Google Cybersecurity Professional Certification Notes

Glossary

Cybersecurity

Terms and definitions from the certificate

A

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

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

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

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

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

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

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

Algorithm: A set of rules used to solve a problem

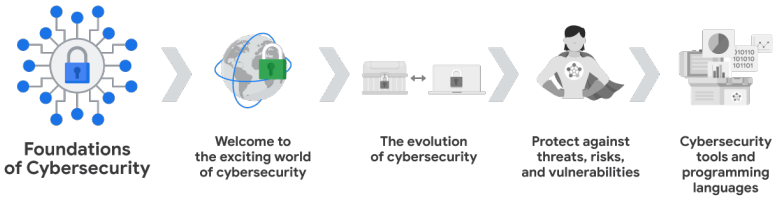
Analysis: The investigation and validation of alerts

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

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

Course 1: Foundations of Cybersecurity

Each module in this course:



Cybersecurity is the practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation.

Threat Actor is any person or group who presents a security risk.

Security protects against external and internal threats:

- **External threat** is someone outside of the organization trying to gain access to private information, networks or devices.
- **Internal threat** comes from current or former employees, external vendors, or trusted partners

Compliance is the process of adhering to internal standards and external regulations and enables organizations to avoid fines and security breaches.

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy.

Security controls are safeguards designed to reduce specific security risks. They are used with security frameworks to establish a strong security posture.

Security posture is an organization's ability to manage its defense of critical assets and data and react to change. A strong security posture leads to lower risk for the organization.

Network security is the practice of keeping an organization's network infrastructure secure from unauthorized access. This includes data, services, systems, and devices that are stored in an organization’s network.

Cloud security is the process of ensuring that assets stored in the cloud are properly configured, or set up correctly, and access to those assets is limited to authorized users. The cloud is a network made up of a collection of servers or computers that store resources and data in remote physical locations known as data centers that can be accessed via the internet. Cloud security is a growing subfield of cybersecurity that specifically focuses on the protection of data, applications, and infrastructure in the cloud.

Core skills for cybersecurity

Transferable Skills:

- Communication
- Collaboration
- Analysis
- Problem solving - recognizing attack patterns, then determining the most efficient solution to minimize risk. Don't be afraid to take risks, and try new things. Also, understand that it's rare to find a perfect solution to a problem. You’ll likely need to compromise.

Technical Skills:

- **Programming language:**
  - Python
  - SQL
- **Security Information and Event Management (SIEM) tools:** identify and analyze security threats, risks, and vulnerabilities
- **Intrusion detection systems (IDSs):** Cybersecurity analysts use IDSs to monitor system activity and alerts for possible intrusions. It’s important to become familiar with IDSs because they’re a key tool that every organization uses to protect assets and data. For example, you might use an IDS to monitor networks for signs of malicious activity, like unauthorized access to a network.
- **Threat landscape knowledge:** Being aware of current trends related to threat actors, malware, or threat methodologies is vital. This knowledge allows security teams to build stronger defenses against threat actor

tactics and techniques. By staying up to date on attack trends and patterns, security professionals are better able to recognize when new types of threats emerge such as a new ransomware variant.
- **Incident response:** Cybersecurity analysts need to be able to follow established policies and procedures to respond to incidents appropriately. For example, a security analyst might receive an alert about a possible malware attack, then follow the organization's outlined procedures to start the incident response process. This could involve conducting an investigation to identify the root issue and establishing ways to remediate it.

Importance of Cybersecurity

Security is essential for ensuring an organization's business continuity and ethical standing. There are both legal implications and moral considerations to maintaining an organization's security.

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

- **Sensitive personally identifiable information (SPII)** is a specific type of PII that falls under stricter handling guidelines and may include social security numbers, medical or financial information, and biometric data, such as facial recognition.
    - More damaging than if PII is stolen

Identity theft is the act of stealing personal information to commit fraud while impersonating a victim. And the primary objective of identity theft is financial gain.

Past cybersecurity attacks

Virus is malicious code written to interfere with computer operations and cause damage to data and software. It attaches itself to programs or documents on a computer, then spreads and infects one or more computers in a network.

viruses are more commonly referred to as **malware**: software designed to harm devices or networks.

Brain virus: intention of the virus was to track illegal copies of medical software and prevent pirated licenses

- Once a person used a pirated copy of the software, the virus-infected that computer.
- Any disk also infected, spread if anyone used infected disk
- Unintended to destroy data and productivity

Morris Worm: Designed a program to asses the size of the internet

- failed to keep track of the computers it had already compromised and continued to re-install itself until the computers ran out of memory and crashed.
- about 6,000 computers were affected, representing 10% of the internet at the time.
- Cost millions of dollars in damages due to business disruptions and effort to remove the worm.

Computer Emergency Response Teams (CERTs)

- Established to respond to computer security incidents
- Still exist today - expanded to include more responsibilities

Attacks in the digital age

LoveLetter Attack: In the year 2000, Onel De Guzman created the LoveLetter malware to steal internet login credentials.

- Attack spread rapidly and took advantage of people who had not developed a healthy suspicion for unsolicited emails.
    1. Users received an email with the subject line, "I Love You." Each email contained an attachment labeled, "Love Letter For You."
    2. When the attachment was opened, the malware scanned a user's address book.
    3. Then, sent itself to each person on the list and installed a program to collect user information and passwords.
    4. Recipients would think they were receiving an email from a friend, but it was actually malware.
- Infecting 45 million computers globally and is believed to have caused

over $10 billion dollars in damages - first example of **social engineering.**

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.

- The number of social engineering attacks is increasing with every new social media application that allows public access to people's data

One way to safeguard your organization is to **conduct regular internal trainings**, which you as a future security analyst may be asked to lead or participate in.

- common for employees to receive training on how to identify social engineering attacks. Specifically, phishing through the emails they receive.

Phishing

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

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

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

Malware

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

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

- **Viruses:** Malicious code written to interfere with computer operations and cause damage to data and software. A virus needs to be initiated by

a user (i.e., a threat actor), who transmits the virus via a malicious attachment or file download. When someone opens the malicious attachment or download, the virus hides itself in other files in the now infected system. When the infected files are opened, it allows the virus to insert its own code to damage and/or destroy data in the system.
- **Worms:** Malware that can duplicate and spread itself across systems on its own. In contrast to a virus, a worm does not need to be downloaded by a user. Instead, it self-replicates and spreads from an already infected computer to other devices on the same network.
- **Ransomware:** A malicious attack where threat actors encrypt an organization's data and demand payment to restore access.

- **Syware:** Malware that’s used to gather and sell information without consent. Spyware can be used to access devices. This allows threat actors to collect personal data, such as private emails, texts, voice and image recordings, and locations.

Social Engineering

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

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

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

Social engineering principles

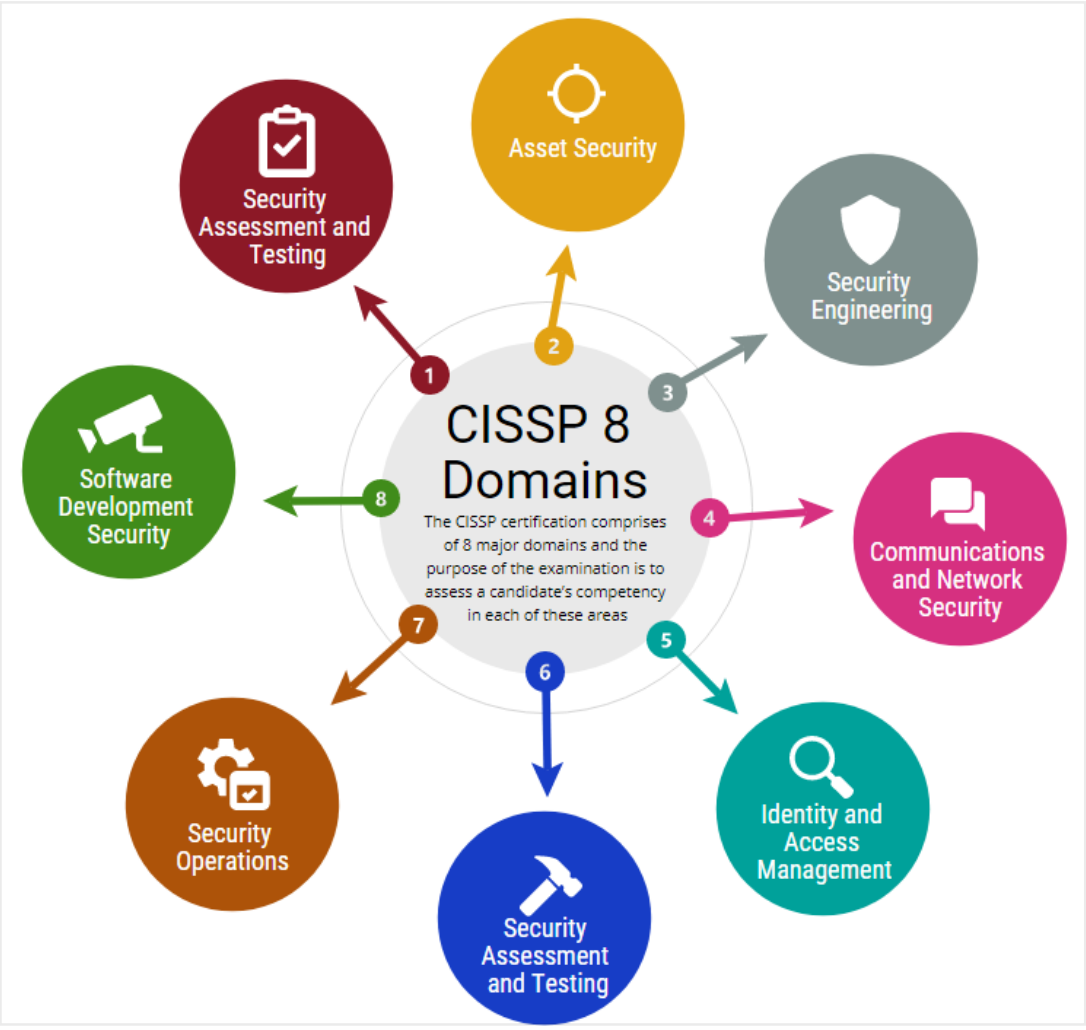
Social engineering is incredibly effective. This is because people are generally trusting and conditioned to respect authority. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Although sharing personal data—such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

Reasons why social engineering attacks are effective include:

- **Authority:** Threat actors impersonate individuals with power. This is because people, in general, have been conditioned to respect and follow authority figures.
- **Intimidation:** Threat actors use bullying tactics. This includes persuading and intimidating victims into doing what they're told.
- **Consensus/Social proof:** Because people sometimes do things that they believe many others are doing, threat actors use others' trust to pretend they are legitimate. For example, a threat actor might try to gain access to private data by telling an employee that other people at the company have given them access to that data in the past.
- **Scarcity:** A tactic used to imply that goods or services are in limited supply.
- **Familiarity:** Threat actors establish a fake emotional connection with users that can be exploited.
- **Trust:** Threat actors establish an emotional relationship with users that can be exploited *over time*. They use this relationship to develop trust and gain personal information.
- **Urgency:** A threat actor persuades others to respond quickly and without questioning.

Introduction to the eight CISSP security domains

Eight domains to organize the work of security professionals:



1. Security and Risk Management

- Security goals and objectives, risk mitigation, compliance, business continuity, and the law.

2. Asset Security

- Securing digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data.
- Security analysts may be tasked with making sure that old equipment is properly disposed of and destroyed, including any type of confidential information.

3. Security Architecture and Engineering

- Focuses on optimizing data security by ensuring effective tools, systems, and processes are in place.
- As a security analyst, you may be tasked with configuring a firewall.

    - A **firewall** is a device used to monitor and filter incoming and outgoing computer network traffic.
    - Setting up a firewall correctly helps prevent attacks that could affect productivity.

4. Communication and Network Security

- Focuses on managing and securing physical networks and wireless communications.
- As a security analyst, you may be asked to analyze user behavior within your organization.

5. Identity and Access Management

- Focuses on keeping data secure, by ensuring users follow established policies to control and manage physical assets
    - Like office spaces, and logical assets, such as networks and applications

6. Security Assessment and Testing

- Focuses on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities.
- Security analysts may conduct regular audits of user permissions, to make sure that users have the correct level of access.

7. Security Operations

- Focuses on conducting investigations and implementing preventative measures.
    - As a security analyst, you receive an alert that an unknown device has been connected to your internal network.
    - You would need to follow the organization's policies and procedures to quickly stop the potential threat.

8. Software Development Security

- Focuses on using secure coding practices, which are a set of recommended guidelines that are used to create secure applications and services.
- A set of recommended guidelines that are used to create secure applications and services.
- A security analyst may work with software development teams to ensure security practices are incorporated into the software development life-cycle.

Understand Attackers

Advanced persistent threats

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

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

Insider threats

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

- Sabotage
- Corruption
- Espionage
- Unauthorized data access or leaks

Hacktivists

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

- Demonstrations
- Propaganda
- Social change campaigns
- Fame

Hacker types

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

Introduction to security frameworks and controls

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy.

The purpose of security frameworks include:

- protecting personally identifiable information, known as PII
- securing financial information
- identifying security weaknesses
- managing organizational risks
- aligning security with business goals.

General Data Protection Regulation (GDPR): a data protection law established to grant European citizens more control over their personal data.

- A security analyst may be asked to identify and document areas where an organization is out of compliance with GDPR.

Secure Design

CIA Triad

a foundational model that helps inform how organizations consider risk when setting up systems and security policies.

CIA stands for *confidentiality, integrity, and availability*

Confidentiality

Only authorized users can access specific assets or data.

- strict access controls that define who should and should not have access to data, must be put in place to ensure confidential data remains safe.

Integrity

The data is correct, authentic, and reliable.

- security professionals can use a form of data protection like encryption to safeguard data from being tampered with.

Availability

Data is accessible to those who are authorized to access it.

Security controls are safeguards designed to reduce specific security risks.

- used alongside frameworks to ensure that security goals
- processes are implemented correctly
- organizations meet regulatory compliance requirements.

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy.
They have four core components:

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

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

Specific controls, frameworks, and compliance

National Institute of Standards and Technology (NIST) developed by the U.S. -based agency, develops a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk.

- NIST CSF, NIST RMF
- a baseline to manage short and long-term risk.

The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)
A regulation that applies to organizations that work with electricity or that are involved with the U.S. and North American power grid.

- These types of organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid.

The Federal Risk and Authorization Management Program (FedRAMP®)
A U.S. federal government program that standardizes security assessment, authorization, monitoring, and handling of cloud services and product offerings.

- Provide consistency across the government sector and third-party cloud providers.

Center for Internet Security (CIS®)
Provides a set of controls that can be used to safeguard systems and networks against attacks

- Help organizations establish a better plan of defense
- CIS also provides actionable controls that security professionals may follow if a security incident occurs.

General Data Protection Regulation (GDPR)
European Union (E.U.) general data regulation that protects the processing of E.U. residents' data and their right to privacy in and out of E.U. territory

Payment Card Industry Data Security Standard (PCI DSS)

An international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

- The objective of this compliance standard is to reduce credit card fraud.

The Health Insurance Portability and Accountability Act (HIPAA)
A U.S. federal law established in 1996 to protect patients' health information. This law prohibits patient information from being shared without their consent.
It is governed by three rules:

1. Privacy
2. Security
3. Breach notification

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

International Organization for Standardization (ISO)
Created to establish international standards related to technology, manufacturing, and management across borders.

- It helps organizations improve their processes and procedures for staff retention, planning, waste, and services.

System and Organizations Controls (SOC type 1, SOC type 2)
The American Institute of Certified Public Accountants® (AICPA) auditing standards board developed this standard. The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels such as:

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

They are used to assess an organization's financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

Ethics in cybersecurity

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

As a security professional, your job is to remain unbiased and maintain security and confidentiality.
You should never abuse the access you've been granted and entrusted with.

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

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

Common cybersecurity tools

Security information and event management tools (SIEM)

- A SIEM tool is an application that collects and analyzes log data to monitor critical activities in an organization.
- SIEM tools collect real-time, or instant, information, and allow security analysts to identify potential breaches as they happen.

  Common used SIEM tools:

  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.

  Google’s Chronicle:
  - Chronicle is a cloud-native SIEM tool that stores security data for search and analysis.

- Cloud-native means that Chronicle allows for fast delivery of new features.

Both of these SIEM tools, and SIEMs in general, collect data from multiple places, then analyze and filter that data to allow security teams to prevent and quickly react to potential security threats.

Playbook
A manual that provides details about any operational action, such as how to respond to an incident. Playbooks, which vary from one organization to the next, guide analysts in how to handle a security incident before, during, and after it has occurred.

Network protocol analyzer (packet sniffer)
A tool designed to capture and analyze data traffic within a network.
- Common network protocol analyzers include tcpdump and Wireshark.

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

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

Linux, SQL, and Python
Linux is an open-source, or publicly available, operating system. Unlike other operating systems you may be familiar with, for example MacOS or Windows, Linux relies on a command line as the primary user interface.
Structured Query Language (SQL) is a programming language used to create, interact with, and request information from a database. A database is an organized collection of information or data.

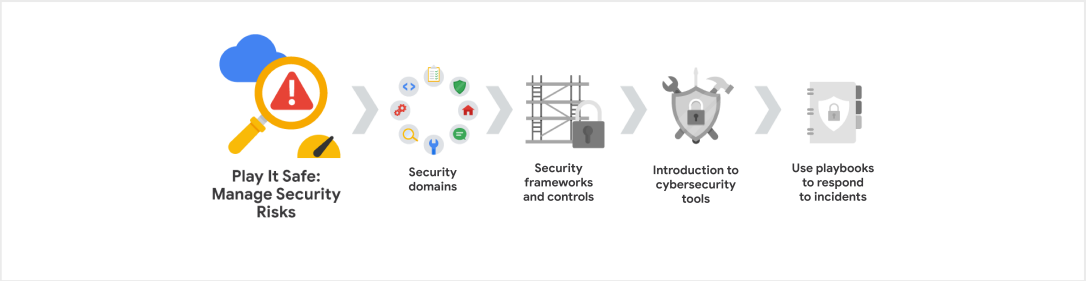
Tools to protect business operations
Web vulnerability
A **web vulnerability** is a unique flaw in a web application that a threat actor could exploit by using malicious code or behavior, to allow unauthorized access, data theft, and malware deployment.

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

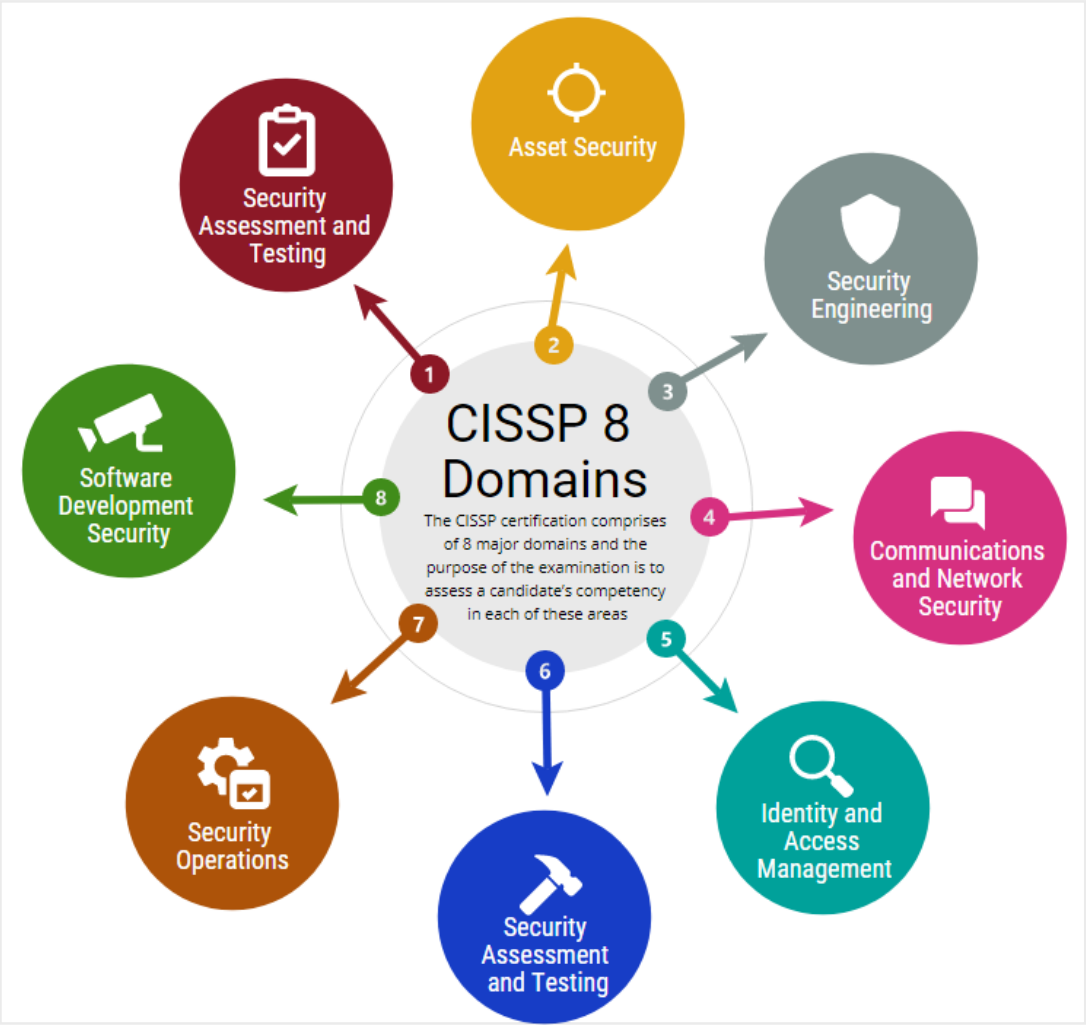
Encryption
Encryption makes data unreadable and difficult to decode for an unauthorized user; its main goal is to ensure confidentiality of private data. **Encryption** is the process of converting data from a readable format to a cryptographically encoded format. **Cryptographic encoding** means converting plaintext into secure cipher text. **Plaintext** is unencrypted information and **secure cipher text** is the result of encryption.

Portfolio projects
These opportunities include:
- Drafting a professional statement
- Conducting a security audit
- Analyzing network structure and security
- Using Linux commands to manage file permissions
- Applying filters to SQL queries
- Identifying vulnerabilities for a small business
- Documenting incidents with an incident handler's journal
- Importing and parsing a text file in a security-related scenario
- Creating or revising a resume

Course 2: Play It Safe: Manage Security Risks



CISSP security Domains (More detail)



1. Security and Risk Management

Security goals and objectives, risk mitigation, compliance, business continuity, and the law.

- **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.
- **Legal regulations**
- **Professional and organizational ethics**
- **Security goals and objectives**

2. Asset Security

Securing digital and physical assets. It's also related to the storage, maintenance,

retention, and destruction of data.
Security analysts may be tasked with making sure that old equipment is properly disposed of and destroyed, including any type of confidential information.

- 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.

3. Security Architecture and Engineering

Focuses on optimizing data security by ensuring effective tools, systems, and processes are in place.
As a security analyst, you may be tasked with configuring a firewall:

  - A firewall is a device used to monitor and filter incoming and outgoing computer network traffic.
  - Setting up a firewall correctly helps prevent attacks that could affect productivity.
- **Shared responsibility** means that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security.
- 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

4. Communication and Network Security

Focuses on managing and securing physical networks and wireless communications.
As a security analyst, you may be asked to analyze user behavior within your organization.

- **Secure networks** keep an organization's data and communications safe whether on-site, or in the cloud, or when connecting to services remotely.

5. Identity and Access Management

Focuses on keeping data secure, by ensuring users follow established policies to

control and manage physical assets like office spaces, and logical assets, such as networks and applications.
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.

6. Security Assessment and Testing

Focuses on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities.
Security analysts may conduct regular audits of user permissions, to make sure that users have the correct level of access.

- 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.

7. Security Operations

Focuses on conducting investigations and implementing preventative measures.
As a security analyst, you receive an alert that an unknown device has been connected to your internal network. You would need to follow the organization's policies and procedures to quickly stop the potential threat.

1. 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.
2. Once the threat has been neutralized, the collection of digital and physical evidence to conduct a forensic investigation will begin. This helps security teams determine areas for improvement and preventative measures that can be taken to mitigate future attacks.

   This includes using strategies, processes, and tools such as:
   - Training and awareness
   - Reporting and documentation
   - Intrusion detection and prevention
   - SIEM tools

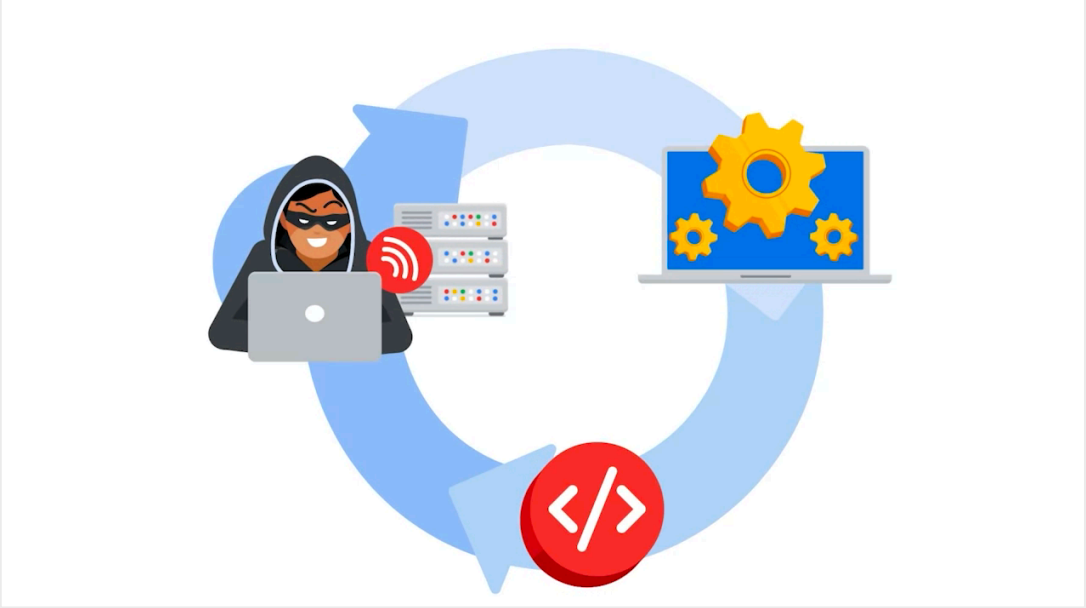
- Log management
- Incident management
- Playbooks
- Post-breach forensics
- Reflecting on lessons learned

8. Software Development Security

Focuses on using secure coding practices, which are a set of recommended guidelines that are used to create secure applications and services.

- A set of recommended guidelines that are used to create secure applications and services.
- A security analyst may work with software development teams to ensure security practices are incorporated into the software development life-cycle.

  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.



Threats, risks, vulnerabilities

A **threat** is any circumstance or event that can negatively impact assets.

A **risk** is anything that can impact the confidentiality, integrity, or availability of an asset.

A risk is the potential for loss when the threat happens.

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

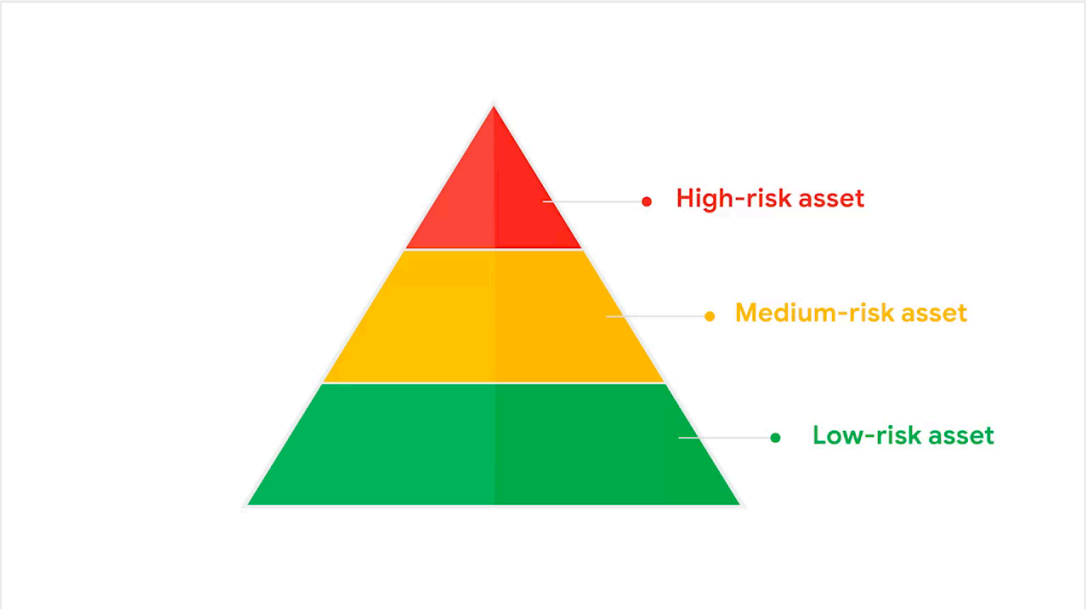
Some common strategies used to manage risks include:

- **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

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



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.

