[Completed] Professional Google Cybersecurity Specialization C2/8; Play It Safe: Manage Security Risks

started at midnight of 6/3 immediatly after finishing the Cybersecurity fundamentals cert part 1 of 8 in the professional Cybersecurity cert series

- Start
  - Play It Safe: Manage Security Risks Introduction to Cert 2
  - Course 2 overview
  - Google Cybersecurity Certificate glossary
  - Welcome to week 1
- Explore the CISSP security domains

- Explore the CISSP security domains, Part 1
- Explore the CISSP security domains, Part 2
- Security domains cybersecurity analysts need to know
- Ashley: My path to cybersecurity

- Negative threats, Risks, and vournerabilities
  - Threats, risks, and vulnerabilities
  - Herbert: Manage threats, risks, and vulnerabilities
  - NIST’s Risk Management Framework
  - Manage common threats, risks, and vulnerabilities
  - Wrap-up

- Glossary terms from week 1
- more about framework and controls
  - Welcome to week 2
  - Frameworks
  - Controls
  - The relationship between frameworks and controls

- The CIA triad: Confidentiality, integrity, and availability
  - Explore the CIA triad
  - Use the CIA triad to protect organizations

- NIST frameworks and OWASP principles and security audits
  - NIST frameworks
  - OWASP security principles
  - More about OWASP security principles
  - Wajih: Stay up-to-date on the latest cybersecurity threats
  - More about security audits

- Glossary terms from week 2
- Security information and event management (SIEM) dashboards
  - Welcome to week 3
  - Logs and SIEM tools

    - SIEM dashboards
    - The future of SIEM tools
    - Parisa: The parallels of accessibility and security

- Explore security information and event management (SIEM) tools
    - Explore common SIEM tools
    - More about cybersecurity tools
    - Talya: Myths about the cybersecurity field
    - Use SIEM tools to protect organizations
    - Wrap-up

- Glossary terms from week 3
- Phases of incident response playbooks
    - Welcome to Week 4
    - Phases of an incident response playbook
    - More about playbooks
    - Zack: Incident response and the value of playbooks

- Explore incident response
    - Use a playbook to respond to threats, risks, or vulnerabilities
    - Erin: The importance of diversity of perspective on a security team
    - Playbooks, SIEM tools, and SOAR tools
    - Wrap-up

- Glossary terms from week 4
- Course wrap-up
- Glossary Cybersecurity Terms and definitions from Course 2

Start

Play It Safe: Manage Security Risks Introduction to Cert 2

My name is Ashley, and I'm a Customer Engineering Enablement Lead for Security Operation Sales at Google. I'm excited to be your instructor for this course.

Let's start by quickly reviewing what we've covered so far. Earlier, we defined security and explored some common job responsibilities for entry-level analysts. We also discussed core skills and knowledge that analysts need to develop. Then, we shared some key events like the LoveLetter and Morris attacks that led to the development and ongoing evolution of the security field. We also introduced you to frameworks, controls, and the CIA triad, which are all used to reduce risk.

In this course, we'll discuss the focus of Certified Information Systems Security Professional's, or CISSP's, eight security domains. We'll also cover security frameworks and controls in more detail, with a focus on NIST's Risk Management Framework. Additionally, we'll explore security audits, including common elements of internal audits. Then, we'll introduce some basic security tools, and you'll have a chance to explore how to use security tools to protect assets and data from threats, risks, and vulnerabilities.

Securing an organization and its assets from threats, risks, and vulnerabilities is an important step in maintaining business operations. In my experience as a security analyst, I helped respond to a severe breach that cost the organization nearly $250,000. So, I hope you're feeling motivated to continue your security journey. I know I'm excited. Let's get started!

Course 2 overview

Image update

Hello, and welcome to **Play It Safe: Manage Security Risks**, the second course in the Google Cybersecurity Certificate. You're on an exciting journey!

By the end of this course, you will develop a greater understanding of the eight Certified Information Systems Security Professional (CISSP) security domains, as well as specific security frameworks and controls. You'll also be introduced to how to use security tools and audits to help protect assets and data. These are key concepts in the cybersecurity field, and understanding them will help you keep organizations, and the people they serve, safe from threats, risks, and vulnerabilities.

Certificate program progress

The Google Cybersecurity Certificate program has eight courses. **Play It Safe: Manage Security Risks** is the second course.

Graphic illustration displays the titles of each of the eight courses, with course two highlighted.

1. **Foundations of Cybersecurity** — Explore the cybersecurity profession, including significant events that led to the development of the cybersecurity field and its continued importance to organizational operations. Learn about entry-level cybersecurity roles and responsibilities.

2. **Play It Safe: Manage Security Risks** — *(current course)* Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools.

3. **Connect and Protect: Networks and Network Security** — Gain an understanding of network-level vulnerabilities and how to secure networks.

4. **Tools of the Trade: Linux and SQL** — Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.

5. **Assets, Threats, and Vulnerabilities** — Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization’s assets from various threats, risks, and vulnerabilities.

6. **Sound the Alarm: Detection and Response** — Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents.

7. **Automate Cybersecurity Tasks with Python** — Explore the Python programming language and write code to automate cybersecurity tasks.

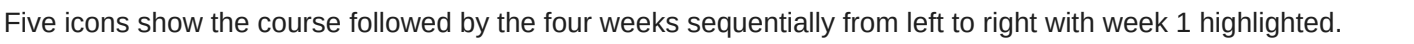
8. **Put It to Work: Prepare for Cybersecurity Jobs** — Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search.

