion (payload) of each packet yet leaves the header unencrypted.

Trojan An executable program that masquerades as performing a benign activity but also does something malicious.

trust A social engineering principle to inspire confidence in a victim.

trust model The type of trust relationship that can exist between individuals or entities.

Trusted Automated Exchange of Intelligence Information (TAXII) An application protocol for exchanging cyberthreat intelligence over Hypertext Transfer Protocol Secure (HTTPS).

Trusted Platform Module (TPM) A chip on the motherboard of the computer that provides cryptographic services.

tunnel mode An IPsec mode that encrypts both the header and the data portion.

two-person integrity/control Using two security guards to prevent a single guard from acting maliciously.

typo squatting Purchasing the domain names of sites that are spelled similarly to actual sites.

U

UEFI (Unified Extensible Firmware Interface) An improved firmware interface developed to replace the BIOS.

unauthentication mode of operation An information service that provides a non-credentializing service such as confidentiality by a block cipher mode of operation.

unified endpoint management (UEM) A group or class of software tools has a single

management interface for mobile devices as well as computer devices.

unified threat management (UTM) An integrated device that combines several security functions.

uninterruptible power supply (UPS) A device that maintains power to equipment in case of an interruption in the primary electrical power source.

Universal Serial Bus (USB) connectors A port on mobile devices used for data transfer.

unmanned aerial vehicle (UAV) An aircraft without a human pilot on board to control its flight.

unmanned aerial vehicle An aircraft piloted by remote control or onboard computers.

unsecure protocols Also called insecure protocols, using protocols for telecommunications that do not provide adequate protections.

unsecured root accounts Unprotected accounts that give unfettered access to all resources.

urgency A social engineering principle that demands immediate action.

URL redirection An attack in which a user is redirected to another site.

USB On-the-Go (OTG) A specification that allows a mobile device with a USB connection to act as either a host or a peripheral used for external media access.

user account An approved identity between a user and an endpoint, network, or service.

user behavior analysis Looking at the normal behavior of users and how they interact with systems to create a picture of typical activity.

user digital certificate The endpoint of the certificate chain.

V

vault A ruggedized steel box with a lock.

vein One of the "tubes" that form part of the blood circulation system in the human body that carries oxygen-depleted blood back toward the heart.

vendor management The process organizations use to monitor and manage the interactions with all external third parties with which they have a relationship.

vendors Entities from whom an organization purchases goods and services.

version control Software that allow changes to be automatically recorded and, if necessary, "rolled back" to a previous version of the software.

virtual desktop infrastructure (VDI) Storing sensitive applications and data on a remote server that is accessed through a smartphone.

virtual firewall A firewall that runs in the cloud. Virtual firewalls are designed for settings, such as public cloud environments, in which deploying an appliance firewall would be difficult or even impossible.

virtual IP (VIP) An IP address and a specific port number that can be used to reference different physical servers.

virtual LAN (VLAN) A technology that allows scattered users to be logically grouped together even though they may be attached to different switches.

virtual machine escape protection Preventing VMs from directly interacting with the host operating system.

virtual machine sprawl avoidance Combating VM sprawl through using different procedures.

virtual network A cloud virtual network that connects services and resources like virtual machines and database applications with each other via a secure, encrypted, and private network.

virtual private network (VPN) A technology that enables the use of an unsecured public network as if it were a secure private network.

virtualization The means of managing and presenting computer resources by function without regard to their physical layout or location.

vishing Using a telephone call to perform phishing.

visitor log A paper or electronic record of people granted access to a property.

Visual Basic for Applications (VBA) An event-driven Microsoft programming language.

voice A physiological biometric identifier.

voice over IP (VoIP) A technology that uses a data-based IP network to add digital voice clients and new voice applications onto the IP network.

vulnerability database A repository of known vulnerabilities and information as to how they have been exploited.

vulnerability feeds Cybersecurity data feeds include that provide information on the latest vulnerabilities.

vulnerability scan A frequent and ongoing process, often automated, that continuously identifies vulnerabilities and monitors cybersecurity progress.

W

walkthrough A review by IT personnel of the steps of the plan by paying particular attention to the IT systems and services that may be targeted in an attack.

war driving Searching for wireless signals from an automobile or on foot while using a portable computing device.

war flying An efficient means of discovering a Wi-Fi signal using drones.

warm site A remote site that contains computer equipment but does not have active Internet or telecommunication facilities, and does not have backups of data.

watering hole attack An attack directed toward a smaller group of specific individuals, such as the major executives working for a manufacturing company.

weak configurations Configuration settings that are not properly implemented, resulting in vulnerabilities.

weak encryption Choosing a known vulnerable encryption mechanism.

weak key A key that causes the cipher to behave in unpredictable ways or may compromise overall security.

web application firewall A firewall that filters by examining the applications using HTTP.

whaling Targeting wealthy individuals or senior executives within a business through phishing.

White box A penetration testing level in which the testers are given full knowledge of the network and the source code of applications.

white hat hackers Also known as ethical attackers, a class of hackers that probe a system with an organization's permission for weaknesses and then privately provide that information to the organization.

White Team A penetration testing team that enforces the rules of the penetration testing.

whitelisting Approving in advance only specific applications to run on the OS so that any item not approved is either restricted or denied.

Wi-Fi A wireless network designed to replace or supplement a wired local area network (LAN). Also called *wireless local area network (WLAN)*.

Wi-Fi analyzer A software tool that helps to visualize the essential details of the wireless network.

Wi-Fi Direct The Wi-Fi Alliance implementation of WLAN ad hoc mode.

Wi-Fi Protected Access 2 (WPA2) The second generation of WPA security from the Wi-Fi Alliance that addresses authentication and encryption on WLANs and is currently the most secure model for Wi-Fi security.

Wi-Fi Protected Setup (WPS) An optional means of configuring security on wireless local area networks primarily intended to help users who have little or no knowledge of security to implement security quickly and easily on their WLANs.

wildcard digital certificate Certificate used to validate a main domain along with all subdomains.

WinHex A hexadecimal editor that can be used for forensics.

wireless access point placement Placing an AP in the optimum location.

Wireshark A popular GUI packet capture and analysis tool.

worm Malicious program that uses a computer network to replicate.

WPA3 The current generation of Wi-Fi Protected Access (WPA) whose goal is to deliver a suite of features to simplify security configuration for users while enhancing network security protections.

X

XML injection An attack that inserts statements to manipulate a database server using eXtensible Markup Language (XML).

Z

zero day A vulnerability that is exploited by attackers before anyone else even knows it exists.

zero trust A strategic initiative about networks that is designed to prevent successful attacks by eliminating the concept of trust from an organization's network architecture.

Zigbee A low-power, short-range, and low-data rate specification designed for occasional data or signal transmission from a sensor or IoT device.