

# Glossary

## Cybersecurity



### Terms and definitions from the certificate

## A

**Absolute file path:** The full file path, which starts from the root

**Access controls:** Security controls that manage access, authorization, and accountability of information

**Active packet sniffing:** A type of attack where data packets are manipulated in transit

**Address Resolution Protocol (ARP):** A network protocol used to determine the MAC address of the next router or device on the path

**Advanced persistent threat (APT):** An instance when a threat actor maintains unauthorized access to a system for an extended period of time

**Adversarial artificial intelligence (AI):** A technique that manipulates artificial intelligence (AI) and machine learning (ML) technology to conduct attacks more efficiently

**Adware:** A type of legitimate software that is sometimes used to display digital advertisements in applications

**Algorithm:** A set of rules used to solve a problem

**Analysis:** The investigation and validation of alerts

**Angler phishing:** A technique where attackers impersonate customer service representatives on social media

**Anomaly-based analysis:** A detection method that identifies abnormal behavior

**Antivirus software:** A software program used to prevent, detect, and eliminate malware and viruses

**Application:** A program that performs a specific task

**Application programming interface (API) token:** A small block of encrypted code that contains information about a user

**Argument (Linux):** Specific information needed by a command

**Argument (Python):** The data brought into a function when it is called

**Array:** A data type that stores data in a comma-separated ordered list

**Assess:** The fifth step of the NIST RMF that means to determine if established controls are implemented correctly

**Asset:** An item perceived as having value to an organization

**Asset classification:** The practice of labeling assets based on sensitivity and importance to an organization

**Asset inventory:** A catalog of assets that need to be protected

**Asset management:** The process of tracking assets and the risks that affect them

**Asymmetric encryption:** The use of a public and private key pair for encryption and decryption of data

**Attack surface:** All the potential vulnerabilities that a threat actor could exploit

**Attack tree:** A diagram that maps threats to assets

**Attack vectors:** The pathways attackers use to penetrate security defenses

**Authentication:** The process of verifying who someone is

**Authorization:** The concept of granting access to specific resources in a system

**Authorize:** The sixth step of the NIST RMF that refers to being accountable for the security and privacy risks that might exist in an organization

**Automation:** The use of technology to reduce human and manual effort to perform common and repetitive tasks

**Availability:** The idea that data is accessible to those who are authorized to access it

# B

**Baiting:** A social engineering tactic that tempts people into compromising their security

**Bandwidth:** The maximum data transmission capacity over a network, measured by bits per second

**Baseline configuration (baseline image):** A documented set of specifications within a system that is used as a basis for future builds, releases, and updates

**Bash:** The default shell in most Linux distributions

**Basic auth:** The technology used to establish a user's request to access a server

**Basic Input/Output System (BIOS):** A microchip that contains loading instructions for the computer and is prevalent in older systems

**Biometrics:** The unique physical characteristics that can be used to verify a person's identity

**Bit:** The smallest unit of data measurement on a computer

**Boolean data:** Data that can only be one of two values: either `True` or `False`

**Bootloader:** A software program that boots the operating system

**Botnet:** A collection of computers infected by malware that are under the control of a single threat actor, known as the "bot-herder"

**Bracket notation:** The indices placed in square brackets

**Broken chain of custody:** Inconsistencies in the collection and logging of evidence in the chain of custody

**Brute force attack:** The trial and error process of discovering private information

**Bug bounty:** Programs that encourage freelance hackers to find and report vulnerabilities

**Built-in function:** A function that exists within Python and can be called directly

**Business continuity:** An organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans

**Business continuity plan (BCP):** A document that outlines the procedures to sustain business operations during and after a significant disruption

**Business Email Compromise (BEC):** A type of phishing attack where a threat actor impersonates a known source to obtain financial advantage

## C

**Categorize:** The second step of the NIST RMF that is used to develop risk management processes and tasks

**CentOS:** An open-source distribution that is closely related to Red Hat

**Central Processing Unit (CPU):** A computer's main processor, which is used to perform general computing tasks on a computer