Course 2 content

Each course of this certificate program is broken into weeks. You can complete courses at your own pace, but the weekly breakdowns are designed to help you finish the entire Google Cybersecurity Certificate in about six months.

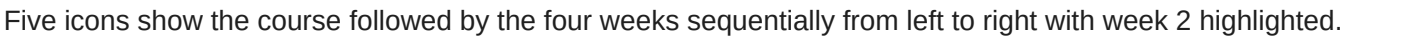
What's to come? Here's a quick overview of the skills you'll learn in each week of this course.

Week 1: Security domains



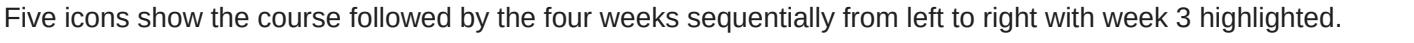
You will gain understanding of the CISSP's eight security domains. Then, you'll learn about primary threats, risks, and vulnerabilities to business operations. In addition, you'll explore the National Institute of Standards and Technology's (NIST) Risk Management Framework and the steps of risk management.

Week 2: Security frameworks and controls



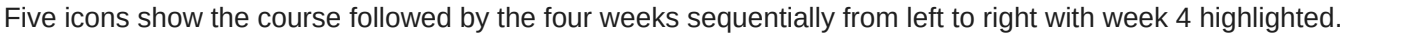
You will focus on security frameworks and controls, along with the core components of the confidentiality, integrity, and availability (CIA) triad. You'll learn about Open Web Application Security Project (OWASP) security principles and security audits.

Week 3: Introduction to cybersecurity tools



You will explore industry leading security information and event management (SIEM) tools that are used by security professionals to protect business operations. You'll learn how entry-level security analysts use SIEM dashboards as part of their every day work.

Week 4: Use playbooks to respond to incidents



You'll learn about the purposes and common uses of playbooks. You'll also explore how cybersecurity professionals use playbooks to respond to identified threats, risks, and vulnerabilities.

What to expect

Each course offers many types of learning opportunities:

- **Videos** led by Google instructors teach new concepts, introduce the use of relevant tools, offer career support, and provide inspirational personal stories.
- **Readings** build on the topics discussed in the videos, introduce related concepts, share useful resources, and describe case studies.
-

Discussion prompts explore course topics for better understanding and allow you to chat and exchange ideas with other learners in the discussion forums.

- **Self-review activities** and **labs** give you hands-on practice in applying the skills you are learning and allow you to assess your own work by comparing it to a completed example.

- **Interactive plug-ins** encourage you to practice specific tasks and help you integrate knowledge you have gained in the course.

- **In-video quizzes** help you check your comprehension as you progress through each video.

- **Practice quizzes** allow you to check your understanding of key concepts and provide valuable feedback.

- **Graded quizzes** demonstrate your understanding of the main concepts of a course. You must score 80% or higher on each graded quiz to obtain a certificate, and you can take a graded quiz multiple times to achieve a passing score.

Tips for success

- It is strongly recommended that you go through the items in each lesson in the order they appear because new information and concepts build on previous knowledge.
- Participate in all learning opportunities to gain as much knowledge and experience as possible.
- If something is confusing, don't hesitate to replay a video, review a reading, or repeat a self-review activity.
- Use the additional resources that are referenced in this course. They are designed to support your learning. You can find all of these resources in the Resources tab.
- When you encounter useful links in this course, bookmark them so you can refer to the information later for study or review.
- Understand and follow the Coursera Code of Conduct to ensure that the learning community remains a welcoming, friendly, and supportive place for all members.

Google Cybersecurity Certificate glossary

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

Welcome to week 1

The world of security, which we also refer to as cybersecurity throughout this program, is vast. So making sure that you have the knowledge, skills, and tools to successfully navigate this world is why we're here.

In the following videos, you'll learn about the focus of CISSP's eight security domains. Then, we'll discuss threats, risks, and vulnerabilities in more detail. We'll also introduce you to the three layers of the web and share some examples to help you understand the different types of attacks that we'll discuss throughout the program. Finally, we'll examine how to manage risks by using the National Institute of Standards and Technology's Risk Management Framework, known as the NIST RMF.

Because these topics and related technical skills are considered core knowledge in the security field, continuing to build your understanding of them will help you mitigate and manage the risks and threats that organizations face on a daily basis.

In the next video, we'll further discuss the focus of the eight security domains introduced in the first course.

Explore the CISSP security domains

Explore the CISSP security domains, Part 1

Welcome back! You might remember from course one that there are eight security domains, or categories, identified by CISSP. Security teams use them to organize daily tasks and identify gaps in security that could cause negative consequences for an organization, and to establish their security posture. Security posture refers to an organization's ability to manage its defense of critical assets and data and react to change.

In this video, we'll discuss the focus of the first four domains: security and risk management, asset security, security architecture and engineering, and communication and network security.

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. Let's discuss each area of focus in more detail.

By defining 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.

And finally, while 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 next 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.

Previously, 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 off. 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.

Now that we've reviewed the focus of our first four domains, let's discuss the last four domains. (Required)
en

Explore the CISSP security domains, Part 2

In this video, we'll cover the last four domains: identity and access management, security assessment and testing, security operations, and software development security.

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.

Next, let's discuss 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 and final security domain is software development security. This domain focuses on using secure coding practices. As you may remember, 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.

Being familiar with these domains can help you better understand how they're used to improve the overall security of an organization and the critical role security teams play. Next, we'll discuss security threats, risks, and vulnerabilities, including ransomware, and introduce you to the three layers of the web.

Explore the CISSP security domains

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.

