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

Hacktivist: 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

O

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

Foundations Of Cybersecurity

Module 1 - Introduction to Cybersecurity

Responsibilities of an entry-level cybersecurity analyst

Security analysts are responsible for monitoring and protecting information and systems.

1. **Protecting computer and Network systems :** Protecting computer and network systems requires an analyst to monitor an organization's internal network. If a threat is detected, then an analyst is generally the first to respond. Analysts also often take part in exercises to search for weaknesses in an organization's own systems. For example, a security analyst may contribute to penetration testing or ethical hacking. The goal is to penetrate or hack their own organization's internal network to identify vulnerabilities and suggest ways to strengthen their security measures.
2. **Install prevention software :** One way they do this is by working with information technology, or IT, teams to install prevention software for the purposes of identifying risks and vulnerabilities.
3. **Periodic security audits :** A security audit is a review of an organization's security records, activities, and other related documents. For example, an analyst may examine in-house security issues, such as making sure that confidential information, like individual computer passwords, isn't available to all employees.

Terms and definitions from Course 1, Module 1

- **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
- **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
- **Internal threat:** A current or former employee, external vendor, or trusted partner who poses a security risk
- **Network security:** The practice of keeping an organization's network infrastructure secure from unauthorized access
- **Personally identifiable information (PII):** Any information used to infer an individual’s identity
- **Security posture:** An organization’s ability to manage its defense of critical assets and data and react to change
- **Sensitive personally identifiable information (SPII):** A specific type of PII that falls under stricter handling guidelines
- **Technical skills:** Skills that require knowledge of specific tools, procedures, and policies
- **Threat:** Any circumstance or event that can negatively impact assets
- **Threat actor:** Any person or group who presents a security risk
- **Transferable skills:** Skills from other areas that can apply to different careers

- **External Threat:** An external threat is someone outside of the organization trying to gain access to private information, networks or devices.
- **Compliance** is the process of adhering to internal standards and external regulations and enables organizations to avoid fines and security breaches.
- **Security frameworks** are guidelines used for building plans to help mitigate risks and threats to data and privacy.
- **Security controls** are safeguards designed to reduce specific security risks. They are used with security frameworks to establish a strong security posture.
- **Programming** is a process that can be used to create a specific set of instructions for a computer to execute tasks. These tasks can include:
    - Automation of repetitive tasks (e.g., searching a list of malicious domains)
    - Reviewing web traffic
    - Alerting suspicious activity

Transferable and technical cybersecurity skills

Transferable skills are skills from other areas of study or practice that can apply to different careers. **Technical skills** may apply to several professions, as well; however, they typically require knowledge of specific tools, procedures, and policies. In this reading, you'll explore both transferable skills and technical skills further.

Transferable skills

You have probably developed many transferable skills through life experiences; some of those skills will help you thrive as a cybersecurity professional. These include:

- **Communication and collaboration:** As a cybersecurity analyst, you will need to communicate and collaborate with others. Understanding others' questions or concerns and communicating information clearly to individuals with technical and non-technical knowledge will help you mitigate security issues quickly.
- **Problem-solving:** One of your main tasks as a cybersecurity analyst will be to proactively identify and solve problems. You can do this by recognizing attack patterns, then determining the most efficient solution to minimize risk. Don't be afraid to take risks, and try new things. Also, understand that it's rare to find a perfect solution to a problem. You'll likely need to compromise.
- **Time management:** Having a heightened sense of urgency and prioritizing tasks appropriately is essential in the cybersecurity field. So, effective time management will help you minimize potential damage and risk to critical assets and data. Additionally, it will be important to prioritize tasks and stay focused on the most urgent issue.
- **Growth mindset and analyze complex scenarios:** This is an evolving industry, so an important transferable skill is a willingness to learn. Technology moves fast, and that's a great thing! It doesn't mean you will need to learn it all, but it does mean that you'll need to continue to learn throughout your career. Fortunately, you will be able to apply much of what you learn in this program to your ongoing professional development.
- **Diverse perspectives:** The only way to go far is together. By having respect for each other and encouraging diverse perspectives and mutual respect, you'll undoubtedly find multiple and better solutions to security problems.

Technical skills

There are many technical skills that will help you be successful in the cybersecurity field. You'll learn and practice these skills as you progress through the certificate program. Some of the tools and concepts you'll need to use and be able to understand include:

- **Programming languages:** By understanding how to use programming languages, cybersecurity analysts can automate tasks that would otherwise be very time consuming. Examples of tasks that programming can be used for include searching data to identify potential threats or organizing and analyzing information to identify patterns related to security issues.
- **Security information and event management (SIEM) tools:** SIEM tools collect and analyze log data, or records of events such as unusual login behavior, and support analysts' ability to monitor critical activities in an organization. This helps cybersecurity professionals identify and analyze potential security threats, risks, and vulnerabilities more efficiently.
- **Intrusion detection systems (IDSs):** Cybersecurity analysts use IDSs to monitor system activity and alerts for possible intrusions. It's important to become familiar with IDSs because they're a key tool that every organization uses to protect assets and data. For example, you might use an IDS to monitor networks for signs of malicious activity, like unauthorized access to a network.
- **Threat landscape knowledge:** Being aware of current trends related to threat actors, malware, or threat methodologies is vital. This knowledge allows security teams to build stronger defenses against threat actor tactics and techniques. By staying up to date on attack trends and patterns, security professionals are better able to recognize when new types of threats emerge such as a new ransomware variant.
- **Incident response and Computer Forensics:** Cybersecurity analysts need to be able to follow established policies and procedures to respond to incidents appropriately. For example, a security analyst might receive an alert about a possible malware attack, then follow the organization's outlined procedures to start the incident response process. This could involve conducting an investigation to identify the root issue and establishing ways to remediate it.

CompTIA Security+

In addition to gaining skills that will help you succeed as a cybersecurity professional, the Google Cybersecurity Certificate helps prepare you for the CompTIA Security+ exam, the industry leading certification for cybersecurity roles. You'll earn a dual credential when you complete both, which can be shared with potential employers. After completing all eight courses in the Google Cybersecurity Certificate, you will unlock a 30% discount for the CompTIA Security+ exam and additional practice materials.

PII and SPII

- Personally identifiable information, known as PII, is any information used to infer an individual's identity.
- PII includes someone's full name, date of birth, physical address, phone number, email address, internet protocol, or IP address and similar information.

- Sensitive personally identifiable information, known as SPII, is a specific type of PII that falls under stricter handling guidelines and may include social security numbers, medical or financial information, and biometric data, such as facial recognition.
- If SPII is stolen, this has the potential to be significantly more damaging to an individual than if PII is stolen.
- PII and SPII data are key assets that a threat actor will look for if an organization experiences a breach. When a person's identifiable information is compromised, leaked, or stolen, identity theft is the primary concern.
- Identity theft is the act of stealing personal information to commit fraud while impersonating a victim. And the primary objective of identity theft is financial gain.

Module 2 - History of Cybersecurity

History of Cyber Attacks

Brain virus

In 1986, the Alvi brothers created the Brain virus, although the intention of the virus was to track illegal copies of medical software and prevent pirated licenses, what the virus actually did was unexpected. Once a person used a pirated copy of the software, the virus-infected that computer. Then, any disk that was inserted into the computer was also infected. The virus spread to a new computer every time someone used one of the infected disks. Undetected, the virus spread globally within a couple of months. Although the intention was not to destroy data or hardware, the virus slowed down productivity and significantly impacted business operations.

The Brain virus fundamentally altered the computing industry, emphasizing the need for a plan to maintain security and productivity. As a security analyst, you will follow and maintain strategies put in place to ensure your organization has a plan to keep their data and people safe.

Morris worm

In 1988, Robert Morris developed a program to assess the size of the internet. The program crawled the web and installed itself onto other computers to tally the number of computers that were connected to the internet. Sounds simple, right? The program, however, failed to keep track of the computers it had already compromised and continued to re-install itself until the computers ran out of memory and crashed. About 6,000 computers were affected, representing 10% of the internet at the time. This attack cost millions of dollars in damages due to business disruptions and the efforts required to remove the worm. After the Morris worm, Computer Emergency Response Teams, known as CERTs®, were established to respond to computer security incidents. CERTs still exist today, but their place in the security industry has expanded to include more responsibilities.

LoveLetter attack

In the year 2000, Onel De Guzman created the LoveLetter malware to steal internet login credentials. This attack spread rapidly and took advantage of people who had not developed a healthy suspicion for unsolicited emails. Users received an email with the subject line, "I Love You." Each email contained an attachment labeled, "Love Letter For You." When the attachment was opened, the malware scanned a user's address book. Then, it automatically sent itself to each person on the list and installed a program to collect user information and passwords. Recipients would think they were receiving an email from a friend, but it was actually malware. The LoveLetter ended up infecting 45 million computers globally and is believed to have caused over $10 billion dollars in damages. The LoveLetter attack is the first example of social engineering.

Equifax breach

In 2017, attackers successfully infiltrated the credit reporting agency, Equifax. This resulted in one of the largest known data breaches of sensitive information. Over 143 million customer records were stolen, and the breach affected approximately 40% of all Americans.

The records included personally identifiable information including social security numbers, birth dates, driver's license numbers, home addresses, and credit card numbers. From a security standpoint, the breach occurred due to multiple failures on Equifax's part. It wasn't just one vulnerability that the attackers took advantage of, there were several. The company failed to take the actions needed to fix multiple known vulnerabilities in the months leading up to the data breach.

In the end, Equifax settled with the U.S. government and paid over $575 million dollars to resolve customer complaints and cover required fines.

Common attacks and their effectiveness

Phishing

Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software.

Some of the most common types of phishing attacks today include:

- Business Email Compromise (BEC): A threat actor sends an email message that seems to be from a known source to make a seemingly legitimate request for information, in order to obtain a financial advantage.
- Spear phishing: A malicious email attack that targets a specific user or group of users. The email seems to originate from a trusted source.
- Whaling: A form of spear phishing. Threat actors target company executives to gain access to sensitive data.
- Vishing: The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source.
- Smishing: The use of text messages to trick users, in order to obtain sensitive information or to impersonate a known source.

Malware

Malware is software designed to harm devices or networks. There are many types of malware. The primary purpose of malware is to obtain money, or in some cases, an intelligence advantage that can be used against a person, an organization, or a territory.

Some of the most common types of malware attacks today include:

- Viruses: Malicious code written to interfere with computer operations and cause damage to data and software. A virus needs to be initiated by a user (i.e., a threat actor), who transmits the virus via a malicious attachment or file download. When someone opens the malicious attachment or download, the virus hides itself in other files in the now infected system. When the infected files are opened, it allows the virus to insert its own code to damage and/or destroy data in the system.

- Worms: Malware that can duplicate and spread itself across systems on its own. In contrast to a virus, a worm does not need to be downloaded by a user. Instead, it self-replicates and spreads from an already infected computer to other devices on the same network.
- Ransomware: A malicious attack where threat actors encrypt an organization's data and demand payment to restore access.
- Spyware: Malware that's used to gather and sell information without consent. Spyware can be used to access devices. This allows threat actors to collect personal data, such as private emails, texts, voice and image recordings, and locations.

Social Engineering

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. Human error is usually a result of trusting someone without question. It's the mission of a threat actor, acting as a social engineer, to create an environment of false trust and lies to exploit as many people as possible.

Some of the most common types of social engineering attacks today include:

- Social media phishing: A threat actor collects detailed information about their target from social media sites. Then, they initiate an attack.
- Watering hole attack: A threat actor attacks a website frequently visited by a specific group of users.
- USB baiting: A threat actor strategically leaves a malware USB stick for an employee to find and install, to unknowingly infect a network.
- Physical social engineering: A threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location.

Social engineering principles

Social engineering is incredibly effective. This is because people are generally trusting and conditioned to respect authority. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Although sharing personal data—such as your location or photos—can be convenient, it's also a risk.

Reasons why social engineering attacks are effective include:

- Authority: Threat actors impersonate individuals with power. This is because people, in general, have been conditioned to respect and follow authority figures.
- Intimidation: Threat actors use bullying tactics. This includes persuading and intimidating victims into doing what they're told.
- Consensus/Social proof: Because people sometimes do things that they believe many others are doing, threat actors use others' trust to pretend they are legitimate. For example, a threat actor might try to gain access to private data by telling an employee that other people at the company have given them access to that data in the past.
- Scarcity: A tactic used to imply that goods or services are in limited supply.
- Familiarity: Threat actors establish a fake emotional connection with users that can be exploited.
- Trust: Threat actors establish an emotional relationship with users that can be exploited *over time*. They use this relationship to develop trust and gain personal information.

- Urgency: A threat actor persuades others to respond quickly and without questioning.

Introduction to the eight CISSP security domains

- The first domain, security and risk management. Security and risk management focuses on defining security goals and objectives, risk mitigation, compliance, business continuity, and the law. For example, security analysts may need to update company policies related to private health information if a change is made to a federal compliance regulation such as the Health Insurance Portability and Accountability Act, also known as HIPAA.

- The second domain is asset security. This domain focuses on securing digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data. When working with this domain, security analysts may be tasked with making sure that old equipment is properly disposed of and destroyed, including any type of confidential information.

- The third domain is security architecture and engineering. This domain focuses on optimizing data security by ensuring effective tools, systems, and processes are in place. As a security analyst, you may be tasked with configuring a firewall. A firewall is a device used to monitor and filter incoming and outgoing computer network traffic. Setting up a firewall correctly helps prevent attacks that could affect productivity.

- The fourth security domain is communication and network security. This domain focuses on managing and securing physical networks and wireless communications. As a security analyst, you may be asked to analyze user behavior within your organization.

- The fifth domain: identity and access management. Identity and access management focuses on keeping data secure, by ensuring users follow established policies to control and manage physical assets, like office spaces, and logical assets, such as networks and applications. Validating the identities of employees and documenting access roles are essential to maintaining the organization's physical and digital security. For example, as a security analyst, you may be tasked with setting up employees' keycard access to buildings.

- The sixth domain is security assessment and testing. This domain focuses on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities. Security analysts may conduct regular audits of user permissions, to make sure that users have the correct level of access. For example, access to payroll information is often limited to certain employees, so analysts may be asked to regularly audit permissions to ensure that no unauthorized person can view employee salaries.

- The seventh domain is security operations. This domain focuses on conducting investigations and implementing preventative measures. Imagine that you, as a security analyst, receive an alert that an unknown device has been connected to your internal network. You would need to follow the organization's policies and procedures to quickly stop the potential threat.

- The eighth domain is software development security. This domain focuses on using secure coding practices, which are a set of recommended guidelines that are used to create secure applications and services. A security analyst may work with software development teams to ensure security practices are incorporated into the software development life-cycle. If, for example, one of your partner teams is creating a new mobile app, then you may be asked to advise on the password policies or ensure that any user data is properly secured and managed.

Attack types

Password attack

A password attack is an attempt to access password-secured devices, systems, networks, or data. Some forms of password attacks that you'll learn about later in the certificate program are:

- Brute force
- Rainbow table

Password attacks fall under the communication and network security domain.

Social engineering attack

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. Some forms of social engineering attacks that you will continue to learn about throughout the program are:

- Phishing
- Smishing
- Vishing
- Spear phishing
- Whaling
- Social media phishing
- Business Email Compromise (BEC)
- Watering hole attack
- USB (Universal Serial Bus) baiting
- Physical social engineering

Social engineering attacks are related to the security and risk management domain.

Physical attack

A physical attack is a security incident that affects not only digital but also physical environments where the incident is deployed. Some forms of physical attacks are:

- Malicious USB cable
- Malicious flash drive
- Card cloning and skimming

Physical attacks fall under the asset security domain.

Adversarial artificial intelligence

Adversarial artificial intelligence is a technique that manipulates artificial intelligence and machine learning technology to conduct attacks more efficiently. Adversarial artificial intelligence falls under both the communication and network security and the identity and access management domains.

Supply-chain attack

A supply-chain attack targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed. Because every item sold undergoes a process that involves third parties, this means that the security breach can occur at any point in the supply chain. These attacks are costly because they can affect multiple organizations and the individuals who work for them. Supply-chain attacks can fall under several domains, including but not limited to the security and risk management, security architecture and engineering, and security operations domains.

Cryptographic attack

A cryptographic attack affects secure forms of communication between a sender and intended recipient. Some forms of cryptographic attacks are:

- Birthday
- Collision
- Downgrade

Cryptographic attacks fall under the communication and network security domain.