**Chain of custody:** The process of documenting evidence possession and control during an incident lifecycle

**Chronicle:** A cloud-native tool designed to retain, analyze, and search data

**Cipher:** An algorithm that encrypts information

**Cloud-based firewalls:** Software firewalls that are hosted by the cloud service provider

**Cloud computing:** The practice of using remote servers, applications, and network services that are hosted on the internet instead of on local physical devices

**Cloud network:** A collection of servers or computers that stores resources and data in remote data centers that can be accessed via the internet

**Cloud security:** The process of ensuring that assets stored in the cloud are properly configured and access to those assets is limited to authorized users

**Command:** An instruction telling the computer to do something

**Command and control (C2):** The techniques used by malicious actors to maintain communications with compromised systems

**Command-line interface (CLI):** A text-based user interface that uses commands to interact with the computer

**Comment:** A note programmers make about the intention behind their code

**Common Event Format (CEF):** A log format that uses key-value pairs to structure data and identify fields and their corresponding values

**Common Vulnerabilities and Exposures (CVE®) list:** An openly accessible dictionary of known vulnerabilities and exposures

**Common Vulnerability Scoring System (CVSS):** A measurement system that scores the severity of a vulnerability

**Compliance:** The process of adhering to internal standards and external regulations

**Computer security incident response teams (CSIRT):** A specialized group of security professionals that are trained in incident management and response

**Computer virus:** Malicious code written to interfere with computer operations and cause damage to data and software

**Conditional statement:** A statement that evaluates code to determine if it meets a specified set of conditions

**Confidentiality:** The idea that only authorized users can access specific assets or data

**Confidential data:** Data that often has limits on the number of people who have access to it

**Confidentiality, integrity, availability (CIA) triad:** A model that helps inform how organizations consider risk when setting up systems and security policies

**Configuration file:** A file used to configure the settings of an application

**Containment:** The act of limiting and preventing additional damage caused by an incident

**Controlled zone:** A subnet that protects the internal network from the uncontrolled zone

**Cross-site scripting (XSS):** An injection attack that inserts code into a vulnerable website or web application

**Crowdsourcing:** The practice of gathering information using public input and collaboration

**Cryptographic attack:** An attack that affects secure forms of communication between a sender and intended recipient

**Cryptographic key:** A mechanism that decrypts ciphertext

**Cryptography:** The process of transforming information into a form that unintended readers can't understand

**Cryptojacking:** A form of malware that installs software to illegally mine cryptocurrencies

**CVE Numbering Authority (CNA):** An organization that volunteers to analyze and distribute information on eligible CVEs

**Cybersecurity (or security):** The practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation

## D

**Data:** Information that is translated, processed, or stored by a computer

**Data at rest:** Data not currently being accessed

**Database:** An organized collection of information or data

**Data controller:** A person that determines the procedure and purpose for processing data

**Data custodian:** Anyone or anything that's responsible for the safe handling, transport, and storage of information

**Data exfiltration:** Unauthorized transmission of data from a system

**Data in transit:** Data traveling from one point to another

**Data in use:** Data being accessed by one or more users

**Data owner:** The person who decides who can access, edit, use, or destroy their information

**Data packet:** A basic unit of information that travels from one device to another within a network

**Data point:** A specific piece of information

**Data processor:** A person that is responsible for processing data on behalf of the data controller

**Data protection officer (DPO):** An individual that is responsible for monitoring the compliance of an organization's data protection procedures

**Data type:** A category for a particular type of data item

**Date and time data:** Data representing a date and/or time

**Debugger:** A software tool that helps to locate the source of an error and assess its causes

**Debugging:** The practice of identifying and fixing errors in code

**Defense in depth:** A layered approach to vulnerability management that reduces risk

**Denial of service (DoS) attack:** An attack that targets a network or server and floods it with network traffic

**Detect:** A NIST core function related to identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections

**Detection:** The prompt discovery of security events

**Dictionary data:** Data that consists of one or more key-value pairs

**Digital certificate:** A file that verifies the identity of a public key holder

**Digital forensics:** The practice of collecting and analyzing data to determine what has happened after an attack

**Directory:** A file that organizes where other files are stored

**Disaster recovery plan:** A plan that allows an organization's security team to outline the steps needed to minimize the impact of a security incident