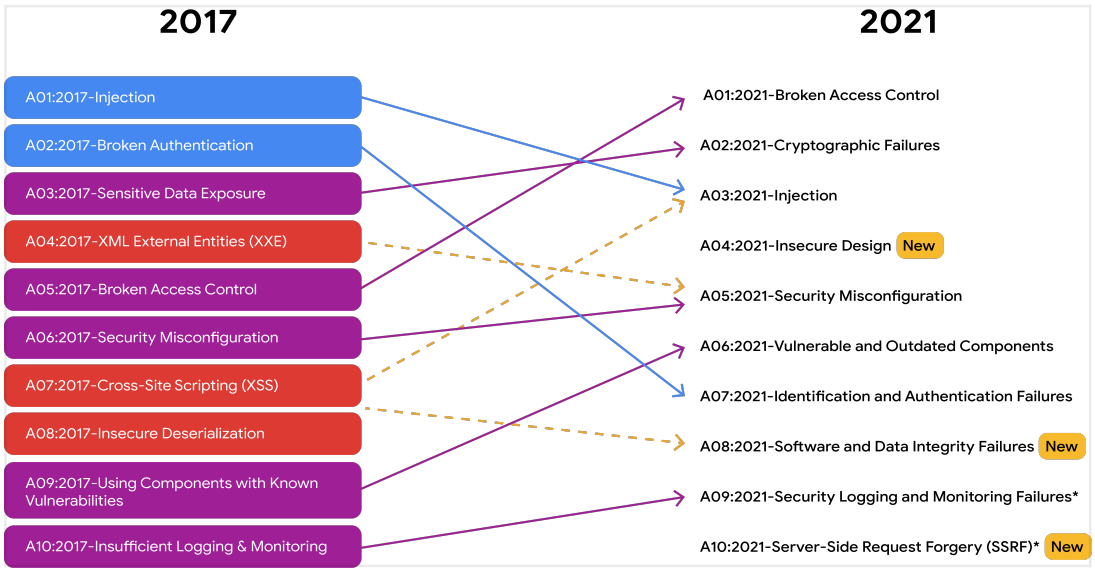
A **medium-risk asset** might include information that's not available to the public and may cause some damage to the organization's finances, reputation, or ongoing operations.

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.

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.

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.

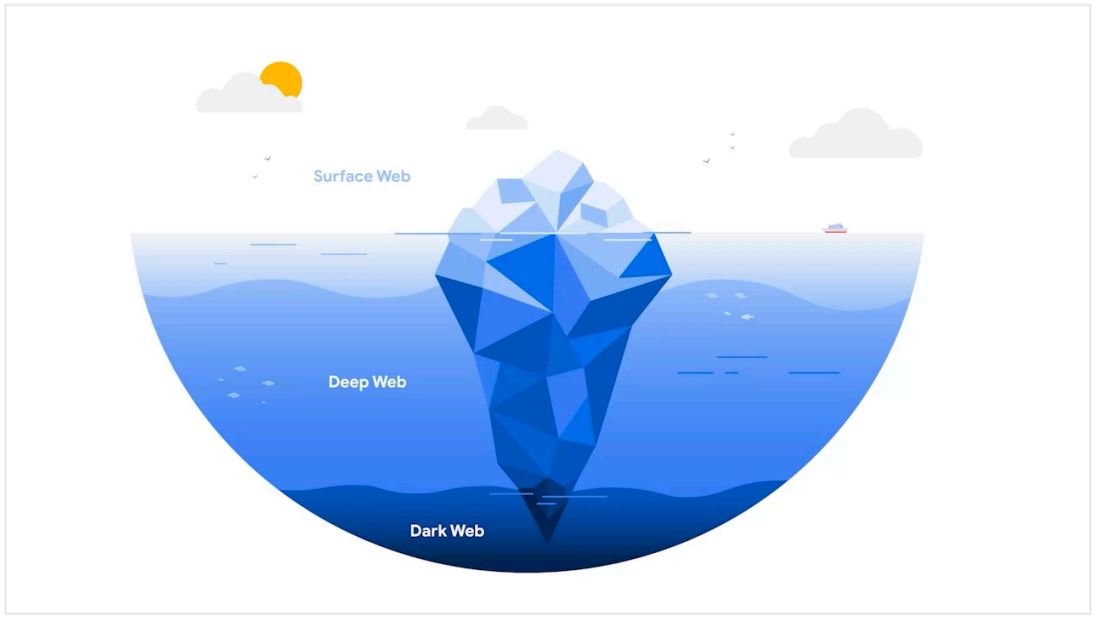


Key impacts of threats, risks, and vulnerabilities

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

- Can freeze network systems, leave devices unusable, and encrypt, or lock confidential data, making devices inaccessible.
- Ransom negotiations occur or data is leaked by threat actors, these events can occur through the dark web.

Layers of the web



Surface Web is the layer that most people use. It contains content that can be

accessed using a web browser.

Deep Web generally requires authorization to access it. An organization's intranet is an example of the deep web, since it can only be accessed by employees or others who have been granted access.

Dark web can only be accessed by using special software. The dark web generally carries a negative connotation since it is the preferred web layer for criminals because of the secrecy that it provides.

Impacts of threats, risks, and vulnerabilities.

- Financial impact
- Identity theft
- Reputation

NIST's Risk Management Framework (RMF)

There are 7 steps in the RMF:

1. Prepare

Activities that are necessary to manage security and privacy risks before a breach occurs.

- Use this step to monitor for risks and identify controls that can be used to reduce those risks.

2. Categorize

Used to develop risk management processes and tasks.

- 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.

3. Select

Choose, customize, and capture documentation of the controls that protect an organization.

- Keeping a playbook up-to-date or helping to manage other documentation that allows you and your team to address issues more efficiently.

4. Implement

Implement security and privacy plans for the organization.

- Having good plans in place is essential for minimizing the impact of ongoing security risks.

5. Asses

Determine if established controls are implemented correctly.

- Analysts identify potential weaknesses and determine whether the organization's tools, procedures, controls, and protocols should

be changed to better manage potential risks.

6. Authorize

Being accountable for the security and privacy risks that may exist in an organization.

- Could involve generating reports, developing plans of action, and establishing project milestones that are aligned to your organization's security goals.

7. Monitor

Aware of how systems are operating.

- Assessing and maintaining technical operations are tasks that analysts complete daily.

Frameworks

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy, such as social engineering attacks and ransomware.

- Include virtual and physical space
- **People are the biggest threat to security** - 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.

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.

Controls

Frameworks are used to create plans to address security risks, threats, and vulnerabilities, **controls are used to reduce specific risks.**

- Can impact financial and reputation if no controls are in place

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.

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

Three common types of controls: **encryption, authentication, and authorization.**

Encryption

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

- Encryption is used to ensure confidentiality of sensitive data, such as customers' account information or social security numbers.

Authentication

The process of verifying who someone or something is.

- Ex: logging into a website with your username and password
- More advanced methods of authentication, such as multi-factor authentication (MFA)

Biometrics

Unique physical characteristics that can be used to verify a person's identity.

- Ex: an eye scan, or a palm scan

Authorization

The concept of granting access to specific resources within a system.

- Used to verify that a person has permission to access a resource.

Specific frameworks and controls

There are many different frameworks and controls that organizations can use to remain compliant with regulations and achieve their security goals. Frameworks

covered in this reading are the Cyber Threat Framework (CTF) and the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001. Several common security controls, used alongside these types of frameworks, are also explained.

Cyber Threat Framework (CTF)

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

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

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

CIA Triad (In-Depth)

a foundational model that helps inform how organizations consider risk when setting up systems and security policies.

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.

CIA stands for *confidentiality, integrity, and availability*

Confidentiality

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.
- strict access controls that define who should and should not have access to data, must be put in place to ensure confidential data remains safe.

Integrity

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.
- security professionals can use a form of data protection like encryption to safeguard data from being tampered with.

Availability

Data is accessible to those who are authorized to access it.

- 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.

NIST Cybersecurity Framework (CSF)

A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk.

The CSF consists of five important core functions, **identify, protect, detect, respond,** and **recover**

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.

These core functions help organizations manage cybersecurity risks, implement risk management strategies, and learn from previous mistakes.

Identify

The management of cybersecurity risk and its effect on an organization's people and assets.

- monitor systems and devices in your organization's internal network

to identify potential security issues

Protect

The strategy used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats.

- You and your team might encounter new and unfamiliar threats and attacks. For this reason, studying historical data and making improvements to policies and procedures is essential.

Detect

Identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections.

- You might be asked to review a new security tool's setup to make sure it's flagging low, medium, or high risk, and then alerting the security team about any potential threats or incidents.

Respond

Making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process.

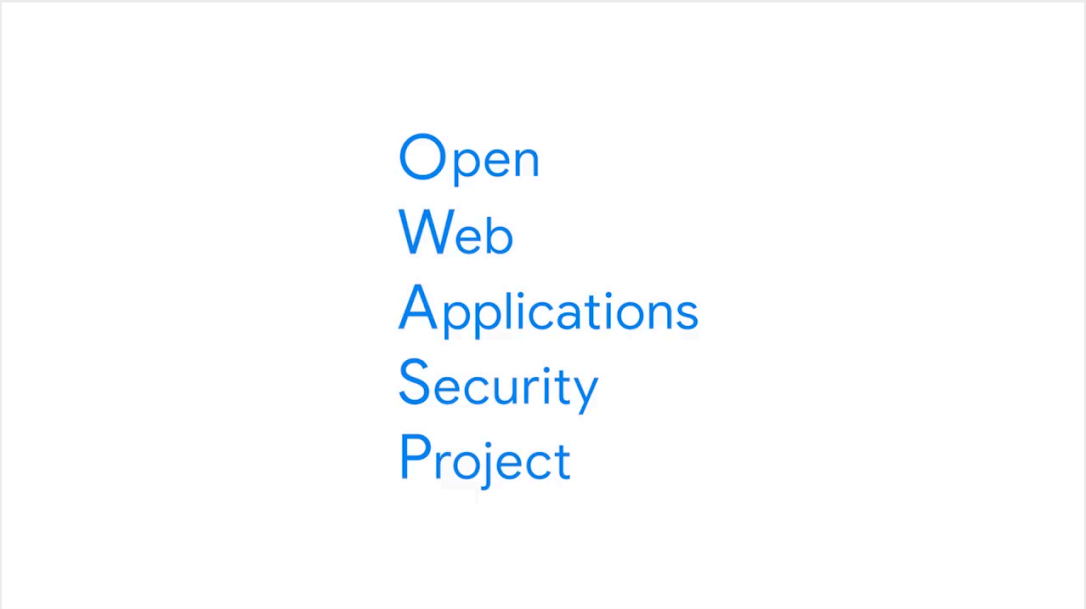
- You could be working with a team to collect and organize data to document an incident and suggest improvements to processes to prevent the incident from happening again.

Recover

The process of returning affected systems back to normal operation.

- You might work with your security team to restore systems, data, and assets, such as financial or legal files, that have been affected by an incident like a breach.

OWASP security principles



Minimize attack surface area

- All the potential vulnerabilities that a threat actor could exploit, like attack vectors, which are pathways attackers use to penetrate security defenses.
  - Ex: phishing emails and weak passwords
- Security teams might disable software features, restrict who can access certain assets, or establish more complex password requirements

Principle of least privilege

- Means making sure that users have the least amount of access required to perform their everyday tasks to reduce the amount of damage a security breach could cause
- You may have access to log data, but may not have access to change user permissions.
  - if a threat actor compromises your credentials, they'll only be able to gain limited access to digital or physical assets

Defense in depth

- An organization should have multiple security controls that address risks and threats in different ways
  - Multi-factor authentication (MFA) takes an additional step beyond simply entering their username and password to gain access to an application
  - Other controls include firewalls, intrusion detection systems, and permission settings that can be used to create multiple points of

defense, a threat actor must get through to breach an organization.

Separation of duties

- Used to prevent individuals from carrying out fraudulent or illegal activities.
- No one should be given so many privileges that they can misuse the system.
  - The person in a company who signs the paychecks shouldn't also be the person who prepares them.

Keep security simple

- When implementing security controls, unnecessarily complicated solutions should be avoided because they can become unmanageable.
  - The more complex the security controls are, the harder it is for people to work collaboratively.

Fix security issues correctly

- 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.
  - Ex: 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

Additional OWASP security principles

Four additional OWASP security principles that cybersecurity analysts and their teams use to keep organizational operations and people safe.

Establish secure defaults

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

Fail securely

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

Don’t trust services

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

Avoid security by obscurity
The security of key systems should not rely on keeping details hidden. Consider the following example from OWASP (2016):
The security of an application should not rely on keeping the source code secret. Its security should rely upon many other factors, including reasonable password policies, defense in depth, business transaction limits, solid network architecture, and fraud and audit controls.

Plan a security audit

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

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

An **internal security audit** is typically conducted by a team of people that might include an organization's compliance officer, security manager, and other security team members. They are used to help improve an organization's security posture and help organizations avoid fines from governing agencies due to a lack of compliance.

- Help security teams identify organizational risk, assess controls, and correct compliance issues.
- Great way to identify gaps within an organization.

Common elements of internal audits

Establishing the scope and goals

- **Scope** refers to the specific criteria of an internal security audit. Scope requires organizations to identify people, assets, policies, procedures, and technologies that might impact an organization's security posture
- **Goals** are an outline of the organization's security objectives, or what they want to achieve in order to improve their security posture.

Conducting a risk assessment

- Identifying potential threats, risks, and vulnerabilities - helps organizations consider what security measures should be implemented and monitored to ensure the safety of assets.

Completing a controls assessment

- Involves closely reviewing an organization's existing assets, then evaluating potential risks to those assets, to ensure internal controls and processes are effective.
    - administrative controls, technical controls, and physical controls.

Assessing compliance

- Are laws that organizations must follow to ensure private data remains secure.
    - Ex: The organization conducts business in the European Union and accepts credit card payments. So they need to adhere to the GDPR and Payment Card Industry Data Security Standard, or PCI DSS

Communicating results

- Summarizes the scope and goals of the audit - then, it lists existing risks and notes how quickly those risks need to be addressed.
- Additionally, it identifies compliance regulations the organization needs to adhere to and provides recommendations for improving the organization's security posture.

Logs and SIEM tools

a log is a record of events that occur within an organization's systems and networks.
Three common log sources include firewall logs, network logs, and server logs.

Firewall log

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.

Network log

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.

Server log
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.

SIEM tools rely on logs to monitor systems and detect security threats.
SIEM dashboards help security analysts quickly and easily access their organization's security information as charts, graphs, or tables.
SIEM dashboards also provide stakeholders with different metrics.

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

Different types of SIEM tools
Self-hosted
Require organizations to install, operate, and maintain the tool using their own physical infrastructure, such as server capacity.
- ideal when an organization is required to maintain physical control over confidential data.

Cloud-hosted
Maintained and managed by the SIEM providers
- ideal for organizations that don't want to invest in creating and maintaining their own infrastructure

Hybrid
An organization can choose to use a combination of both self-hosted and cloud-hosted SIEM tools
- Organizations might choose a hybrid SIEM solution to leverage the benefits of the cloud while also maintaining physical control over confidential data.

Splunk
A data analysis platform and Splunk Enterprise provides SIEM solutions.
- 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
Helpful for organizations running hybrid or cloud-only environments, where some or all of the organization's services are in the cloud.

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

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

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

Chronicle allows you to collect and analyze log data according to:

- A specific asset

- A domain name
- A user
- An IP address

Examples of open-source tools

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

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.

Phases of an incident response playbook

A **playbook** is a manual that provides details about any operational action. Playbooks also clarify what tools should be used in response to a security incident.

- 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.

Incident response is an organization's quick attempt to identify an attack, contain

the damage, and correct the effects of a security breach.

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

Preparation

Sets the foundation for successful incident response.

- Organizations can create incident response plans and procedures that outline the roles and responsibilities of each security team member.

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.

Containment

The goal of containment is to prevent further damage and reduce the immediate impact of a security incident

- security professionals take actions to contain an incident and minimize damage.
- Containment is a high priority for organizations because it helps prevent ongoing risks to critical assets and data.

Eradication and Recovery

Involves the complete removal of an incident's artifacts so that an organization can return to normal operations.

- 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.

Post-incident activity

Documenting the incident, informing organizational leadership, and applying lessons learned to ensure that an organization is better prepared to handle future incidents.

- Organizations can conduct a full-scale incident analysis to determine the root cause of the incident and implement various updates or improvements to enhance its overall security posture.

Coordination

Reporting incidents and sharing information, throughout the incident response process, based on the organization's established standards.

- It ensures that organizations meet compliance requirements and it allows for coordinated response and resolution.

More about Playbooks

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.

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.

Playbook to address a SIEM alert

- A playbook is invaluable for guiding an analyst through the necessary actions to properly address the alert.

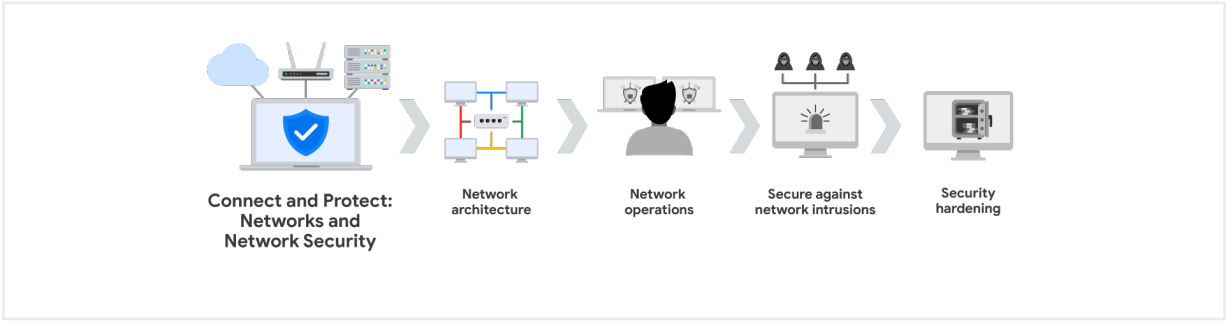
1. Asses the alert
   - Determining if the alert is actually valid by identifying why the alert was generated by the SIEM.
   - This can be done by analyzing log data and related metrics.
2. Actions and tools to use to contain the malware
   - instructs the analyst to isolate, or disconnect, the infected network system to prevent the malware from spreading into other parts of the network.
3. Ways to eliminate all traces of the incident and restore the affected systems back to normal operations.
4. Instructs the analyst to perform various post-incident activities
   - Creating a final report to communicate the security incident to stakeholders, or reporting the incident to the appropriate authorities

Playbooks provide a consistent process for security professionals to follow.

Security orchestration, automation, and response (SOAR)

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.

Course 3: Connect and Protect: Networks and Network Security



What are Networks?

A **network** is a group of connected devices. At home, the devices connected to your network might be your laptop, cell phones, and smart devices, like your refrigerator or air conditioner. In an office, devices like workstations, printers, and servers all connect to the network.

IP and MAC address

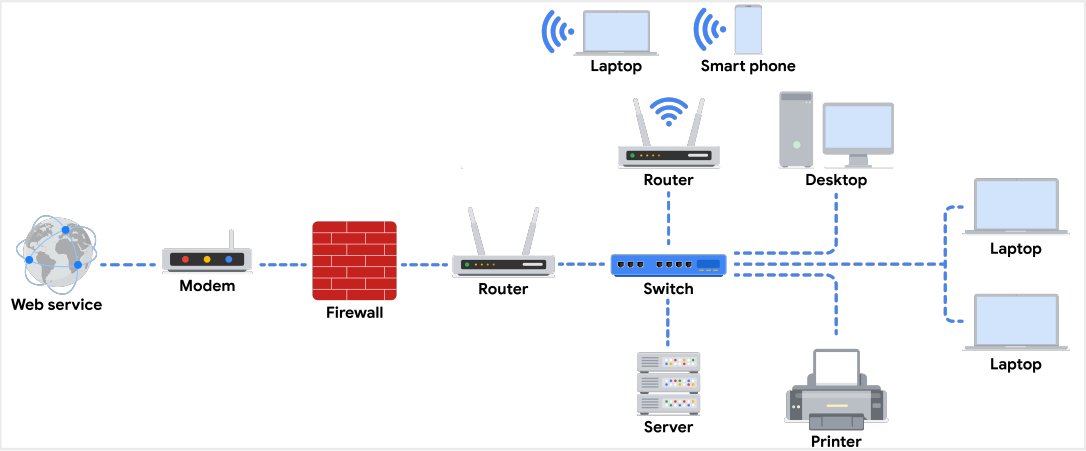
Devices need to find each other on a network to establish communications. These devices will use unique addresses, or identifiers, to locate each other. The addresses will ensure that communications happens with the right device.

Devices can communicate on two types of networks:

Local area network (LAN)
spans a small area like an office building, a school, or a home.
- when a personal device like your cell phone or tablet connects to the WIFI in your house, they form a LAN.
- The LAN then connects to the internet.

Wide area network (WAN).
spans a large geographical area like a city, state, or country.
- think of the internet as one big WAN
- An employee of a company in San Francisco can communicate and share resources with another employee in Dublin, Ireland over the WAN.

Network Tools



Hub
A **hub** is a network device that broadcasts information to every device on the network.
- like a radio tower that broadcasts a signal to any radio tuned to the correct frequency.

Hubs and switches both direct traffic on a local network. A hub is a device that provides a common point of connection for all devices directly connected to it. Hubs additionally repeat all information out to all ports. From a security perspective, this makes hubs vulnerable to eavesdropping. For this reason, hubs are not used as often on modern networks; most organizations use switches

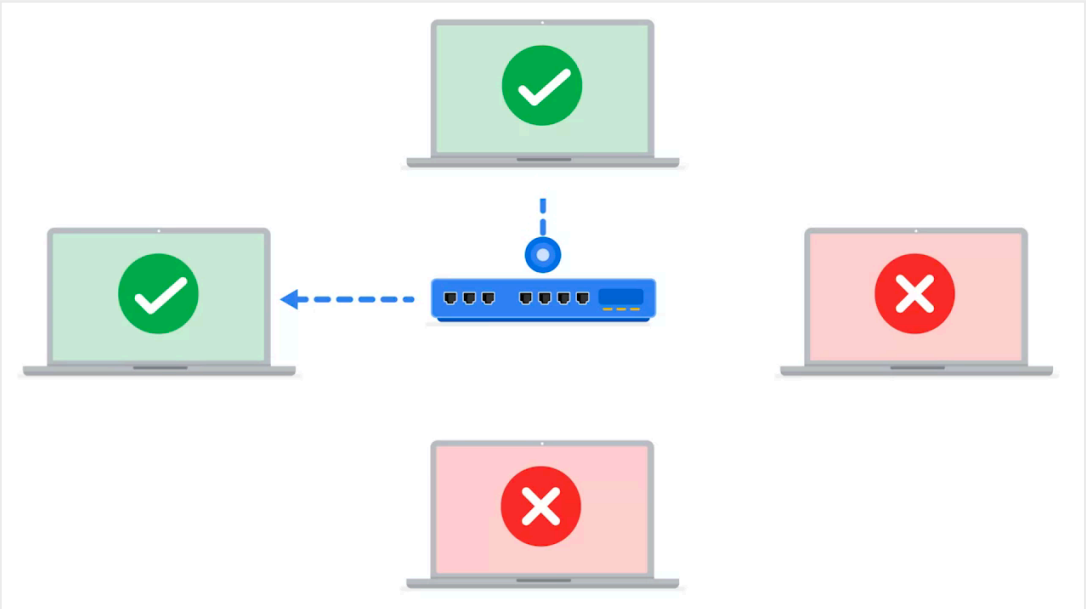
instead.

Switch

A **switch** makes connections between specific devices on a network by sending and receiving data between them.

- A switch is more intelligent than a hub.
- It only passes data to the intended destination.
- This makes switches more secure than hubs, and enables them to control the flow of traffic and improve network performance.

A switch forwards packets between devices directly connected to it. It maintains a MAC address table that matches MAC addresses of devices on the network to port numbers on the switch and forwards incoming data packets according to the destination MAC address.



Router

A **router** is a network device that connects multiple networks together.

- if a computer in one network wants to send information to a tablet on another network, then the information will be transferred as follows:
  - First, the information travels from the computer to the router.
  - Then, the router reads the destination address, and forwards the data to the intended network's router.
  - Finally, the receiving router directs that information to the tablet.

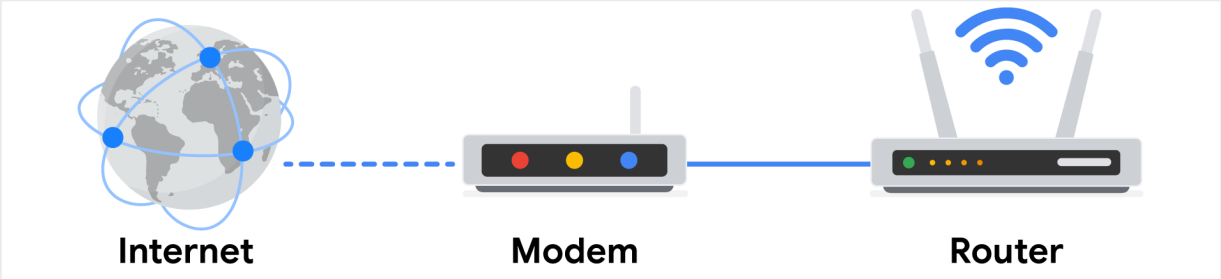
Routers sit between networks and direct traffic, based on the IP address of the destination network. The IP address of the destination network is contained in the IP header. The router reads the header information and forwards the packet to the next router on the path to the destination. This continues until the packet reaches the destination network. Routers can also include a firewall feature that allows or

blocks incoming traffic based on information in the transmission. This stops malicious traffic from entering the private network and damaging the local area network.

Modem

A **modem** is a device that connects your router to the internet, and brings internet access to the LAN.

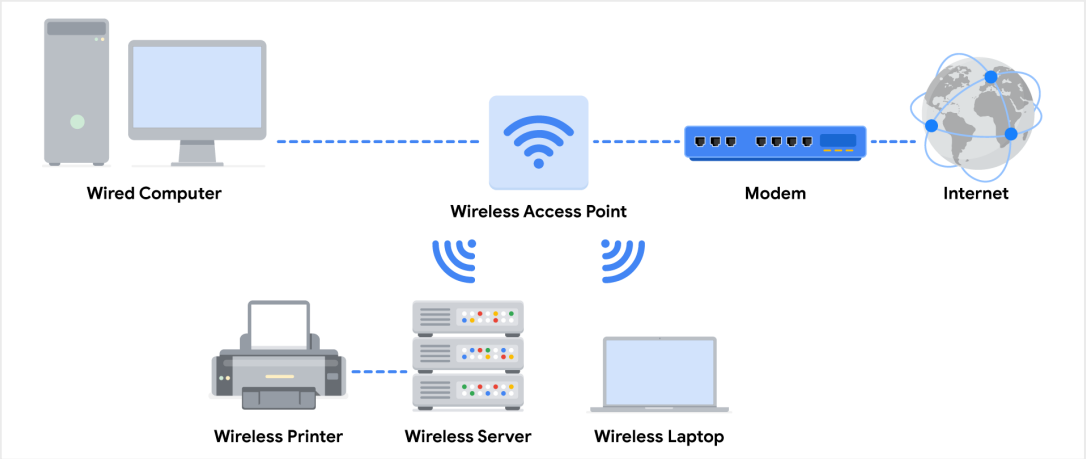
Modems receive transmissions from the internet and translate them into digital signals that can be understood by the devices on the network. Usually, modems connect to a router that takes the decoded transmissions and sends them on to the local network.



Note: Enterprise networks used by large organizations to connect their users and devices often use other broadband technologies to handle high-volume traffic, instead of using a modem.

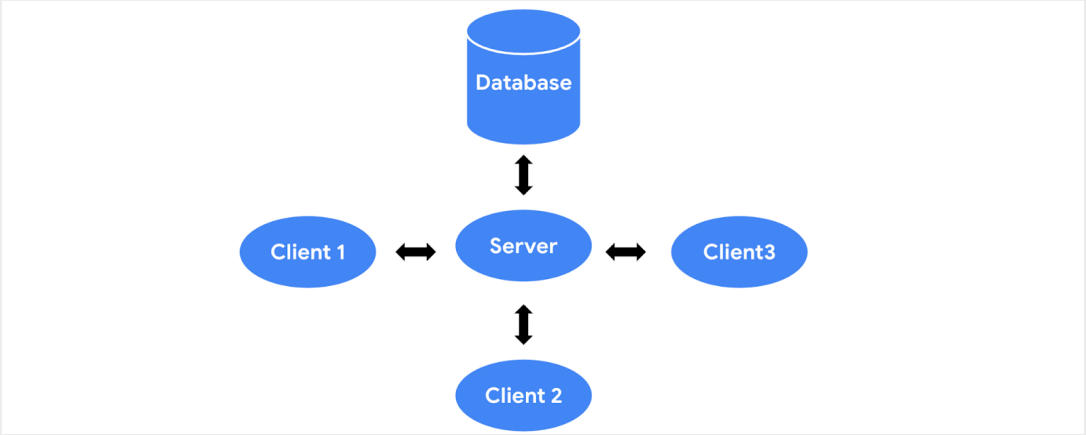
Wireless access point

A wireless access point sends and receives digital signals over radio waves creating a wireless network. Devices with wireless adapters connect to the access point using Wi-Fi. Wi-Fi refers to a set of standards that are used by network devices to communicate wirelessly. Wireless access points and the devices connected to them use Wi-Fi protocols to send data through radio waves where they are sent to routers and switches and directed along the path to their final destination.