Threat actor types

Advanced persistent threats

Advanced persistent threats (APTs) have significant expertise accessing an organization's network without authorization. APTs tend to research their targets (e.g., large corporations or government entities) in advance and can remain undetected for an extended period of time. Their intentions and motivations can include:

- Damaging critical infrastructure, such as the power grid and natural resources
- Gaining access to intellectual property, such as trade secrets or patents

Insider threats

Insider threats abuse their authorized access to obtain data that may harm an organization. Their intentions and motivations can include:

- Sabotage நாசவேலை
- Corruption ஊழல்
- Espionage உளவு வேலை
- Unauthorized data access or leaks அங்கீகரிக்கப்படாத தரவு அணுகல் அல்லது கசிவுகள்

Hacktivists

Hacktivists are threat actors that are driven by a political agenda. They abuse digital technology to accomplish their goals, which may include:

- Demonstrations ஆர்ப்பாட்டங்கள்
- Propaganda பிரச்சாரம்
- Social change campaigns சமூக மாற்ற பிரச்சாரங்கள்
- Fame புகழ்

Hacker types

A **hacker** is any person who uses computers to gain access to computer systems, networks, or data. They can be beginner or advanced technology professionals who use their skills for a variety of reasons. There are three main categories of hackers:

- Authorized hackers are also called ethical hackers. They follow a code of ethics and adhere to the law to conduct organizational risk evaluations. They are motivated to safeguard people and organizations from malicious threat actors.
- Semi-authorized hackers are considered researchers. They search for vulnerabilities but don't take advantage of the vulnerabilities they find.
- Unauthorized hackers are also called unethical hackers. They are malicious threat actors who do not follow or respect the law. Their goal is to collect and sell confidential data for financial gain.

Note: There are multiple hacker types that fall into one or more of these three categories. New and unskilled threat actors have various goals, including:

- To learn and enhance their hacking skills
- To seek revenge
- To exploit security weaknesses by using existing malware, programming scripts, and other tactics

Other types of hackers are not motivated by any particular agenda other than completing the job they were contracted to do. These types of hackers can be considered unethical or ethical hackers. They have been known to work on both illegal and legal tasks for pay. There are also hackers who consider themselves vigilantes. Their main goal is to protect the world from unethical hackers.

Terms and definitions from Course 1, Module 2

- **Adversarial artificial intelligence (AI):** A technique that manipulates artificial intelligence (AI) and machine learning (ML) technology to conduct attacks more efficiently
- **Business Email Compromise (BEC):** A type of phishing attack where a threat actor impersonates a known source to obtain financial advantage
- **CISSP:** Certified Information Systems Security Professional is a globally recognized and highly sought-after information security certification, awarded by the International Information Systems Security Certification Consortium
- **Computer virus:** Malicious code written to interfere with computer operations and cause damage to data and software
- **Cryptographic attack:** An attack that affects secure forms of communication between a sender and intended recipient
- **Hacker:** Any person who uses computers to gain access to computer systems, networks, or data
- **Malware:** Software designed to harm devices or networks
- **Password attack:** An attempt to access password secured devices, systems, networks, or data
- **Phishing:** The use of digital communications to trick people into revealing sensitive data or deploying malicious software
- **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

- **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
- **Supply-chain attack:** An attack that targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed
- **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
- **Virus:** refer to "computer virus"
- **Vishing:** The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source
- **Watering hole attack**: A type of attack when a threat actor compromises a website frequently visited by a specific group of users

Module 3 - Protect against threats, risks and vulnerabilities

Terms and definitions from Course 1, Module 3

- **Asset**: An item perceived as having value to an organization
- **Availability**: The idea that data is accessible to those who are authorized to access it
- **Compliance**: The process of adhering to internal standards and external regulations
- **Confidentiality**: The idea that only authorized users can access specific assets or data
- **Confidentiality, integrity, availability (CIA) triad**: A model that helps inform how organizations consider risk when setting up systems and security policies
- **Hacktivist**: A person who uses hacking to achieve a political goal
- **Health Insurance Portability and Accountability Act (HIPAA)**: A U.S. federal law established to protect patients' health information
- **Integrity**: The idea that the data is correct, authentic, and reliable
- **National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF):** A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk
- **Privacy protection**: The act of safeguarding personal information from unauthorized use
- **Protected health information (PHI)**: Information that relates to the past, present, or future physical or mental health or condition of an individual
- **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 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
- **Sensitive personally identifiable information (SPII)**: A specific type of PII that falls under stricter handling guidelines.

Security frameworks

- Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy. Security frameworks provide a structured approach to implementing a security lifecycle. The security lifecycle is a constantly evolving set of policies and standards that define how an organization manages risks, follows established guidelines, and meets regulatory compliance, or laws.
- The purpose of security frameworks include protecting personally identifiable information, known as PII, securing financial information, identifying security weaknesses, managing organizational risks, and aligning security with business goals.
- Frameworks have four core components and understanding them will allow you to better manage potential risks.
- The first core component is **identifying and documenting security goals.** For example, an organization may have a goal to align with the E.U.'s General Data Protection Regulation, also known as GDPR. GDPR is a data protection law established to grant European citizens more control over their personal data. A security analyst may be asked to identify and document areas where an organization is out of compliance with GDPR.
- The second core component is setting **guidelines to achieve security goals**. For example, when implementing guidelines to achieve GDPR compliance, your organization may need to develop new policies for how to handle data requests from individual users.
- The third core component of security frameworks is **implementing strong security processes**. In the case of GDPR, a security analyst working for a social media company may help design procedures to ensure the organization complies with verified user data requests. An example of this type of request is when a user attempts to update or delete their profile information.
- The last core component of **security frameworks is monitoring and communicating results**. As an example, you may monitor your organization's internal network and report a potential security issue affecting GDPR to your manager or regulatory compliance officer.
- Security controls are safeguards designed to reduce specific security risks. For example, your company may have a guideline that requires all employees to complete a privacy training to reduce the risk of data breaches. As a security analyst, you may use a software tool to automatically assign and track which employees have completed this training.

CIA triad

The CIA triad is a foundational model that helps inform how organizations consider risk when setting up systems and security policies. CIA stands for confidentiality, integrity, and availability.

1. Confidentiality means that only authorized users can access specific assets or data. For example, strict access controls that define who should and should not

have access to data, must be put in place to ensure confidential data remains safe.

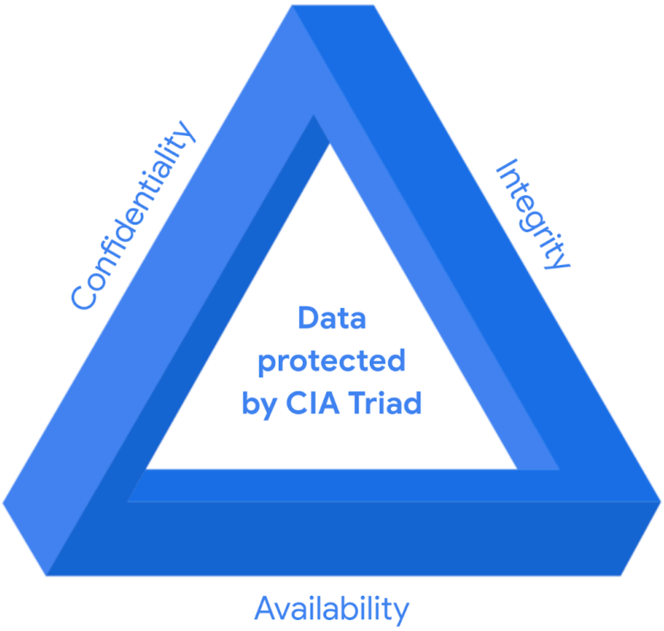
2. Integrity means the data is correct, authentic, and reliable. To maintain integrity, security professionals can use a form of data protection like encryption to safeguard data from being tampered with.
3. Availability means data is accessible to those who are authorized to access it. Let's define a term that came up during our discussion of the CIA triad: An asset is an item perceived as having value to an organization.And value is determined by the cost associated with the asset in question.

For example, an application that stores sensitive data, such as social security numbers or bank accounts, is a valuable asset to an organization. It carries more risk and therefore requires tighter security controls in comparison to a website that shares publicly available news content.

A specific framework developed by the U.S.-based National Institute of Standards and Technology: the Cybersecurity Framework, also referred to as the NIST CSF. The NIST Cybersecurity Framework is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk.

Controls, frameworks, and compliance

A security lifecycle is a constantly evolving set of policies and standards.
The confidentiality, integrity, and availability (CIA) triad is a model that helps inform how organizations consider risk when setting up systems and security policies.



CIA are the three foundational principles used by cybersecurity professionals to establish appropriate controls that mitigate threats, risks, and vulnerabilities.
They are used alongside frameworks to ensure that security goals and processes are implemented correctly and that organizations meet regulatory compliance requirements.
Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy. They have four core components:

1. Identifying and documenting security goals
2. Setting guidelines to achieve security goals
3. Implementing strong security processes
4. Monitoring and communicating results

Compliance is the process of adhering to internal standards and external regulations.

Specific controls, frameworks, and compliance

The National Institute of Standards and Technology (NIST) is a U.S.-based agency that develops multiple voluntary compliance frameworks that organizations worldwide can use to help manage risk. Examples of frameworks include the NIST Cybersecurity Framework (CSF) and the NIST Risk Management Framework (RMF).

Note: Specifications and guidelines can change depending on the type of organization you work for.

In addition to the NIST CSF and NIST RMF, there are several other controls, frameworks, and compliance standards that it is important for security professionals to be familiar with to help keep organizations and the people they serve safe.

The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)

FERC-NERC is a regulation that applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. These types of organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. They are also legally required to adhere to the Critical Infrastructure Protection (CIP) Reliability Standards defined by the FERC.

The Federal Risk and Authorization Management Program (FedRAMP®)

FedRAMP is a U.S. federal government program that standardizes security assessment, authorization, monitoring, and handling of cloud services and product offerings. Its purpose is to provide consistency across the government sector and third-party cloud providers.

Center for Internet Security (CIS®)

CIS is a nonprofit with multiple areas of emphasis. It provides a set of controls that can be used to safeguard systems and networks against attacks. Its purpose is to help organizations establish a better plan of defense. CIS also provides actionable controls that security professionals may follow if a security incident occurs.

General Data Protection Regulation (GDPR)

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. residents' data and their right to privacy in and out of E.U. territory. For example, if an organization is not being transparent about the data they are holding about an E.U. citizen and why they are holding that data, this is an infringement that can result in a fine to the organization. Additionally, if a breach occurs and an E.U. citizen's data is compromised, they must be informed. The affected organization has 72 hours to notify the E.U. citizen about the breach.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment. The objective of this compliance standard is to reduce credit card fraud.

The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a U.S. federal law established in 1996 to protect patients' health information. This law prohibits patient information from being shared without their consent. It is governed by three rules:

1. Privacy
2. Security
3. Breach notification

Organizations that store patient data have a legal obligation to inform patients of a breach because if patients' Protected Health Information (PHI) is exposed, it can lead to identity theft and insurance fraud. PHI relates to the past, present, or future physical or mental health or condition of an individual, whether it's a plan of care or payments for care. Along with understanding HIPAA as a law, security professionals also need to be familiar with the Health Information Trust Alliance (HITRUST®), which is a security framework and assurance program that helps institutions meet HIPAA compliance.

International Organization for Standardization (ISO)

ISO was created to establish international standards related to technology, manufacturing, and management across borders. It helps organizations improve their processes and procedures for staff retention, planning, waste, and services.

System and Organizations Controls (SOC type 1, SOC type 2)

The American Institute of Certified Public Accountants® (AICPA) auditing standards board developed this standard. The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels such as:

- Associate
- Supervisor
- Manager
- Executive
- Vendor
- Others

They are used to assess an organization's financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.
Pro tip: There are a number of regulations that are frequently revised. You are encouraged to keep up-to-date with changes and explore more frameworks, controls, and compliance. Two suggestions to research: the Gramm-Leach-Bliley Act and the Sarbanes-Oxley Act.

United States Presidential Executive Order 14028

On May 12, 2021, President Joe Biden released an executive order related to improving the nation's cybersecurity to remediate the increase in threat actor activity. Remediation efforts are directed toward federal agencies and third parties with ties to U.S. critical infrastructure. For additional information, review the Executive Order on Improving the Nation's Cybersecurity.

- First, you might see a government regulator become more interested in understanding the practices around how a company is handling data.

- Secondly, consumers, customers, businesses may actually begin to directly inquire of the company how they're handling data. And this may become part of the customer relationship and increasingly important if that data is very sensitive.
- And third, the last consequence is legal action. And it's not uncommon for us to see victims of cybersecurity incidents now suing companies for mishandling their data. You can keep up to date with compliance, regulation and laws around PII by consulting the relevant website in the jurisdiction that you have a question for.

Ethics in cybersecurity

Situation :

For example, imagine that you're working as an entry-level security analyst and you have received a high risk alert. You investigate the alert and discover data has been transferred without authorization. You work diligently to identify who made the transfer and discover it is one of your friends from work. What do you do?

Reaction :

Ethically, as a security professional, your job is to remain unbiased and maintain security and confidentiality.

While it's normal to want to protect a friend, regardless of who the user in question may be, your responsibility and obligation is to adhere to the policies and protocols you've been trained to follow.

In many cases, security teams are entrusted with greater access to data and information than other employees. Security professionals must respect that privilege and act ethically at all times.

Principles of Ethics:

Confidentiality:

Confidentiality means that only authorized users can access specific assets or data. Confidentiality as it relates to professional ethics means that there needs to be a high level of respect for privacy to safeguard private assets and data.

As a security professional, you'll encounter proprietary or private information, such as PII. It's your ethical duty to keep that information confidential and safe.

For example, you may want to help out a coworker by providing computer system access outside of properly documented channels. However, this ethical violation can result in serious consequences, including reprimands, the loss of your professional reputation, and legal repercussions for both you and your friend.

Privacy protection:

Privacy protection means safeguarding personal information from unauthorized use.

- Personally identifiable information (PII) and sensitive personally identifiable information (SPII) are types of personal data that can cause people harm if they are stolen.
- **PII** data is any information used to infer an individual's identity, like their name and phone number.
- **SPII** data is a specific type of PII that falls under stricter handling guidelines, including social security numbers and credit card numbers.
- To effectively safeguard PII and SPII data, security professionals hold an ethical obligation to secure private information, identify security vulnerabilities, manage organizational risks, and align security with business goals.

For example, imagine you receive a personal email after hours from your manager requesting a colleague's home phone number. Your manager explains that they can't access the employee database at the moment, but they need to discuss an urgent matter with that person. As a security analyst, your role is to follow the policies and procedures of your company, which in this example, state that employee information is stored in a secure database and should never be accessed or shared in any other format. So, accessing and sharing the employee's personal information would be unethical.

Law:

Laws are rules that are recognized by a community and enforced by a governing entity.

For example, consider a staff member at a hospital who has been trained to handle PII, and SPII for compliance. The staff member has files with confidential data that should never be left unsupervised, but the staff member is late for a meeting. Instead of locking the files in a designated area, the files are left on the staff member's desk, unsupervised. Upon the employee's return, the files are missing. The staff member has just violated multiple compliance regulations, and their actions were unethical and illegal, since their negligence has likely resulted in the loss of private patient and hospital data.

As a security professional, you will have an ethical obligation to protect your organization, its internal infrastructure, and the people involved with the organization. To do this:

- You must remain unbiased and conduct your work honestly, responsibly, and with the highest respect for the law.
- Be transparent and just, and rely on evidence.
- Ensure that you are consistently invested in the work you are doing, so you can appropriately and ethically address issues that arise.
- Stay informed and strive to advance your skills, so you can contribute to the betterment of the cyber landscape.

For example, consider the **Health Insurance Portability and Accountability Act (HIPAA)**, which is a U.S. federal law established to protect patients' health information, also known as PHI, or protected health information. This law prohibits patient information from being shared without their consent. So, as a security professional, you might help ensure that the organization you work for adheres to both its legal and ethical obligation to inform patients of a breach if their health care data is exposed.

Security Ethics:

- **Security ethics** are guidelines for making appropriate decisions as a security professional.
- Being ethical requires that security professionals remain unbiased and maintain the security and confidentiality of private data.