**Distributed denial of service (DDoS) attack:** A type of denial or service attack that uses multiple devices or servers located in different locations to flood the target network with unwanted traffic

**Distributions:** The different versions of Linux

**Documentation:** Any form of recorded content that is used for a specific purpose

**DOM-based XSS attack:** An instance when malicious script exists in the webpage a browser loads

**Domain Name System (DNS):** A networking protocol that translates internet domain names into IP addresses

**Dropper:** A program or a file used to install a rootkit on a target computer

## E

**Elevator pitch:** A brief summary of your experience, skills, and background

**Encapsulation:** A process performed by a VPN service that protects your data by wrapping sensitive data in other data packets

**Encryption:** The process of converting data from a readable format to an encoded format

**Endpoint:** Any device connected on a network

**Endpoint detection and response (EDR):** An application that monitors an endpoint for malicious activity

**Eradication:** The complete removal of the incident elements from all affected systems

**Escalation policy:** A set of actions that outline who should be notified when an incident alert occurs and how that incident should be handled

**Event:** An observable occurrence on a network, system, or device

**Exception:** An error that involves code that cannot be executed even though it is syntactically correct



**Exclusive operator:** An operator that does not include the value of comparison

**Exploit:** A way of taking advantage of a vulnerability

**Exposure:** A mistake that can be exploited by a threat

**External threat:** Anything outside the organization that has the potential to harm organizational assets

## F

**False negative:** A state where the presence of a threat is not detected

**False positive:** An alert that incorrectly detects the presence of a threat

**Fileless malware:** Malware that does not need to be installed by the user because it uses legitimate programs that are already installed to infect a computer

**File path:** The location of a file or directory

**Filesystem Hierarchy Standard (FHS):** The component of the Linux OS that organizes data

**Filtering:** Selecting data that match a certain condition

**Final report:** Documentation that provides a comprehensive review of an incident

**Firewall:** A network security device that monitors traffic to or from a network

**Float data:** Data consisting of a number with a decimal point

**Foreign key:** A column in a table that is a primary key in another table

**Forward proxy server:** A server that regulates and restricts a person's access to the internet

**Function:** A section of code that can be reused in a program

## G

**Global variable:** A variable that is available through the entire program

**Graphical user interface (GUI):** A user interface that uses icons on the screen to manage different tasks on the computer

## H

**Hacker:** Any person or group who uses computers to gain unauthorized access to data

**Hactivist:** A person who uses hacking to achieve a political goal

**Hard drive:** A hardware component used for long-term memory

**Hardware:** The physical components of a computer

**Hash collision:** An instance when different inputs produce the same hash value

**Hash function:** An algorithm that produces a code that can't be decrypted

**Hash table:** A data structure that's used to store and reference hash values

**Health Insurance Portability and Accountability Act (HIPAA):** A U.S. federal law established to protect patients' health information

**Honeypot:** A system or resource created as a decoy vulnerable to attacks with the purpose of attracting potential intruders

**Host-based intrusion detection system (HIDS):** An application that monitors the activity of the host on which it's installed

**Hub:** A network device that broadcasts information to every device on the network

**Hypertext Transfer Protocol (HTTP):** An application layer protocol that provides a method of communication between clients and website servers

**Hypertext Transfer Protocol Secure (HTTPS):** A network protocol that provides a secure method of communication between clients and website servers

## I

**Identify:** A NIST core function related to management of cybersecurity risk and its effect on an organization's people and assets

**Identity and access management (IAM):** A collection of processes and technologies that helps organizations manage digital identities in their environment

**IEEE 802.11 (Wi-Fi):** A set of standards that define communication for wireless LANs

**Immutable:** An object that cannot be changed after it is created and assigned a value

**Implement:** The fourth step of the NIST RMF that means to implement security and privacy plans for an organization

**Improper usage:** An incident type that occurs when an employee of an organization violates the organization's acceptable use policies