Servers

Servers provide a service for other devices on the network. The devices that connect to a server are called clients. The following graphic outlines this model, which is called the client-server model. In this model, clients send requests to the server for information and services. The server performs the requests for the clients. Common examples include DNS servers that perform domain name lookups for internet sites, file servers that store and retrieve files from a database, and corporate mail servers that organize mail for a company.



Network diagrams are topographical maps that show the devices on the network and how they connect. Network diagrams use small representative graphics to portray each network device and dotted lines to show how each device connects to the other. Security analysts use network diagrams to learn about network architecture and how to design networks.

Cloud Networks

- a lot of companies are now using third-party providers to manage their networks.
- helps companies save money while giving them access to more network resources.

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

Cloud providers offer an alternative to traditional on-premise networks, and allow organizations to have the benefits of the traditional network without storing the devices and managing the network on their own.

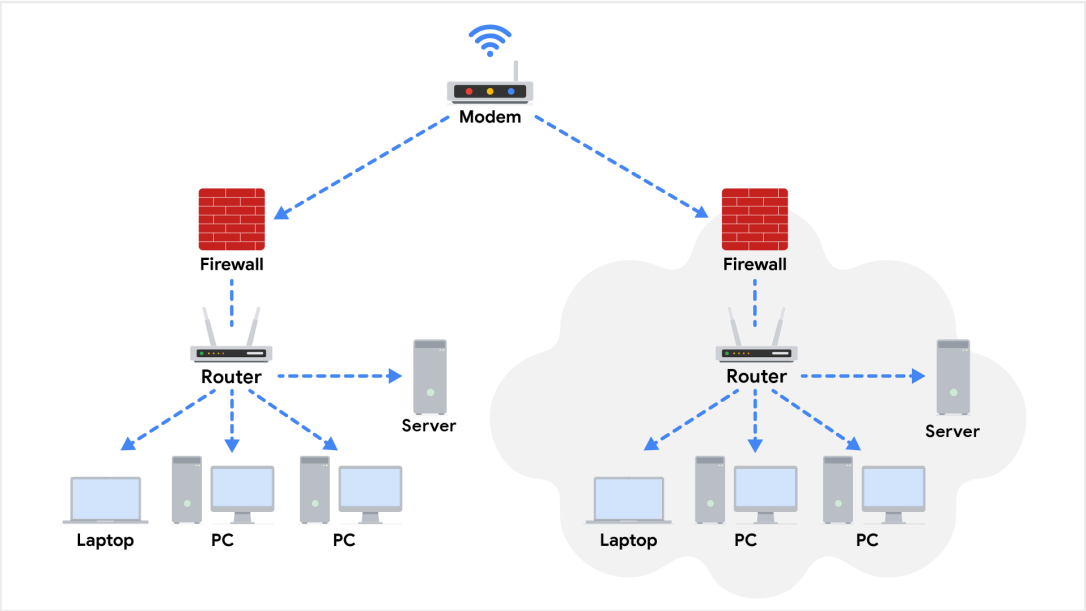
A **cloud network** is a collection of servers or computers that stores resources and data in a remote data center that can be accessed via the internet.

- Because companies don't house the servers at their physical location, these servers are referred to as being "in the cloud".

Traditional networks host web servers from a business in its physical location.

Cloud service providers offer

- provide on-demand storage and processing power that their customers only pay as needed.
- provide business and web analytics that organizations can use to monitor their web traffic and sales.



Computing process in the cloud

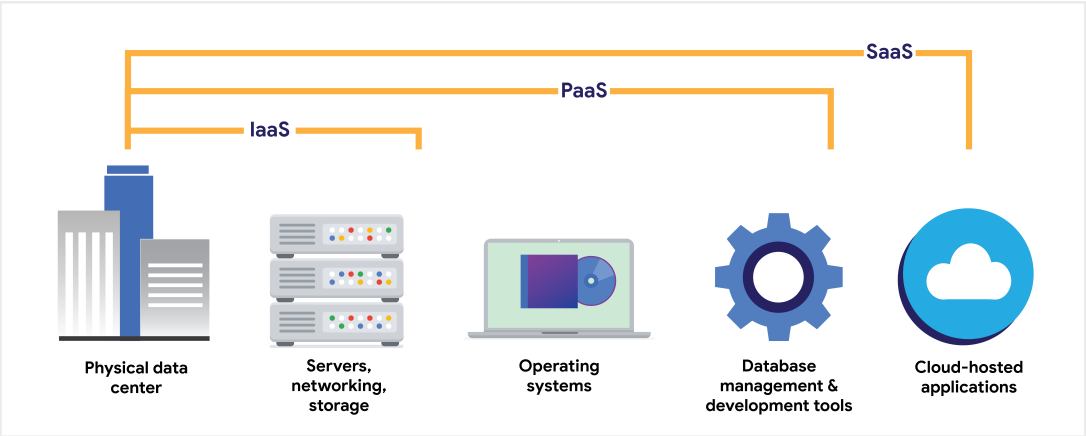
A cloud service provider (CSP) is a company that offers cloud computing services. These companies own large data centers in locations around the globe that house millions of servers. Data centers provide technology services, such as storage, and compute at such a large scale that they can sell their services to other companies for a fee. Companies can pay for the storage and services they need and consume them through the CSP's application programming interface (API) or web console.

CSPs provide three main categories of services:

- **Software as a service (SaaS)** refers to software suites operated by the CSP that a company can use remotely without hosting the software.

- **Infrastructure as a service (Iaas)** refers to the use of virtual computer components offered by the CSP. These include virtual containers and storage that are configured remotely through the CSP's API or web console. Cloud-compute and storage services can be used to operate existing applications and other technology workloads without significant modifications. Existing applications can be modified to take advantage of the availability, performance, and security features that are unique to cloud provider services.

- **Platform as a service (PaaS)** refers to tools that application developers can use to design custom applications for their company. Custom applications are designed and accessed in the cloud and used for a company's specific business needs.



Hybrid cloud environments

When organizations use a CSP's services in addition to their on-premise computers, networks, and storage, it is referred to as a hybrid cloud environment. When organizations use more than one CSP, it is called a **multi-cloud environment**. The vast majority of organizations use hybrid cloud environments to reduce costs and maintain control over network resources.

Software-defined networks

Software-defined networks (SDNs) are made up of virtual network devices and services. Many SDNs also provide virtual switches, routers, firewalls, and more. Most modern network hardware devices also support network virtualization and software-defined networking. This means that physical switches and routers use software to perform packet routing. In the case of cloud networking, the SDN tools are hosted on servers located at the CSP's data center.

Benefits of cloud computing and software-defined networks

Reliability

Reliability in cloud computing is based on how available cloud services and resources are, how secure connections are, and how often the services are effectively running. Cloud computing allows employees and customers to access the resources they need consistently and with minimal interruption.

Cost

Because CSPs have such large data centers, they are able to offer virtual devices and services at a fraction of the cost required for companies to install, patch, upgrade, and manage the components and software themselves.

Scalability

CSPs reduce this risk by making it easy to consume services in an elastic utility model as needed. This means that companies only pay for what they need when

they need it.

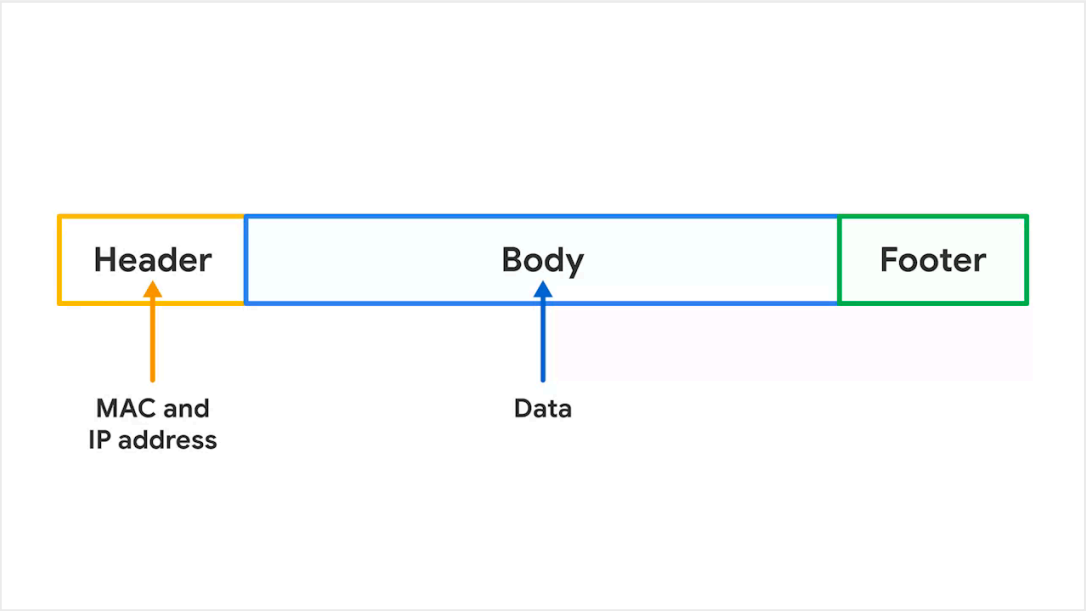
Changes can be made quickly through the CSPs, APIs, or web console—much more quickly than if network technicians had to purchase their own hardware and set it up. For example, if a company needs to protect against a threat to their network, web application firewalls (WAFs), intrusion detection/protection systems (IDS/IPS), or L3/L4 firewalls can be configured quickly whenever necessary, leading to better network performance and security.

Network Communication

Communication over a network happens when data is transferred from one point to another. Pieces of data are typically referred to as **data packets.**

A **data packet** is a basic unit of information that travels from one device to another within a network.

- When data is sent from one device to another across a network, it is sent as a packet that contains information about where the packet is going, where it's coming from, and the content of the message.



The movement of data packets across a network can provide an indication of how well the network is performing. Network performance can be measured by bandwidth.

Bandwidth refers to the amount of data a device receives every second.

- You can calculate bandwidth by dividing the quantity of data by the time in seconds.
- Speed refers to the rate at which data packets are received or

downloaded.
    - Security personnel are interested in network bandwidth and speed because if either are irregular, it could be an indication of an attack.

Packet sniffing is the practice of capturing and inspecting data packets across the network.

As a security professional, it's important that you understand the TCP/IP model because all communication on a network is organized using network protocols.

TCP/IP Model

TCP/IP is the standard model used for network communication.

Tranmission Control Protocol (TCP)

is an internet communication protocol that allows two devices to form a connection and stream data.

- The protocol includes a set of instructions to organize data, so it can be sent across a network.
- It also establishes a connection between two devices and makes sure that packets reach their appropriate destination.

User Datagram Protocol

The **User Datagram Protocol (UDP)** is a connectionless protocol that does not establish a connection between devices before transmissions. It is used by applications that are not concerned with the reliability of the transmission. Data sent over UDP is not tracked as extensively as data sent using TCP. Because UDP does not establish network connections, it is used mostly for performance sensitive applications that operate in real time, such as video streaming.

Internet Protocol (IP)

IP has a set of standards used for routing and addressing data packets as they travel between devices on a network.

- Included in the Internet Protocol (IP) is the IP address that functions as an address for each private network.

IP sends the data packets to the correct destination and relies on the Transmission Control Protocol/User Datagram Protocol (TCP/UDP) to deliver them to the corresponding service. IP packets allow communication between two networks. They are routed from the sending network to the receiving network. The TCP/UDP retransmits any data that is lost or corrupt.

When data packets are sent and received across a network, they are assigned a port.

Port

a port is a software-based location that organizes the sending and receiving of data between devices on a network.

- Ports divide network traffic into segments based on the service they will perform between two devices.
- Computers sending and receiving these data segments know how to prioritize and process these segments based on their port number.

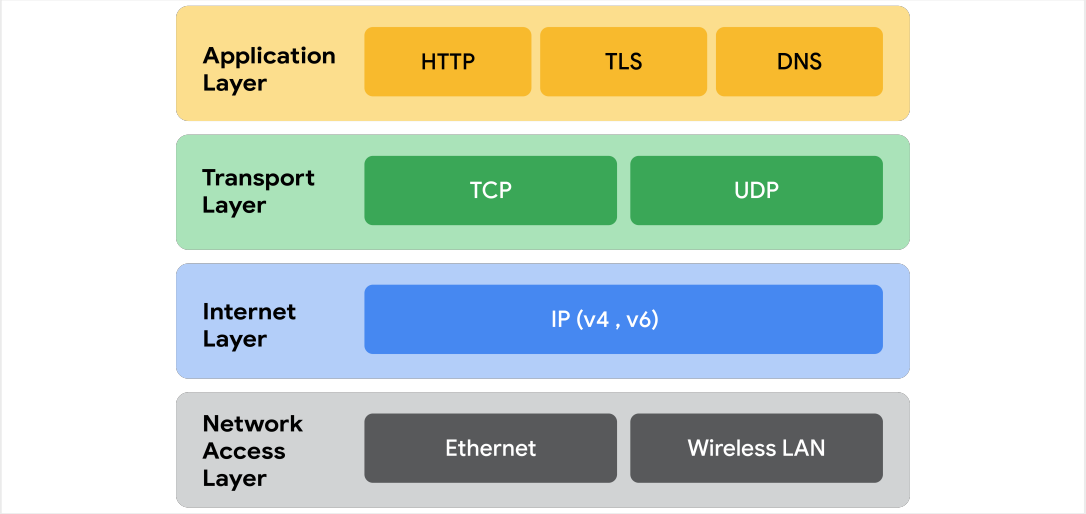
Data packets include instructions that tell the receiving device what to do with the information. These instructions come in the form of a port number.
Port numbers allow computers to split the network traffic and prioritize the operations they will perform with the data.

Port Numbers

port 25 = used for email
port 443 = used for secure internet communication
port 20 = large file transfers

The four layers of the TCP/IP model

The TCP/IP model is a framework that is used to visualize how data is organized and transmitted across the network.
Knowing how the TCP/IP model organizes network activity allows security professionals to monitor and secure against risks.



Network Access

The network access layer deals with creation of data packets and their transmission across a network.

- This includes hardware devices connected to physical cables and switches that direct data to its destination.
- . The address resolution protocol (ARP) is part of the network access layer.
    - ARP assists IP with directing data packets on the same physical network by mapping IP addresses to MAC addresses on the same physical network.

Internet

The internet layer is where IP addresses are attached to data packets to indicate the location of the sender and receiver.

- internet layer also focuses on how networks connect to each other.
- also determines which protocol is responsible for delivering the data packets and ensures the delivery to the destination host

Transport

is responsible for delivering data between two systems or networks and includes protocols to control the flow of traffic across a network.

- permit or deny communication with other devices and include information about the status of the connection.
- TCP and UDP are the two transport protocols that occur at this layer.

Application

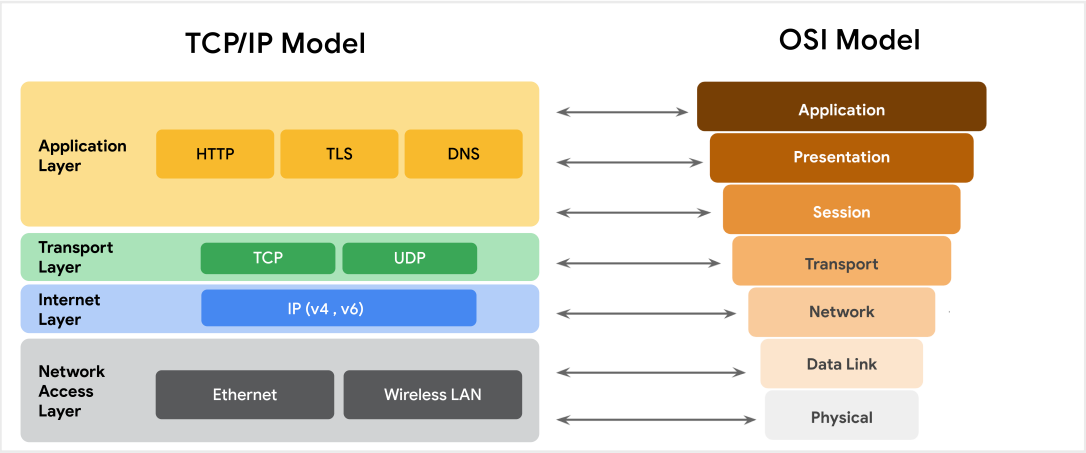
Protocols determine how the data packets will interact with receiving devices.

- Responsible for making network requests or responding to requests.
- Defines which internet services and applications any user can access.
- Functions that are organized at application layer include file transfers and email services.

Some common protocols used on this layer are:

- Hypertext transfer protocol (HTTP)
- Simple mail transfer protocol (SMTP)
- Secure shell (SSH)
- File transfer protocol (FTP)
- Domain name system (DNS)

TCP/IP model versus OSI model

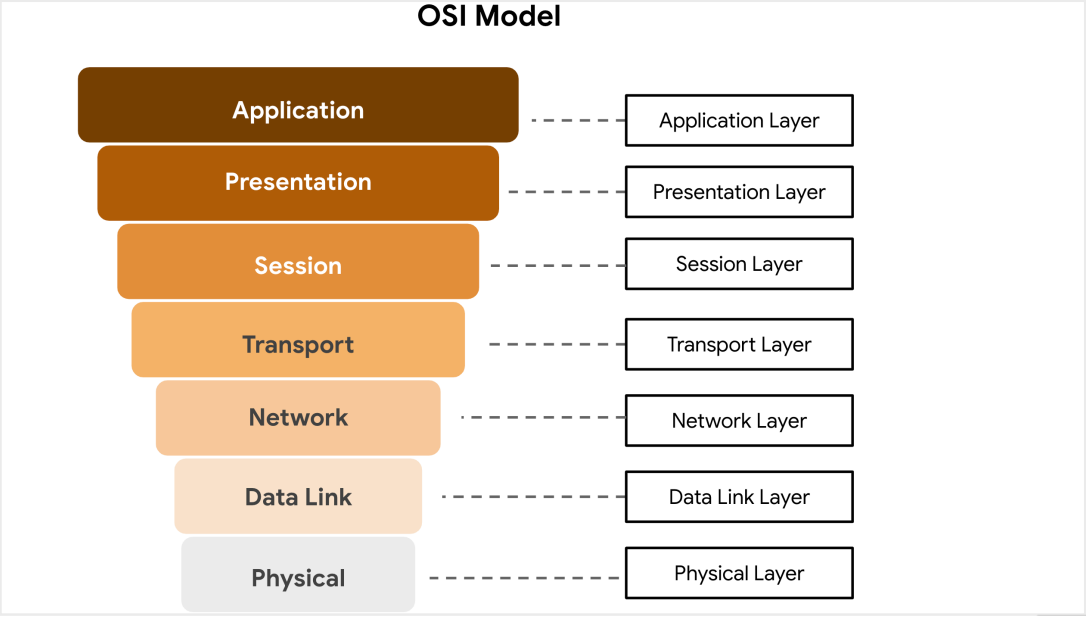


The **OSI** visually organizes network protocols into different layers. Network professionals often use this model to communicate with each other about potential sources of problems or security threats when they occur.

The TCP/IP model is a simplified version of the OSI model.

The OSI model

The **OSI model** is a standardized concept that describes the seven layers computers use to communicate and send data over the network. Network and security professionals often use this model to communicate with each other about potential sources of problems or security threats when they occur.



Layer 7: Application layer

The application layer includes processes that directly involve the everyday user. This layer includes all of the networking protocols that software applications use to connect a user to the internet. This characteristic is the identifying feature of

the application layer—user connection to the network via applications and requests.

An example of a type of communication that happens at the application layer is using a web browser. The internet browser uses HTTP or HTTPS to send and receive information from the website server. The email application uses simple mail transfer protocol (SMTP) to send and receive email information. Also, web browsers use the domain name system (DNS) protocol to translate website domain names into IP addresses which identify the web server that hosts the information for the website.

Layer 6: Presentation layer

Functions at the presentation layer involve data translation and encryption for the network. This layer adds to and replaces data with formats that can be understood by applications (layer 7) on both sending and receiving systems. Formats at the user end may be different from those of the receiving system. Processes at the presentation layer require the use of a standardized format.

Some formatting functions that occur at layer 6 include encryption, compression, and confirmation that the character code set can be interpreted on the receiving system. One example of encryption that takes place at this layer is SSL, which encrypts data between web servers and browsers as part of websites with HTTPS.

Layer 5: Session layer

A session describes when a connection is established between two devices. An open session allows the devices to communicate with each other. Session layer protocols occur to keep the session open while data is being transferred and terminate the session once the transmission is complete.

The session layer is also responsible for activities such as authentication, reconnection, and setting checkpoints during a data transfer. If a session is interrupted, checkpoints ensure that the transmission picks up at the last session checkpoint when the connection resumes. Sessions include a request and response between applications. Functions in the session layer respond to requests for service from processes in the presentation layer (layer 6) and send requests for services to the transport layer (layer 4).

Layer 4: Transport layer

The transport layer is responsible for delivering data between devices. This layer also handles the speed of data transfer, flow of the transfer, and breaking data down into smaller segments to make them easier to transport.
Segmentation is the process of dividing up a large data transmission into smaller pieces that can be processed by the receiving system. These segments need to be

reassembled at their destination so they can be processed at the session layer (layer 5). The speed and rate of the transmission also has to match the connection speed of the destination system. TCP and UDP are transport layer protocols.

Layer 3: Network layer

The network layer oversees receiving the frames from the data link layer (layer 2) and delivers them to the intended destination. The intended destination can be found based on the address that resides in the frame of the data packets. Data packets allow communication between two networks. These packets include IP addresses that tell routers where to send them. They are routed from the sending network to the receiving network.

Layer 2: Data link layer

The data link layer organizes sending and receiving data packets within a single network. The data link layer is home to switches on the local network and network interface cards on local devices.

Protocols like network control protocol (NCP), high-level data link control (HDLC), and synchronous data link control protocol (SDLC) are used at the data link layer.

Layer 1: Physical layer

As the name suggests, the physical layer corresponds to the physical hardware involved in network transmission. Hubs, modems, and the cables and wiring that connect them are all considered part of the physical layer. To travel across an ethernet or coaxial cable, a data packet needs to be translated into a stream of 0s and 1s. The stream of 0s and 1s are sent across the physical wiring and cables, received, and then passed on to higher levels of the OSI model.

IP addresses and network communication

An **internet protocol address (IP address)**, is a unique string of characters that identifies a location of a device on the internet. Each device on the internet has a unique IP address, just like every house on a street has its own mailing address.

There are two types of IP addresses:
IP addresses were all IPV4. But as the use of the internet grew, all the IPv4 addresses started to get used up, so IPv6 was developed.

IP version (IPv4)

- Ex: 19.117.63.126
- are written as four, 1, 2, or 3-digit numbers separated by a decimal point.
- Each one containing values of 0-255

IP version (IPv6)

- 2002:0db8:0000:0000:0000:ff21:0023:1234.
- IPv6 addresses are made of eight hexadecimal numbers consisting of four hexadecimal digits.
- IPv6 addresses are made up of 32 characters.

IP addresses can be either public or private.

Your internet service provider assigns a **public IP** address that is connected to your geographic location.
Just like all the roommates in one home share the same mailing address, all the devices on a network share the same public-facing IP address.

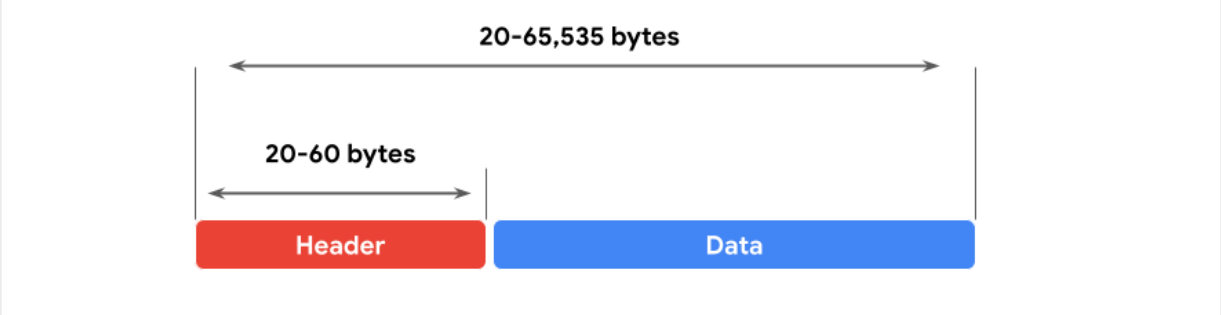
Private IP addresses are only seen by other devices on the same local network. This means that all the devices on your home network can communicate with each other using unique IP addresses that the rest of the internet can't see.

Another kind of address used in network communications is called a MAC address.

A **MAC address** is a unique alphanumeric identifier that is assigned to each physical device on a network.

All data packets include an IP address; this is referred to as an IP packet or datagram. A router uses the IP address to route packets from network to network based on information contained in the IP header of a data packet. Header information communicates more than just the address of the destination.
It also includes information such as the source IP address, the size of the packet, and which protocol will be used for the data portion of the packet.

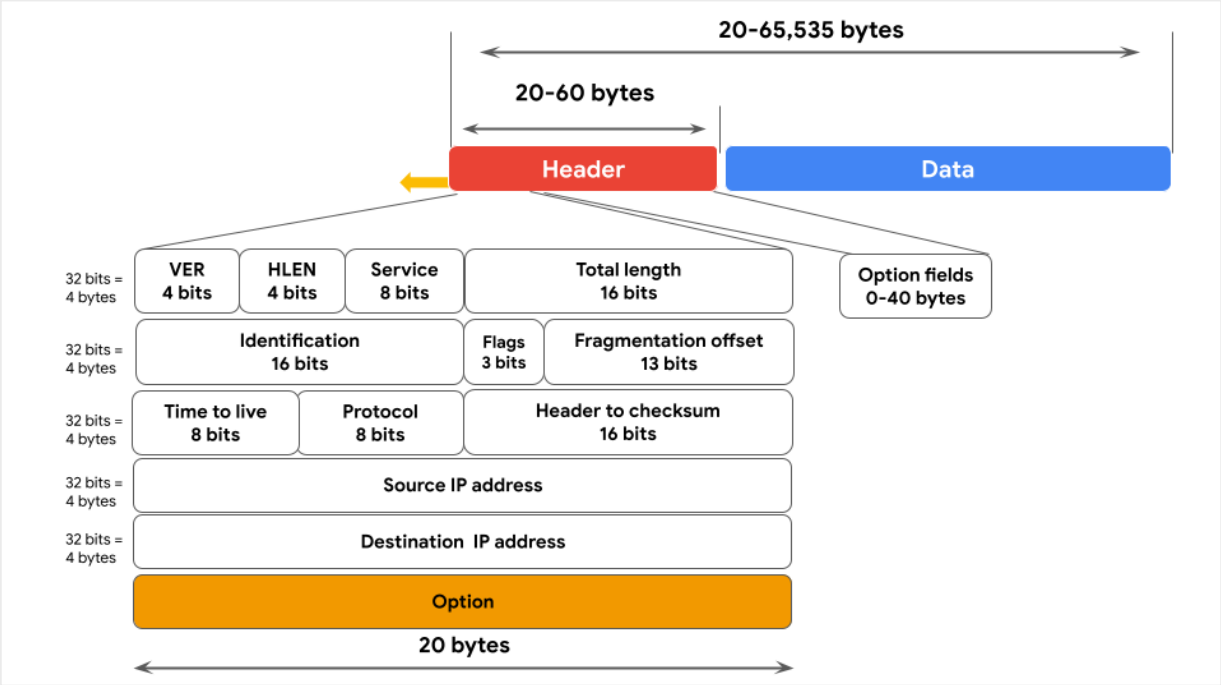
Format of an IPv4 packet



- An IPv4 header format is determined by the IPv4 protocol and includes the IP routing information that devices use to direct the packet. The size of the IPv4 header ranges from 20 to 60 bytes. The first 20 bytes are a

fixed set of information containing data such as the source and destination IP address, header length, and total length of the packet. The last set of bytes can range from 0 to 40 and consists of the options field.

- The length of the data section of an IPv4 packet can vary greatly in size. However, the maximum possible size of an IPv4 packet is 65,535 bytes. It contains the message being transferred over the internet, like website information or email text.



There are 13 fields within the header of an IPv4 packet:

- **Version (VER):** This 4 bit component tells receiving devices what protocol the packet is using. The packet used in the illustration above is an IPv4 packet.

- **IP Header Length (HLEN or IHL):** HLEN is the packet's header length. This value indicates where the packet header ends and the data segment begins.

- **Type of Service (ToS):** Routers prioritize packets for delivery to maintain quality of service on the network. The ToS field provides the router with this information.