Ethical concerns and laws related to counterattacks

United States standpoint on counterattacks

- In the U.S., deploying a counterattack on a threat actor is illegal because of laws like the Computer Fraud and Abuse Act of 1986 and the Cybersecurity Information Sharing Act of 2015, among others.
- You can only defend.
- The act of counter attacking in the U.S. is perceived as an act of vigilantism.
- A **vigilante** is a person who is not a member of law enforcement who decides to stop a crime on their own.
- And because threat actors are criminals, counterattacks can lead to further escalation of the attack, which can cause even more damage and harm.
- Lastly, if the threat actor in question is a state-sponsored hacktivist, a counterattack can lead to serious international implications.
- A **hacktivist** is a person who uses hacking to achieve a political goal. The political goal may be to promote social change or civil disobedience.
- For these reasons, the only individuals in the U.S. who are allowed to counterattack are approved employees of the federal government or military personnel.

International standpoint on counterattacks

The International Court of Justice (ICJ), which updates its guidance regularly, states that a person or group can counterattack if:

- The counterattack will only affect the party that attacked first.
- The counterattack is a direct communication asking the initial attacker to stop.
- The counterattack does not escalate the situation.
- The counterattack effects can be reversed.

1. Organizations typically do not counterattack because the above scenarios and parameters are hard to measure.
2. There is a lot of uncertainty dictating what is and is not lawful, and at times negative outcomes are very difficult to control.
3. Counterattack actions generally lead to a worse outcome, especially when you are not an experienced professional in the field.
4. To learn more review updates provided in the Tallinn Manual online.

Real Life Examples:

- Examples of unethical behavior are usually honestly just slight laziness, people taking shortcuts and not really thinking about the consequences of their actions.
- So, certainly when people share passwords to systems or give out private information, or look into systems for their own personal information or purposes about people they know or about celebrities.
- One of the most difficult situations that I ever faced in my technology career related to ethics was shortly after 9/11, my boss's boss's boss came to me with a bunch of keywords that were clearly related to the attack in New York and asked me to query the database that I administered that had everybody's text messages in it for the entire telecommunications company without anything in writing and without a court order.
- I was in a very uncomfortable position to tell someone that was much senior than me that I wasn't comfortable doing that.
- I suggested that he bring something in writing to me to do that and he found someone else who did it for him. When you're faced with one of these difficult decisions, it's good to think about what would be the consequences of your decision.

Module - 4 Cybersecurity Tools and Programming Languages

Common cybersecurity tools

Log : A log is a record of events that occur within an organization's systems. Examples of security-related logs include records of employees signing into their computers or accessing web-based services. Logs help security professionals identify vulnerabilities and potential security breaches.

SIEM Tools : A SIEM tool is an application that collects and analyzes log data to monitor critical activities in an organization. SIEM tools collect real-time, or instant, information, and allow security analysts to identify potential breaches as they happen.SIEM tools reduce the amount of data an analyst must review by providing alerts for specific types of risks and threats.

Commonly used SIEM tools: Splunk and Chronicle.

- **Splunk** is a data analysis platform, and Splunk Enterprise provides SIEM solutions. Splunk Enterprise is a self-hosted tool used to retain, analyze, and search an organization's log data.
- **Google's Chronicle** is a cloud-native SIEM tool that stores security data for search and analysis. Cloud-native means that Chronicle allows for fast delivery of new features.

Both collect data from multiple places, then analyze and filter that data to allow security teams to prevent and quickly react to potential security threats.

Other key tools that you will use in your role as a security analyst are playbooks and network protocol analyzers.

- A playbook is a manual that provides details about any operational action, including incident response, security or compliance reviews, access management, and many other organizational tasks that require a documented process from beginning to end.
- Playbooks, which vary from one organization to the next, guide analysts in how to handle a security incident before, during, and after it has occurred.
- Playbooks can pertain to security or compliance reviews, access management, and many other organizational tasks that require a documented process from beginning to end.

- **Network protocol analyzer**, also called packet sniffer. A packet sniffer is a tool designed to capture and analyze data traffic within a network. Common network protocol analyzers include tcpdump and Wireshark.

Tools for protecting business operations

An entry-level analyst's toolkit

Security information and event management (SIEM) tools

- A **SIEM tool** is an application that collects and analyzes log data to monitor critical activities in an organization.
- A **log** is a record of events that occur within an organization's systems. Depending on the amount of data you're working with, it could take hours or days to filter through log data on your own.
- SIEM tools reduce the amount of data an analyst must review by providing alerts for specific types of threats, risks, and vulnerabilities.
- SIEM tools provide a series of dashboards that visually organize data into categories, allowing users to select the data they wish to analyze. Different SIEM tools have different dashboard types that display the information you have access to.
- SIEM tools also come with different hosting options, including on-premise and cloud.
- Organizations may choose one hosting option over another based on a security team member's expertise.
- For example, because a cloud-hosted version tends to be easier to set up, use, and maintain than an on-premise version, a less experienced security team may choose this option for their organization

Network protocol analyzers (packet sniffers)

A **network protocol analyzer**, also known as a **packet sniffer**, is a tool designed to capture and analyze data traffic in a network. This means that the tool keeps a record of all the data that a computer within an organization's network encounters. Later in the program, you'll have an opportunity to practice using some common network protocol analyzer (packet sniffer) tools.

Playbooks

A **playbook** is a manual that provides details about any operational action, such as how to respond to a security incident.

Organizations usually have multiple playbooks documenting processes and procedures for their teams to follow. Playbooks vary from one organization to the next, but they all have a similar purpose: To guide analysts through a series of steps to complete specific security-related tasks.

For example, consider the following scenario: You are working as a security analyst for an incident response firm. You are given a case involving a small medical practice that has suffered a security breach. Your job is to help with the forensic investigation and provide evidence to a cybersecurity insurance company. They will then use your investigative findings to determine whether the medical practice will receive their insurance payout.

In this scenario, playbooks would outline the specific actions you need to take to conduct the investigation. Playbooks also help ensure that you are following proper protocols and procedures. When working on a forensic case, there are two playbooks you might follow:

- The first type of playbook you might consult is called the **chain of custody** playbook. Chain of custody is the process of documenting evidence possession and control during an incident lifecycle. As a security analyst involved in a forensic analysis, you will work with the computer data that was breached. You and the forensic team will also need to document who, what, where, and why you have the collected evidence. The evidence is your responsibility while it is in your possession. Evidence must be kept safe and tracked. Every time evidence is moved, it should be reported. This allows all parties involved to know exactly where the evidence is at all times.

- The second playbook your team might use is called the **protecting and preserving evidence** playbook. Protecting and preserving evidence is the process of properly working with fragile and volatile digital evidence. As a security analyst, understanding what fragile and volatile digital evidence is, along with why there is a procedure, is critical. As you follow this playbook, you will consult the **order of volatility**, which is a sequence outlining the order of data that must be preserved from first to last. It prioritizes volatile data, which is data that may be lost if the device in question powers off, regardless of the reason. While conducting an investigation, improper management of digital evidence can compromise and alter that evidence. When evidence is improperly managed during an investigation, it can no longer be used. For this reason, the first priority in any investigation is to properly preserve the data. You can preserve the data by making copies and conducting your investigation using those copies.

Resources for more information

- The Google Cybersecurity Action Team's Threat Horizon Report provides strategic intelligence for dealing with threats to cloud enterprise.
- The Cybersecurity & Infrastructure Security Agency (CISA) has a list of Free Cybersecurity Services and Tools. Review the list to learn more about open-source cybersecurity tools.

Core cybersecurity knowledge and skills

Introduction to Linux, SQL, and Python

- **Programming** allows analysts to complete repetitive tasks and processes with a high degree of accuracy and efficiency. It also helps reduce the risk of human error, and can save hours or days compared to performing the work manually.
- **Linux** is an open-source, or publicly available, operating system. Linux relies on a command line as the primary user interface. Linux itself is not a programming language, but it does allow for the use of text-based commands between the user and the operating system.
- **SQL** stands for Structured Query Language. SQL is a programming language used to create, interact with, and request information from a database.
- **Database** is an organized collection of information or data.
- **Python** is used to perform tasks that are repetitive and time-consuming and that require a high level of detail and accuracy.

Tools and their purposes

Programming

- **Programming** is a process that can be used to create a specific set of instructions for a computer to execute tasks. Security analysts use programming languages, such as Python, to execute automation.
- **Automation** is the use of technology to reduce human and manual effort in performing common and repetitive tasks. Automation also helps reduce the risk of human error.
- Another programming language used by analysts is called Structured Query Language (SQL).
- **SQL** is used to create, interact with, and request information from a database.
- A **database** is an organized collection of information or data. There can be millions of data points in a database.
- A **data point** is a specific piece of information.

Operating systems

- An **operating system** is the interface between computer hardware and the user. Linux®, macOS®, and Windows are operating systems. They each offer different functionality and user experiences.
- **Linux** as an open-source operating system. Open source means that the code is available to the public and allows people to make contributions to improve the software. Linux is not a programming language; however, it does involve the use of a command line within the operating system.
- A **command** is an instruction telling the computer to do something.

- A **command-line** interface is a text-based user interface that uses commands to interact with the computer.

Web vulnerability

- A **web vulnerability** is a unique flaw in a web application that a threat actor could exploit by using malicious code or behavior, to allow unauthorized access, data theft, and malware deployment.
- To stay up-to-date on the most critical risks to web applications, review the Open Web Application Security Project (OWASP) Top 10.

Antivirus software

Antivirus software is a software program used to prevent, detect, and eliminate malware and viruses. It is also called anti-malware. Depending on the type of antivirus software, it can scan the memory of a device to find patterns that indicate the presence of malware.

Intrusion detection system

An **intrusion detection system** (IDS) is an application that monitors system activity and alerts on possible intrusions. The system scans and analyzes network packets, which carry small amounts of data through a network. The small amount of data makes the detection process easier for an IDS to identify potential threats to sensitive data. Other occurrences an IDS might detect can include theft and unauthorized access.

Encryption

- Encryption makes data unreadable and difficult to decode for an unauthorized user; its main goal is to ensure confidentiality of private data.
- **Encryption** is the process of converting data from a readable format to a cryptographically encoded format.
- **Cryptographic encoding** means converting plaintext into secure ciphertext.
- **Plaintext** is unencrypted information and **secure ciphertext** is the result of encryption.
- **Note:** Encoding and encryption serve different purposes. Encoding uses a public conversion algorithm to enable systems that use different data representations to share information.

Penetration testing

Penetration testing, also called pen testing, is the act of participating in a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes. It is a thorough risk assessment that can evaluate and identify external and internal threats as well as weaknesses.

Terms and definitions from Course 1, Module 4

- **Antivirus software:** A software program used to prevent, detect, and eliminate malware and viruses
- **Database:** An organized collection of information or data
- **Data point:** A specific piece of information
- **Intrusion detection system (IDS):** An application that monitors system activity and alerts on possible intrusions

- **Linux:** An open-source operating system
- **Log:** A record of events that occur within an organization’s systems
- **Network protocol analyzer (packet sniffer):** A tool designed to capture and analyze data traffic within a network
- **Order of volatility:** A sequence outlining the order of data that must be preserved from first to last
- **Programming:** A process that can be used to create a specific set of instructions for a computer to execute tasks
- **Protecting and preserving evidence:** The process of properly working with fragile and volatile digital evidence
- **Security information and event management (SIEM)**: An application that collects and analyzes log data to monitor critical activities in an organization
- **SQL (Structured Query Language):** A programming language used to create, interact with, and request information from a database

Create a cybersecurity portfolio

What is a portfolio, and why is it necessary?

Cybersecurity professionals use portfolios to demonstrate their security education, skills, and knowledge. Professionals typically use portfolios when they apply for jobs to show potential employers that they are passionate about their work and can do the job they are applying for. Portfolios are more in depth than a resume, which is typically a one-to-two page summary of relevant education, work experience, and accomplishments. You will have the opportunity to develop a resume, and finalize your portfolio, in the last course of this program.

Options for creating your portfolio

There are many ways to present a portfolio, including self-hosted and online options such as:

- Documents folder
- Google Drive or Dropbox™
- Google Sites
- Git repository

Option 1: Documents folder

Description: A documents folder is a folder created and saved to your computer’s hard drive. You manage the folder, subfolders, documents, and images within it.
Document folders allow you to have direct access to your documentation. Ensuring that your professional documents, images, and other information are well organized can save you a lot of time when you’re ready to apply for jobs. For example, you may want to create a main folder titled something like “Professional documents.” Then, within your main folder, you could create subfolders with titles such as:

- Resume
- Education
- Portfolio documents
- Cybersecurity tools

- Programming

Setup: Document folders can be created in multiple ways, depending on the type of computer you are using. If you're unsure about how to create a folder on your device, you can search the internet for instructional videos or documents related to the type of computer you use.

Option 2: Google Drive or Dropbox

Description: Google Drive and Dropbox offer similar features that allow you to store your professional documentation on a cloud platform. Both options also have file-sharing features, so you can easily share your portfolio documents with potential employers. Any additions or changes you make to a document within that folder will be updated automatically for anyone with access to your portfolio.

Similar to a documents folder, keeping your Google Drive or Dropbox-based portfolio well organized will be helpful as you begin or progress through your career.

Setup: To learn how to upload and share files on these applications, visit the Google Drive and Dropbox websites for more information.

Option 3: Google Sites

Description: Google Sites and similar website hosting options have a variety of easy-to-use features to help you present your portfolio items, including customizable layouts, responsive webpages, embedded content capabilities, and web publishing. Responsive webpages automatically adjust their content to fit a variety of devices and screen sizes. This is helpful because potential employers can review your content using any device and your media will display just as you intend. When you're ready, you can publish your website and receive a unique URL. You can add this link to your resume so hiring managers can easily access your work.

Setup: To learn how to create a website in Google Sites, visit the Google Sites website.

Option 4: Git repository

Description: A Git repository is a folder within a project. In this instance, the project is your portfolio, and you can use your repository to store the documents, labs, and screenshots you complete during each course of the certificate program. There are several Git repository sites you can use, including:

- GitLab
- Bitbucket™
- GitHub

Each Git repository allows you to showcase your skills and knowledge in a customizable space. To create an online project portfolio on any of the repositories listed, you need to use a version of Markdown.

Setup: To learn about how to create a GitHub account and use Markdown, follow the steps outlined in the document Get started with GitHub.

Portfolio projects

As previously mentioned, you will have multiple opportunities throughout the certificate program to develop items to include in your portfolio. These opportunities include:

- Drafting a professional statement
- Conducting a security audit

- Analyzing network structure and security
- Using Linux commands to manage file permissions
- Applying filters to SQL queries
- Identifying vulnerabilities for a small business
- Documenting incidents with an incident handler's journal
- Importing and parsing a text file in a security-related scenario
- Creating or revising a resume

Note: Do not include any private, copyrighted, or proprietary documents in your portfolio. Also, if you use one of the sites described in this reading, keep your site set to "private" until it is finalized.

Activity

Scenario

You are excited to enter the field of cybersecurity. As you begin to consider the types of jobs you could apply for, you decide to create a draft professional statement that you can continue to refine, as your knowledge and skills evolve throughout the certificate program. Your goal is to have a professional statement that can be shared with potential employers, when you're ready to begin your job search.

Note: Creating a unique and authentic professional statement helps establish people's perception of who you are and what you care about.

Step-By-Step Instructions

Step 1: Access supporting materials

To use the supporting materials for this course item, click the link. Link to supporting materials: Professional statement outline

OR

If you don't have a Google account, you can download the supporting materials directly from the following attachment.

Professional statement outline
DOCX File

Step 2: Draft your professional statement

Your professional statement is your opportunity to show prospective employers who you are as a person and potential employee, and it allows them to understand the value you can bring to the organization.

Use these guidelines to develop your draft professional statement:

1. Use your own device to open a word processing document or application (or use a blank piece of paper).
2. Refer to your professional statement outline notes from step one and consider:
    a. What are your strengths (ones you currently have or plan to develop)?
    b. What are your values?
    c. What interests you most about a career in cybersecurity?
    d. How can your strengths, values, and interest in cybersecurity support the security goals of various organizations?
3. Draft a two- to three-sentence professional statement that includes details about your strengths, values, and interest in cybersecurity, as well as how they can support the security goals of various organizations.

Refer to the following professional statement examples for ideas:

- Example A: I am a highly motivated and detail-oriented cybersecurity analyst. I actively work to identify and analyze potential risks, threats, and vulnerabilities to security and ensure the confidentiality, integrity, and availability of assets, to help safeguard organizations and people alike.
- Example B: I am enthusiastic about information security and enjoy finding solutions that can positively impact an organization and the people it serves. I place a high value on maintaining a strong security posture to help protect sensitive information and mitigate risk.