**Incident:** An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies

**Incident escalation:** The process of identifying a potential security incident, triaging it, and handing it off to a more experienced team member

**Incident handler's journal:** A form of documentation used in incident response

**Incident response:** An organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach

**Incident response plan:** A document that outlines the procedures to take in each step of incident response

**Inclusive operator:** An operator that includes the value of comparison

**Indentation:** Space added at the beginning of a line of code

**Index:** A number assigned to every element in a sequence that indicates its position

**Indicators of attack (IoA):** The series of observed events that indicate a real-time incident

**Indicators of compromise (IoC):** Observable evidence that suggests signs of a potential security incident

**Information privacy:** The protection of unauthorized access and distribution of data

**Information security (InfoSec):** The practice of keeping data in all states away from unauthorized users

**Injection attack:** Malicious code inserted into a vulnerable application

**Input validation:** Programming that validates inputs from users and other programs

**Integer data:** Data consisting of a number that does not include a decimal point

**Integrated development environment (IDE):** A software application for writing code that provides editing assistance and error correction tools

**Integrity:** The idea that the data is correct, authentic, and reliable

**Internal hardware:** The components required to run the computer

**Internal threat:** A current or former employee, external vendor, or trusted partner who poses a security risk

**Internet Control Message Protocol (ICMP):** An internet protocol used by devices to tell each other about data transmission errors across the network

**Internet Control Message Protocol flood (ICMP flood):** A type of DoS attack performed by an attacker repeatedly sending ICMP request packets to a network server

**Internet Protocol (IP):** A set of standards used for routing and addressing data packets as they travel between devices on a network

**Internet Protocol (IP) address:** A unique string of characters that identifies the location of a device on the internet

**Interpreter:** A computer program that translates Python code into runnable instructions line by line

**Intrusion detection system (IDS):** An application that monitors system activity and alerts on possible intrusions

**Intrusion prevention system (IPS):** An application that monitors system activity for intrusive activity and takes action to stop the activity

**IP spoofing:** A network attack performed when an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to a network

**Iterative statement:** Code that repeatedly executes a set of instructions

## K

**KALI LINUX™:** An open-source distribution of Linux that is widely used in the security industry

**Kernel:** The component of the Linux OS that manages processes and memory

**Key-value pair:** A set of data that represents two linked items: a key, and its corresponding value

## L

**Legacy operating system:** An operating system that is outdated but still being used

**Lessons learned meeting:** A meeting that includes all involved parties after a major incident

**Library:** A collection of modules that provide code users can access in their programs

**Linux:** An open-source operating system

**List concatenation:** The concept of combining two lists into one by placing the elements of the second list directly after the elements of the first list

**List data:** Data structure that consists of a collection of data in sequential form

**Loader:** Malicious code that launches after a user initiates a dropper program

**Local Area Network (LAN):** A network that spans small areas like an office building, a school, or a home

**Local variable:** A variable assigned within a function

**Log:** A record of events that occur within an organization's systems

**Log analysis:** The process of examining logs to identify events of interest

**Logging:** The recording of events occurring on computer systems and networks

**Logic error:** An error that results when the logic used in code produces unintended results

**Log management:** The process of collecting, storing, analyzing, and disposing of log data

**Loop condition:** The part of a loop that determines when the loop terminates

**Loop variable:** A variable that is used to control the iterations of a loop

## M

**Malware:** Software designed to harm devices or networks

**Malware infection:** An incident type that occurs when malicious software designed to disrupt a system infiltrates an organization's computers or network

**Media Access Control (MAC) address:** A unique alphanumeric identifier that is assigned to each physical device on a network

**Method:** A function that belongs to a specific data type

**Metrics:** Key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application

**MITRE:** A collection of non-profit research and development centers

**Modem:** A device that connects your router to the internet and brings internet access to the LAN

**Module:** A Python file that contains additional functions, variables, classes, and any kind of runnable code

**Monitor:** The seventh step of the NIST RMF that means be aware of how systems are operating

**Multi-factor authentication (MFA):** A security measure that requires a user to verify their identity in two or more ways to access a system or network