- **Total Length:** This field communicates the total length of the entire IP packet, including the header and data. The maximum size of an IPv4 packet is 65,535 bytes.

- **Identification:** For IPv4 packets that are larger than 65, 535 bytes, the

packets are divided, or fragmented, into smaller IP packets. The identification field provides a unique identifier for all the fragments of the original IP packet so that they can be reassembled once they reach their destination.

- **Flags:** This field provides the routing device with more information about whether the original packet has been fragmented and if there are more fragments in transit.

- **Fragmentation Offset:** The fragment offset field tells routing devices where in the original packet the fragment belongs.

- **Time to Live (TTL):** TTL prevents data packets from being forwarded by routers indefinitely. It contains a counter that is set by the source. The counter is decremented by one as it passes through each router along its path. When the TTL counter reaches zero, the router currently holding the packet will discard the packet and return an ICMP Time Exceeded error message to the sender.

- **Protocol:** The protocol field tells the receiving device which protocol will be used for the data portion of the packet.

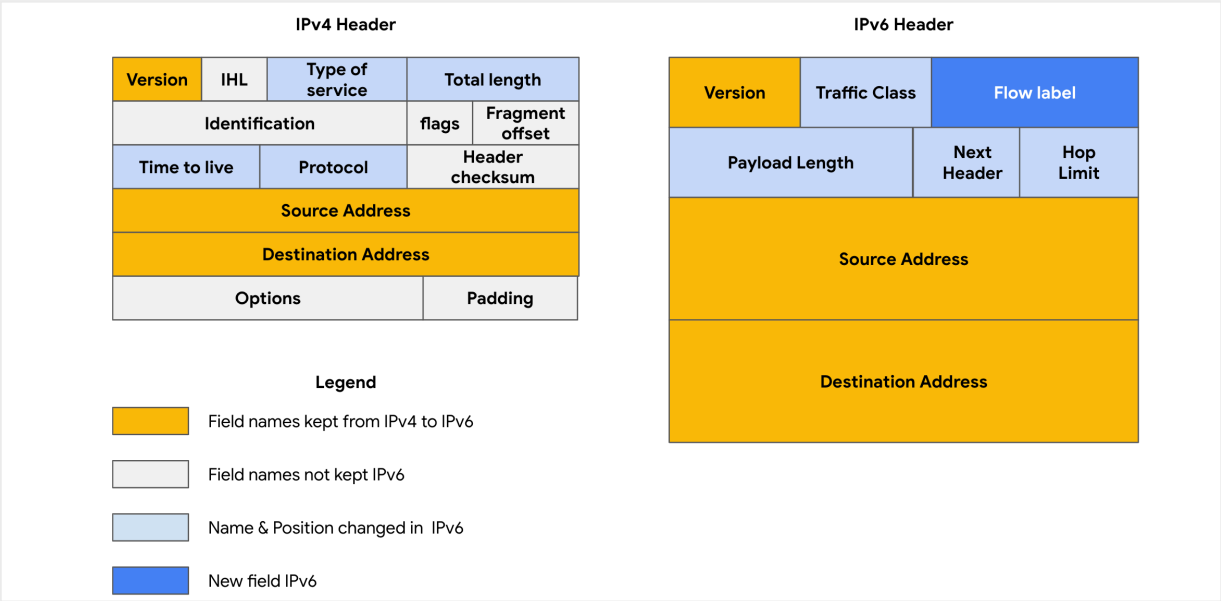
- **Header Checksum:** The header checksum field contains a checksum that can be used to detect corruption of the IP header in transit. Corrupted packets are discarded.

- **Source IP Address:** The source IP address is the IPv4 address of the sending device.

- **Destination IP Address:** The destination IP address is the IPv4 address of the destination device.

- **Options:** The options field allows for security options to be applied to the packet if the HLEN value is greater than five. The field communicates these options to the routing devices.

There are also some differences in the layout of an IPv6 packet header. The IPv6 header format is much simpler than IPv4. For example, the IPv4 Header includes the IHL, Identification, and Flags fields, whereas the IPv6 does not. The IPv6 header only introduces the Flow Label field, where the Flow Label identifies a packet as requiring special handling by other IPv6 routers.



There are some important security differences between IPv4 and IPv6. IPv6 offers more efficient routing and eliminates private address collisions that can occur on IPv4 when two devices on the same network are attempting to use the same address.

Network Protocols

are a set of rules used by two or more devices on a network to describe the order of delivery and the structure of the data.

Before you gain access to the website, your device will establish communications with a web server.
That communication uses a protocol called the **Transmission Control Protocol, or TCP**.

TCP is an internet communications protocol that allows two devices to form a connection and stream data.

- also verifies both devices before allowing any further communications to take place.

As data packets move across the network, they move between network devices such as routers.

The Address Resolution Protocol (ARP)
used to determine the MAC address of the next router or device on the path. This

ensures that the data gets to the right place.

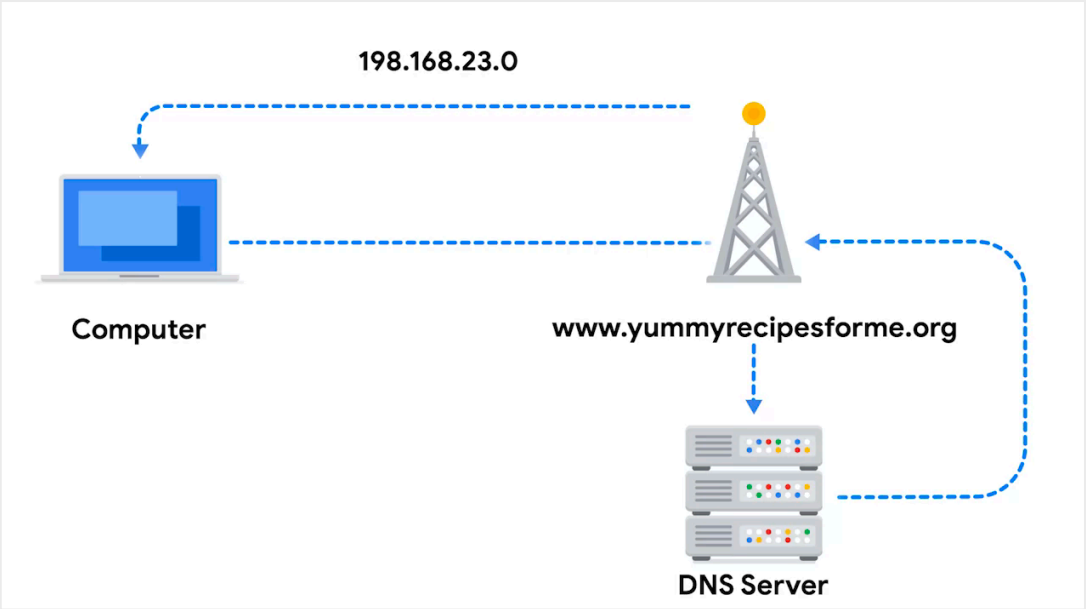
The Hypertext Transfer Protocol Secure (https) is a network protocol that provides a secure method of communication between client and website servers. It allows your web browser to securely send a request for a webpage

- HTTPS encrypts data using the Secure Sockets Layer and Transport Layer Security, otherwise known as SSL/TLS.
- This helps keep the information secure from malicious actors who want to steal valuable information.

Domain Name System (DNS) which is a network protocol that translate internet domain names into IP addresses.

- The DNS protocol sends the domain name and the web address to a DNS server that retrieves the IP address of the website you were trying to access

Just by visiting one website, the device on your networks are using four different protocols: TCP, ARP, HTTPS, and DNS.



Three categories of network protocols

Network protocols can be divided into three main categories: **communication protocols, management protocols, and security protocols**. There are dozens of different network protocols, but you don't need to memorize all of them for an entry-level security analyst role.

Communication protocols

govern the exchange of information in network transmission. They dictate how the data is transmitted between devices and the timing of the communication. They

also include methods to recover data lost in transit. Here are a few of them.

- **Transmission Control Protocol (TCP)** is an internet communication protocol that allows two devices to form a connection and stream data. TCP uses a three-way handshake process. First, the device sends a synchronize (SYN) request to a server. Then the server responds with a SYN/ACK packet to acknowledge receipt of the device's request. Once the server receives the final ACK packet from the device, a TCP connection is established. In the TCP/IP model, TCP occurs at the transport layer.
- **User Datagram Protocol (UDP)** is a connectionless protocol that does not establish a connection between devices before a transmission. This makes it less reliable than TCP. But it also means that it works well for transmissions that need to get to their destination quickly. For example, one use of UDP is for internet gaming transmissions. In the TCP/IP model, UDP occurs at the transport layer.
- **Hypertext Transfer Protocol (HTTP)** is an application layer protocol that provides a method of communication between clients and website servers. HTTP uses port 80. HTTP is considered insecure, so it is being replaced on most websites by a secure version, called HTTPS. However, there are still many websites that use the insecure HTTP protocol. In the TCP/IP model, HTTP occurs at the application layer.
- **Domain Name System (DNS)** is a protocol that translates internet domain names into IP addresses. When a client computer wishes to access a website domain using their internet browser, a query is sent to a dedicated DNS server. The DNS server then looks up the IP address that corresponds to the website domain. DNS normally uses UDP on port 53. However, if the DNS reply to a request is large, it will switch to using the TCP protocol. In the TCP/IP model, DNS occurs at the application layer.

Management Protocols

The next category of network protocols is management protocols. Management protocols are used for monitoring and managing activity on a network. They include protocols for error reporting and optimizing performance on the network.

- **Simple Network Management Protocol (SNMP)** is a network protocol used for monitoring and managing devices on a network. SNMP can reset a password on a network device or change its baseline configuration. It can also send requests to network devices for a report on how much of the network’s bandwidth is being used up. In the TCP/IP model, SNMP occurs at the application layer.
- **Internet Control Message Protocol (ICMP)** is an internet protocol used

by devices to tell each other about data transmission errors across the network. ICMP is used by a receiving device to send a report to the sending device about the data transmission. ICMP is commonly used as a quick way to troubleshoot network connectivity and latency by issuing the “ping” command on a Linux operating system. In the TCP/IP model, ICMP occurs at the internet layer.

Security Protocols

Security protocols are network protocols that ensure that data is sent and received securely across a network. Security protocols use encryption algorithms to protect data in transit. Below are some common security protocols.

- **Hypertext Transfer Protocol Secure (HTTPS)** is a network protocol that provides a secure method of communication between clients and website servers. HTTPS is a secure version of HTTP that uses secure sockets layer/transport layer security (SSL/TLS) encryption on all transmissions so that malicious actors cannot read the information contained. HTTPS uses port 443. In the TCP/IP model, HTTPS occurs at the application layer.
- **Secure File Transfer Protocol (SFTP)** is a secure protocol used to transfer files from one device to another over a network. SFTP uses secure shell (SSH), typically through TCP port 22. SSH uses Advanced Encryption Standard (AES) and other types of encryption to ensure that unintended recipients cannot intercept the transmissions. In the TCP/IP model, SFTP occurs at the application layer. SFTP is used often with cloud storage. Every time a user uploads or downloads a file from cloud storage, the file is transferred using the SFTP protocol.

Additional network protocols

a few additional concepts and protocols that will come up regularly in your work as a security analyst. Some protocols are assigned port numbers by the Internet Assigned Numbers Authority (IANA). These port numbers are included in the description of each protocol, if assigned.

Network Address Translation

In order for the devices with private IP addresses to communicate with the public internet, they need to have a public IP address. Otherwise, responses will not be routed correctly. Instead of having a dedicated public IP address for each of the devices on the local network, the router can replace a private source IP address with its public IP address and perform the reverse operation for responses. This process is known as Network Address Translation (NAT) and it generally requires a

router or firewall to be specifically configured to perform NAT.

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is in the management family of network protocols. DHCP is an application layer protocol used on a network to configure devices. It assigns a unique IP address and provides the addresses of the appropriate DNS server and default gateway for each device. DHCP servers operate on UDP port 67 while DHCP clients operate on UDP port 68.

Address Resolution Protocol (ARP)

A device's IP address may change over time, but its MAC address is permanent. Address Resolution Protocol (ARP) is mainly a network access layer protocol in the TCP/IP model used to translate the IP addresses that are found in data packets into the MAC address of the hardware device.
Each device on the network performs ARP and keeps track of matching IP and MAC addresses in an ARP cache. ARP does not have a specific port number.

Telnet

Telnet is an application layer protocol that allows a device to communicate with another device or server. Telnet sends all information in clear text. It uses command line prompts to control another device similar to secure shell (SSH), but Telnet is not as secure as SSH. Telnet can be used to connect to local or remote devices and uses TCP port 23.

Secure shell

Secure shell protocol (SSH) is used to create a secure connection with a remote system. This application layer protocol provides an alternative for secure authentication and encrypted communication. SSH operates over the TCP port 22 and is a replacement for less secure protocols, such as Telnet.

Post office protocol

Post office protocol (POP) is an application layer (layer 4 of the TCP/IP model) protocol used to manage and retrieve email from a mail server. Many organizations have a dedicated mail server on the network that handles incoming and outgoing mail for users on the network. User devices will send requests to the remote mail server and download email messages locally. If you have ever refreshed your email application and had new emails populate in your inbox, you are experiencing POP and internet message access protocol (IMAP) in action. Unencrypted, plaintext authentication uses TCP/UDP port 110 and encrypted emails use Secure Sockets Layer/Transport Layer Security (SSL/TLS) over TCP/UDP port 995. When using POP, mail has to finish downloading on a local device before it can be read and it does not allow a user to sync emails.

Internet Message Access Protocol (IMAP)

IMAP is used for incoming email. It downloads the headers of emails, but not the content. The content remains on the email server, which allows users to access their email from multiple devices. IMAP uses TCP port 143 for unencrypted email and TCP port 993 over the TLS protocol. Using IMAP allows users to partially read email before it is finished downloading and to sync emails. However, IMAP is slower than POP3.

Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) is used to transmit and route email from the sender to the recipient's address. SMTP works with Message Transfer Agent (MTA) software, which searches DNS servers to resolve email addresses to IP addresses, to ensure emails reach their intended destination. SMTP uses TCP/UDP port 25 for unencrypted emails and TCP/UDP port 587 using TLS for encrypted emails. The TCP port 25 is often used by high-volume spam. SMTP helps to filter out spam by regulating how many emails a source can send at a time.

Protocols and port numbers

Remember that port numbers are used by network devices to determine what should be done with the information contained in each data packet once they reach their destination. Firewalls can filter out unwanted traffic based on port numbers. For example, an organization may configure a firewall to only allow access to TCP port 995 (POP3) by IP addresses belonging to the organization.

Protocol	Port
DHCP	UDP port 67 (servers) UDP port 68 (clients)
ARP	none
Telnet	TCP port 23
SSH	TCP port 22
POP3	TCP/UDP port 110 (unencrypted) TCP/UDP port 995 (encrypted, SSL/TLS)
IMAP	TCP port 143 (unencrypted) TCP port 993 (encrypted, SSL/TLS)
SMTP	TCP/UDP port 587 (encrypted, TLS)

Wireless Protocols

IEEE802.11, commonly known as Wi-Fi

is a set of standards that define communications for wireless LANs.

- IEEE stands for the Institute of Electrical and Electronics Engineers, which is an organization that maintains Wi-Fi standards, and 802.11 is a suite of protocols used in wireless communications.

Wi-Fi Protected Access (WPA)

a wireless security protocol for devices to connect to the internet.

- WPA has evolved into newer versions, like WPA2 and WPA3, which include further security improvements

Wired Equivalent Privacy

Wired equivalent privacy (WEP) is a wireless security protocol designed to provide users with the same level of privacy on wireless network connections as they have on wired network connections.

- a network router might have used WEP as the default security protocol and the network administrator never changed it.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) was developed in 2003 to improve upon WEP,

address the security issues that it presented, and replace it. WPA was always intended to be a transitional measure so backwards compatibility could be established with older hardware.

- Despite the security improvements of WPA, it still has vulnerabilities. Malicious actors can use a key reinstallation attack (or KRACK attack) to decrypt transmissions using WPA.
- Attackers can insert themselves in the WPA authentication handshake process and insert a new encryption key instead of the dynamic one assigned by WPA.

WPA2 & WPA3

WPA2

The second version of Wi-Fi Protected Access—known as WPA2—was released in 2004. WPA2 improves upon WPA by using the Advanced Encryption Standard (AES). WPA2 also improves upon WPA's use of TKIP. WPA2 uses the Counter Mode Cipher Block Chain Message Authentication Code Protocol (CCMP), which provides encapsulation and ensures message authentication and integrity. Because of the strength of WPA2, it is considered the security standard for all Wi-Fi transmissions today. WPA2, like its predecessor, is vulnerable to KRACK attacks. This led to the development of WPA3 in 2018.

Personal

WPA2 personal mode is best suited for home networks for a variety of reasons. It is easy to implement, initial setup takes less time for personal than enterprise version. The global passphrase for WPA2 personal version needs to be applied to each individual computer and access point in a network. This makes it ideal for home networks, but unmanageable for organizations.

Enterprise

WPA2 enterprise mode works best for business applications. It provides the necessary security for wireless networks in business settings. The initial setup is more complicated than WPA2 personal mode, but enterprise mode offers individualized and centralized control over the Wi-Fi access to a business network. This means that network administrators can grant or remove user access to a network at any time. Users never have access to encryption keys, this prevents potential attackers from recovering network keys on individual computers.

WPA3

WPA3 is a secure Wi-Fi protocol and is growing in usage as more WPA3 compatible devices are released. These are the key differences between WPA2 and WPA3:

- WPA3 addresses the authentication handshake vulnerability to KRACK attacks, which is present in WPA2.
- WPA3 uses Simultaneous Authentication of Equals (SAE), a password-authenticated, cipher-key-sharing agreement. This prevents attackers

from downloading data from wireless network connections to their systems to attempt to decode it.
- WPA3 has increased encryption to make passwords more secure by using 128-bit encryption, with WPA3-Enterprise mode offering optional 192-bit encryption.

Firewalls and network security measures

Firewall

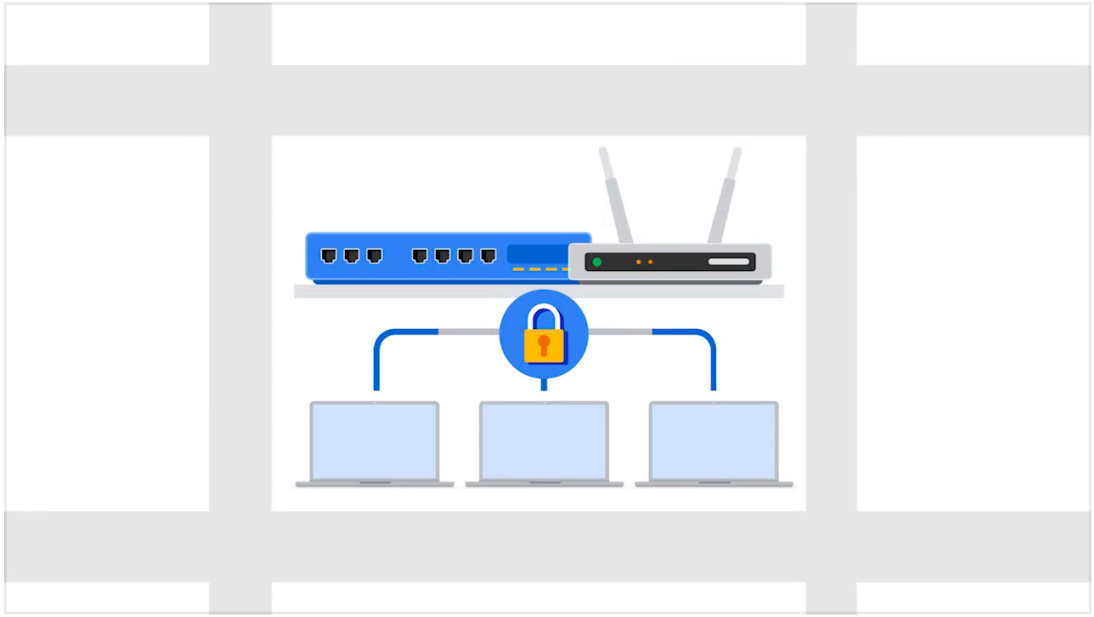
a network security device that monitors traffic to and from your network.

- It either allows traffic or it blocks it based on a defined set of security rules.
- A firewall can use port filtering, which blocks or allows certain port numbers to limit unwanted communication.
    - Ex: a rule that only allows communications on port 443 for HTTPS or port 25 for email and blocks everything else.

Hardware Firewall

A hardware firewall is considered the most basic way to defend against threats to a network.

- A hardware firewall inspects each data packet before it's allowed to enter the network.



Software Firewall

A software firewall performs the same functions as a hardware firewall, but it's not a physical device.

- If the software firewall is installed on a computer, it will analyze all the traffic received by that computer.
- If the software firewall is installed on a server, it will protect all the devices connected to the server.
    - because it is a software program, it will add some processing burden to the individual devices.

Cloud-Based Firewalls

are software firewalls hosted by a cloud service provider.

- Organizations can configure the firewall rules on the cloud service provider's interface, and the firewall will perform security operations on all incoming traffic before it reaches the organization’s onsite network.

All the firewalls we have discussed can be either stateful or stateless. The terms **"stateful" and "stateless"** refer to how the firewall operates.

Stateful refers to a class of firewall that keeps track of information passing through it and proactively filters out threats.

- A stateful firewall analyzes network traffic for characteristics and behavior that appear suspicious and stops them from entering the network.

Stateless refers to a class of firewall that operates based on predefined rules and does not keep track of information from data packets.

- A stateless firewall only acts according to preconfigured rules set by the firewall administrator.
- A stateless firewall doesn't store analyzed information. It also doesn't

discover suspicious trends like a stateful firewall does.

A next generation firewall (NGFW), provides even more security than a stateful firewall.
performs more in-depth security functions like deep packet inspection and intrusion protection.
Some NGFWs connect to cloud-based threat intelligence services so they can quickly update to protect against emerging cyber threats.

Virtual Private network (VPN)

is 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're using a public network like the internet.

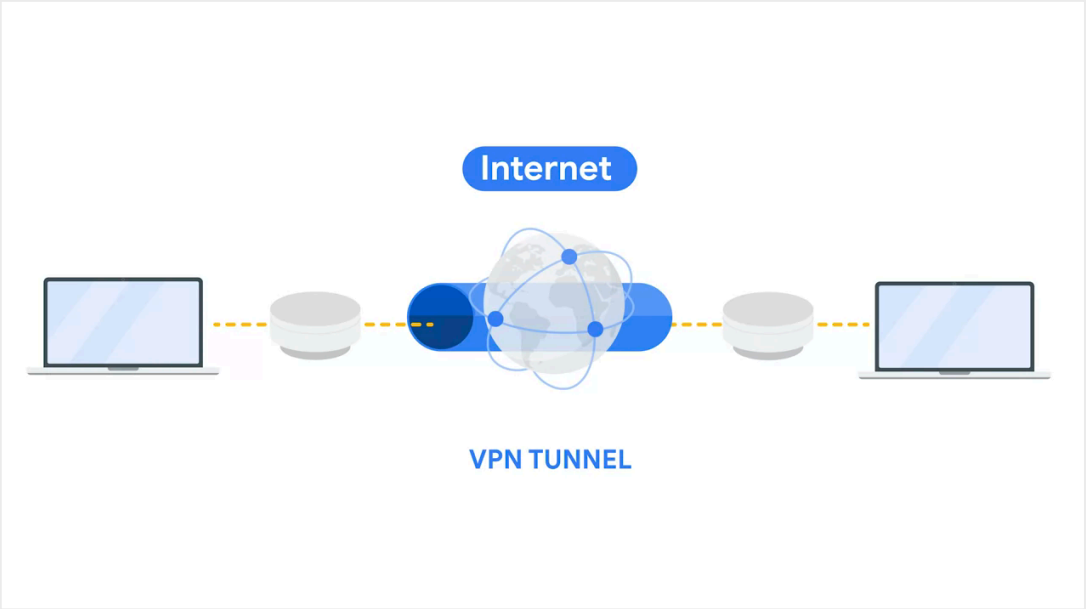
VPNs also encrypt your data as it travels across the internet to preserve confidentiality. A VPN service performs encapsulation on your data in transit.

Encapsulation is a process performed by a VPN service that protects your data by wrapping sensitive data in other data packets.

VPN services encrypt your data packets and encapsulate them in other data packets that the routers can read.

- This allows your network requests to reach their destination, but still encrypts your personal data so it's unreadable while in transit.

A VPN also uses an **encrypted tunnel** between your device and the VPN server. The encryption is unhackable without a cryptographic key, so no one can access your data.



Remote access and site-to-site VPNs

Individual users use **remote access VPNs** to establish a connection between a personal device and a VPN server. Remote access VPNs encrypt data sent or received through a personal device. The connection between the user and the remote access VPN is established through the internet.

Enterprises **use site-to-site VPNs** largely to extend their network to other networks and locations. This is particularly useful for organizations that have many offices across the globe. IPSec is commonly used in site-to-site VPNs to create an encrypted tunnel between the primary network and the remote network. One disadvantage of site-to-site VPNs is how complex they can be to configure and manage compared to remote VPNs.

WireGuard VPN vs. IPSec VPN

WireGuard and IPSec are two different VPN protocols used to encrypt traffic over a secure network tunnel. The majority of VPN providers offer a variety of options for VPN protocols, such as WireGuard or IPSec. Ultimately, choosing between IPSec and WireGuard depends on many factors, including connection speeds, compatibility with existing network infrastructure, and business or individual needs.

WireGuard VPN

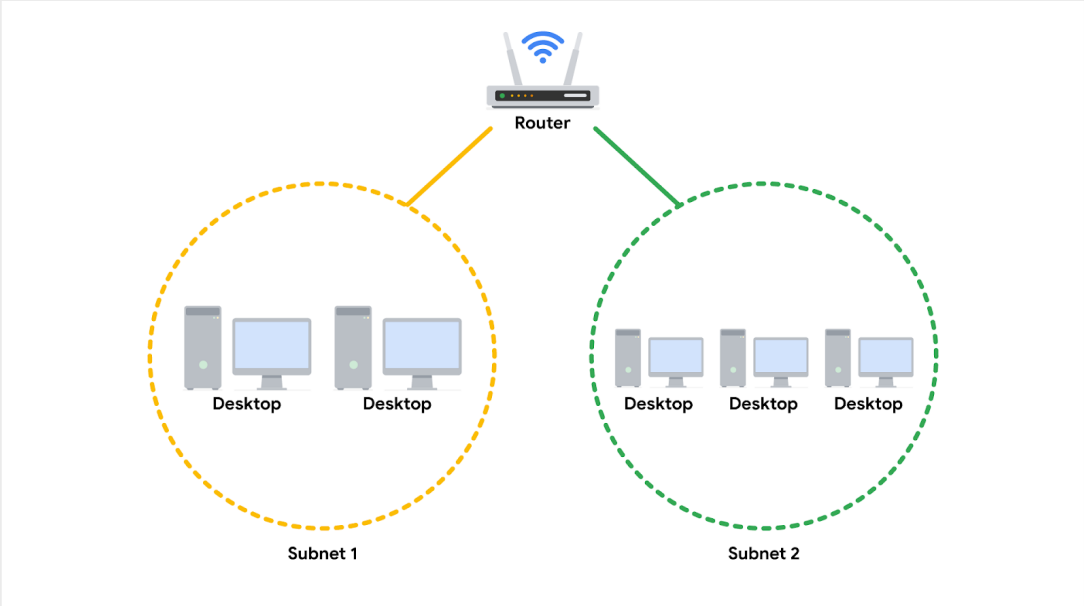
WireGuard is a high-speed VPN protocol, with advanced encryption, to protect users when they are accessing the internet. It's designed to be simple to set up and maintain. WireGuard can be used for both site-to-site connection and client-server connections. WireGuard is relatively newer than IPSec, and is used by many people due to the fact that its download speed is enhanced by using fewer lines of code. WireGuard is also open source, which makes it easier for users to deploy

and debug. This protocol is useful for processes that require faster download speeds, such as streaming video content or downloading large files.

IPSec VPN
IPSec is another VPN protocol that may be used to set up VPNs. Most VPN providers use IPSec to encrypt and authenticate data packets in order to establish secure, encrypted connections. Since IPSec is one of the earlier VPN protocols, many operating systems support IPSec from VPN providers.
Although IPSec and WireGuard are both VPN protocols, IPSec is older and more complex than WireGuard. Some clients may prefer IPSec due to its longer history of use, extensive security testing, and widespread adoption. However, others may prefer WireGuard because of its potential for better performance and simpler configuration.

Security Zones

Security zones are a segment of a network that protects the internal network from the internet.
Creating security zones is one example of a networking strategy called **subnetting**.
Subnetting is the subdivision of a network into logical groups called subnets. It works like a network inside a network.



They are a part of a security technique called network **segmentation** that divides the network into segments.

- Ex: hotel that offers free public Wi-Fi. The unsecured guest network is kept separate from another encrypted network used by the hotel staff.