Step 3: Refine your professional statement

Be sure to address the following elements in your completed activity:

- Be intentional about how you want to be perceived by potential employers.
- Include your strengths and values, and be genuine about why you want to enter the cybersecurity profession.
- Regularly update your statement to reflect your growing professional skills and knowledge.

Glossary

Cybersecurity

Terms and definitions from Course 1

A

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

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

Asset: An item perceived as having value to an organization

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

B

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

C

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

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

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

Confidentiality: Only authorized users can access specific assets or data

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

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

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

Database: An organized collection of information or data

Data point: A specific piece of information

H

Hacker: Any person who uses computers to gain access to computer systems, networks, or data

Hacktivist: A person who uses hacking to achieve a political goal

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

I

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

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

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

L

Linux: An open-source operating system

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

M

Malware: Software designed to harm devices or networks

N

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

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

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

O

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

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

P

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

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

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

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

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

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

S

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

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

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

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

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

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

T

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

Threat: Any circumstance or event that can negatively impact assets

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

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

U

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

V

Virus: refer to “computer virus”

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

W

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

Professional statement outline

To develop a professional statement that briefly explains who you are and what you are passionate about, follow the steps outlined.

Note: You will need a piece of paper or a blank word processing document to complete this activity

Step one

List two to three strengths that you currently have or are committed to developing (e.g., strong written and verbal communication, time management, programming, etc.).

Having an inventory of your strengths can help you create your professional statement. It may also encourage you to focus on skills you want to develop as you progress through the certificate program.

Step two

List one to two values you have (e.g., protecting organizations, protecting people, adhering to laws, ensuring equitable access, etc.).

Establishing your values can help you and a prospective employer determine if your goals are aligned. Ensure that you are representing yourself accurately, and be honest about what motivates you.

Step three

Ask yourself some **clarifying questions** to determine what to include in your professional statement:

1. What most interests me about the field of cybersecurity?
2. Who is the audience for my professional statement (e.g., cybersecurity recruiters, specific organizations, government employers, etc.)?
3. In what ways can my strengths, values, and interest in cybersecurity support the security goals of various organizations?

Note: This is just a draft. You should continue to revise and refine your professional statement, throughout the program, until you feel that it's ready to share with potential employers.

Get started with GitHub

Set up a GitHub account

To create your GitHub account, access the links and follow the steps provided.

1. Set up an account on GitHub
2. After setting up a GitHub account, create separate repositories for your portfolio documentation. Repositories are like folders and often referred to as "repos" for short. Review Create a repo for more information.
3. Each repository, or repo folder, will contain your project files and a "README" file. A README is a text file that provides an overview of your project.
    - Some example sections you may want to include are:
        - **A Project Title:** A descriptive title related to the project that may interest your prospective employer. Do not title your project "Portfolio Project"; instead, try adding a title that defines the project you have worked on.
        - **A Project Introduction**: Two to three sentences that state the problem you solved, the data used for the project, and your modeling results.
        - **Modeling and Evaluation**: Name and describe the models you used for the project and any corresponding evaluation metrics.
        - **Conclusion**: Your recommendations for solving the problem and a description of any future steps you want to take to expand on your project.

How to use Markdown

Markdown is a simple markup language, similar to HTML. Markdown allows you to format plaintext documents via GitHub.

Here are a few resource options for you to learn more:

- Basic Syntax
- Markdown Cheat Sheet
- GitHub Markdown Cheatsheet
- GitHub basic writing and formatting syntax

Citations:

#	APA Citation	Use of Source
	GitHub Docs. (2022). *Signing up for a new GitHub account.* https://docs.github.com/en/get-started/signing-up-for-github/signing-up-for-a-new-github-account	Linked/quoted ▾
	GitHub Docs. (2022). *About READMEs*. https://docs.github.com/en/repositories/managing-your-repositorys-settings-and-features/customizing-your-repository/about-readmes	Linked/quoted ▾
	Markdown Guide. (2022). https://www.markdownguide.org/basic-syntax/	Linked/quoted ▾
	Markdown Guide. (2022). https://www.markdownguide.org/cheat-sheet/	Linked/quoted ▾
	GitHub. (2022). *Markdown Cheatsheet.* https://github.com/adam-p/markdown-here/wiki/Markdown-Cheatsheet	Linked/quoted ▾
	GitHub Docs. (2022). *Basic writing and formatting syntax.* https://docs.github.com/en/get-started/writing-on-github/getting-started-with-writing-and-formatting-on-github/basic-writing-and-formatting-syntax	Linked/quoted ▾

Professional statement exemplar

Fictional persona:

Following is a fictional persona that may represent someone interested in becoming a cybersecurity analyst.

Melodie is a high school graduate and her strongest subjects in school were math and science. She enjoys learning and excelled in school. She likes creating spreadsheets to organize everyday tasks. She also likes analyzing complex tasks. Melodie has a passion for technology and enjoys helping others. She is interested in the field of security but has no previous experience. She wants an entry-level cybersecurity position that will utilize her drive and thirst for knowledge. She believes the Google Cybersecurity Certificate will make her a better candidate and will help her develop the professional skills she lacks.

Fictional persona's draft professional statement:

My name is Melodie. I am driven and passionate about safeguarding people's security, including their financial well being. I enjoy working with technology and analyzing and solving complex problems.

Play It Safe: Manage Security Risks

Module 1 - Security Domains

Explore the CISSP security domains

Security posture : Security posture refers to an organization's ability to manage its defense of critical assets and data and react to change.

- The first domain is security and risk management. There are several areas of focus for this domain: defining security goals and objectives, risk mitigation, compliance, business continuity, and legal regulations.
    - Security goals and objectives, organizations can reduce risks to critical assets and data like PII, or personally identifiable information.
    - Risk mitigation means having the right procedures and rules in place to quickly reduce the impact of a risk like a breach.
    - Compliance is the primary method used to develop an organization's internal security policies, regulatory requirements, and independent standards.
    - Business continuity relates to an organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans.
    - Laws related to security and risk management are different worldwide, the overall goals are similar. As a security professional, this means following rules and expectations for ethical behavior to minimize negligence, abuse, or fraud.
- The second domain is asset security. The asset security domain is focused on securing digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data.
    - This means that assets such as PII or SPII should be securely handled and protected, whether stored on a computer, transferred over a network like the internet, or even physically collected. Organizations also need to have policies and procedures that ensure data is properly stored, maintained, retained, and destroyed. Knowing what data you have and who has access to it is necessary for having a strong security posture that mitigates risk to critical assets and data.
    - We provided a few examples that touched on the disposal of data. For example, an organization might have you, as a security analyst, oversee the destruction of hard drives to make sure that they're properly disposed of. This ensures that private data stored on those drives can't be accessed by threat actors.
- The third domain is security architecture and engineering. This domain is focused on optimizing data security by ensuring effective tools, systems, and processes are in place to protect an organization's assets and data. One of the core concepts of secure design architecture is shared responsibility.
    - Shared responsibility means that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security. By having policies that encourage users to recognize and report security concerns, many issues can be handled quickly and effectively.
- The fourth domain is communication and network security, which is mainly focused on managing and securing physical networks and wireless communications.

    - Secure networks keep an organization's data and communications safe whether on-site, or in the cloud, or when connecting to services remotely.
    - For example, employees working remotely in public spaces need to be protected from vulnerabilities that can occur when they use insecure bluetooth connections or public wifi hotspots.
    - By having security team members remove access to those types of communication channels at the organizational level, employees may be discouraged from practicing insecure behavior that could be exploited by threat actors.
- The fifth domain is identity and access management, or IAM. And it's focused on access and authorization to keep data secure by making sure users follow established policies to control and manage assets.
    - As an entry-level analyst, it's essential to keep an organization's systems and data as secure as possible by ensuring user access is limited to what employees need. Basically, the goal of IAM is to reduce the overall risk to systems and data. For example, if everyone at a company is using the same administrator login, there is no way to track who has access to what data. In the event of a breach, separating valid user activity from the threat actor would be impossible.
    - There are four main components to IAM.
        - Identification is when a user verifies who they are by providing a user name, an access card, or biometric data such as a fingerprint.
        - Authentication is the verification process to prove a person's identity, such as entering a password or PIN.
        - Authorization takes place after a user's identity has been confirmed and relates to their level of access, which depends on the role in the organization.
        - Accountability refers to monitoring and recording user actions, like login attempts, to prove systems and data are used properly.
- The sixth security domain is security assessment and testing. This domain focuses on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities.
    - Security control testing can help an organization identify new and better ways to mitigate threats, risks, and vulnerabilities. This involves examining organizational goals and objectives, and evaluating if the controls being used actually achieve those goals.
    - Collecting and analyzing security data regularly also helps prevent threats and risks to the organization.
    - Analysts might use security control testing evaluations and security assessment reports to improve existing controls or implement new controls. An example of implementing a new control could be requiring the use of multi-factor authentication to better protect the organization from potential threats and risks.
- The seventh security domain is security operations. The security operations domain is focused on conducting investigations and implementing preventative measures.
    - Investigations begin once a security incident has been identified. This process requires a heightened sense of urgency in order to minimize potential risks to the organization. If there is an active attack, mitigating the attack and preventing it from escalating further is essential for ensuring that private information is protected from threat actors.
    - Once the threat has been neutralized, the collection of digital and physical evidence to conduct a forensic investigation will begin. A digital forensic investigation must take place to identify when, how, and why the breach

occurred. This helps security teams determine areas for improvement and preventative measures that can be taken to mitigate future attacks.

- The eighth security domain is software development security. This domain focuses on using secure coding practices.
  - secure coding practices are recommended guidelines that are used to create secure applications and services. The software development lifecycle is an efficient process used by teams to quickly build software products and features. In this process, security is an additional step. By ensuring that each phase of the software development lifecycle undergoes security reviews, security can be fully integrated into the software product.
  - For example, performing a secure design review during the design phase, secure code reviews during the development and testing phases, and penetration testing during the deployment and implementation phase ensures that security is embedded into the software product at every step. This keeps software secure and sensitive data protected, and mitigates unnecessary risk to an organization.

Security domains cybersecurity analysts need to know

As an analyst, you can explore various areas of cybersecurity that interest you. One way to explore those areas is by understanding different security domains and how they're used to organize the work of security professionals. In this reading you will learn more about CISSP's eight security domains and how they relate to the work you'll do as a security analyst.

Domain one: Security and risk management

All organizations must develop their security posture. Security posture is an organization's ability to manage its defense of critical assets and data and react to change. Elements of the security and risk management domain that impact an organization's security posture include:

- Security goals and objectives
- Risk mitigation processes
- Compliance
- Business continuity plans
- Legal regulations

- Professional and organizational ethics

Information security, or InfoSec, is also related to this domain and refers to a set of processes established to secure information. An organization may use playbooks and implement training as a part of their security and risk management program, based on their needs and perceived risk. There are many InfoSec design processes, such as:

- Incident response
- Vulnerability management
- Application security
- Cloud security
- Infrastructure security

As an example, a security team may need to alter how personally identifiable information (PII) is treated in order to adhere to the European Union's General Data Protection Regulation (GDPR).

Domain two: Asset security

Asset security involves managing the cybersecurity processes of organizational assets, including the storage, maintenance, retention, and destruction of physical and virtual data. Because the loss or theft of assets can expose an organization and increase the level of risk, keeping track of assets and the data they hold is essential. Conducting a security impact analysis, establishing a recovery plan, and managing data exposure will depend on the level of risk associated with each asset. Security analysts may need to store, maintain, and retain data by creating backups to ensure they are able to restore the environment if a security incident places the organization’s data at risk.

Domain three: Security architecture and engineering

This domain focuses on managing data security. Ensuring effective tools, systems, and processes are in place helps protect an organization’s assets and data. Security architects and engineers create these processes.

One important aspect of this domain is the concept of shared responsibility. Shared responsibility means all individuals involved take an active role in lowering risk during the design of a security system. Additional design principles related to this domain, which are discussed later in the program, include:

- Threat modeling
- Least privilege
- Defense in depth
- Fail securely
- Separation of duties
- Keep it simple
- Zero trust
- Trust but verify

An example of managing data is the use of a security information and event management (SIEM) tool to monitor for flags related to unusual login or user activity that could indicate a threat actor is attempting to access private data.

Domain four: Communication and network security

This domain focuses on managing and securing physical networks and wireless communications. This includes on-site, remote, and cloud communications.

Organizations with remote, hybrid, and on-site work environments must ensure data remains secure, but managing external connections to make certain that remote workers are securely accessing an organization's networks is a challenge. Designing network security controls—such as restricted network access—can help protect users and ensure an organization's network remains secure when employees travel or work outside of the main office.

Domain five: Identity and access management

The identity and access management (IAM) domain focuses on keeping data secure. It does this by ensuring user identities are trusted and authenticated and that access to physical and logical assets is authorized. This helps prevent unauthorized users, while allowing authorized users to perform their tasks.

Essentially, IAM uses what is referred to as the principle of least privilege, which is the concept of granting only the minimal access and authorization required to complete a task. As an example, a cybersecurity analyst might be asked to ensure that customer service representatives can only view the private data of a customer, such as their phone number, while working to resolve the customer's issue; then remove access when the customer's issue is resolved.

Domain six: Security assessment and testing

The security assessment and testing domain focuses on identifying and mitigating risks, threats, and vulnerabilities. Security assessments help organizations determine whether their internal systems are secure or at risk. Organizations might employ penetration testers, often referred to as "pen testers," to find vulnerabilities that could be exploited by a threat actor.

This domain suggests that organizations conduct security control testing, as well as collect and analyze data. Additionally, it emphasizes the importance of conducting security audits to monitor for and reduce the probability of a data breach. To contribute to these types of tasks, cybersecurity professionals may be tasked with auditing user permissions to validate that users have the correct levels of access to internal systems.

Domain seven: Security operations

The security operations domain focuses on the investigation of a potential data breach and the implementation of preventative measures after a security incident has occurred. This includes using strategies, processes, and tools such as:

- Training and awareness
- Reporting and documentation
- Intrusion detection and prevention
- SIEM tools
- Log management
- Incident management
- Playbooks
- Post-breach forensics
- Reflecting on lessons learned

The cybersecurity professionals involved in this domain work as a team to manage, prevent, and investigate threats, risks, and vulnerabilities. These individuals are trained to handle active attacks, such as large amounts of data being accessed from an organization's internal network, outside of normal working hours. Once a threat is identified, the team works diligently to keep private data and information safe from threat actors.

Domain eight: Software development security

The software development security domain is focused on using secure programming practices and guidelines to create secure applications. Having secure applications helps deliver secure and reliable services, which helps protect organizations and their users.
Security must be incorporated into each element of the software development life cycle, from design and development to testing and release. To achieve security, the software development process must have security in mind at each step. Security cannot be an afterthought.
Performing application security tests can help ensure vulnerabilities are identified and mitigated accordingly. Having a system in place to test the programming conventions, software executables, and security measures embedded in the software is necessary. Having quality assurance and pen tester professionals ensure the software has met security and performance standards is also an essential part of the software development process. For example, an entry-level analyst working for a pharmaceutical company might be asked to make sure encryption is properly configured for a new medical device that will store private patient data.

Threats, risks, and vulnerabilities

- **Asset** : An asset is an item perceived as having value to an organization.
- **Threat** : A threat is any circumstance or event that can negatively impact assets. One example of a threat is a social engineering attack
- **Social engineering** : Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.
    - **Example** : Malicious links in email messages that look like they're from legitimate companies or people is one method of social engineering known as phishing. phishing is a technique that is used to acquire sensitive data, such as user names, passwords, or banking information.
- **Risk :** A risk is anything that can impact the confidentiality, integrity, or availability of an asset. Think of a risk as the likelihood of a threat occurring.
    - **Example :** the lack of backup protocols for making sure its stored information can be recovered in the event of an accident or security incident.

Organizations tend to rate risks at different levels: low, medium, and high, depending on possible threats and the value of an asset.

- A low-risk asset is information that would not harm the organization's reputation or ongoing operations, and would not cause financial damage if compromised. This includes public information such as website content, or published research data.
- A medium-risk asset might include information that's not available to the public and may cause some damage to the organization's finances, reputation, or ongoing operations. For example, the early release of a company's quarterly earnings could impact the value of their stock.
- A high-risk asset is any information protected by regulations or laws, which if compromised, would have a severe negative impact on an organization's finances, ongoing operations, or reputation. This could include leaked assets with SPII, PII, or intellectual property.