## N

**nano:** A command-line file editor that is available by default in many Linux distributions

**National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF):** A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk

## **National Institute of Standards and Technology (NIST) Incident Response**

**Lifecycle:** A framework for incident response consisting of four phases: Preparation; Detection and Analysis; Containment, Eradication and Recovery, and Post-incident activity

**National Institute of Standards and Technology (NIST) Special Publication (S.P.) 800-53:** A unified framework for protecting the security of information systems within the U.S. federal government

**Network:** A group of connected devices

**Network-based intrusion detection system (NIDS):** An application that collects and monitors network traffic and network data

**Network data:** The data that's transmitted between devices on a network

**Network Interface Card (NIC):** Hardware that connects computers to a network

**Network log analysis:** The process of examining network logs to identify events of interest

**Network protocol analyzer (packet sniffer):** A tool designed to capture and analyze data traffic within a network

**Network protocols:** A set of rules used by two or more devices on a network to describe the order of delivery and the structure of data

**Network security:** The practice of keeping an organization's network infrastructure secure from unauthorized access

**Network segmentation:** A security technique that divides the network into segments

**Network traffic:** The amount of data that moves across a network

**Non-repudiation:** The concept that the authenticity of information can't be denied

**Notebook:** An online interface for writing, storing, and running code

**Numeric data:** Data consisting of numbers



**OAuth:** An open-standard authorization protocol that shares designated access between applications

**Object:** A data type that stores data in a comma-separated list of key-value pairs

**On-path attack:** An attack where a malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit

**Open-source intelligence (OSINT):** The collection and analysis of information from publicly available sources to generate usable intelligence

**Open systems interconnection (OSI) model:** A standardized concept that describes the seven layers computers use to communicate and send data over the network

**Open Web Application Security Project (OWASP):** A non-profit organization focused on improving software security

**Operating system (OS):** The interface between computer hardware and the user

**Operator:** A symbol or keyword that represents an operation

**Options:** Input that modifies the behavior of a command

**Order of volatility:** A sequence outlining the order of data that must be preserved from first to last

**OWASP Top 10:** A globally recognized standard awareness document that lists the top 10 most critical security risks to web applications

## P

**Package:** A piece of software that can be combined with other packages to form an application

**Package manager:** A tool that helps users install, manage, and remove packages or applications

**Packet capture (P-cap):** A file containing data packets intercepted from an interface or network

**Packet sniffing:** The practice of capturing and inspecting data packets across a network



**Parameter (Python):** An object that is included in a function definition for use in that function

**Parrot:** An open-source distribution that is commonly used for security

**Parsing:** The process of converting data into a more readable format

**Passive packet sniffing:** A type of attack where a malicious actor connects to a network hub and looks at all traffic on the network

**Password attack:** An attempt to access password secured devices, systems, networks, or data

**Patch update:** A software and operating system update that addresses security vulnerabilities within a program or product

**Payment Card Industry Data Security Standards (PCI DSS):** Any cardholder data that an organization accepts, transmits, or stores

**Penetration test (pen test):** A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes

**PEP 8 style guide:** A resource that provides stylistic guidelines for programmers working in Python

**Peripheral devices:** Hardware components that are attached and controlled by the computer system

**Permissions:** The type of access granted for a file or directory

**Personally identifiable information (PII):** Any information used to infer an individual's identity

**Phishing:** The use of digital communications to trick people into revealing sensitive data or deploying malicious software

**Phishing kit:** A collection of software tools needed to launch a phishing campaign

**Physical attack:** A security incident that affects not only digital but also physical environments where the incident is deployed

**Physical social engineering:** An attack in which a threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location

**Ping of death:** A type of DoS attack caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64KB

**Playbook:** A manual that provides details about any operational action

**Policy:** A set of rules that reduce risk and protect information

**Port:** A software-based location that organizes the sending and receiving of data between devices on a network

**Port filtering:** A firewall function that blocks or allows certain port numbers to limit unwanted communication

**Post-incident activity:** The process of reviewing an incident to identify areas for improvement during incident handling