Key takeaways

In this reading, you learned more about the focus areas of the eight CISSP security domains. In addition, you learned about InfoSec and the principle of least privilege. Being familiar with these security domains and related concepts will help you gain insight into the field of cybersecurity.

Ashley: My path to cybersecurity

My name is Ashley and my role at Google is CE Enablement Lead for SecOps sales. All that means is I help set up training for customer engineers that support our products. Grew up with a computer, loved the Internet. I have one of the earliest AOL screen names in history and I'm very proud of that. My dad is an engineer and I think there was always an interest in tech. But when I got out of high school, there wasn't a clear path to get there. It wasn't a linear path at all. I was a knucklehead growing up. I gave up in 10th grade and I just didn't care for a long time and I was getting in trouble a lot and I pretty much told myself if I don't join the military and get out of here, I will probably not be here in about 2-3 years if I continue down this path. I joined the army right out of high school, graduated in June, and four days later I was at bootcamp at Fort Jackson, South Carolina as a trumpet player, believe it or not, I come back and had to get a job and was not even tracking on tech jobs or anything like that. I was pulling in carts for a big hardware store, selling video games, retail, box slinger for a freight company. All of that stuff has happened before I even figured out that tech was an option. The military was kind enough to retrain me in IT, and that's kind of how I actually got the official first wave of schooling to be able to actually say, hey, I have the skills to at least be a PC technician. I went back to community college and I actually did find a cybersecurity associates degree program, worked on some certifications. I went to my first DEFCON, which is a big hacking conference, and that set off a light bulb, I think to actually get that clarity on what the path could look like. I landed my first security analyst job back in 2017 and I went to a Veterans Training Program at my last company that was free for vets and ended up getting hired out of the training. I was with that company for almost five years before I came to Google. If you're new and you're just coming in, you have to know how to work with a team. I think a lot of us learned that in customer service settings. Some of the skills I learned working in retail, dealing with hard customers, learning how to even talk to people or diffuse a situation if people are upset about things, just learning how to talk to people. In IT we need that. It's no longer just the tech skills we need, the more T-shaped which they're soft skills, there's people skills, and there's technical skills. You have to have good analysis skills, and again, it doesn't even have to be technical analysis, if you can read a book and pick apart the rhetorical devices of that story, you can do analysis work. I didn't have to be a software engineer to work in this field. For many of us, there's like a math fear, programming is a big hurdle, but we work with people, we work with processes, and you don't necessarily need to have that coding knowledge to understand people or processes. There's so many ways to break in, so do not get discouraged and don't be scared to think outside of the box to get your foot in the door.

Negative threats, Risks, and vournerabilities

Threats, risks, and vulnerabilities

As an entry-level security analyst, one of your many roles will be to handle an organization's digital and physical assets.
As a reminder,
an asset is an item perceived as having value to an organization.
During their lifespan, organizations acquire all types of assets, including physical office spaces, computers, customers' PII, intellectual property, such as patents or copyrighted data, and so much more.
Unfortunately, organizations operate in an environment that presents multiple security threats, risks, and vulnerabilities to their assets.
Let's review what threats, risks, and vulnerabilities are and discuss some common examples of each.

A threat is any circumstance or event that can negatively impact assets.
One example of a threat is a social engineering attack.
Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.
Malicious links in email messages that look like they're from legitimate companies or people is one method of social engineering known as phishing.
As a reminder, phishing is a technique that is used to acquire sensitive data, such as user names, passwords, or banking information.

Risks are different from threats.
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.
An example of a risk to an organization might be 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.

Now, let's discuss vulnerabilities.
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 include: 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.

Now that you're familiar with some of the threats, risks, and
vulnerabilities analysts frequently encounter,
coming up, we'll discuss how they impact business operations.

Herbert: Manage threats, risks, and vulnerabilities

My name is Herbert and I am a Security Engineer at Google.
I think I've always been interested in security,
in high school our school gave us these huge Dell laptops.
There wasn't a whole lot of security within those computers.
So, many of my friends would have cracked versions of like video games like Halo,
that's really where I learned how to start manipulating computers to kind of do what I want.
I guess [LAUGH] my day to day consists of analyzing security risks and
providing solutions to those risks.
A typical task for
cybersecurity analysts would usually be something like exceptions requests.
Analyzing if someone needs to have special access to a device or document
based on the role that the person has or the project that they're working on.
One of the more common threats that we come across is misconfigurations or
requesting access for something that you don't really need.
For example, I recently had a case where a vendor we
were working with had changed their OAuth scope requests.
And basically that means that they were requesting more permissions to use Google services than they had before in the past.
We weren't sure really how to go about that because that wasn't
a situation we've come across before.
So it's still ongoing, but
we're working with partner teams to kind of develop a solution for that.
I think another thing that we've seen is outdated systems,
machines that need to be patched.
That sounds like an IT issue, but it's also definitely a cybersecurity issue.
Having outdated machines, not having proper device management policies,
working with a team or many teams is a huge part of the job.
In order to get really anything done, you need to communicate with not just the team that you're a part of, but with other teams.
Ten years ago I was working at a pizza joint and ten years later,
here I am, at Google as a Security Engineer.
If I told my 16 year old self that I would be here,
I wouldn't have believed myself, but it is possible.

NIST’s Risk Management Framework

As you might remember from earlier in the program, the National Institute of Standards and Technology, NIST, provides many frameworks that are used by security professionals to manage risks, threats, and vulnerabilities.

In this video, we're going to focus on NIST's Risk Management Framework or RMF. As an entry-level analyst, you may not engage in all of these steps, but it's important to be familiar with this framework. Having a solid foundational understanding of how to mitigate and manage risks can set yourself apart from other candidates as you begin your job search in the field of security.