Vulnerability:

A vulnerability is a weakness that can be exploited by a threat. And it's worth noting that both a vulnerability and threat must be present for there to be a risk.

Examples of vulnerabilities:

- An outdated firewall, software, or application; weak passwords; or unprotected confidential data.
- People can also be considered a vulnerability. People's actions can significantly affect an organization's internal network. Whether it's a client, external vendor, or employee, maintaining security must be a united effort.

So entry-level analysts need to educate and empower people to be more security conscious. For example, educating people on how to identify a phishing email is a great starting point. Using access cards to grant employee access to physical spaces while restricting outside visitors is another good security measure.

Organizations must continually improve their efforts when it comes to identifying and mitigating vulnerabilities to minimize threats and risks. Entry-level analysts can support this goal by encouraging employees to report suspicious activity and actively monitoring and documenting employees' access to critical assets.

Ransomware

Ransomware is a malicious attack where threat actors encrypt an organization's data then demand payment to restore access.

Once ransomware is deployed by an attacker, it can freeze network systems, leave devices unusable, and encrypt, or lock confidential data, making devices inaccessible.

The threat actor then demands a ransom before providing a decryption key to allow organizations to return to their normal business operations.

Think of a decryption key as a password provided to regain access to your data. Note that when ransom negotiations occur or data is leaked by threat actors, these events can occur through the dark web.

The web is actually an interlinked network of online content that's made up of three layers: the surface web, the deep web, and the dark web.

- The surface web is the layer that most people use. It contains content that can be accessed using a web browser.
- The deep web generally requires authorization to access it. An organization's intranet is an example of the deep web, since it can only be accessed by employees or others who have been granted access.
- The dark web can only be accessed by using special software. The dark web generally carries a negative connotation since it is the preferred web layer for criminals because of the secrecy that it provides.

Three key impacts of threats, risks, and vulnerabilities:

- The first impact we'll discuss is financial impact. When an organization's assets are compromised by an attack, such as the use of malware, the financial consequences can be significant for a variety of reasons. These can include interrupted production and services, the cost to correct the issue, and fines if assets are compromised because of non-compliance with laws and regulations.
- The second impact is identity theft. Organizations must decide whether to store private customer, employee, and outside vendor data, and for how long. Storing any type of

sensitive data presents a risk to the organization. Sensitive data can include personally identifiable information, or PII, which can be sold or leaked through the dark web. That's because the dark web provides a sense of secrecy and threat actors may have the ability to sell data there without facing legal consequences.

- The last impact is damage to an organization's reputation. A solid customer base supports an organization's mission, vision, and financial goals. An exploited vulnerability can lead customers to seek new business relationships with competitors or create bad press that causes permanent damage to an organization's reputation. The loss of customer data doesn't only affect an organization's reputation and financials, it may also result in legal penalties and fines. Organizations are strongly encouraged to take proper security measures and follow certain protocols to prevent the significant impact of threats, risks, and vulnerabilities.

NIST’s Risk Management Framework

National Institute of Standards and Technology, NIST, provides many frameworks that are used by security professionals to manage risks, threats, and vulnerabilities.There are seven steps in the RMF: prepare, categorize, select, implement, assess, authorize, and monitor.

- **Prepare:** Prepare refers to activities that are necessary to manage security and privacy risks before a breach occurs. As an entry-level analyst, you'll likely use this step to monitor for risks and identify controls that can be used to reduce those risks.
- **Categorize** : Categorize is used to develop risk management processes and tasks. Security professionals then use those processes and develop tasks by thinking about how the confidentiality, integrity, and availability of systems and information can be impacted by risk. As an entry-level analyst, you'll need to be able to understand how to follow the processes established by your organization to reduce risks to critical assets, such as private customer information.
- **Select** : Select means to choose, customize, and capture documentation of the controls that protect an organization. An example of the select step would be keeping a playbook up-to-date or helping to manage other documentation that allows you and your team to address issues more efficiently.
- **Implement security and privacy plans for the organization**: Having good plans in place is essential for minimizing the impact of ongoing security risks. For example, if you notice a pattern of employees constantly needing password resets, implementing a change to password requirements may help solve this issue.
- **Assess** : Assess means to determine if established controls are implemented correctly. An organization always wants to operate as efficiently as possible. So it's essential to take the time to analyze whether the implemented protocols, procedures, and controls that are in place are meeting organizational needs. During this step, analysts identify potential weaknesses and determine whether the organization's tools, procedures, controls, and protocols should be changed to better manage potential risks.
- **Authorize** : Authorize means being accountable for the security and privacy risks that may exist in an organization. As an analyst, the authorization step could involve generating reports, developing plans of action, and establishing project milestones that are aligned to your organization's security goals.
- **Monitor**: Monitor means to be aware of how systems are operating. Assessing and maintaining technical operations are tasks that analysts complete daily. Part of maintaining a low level of risk for an organization is knowing how the current systems support the organization's security goals. If the systems in place don't meet those goals, changes may be needed.

Manage common threats, risks, and vulnerabilities

Previously, you learned that security involves protecting organizations and people from threats, risks, and vulnerabilities. Understanding the current threat landscapes gives organizations the ability to create policies and processes designed to help prevent and mitigate these types of security issues. In this reading, you will further explore how to manage risk and some common threat actor tactics and techniques, so you are better prepared to protect organizations and the people they serve when you enter the cybersecurity field.

Risk management

A primary goal of organizations is to protect assets. An **asset** is an item perceived as having value to an organization. Assets can be digital or physical. Examples of digital assets include the personal information of employees, clients, or vendors, such as:

- Social Security Numbers (SSNs), or unique national identification numbers assigned to individuals
- Dates of birth
- Bank account numbers
- Mailing addresses

Examples of physical assets include:

- Payment kiosks
- Servers
- Desktop computers
- Office spaces

Some common strategies used to manage risks include:

- **Acceptance**: Accepting a risk to avoid disrupting business continuity
- **Avoidance**: Creating a plan to avoid the risk altogether
- **Transference**: Transferring risk to a third party to manage
- **Mitigation**: Lessening the impact of a known risk

Additionally, organizations implement risk management processes based on widely accepted frameworks to help protect digital and physical assets from various threats, risks, and vulnerabilities. Examples of frameworks commonly used in the cybersecurity industry include the National Institute of Standards and Technology Risk Management Framework (NIST RMF) and Health Information Trust Alliance (HITRUST).
Following are some common types of threats, risks, and vulnerabilities you'll help organizations manage as a security professional.

Today's most common threats, risks, and vulnerabilities

Threats

A **threat** is any circumstance or event that can negatively impact assets. As an entry-level security analyst, your job is to help defend the organization's assets from inside and outside threats. Therefore, understanding common types of threats is important to an analyst's daily work. As a reminder, common threats include:

- **Insider threats:** Staff members or vendors abuse their authorized access to obtain data that may harm an organization.

- **Advanced persistent threats (APTs):** A threat actor maintains unauthorized access to a system for an extended period of time.

Risks

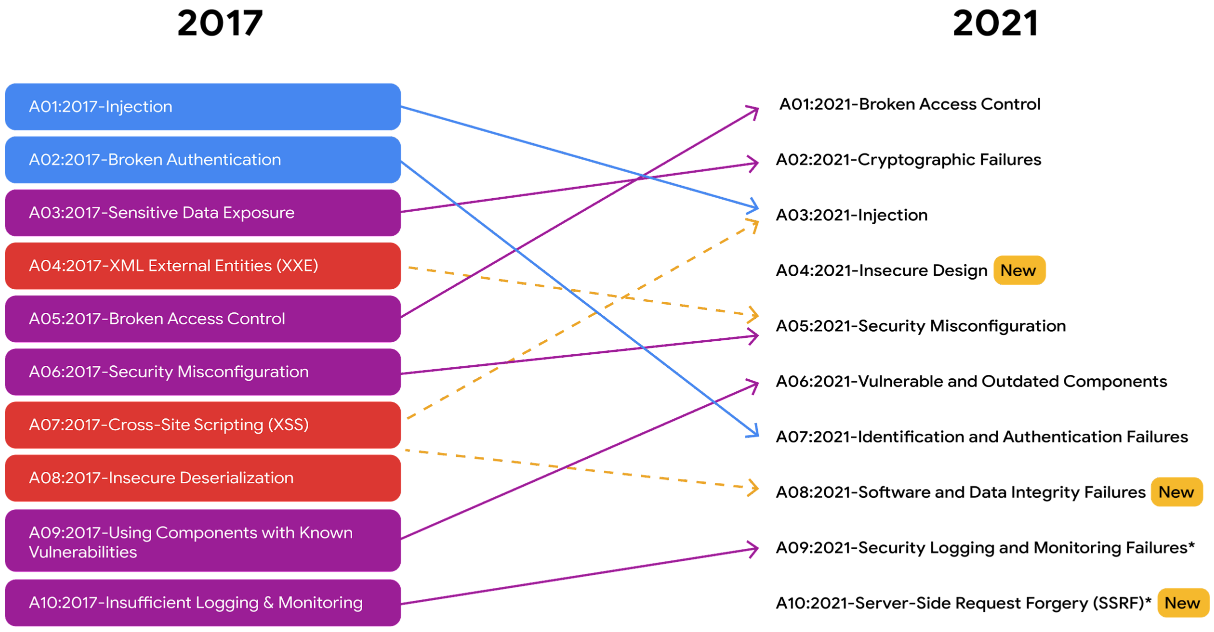
A **risk** is anything that can impact the confidentiality, integrity, or availability of an asset. A basic formula for determining the level of risk is that risk equals the likelihood of a threat. One way to think about this is that a risk is being late to work and threats are traffic, an accident, a flat tire, etc.

There are different factors that can affect the likelihood of a risk to an organization's assets, including:

- **External risk:** Anything outside the organization that has the potential to harm organizational assets, such as threat actors attempting to gain access to private information
- **Internal risk:** A current or former employee, vendor, or trusted partner who poses a security risk
- **Legacy systems:** Old systems that might not be accounted for or updated, but can still impact assets, such as workstations or old mainframe systems. For example, an organization might have an old vending machine that takes credit card payments or a workstation that is still connected to the legacy accounting system.
- **Multiparty risk:** Outsourcing work to third-party vendors can give them access to intellectual property, such as trade secrets, software designs, and inventions.
- **Software compliance/licensing:** Software that is not updated or in compliance, or patches that are not installed in a timely manner

There are many resources, such as the NIST, that provide lists of cybersecurity risks. Additionally, the Open Web Application Security Project (OWASP) publishes a standard awareness document about the top 10 most critical security risks to web applications, which is updated regularly.

Note: The OWASP's common attack types list contains three new risks for the years 2017 to 2021: insecure design, software and data integrity failures, and server-side request forgery. This update emphasizes the fact that security is a constantly evolving field. It also demonstrates the importance of staying up to date on current threat actor tactics and techniques, so you can be better prepared to manage these types of risks.


2017
2021
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design New
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures New
A09:2021-Security Logging and Monitoring Failures*
A10:2021-Server-Side Request Forgery (SSRF)* New

Vulnerabilities

A **vulnerability** is a weakness that can be exploited by a threat. Therefore, organizations need to regularly inspect for vulnerabilities within their systems. Some vulnerabilities include:

- **ProxyLogon:** A pre-authenticated vulnerability that affects the Microsoft Exchange server. This means a threat actor can complete a user authentication process to deploy malicious code from a remote location.
- **ZeroLogon:** A vulnerability in Microsoft's Netlogon authentication protocol. An authentication protocol is a way to verify a person's identity. Netlogon is a service that ensures a user's identity before allowing access to a website's location.
- **Log4Shell:** Allows attackers to run Java code on someone else's computer or leak sensitive information. It does this by enabling a remote attacker to take control of devices connected to the internet and run malicious code.
- **PetitPotam:** Affects Windows New Technology Local Area Network (LAN) Manager (NTLM). It is a theft technique that allows a LAN-based attacker to initiate an authentication request.
- **Security logging and monitoring failures:** Insufficient logging and monitoring capabilities that result in attackers exploiting vulnerabilities without the organization knowing it
- **Server-side request forgery:** Allows attackers to manipulate a server-side application into accessing and updating backend resources. It can also allow threat actors to steal data.

As an entry-level security analyst, you might work in vulnerability management, which is monitoring a system to identify and mitigate vulnerabilities. Although patches and updates may exist, if they are not applied, intrusions can still occur. For this reason, constant monitoring is important. The sooner an organization identifies a vulnerability and addresses it by patching it or updating their systems, the sooner it can be mitigated, reducing the organization's exposure to the vulnerability.

To learn more about the vulnerabilities explained in this section of the reading, as well as other vulnerabilities, explore the NIST National Vulnerability Database and CISA Known Exploited Vulnerabilities Catalog.

Terms and definitions from Course 2, Module 1

- **Assess:** The fifth step of the NIST RMF that means to determine if established controls are implemented correctly
- **Authorize:** The sixth step of the NIST RMF that refers to being accountable for the security and privacy risks that may exist in an organization
- **Business continuity:** An organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans
- **Categorize:** The second step of the NIST RMF that is used to develop risk management processes and tasks
- **External threat:** Anything outside the organization that has the potential to harm organizational assets
- **Implement:** The fourth step of the NIST RMF that means to implement security and privacy plans for an organization
- **Internal threat:** A current or former employee, external vendor, or trusted partner who poses a security risk
- **Monitor**: The seventh step of the NIST RMF that means be aware of how systems are operating
- **Prepare:** The first step of the NIST RMF related to activities that are necessary to manage security and privacy risks before a breach occurs

- **Ransomware:** A malicious attack where threat actors encrypt an organization's data and demand payment to restore access
- **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
- **Security posture:** An organization's ability to manage its defense of critical assets and data and react to change
- **Select**: The third step of the NIST RMF that means to choose, customize, and capture documentation of the controls that protect an organization
- **Shared responsibility:** The idea that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security
- **Social engineering:** A manipulation technique that exploits human error to gain private information, access, or valuables
- **Vulnerability:** A weakness that can be exploited by a threat

Module 2 - Security Frameworks and Controls

The relationship between frameworks and controls

Previously, you learned how organizations use security frameworks and controls to protect against threats, risks, and vulnerabilities. This included discussions about the National Institute of Standards and Technology's (NIST's) Risk Management Framework (RMF) and Cybersecurity Framework (CSF), as well as the confidentiality, integrity, and availability (CIA) triad. In this reading, you will further explore security frameworks and controls and how they are used together to help mitigate organizational risk.

Frameworks and controls

Security frameworks are guidelines used for building plans to help mitigate risk and threats to data and privacy. Frameworks support organizations' ability to adhere to compliance laws and regulations. For example, the healthcare industry uses frameworks to comply with the United States' Health Insurance Portability and Accountability Act (HIPAA), which requires that medical professionals keep patient information safe.

Security controls are safeguards designed to reduce *specific* security risks. Security controls are the measures organizations use to lower risk and threats to data and privacy. For example, a control that can be used alongside frameworks to ensure a hospital remains compliant with HIPAA is requiring that patients use multi-factor authentication (MFA) to access their medical records. Using a measure like MFA to validate someone's identity is one way to help mitigate potential risks and threats to private data.

Specific frameworks and controls

There are many different frameworks and controls that organizations can use to remain compliant with regulations and achieve their security goals. Frameworks covered in this reading are the Cyber Threat Framework (CTF) and the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001. Several common security controls, used alongside these types of frameworks, are also explained.

Cyber Threat Framework (CTF)

According to the Office of the Director of National Intelligence, the CTF was developed by the U.S. government to provide “a common language for describing and communicating information about cyber threat activity.” By providing a common language to communicate information about threat activity, the CTF helps cybersecurity professionals analyze and share information more efficiently. This allows organizations to improve their response to the constantly evolving cybersecurity landscape and threat actors' many tactics and techniques.

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001

An internationally recognized and used framework is ISO/IEC 27001. The ISO 27000 family of standards enables organizations of all sectors and sizes to manage the security of assets, such as financial information, intellectual property, employee data, and information entrusted to third parties. This framework outlines requirements for an information security management system, best practices, and controls that support an organization’s ability to manage risks. Although the ISO/IEC 27001 framework does not require the use of specific controls, it does provide a collection of controls that organizations can use to improve their security posture.