**Potentially unwanted application (PUA):** A type of unwanted software that is bundled in with legitimate programs which might display ads, cause device slowdown, or install other software

**Private data:** Information that should be kept from the public

**Prepare:** The first step of the NIST RMF related to activities that are necessary to manage security and privacy risks before a breach occurs

**Prepared statement:** A coding technique that executes SQL statements before passing them on to a database

**Primary key:** A column where every row has a unique entry

**Principle of least privilege:** The concept of granting only the minimal access and authorization required to complete a task or function

**Privacy protection:** The act of safeguarding personal information from unauthorized use

**Procedures:** Step-by-step instructions to perform a specific security task

**Process of Attack Simulation and Threat Analysis (PASTA):** A popular threat modeling framework that's used across many industries

**Programming:** A process that can be used to create a specific set of instructions for a computer to execute tasks

**Protect:** A NIST core function used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats

**Protected health information (PHI):** Information that relates to the past, present, or future physical or mental health or condition of an individual

**Protecting and preserving evidence:** The process of properly working with fragile and volatile digital evidence

**Proxy server:** A server that fulfills the requests of its clients by forwarding them to other servers

**Public data:** Data that is already accessible to the public and poses a minimal risk to the organization if viewed or shared by others

**Public key infrastructure (PKI):** An encryption framework that secures the exchange of online information

**Python Standard Library:** An extensive collection of Python code that often comes packaged with Python

## Q

**Query:** A request for data from a database table or a combination of tables

**Quid pro quo:** A type of baiting used to trick someone into believing that they'll be rewarded in return for sharing access, information, or money

## R

**Rainbow table:** A file of pre-generated hash values and their associated plaintext

**Random Access Memory (RAM):** A hardware component used for short-term memory

**Ransomware:** A malicious attack where threat actors encrypt an organization's data and demand payment to restore access

**Rapport:** A friendly relationship in which the people involved understand each other's ideas and communicate well with each other

**Recover:** A NIST core function related to returning affected systems back to normal operation

**Recovery:** The process of returning affected systems back to normal operations

**Red Hat® Enterprise Linux®** (also referred to simply as Red Hat in this course): A subscription-based distribution of Linux built for enterprise use

**Reflected XSS attack:** An instance when malicious script is sent to a server and activated during the server's response

**Regular expression (regex):** A sequence of characters that forms a pattern

**Regulations:** Rules set by a government or other authority to control the way something is done

**Relational database:** A structured database containing tables that are related to each other

**Relative file path:** A file path that starts from the user's current directory

**Replay attack:** A network attack performed when a malicious actor intercepts a data packet in transit and delays it or repeats it at another time

**Resiliency:** The ability to prepare for, respond to, and recover from disruptions

**Respond:** A NIST core function related to making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process

**Return statement:** A Python statement that executes inside a function and sends information back to the function call

**Reverse proxy server:** A server that regulates and restricts the internet's access to an internal server

**Risk:** Anything that can impact the confidentiality, integrity, or availability of an asset

**Risk mitigation:** The process of having the right procedures and rules in place to quickly reduce the impact of a risk like a breach

**Root directory:** The highest-level directory in Linux

**Rootkit:** Malware that provides remote, administrative access to a computer

**Root user (or superuser):** A user with elevated privileges to modify the system

**Router:** A network device that connects multiple networks together

## S

**Salting:** An additional safeguard that's used to strengthen hash functions

**Scareware:** Malware that employs tactics to frighten users into infecting their device

**Search Processing Language (SPL):** Splunk's query language

**Secure File Transfer Protocol (SFTP):** A secure protocol used to transfer files from one device to another over a network

**Secure shell (SSH):** A security protocol used to create a shell with a remote system

**Security architecture:** A type of security design composed of multiple components, such as tools and processes, that are used to protect an organization from risks and external threats