There are seven steps in the RMF: prepare, categorize, select, implement, assess, authorize, and monitor.

Let's start with Step one, 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.

Step two is categorize, which 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.

Step three is 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.

Step four is to 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.

Step five is 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.

Step six is 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.

Step seven is 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.

Although it may not be your job to establish these procedures, you will need to make sure they're working as intended so that risks to the organization itself, and the people it serves, are minimized.

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.

Lists that compare the top 10 most common attack types between 2017 and 2021

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.

Key takeaways

In this reading, you learned about some risk management strategies and frameworks that can be used to develop organization-wide policies and processes to mitigate threats, risks, and vulnerabilities. You also learned about some of today's most common threats, risks, and vulnerabilities to business operations. Understanding these concepts can better prepare you to not only protect against, but also mitigate, the types of security-related issues that can harm organizations and people alike.

Resources for more information

To learn more, click the linked terms in this reading. Also, consider exploring the following sites:

- OWASP Top Ten
- NIST RMF

Wrap-up

You've now completed the first section of this course! Let's review what we've discussed so far.

We started out by exploring the focus of CISSP's eight security domains. Then, we discussed threats, risks, and vulnerabilities, and how they can impact organizations. This included a close examination of ransomware and an introduction to the three layers of the web.

Finally, we focused on seven steps of the NIST Risk Management Framework, also called the RMF.

You did a fantastic job adding new knowledge to your security analyst toolkit. In upcoming videos, we'll go into more detail about some common tools used by entry-level security analysts. Then, you'll have an opportunity to analyze data generated by those tools to identify risks, threats, or vulnerabilities. You'll also have a chance to use a playbook to respond to incidents. That's all for now. Keep up the great work!

Glossary terms from week 1

Terms and definitions from Course 2, Week 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

more about framework and controls

Welcome to week 2

Welcome back! As a security analyst, your job isn't just keeping organization safe. Your role is much more important. You're also helping to keep people safe. Breaches that affect customers', vendors', and employees' data can cause significant damage to people's financial stability and their reputations. As an analyst, your day-to-day work will help keep people and organizations safe.

In this section of the course, we'll discuss security frameworks, controls, and design principles in more detail, and how they can be applied to security audits to help protect organizations and people.

Keeping customer information confidential is a crucial part of my daily work at Google. The NIST Cybersecurity Framework plays a large part in this. The framework ensures the protection and compliance of customer tools and personal work devices through the use of security controls.

Welcome to the world of security frameworks and controls. Let's get started!

Frameworks

In an organization, plans are put in place to protect against a variety of threats, risks, and vulnerabilities. However, the requirements used to protect organizations and people often overlap. Because of this, organizations use security frameworks as a starting point to create their own security policies and processes.

Let's start by quickly reviewing what frameworks are. 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.

Other security frameworks provide guidance for how to prevent, detect, and respond to security breaches. This is particularly important when trying to protect an organization from social engineering attacks like phishing that target their employees.

Remember, people are the biggest threat to security. So frameworks can be used to create plans that increase employee awareness and educate them about how they can protect the organization, their co-workers, and themselves. Educating employees about existing security challenges is essential for minimizing the possibility of a breach.

Providing employee 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. As an analyst, it will be important for you to understand and implement the plans your organization has in place to keep the organization, its employees, and the people it serves safe from social engineering attacks, breaches, and other harmful security incidents.

Coming up, we'll review and discuss security controls, which are used alongside frameworks to achieve an organization's security goals.

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.

Let's review the definition of controls. Security controls are safeguards designed to reduce specific security risks. In this video, we'll discuss 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.

Another control that can be used to protect sensitive data is authentication. 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.

Another very important security control is authorization. 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.

The security controls we discussed today are only one element of a core security model known as the CIA triad. Coming up, we'll talk more about this model and how security teams use it to protect

their organizations.

The relationship between frameworks and controls

Previously, you learned how organizations use security frameworks and controles to protect againced threads, risks, and vulnerabilities. This inclueds 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, avalability (CIA) triad. in this reading, you will further explore security frameworks, and controls and how they are used together to help mitigate organizational risk

Framework 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 Portability9 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 framework and corntrols

There are many different frameworks and controls that organizations can use to remain complient with regulations and achive their security goals. Frameworks covered in this reading are Cyber Threat Framework (CTF) and hte International Organizations for Standaridization/International Electronics Commisions (ISO/IEC) 27001. Several common security controls, used alongiside 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.

Controles
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.

Key takeaways

Cybersecurity frameworks and controls are used together to establish an organization’s security posture. They also support an organization’s ability to meet security goals and comply with laws and regulations. Although these frameworks and controls are typically voluntary, organizations are strongly encouraged to implement and use them to help ensure the safety of critical assets.

The CIA triad: Confidentiality, integrity, and availability

Explore the CIA triad

Great to see you again! 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 core security model that will help you do that.

In this video, we'll explore the CIA triad and discuss the importance of each component for keeping an organization safe from threats, risks, and vulnerabilities. Let's get started!

The CIA triad is a model that helps inform how organizations consider risk when setting up systems and security policies. As a reminder, the three letters in the CIA triad stand for confidentiality, integrity, and availability. As an entry-level analyst, you'll find yourself constantly referring to these three core principles as you work to protect your organization and the people it serves.

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.

Now that we've defined the CIA triad and its components, let's explore how you might use the CIA triad to protect an organization. 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.

As an analyst, you'll regularly use each component of the triad to help protect your organization and the people it serves. And having the CIA triad constantly in mind, will help you keep sensitive data and assets safe from a variety of threats, risks, and vulnerabilities including the social engineering attacks, malware, and data theft we discussed earlier.