Controls

Controls are used alongside frameworks to reduce the possibility and impact of a security threat, risk, or vulnerability. Controls can be physical, technical, and administrative and are typically used to prevent, detect, or correct security issues.
Examples of physical controls:

- Gates, fences, and locks
- Security guards
- Closed-circuit television (CCTV), surveillance cameras, and motion detectors
- Access cards or badges to enter office spaces

Examples of technical controls:

- Firewalls
- MFA
- Antivirus software

Examples of administrative controls:

- Separation of duties
- Authorization
- Asset classification

To learn more about controls, particularly those used to protect health-related assets from a variety of threat types, review the U.S. Department of Health and Human Services’ Physical Access Control presentation.

Frameworks

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy, such as social engineering attacks and ransomware. Security involves more than just the virtual space. It also includes the physical, which is why many organizations have plans to maintain safety in the work environment. For example, access to a building may require using a key card or badge.

People are the biggest threat to security.Educating employees about existing security challenges is essential for minimizing the possibility of a breach. Providing training about how to recognize red flags, or potential threats, is essential, along with having plans in place to quickly report and address security issues.

Controls

While frameworks are used to create plans to address security risks, threats, and vulnerabilities, controls are used to reduce specific risks. If proper controls are not in place, an organization could face significant financial impacts and damage to their reputation because of exposure to risks including trespassing, creating fake employee accounts, or providing free benefits.

Security controls are safeguards designed to reduce specific security risks.Three common types of controls: encryption, authentication, and authorization.

- Encryption is the process of converting data from a readable format to an encoded format. Typically, encryption involves converting data from plaintext to ciphertext. Ciphertext is the raw, encoded message that's unreadable to humans and computers. Ciphertext data cannot be read until it's been decrypted into its original plaintext form. Encryption is used to ensure confidentiality of sensitive data, such as customers' account information or social security numbers.
- Authentication is the process of verifying who someone or something is. A real-world example of authentication is logging into a website with your username and password. This basic form of authentication proves that you know the username and password and should be allowed to access the website. More advanced methods of authentication, such as multi-factor authentication, or MFA, challenge the user to demonstrate that they are who they claim to be by requiring both a password and an additional form of authentication, like a security code or biometrics, such as a fingerprint, voice, or face scan.
    - Biometrics are unique physical characteristics that can be used to verify a person's identity. Examples of biometrics are a fingerprint, an eye scan, or a palm scan. One example of a social engineering attack that can exploit biometrics is vishing. Vishing is the exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source. For example, vishing could be used to impersonate a person's voice to steal their identity and then commit a crime.
- Authorization refers to the concept of granting access to specific resources within a system. Essentially, authorization is used to verify that a person has permission to access a resource. As an example, if you're working as an entry-level security analyst for the federal government, you could have permission to access data through the deep web or other internal data that is only accessible if you're a federal employee.

Explore the CIA triad

While working as an entry-level security analyst, your main responsibility is to help protect your organization's sensitive assets and data from threat actors.

The CIA triad is a model that helps inform how organizations consider risk when setting up systems and security policies.

- Confidentiality means that only authorized users can access specific assets or data. Sensitive data should be available on a "need to know" basis, so that only the people who are authorized to handle certain assets or data have access.
- Integrity means that the data is correct, authentic, and reliable. Determining the integrity of data and analyzing how it's used will help you, as a security professional, decide whether the data can or cannot be trusted.
- Availability means that the data is accessible to those who are authorized to access it. Inaccessible data isn't useful and can prevent people from being able to do their jobs. As a security professional, ensuring that systems, networks, and applications are functioning properly to allow for timely and reliable access, may be a part of your everyday work responsibilities.

Example :

- If you work for an organization that has large amounts of private data like a bank, the principle of confidentiality is essential because the bank must keep people's personal and financial information safe.
- The principle of integrity is also a priority. For example, if a person's spending habits or purchasing locations change dramatically, the bank will likely disable access to the account until they can verify that the account owner, not a threat actor, is actually the one making purchases.
- The availability principle is also critical. Banks put a lot of effort into making sure that people can access their account information easily on the web. And to make sure that information is protected from threat actors, banks use a validation process to help minimize damage if they suspect that customer accounts have been compromised.

Use the CIA triad to protect organizations

The CIA triad for analysts

The **CIA triad** is a model that helps inform how organizations consider risk when setting up systems and security policies. It is made up of three elements that cybersecurity analysts and organizations work toward upholding: confidentiality, integrity, and availability. Maintaining an acceptable level of risk and ensuring systems and policies are designed with these elements in mind helps establish a successful **security posture**, which refers to an organization's ability to manage its defense of critical assets and data and react to change.

Confidentiality

Confidentiality is the idea that only authorized users can access specific assets or data. In an organization, confidentiality can be enhanced through the implementation of design principles, such as the principle of least privilege. The principle of least privilege limits users' access to only the information they need to complete work-related tasks. Limiting access is one way of maintaining the confidentiality and security of private data.

Integrity

Integrity is the idea that the data is verifiably correct, authentic, and reliable. Having protocols in place to verify the authenticity of data is essential. One way to verify data integrity is through cryptography, which is used to transform data so unauthorized parties cannot read or tamper with it (NIST, 2022). Another example of how an organization might implement integrity is by enabling encryption, which is the process of converting data from a readable format to an encoded format. Encryption can be used to prevent access and ensure data, such as messages on an organization's internal chat platform, cannot be tampered with.

Availability

Availability is the idea that data is accessible to those who are authorized to use it. When a system adheres to both availability and confidentiality principles, data can be used when needed. In the workplace, this could mean that the organization allows remote employees to access its internal network to perform their jobs. It's worth noting that access to data on the internal network is still limited, depending on what type of access employees need to do their jobs. If, for example, an employee works in the organization's accounting department, they might need access to corporate accounts but not data related to ongoing development projects.

NIST frameworks

Organizations use frameworks as a starting point to develop plans that mitigate risks, threats, and vulnerabilities to sensitive data and assets.

The National Institute of Standards and Technology, or NIST's frameworks that can support ongoing security efforts for all types of organizations, including for profit and nonprofit businesses, as well as government agencies. While NIST is a US based organization, the guidance it provides can help analysts all over the world understand how to implement essential cybersecurity practices. One NIST framework that we'll discuss throughout the program is the NIST Cybersecurity Framework, or CSF.

CSF

- The CSF is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk.
- This framework is widely respected and essential for maintaining security regardless of the organization you work for.
- The CSF consists of five important core functions, identify, protect, detect, respond, and recover.
    - Example : Imagine that one morning you receive a high-risk notification that a workstation has been compromised. You identify the workstation, and discover that there's an unknown device plugged into it. You block the unknown device remotely to stop any potential threat and protect the organization. Then you remove the infected workstation to prevent the spread of the damage and use tools to detect any additional threat actor behavior and identify the unknown device. You respond by investigating the incident to determine who used the unknown device, how the threat occurred, what was affected, and where the attack originated.In this case, you discover that an employee was charging their infected phone using a USB port on their work laptop. Finally, you do your best to recover any files or data that were affected and correct any damage the threat caused to the workstation itself.
- The core functions of the NIST CSF provide specific guidance and direction for security professionals. This framework is used to develop plans to handle an

    incident appropriately and quickly to lower risk, protect an organization against a threat, and mitigate any potential vulnerabilities.
    - The NIST CSF also expands into the protection of the United States federal government with NIST special publication, or SP 800-53. It provides a unified framework for protecting the security of information systems within the federal government, including the systems provided by private companies for federal government use.

The five functions of the NIST Cybersecurity Framework

NIST CSF focuses on five core functions: identify, protect, detect, respond, and recover. These core functions help organizations manage cybersecurity risks, implement risk management strategies, and learn from previous mistakes.

- The first core function is identify, which is related to the management of cybersecurity risk and its effect on an organization's people and assets. For example, as a security analyst, you may be asked to monitor systems and devices in your organization's internal network to identify potential security issues
- The second core function is protect, which is the strategy used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats.
    - For example, as a security analyst, you and your team might encounter new and unfamiliar threats and attacks. For this reason, studying historical data and making improvements to policies and procedures is essential.
- The third core function is detect, which means identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections. For example, as an analyst, you might be asked to review a new security tool's setup to make sure it's flagging low, medium, or high risk, and then alerting the security team about any potential threats or incidents.
- The fourth function is respond, which means making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process.
    - For Example, As an analyst, you could be working with a team to collect and organize data to document an incident and suggest improvements to processes to prevent the incident from happening again.
- The fifth core function is recover, which is the process of returning affected systems back to normal operation.
    - For example, as an entry-level security analyst, you might work with your security team to restore systems, data, and assets, such as financial or legal files, that have been affected by an incident like a breach.

OWASP security principles (Open Web Application Security Project, or OWASP)

- **Minimize the attack surface area**
    - An attack surface refers to all the potential vulnerabilities that a threat actor could exploit, like attack vectors, which are pathways attackers use to penetrate security defenses.
    - Examples of common attack vectors are phishing emails and weak passwords. To minimize the attack surface and avoid incidents from these types of vectors,

security teams might disable software features, restrict who can access certain assets, or establish more complex password requirements.

- **Principle of least privilege**
    - It means making sure that users have the least amount of access required to perform their everyday tasks. The main reason for limiting access to organizational information and resources is to reduce the amount of damage a security breach could cause.
    - For example, as an entry-level analyst, you may have access to log data, but may not have access to change user permissions. Therefore, if a threat actor compromises your credentials, they'll only be able to gain limited access to digital or physical assets, which may not be enough for them to deploy their intended attack.

- **Defense in depth**
    - Defense in depth means that an organization should have multiple security controls that address risks and threats in different ways.
    - One example of a security control is multi-factor authentication, or MFA, which requires users to take an additional step beyond simply entering their username and password to gain access to an application.
    - Other controls include firewalls, intrusion detection systems, and permission settings that can be used to create multiple points of defense, a threat actor must get through to breach an organization.
- **Separation of duties :**
    - It can be used to prevent individuals from carrying out fraudulent or illegal activities. This principle means that no one should be given so many privileges that they can misuse the system.
    - For example, the person in a company who signs the paychecks shouldn't also be the person who prepares them.
- **Keep security simple**:
    - when implementing security controls, unnecessarily complicated solutions should be avoided because they can become unmanageable. The more complex the security controls are, the harder it is for people to work collaboratively.
- **Fix security issues correctly**:
    - Technology is a great tool, but can also present challenges. When a security incident occurs, security professionals are expected to identify the root cause quickly. From there, it's important to correct any identified vulnerabilities and conduct tests to ensure that repairs are successful.
    - An example of an issue is a weak password to access an organization's wifi because it could lead to a breach. To fix this type of security issue, stricter password policies could be put in place.

Security principles

In the workplace, security principles are embedded in your daily tasks. Whether you are analyzing logs, monitoring a security information and event management (SIEM) dashboard, or using a vulnerability scanner, you will use these principles in some way.
Previously, you were introduced to several OWASP security principles. These included:

- **Minimize attack surface area**: Attack surface refers to all the potential vulnerabilities a threat actor could exploit.
- **Principle of least privilege**: Users have the least amount of access required to perform their everyday tasks.
- **Defense in depth**: Organizations should have varying security controls that mitigate risks and threats.

- **Separation of duties**: Critical actions should rely on multiple people, each of whom follow the principle of least privilege.
- **Keep security simple**: Avoid unnecessarily complicated solutions. Complexity makes security difficult.
- **Fix security issues correctly**: When security incidents occur, identify the root cause, contain the impact, identify vulnerabilities, and conduct tests to ensure that remediation is successful.

Additional OWASP security principles

Next, you'll learn about four additional OWASP security principles that cybersecurity analysts and their teams use to keep organizational operations and people safe.

Establish secure defaults

This principle means that the optimal security state of an application is also its default state for users; it should take extra work to make the application insecure.

Fail securely

Fail securely means that when a control fails or stops, it should do so by defaulting to its most secure option. For example, when a firewall fails it should simply close all connections and block all new ones, rather than start accepting everything.

Don't trust services

Many organizations work with third-party partners. These outside partners often have different security policies than the organization does. And the organization shouldn't explicitly trust that their partners' systems are secure. For example, if a third-party vendor tracks reward points for airline customers, the airline should ensure that the balance is accurate before sharing that information with their customers.

Avoid security by obscurity

The security of key systems should not rely on keeping details hidden. Consider the following example from OWASP (2016):

The security of an application should not rely on keeping the source code secret. Its security should rely upon many other factors, including reasonable password policies, defense in depth, business transaction limits, solid network architecture, and fraud and audit controls.

Plan a security audit

A security audit is a review of an organization's security controls, policies, and procedures against a set of expectations.

There are two main types of security audits: external and internal.

We'll focus on internal security audits because those are the types of audits that entry-level analysts might be asked to contribute to.

- An internal security audit is typically conducted by a team of people that might include an organization's compliance officer, security manager, and other security team members. Internal security audits are used to help improve an organization's security posture and help organizations avoid fines from governing agencies due to a lack of compliance. Internal security audits help security teams identify organizational risk, assess controls, and correct compliance issues.

- Some common elements of internal audits. These include establishing the scope and goals of the audit, conducting a risk assessment of the organization's assets, completing a controls assessment, assessing compliance, and communicating results to stakeholders.

- **Establishing the scope and goals**
  - Scope refers to the specific criteria of an internal security audit. Scope requires organizations to identify people, assets, policies, procedures, and technologies that might impact an organization's security posture.
  - Goals are an outline of the organization's security objectives, or what they want to achieve in order to improve their security posture.
  - Although more senior-level security team members and other stakeholders usually establish the scope and goals of the audit, entry-level analysts might be asked to review and understand the scope and goals in order to complete other elements of the audit.
  - As an example, the scope of this audit involves assessing user permissions; identifying existing controls, policies, and procedures; and accounting for the technology currently in use by the organization. The goals outlined include implementing core functions of frameworks, like the NIST CSF; establishing policies and procedures to ensure compliance; and strengthening system controls.

- **Conducting a risk assessment**
  - It is focused on identifying potential threats, risks, and vulnerabilities. This helps organizations consider what security measures should be implemented and monitored to ensure the safety of assets. Similar to establishing the scope and goals, a risk assessment is oftentimes completed by managers or other stakeholders.
  - However, you might be asked to analyze details provided in the risk assessment to consider what types of controls and compliance regulations need to be in place to help improve the organization's security posture.
  - For example, this risk assessment highlights that there are inadequate controls, processes, and procedures in place to protect the organization's assets. Specifically, there is a lack of proper management of physical and digital assets, including employee equipment.
  - The equipment used to store data is not properly secured. And access to private information stored in the organization's internal network likely needs more robust controls in place. Now that we've discussed the initial planning elements of an internal security audit, coming up, we'll focus on the last three elements.

- **Controls assessment.**
  - A controls assessment involves closely reviewing an organization's existing assets, then evaluating potential risks to those assets, to ensure internal controls and processes are effective.
  - To do this, entry-level analysts might be tasked with classifying controls into the following categories: administrative controls, technical controls, and physical
  - Administrative controls are related to the human component of cybersecurity. They include policies and procedures that define how an organization manages data, such as the implementation of password policies.
  - Technical controls are hardware and software solutions used to protect assets, such as the use of intrusion detection systems, or IDS's, and encryption.

    - Physical controls refer to measures put in place to prevent physical access to protected assets, such as surveillance cameras and locks.

- **Determining whether or not the organization is adhering to necessary compliance regulations.**
    - As a reminder, compliance regulations are laws that organizations must follow to ensure private data remains secure. In this example, the organization conducts business in the European Union and accepts credit card payments. So they need to adhere to the GDPR and Payment Card Industry Data Security Standard, or PCI DSS.

- **Communication.**
    - Once the internal security audit is complete, results and recommendations need to be communicated to stakeholders. In general, this type of communication summarizes the scope and goals of the audit.
    - Then, it lists existing risks and notes how quickly those risks need to be addressed.
    - Additionally, it identifies compliance regulations the organization needs to adhere to and provides recommendations for improving the organization's security posture.