**Security audit:** A review of an organization's security controls, policies, and procedures against a set of expectations

**Security controls:** Safeguards designed to reduce specific security risks

**Security ethics:** Guidelines for making appropriate decisions as a security professional

**Security frameworks:** Guidelines used for building plans to help mitigate risk and threats to data and privacy

**Security governance:** Practices that help support, define, and direct security efforts of an organization

**Security hardening:** The process of strengthening a system to reduce its vulnerabilities and attack surface

**Security information and event management (SIEM):** An application that collects and analyzes log data to monitor critical activities in an organization

**Security mindset:** The ability to evaluate risk and constantly seek out and identify the potential or actual breach of a system, application, or data

**Security operations center (SOC):** An organizational unit dedicated to monitoring networks, systems, and devices for security threats or attacks

**Security orchestration, automation, and response (SOAR):** A collection of applications, tools, and workflows that use automation to respond to security events

**Security posture:** An organization's ability to manage its defense of critical assets and data and react to change

**Security zone:** A segment of a company's network that protects the internal network from the internet

**Select:** The third step of the NIST RMF that means to choose, customize, and capture documentation of the controls that protect an organization

**Sensitive data:** A type of data that includes personally identifiable information (PII), sensitive personally identifiable information (SPII), or protected health information (PHI)

**Sensitive personally identifiable information (SPII):** A specific type of PII that falls under stricter handling guidelines

**Separation of duties:** The principle that users should not be given levels of authorization that would allow them to misuse a system

**Session:** a sequence of network HTTP requests and responses associated with the same user

**Session cookie:** A token that websites use to validate a session and determine how long that session should last

**Session hijacking:** An event when attackers obtain a legitimate user's session ID

**Session ID:** A unique token that identifies a user and their device while accessing a system

**Set data:** Data that consists of an unordered collection of unique values

**Shared responsibility:** The idea that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security

**Shell:** The command-line interpreter

**Signature:** A pattern that is associated with malicious activity

**Signature analysis:** A detection method used to find events of interest

**Simple Network Management Protocol (SNMP):** A network protocol used for monitoring and managing devices on a network

**Single sign-on (SSO):** A technology that combines several different logins into one

**Smishing:** The use of text messages to trick users to obtain sensitive information or to impersonate a known source

**Smurf attack:** A network attack performed when an attacker sniffs an authorized user's IP address and floods it with ICMP packets

**Social engineering:** A manipulation technique that exploits human error to gain private information, access, or valuables

**Social media phishing:** A type of attack where a threat actor collects detailed information about their target on social media sites before initiating the attack

**Spear phishing:** A malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source

**Speed:** The rate at which a device sends and receives data, measured by bits per second

**Splunk Cloud:** A cloud-hosted tool used to collect, search, and monitor log data

**Splunk Enterprise:** A self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time

**Spyware:** Malware that's used to gather and sell information without consent

**SQL (Structured Query Language):** A programming language used to create, interact with, and request information from a database

**SQL injection:** An attack that executes unexpected queries on a database

**Stakeholder:** An individual or group that has an interest in any decision or activity of an organization

**Standard error:** An error message returned by the OS through the shell

**Standard input:** Information received by the OS via the command line

**Standard output:** Information returned by the OS through the shell

**Standards:** References that inform how to set policies

**STAR method:** An interview technique used to answer behavioral and situational questions

**Stateful:** A class of firewall that keeps track of information passing through it and proactively filters out threats

**Stateless:** A class of firewall that operates based on predefined rules and that does not keep track of information from data packets

**Stored XSS attack:** An instance when malicious script is injected directly on the server

**String concatenation:** The process of joining two strings together

**String data:** Data consisting of an ordered sequence of characters

**Style guide:** A manual that informs the writing, formatting, and design of documents

**Subnetting:** The subdivision of a network into logical groups called subnets

**Substring:** A continuous sequence of characters within a string

**Sudo:** A command that temporarily grants elevated permissions to specific users

**Supply-chain attack:** An attack that targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed

**Suricata:** An open-source intrusion detection system, intrusion prevention system, and network analysis tool

**Switch:** A device that makes connections between specific devices on a network by sending and receiving data between them