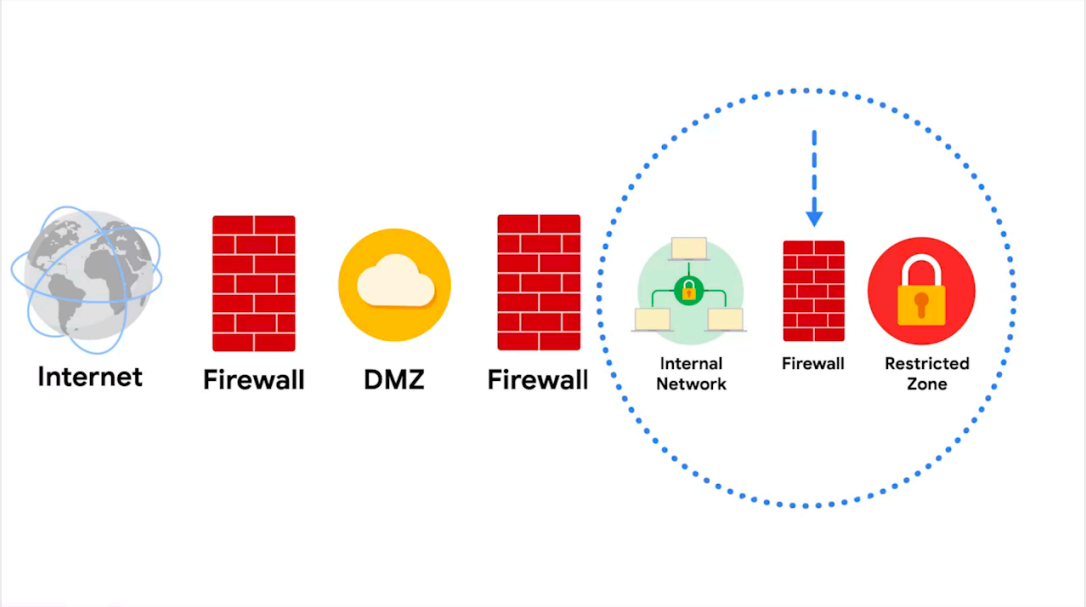
An organization's network is classified into two types of security zones.

Uncontrolled Zone
any network outside of the organization's control, like the internet.

Controlled Zone
a subnet that protects the internal network from the uncontrolled zone.
There are several types of networks within the controlled zone:

- **Demilitarized zone(DMZ)** - contains public-facing services that can access the internet.
    - This includes web servers, proxy servers that host websites for the public, and DNS servers that provide IP addresses for internet users.
- **Internal Network** - contains private servers and data that the organization needs to protect.
- **Restricted Zone** - highly confidential information that is only accessible to employees with certain privileges.

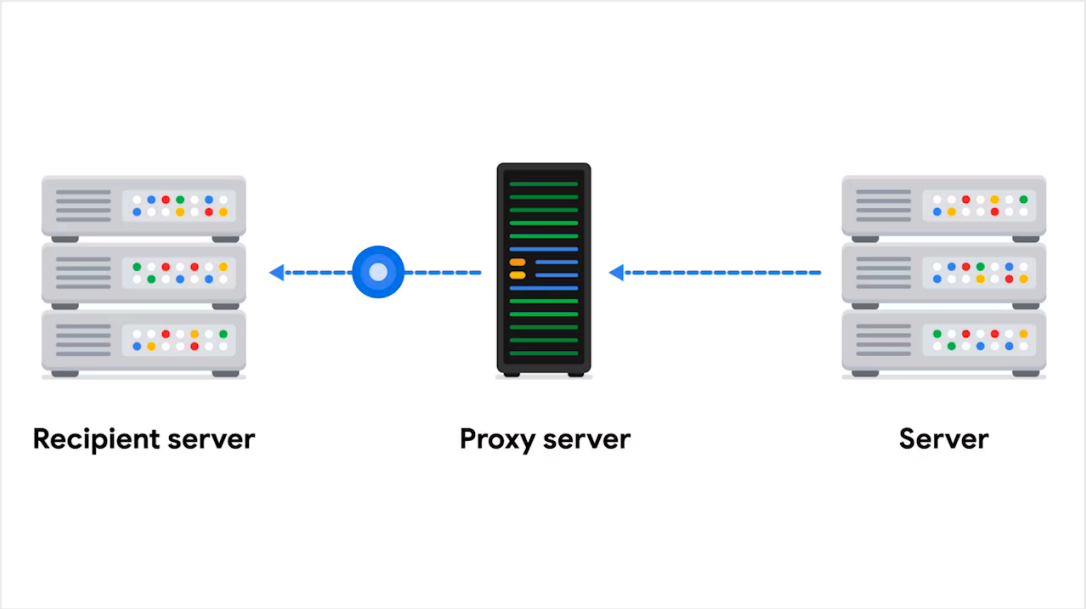
This protects the internal network with several lines of defense.



Proxy Servers
Proxy servers are another system that helps secure networks.
A proxy server is a server that fulfills the request of a client by forwarding them on to other servers.

- The proxy server is a dedicated server that sits between the internet and the rest of the network.

When a client receives an HTTPS response, they will notice a distorted IP address or no IP address rather than the real IP address of the organization's web server.



A proxy server can also be used to block unsafe websites that users aren't allowed to access on an organization's network.

Forward Proxy Server

regulates and restricts a person with access to the internet.

- The goal is to hide a user's IP address and approve all outgoing requests.

Reverse Proxy Server

regulates and restricts the internet access to an internal server. The goal is to accept traffic from external parties, approve it, and forward it to the internal servers.

Email proxy server

It filters spam email by verifying whether a sender's address was forged.

- The proxy servers would've allowed us to filter and then scale those filters without impacting the underlying email platform.

How intrusions compromise your system

network interception attacks and backdoor attacks, and the possible impacts these attacks could have on an organization.

Network interception attacks

work by intercepting network traffic and stealing valuable information or interfering with the transmission in some way.

Malicious actors can use hardware or software tools to capture and inspect data in transit.

- This is referred to as **packet sniffing**. In addition to seeing information that they are not entitled to, malicious actors can also intercept network traffic and alter it.
- These attacks can cause damage to an organization's network by inserting malicious code modifications or altering the message and interrupting network operations.
    - For example, an attacker can intercept a bank transfer and change the account receiving the funds to one that the attacker controls.

Backdoor attacks

- An organization may have a lot of security measures in place, including cameras, biometric scans and access codes to keep employees from entering and exiting without being seen. An employee might work around the security measures by finding a backdoor to the building that is not as heavily monitored, allowing them to sneak out for the afternoon without being seen.

In cybersecurity, **backdoors** are weaknesses intentionally left by programmers or system and network administrators that bypass normal access control mechanisms. Backdoors are intended to help programmers conduct troubleshooting or administrative tasks.

- However, backdoors can also be installed by attackers after they've compromised an organization to ensure they have persistent access.

Once the hacker has entered an insecure network through a backdoor, they can cause extensive damage: installing malware, performing a denial of service (DoS) attack, stealing private information or changing other security settings that leaves the system vulnerable to other attacks.

- A **DoS attack** is an attack that targets a network or server and floods it with network traffic.

Secure networks against Denial of Service (DoS) attacks

The objective of a DoS attack, is to disrupt normal business operations by overloading an organization's network.
The goal of the attack is to send so much information to a network device that it crashes or is unable to respond to legitimate users.

A distributed denial of service attack (DDoS)
is a kind of DoS attack that uses multiple devices or servers in different locations

to flood the target network with unwanted traffic.

- Use of numerous devices makes it more likely that the total amount of traffic sent will overwhelm the target server.

Syn-Flood Attack

is a type of DoS attack that simulates the TCP connection and floods the server with SYN packets.

Internet Control Message Protocol (ICMP)

an internet protocol used by devices to tell each other about data transmission errors across the network.

An **ICMP flood attack** is a type of DoS attack performed by an attacker repeatedly sending ICMP packets to a network server.

SYN flood and ICMP flood, take advantage of communication protocols by sending an overwhelming number of requests.

There are also attacks that can overwhelm the server with one big request.

Ping of death attack

is a type of DoS attack that is caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64 kilobytes, the maximum size for a correctly formed ICMP packet.

- will overload the system and cause it to crash
    - Ex: dropping a rock on a small ant hill

A **network protocol analyzer**, sometimes called a packet sniffer or a packet analyzer, is a tool designed to capture and analyze data traffic within a network. They are commonly used as investigative tools to monitor networks and identify suspicious activity. There are a wide variety of network protocol analyzers available, but some of the most common analyzers include:

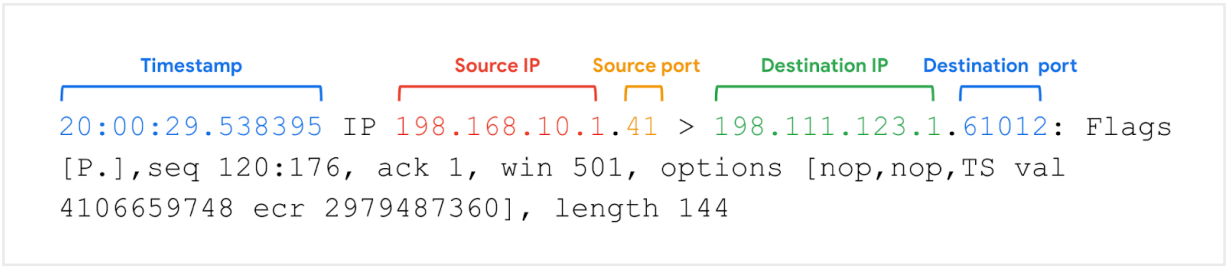
- SolarWinds NetFlow Traffic Analyzer
- ManageEngine OpManager
- Azure Network Watcher
- Wireshark
- tcpdump

tcpdump

is a command-line network protocol analyzer. It is popular, lightweight–meaning it uses little memory and has a low CPU usage–and uses the open-source libpcap library.

- tcpdump is text based, meaning all commands in tcpdump are executed in the terminal.
- It can also be installed on other Unix-based operating systems, such as macOS®. It is preinstalled on many Linux distributions.
- tcpdump provides a brief packet analysis and converts key information about network traffic into formats easily read by humans.
- It prints information about each packet directly into your terminal. tcpdump also displays the source IP address, destination IP addresses, and the port numbers being used in the communications.

tcpdump prints the output of the command as the sniffed packets in the command line, and optionally to a log file, after a command is executed.



Some information you receive from a packet capture includes:

- **Timestamp**: The output begins with the timestamp, formatted as hours, minutes, seconds, and fractions of a second.
- **Source IP**: The packet's origin is provided by its source IP address.
- **Source port**: This port number is where the packet originated.
- **Destination IP**: The destination IP address is where the packet is being transmitted to.
- **Destination port**: This port number is where the packet is being transmitted to.

tcpdump and other network protocol analyzers are commonly used to capture and view network communications and to collect statistics about the network, such as troubleshooting network performance issues. They can also be used to:

- Establish a baseline for network traffic patterns and network utilization metrics.
- Detect and identify malicious traffic
- Create customized alerts to send the right notifications when network issues or security threats arise.
- Locate unauthorized instant messaging (IM), traffic, or wireless access points.

Malicious packet sniffing

Packet sniffing is the practice of using software tools to observe data as it moves across a network.

It's important for you to learn about how threat actors use packet sniffing with harmful intent so you can be prepared to protect against these malicious acts.

Malicious actors can access a network packet with a packet sniffer and make changes to the data.
They may change the information in the body of the packet, like altering a recipient's bank account number.

Packet sniffing can be passive or active.

Passive packet sniffing is a type of attack where data packets are read in transit.

- Since all the traffic on a network is visible to any host on the hub, malicious actors can view all the information going in and out of the device they are targeting.
- Ex: a postal delivery person maliciously reading somebody's mail.

Active packet sniffing is a type of attack where data packets are manipulated in transit. This may include injecting internet protocols to redirect the packets to an unintended port or changing the information the packet contains.

Active packet sniffing attack would be like a neighbor telling the delivery person "I'll deliver that mail for you" and then reading the mail or changing the letter before putting it in your mailbox.

Malicious packet sniffing can be prevented

- Use a VPN to encrypt and protect data as it travels across the network
  - hackers might interfere with your traffic, but they won't be able to decode it to read it and read your private information.
- Make sure that websites you have use HTTPS at the beginning of the domain address.
- Avoid using unprotected WiFi
  - avoiding free public WiFi unless you have a VPN service already installed on your device.

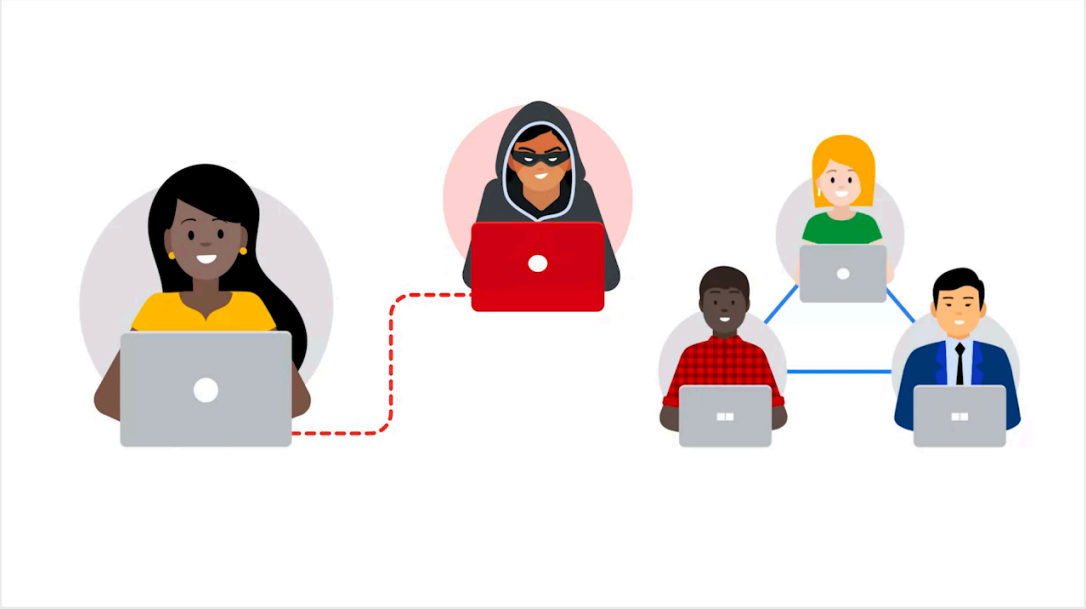
IP Spoofing

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

- the hacker is pretending to be someone they are not, so they can communicate over the network with the target computer and get past firewall rules that may prevent outside traffic.

On-path Attack

An on-path attack is an attack where the malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit.



Replay Attack

A replay attack is a network attack performed when a malicious actor intercepts a data packet in transit and delays it or repeats it at another time.

- A delayed packet can cause connection issues between target computers
- or a malicious actor may take a network transmission that was sent by an authorized user and repeat it at a later time to impersonate the authorized user.

Smurf Attack

a combination of a DDoS attack and an IP spoofing attack. The attacker sniffs an authorized user's IP address and floods it with packets.

- This overwhelms the target computer and can bring down a server or the entire network.

How to protect from IP spoofing:

- **encryption** should always be implemented so that the data in your network transfers can't be read by malicious actors.
- **Firewalls**
  - if a firewall receives a data packet from the internet where the sender's IP address is the same as the private network, then the firewall will deny the transmission since all the devices with that IP address should already be on the local network.
  - configure correctly by creating a rule to reject all incoming traffic that has the same IP address as the local network.

Security Hardening

Security hardening is the process of strengthening a system to reduce its vulnerability and attack surface.

All the potential vulnerabilities that a threat actor could exploit are referred to as a system's **attack surface**.

Security hardening can be conducted on any device or system that can be compromised, such as

- hardware, operating systems, applications, computer networks, and databases.

Some common types of hardening procedures include:

- software updates, also called patches
- device application configuration changes.

Another important strategy for security hardening is to conduct regular **penetration testing**.

- a simulated attack that helps identify vulnerabilities in a system, network, website, application, and process.
- security teams can determine the type of security vulnerabilities that require fixing

OS hardening practices

The operating system is the interface between computer hardware and the user.

A **patch update** is a software and operating system, or OS, update that addresses security vulnerabilities within a program or product.

- with patch updates, the OS should be upgraded to its latest software version
- released to fix a security vulnerability in the software

The newly updated OS should be added to the **baseline configuration**, also called the baseline image.

A **baseline configuration** is a documented set of specifications within a system that is used as a basis for future builds, releases, and updates.

- Ex: a baseline may contain a firewall rule with a list of allowed and

disallowed network ports.

Another hardening task performed regularly is **hardware and software disposal**

- Removing unused software makes sure that there aren't any unnecessary vulnerabilities connected with the programs that the software uses.

Strong password policies require that passwords follow specific rules.

- Ex: organization may set a password policy that requires a minimum of eight characters, a capital letter, a number, and a symbol.

Brute force attacks

A **brute force attack** is a trial-and-error process of discovering private information. There are different types of brute force attacks that malicious actors use to guess passwords, including:

- *Simple brute force attacks*. When attackers try to guess a user's login credentials, it's considered a simple brute force attack. They might do this by entering any combination of usernames and passwords that they can think of until they find the one that works.
- *Dictionary attacks* use a similar technique. In dictionary attacks, attackers use a list of commonly used passwords and stolen credentials from previous breaches to access a system. These are called "dictionary" attacks because attackers originally used a list of words from the dictionary to guess the passwords, before complex password rules became a common security practice.

Using brute force to access a system can be a tedious and time consuming process, especially when it's done manually. There are a range of tools attackers use to conduct their attacks.

Virtual machines (VMs)

Virtual machines (VMs) are software versions of physical computers. VMs provide an additional layer of security for an organization because they can be used to run code in an isolated environment, preventing malicious code from affecting the rest of the computer or system. VMs can also be deleted and replaced by a pristine image after testing malware.

Sandbox environments

A sandbox is a type of testing environment that allows you to execute software or programs separate from your network. They are commonly used for testing patches, identifying and addressing bugs, or detecting cybersecurity

vulnerabilities. Sandboxes can also be used to evaluate suspicious software, evaluate files containing malicious code, and simulate attack scenarios

- Sandboxes can be stand-alone physical computers that are not connected to a network; however, it is often more time- and cost-effective to use software or cloud-based virtual machines as sandbox environments.

Prevention measures

Some common measures organizations use to prevent brute force attacks and similar attacks from occurring include:

- **Salting and hashing:** Hashing converts information into a unique value that can then be used to determine its integrity. It is a one-way function, meaning it is impossible to decrypt and obtain the original text. Salting adds random characters to hashed passwords. This increases the length and complexity of hash values, making them more secure.
- **Multi-factor authentication (MFA) and two-factor authentication (2FA):** MFA is a security measure which requires a user to verify their identity in two or more ways to access a system or network. This verification happens using a combination of authentication factors: a username and password, fingerprints, facial recognition, or a one-time password (OTP) sent to a phone number or email. 2FA is similar to MFA, except it uses only two forms of verification.
- **CAPTCHA and reCAPTCHA:** CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. It asks users to complete a simple test that proves they are human. This helps prevent software from trying to brute force a password. reCAPTCHA is a free CAPTCHA service from Google that helps protect websites from bots and malicious software.
- **Password policies:** Organizations use password policies to standardize good password practices throughout the business. Policies can include guidelines on how complex a password should be, how often users need to update passwords, and if there are limits to how many times a user can attempt to log in before their account is suspended.

Network Hardening Practices

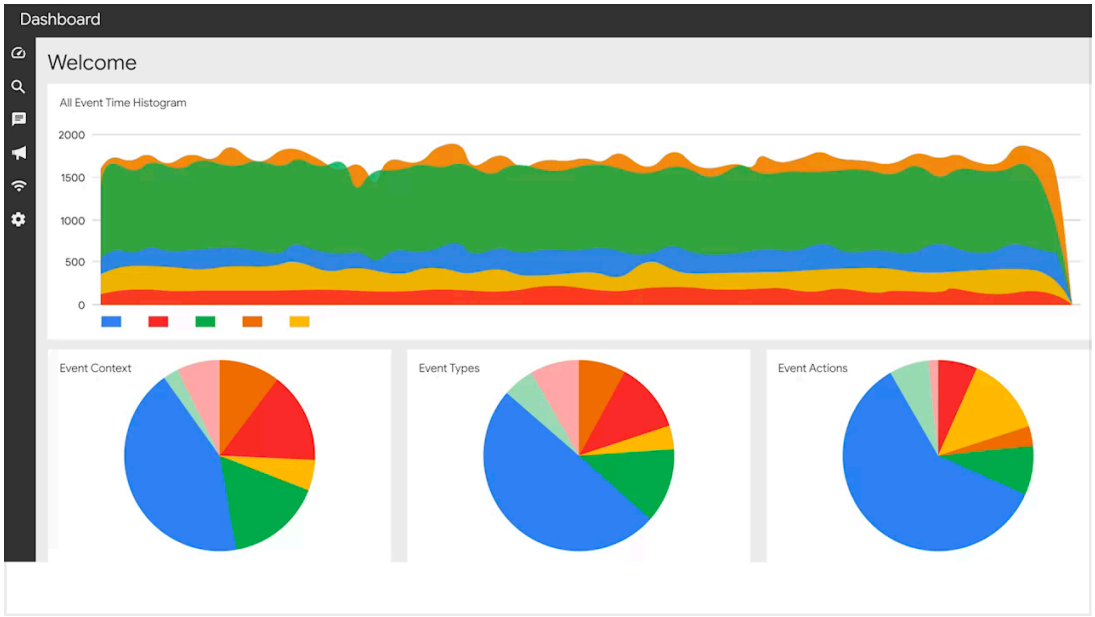
Tasks Performed

- Firewall rules maintenance
- Network log analysis
- Patch updates

- Server backups

Network log analysis is the process of examining network logs to identify events of interest.

A **SIEM tool** is an application that collects and analyzes log data to monitor critical activities in an organization.



Reports from the SIEM provide a list of new or ongoing network vulnerabilities and list them on a scale of priority from high to low, where high priority vulnerabilities have a much shorter deadline for mitigation.

Port filtering is a firewall function that blocks or allows certain port numbers to limit unwanted communication.

- can be formed over the network
- protects against port vulnerabilities

Networks should be set up with the most up-to-date wireless protocols available and older wireless protocols should be disabled.

Security analysts also use **network segmentation** to create isolated subnets for different departments in an organization.

- so the issues in each subnet don't spread across the whole company
- only specified users are given access to the part of the network that they require for their role

Encryption standards are rules or methods used to conceal outgoing data and uncover or decrypt incoming data.

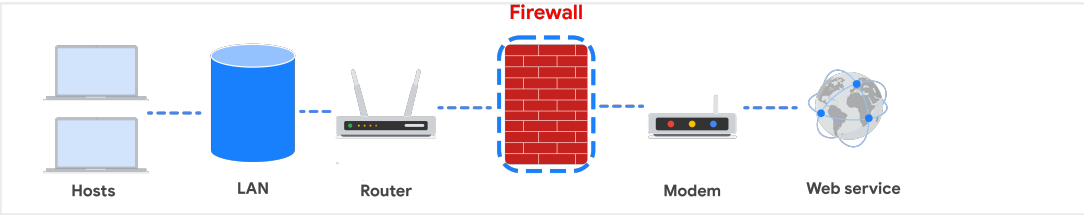
- Data in restricted zones should have much higher encryption standards
    - which makes them more difficult to access.

firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and security incident and event management tools (SIEM)

- four devices used to secure a network

Firewalls

Firewalls allow or block traffic based on a set of rules. As data packets enter a network, the packet header is inspected and allowed or denied based on its port number. NGFWs are also able to inspect packet payloads. Each system should have its own firewall, regardless of the network firewall.



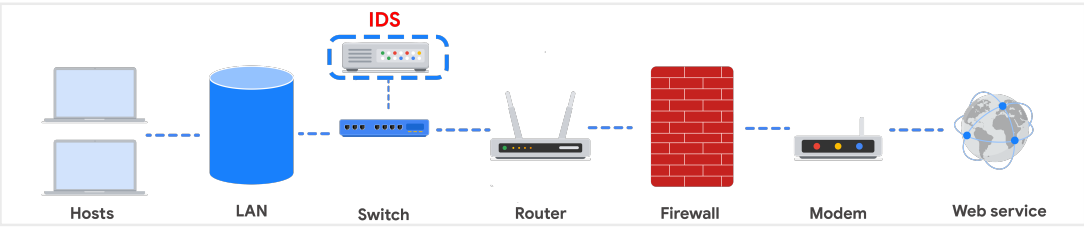
Intrusion Detection System

an application that monitors system activity and alerts on possible intrusions. An IDS alerts administrators based on the signature of malicious traffic.

- configured to detect known attacks
- often sniff data packets as they move across the network and analyze them for the characteristics of known attacks
- also review for anomalies that could be the sign of malicious activity

Limitations:

- limitations to IDS systems are that they can only scan for known attacks or obvious anomalies
- Also it doesn't actually stop the incoming traffic if it detects something awry.



Intrusion Prevention System

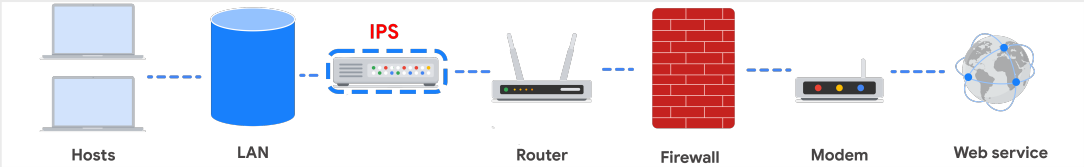
application that monitors system activity for intrusive activity and takes action to stop the activity.

- offers even more protection than an IDS because it actively stops anomalies when they are detected
- reports the anomaly to security analysts and blocks a specific sender or

drops network packets that seem suspect.

Limitation:

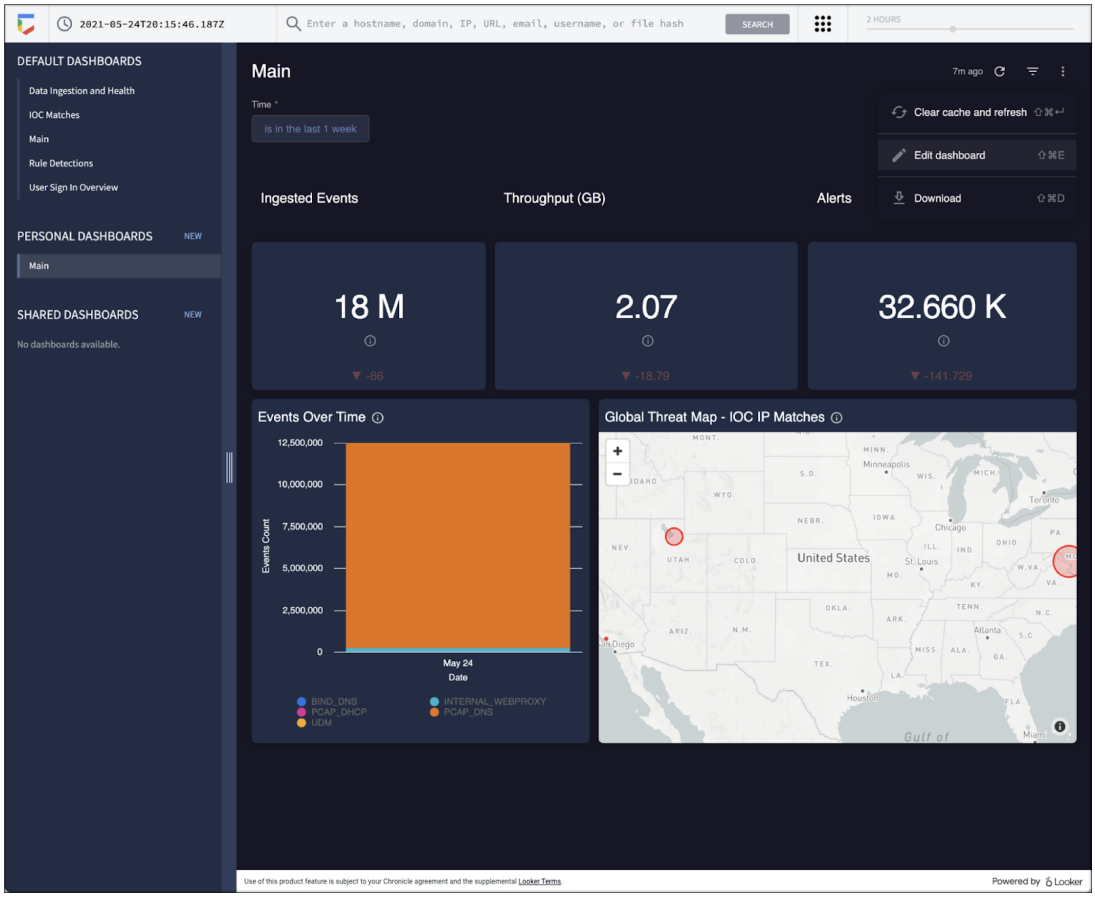
- it is inline: If it breaks, the connection between the private network and the internet breaks.
- possibility of false positives, which can result in legitimate traffic getting dropped.