➔ Internal audits are a great way to identify gaps within an organization.
➔ When I worked at a previous company, my team and I conducted an internal password audit and found that many of the passwords were weak.
➔ Once we identified this issue, the compliance team took the lead and began enforcing stricter password policies

Security audits

A **security audit** is a review of an organization's security controls, policies, and procedures against a set of expectations. Audits are independent reviews that evaluate whether an organization is meeting internal and external criteria. Internal criteria include outlined policies, procedures, and best practices. External criteria include regulatory compliance, laws, and federal regulations.
Additionally, a security audit can be used to assess an organization's established security controls. As a reminder, **security controls** are safeguards designed to reduce specific security risks.
Audits help ensure that security checks are made (i.e., daily monitoring of security information and event management dashboards), to identify threats, risks, and vulnerabilities. This helps maintain an organization’s security posture. And, if there are security issues, a remediation process must be in place.

Goals and objectives of an audit

The goal of an audit is to ensure an organization's information technology (IT) practices are meeting industry and organizational standards. The objective is to identify and address areas of remediation and growth. Audits provide direction and clarity by identifying what the current failures are and developing a plan to correct them.

Security audits must be performed to safeguard data and avoid penalties and fines from governmental agencies. The frequency of audits is dependent on local laws and federal compliance regulations.

Factors that affect audits

Factors that determine the types of audits an organization implements include:

- Industry type
- Organization size
- Ties to the applicable government regulations
- A business's geographical location
- A business decision to adhere to a specific regulatory compliance

To review common compliance regulations that different organizations need to adhere to, refer to the reading about controls, frameworks, and compliance.

The role of frameworks and controls in audits

Along with compliance, it's important to mention the role of frameworks and controls in security audits. Frameworks such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and the international standard for information security (ISO 27000) series are designed to help organizations prepare for regulatory compliance security audits. By adhering to these and other relevant frameworks, organizations can save time when conducting external and internal audits. Additionally, frameworks, when used alongside controls, can support organizations' ability to align with regulatory compliance requirements and standards.

There are three main categories of controls to review during an audit, which are administrative and/or managerial, technical, and physical controls.

To learn more about specific controls related to each category, click the following link and select "Use Template."

Link to template: Control categories

OR

If you don't have a Google account, you can download the template directly from the following attachment

Control categories

DOCX File

Control categories

Control categories

Controls within cybersecurity are grouped into three main categories:

- Administrative/Managerial controls
- Technical controls
- Physical controls

Administrative/Managerial controls address the human component of cybersecurity. These controls include policies and procedures that define how an organization manages data and clearly defines employee responsibilities, including their role in protecting the organization. While administrative controls are typically policy based, the enforcement of those policies may require the use of technical or physical controls.

Technical controls consist of solutions such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus (AV) products, encryption, etc. Technical controls can be used in a number of ways to meet organizational goals and objectives.

Physical controls include door locks, cabinet locks, surveillance cameras, badge readers, etc. They are used to limit physical access to physical assets by unauthorized personnel.

Control types

Control types include, but are not limited to:

1. Preventative
2. Corrective
3. Detective
4. Deterrent

These controls work together to provide defense in depth and protect assets. **Preventative controls** are designed to prevent an incident from occurring in the first place. **Corrective controls** are used to restore an asset after an incident. **Detective controls** are implemented to determine whether an incident has occurred or is in progress. **Deterrent controls** are designed to discourage attacks.

Review the following charts for specific details about each type of control and its purpose.

Administrative Controls		
Control Name	**Control Type**	**Control Purpose**
Least Privilege	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts
Disaster recovery plans	Corrective	Provide business continuity
Password policies	Preventative	Reduce likelihood of account compromise through brute force or dictionary attack techniques
Access control policies	Preventative	Bolster confidentiality and integrity by defining which

Administrative Controls		
		groups can access or modify data
Account management policies	Preventative	Managing account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage
Separation of duties	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts

Technical Controls		
Control Name	**Control Type**	**Control Purpose**
Firewall	Preventative	To filter unwanted or malicious traffic from entering the network
IDS/IPS	Detective	To detect and prevent anomalous traffic that matches a signature or rule
Encryption	Deterrent	Provide confidentiality to sensitive information
Backups	Corrective	Restore/recover from an event
Password management	Preventative	Reduce password fatigue
Antivirus (AV) software	Corrective	Detect and quarantine known threats
Manual monitoring, maintenance, and intervention	Preventative	Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems

Physical Controls		
Control Name	**Control Type**	**Control Purpose**
Time-controlled safe	Deterrent	Reduce attack surface and overall impact from physical

		threats
Adequate lighting	Deterrent	Deter threats by limiting “hiding” places
Closed-circuit television (CCTV)	Preventative/Detective	Closed circuit television is both a preventative and detective control because it’s presence can reduce risk of certain types of events from occurring, and can be used after an event to inform on event conditions
Locking cabinets (for network gear)	Preventative	Bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear
Signage indicating alarm service provider	Deterrent	Deter certain types of threats by making the likelihood of a successful attack seem low
Locks	Deterrent/Preventative	Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative	Detect fire in physical location and prevent damage to physical assets such as inventory, servers, etc.

Audit checklist

It’s necessary to create an audit checklist before conducting an audit. A checklist is generally made up of the following areas of focus:

Identify the scope of the audit

- The audit should:
    - List assets that will be assessed (e.g., firewalls are configured correctly, PII is secure, physical assets are locked, etc.)
    - Note how the audit will help the organization achieve its desired goals
    - Indicate how often an audit should be performed
    - Include an evaluation of organizational policies, protocols, and procedures to make sure they are working as intended and being implemented by employees

Complete a risk assessment

- A risk assessment is used to evaluate identified organizational risks related to budget, controls, internal processes, and external standards (i.e., regulations).

Conduct the audit

- When conducting an internal audit, you will assess the security of the identified assets listed in the audit scope.

Create a mitigation plan

- A mitigation plan is a strategy established to lower the level of risk and potential costs, penalties, or other issues that can negatively affect the organization's security posture.

Communicate results to stakeholders

- The end result of this process is providing a detailed report of findings, suggested improvements needed to lower the organization's level of risk, and compliance regulations and standards the organization needs to adhere to.

Resources for more information

Resources that you can explore to further develop your understanding of audits in the cybersecurity space are:

- Assessment and Auditing Resources
- IT Disaster Recovery Plan

Terms and definitions from Course 2, Module 2

- **Asset:** An item perceived as having value to an organization
- **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
- **Availability:** The idea that data is accessible to those who are authorized to access it
- **Biometrics:** The unique physical characteristics that can be used to verify a person's identity
- **Confidentiality:** The idea that only authorized users can access specific assets or data
- **Confidentiality, integrity, availability (CIA) triad:** A model that helps inform how organizations consider risk when setting up systems and security policies
- **Detect:** A NIST core function related to identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections
- **Encryption:** The process of converting data from a readable format to an encoded format
- **Identify**: A NIST core function related to management of cybersecurity risk and its effect on an organization's people and assets
- **Integrity:** The idea that the data is correct, authentic, and reliable
- **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) Special Publication (S.P.) 800-53:** A unified framework for protecting the security of information systems within the U.S. federal government
- **Open Web Application Security Project/Open Worldwide Application Security Project (OWASP):** A non-profit organization focused on improving software security
- **Protect:** A NIST core function used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats

- **Recover:** A NIST core function related to returning affected systems back to normal operation
- **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
- **Risk:** Anything that can impact the confidentiality, integrity, or availability of an asset
- **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 frameworks:** Guidelines used for building plans to help mitigate risk and threats to data and privacy
- **Security posture:** An organization's ability to manage its defense of critical assets and data and react to change
- **Threat:** Any circumstance or event that can negatively impact assets

Activity

Scenario

Review the following scenario. Then complete the step-by-step instructions.

This scenario is based on a fictional company:

Botium Toys is a small U.S. business that develops and sells toys. The business has a single physical location, which serves as their main office, a storefront, and warehouse for their products. However, Botium Toy's online presence has grown, attracting customers in the U.S. and abroad. As a result, their information technology (IT) department is under increasing pressure to support their online market worldwide.

The manager of the IT department has decided that an internal IT audit needs to be conducted. She expresses concerns about not having a solidified plan of action to ensure business continuity and compliance, as the business grows. She believes an internal audit can help better secure the company's infrastructure and help them identify and mitigate potential risks, threats, or vulnerabilities to critical assets. The manager is also interested in ensuring that they comply with regulations related to internally processing and accepting online payments and conducting business in the European Union (E.U.).

The IT manager starts by implementing the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), establishing an audit scope and goals, listing assets currently managed by the IT department, and completing a risk assessment. The goal of the audit is to provide an overview of the risks and/or fines that the company might experience due to the current state of their security posture.

Your task is to review the IT manager's scope, goals, and risk assessment report. Then, perform an internal audit by completing a controls and compliance checklist.

Step-By-Step Instructions

Step 1: Access supporting materials

The following supporting materials will help you complete this activity. Keep materials open as you proceed to the next steps.
To use the supporting materials for this course item, click the links.
Links to supporting materials:

- Botium Toys: Scope, goals, and risk assessment report
- Control categories

OR
If you don't have a Google account, you can download the supporting materials directly from the following attachments.
Botium Toys Scope, goals, and risk assessment report
DOCX File
Control categories
DOCX File

Step 2: Conduct the audit: Controls and compliance checklist

Conduct the next step of the security audit by completing the controls and compliance checklist.
To complete the checklist, open the supporting materials provided in Step 1. Then:
1. Review the scope, goals, and risk assessment report details, with a focus on:
a. The assets currently managed by the IT department
b. The bullet points under "Additional comments" in the Risk assessment section
2. Consider information provided in the scenario, the scope, goals, and risk assessment report, as well as details provided in other documents linked within the checklist.
3. Then, review the question in the controls and compliance sections of the checklist and select "yes" or "no" to answer the question in each section *(note: the recommendations section is optional).**

To use the supporting materials for this step, click the following link.
Link to supporting materials: Controls and compliance checklist
OR
If you don't have a Google account, you can download the supporting materials directly from the following attachment.
*If using the DOCX File, type an X to select "yes" or "no".
Controls and compliance checklist
DOCX File

Module 3 - Introduction to CyberSecurity Tools

Terms and definitions from Course 2, Module 3

- **Chronicle:** A cloud-native tool designed to retain, analyze, and search data
- **Incident response:** An organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach
- **Log:** A record of events that occur within an organization's systems
- **Metrics:** Key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application
- **Operating system (OS):** The interface between computer hardware and the user
- **Playbook:** A manual that provides details about any operational action
- **Security information and event management (SIEM):** An application that collects and analyzes log data to monitor critical activities in an organization
- **Security orchestration, automation, and response (SOAR):** A collection of applications, tools, and workflows that use automation to respond to security events
- **SIEM tools:** A software platform that collects, analyzes, and correlates security data from various sources across your IT infrastructure that helps identify and respond to security threats in real-time, investigate security incidents, and comply with security regulations
- **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

Logs and SIEM tools

As a security analyst, one of your responsibilities might include analyzing log data to mitigate and manage threats, risks, and vulnerabilities.

A log is a record of events that occur within an organization's systems and networks. Security analysts access a variety of logs from different sources.

Three common log sources include firewall logs, network logs, and server logs.

- A firewall log is a record of attempted or established connections for incoming traffic from the internet. It also includes outbound requests to the internet from within the network.
- A network log is a record of all computers and devices that enter and leave the network. It also records connections between devices and services on the network.
- A server log is a record of events related to services such as websites, emails, or file shares. It includes actions such as login, password, and username requests.

SEIM TOOLS USING LOG

SIEM tools rely on logs to monitor systems and detect security threats.

A security information and event management, or SIEM, tool is an application that collects and analyzes log data to monitor critical activities in an organization. It provides real-time visibility, event monitoring and analysis, and automated alerts. It also stores all log data in a centralized location.

Because SIEM tools index and minimize the number of logs a security professional must manually review and analyze, they increase efficiency and save time.

But, SIEM tools must be configured and customized to meet each organization's unique security needs. As new threats and vulnerabilities emerge, organizations must continually customize their SIEM tools to ensure that threats are detected and quickly addressed.

SIEM dashboards

- SIEM tools can also be used to create dashboards.Just like weather apps help people make quick and informed decisions based on data, SIEM dashboards help security analysts quickly and easily access their organization's security information as charts, graphs, or tables.
- For example, a security analyst receives an alert about a suspicious login attempt. The analyst accesses their SIEM dashboard to gather information about this alert. Using the dashboard, the analyst discovers that there have been 500 login attempts for Ymara's account in the span of five-minutes. They also discover that the login attempts happened from geographic locations outside of Ymara's usual location and outside of her usual working hours. By using a dashboard, the security analyst was able to quickly review visual representations of the timeline of the login attempts, the location, and the exact time of the activity, then determine that the activity was suspicious.

- In addition to providing a comprehensive summary of security-related data, SIEM dashboards also provide stakeholders with different metrics. Metrics are key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application.
- SIEM dashboards can be customized to display specific metrics or other data that are relevant to different members in an organization. For example, a security analyst may create a dashboard that displays metrics for monitoring everyday business operations, like the volume of incoming and outgoing network traffic.

Current SIEM solutions

A **SIEM** tool is an application that collects and analyzes log data to monitor critical activities in an organization. SIEM tools offer real-time monitoring and tracking of security event logs. The data is then used to conduct a thorough analysis of any potential security threat, risk, or vulnerability identified. SIEM tools have many dashboard options. Each dashboard option helps cybersecurity team members manage and monitor organizational data. However, currently, SIEM tools require human interaction for analysis of security events.

The future of SIEM tools

- As cybersecurity continues to evolve, the need for cloud functionality has increased. SIEM tools have and continue to evolve to function in cloud-hosted and cloud-native environments. Cloud-hosted SIEM tools are operated by vendors who are responsible for maintaining and managing the infrastructure required to use the tools. Cloud-hosted tools are simply accessed through the internet and are an ideal solution for organizations that don’t want to invest in creating and maintaining their own infrastructure.

- Similar to cloud-hosted SIEM tools, cloud-native SIEM tools are also fully maintained and managed by vendors and accessed through the internet. However, cloud-native tools are designed to take full advantage of cloud computing capabilities, such as availability, flexibility, and scalability.

- Yet, the evolution of SIEM tools is expected to continue in order to accommodate the changing nature of technology, as well as new threat actor tactics and techniques. For example, consider the current development of interconnected devices with access to the internet, known as the Internet of Things (IoT). The more interconnected devices there are, the larger the cybersecurity attack surface and the amount of data that threat actors can exploit. The diversity of attacks and data that require special attention is expected to grow significantly. Additionally, as artificial intelligence (AI) and machine learning (ML) technology continues to progress, SIEM capabilities will be enhanced to better identify threat-related terminology, dashboard visualization, and data storage functionality.

- The implementation of automation will also help security teams respond faster to possible incidents, performing many actions without waiting for a human response. **Security orchestration, automation, and response (SOAR)** is a collection of applications, tools, and workflows that uses automation to respond to security events. Essentially, this means that handling common security-related incidents with the use of SIEM tools is expected to become a more streamlined process requiring less manual intervention. This frees up security analysts to handle more complex and uncommon incidents that, consequently, can't be automated with a SOAR. Nevertheless, the expectation is for cybersecurity-related platforms to communicate and interact with one another. Although the technology allowing interconnected systems and devices to communicate with each other exists, it is still a work in progress.

Explore common SIEM tools

Self-hosted SIEM tools

- Self-hosted SIEM tools require organizations to install, operate, and maintain the tool using their own physical infrastructure, such as server capacity.
- These applications are then managed and maintained by the organization's IT department, rather than a third party vendor.
- Self-hosted SIEM tools are ideal when an organization is required to maintain physical control over confidential data.

Cloud-hosted SIEM tools

- Cloud-hosted SIEM tools are maintained and managed by the SIEM providers, making them accessible through the internet.
- Cloud-hosted SIEM tools are ideal for organizations that don't want to invest in creating and maintaining their own infrastructure.

Hybrid solution

- An organization can choose to use a combination of both self-hosted and cloud-hosted SIEM tools, known as a hybrid solution.
- Organizations might choose a hybrid SIEM solution to leverage the benefits of the cloud while also maintaining physical control over confidential data.
- Splunk Enterprise, Splunk Cloud, and Chronicle are common SIEM tools that many organizations use to help protect their data and systems.

Splunk

- Splunk is a data analysis platform and Splunk Enterprise provides SIEM solutions.
- Splunk Enterprise is a self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time.
- Splunk Cloud is a cloud-hosted tool used to collect, search, and monitor log data.
- Splunk Cloud is helpful for organizations running hybrid or cloud-only environments, where some or all of the organization's services are in the cloud.