**Symmetric encryption:** The use of a single secret key to exchange information

**Synchronize (SYN) flood attack:** A type of DoS attack that simulates a TCP/IP connection and floods a server with SYN packets

**Syntax:** The rules that determine what is correctly structured in a computing language

**Syntax error:** An error that involves invalid usage of a programming language

T



**Tailgating:** A social engineering tactic in which unauthorized people follow an authorized person into a restricted area

**TCP/IP model:** A framework used to visualize how data is organized and transmitted across a network

**tcpdump:** A command-line network protocol analyzer

**Technical skills:** Skills that require knowledge of specific tools, procedures, and policies

**Telemetry:** The collection and transmission of data for analysis

**Threat:** Any circumstance or event that can negatively impact assets

**Threat actor:** Any person or group who presents a security risk

**Threat hunting:** The proactive search for threats on a network

**Threat intelligence:** Evidence-based threat information that provides context about existing or emerging threats

**Threat modeling:** The process of identifying assets, their vulnerabilities, and how each is exposed to threats

**Transferable skills:** Skills from other areas that can apply to different careers

**Transmission Control Protocol (TCP):** An internet communication protocol that allows two devices to form a connection and stream data

**Triage:** The prioritizing of incidents according to their level of importance or urgency

**Trojan horse:** Malware that looks like a legitimate file or program

**True negative:** A state where there is no detection of malicious activity

**True positive** An alert that correctly detects the presence of an attack

**Tuple data:** Data that consists of a collection of data that cannot be changed

**Type error:** An error that results from using the wrong data type

U

**Ubuntu:** An open-source, user-friendly distribution that is widely used in security and other industries

**Unauthorized access:** An incident type that occurs when an individual gains digital or physical access to a system or application without permission

**Uncontrolled zone:** Any network outside your organization's control

**Unified Extensible Firmware Interface (UEFI):** A microchip that contains loading instructions for the computer and replaces BIOS on more modern systems

**USB baiting:** An attack in which a threat actor strategically leaves a malware USB stick for an employee to find and install to unknowingly infect a network

**User:** The person interacting with a computer

**User Datagram Protocol (UDP):** A connectionless protocol that does not establish a connection between devices before transmissions

**User-defined function:** A function that programmers design for their specific needs

**User interface:** A program that allows the user to control the functions of the operating system

**User provisioning:** The process of creating and maintaining a user's digital identity

## V

**Variable:** A container that stores data

**Virtual Private Network (VPN):** A network security service that changes your public IP address and hides your virtual location so that you can keep your data private when you are using a public network like the internet

**Virus:** Malicious code written to interfere with computer operations and cause damage to data and software

**VirusTotal:** A service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content

**Vishing:** The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source

**Visual dashboard:** A way of displaying various types of data quickly in one place

**Vulnerability:** A weakness that can be exploited by a threat

**Vulnerability assessment:** The internal review process of an organization's security systems

**Vulnerability management:** The process of finding and patching vulnerabilities

**Vulnerability scanner:** Software that automatically compares existing common vulnerabilities and exposures against the technologies on the network

## W

**Watering hole attack:** A type of attack when a threat actor compromises a website frequently visited by a specific group of users

**Web-based exploits:** Malicious code or behavior that's used to take advantage of coding flaws in a web application

**Whaling:** A category of spear phishing attempts that are aimed at high-ranking executives in an organization

**Wide Area Network (WAN):** A network that spans a large geographic area like a city, state, or country

**Wi-Fi Protected Access (WPA):** A wireless security protocol for devices to connect to the internet

**Wildcard:** A special character that can be substituted with any other character

**Wireshark:** An open-source network protocol analyzer

**World-writable file:** A file that can be altered by anyone in the world

**Worm:** Malware that can duplicate and spread itself across systems on its own

## Y

**YARA-L:** A computer language used to create rules for searching through ingested log data

## Z

**Zero-day:** An exploit that was previously unknown