Coming up, we'll explore specific frameworks and principles that will also help you protect your organization from threats, risks, and vulnerabilities. See you soon!

Use the CIA triad to protect organizations

Use the CIA triad to protect organizations

Previously, you were introduced to the confidentiality, integrity, and availability (CIA) triad and how it helps organizations consider and mitigate risk. In this reading, you will learn how cybersecurity analysts use the CIA triad in the workplace.

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. It can be used to prevent access to data, such as messages on an organization's internal chat

platform.

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.

Key takeaways

The CIA triad is essential for establishing an organization’s security posture. Knowing what it is and how it’s applied can help you better understand how security teams work to protect organizations and the people they serve.

NIST frameworks and OWASP principles and security audits

NIST frameworks

Welcome back. Before we get started, let's quickly review the purpose of frameworks. Organizations use frameworks as a starting point to develop plans that mitigate risks, threats, and vulnerabilities to sensitive data and assets. Fortunately, there are organizations worldwide that create frameworks security professionals can use to develop those plans.

In this video, we'll discuss two of 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.

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, which we'll discuss in detail in a future video. For now, we'll focus on how the CSF benefits organizations and how it can be used to protect against threats, risks, and vulnerabilities by providing a workplace 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.

As demonstrated by the previous example, 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 security controls provided by this framework are used to maintain the CIA triad for those systems used by the government. Isn't it amazing how all of these frameworks and controls work together. We've discussed some really important security topics in this video that will be very useful for you as you continue your security journey. Because they're core elements of the security profession, the NIST CSF is a useful framework that most security professionals are familiar with, and having an understanding of the NIST, SP 800-53 is crucial if you have an interest in working for the US federal government. Coming up, we'll continue to explore the five NIST CSF functions and how organizations use them to protect assets and data.

OWASP security principles

It's important to understand how to protect an organization's data and assets because that will be part of your role as a security analyst. Fortunately, there are principles and guidelines that can be used, along with NIST frameworks and the CIA triad, to help security teams minimize threats and risks.

In this video, we'll explore some Open Web Application Security Project, or OWASP, security principles that are useful to know as an entry-level analyst.

The first OWASP principle is to 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.

The principle of least privilege 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.

The next principle we'll discuss is 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.

Another principle is separation of duties, which 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.

Only two more principles to go! You're doing great. Keep security simple is the next principle. As the name suggests, 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.

The last principle is to 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.

I know we've covered a lot, but understanding these principles increases your overall security knowledge and can help you stand out as a security professional.

More about OWASP security principles

Previously, you learned that cybersecurity analysts help keep data safe and reduce risk for an organization by using a variety of security frameworks, controls, and security principles. In this reading, you will learn about more Open Web Application Security Project, recently renamed Open Worldwide Application Security Project® (OWASP), security principles and how entry-level analysts use them.

Security principles

In the workplace, security principles are embedded in your daily tasks. Whether you are analyzing logs, monitoring a security information and event (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.

Key takeaways
Cybersecurity professionals are constantly applying security principles to safeguard organizations and the people they serve. As an entry-level security analyst, you can use these security principles to promote safe development practices that reduce risks to companies and users alike.

Wajih: Stay up-to-date on the latest cybersecurity threats

My name is Wajih and I'm a security engineer at Google working in the digital forensics department. Do you need a background in cybersecurity? No you don't. My past experiences is working at a water park as a snow cone machine guy. I worked at a movie theater selling popcorn in concession stands. During my undergrad, I was a bio major at first like my freshman year. I met someone in a bus who was mentioning about this cool cybersecurity startup that just sounded really cool. Some strategies I leveraged to keep up to date on the latest cybersecurity trends is going on online forums such as Medium to research different security trends and topics. I personally use Medium a lot as I could filter by the tag of like I want to find articles related to cybersecurity and or I want to find articles related to cloud security. Based off their filtering algorithm, I just go on and see like what other people are talking about and then that's what helps me keep up to date. If it's more of like networking that you're looking forward to, then I highly recommend just going out to those like conferences. My advice for people wanting to get into cybersecurity is don't be too overwhelmed with trying to understand every single specialization within cybersecurity. There's so much going on within the cybersecurity field in terms of trends and it's nice to stay up to date with all of those but sometimes you need to take a step back and prioritize what subjects within cybersecurity you are staying most up to date like on. I love this job. I love the challenges. I feel like there is a shortage in cybersecurity professionals out there from just past experiences, hearing from other friends in computer science fields. Most of them say that oh it's too hard, too complicated to get in. Don't listen to those people. I encourage you to push through. It's definitely well worth it. First just get the fundamentals down and be persistent.

More about security audits

Previously, you were introduced to how to plan and complete an internal security audit. In this reading, you will learn more about security audits, including the goals and objectives of audits.

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

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.

Key takeaways

In this reading you learned more about security audits, including what they are; why they're conducted; and the role of frameworks, controls, and compliance in audits.

Although there is much more to learn about security audits, this introduction is meant to support your ability to complete an audit of your own for a self-reflection portfolio activity later in this course.

Resources for more information

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

- IT Security Procedural Guide: Audit and Accountability (AU) CIO-IT Security-01-08
- Assessment and Auditing Resources
- IT Disaster Recovery Plan

Glossary terms from week 2

Terms and definitions from Course 2, Week 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

Security information and event management (SIEM) dashboards

Welcome to week 3

Welcome back! Previously, we discussed security frameworks, controls, and design principles, and how security professionals apply these to security audits.