Security Information and Event Management

application that collects and analyzes log data to monitor critical activities in an organization

- Works in real time
- Analyze network log data sourced from IDSs, IPSs, firewalls, VPNs, proxies, and DNS logs
- It all appears in one place on dashboard



Network Security in the cloud

cloud network is a collection of servers or computers that stores resources and data in a remote data center that can be accessed via the internet.

Just like regular web servers, cloud servers also require proper maintenance done through various security hardening procedures.

One distinction between cloud network hardening and traditional network hardening is the use of a server baseline image for all server instances stored in the cloud.

Cloud computing is a model for allowing convenient and on-demand network access to a shared pool of configurable computing resources.

- can be configured and released with minimal management effort or interaction with the service provider.

Many organizations choose to use cloud services because of the ease of deployment, speed of deployment, cost savings, and scalability of these options.

Identity access management (IAM) is a collection of processes and technologies that helps organizations manage digital identities in their environment.

- This service also authorizes how users can use different cloud resources.
- A common problem that organizations face when using the cloud is the loose configuration of cloud user roles.

Configuration

The number of available cloud services adds complexity to the network. Each service must be carefully configured to meet security and compliance requirements.

- must ensure that every process moved into the cloud has been configured correctly
- could leave the network open to compromise.

Attack surface

Cloud service providers (CSPs) offer numerous applications and services for organizations at a low cost.
Every service or application on a network carries its own set of risks and vulnerabilities and increases an organization’s overall attack surface.

- An increased attack surface must be compensated for with increased security measuresw

Zero-day attacks

is an exploit that was previously unknown.

- CSPs are more likely to know about a zero day attack occurring before a traditional IT organization does

Visibility and tracking

Network administrators have access to every data packet crossing the network with both on-premise and cloud networks.

- They can sniff and inspect data packets to learn about network performance or to check for possible threats and attacks.

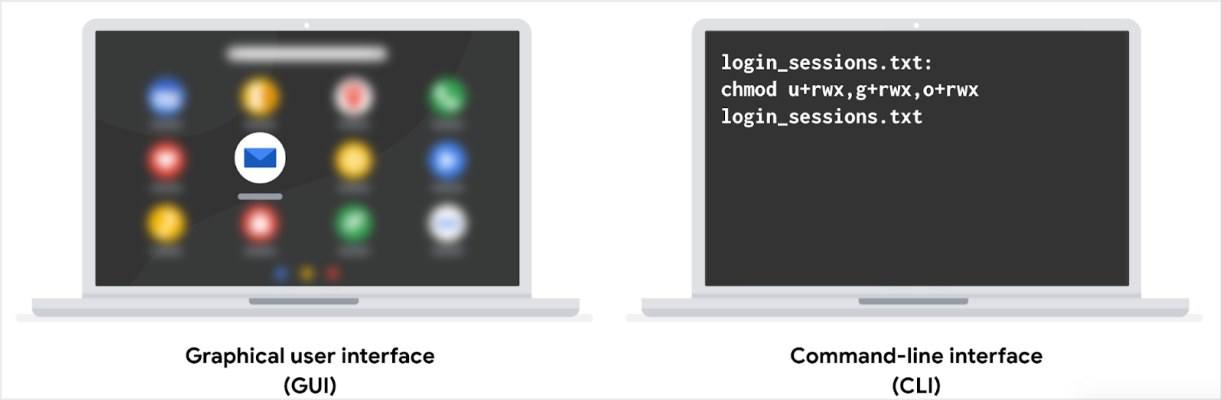
Course 3: Tools of the trade: Linux and SQL

CLI vs. GUI

A **graphical user interface (GUI)** is a user interface that uses icons on the screen to manage different tasks on the computer. A **command-line interface (CLI)** is a text-based user interface that uses commands to interact with the computer.

Display

One notable difference between these two interfaces is how they appear on the screen. A GUI has graphics and icons, such as the icons on your desktop or taskbar for launching programs. In contrast, a CLI only has text. It looks similar to lines of code.



Advantages of a CLI in cybersecurity

The choice between using a GUI or CLI is partly based on personal preference, but security analysts should be able to use both interfaces. Using a CLI can provide certain advantages.

Efficiency

Some prefer the CLI because it can be used more quickly when you know how to manage this interface. For a new user, a GUI might be more efficient because they're easier for beginners to navigate.

Because a CLI can accept multiple requests at one time, it's more powerful when you need to perform multiple tasks efficiently. For example, if you had to create multiple new files in your system, you could quickly perform this task in a CLI. If you were using a GUI, this could take much longer, because you have to repeat the same steps for each new file.

History file
For security analysts, using the Linux CLI is helpful because it records a history file of all the commands and actions in the CLI. If you were using a GUI, your actions are not necessarily saved in a history file.

For example, you might be in a situation where you're responding to an incident using a playbook. The playbook's instructions require you to run a series of different commands. If you used a CLI, you'd be able to go back to the history and ensure all of the commands were correctly used. This could be helpful if there were issues using the playbook and you had to review the steps you performed in the command line.

Additionally, if you suspect an attacker has compromised your system, you might be able to trace their actions using the history file.

Linux distributions

KALI LINUX ™ is an open-source distribution of Linux that is widely used in the security industry. This is because KALI LINUX ™, which is Debian-based, is pre-installed with many useful tools for penetration testing and digital forensics. A **penetration test** is a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes. **Digital forensics** is the practice of collecting and analyzing data to determine what has happened after an attack. These are key activities in the security industry.

Ubuntu is an open-source, user-friendly distribution that is widely used in security and other industries. It has both a command-line interface (CLI) and a graphical user interface (GUI). Ubuntu is also Debian-derived and includes common applications by default. Users can also download many more applications from a package manager, including security-focused tools. Because of its wide use, Ubuntu has an especially large number of community resources to support users. Ubuntu is also widely used for cloud computing. As organizations migrate to cloud

servers, cybersecurity work may more regularly involve Ubuntu derivatives.

Red Hat® Enterprise Linux®
Red Hat Enterprise Linux is a subscription-based distribution of Linux built for enterprise use. Red Hat is not free, which is a major difference from the previously mentioned distributions. Because it's built and supported for enterprise use, Red Hat also offers a dedicated support team for customers to call about issues.

Package managers for installing applications

A **package** is a piece of software that can be combined with other packages to form an application. Some packages may be large enough to form applications on their own.

Package managers can help resolve any issues with dependencies and perform other management tasks.
A **package manager** is a tool that helps users install, manage, and remove packages or applications. Linux uses multiple package managers.

Different types of shells

Knowing how to work with Linux shells is an important skill for cybersecurity professionals. Shells can be used for many common tasks. Previously, you were introduced to shells and their functions. This reading will review shells and introduce you to different types, including the one that you'll use in this course.

Communicate through a shell

As you explored previously, the **shell** is the command-line interpreter. You can think of a shell as a translator between you and the computer system. Shells allow you to give commands to the computer and receive responses from it. When you enter a command into a shell, the shell executes many internal processes to interpret your command, send it to the kernel, and return your results.

Types of shells

The many different types of Linux shells include the following:

- Bourne-Again Shell (bash)
- C Shell (csh)
- Korn Shell (ksh)
- Enhanced C shell (tcsh)

- Z Shell (zsh)

Course 5: Assets, Threats, and Vulnerabilities

Security plans are based on the analysis of three elements: assets, threats, and vulnerabilities.

- they each represent the what, why, and how of security

a **risk** is anything that can impact the confidentiality, integrity, or availability of an asset.

Likelihood x Impact = Risk

Asset

is an item perceived as having value to an organization

Threat

a threat is any circumstance or event that can negatively impact assets

Vulnerability

a weakness that can be exploited by a threat

Why asset management matters

Keeping assets safe requires a workable system that helps businesses operate smoothly. Setting these systems up requires having detailed knowledge of the assets in an environment. For example, a bank needs to have money available each day to serve its customers. Equipment, devices, and processes need to be in place to ensure that money is available and secure from unauthorized access.

asset classification is the practice of labeling assets based on sensitivity and

importance to an organization.

The most common classification scheme is: restricted, confidential, internal-only, and public.

- **Restricted** is the highest level. This category is reserved for incredibly sensitive assets, like need-to-know information.
- **Confidential** refers to assets whose disclosure may lead to a significant negative impact on an organization.
- **Internal-only** describes assets that are available to employees and business partners.
- **Public** is the lowest level of classification. These assets have no negative consequences to the organization if they’re released.

There are three main categories of cloud-based services:

- Software as a service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)

Software as a service (SaaS)
SaaS refers to front-end applications that users access via a web browser. The service providers host, manage, and maintain all of the back-end systems for those applications. Common examples of SaaS services include applications like Gmail™ email service, Slack, and Zoom software.

Platform as a service (PaaS)
PaaS refers to back-end application development tools that clients can access online. Developers use these resources to write code and build, manage, and deploy their own apps. Meanwhile, the cloud service providers host and maintain the back-end hardware and software that the apps use to operate. Some examples of PaaS services include Google App Engine™ platform, Heroku®, and VMware Cloud Foundry.

Infrastructure as a service (IaaS)
IaaS customers are given remote access to a range of back-end systems that are hosted by the cloud service provider. This includes data processing servers, storage, networking resources, and more. Resources are commonly licensed as needed, making it a cost-effective alternative to buying and maintaining on premises.
Cloud-based services allow companies to connect with their customers, employees, and business partners over the internet. Some of the largest organizations in the world offer cloud-based services:

- Google Cloud Platform
- Microsoft Azure

Types of risk categories

Some common risk categories might include, the damage, disclosure, or loss of information.

Security plans consist of three basic elements: **policies, standards, and procedures.**

Policy

Policies are the foundation of every security plan. They give everyone in and out of an organization guidance by addressing questions like, what are we protecting and why?

Standards

standards are references that inform how to set policies. A good way to think of standards is that they create a point of reference.

Procedures

Procedures are step-by-step instructions to perform a specific security task.

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

Regulations are rules set by a government or other authority to control the way something is done.

- Like policies, regulations exist to protect people and their information, but on a larger scale.

Components of the CSF

Core

The CSF core is a set of desired cybersecurity outcomes that help organizations customize their security plan. It consists of five functions, or parts: Identify, Protect, Detect, Respond, and Recover. These functions are commonly used as an informative reference to help organizations *identify* their most important assets and *protect* those assets with appropriate safeguards. The CSF core is also used to understand ways to *detect* attacks and develop *response* and *recovery* plans should an attack happen.

Tiers

The CSF tiers are a way of measuring the sophistication of an organization's cybersecurity program. CSF tiers are measured on a scale of 1 to 4. Tier 1 is the lowest score, indicating that a limited set of security controls have been implemented. Overall, CSF tiers are used to assess an organization's security posture and identify areas for improvement.

Profiles

The CSF profiles are pre-made templates of the NIST CSF that are developed by a team of industry experts. CSF profiles are tailored to address the specific risks of an organization or industry. They are used to help organizations develop a baseline for their cybersecurity plans, or as a way of comparing their current cybersecurity posture to a specific industry standard.

Implementing the CSF

- **Create a current profile** of the security operations and outline the specific needs of your business.
- **Perform a risk assessment** to identify which of your current operations are meeting business and regulatory standards.
- **Analyze and prioritize existing gaps** in security operations that place the businesses assets at risk.

- **Implement a plan of action** to achieve your organization’s goals and objectives.

Security controls
Security controls are safeguards designed to reduce specific security risks.

Types of security controls:
Technical
many technologies used to protect assets. This includes encryption, authentication systems, and others.

Operational
maintaining the day-to-day security environment. Generally, people perform these controls like awareness training and incident response.

Managerial
centered around how the other two reduce risk. Examples of management controls include policies, standards, and procedures.

A **data owner** is a person who decides who can access, edit, use, or destroy their information.

A **data custodian** is anyone or anything that's responsible for the safe handling, transport, and storage of information.

A **data steward** is the person or group that maintains and implements data governance policies set by an organization.

Limiting access reduces risk
Every business needs to plan for the risk of data theft, misuse, or abuse. Implementing the principle of least privilege can greatly reduce the risk of costly incidents like data breaches by:
- Limiting access to sensitive information
- Reducing the chances of accidental data modification, tampering, or loss
- Supporting system monitoring and administration

Determining access and authorization
To implement least privilege, access and authorization must be determined first. There are two questions to ask to do so:

- Who is the user?
- How much access do they need to a specific resource?

Auditing account privileges

Setting up the right user accounts and assigning them the appropriate privileges is a helpful first step. Periodically auditing those accounts is a key part of keeping your company's systems secure.

There are three common approaches to auditing user accounts:

- Usage audits
- Privilege audits
- Account change audits

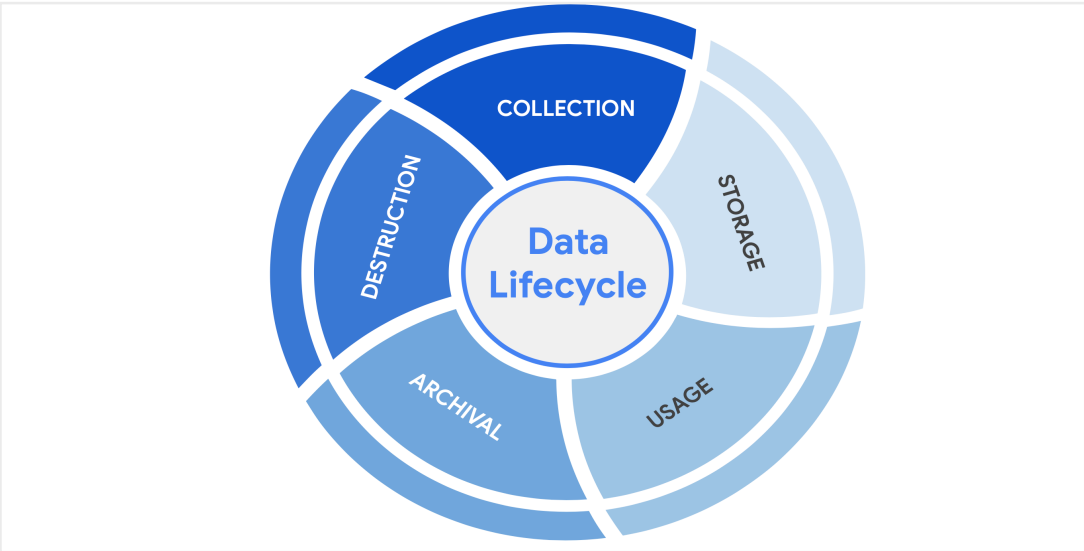
The data lifecycle

Organizations of all sizes handle a large amount of data that must be kept private. You learned that data can be vulnerable whether it is at rest, in use, or in transit. Regardless of the state it is in, information should be kept private by limiting access and authorization.

Each stage of the data lifecycle plays an important role in the security controls that are put in place to maintain the CIA triad of information.

In general, the data lifecycle has five stages. Each describe how data flows through an organization from the moment it is created until it is no longer useful:

- Collect
- Store
- Use
- Archive
- Destroy

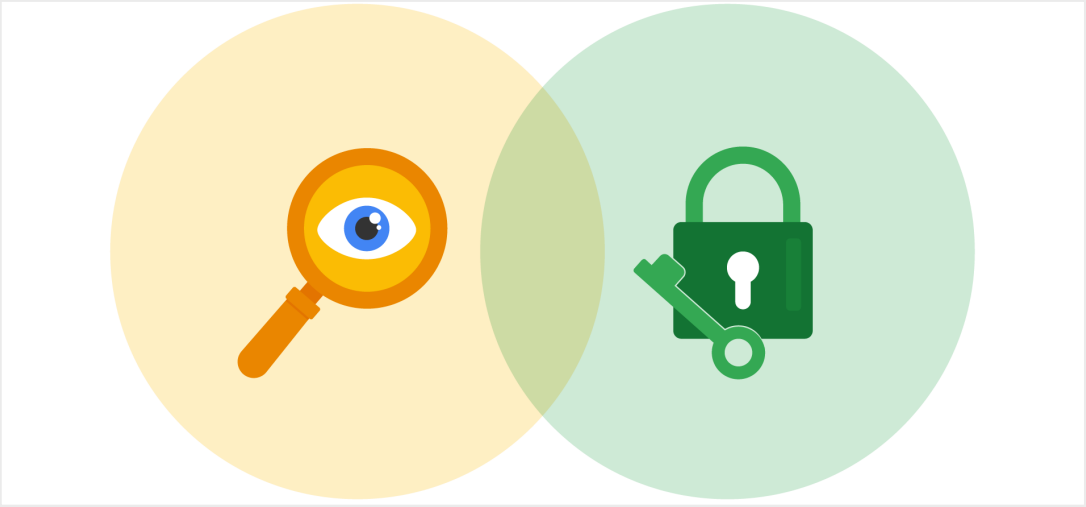


Protecting information at each stage of this process describes the need to keep it accessible and recoverable should something go wrong.'

Information security vs. information privacy

Security and privacy are two terms that often get used interchangeably outside of this field. Although the two concepts are connected, they represent specific functions:

- **Information privacy** refers to the protection of unauthorized access and distribution of data.
- **Information security** (InfoSec) refers to the practice of keeping data in all states away from unauthorized users.



Privacy is about providing people with control over their personal information and how it's shared. Security is about protecting people's choices and keeping their information safe from potential threats.

Notable privacy regulations

Businesses are required to abide by certain laws to operate. As you might recall, **regulations** are rules set by a government or another authority to control the way something is done. Privacy regulations in particular exist to protect a user from having their information collected, used, or shared without their consent. Regulations may also describe the security measures that need to be in place to keep private information away from threats.
Three of the most influential industry regulations that every security professional should know about are:

General Data Protection Regulation (GDPR)
a set of rules and regulations developed by the European Union (EU) that puts data owners in total control of their personal information.
Under GDPR, types of personal information include a person's name, address,

phone number, financial information, and medical information.

Payment Card Industry Data Security Standard (PCI DSS)
set of security standards formed by major organizations in the financial industry. This regulation aims to secure credit and debit card transactions against data theft and fraud.

Health Insurance Portability and Accountability Act (HIPAA)
a U.S. law that requires the protection of sensitive patient health information. HIPAA prohibits the disclosure of a person's medical information without their knowledge and consent.

Security assessments and audits

Meeting compliance standards is usually a continual, two-part process of security audits and assessments:

- A **security audit** is a review of an organization's security controls, policies, and procedures against a set of expectations.
- A **security assessment** is a check to determine how resilient current security implementations are against threats.

Fundamentals of cryptography

Cryptography is the process of transforming information into a form that unintended readers can't understand.

Data of any kind is kept secret using a two-step process: **encryption to hide the information, and decryption to unhide it.**

An **algorithm** is a set of rules that solve a problem. Specifically in cryptography, a cipher is an algorithm that encrypts information.

A **cryptographic key** is a mechanism that decrypts ciphertext.

Public key infrastructure

PKI, is an encryption framework that secures the exchange of information online. It's a broad system that makes accessing information fast, easy, and secure.

- **Symmetric encryption** is the use of a single secret key to exchange information. Because it uses one key for encryption and decryption, the sender and receiver must know the secret key to lock or unlock the cipher.
- **Asymmetric encryption** is the use of a public and private key pair for encryption and decryption of data. It uses two separate keys: a public

key and a private key. The public key is used to encrypt data, and the private key decrypts it. The private key is only given to users with authorized access.

Approved algorithms

Many web applications use a combination of symmetric and asymmetric encryption. This is how they balance user experience with safeguarding information. As an analyst, you should be aware of the most widely-used algorithms.

Symmetric algorithms

- *Triple DES (3DES)* is known as a block cipher because of the way it converts plaintext into ciphertext in "blocks." Its origins trace back to the Data Encryption Standard (DES), which was developed in the early 1970s. DES was one of the earliest symmetric encryption algorithms that generated 64-bit keys. A **bit** is the smallest unit of data measurement on a computer. As you might imagine, Triple DES generates keys that are 192 bits, or three times as long. Despite the longer keys, many organizations are moving away from using Triple DES due to limitations on the amount of data that can be encrypted. However, Triple DES is likely to remain in use for backwards compatibility purposes.

- *Advanced Encryption Standard (AES)* is one of the most secure symmetric algorithms today. AES generates keys that are 128, 192, or 256 bits. Cryptographic keys of this size are considered to be safe from brute force attacks. It's estimated that brute forcing an AES 128-bit key could take a modern computer billions of years!

Asymmetric algorithms

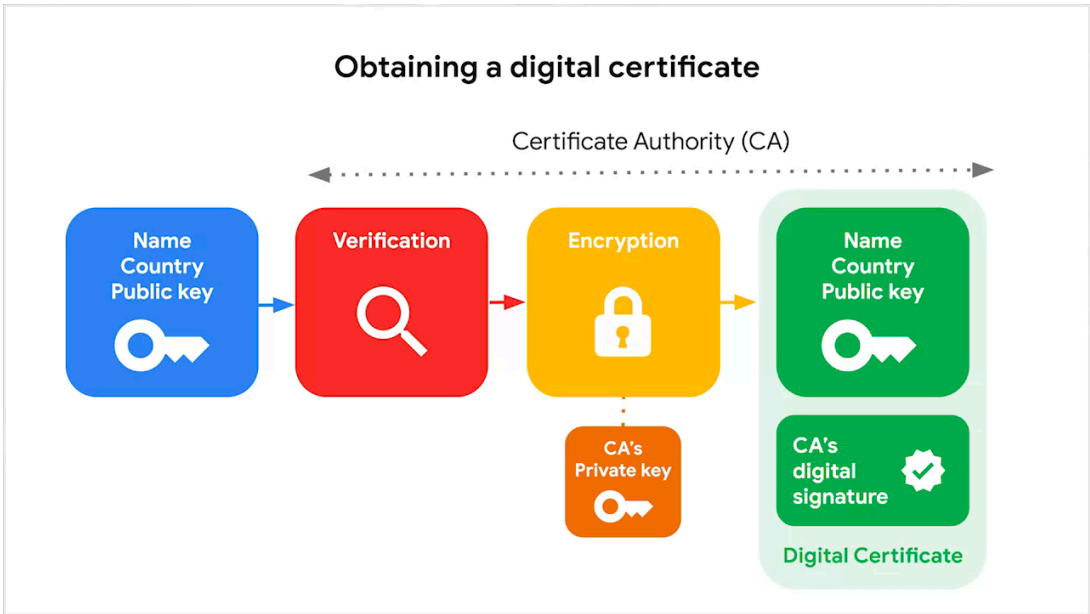
- *Rivest Shamir Adleman (RSA)* is named after its three creators who developed it while at the Massachusetts Institute of Technology (MIT). RSA is one of the first asymmetric encryption algorithms that produces a public and private key pair. Asymmetric algorithms like RSA produce even longer key lengths. In part, this is due to the fact that these functions are creating two keys. RSA key sizes are 1,024, 2,048, or 4,096 bits. RSA is mainly used to protect highly sensitive data.

- *Digital Signature Algorithm (DSA)* is a standard asymmetric algorithm that was introduced by NIST in the early 1990s. DSA also generates key lengths of 2,048 bits. This algorithm is widely used today as a complement to RSA in public key infrastructure.

Pro tip: A cryptographic system *should not* be considered secure if it requires secrecy around how it works.

PKI uses both asymmetric and symmetric encryption, sometimes in conjunction with one another. It all depends on whether speed or security is the priority.

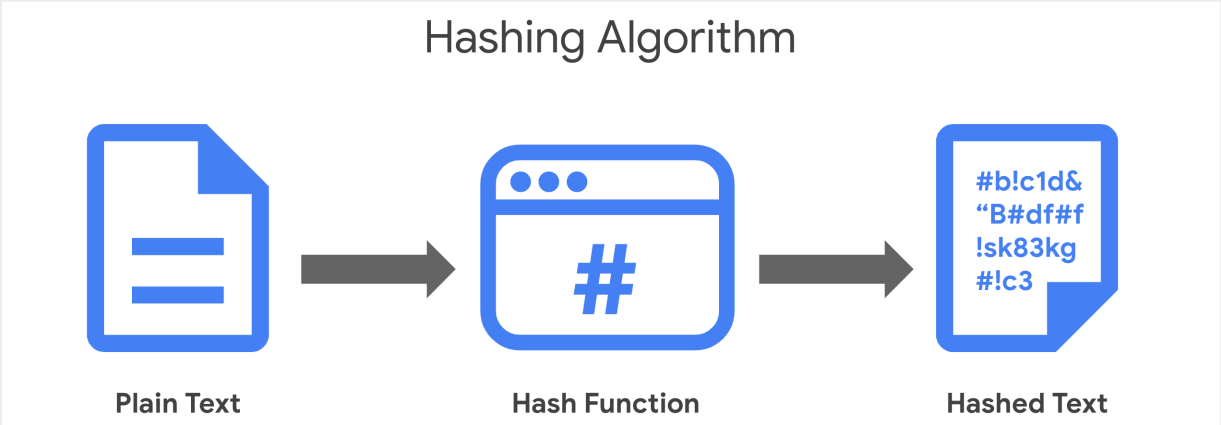
A **digital certificate** is a file that verifies the identity of a public key holder.



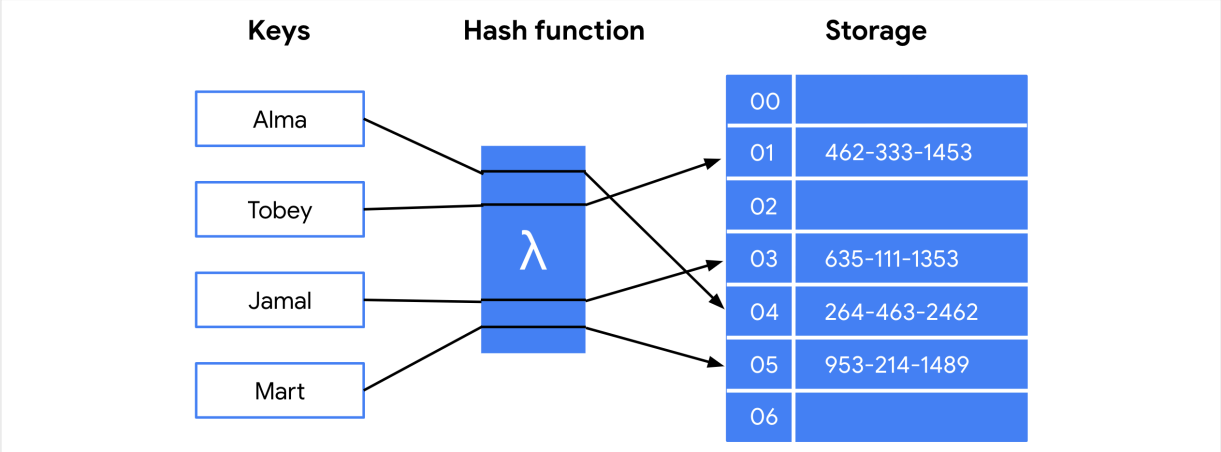
Non-repudiation and hashing

A hash function is an algorithm that produces a code that can't be decrypted. Unlike asymmetric and symmetric algorithms, hash functions are one-way processes that do not generate decryption keys.

Data integrity relates to the accuracy and consistency of information. This is known as **non-repudiation**, the concept that authenticity of information can't be denied.



Here is an example of how plaintext gets turned into hash values:



MD5 values are limited to 32 characters in length. Due to the limited output size, the algorithm is considered to be vulnerable to **hash collision**, an instance when different inputs produce the same hash value.

- a hash collision is similar to copying someone’s identity

Rainbow tables

A **rainbow table** is a file of pre-generated hash values and their associated plaintext. They’re like dictionaries of weak passwords. Attackers capable of obtaining an organization’s password database can use a rainbow table to compare them against all possible values.

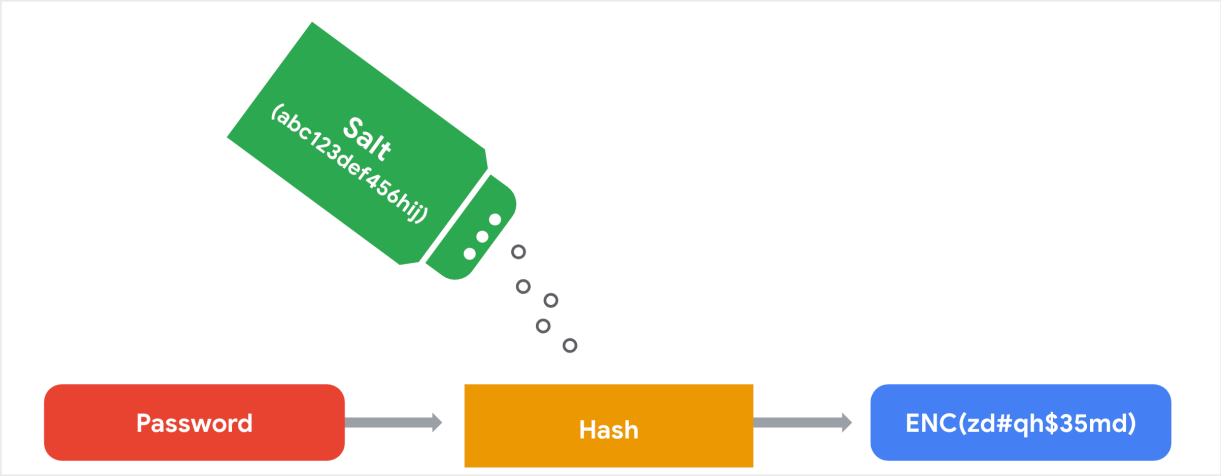
Adding some “salt”

Functions with larger digests are less vulnerable to collision and rainbow table attacks. But as you’re learning, no security control is perfect.