Google's Chronicle:

- Chronicle is a cloud-native tool designed to retain, analyze, and search data.
- Chronicle provides log monitoring, data analysis, and data collection. Like cloud-hosted tools, cloud-native tools are also fully maintained and managed by the vendor.
- But cloud-native tools are specifically designed to take full advantage of cloud computing capabilities such as availability, flexibility, and scalability.

Open-source tools

Open-source tools are often free to use and can be user friendly. The objective of open-source tools is to provide users with software that is built by the public in a collaborative way, which can result in the software being more secure. Additionally, open-source tools allow for more customization by users, resulting in a variety of new services built from the same open-source software package.
Software engineers create open-source projects to improve software and make it available for anyone to use, as long as the specified license is respected. The source code for open-source projects is readily available to users, as well as the training material that accompanies them. Having these sources readily available allows users to modify and improve project materials.

Proprietary tools

Proprietary tools are developed and owned by a person or company, and users typically pay a fee for usage and training. The owners of proprietary tools are the only ones who can access and modify the source code. This means that users generally need to wait for updates to be made to the software, and at times they might need to pay a fee for those updates. Proprietary software generally allows users to modify a limited number of features to meet individual and organizational needs. Examples of proprietary tools include Splunk® and Chronicle SIEM tools.

Common misconceptions

There is a common misconception that open-source tools are less effective and not as safe to use as proprietary tools. However, developers have been creating open-source materials for years that have become industry standards. Although it is true that threat actors have attempted to manipulate open-source tools, because these tools are open source it is actually harder for people with malicious intent to successfully cause harm. The wide exposure and immediate access to the source code by well-intentioned and informed users and professionals makes it less likely for issues to occur, because they can fix issues as soon as they're identified.

Examples of open-source tools

In security, there are many tools in use that are open-source and commonly available. Two examples are Linux and Suricata.

Linux

Linux is an open-source operating system that is widely used. It allows you to tailor the operating system to your needs using a command-line interface. An **operating system** is the interface between computer hardware and the user. It's used to communicate with the hardware of a computer and manage software applications.

There are multiple versions of Linux that exist to accomplish specific tasks. Linux and its command-line interface will be discussed in detail, later in the certificate program.

Suricata

Suricata is an open-source network analysis and threat detection software. Network analysis and threat detection software is used to inspect network traffic to identify suspicious behavior and generate network data logs. The detection software finds activity across users, computers, or Internet Protocol (IP) addresses to help uncover potential threats, risks, or vulnerabilities.

Suricata was developed by the Open Information Security Foundation (OISF). OISF is dedicated to maintaining open-source use of the Suricata project to ensure it's free and publicly available. Suricata is widely used in the public and private sector, and it integrates with many SIEM tools and other security tools. Suricata will also be discussed in greater detail later in the program.

Use SIEM tools to protect organizations

Previously, you were introduced to security information and event management (SIEM) tools and a few SIEM dashboards. You also learned about different threats, risks, and vulnerabilities an organization may experience. In this reading, you will learn more about SIEM dashboard data and how cybersecurity professionals use that data to identify a potential threat, risk, or vulnerability.

Splunk

Splunk offers different SIEM tool options: Splunk® Enterprise and Splunk® Cloud. Both allow you to review an organization's data on dashboards. This helps security professionals manage an organization's internal infrastructure by collecting, searching, monitoring, and analyzing log data from multiple sources to obtain full visibility into an organization's everyday operations.

Review the following Splunk dashboards and their purposes:

Security posture dashboard

The security posture dashboard is designed for security operations centers (SOCs). It displays the last 24 hours of an organization's notable security-related events and trends and allows security professionals to determine if security infrastructure and policies are performing as designed. Security analysts can use this dashboard to monitor and investigate potential threats in real time, such as suspicious network activity originating from a specific IP address.

Executive summary dashboard

The executive summary dashboard analyzes and monitors the overall health of the organization over time. This helps security teams improve security measures that reduce risk. Security analysts might use this dashboard to provide high-level insights to stakeholders, such as generating a summary of security incidents and trends over a specific period of time.

Incident review dashboard

The incident review dashboard allows analysts to identify suspicious patterns that can occur in the event of an incident. It assists by highlighting higher risk items that need immediate review by an analyst. This dashboard can be very helpful because it provides a visual timeline of the events leading up to an incident.

Risk analysis dashboard

The risk analysis dashboard helps analysts identify risk for each risk object (e.g., a specific user, a computer, or an IP address). It shows changes in risk-related activity or behavior, such as a user logging in outside of normal working hours or unusually high network traffic from a specific computer. A security analyst might use this dashboard to analyze the potential impact of vulnerabilities in critical assets, which helps analysts prioritize their risk mitigation efforts.

Chronicle

Chronicle is a cloud-native SIEM tool from Google that retains, analyzes, and searches log data to identify potential security threats, risks, and vulnerabilities. Chronicle allows you to collect and analyze log data according to:

- A specific asset
- A domain name
- A user
- An IP address

Chronicle provides multiple dashboards that help analysts monitor an organization’s logs, create filters and alerts, and track suspicious domain names.
Review the following Chronicle dashboards and their purposes:

Enterprise insights dashboard

The enterprise insights dashboard highlights recent alerts. It identifies suspicious domain names in logs, known as indicators of compromise (IOCs). Each result is labeled with a confidence score to indicate the likelihood of a threat. It also provides a severity level that indicates the significance of each threat to the organization. A security analyst might use this dashboard to monitor login or data access attempts related to a critical asset—like an application or system—from unusual locations or devices.

Data ingestion and health dashboard

The data ingestion and health dashboard shows the number of event logs, log sources, and success rates of data being processed into Chronicle. A security analyst might use this dashboard to ensure that log sources are correctly configured and that logs are received without error. This helps ensure that log related issues are addressed so that the security team has access to the log data they need.

IOC matches dashboard

The IOC matches dashboard indicates the top threats, risks, and vulnerabilities to the organization. Security professionals use this dashboard to observe domain names, IP addresses, and device IOCs over time in order to identify trends. This information is then used to direct the security team’s focus to the highest priority threats. For example, security analysts can use this dashboard to search for additional activity associated with an alert, such as a suspicious user login from an unusual geographic location.

Main dashboard

The main dashboard displays a high-level summary of information related to the organization’s data ingestion, alerting, and event activity over time. Security professionals can use this dashboard to access a timeline of security events—such as a spike in failed login attempts— to identify threat trends across log sources, devices, IP addresses, and physical locations.

Rule detections dashboard

The rule detections dashboard provides statistics related to incidents with the highest occurrences, severities, and detections over time. Security analysts can use this dashboard to access a list of all the alerts triggered by a specific detection rule, such as a rule designed to alert whenever a user opens a known malicious attachment from an email. Analysts then use those statistics to help manage recurring incidents and establish mitigation tactics to reduce an organization's level of risk.

User sign in overview dashboard

The user sign in overview dashboard provides information about user access behavior across the organization. Security analysts can use this dashboard to access a list of all user sign-in events to identify unusual user activity, such as a user signing in from multiple locations at the same time. This information is then used to help mitigate threats, risks, and vulnerabilities to user accounts and the organization’s applications.

Module 4 - Use PlayBooks to respond to Incidents

Phases of an incident response playbook

- A playbook is a manual that provides details about any operational action. Playbooks also clarify what tools should be used in response to a security incident. In the security field, playbooks are essential.
- Urgency, efficiency, and accuracy are necessary to quickly identify and mitigate a security threat to reduce potential risk.
- Playbooks ensure that people follow a consistent list of actions in a prescribed way, regardless of who is working on the case.
- Different types of playbooks are used. These include playbooks for incident response, security alerts, teams-specific, and product-specific purposes.

Incident response playbook:

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

An incident response playbook is a guide with six phases used to help mitigate and manage security incidents from beginning to end.

- **Preparation:**
  - Before incidents occur, mitigate potential impacts on the organization by documenting, establishing staffing plans, and educating users.
  - Organizations must prepare to mitigate the likelihood, risk, and impact of a security incident by documenting procedures, establishing staffing plans, and educating users. Preparation sets the foundation for successful incident response.
  - For example, organizations can create incident response plans and procedures that outline the roles and responsibilities of each security team member.

- ➔ **Detection and analysis:**
  - ◆ Detect and analyze events by implementing defined processes and appropriate technology.
  - ◆ The objective of this phase is to detect and analyze events using defined processes and technology. Using appropriate tools and strategies during this phase helps security analysts determine whether a breach has occurred and analyze its possible magnitude.

- ➔ **Containment:**
  - ◆ Prevent further damage and reduce immediate impact of incidents.
  - ◆ The goal of containment is to prevent further damage and reduce the immediate impact of a security incident. During this phase, security professionals take actions to contain an incident and minimize damage.
  - ◆ Containment is a high priority for organizations because it helps prevent ongoing risks to critical assets and data.

- ➔ **Eradication and recovery:**
  - ◆ Completely remove artifacts of the incident so that an organization can return to normal operations.
  - ◆ This phase involves the complete removal of an incident's artifacts so that an organization can return to normal operations. During this phase, security professionals eliminate artifacts of the incident by removing malicious code and mitigating vulnerabilities.
  - ◆ Once they've exercised due diligence, they can begin to restore the affected environment to a secure state. This is also known as IT restoration.

- ➔ **Post-incident activity:**
  - ◆ Document the incident, inform organizational leadership, and apply lessons learned.
  - ◆ This phase includes documenting the incident, informing organizational leadership, and applying lessons learned to ensure that an organization is better prepared to handle future incidents.
  - ◆ Depending on the severity of the incident, organizations can conduct a full-scale incident analysis to determine the root cause of the incident and implement various updates or improvements to enhance its overall security posture.

- ➔ **Coordination :**
  - ◆ Report incidents and share information throughout the response process, based on established standards.
  - ◆ Coordination involves reporting incidents and sharing information, throughout the incident response process, based on the organization's established standards. Coordination is important for many reasons.
  - ◆ It ensures that organizations meet compliance requirements and it allows for coordinated response and resolution.

Playbook overview

A **playbook** is a manual that provides details about any operational action. Essentially, a playbook provides a predefined and up-to-date list of steps to perform when responding to an incident.

Playbooks are accompanied by a strategy. The strategy outlines expectations of team members who are assigned a task, and some playbooks also list the individuals responsible. The outlined expectations are accompanied by a plan. The plan dictates how the specific task outlined in the playbook must be completed.

Playbooks should be treated as living documents, which means that they are frequently updated by security team members to address industry changes and new threats.

Playbooks are generally managed as a collaborative effort, since security team members have different levels of expertise.

Updates are often made if:

- A failure is identified, such as an oversight in the outlined policies and procedures, or in the playbook itself.
- There is a change in industry standards, such as changes in laws or regulatory compliance.
- The cybersecurity landscape changes due to evolving threat actor tactics and techniques.

Types of playbooks

- Playbooks sometimes cover specific incidents and vulnerabilities. These might include ransomware, vishing, business email compromise (BEC), and other attacks previously discussed. Incident and vulnerability response playbooks are very common, but they are not the only types of playbooks organizations develop.
- Each organization has a different set of playbook tools, methodologies, protocols, and procedures that they adhere to, and different individuals are involved at each step of the response process, depending on the country they are in. For example, incident notification requirements from government-imposed laws and regulations, along with compliance standards, affect the content in the playbooks. These

requirements are subject to change based on where the incident originated and the type of data affected.

Incident and vulnerability response playbooks

- Incident and vulnerability response playbooks are commonly used by entry-level cybersecurity professionals. They are developed based on the goals outlined in an organization's business continuity plan. A business continuity plan is an established path forward allowing a business to recover and continue to operate as normal, despite a disruption like a security breach.
- These two types of playbooks are similar in that they both contain predefined and up-to-date lists of steps to perform when responding to an incident. Following these steps is necessary to ensure that you, as a security professional, are adhering to legal and organizational standards and protocols. These playbooks also help minimize errors and ensure that important actions are performed within a specific timeframe.
- When an incident, threat, or vulnerability occurs or is identified, the level of risk to the organization depends on the potential damage to its assets. A basic formula for determining the level of risk is that risk equals the likelihood of a threat. For this reason, a sense of urgency is essential. Following the steps outlined in playbooks is also important if any forensic task is being carried out. Mishandling data can easily compromise forensic data, rendering it unusable.

Common steps included in incident and vulnerability playbooks include:

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery from an incident

Additional steps include performing post-incident activities, and a coordination of efforts throughout the investigation and incident and vulnerability response stages.

Resources for more information

Incident and vulnerability response playbooks are only two examples of the many playbooks that an organization uses. If you plan to work as a cybersecurity professional outside of the U.S., you may want to explore the following resources:

- United Kingdom, National Cyber Security Center (NCSC) - Incident Management
- Australian Government - Cyber Incident Response Plan
- Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) - Vulnerability Handling and related guidelines
- Government of Canada - Ransomware Playbook
- Scottish Government - Playbook Templates

Use a playbook to respond to threats, risks, or vulnerabilities

SIEM tools and how they're used alongside playbooks to reduce organizational threats, risks, and vulnerabilities.

An incident response playbook is a guide that helps security professionals mitigate issues with a heightened sense of urgency, while maintaining accuracy. Playbooks create structure, ensure compliance, and outline processes for communication and documentation.

Organizations may use different types of incident response playbooks depending on the situation. For example, an organization may have specific playbooks for addressing different types of attacks, such as ransomware, malware, distributed denial of service, and more.

- The first action in the playbook is to assess the alert. This means determining if the alert is actually valid by identifying why the alert was generated by the SIEM. This can be done by analyzing log data and related metrics.
- Next, the playbook outlines the actions and tools to use to contain the malware and reduce further damage. For example, this playbook instructs the analyst to isolate, or disconnect, the infected network system to prevent the malware from spreading into other parts of the network.
- After containing the incident, step three of the playbook describes ways to eliminate all traces of the incident and restore the affected systems back to normal operations. For example, the playbook might instruct the analyst to restore the impacted operating system, then restore the affected data using a clean backup, created before the malware outbreak.
- Finally, once the incident has been resolved, step four of the playbook instructs the analyst to perform various post-incident activities and coordination efforts with the security team. Some actions include creating a final report to communicate the security incident to stakeholders, or reporting the incident to the appropriate authorities, like the U.S. Federal Bureau of Investigations or other agencies that investigate cyber crimes.

Note that playbooks are living documents, meaning the security team will make frequent changes, updates, and improvements to address new threats and vulnerabilities. In addition, organizations learn from past security incidents to improve their security posture, refine policies and procedures, and reduce the likelihood and impact of future incidents. Then, they update their playbooks accordingly.

Playbooks and SIEM tools

Playbooks are used by cybersecurity teams in the event of an incident. Playbooks help security teams respond to incidents by ensuring that a consistent list of actions are followed in a prescribed way, regardless of who is working on the case. Playbooks can be very detailed and may include flow charts and tables to clarify what actions to take and in which order. Playbooks are also used for recovery procedures in the event of a ransomware attack. Different types of security incidents have their own playbooks that detail who should take what action and when. Playbooks are generally used alongside SIEM tools. If, for example, unusual user behavior is flagged by a SIEM tool, a playbook provides analysts with instructions about how to address the issue.

Playbooks and SOAR tools

Playbooks are also used with SOAR tools. SOAR tools are similar to SIEM tools in that they are used for threat monitoring. SOAR is a piece of software used to automate repetitive tasks generated by tools such as a SIEM or managed detection and response (MDR). For example, if a user attempts to log into their computer too many times with the wrong password, a SOAR would automatically block their account to stop a possible intrusion. Then, analysts would refer to a playbook to take steps to resolve the issue.

Terms and definitions from Course 2, Module 4

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

Playbook: A manual that provides details about any operational action

Glossary

Cybersecurity

Terms and definitions from Course 2

A

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

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

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

B

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

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

C

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

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

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

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

D

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

E

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

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

I

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

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

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

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

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

L

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

M

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

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

N

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) Special Publication (S.P.) 800-53: A unified framework for protecting the security of information systems within the U.S. federal government

O

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

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

P

Playbook: A manual that provides details about any operational action

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

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

R

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

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

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

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

S

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

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

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

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

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

SIEM tools: A software platform that collects, analyzes, and correlates security data from various sources across your IT infrastructure that helps identify and respond to security threats in real-time, investigate security incidents, and comply with security regulations

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

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

T

Threat: Any circumstance or event that can negatively impact assets

V

Vulnerability: A weakness that can be exploited by a threat