In this section, we'll continue to explore security tools and how they can help you keep organizations and the people they serve safe. Security professionals often use a variety of tools to address specific security challenges, such as collecting security data, detecting and analyzing threats, or automating tasks. Security tools help organizations achieve a more comprehensive security posture.

We'll begin by covering different types of logs, what they track, and how they're used.

Then we'll explore security information and event management, otherwise known as SIEM, dashboards. Finally, we'll discuss some common SIEM tools used in the security industry. Let's get started!

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.
As a reminder, 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.
Let's explore each of these log sources in more detail.

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.

Finally, 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.

By monitoring logs, like the one shown here,
security teams can identify
vulnerabilities and potential data breaches.
Understanding logs is important
because 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.

Later in the certificate program,
you'll have a chance to practice using
different SIEM tools to
identify potential security incidents.

Coming up, we'll explore
SIEM dashboards and how cybersecurity
professionals use them to monitor for
threats, risks, and vulnerabilities.

SIEM dashboards

We've explored how SIEM tools are used to collect and analyze log data. However, this is just one of the many ways SIEM tools are used in cybersecurity.

SIEM tools can also be used to create dashboards. You might have encountered dashboards in an app on your phone or other device. They present information about your account or location in a format that's easy to understand.

For example, weather apps display data like temperature, precipitation, wind speed, and the forecast using charts, graphs, and other visual elements. This format makes it easy to quickly identify weather patterns and trends, so you can stay prepared and plan your day accordingly.

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.

We've examined how security analysts use SIEM dashboards to help organizations maintain their security posture. Well done!

Coming up, we'll discuss some common SIEM tools used in the cybersecurity industry. Meet you there.

The future of SIEM tools

Previously, you were introduced to security information and event management (SIEM) tools, along with a few examples of SIEM tools. In this reading, you will learn more about how SIEM tools are used to protect organizational operations. You will also gain insight into how and why SIEM tools are changing to help protect organizations and the people they serve from evolving threat actor tactics and techniques.

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.

Key takeaways

SIEM tools play a major role in monitoring an organization’s data. As an entry-level security analyst, you might monitor SIEM dashboards as part of your daily tasks. Regularly researching new developments in SIEM technology will help you grow and adapt to the changes in the cybersecurity field. Cloud computing, SIEM-application integration, and automation are only some of the advancements security professionals can expect in the future evolution of SIEM tools.

Parisa: The parallels of accessibility and security

My name is Parisa and I'm a vice president of engineering and lead the Chrome Team. So as General manager of the Chrome Team, I lead a team of engineers and product managers and designers around the world who actually build Chrome and keep all of our users safe. I think accessibility is important to all aspects of technology, and when we think about its relevance for cybersecurity, you know, we ultimately want to keep everybody safe. I think of accessibility as making information, activities, or even environments meaningful, sensible, usable to as many people as possible. And when we're talking about this in a technology standpoint, it's usually about making information or services available to people with disabilities. Decisions we make based on our own abilities to enhance security can actually be ineffective. For example, you'll sometimes see the color red used for indication of a warning. Well, for somebody who's colorblind, like that is going to be ineffective. And so really thinking about accessibility when we're trying to keep people safe is super important for them to be effective. I've worked in the space of security for a really long time. And I do see some parallels between the spaces. I've really been able to see innovation driven when you're trying to solve a very specific security problem or a specific accessibility problem. Closed Captioning was originally designed and built to help people with hearing impairments, but it ends up helping everybody. For people who are new to the field of cybersecurity, it's just really important to remember that there's a range of abilities that you are wanting to serve. It's so important to get user research and feedback and a range of abilities in terms of testing the effectiveness of your security mitigations. I know it was scary for me early on. I didn't look like everybody else. I really struggled with whether I belonged. Finding people who could be mentors, having the courage to ask questions and recognize that you're rarely the only person with that question. And just sort of persevering through, sometimes hard moments can lead to breakthroughs and also just growing confidence. And one of the things I've learned is me having a different background than other people in this space was my own superpower. Instead of focusing on the delta between what I was and what the norm was in the room, I should feel a lot of pride in what made me unique and what unique skills and perspective I brought to the table.

Explore security information and event management (SIEM) tools

Explore common SIEM tools

Hello again! Previously, we discussed how SIEM tools help security analysts monitor systems and detect security threats.

In this video, we'll cover some industry leading SIEM tools that you'll likely encounter as a security analyst. First, let's discuss the different types of SIEM tools that organizations can choose from, based on their unique security needs.

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.

Alternatively, 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.

Or, 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. Let's begin by discussing 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.

Finally, there's 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.

Because threat actors are frequently improving their strategies to compromise the confidentiality, integrity, and availability of their targets, it's important for organizations to use a variety of security tools to help defend against attacks. The SIEM tools we just discussed are only a few examples of the tools available for security teams to use to help defend their organizations. And later in the

certificate program, you'll have the exciting opportunity to practice using Splunk Cloud and Chronicle.

More about cybersecurity tools

Previously, you learned about several tools that are used by cybersecurity team members to monitor for and identify potential security threats, risks, and vulnerabilities. In this reading, you'll learn more about common open-source and proprietary cybersecurity tools that you may use as a cybersecurity professional.

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.

Key takeaways

Open-source tools are widely used in the cybersecurity profession. Throughout the certificate program, you will have multiple opportunities to learn about and explore both open-source and

proprietary tools in more depth.