Salting is an additional safeguard that's used to strengthen hash functions. A *salt* is a random string of characters that's added to data before it's hashed. The additional characters produce a more unique hash value, making salted data resilient to rainbow table attacks.

For example, a database containing passwords might have several hashed entries for the password "password." If those passwords were all salted, each entry would

be completely different. That means an attacker using a rainbow table would be unable to find matching values for "password" in the database.



AAA Framework

- **Authentication**
- **Authorization**
- **Accounting**

Authentication

are access controls that serve a very basic purpose. They ask anything attempting to access information this simple question: who are you?

- Authentication by knowledge refers to something the user knows
- Another factor is ownership, referring to something the user possesses.
- Authentication by this factor is something the user is

SSO

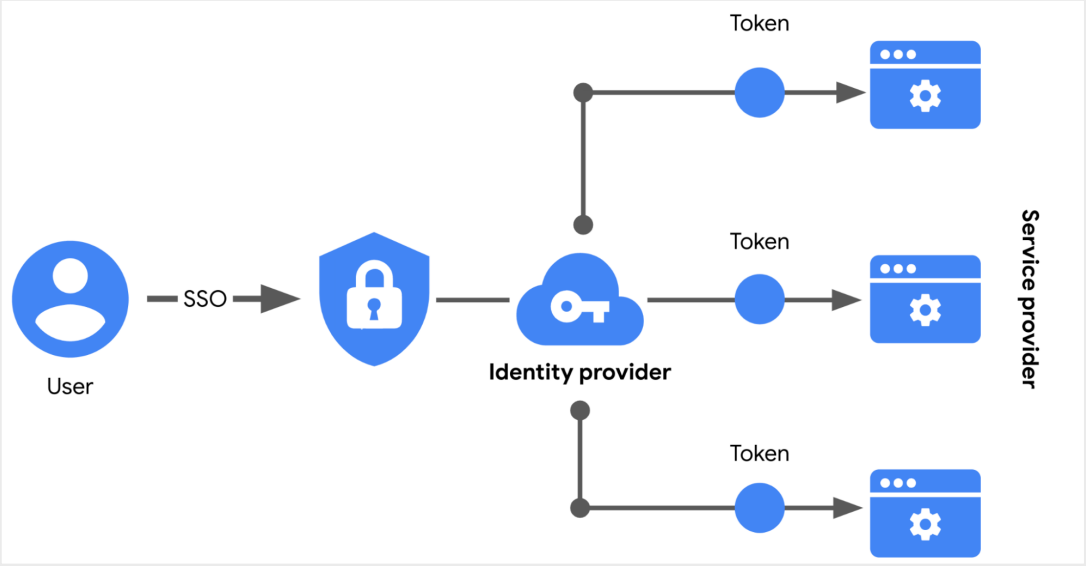
Single sign-on, or SSO, is a technology that combines several different logins into one.

- SSO establishes their identity once, allowing them to gain access to company resources faster.
- While SSO systems are helpful when it comes to speeding up the authentication process, they present a significant vulnerability when used alone.

More companies are turning to SSO as a solution to their authentication needs for three reasons:

1. **SSO improves the user experience** by eliminating the number of usernames and passwords people have to remember.
2. **Companies can lower costs** by streamlining how they manage

connected services.
3. **SSO improves overall security** by reducing the number of access points attackers can target.



MFA
is a security measure, which requires a user to verify their identity in two or more ways to access a system or network.

Authorization

Authorization is linked to the idea that access to information only lasts as long as needed.
Authorization systems are also heavily influenced by this idea in addition to another important security principle, the separation of duties.

Basic auth works by sending an identifier every time a user communicates with a web page.

OAuth is an open-standard authorization protocol that shares designated access between applications. For example, you can tell Google that it's okay for another

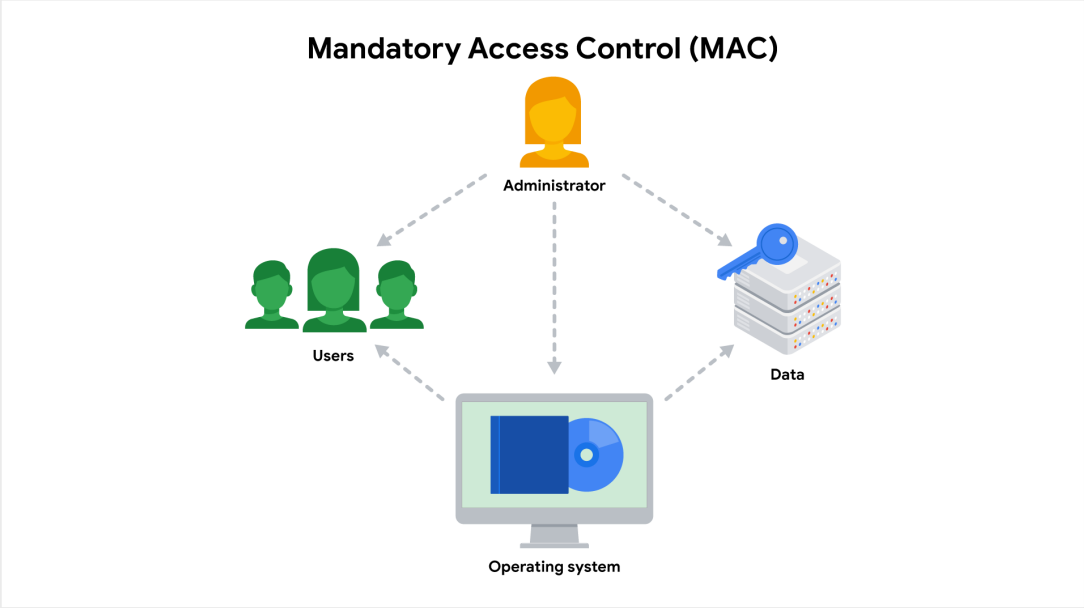
website to access your profile to create an account.

An **API token** is a small block of encrypted code that contains information about a user. These tokens contain things like your identity, site permissions, and more. OAuth sends and receives access requests using API tokens by passing them from a server to a user's device.

Granting authorization

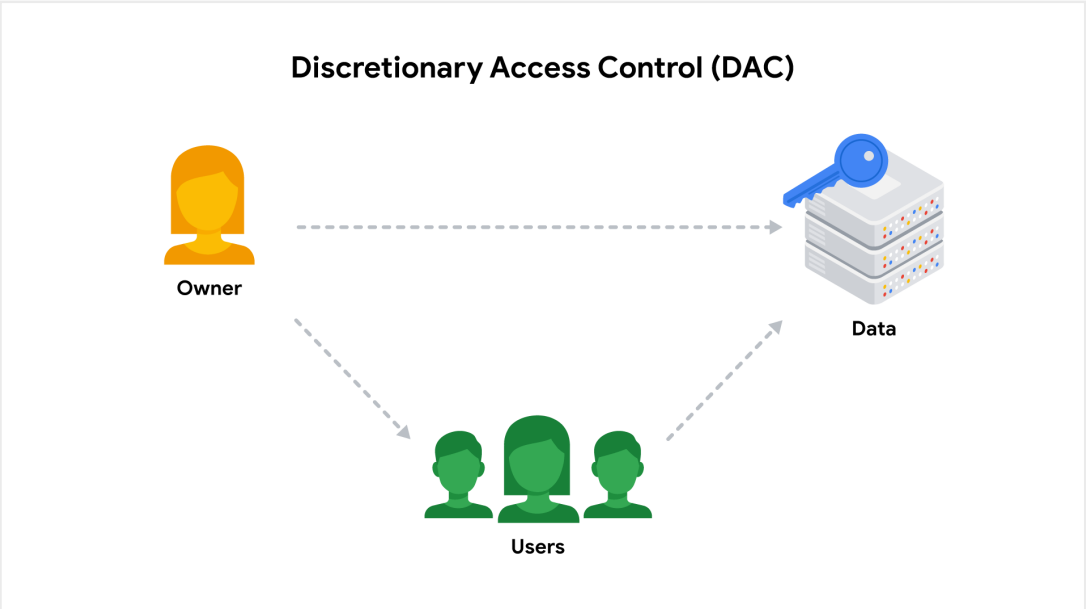
If the right user has been authenticated, the network should ensure the right resources are made available. There are three common frameworks that organizations use to handle this step of IAM:

- Mandatory access control (MAC)
- Discretionary access control (DAC)
- Role-based access control (RBAC)

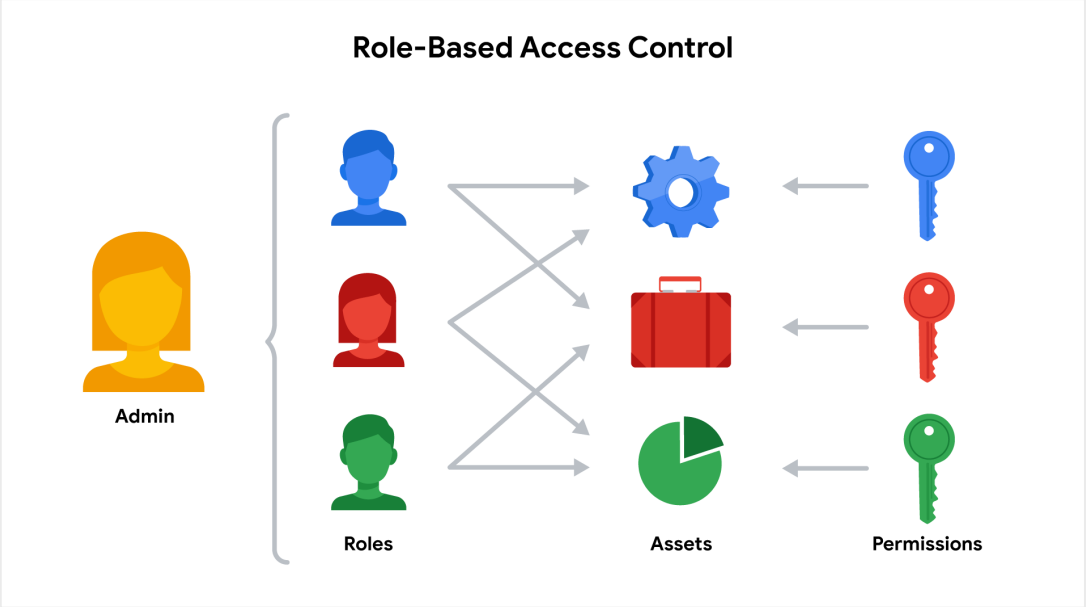


Mandatory Access Control (MAC)

MAC is the strictest of the three frameworks. Authorization in this model is based on a strict need-to-know basis. Access to information must be granted manually by a central authority or system administrator. For example, MAC is commonly applied in law enforcement, military, and other government agencies where users must request access through a chain of command. MAC is also known as non-discretionary control because access isn't given at the discretion of the data owner.



Discretionary Access Control (DAC)
DAC is typically applied when a data owner decides appropriate levels of access. One example of DAC is when the owner of a Google Drive folder shares editor, viewer, or commentor access with someone else.



Role-Based Access Control (RBAC)
RBAC is used when authorization is determined by a user's role within an organization. For example, a user in the marketing department may have access to user analytics but not network administration.

Accounting

Accounting is the practice of monitoring the access logs of a system. These logs contain information like who accessed the system, and when they

accessed it, and what resources they used.

Two actions are triggered when the session begins:
The first is the creation of a session ID. A session ID is a unique token that identifies a user and their device while accessing the system. Session IDs are attached to the user until they either close their browser or the session times out.

Session hijacking is an event when attackers obtain a legitimate user's session ID. During these kinds of attacks, cyber criminals impersonate the user, causing all sorts of harm. Money or private data can be stolen.

Vulnerability Management

In security, an **exploit** is a way of taking advantage of a vulnerability.

- Homes have vulnerable systems that can be exploited by a burglar
- A burglar can exploit this vulnerability by using a rock to break the window.

Security teams spend a lot of time finding vulnerabilities and thinking of how they can be exploited

Vulnerability management is the process of finding and patching vulnerabilities.

- Vulnerability management helps keep assets safe.

Vulnerability management is a four step process.

1. The first step is to identify vulnerabilities.
2. The next step is to consider potential exploits of those vulnerabilities.
3. Third is to prepare defenses against threats.
4. And finally, the fourth step is to evaluate those defenses.

When the last step ends, the process starts again.

A **zero-day** is an exploit that was previously unknown.
The term zero-day refers to the fact that the exploit is happening in real time with zero days to fix it.

Defense in depth

It's a layered approach to vulnerability management that reduces risk.

The defense in depth concept can be used to protect any asset. It's mainly used in cybersecurity to protect information using a **five layer design.**

1. Perimeter layer - to only allow access to trusted partners to reach the

next layer of defense
2. Network layer - made up of other technologies like network firewalls and others.
3. Endpoint layer - the devices that have access on a network
4. Application layer - all the interfaces that are used to interact with technology
5. Data layer - the critical data that must be protected

The common vulnerabilities and exposures list, or CVE list is an openly accessible dictionary of known vulnerabilities and exposures. It is a popular resource.

OWASP is a nonprofit foundation that works to improve the security of software. OWASP is an open platform that security professionals from around the world use to share information, tools, and events that are focused on securing the web.

Common Vulnerabilities

Broken access control

Access controls limit what users can do in a web application. For example, a blog might allow visitors to post comments on a recent article but restricts them from deleting the article entirely. Failures in these mechanisms can lead to unauthorized information disclosure, modification, or destruction. They can also give someone unauthorized access to other business applications.

Cryptographic failures

Information is one of the most important assets businesses need to protect. Privacy laws such as General Data Protection Regulation (GDPR) require sensitive data to be protected by effective encryption methods. Vulnerabilities can occur when businesses fail to encrypt things like personally identifiable information (PII). For example, if a web application uses a weak hashing algorithm, like MD5, it’s more at risk of suffering a data breach.

Injection

Injection occurs when malicious code is inserted into a vulnerable application. Although the app appears to work normally, it does things that it wasn’t intended to do. Injection attacks can give threat actors a backdoor into an organization’s information system. A common target is a website’s login form. When these forms are vulnerable to injection, attackers can insert malicious code that gives them access to modify or steal user credentials.

Insecure design

Applications should be designed in such a way that makes them resilient to attack. When they aren’t, they’re much more vulnerable to threats like injection attacks or malware infections. Insecure design refers to a wide range of missing or poorly implemented security controls that should have been programmed into an application when it was being developed.

Security misconfiguration
Misconfigurations occur when security settings aren’t properly set or maintained. Companies use a variety of different interconnected systems. Mistakes often happen when those systems aren’t properly set up or audited. A common example is when businesses deploy equipment, like a network server, using default settings. This can lead businesses to use settings that fail to address the organization's security objectives.

Vulnerable and outdated components
Vulnerable and outdated components is a category that mainly relates to application development. Instead of coding everything from scratch, most developers use open-source libraries to complete their projects faster and easier. This publicly available software is maintained by communities of programmers on a volunteer basis. Applications that use vulnerable components that have not been maintained are at greater risk of being exploited by threat actors.

Identification and authentication failures
Identification is the keyword in this vulnerability category. When applications fail to recognize who should have access and what they’re authorized to do, it can lead to serious problems. For example, a home Wi-Fi router normally uses a simple login form to keep unwanted guests off the network. If this defense fails, an attacker can invade the homeowner’s privacy.

Software and data integrity failures
Software and data integrity failures are instances when updates or patches are inadequately reviewed before implementation. Attackers might exploit these weaknesses to deliver malicious software. When that occurs, there can be serious downstream effects. Third parties are likely to become infected if a single system is compromised, an event known as a supply chain attack.

Security logging and monitoring failures
In security, it’s important to be able to log and trace back events. Having a record of events like user login attempts is critical to finding and fixing problems. Sufficient monitoring and incident response is equally important.

Server-side request forgery
Companies have public and private information stored on web servers. When you use a hyperlink or click a button on a website, a request is sent to a server that

should validate who you are, fetch the appropriate data, and then return it to you.

Server-side request forgeries (SSRFs) are when attackers manipulate the normal operations of a server to read or update other resources on that server. These are possible when an application on the server is vulnerable. Malicious code can be carried by the vulnerable app to the host server that will fetch unauthorized data.

OSINT

OSINT is the collection and analysis of information from publicly available sources to generate usable intelligence. It's commonly used to support cybersecurity activities, like identifying potential threats and vulnerabilities.

Information refers to the collection of raw data or facts about a specific subject. *Intelligence*, on the other hand, refers to the analysis of information to produce knowledge or insights that can be used to support decision-making.

Here are some of the ways OSINT can be used to generate intelligence:

- To provide insights into cyber attacks
- To detect potential data exposures
- To evaluate existing defenses
- To identify unknown vulnerabilities

OSINT tools

There's an enormous amount of open-source information online. Finding relevant information that can be used to gather intelligence is a challenge. Information can be gathered from a variety of sources, such as search engines, social media, discussion boards, blogs, and more. Several tools also exist that can be used in your intelligence gathering process. Here are just a few examples of tools that you can explore:

- VirusTotal
  is a service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content.
- MITRE ATT&CK®
  is a knowledge base of adversary tactics and techniques based on real-world observations.
- OSINT Framework
  is a web-based interface where you can find OSINT tools for almost any kind of source or platform.
- Have I been Pwned
  is a tool that can be used to search for breached email accounts.

Approaches to vulnerability scanning

vulnerability assessment, which is the internal review process of an organization's security systems. An organization performs vulnerability assessments to identify weaknesses and prevent attacks.

A **vulnerability scanner** is software that automatically compares known vulnerabilities and exposures against the technologies on the network. In general, these tools scan systems to find misconfigurations or programming flaws.

External and internal scans simulate an attacker's approach.
External scans test the perimeter layer outside of the internal network. They analyze outward facing systems, like websites and firewalls. These kinds of scans can uncover vulnerable things like vulnerable network ports or servers.

Internal scans start from the opposite end by examining an organization's internal systems. For example, this type of scan might analyze application software for weaknesses in how it handles user input.

Authenticated vs. unauthenticated
Authenticated and unauthenticated scans simulate whether or not a user has access to a system.
Authenticated scans might test a system by logging in with a real user account or even with an admin account. These service accounts are used to check for vulnerabilities, like broken access controls.

Unauthenticated scans simulate external threat actors that do not have access to your business resources. For example, a scan might analyze file shares within the organization that are used to house internal-only documents. Unauthenticated

users should receive "access denied" results if they tried opening these files. However, a vulnerability would be identified if you were able to access a file.

Limited vs. comprehensive
Limited and comprehensive scans focus on particular devices that are accessed by internal and external users.
Limited scans analyze particular devices on a network, like searching for misconfigurations on a firewall.

Comprehensive scans analyze all devices connected to a network. This includes operating systems, user databases, and more.

Importance of updates

A **patch update** is a software and operating system update that addresses security vulnerabilities within a program or product. Patches usually contain bug fixes that address common security vulnerabilities and exposure

Penetration testing

A **penetration test**, or pen test, is a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes. The simulated attack in a pen test involves using the same tools and techniques as malicious actors in order to mimic a real life attack. Since a pen test is an authorized attack, it is considered to be a form of ethical hacking.

These authorized attacks are performed by pen testers who are skilled in programming and network architecture.
Depending on their objectives, organizations might use a few different approaches to penetration testing:

- **Red team** tests *simulate attacks* to identify vulnerabilities in systems, networks, or applications.
- **Blue team** tests focus on *defense and incident response* to validate an organization's existing security systems.
- **Purple team** tests are *collaborative*, focusing on improving the security posture of the organization by combining elements of red and blue team exercises.

Penetration testing strategies
There are three common penetration testing strategies:

- **Open-box testing** is when the tester has the same privileged access that an internal developer would have—information like system architecture, data flow, and network diagrams. This strategy goes by several different names, including internal, full knowledge, white-box, and clear-box penetration testing.
- **Closed-box testing** is when the tester has little to no access to internal systems—similar to a malicious hacker. This strategy is sometimes referred to as external, black-box, or zero knowledge penetration testing.
- **Partial knowledge testing** is when the tester has limited access and knowledge of an internal system—for example, a customer service representative. This strategy is also known as gray-box testing.

Protect all entry points

To position themselves ahead of threats and make the most of their limited resources, companies start by understanding the environment surrounding their operations. An important part of this is getting a sense of their attack surface.

An **attack surface** is all the potential vulnerabilities that a threat actor could exploit. Analyzing the attack surface is usually the first thing security teams do.

Being prepared for anything

Applying an **attacker mindset** is a lot like conducting an experiment. It's about causing problems in a controlled environment and evaluating the outcome to gain insights. Adopting an attacker mindset is a beneficial skill in security because it offers a different perspective about the challenges you're trying to solve. The insights you gain can be valuable when it's time to establish a security plan or modify an existing one.

Simulating threats

One method of applying an attacker mindset is using attack simulations. These activities are normally performed in one of two ways: *proactively* and *reactively*. Both approaches share a common goal, which is to make systems safer.

- *Proactive simulations* assume the role of an attacker by exploiting vulnerabilities and breaking through defenses. This is sometimes called a red team exercise.
- *Reactive simulations* assume the role of a defender responding to an attack. This is sometimes called a blue team exercise.

Threat actors

A **threat actor** is any person or group who presents a security risk. This broad definition refers to people inside and outside an organization. It also includes individuals who intentionally pose a threat, and those that accidentally put assets at risk. That’s a wide range of people!

Threat actors are normally divided into five categories based on their motivations:

- **Competitors** refers to rival companies who pose a threat because they might benefit from leaked information.
- **State actors** are government intelligence agencies.
- **Criminal syndicates** refer to organized groups of people who make money from criminal activity.
- **Insider threats** can be any individual who has or had authorized access to an organization’s resources. This includes employees who accidentally compromise assets or individuals who purposefully put them at risk for their own benefit.
- **Shadow IT** refers to individuals who use technologies that lack IT governance. A common example is when an employee uses their personal email to send work-related communications.

By definition, a **hacker** is any person who uses computers to gain unauthorized access to computer systems, networks, or data.

Access points

Each threat actor has a unique motivation for targeting an organization's assets. Keeping them out takes more than knowing their intentions and capabilities. It’s also important to recognize the types of attack vectors they’ll use.

For the most part, threat actors gain access through one of these attack vector categories:

- **Direct access**, referring to instances when they have physical access to a system
- **Removable media**, which includes portable hardware, like USB flash drives
- **Social media platforms** that are used for communication and content sharing
- **Email**, including both personal and business accounts
- **Wireless networks** on premises
- **Cloud services** usually provided by third-party organizations
- **Supply chains** like third-party vendors that can present a backdoor into systems

A matter of trial and error

One way of opening a closed lock is trying as many combinations as possible. Threat actors sometimes use similar tactics to gain access to an application or a network.

Attackers use a variety of tactics to find their way into a system:

- *Simple brute force attacks* are an approach in which attackers guess a user's login credentials. They might do this by entering any combination of username and password that they can think of until they find the one that works.
- *Dictionary attacks* are a similar technique except in these instances attackers use a list of commonly used credentials to access a system. This list is similar to matching a definition to a word in a dictionary.
- *Reverse brute force attacks* are similar to dictionary attacks, except they start with a single credential and try it in various systems until a match is found.
- *Credential stuffing* is a tactic in which attackers use stolen login credentials from previous data breaches to access user accounts at another organization. A specialized type of credential stuffing is called *pass the hash*. These attacks reuse stolen, unsalted hashed credentials to trick an authentication system into creating a new authenticated user session on the network.

Tools of the trade

There are so many combinations that can be used to create a single set of login credentials. The number of characters, letters, and numbers that can be mixed together is truly incredible. When done manually, it could take someone years to try every possible combination.

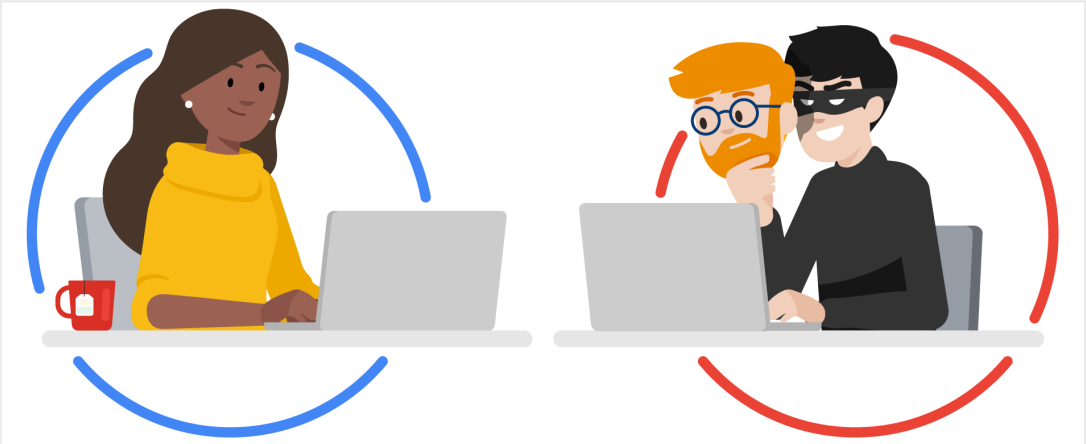
Instead of dedicating the time to do this, attackers often use software to do the guess work for them. These are some common brute forcing tools:

- Aircrack-ng
- Hashcat
- John the Ripper
- Ophcrack
- THC Hydra

Sometimes, security professionals use these tools to test and analyze their own systems. They each serve different purposes. For example, you might use Aircrack-ng to test a Wi-Fi network for vulnerabilities to brute force attack.

Social Engineering Tactics

social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. It's an umbrella term that can apply to a broad range of attacks. Each technique is designed to capitalize on the trusting nature of people and their willingness to help.



Signs of an attack

Oftentimes, people are unable to tell that an attack is happening until it's too late. Social engineering is such a dangerous threat because it typically allows attackers to bypass technological defenses that are in their way. Although these threats are difficult to prevent, recognizing the signs of social engineering is a key to reducing the likelihood of a successful attack.

These are common types of social engineering to watch out for:

- **Baiting** is a social engineering tactic that tempts people into compromising their security. A common example is USB baiting that relies on someone finding an infected USB drive and plugging it into their device.
- **Phishing** is the use of digital communications to trick people into revealing sensitive data or deploying malicious software. It is one of the most common forms of social engineering, typically performed via email.
- **Quid pro quo** is a type of baiting used to trick someone into believing that they'll be rewarded in return for sharing access, information, or money. For example, an attacker might impersonate a loan officer at a bank and call customers offering them a lower interest rate on their credit card. They'll tell the customers that they simply need to provide their account details to claim the deal.
- **Tailgating** is a social engineering tactic in which unauthorized people follow an authorized person into a restricted area. This technique is also

sometimes referred to as piggybacking.
- **Watering hole** is a type of attack when a threat actor compromises a website frequently visited by a specific group of users. Oftentimes, these watering hole sites are infected with malicious software. An example is the *Holy Water attack of 2020* that infected various religious, charity, and volunteer websites.

Encouraging caution

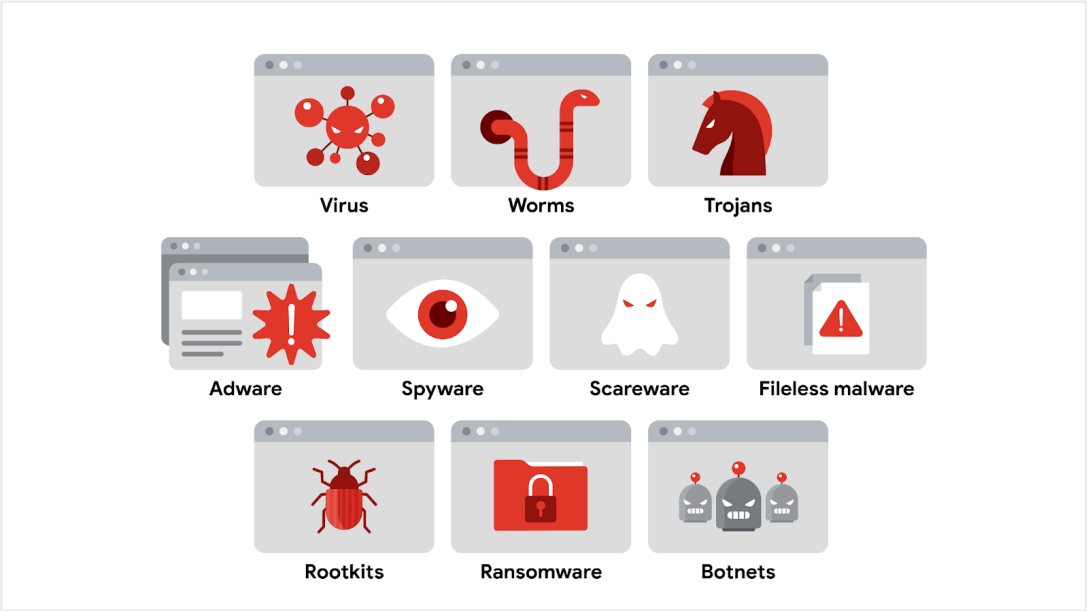
Spreading awareness usually starts with comprehensive security training. When it comes to social engineering, there are three main areas to focus on when teaching others:

- **Stay alert** of suspicious communications and unknown people, especially when it comes to email. For example, look out for spelling errors and double-check the sender's name and email address.
- **Be cautious** about sharing information, especially over social media. Threat actors often search these platforms for any information they can use to their advantage.
- **Control curiosity** when something seems too good to be true. This can include wanting to click on attachments or links in emails and advertisements.