Talya: Myths about the cybersecurity field

I'm Talia, and I'm an engineer within privacy, safety and security at Google. So there are a lot of myths in the cybersecurity space. One big one is, you must know how to code, or you must know how to hack, or you must be a math wiz. I don't know how to code, although I have learned how to read code over time. I'm not a hacker. I'm not on the red team site of security, I'm more on like the blue team. I'm not a math wiz. I definitely took the business route, but I'm not a mathematician. That wasn't really the path. A lot of my strength really lies in my ability to build relationships, learn quickly on the job, doing, conducting research, asking all the right questions. I think those have been my strongest strength. Another big myth, is that, you are required to have a cybersecurity degree. I actually went to school for business, an advanced degree is not required. Even though I did later on go back, That was my preference. You do not need to pursue that in order for you to be considered a great candidate for cybersecurity. Another big one is you work in isolation within cybersecurity. It really depends on the path that you choose. But I found that to be one of the most that couldn't be further from the truth. My biggest advice for anyone who's interested in cybersecurity is, be okay with creating your own path. The path looks different for everyone. If you were to talk to five different people, their journeys are all different. So own your journey, and identify people who can support you. Let them know that you're sitting for the certificate, and see what support that you can get as you start your journey.

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.

Key takeaways

SIEM tools provide dashboards that help security professionals organize and focus their security efforts. This is important because it allows analysts to reduce risk by identifying, analyzing, and remediating the highest priority items in a timely manner. Later in the program, you’ll have an opportunity to practice using various SIEM tool features and commands for search queries.

Wrap-up

Let's quickly review what we covered in this section of the course. We started by discussing the importance of logs and cybersecurity, and we explored different log types, like firewall, network, and server logs. Next, we explored SIEM dashboards and how they use visual representations to provide security teams with quick and clear insights into the security posture of an organization.

Finally, we introduced common SIEM tools used in the cybersecurity industry, including Splunk and Chronicle.

We'll be exploring even more security tools later in the program, and you'll have opportunities to practice using them. Coming up, we'll discuss playbooks and how they help security professionals respond appropriately to identify threats, risks, and vulnerabilities. Meet you there.

Glossary terms from week 3

Terms and definitions from Course 2, Week 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

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

Phases of incident response playbooks

Welcome to Week 4

Hello and welcome back.
You've reached the final section of this course!
Previously, we discussed security information and
event management, or SIEM tools, and
how they can be used to help organizations improve their security posture.

Let's continue our security journey by exploring another tool
security professionals use: playbooks.
In this section, we'll explore how playbooks help security teams respond
to threats, risks, or vulnerabilities identified by SIEM tools.

Then, we'll discuss the six phases of incident response.
Let's get started!

Phases of an incident response playbook

Previously, we discussed how SIEM tools are used to help protect an organization's critical assets and data. In this video, we'll introduce another important tool for maintaining an organization's security, known as a 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.

Here, we'll focus on a playbook that's commonly used in cybersecurity, called an 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. Let's discuss each phase.

The first phase is preparation. 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.

The second phase is detection and analysis. 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.

The third phase is containment. 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.

The fourth phase in an incident response playbook is eradication and recovery. 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.

The fifth phase is post-incident activity. 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.

The sixth and final phase in an incident response playbook is coordination. 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.

There are many ways security professionals may be alerted to an incident. You recently learned about SIEM tools and how they collect and analyze data. They use this data to detect threats and generate alerts, which can inform the security team of a potential incident. Then, when a security analyst receives a SIEM alert, they can use the appropriate playbook to guide the response process. SIEM tools and playbooks work together to provide a structured and efficient way of responding to potential security incidents.

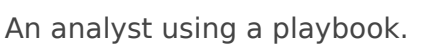
Throughout the program, you'll have opportunities to continue to build your understanding of these important concepts.

More about playbooks

Previously, you learned that playbooks are tools used by cybersecurity professionals to identify and respond to security issues. In this reading, you'll learn more about playbooks and their purpose in the field of cybersecurity.

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.



An analyst using a playbook.

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.

Key takeaways

It is essential to refine processes and procedures outlined in a playbook. With every documented incident, cybersecurity teams need to consider what was learned from the incident and what improvements should be made to handle incidents more effectively in the future. Playbooks create structure and ensure compliance with the law.

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

Zack: Incident response and the value of playbooks

My name is Zack. I'm a Software Engineer on the security team in Google Workspace. I have non-traditional background. When I graduated college, I originally thought that I would pursue law, but I was accepted and I decided not to go. Instead, I joined Google in recruiting. Through that work, I did a little bit of strategy work where I taught myself web scraping and I really liked it, so I took one of Google's internal training courses that helped me move from recruiting to software engineering. Processes and playbooks are documentation that software engineers and other people at Google use to determine how we can respond to things that happen. Whether that's a security or privacy incident, whether that's an active attack, we have sets of guidelines or algorithms that we use to determine the best course of action to make sure that we manage people's data and security well. I'm relatively new to cybersecurity. I've been a software engineer here for about two years, and I don't have enough knowledge to be able to respond to every single thing that could possibly come my way when I'm on call or when I'm helping resolve a vulnerability. The playbooks are super important to people like me and other folks who are joining the industry new because they allow you to solve the problem with the experience of a much more experienced person, basically decades of experience in your own resolution because you can rely on this playbook and other people's advice. The kind of things that we use playbooks for our open attacks, privacy incidents, data leaks, denial of service attacks, service alerts, and others. When I first started out at Google, my first task on the security team was to fix an externally reported vulnerability. That means some security researcher out in the wild was playing with our app and found something that could potentially leak our user's data. When I received that, it was my first task on the team. Looking back on it, it's a relatively easy thing to solve, but it felt really overwhelming at the time. But when we receive a vulnerability report, it comes with remediation guidance. There were steps in the bug that was sent toe saying this is the things that we think that you should do. The things that I would say to somebody who's interested in starting out in cybersecurity is talk to as many people in the industry as you can. You'll learn about what the job is like. You'll learn about the skills that you need to get yourself there. If that's something that you're interested in, you'll learn about open jobs and roles, what it's like to work at different companies. I wish people had told me when I graduated college that what these jobs are really like. I thought that coding would be heads down, typing away at a computer and a dark office for 12 hours a day. But it's not like that at all. 50% is communicating with other people and reviewing designs and talking about ideas. That's really compelling and I think if somebody had said that to me at the beginning of my career would have been totally different. Some teams come in and out of fashion, but security is ever-present. It's really important now it's only getting more important. There's a certain amount of security that comes with being in a security team. Definitely, a good place to be.

Explore incident response

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

Welcome back! In this video, we're going to revisit 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.

To start, let's discuss how a security analyst might use a playbook to address a SIEM alert, like a potential malware attack. In this situation, a playbook is invaluable for guiding an analyst through the necessary actions to properly address the alert.

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.

This is just one example of how you might follow the steps in a playbook, since organizations develop their own internal procedures for addressing security incidents. What's most important to understand is that playbooks provide a consistent process for security professionals to follow.

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.

As an entry-level security analyst, you may be required to use playbooks frequently, especially when monitoring networks and responding to incidents. Having an understanding of why playbooks are important and how they can help you achieve your working objectives will help ensure your success within this field.

Erin: The importance of diversity of perspective on a security team

Hi everyone. My name is Erin and I am a privacy engineer at Google. I work on speculative and emerging technology. So think of things that don't exist in the world, and that are coming within the next two to five years. My role is basically to take a look at all of the things that we are creating in terms of technology, and making sure that privacy is embedded in that. I am thinking for users before they even touch the product, making sure that when they utilize them, they'll have some form of trust in the engagement with that product. As well as knowing that we are protecting their privacy, things that they don't want to share or broadcast, and making sure that they're informed before they even touch the product. I always talk about soft skills being the most important thing over the technical skills. Because we can teach you anything but we can't teach you how to relate to people. That is something that you bring to the table. Diversity of thought and diversity of perspectives are very useful in understanding the world that we exist in. Because if we are designing products for everyday people, we need everyday people to basically help us understand those perspectives. Because I may look at something one way, but my colleague may see it another way based on their own experiences. And so, when you work together and come from different environments, you actually bring more equity and more depth to the things that you're looking at. And the perspective that you bring is the essential voice that is required in order to make a product better. When you look at people who work in journalism, or people who, like myself, worked in entertainment, they are bringing a different perspective for how they would tackle something. Or if we have a product where we are trying to convince a product team that maybe we shouldn't do this, it's always helpful to say, from someone who worked in journalism, do we really want this to end up in The Times? Probably not, right? And that is a way to come at people that, on the ground floor, they understand what that looks like. All of the experiences that you have had from the time you were born to now, they have been your experience. And you have to think about that in terms of where we're going with technology. When we're developing for a wide array of people, your experience may be someone else's experience. And so if we don't have you in the room, then we are missing the opportunity to actually bring something beautiful, I would say, to the equation. Which is why I encourage people, please come work with us in terms of technology. Get involved in STEM because the equity across product security, privacy, you name it, whether it be software engineering, everything requires a different voice. And it actually requires your voice.

Playbooks, SIEM tools, and SOAR tools

Playbooks and SIEM tools

Previously, you learned that security teams encounter threats, risks, vulnerabilities, and incidents on a regular basis and that they follow playbooks to address security-related issues. In this reading, you will learn more about playbooks, including how they are used in security information and event management (SIEM) and security orchestration, automation, and response (SOAR).

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.

Key takeaways

What is most important to know is that playbooks, also sometimes referred to as runbooks, provide detailed actions for security teams to take in the event of an incident. Knowing exactly who needs to do what and when can help reduce the impact of an incident and reduce the risk of damage to an organization’s critical assets

Wrap-up

Let's review what we covered in this section. We began by discussing the purpose of playbooks.

Then, we examined the six phases of an incident response playbook, including an example of how a playbook might be used to address an incident.

Playbooks are just one of the essential tools you'll use as a security analyst. They provide a structured, consistent approach to handling security incidents and can help you respond to security incidents quickly.

Knowing how and when to use a playbook, will allow you to make informed decisions about how to respond to a security incident when it occurs and help to minimize the impact and damage it may cause your organization and the people it serves.

Following the steps of the playbook and communicating appropriately with your team, will ensure your effectiveness as a security professional.

Glossary terms from week 4

Terms and definitions from Course 2, Week 4

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

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

Course wrap-up

Congratulations on completing this course! Let's recap what we've covered so far. First, we reviewed CISSP's eight security domains and focused on threats, risks, and vulnerabilities to business operations.

Then, we explored security frameworks and controls, and how they're a starting point for creating policies and processes for security management. This included a discussion of the CIA triad, NIST frameworks, and security design principles, and how they benefit the security community as a whole. This was followed by a discussion about how frameworks, controls, and principles are related to security audits.

We also explored basic security tools, such as SIEM dashboards, and how they are used to protect business operations. And finally, we covered how to protect assets and data by using playbooks.

As a security analyst, you may be working on multiple tasks at once. Understanding the tools you have at your disposal, and how to use them, will elevate your knowledge in the field while helping you successfully accomplish your everyday tasks.

Coming up next in the program, my colleague, Chris, will provide more details about topics covered in this course and introduce you to some new core security concepts. I've enjoyed sharing this journey with you.

Glossary Cybersecurity Terms and definitions from Course 2

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