A number of techniques began to appear around this time period, many of which are still used today. There are five common types of phishing that every security analyst should know:

- **Email phishing** is a type of attack sent via email in which threat actors send messages pretending to be a trusted person or entity.
- **Smishing** is a type of phishing that uses Short Message Service (SMS), a technology that powers text messaging. Smishing covers all forms of text messaging services, including Apple’s iMessages, WhatsApp, and other chat mediums on phones.
- **Vishing** refers to the use of voice calls or voice messages to trick targets into providing personal information over the phone.
- **Spear phishing** is a subset of email phishing in which specific people are purposefully targeted, such as the accountants of a small business.
- **Whaling** refers to a category of spear phishing attempts that are aimed at high-ranking executives in an organization.

Malware



Virus

A **virus** is malicious code written to interfere with computer operations and cause damage to data and software. This type of malware must be installed by the target user before it can spread itself and cause damage. One of the many ways that viruses are spread is through phishing campaigns where malicious links are hidden within links or attachments.

Worm

A **worm** is malware that can duplicate and spread itself across systems on its own. Similar to a virus, a worm must be installed by the target user and can also be spread with tactics like malicious email. Given a worm's ability to spread on its own, attackers sometimes target devices, drives, or files that have shared access over a network.

A well known example is the Blaster worm, also known as Lovesan, Lovsan, or MSBlast. In the early 2000s, this worm spread itself on computers running Windows XP and Windows 2000 operating systems. It would force devices into a continuous loop of shutting down and restarting. Although it did not damage the infected devices, it was able to spread itself to hundreds of thousands of users around the world. Many variants of the Blaster worm have been deployed since the original and can infect modern computers.

Note: Worms were very popular attacks in the mid 2000s but are less frequently used in recent years.

Trojan

A trojan, also called a **Trojan horse**, is malware that looks like a legitimate file or program. This characteristic relates to how trojans are spread. Similar to viruses,

attackers deliver this type of malware hidden in file and application downloads. Attackers rely on tricking unsuspecting users into believing they're downloading a harmless file, when they're actually infecting their own device with malware that can be used to spy on them, grant access to other devices, and more.

Adware

Advertising-supported software, or **adware**, is a type of legitimate software that is sometimes used to display digital advertisements in applications. Software developers often use adware as a way to lower their production costs or to make their products free to the public—also known as freeware or shareware. In these instances, developers monetize their product through ad revenue rather than at the expense of their users.

Malicious adware falls into a sub-category of malware known as a **potentially unwanted application (PUA)**. A PUA is a type of unwanted software that is bundled in with legitimate programs which might display ads, cause device slowdown, or install other software. Attackers sometimes hide this type of malware in freeware with insecure design to monetize ads for themselves instead of the developer. This works even when the user has declined to receive ads.

Spyware

Spyware is malware that's used to gather and sell information without consent. It's also considered a PUA. Spyware is commonly hidden in *bundleware*, additional software that is sometimes packaged with other applications. PUAs like spyware have become a serious challenge in the open-source software development ecosystem. That's because developers tend to overlook how their software could be misused or abused by others.

Scareware

Another type of PUA is **scareware**. This type of malware employs tactics to frighten users into infecting their own device. Scareware tricks users by displaying fake warnings that appear to come from legitimate companies. Email and pop-ups are just a couple of ways scareware is spread. Both can be used to deliver phony warnings with false claims about the user's files or data being at risk.

Fileless malware

Fileless malware does not need to be installed by the user because it uses legitimate programs that are already installed to infect a computer. This type of infection resides in memory where the malware never touches the hard drive. This is unlike the other types of malware, which are stored within a file on disk. Instead, these stealthy infections get into the operating system or hide within trusted applications.

Pro tip: Fileless malware is detected by performing memory analysis, which

requires experience with operating systems.

Rootkits

A **rootkit** is malware that provides remote, administrative access to a computer. Most attackers use rootkits to open a backdoor to systems, allowing them to install other forms of malware or to conduct network security attacks.
This kind of malware is often spread by a combination of two components: a dropper and a loader. A **dropper** is a type of malware that comes packed with malicious code which is delivered and installed onto a target system. For example, a dropper is often disguised as a legitimate file, such as a document, an image, or an executable to deceive its target into opening, or dropping it, onto their device. If the user opens the dropper program, its malicious code is executed and it hides itself on the target system.
Multi-staged malware attacks, where multiple packets of malicious code are deployed, commonly use a variation called a loader. A **loader** is a type of malware that downloads strains of malicious code from an external source and installs them onto a target system. Attackers might use loaders for different purposes, such as to set up another type of malware---a botnet.

Botnet

A **botnet**, short for “robot network,” is a collection of computers infected by malware that are under the control of a single threat actor, known as the “bot-herder.” Viruses, worms, and trojans are often used to spread the initial infection and turn the devices into a bot for the bot-herder. The attacker then uses file sharing, email, or social media application protocols to create new bots and grow the botnet. When a target unknowingly opens the malicious file, the computer, or bot, reports the information back to the bot-herder, who can execute commands on the infected computer.

Ransomware

Ransomware describes a malicious attack where threat actors encrypt an organization's data and demand payment to restore access. According to the Cybersecurity and Infrastructure Security Agency (CISA), ransomware crimes are on the rise and becoming increasingly sophisticated. Ransomware infections can cause significant damage to an organization and its customers.

Cryptojacking is a form of malware that installs software to illegally mine cryptocurrencies.
sign of a cryptojacking infection is:

- Slowdown
- CPU usage
- sudden system crashes

- fast draining batteries
- high electricity costs related to the resource- intensive process of crypto mining.

A common and dangerous type of injection attack that's a threat to web apps is cross-site scripting.

Cross site scripting, or XSS, is an injection attack that inserts code into a vulnerable website or web application.

- Give cybercriminals access to everything that loads on the infected web page.
- This can include session cookies, geolocation, and even webcams and microphones.

Stored XSS attack is an instance when malicious script is injected directly on the server.

- Attackers target elements of a site that are served to the user.
- This could be things like images and buttons that load when the site is visited

A **DOM-based XSS attack** is an instance when malicious script exists in the web page a browser loads.

- Unlike reflected XSS, these attacks don't need to be sent to the server to activate.
- DOM-based attack, criminals change the parameter that's expecting an input.
    - For example, they could hide malicious JavaScript in the HTML tags.
    - The browser would process the HTML and execute the JavaScript.

SQL injection

is an attack that executes unexpected queries on a database. Like cross-site scripting, SQL injection occurs due to a lack of sanitized input.

- Threat actors perform SQL injections to modify, delete, or steal information from databases.

There are three main categories of SQL injection:

- In-band
- Out-of-band
- Inferential

In-band SQL Injection

In-band, or classic, SQL injection is the most common type. An in-band injection is one that uses the *same communication channel* to launch the attack and gather the results.

For example, this might occur in the search box of a retailer's website that lets customers find products to buy.

Out-of-band SQL Injection

An out-of-band injection is one that uses a *different communication channel* to launch the attack and gather the results.

For example, an attacker could use a malicious query to create a connection between a vulnerable website and a database they control. This separate channel would allow them to bypass any security controls that are in place on the website's server, allowing them to steal sensitive data

Inferential SQL Injection

Inferential SQL injection occurs when an attacker is unable to directly see the results of their attack. Instead, they can interpret the results by analyzing the *behavior* of the system.

For example, an attacker might perform a SQL injection attack on the login form of a website that causes the system to respond with an error message. Although sensitive data is not returned, the attacker can figure out the database's structure based on the error. They can then use this information to craft attacks that will give them access to sensitive data or to take control of the system.

Injection Prevention

A key to preventing SQL injection attacks is to *escape user inputs*—preventing someone from inserting any code that a program isn't expecting.

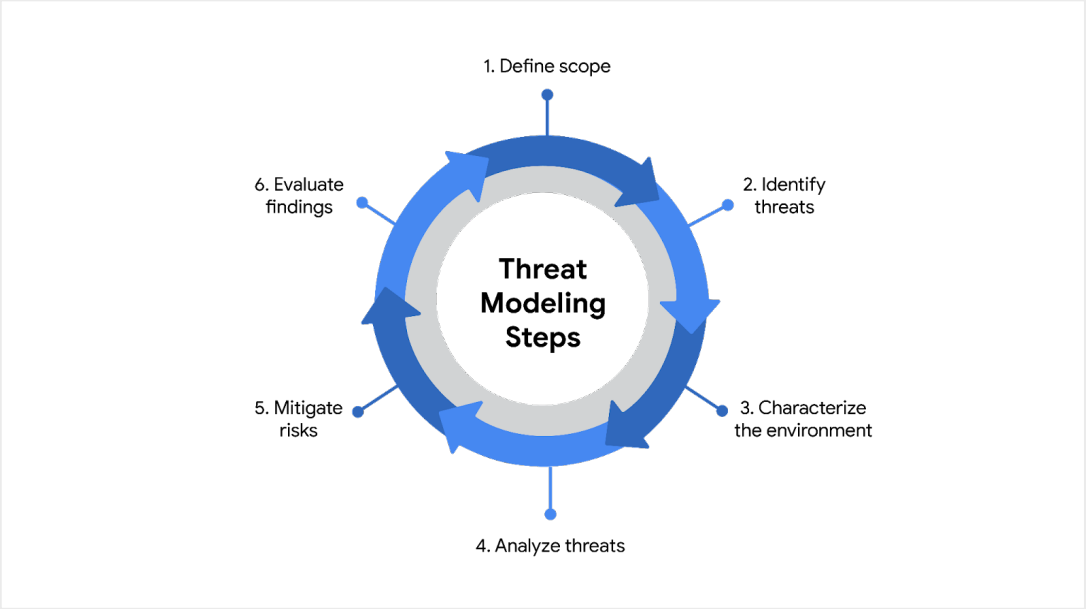
There are several ways to escape user inputs:

- **Prepared statements**: a coding technique that executes SQL statements before passing them on to a database
- **Input sanitization**: programming that removes user input which could be interpreted as code.
- **Input validation**: programming that ensures user input meets a system's expectations.

Threat modeling
is a process of identifying assets, their vulnerabilities, and how each is exposed to threats. We apply threat modeling to everything we protect. Entire systems, applications, or business processes all get examined from this security-related perspective.

Threat Modeling Steps:

1. Define the scope
2. Identify threats
3. Characterize the environmoent
4. Analyze threats
5. Mitigate risks
6. Evaluate Findings



Common Threat Modeling Frameworks

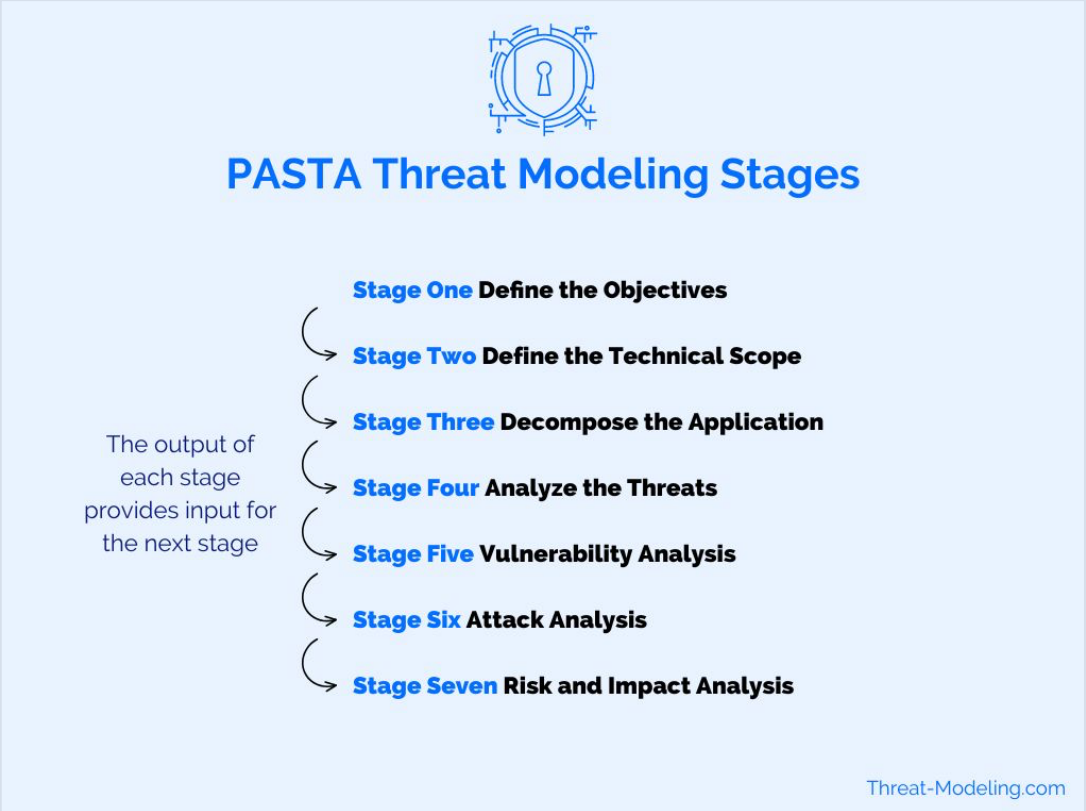
When performing threat modeling, there are multiple methods that can be used, such as:

- STRIDE
- PASTA
- Trike
- VAST

Stride
STRIDE is a threat-modeling framework developed by Microsoft. It's commonly used to identify vulnerabilities in six specific attack vectors. The acronym represents each of these vectors: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.

PASTA

The **Process of Attack Simulation and Threat Analysis** (PASTA) is a risk-centric threat modeling process developed by two OWASP leaders and supported by a cybersecurity firm called VerSprite. Its main focus is to discover evidence of viable threats and represent this information as a model.



Trike

Trike is an open source methodology and tool that takes a security-centric approach to threat modeling. It's commonly used to focus on security permissions, application use cases, privilege models, and other elements that support a secure environment.

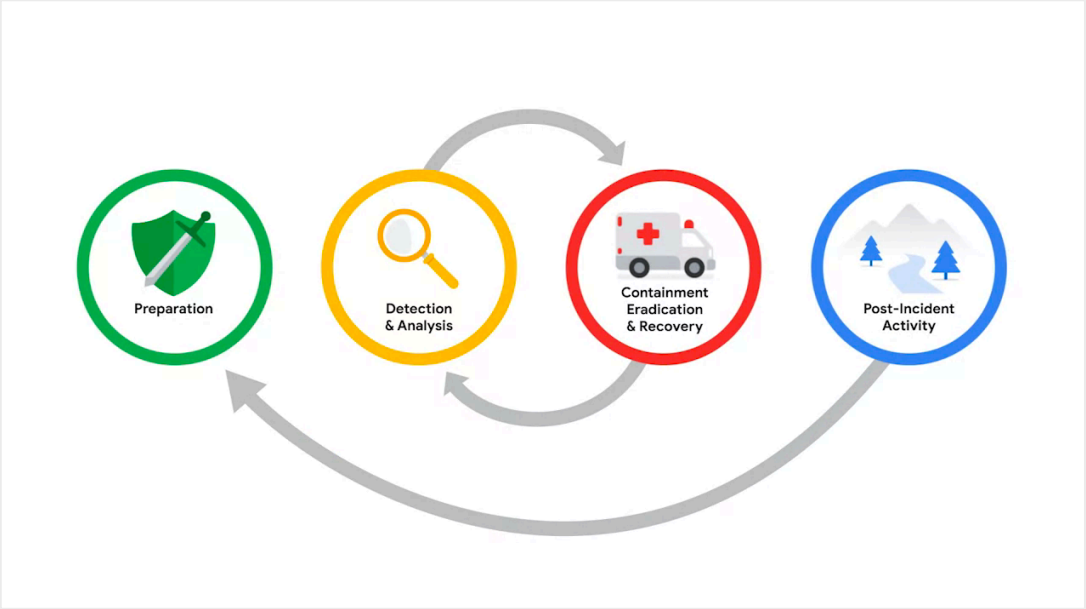
VAST

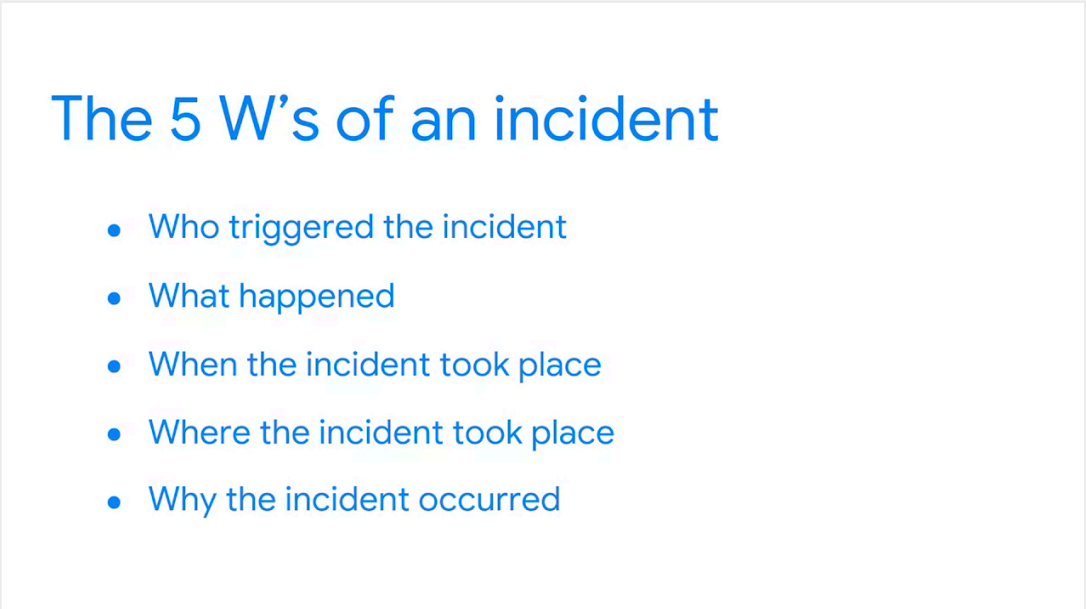
The Visual, Agile, and Simple Threat (VAST) Modeling framework is part of an automated threat-modeling platform called ThreatModeler®. Many security teams opt to use VAST as a way of automating and streamlining their threat modeling assessments.

Course 6: Sound the Alarm: Detection and Response

This course will explore the last three steps of this framework: detect, respond, and recover.

How to respond to Incident





Keeping track of this information is essential not only during an incident investigation, but also during the closure of an investigation when it comes time to write the final report. As an analyst, you'll need a method to document and reference this information for easy access when you need it.

A great way to do this is to use an **incident handler's journal**, which is a form of documentation used in incident response.

Incident Response Teams

Computer security incident response teams (CSIRT)

are a specialized group of security professionals that are trained in incident management and response. The goal of CSIRTs are to effectively and efficiently manage incidents, provide services and resources for response and recovery, and prevent future incidents from occurring.

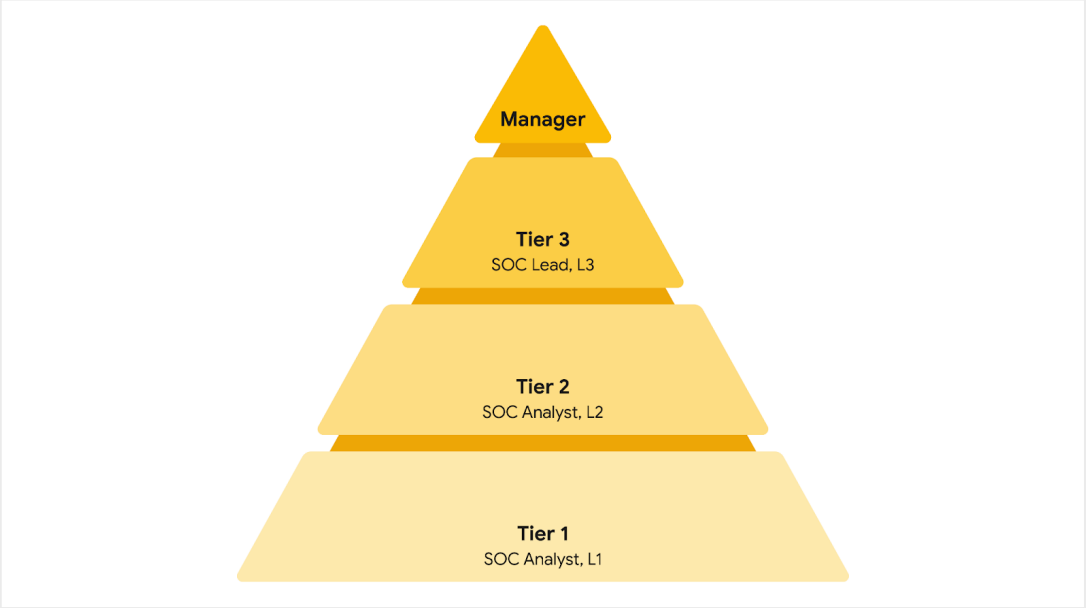
- **Command** refers to having the appropriate leadership and direction to oversee the response.
- **Control** refers to the ability to manage technical aspects during incident response, like coordinating resources and assigning tasks.
- **Communication** refers to the ability to keep stakeholders informed.

Roles in CSIRT

- Security analyst
- Technical lead
- Incident coordinator

SOC organization

A **security operations center (SOC)** is an organizational unit dedicated to monitoring networks, systems, and devices for security threats or attacks.
A SOC is composed of SOC analysts, SOC leads, and SOC managers. Each role has its own respective responsibilities. SOC analysts are grouped into three different tiers.



Tier 1 SOC analyst

The first tier is composed of the least experienced SOC analysts who are known as level 1s (L1s). They are responsible for:

- Monitoring, reviewing, and prioritizing alerts based on criticality or severity
- Creating and closing alerts using ticketing systems
- Escalating alert tickets to Tier 2 or Tier 3

Tier 2 SOC analyst

The second tier comprises the more experienced SOC analysts, or level 2s (L2s). They are responsible for:

- Receiving escalated tickets from L1 and conducting deeper investigations
- Configuring and refining security tools
- Reporting to the SOC Lead

Tier 3 SOC lead

The third tier of a SOC is composed of the SOC leads, or level 3s (L3s). These highly experienced professionals are responsible for:

- Managing the operations of their team
- Exploring methods of detection by performing advanced detection

techniques, such as malware and forensics analysis
- Reporting to the SOC manager

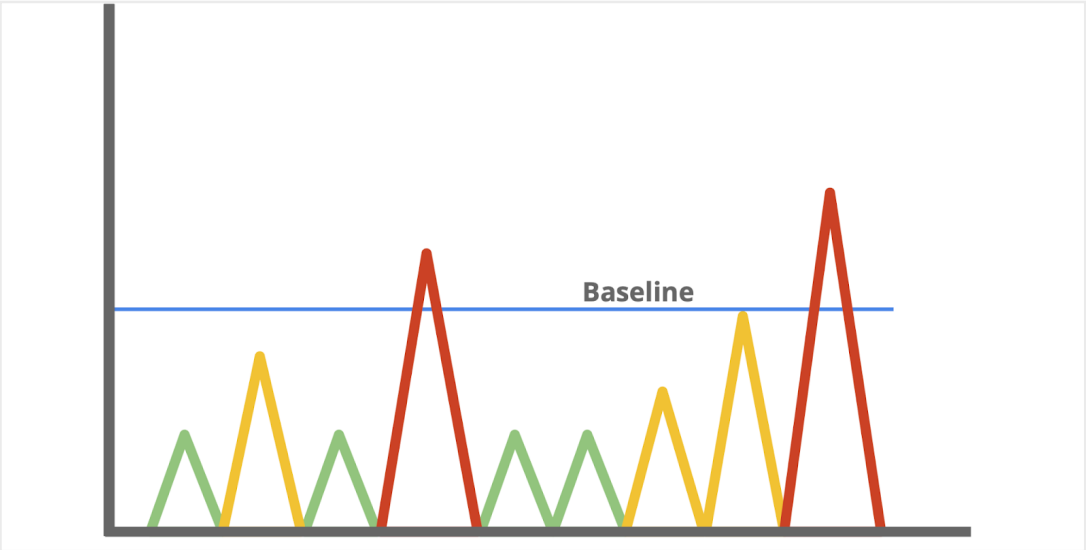
SOC manager
The SOC manager is at the top of the pyramid and is responsible for:
- Hiring, training, and evaluating the SOC team members
- Creating performance metrics and managing the performance of the SOC team
- Developing reports related to incidents, compliance, and auditing
- Communicating findings to stakeholders such as executive management

Network traffic
is the amount of data that moves across a network. While **network data** is the data that's transmitted between devices on a network.
- there can be a huge volume of network traffic at any given moment

By understanding how data should be flowing across the network, you can develop an understanding of expected network traffic flow.
By knowing what's normal, you can easily spot what's abnormal.

Attackers use data exfiltration to steal or leak data such as user names, passwords, or intellectual property.

Maintaining awareness with network monitoring
Know your network
Network communications provide information about connections such as source and destination IP addresses, amount of data transferred, date and time, and more. This information can be valuable for security professionals when developing a **baseline** of normal or expected behavior.



Monitor your network

Monitoring involves examining network components to detect unusual activities, such as large and unusual data transfers.

Flow Analysis

Flow refers to the movement of network communications and includes information related to packets, protocols, and ports.

Packets can travel to ports, which receive and transmit communications. Ports are often, but not always, associated with network protocols. For example, port 443 is commonly used by HTTPS which is a protocol that provides website traffic encryption.

Temporal patterns

Network packets contain information relating to time. This information is useful in understanding time patterns. For example, a company operating in North America experiences bulk traffic flows between 9 a.m. to 5 p.m., which is the baseline of normal network activity. If large volumes of traffic are suddenly outside of the normal hours of network activity, then this is considered *off baseline* and should be investigated.

Network monitoring tools

Network monitoring can be automated or performed manually. Some common network monitoring tools can include:

- **Intrusion detection systems** (**IDS**) monitor system activity and alert on possible intrusions. An IDS will detect and alert on the deviations you've configured it to detect. Most commonly, IDS tools will monitor the content of packet payload to detect patterns associated with threats such as malware or phishing attempts.
- **Network protocol analyzers**, also known as packet sniffers, are tools

designed to capture and analyze data traffic within a network. They can be used to analyze network communications manually in detail. Examples include tools such as tcpdump and Wireshark, which can be used by security professionals to record network communications through packet captures. Packet captures can then be investigated to identify potentially malicious activity.

Defense measures

1. Prevent attacker access
2. Monitor network activity
3. Protect assets
4. Detect and stop the exfiltration

Packets and packet captures

a **data packet** is a basic unit of information that travels from one device to another within a network. Detecting network intrusions begins at the packet level. That's because packets form the basis of information exchange over a network.

Components of a packet

1. **Header** - like name and mailing address located on an envelope.

   Packets can have several headers depending on the protocols used such as an Ethernet header, an IP header, a TCP header, and more. Headers provide information that’s used to route packets to their destination.

2. **Payload** - content

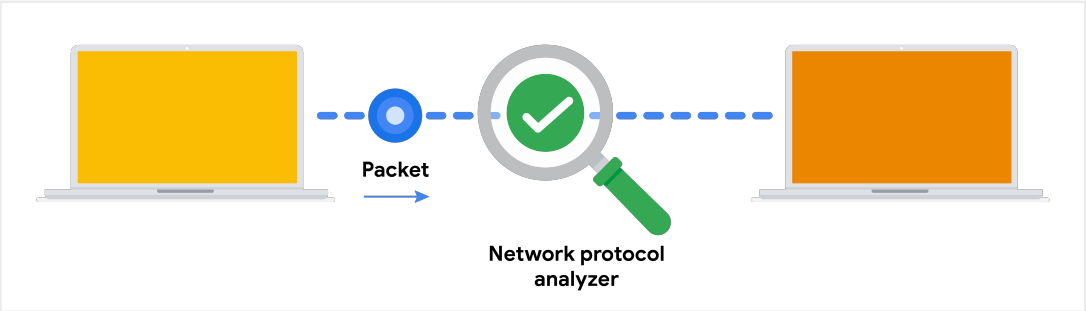
   The payload component directly follows the header and contains the actual data being delivered. Think back to the example of uploading an image to a website; the payload of this packet would be the image itself.

3. **Footer** - signifies the end of the packet

   The Ethernet protocol uses footers to provide error-checking information to determine if data has been corrupted.

Network protocol analyzers

Network protocol analyzers (packet sniffers) are tools designed to capture and analyze data traffic within a network. Examples of network protocol analyzers include tcpdump, Wireshark, and TShark.



How network protocol analyzers work

Network protocol analyzers use both software and hardware capabilities to capture network traffic and display it for security analysts to examine and analyze. Here's how:

1. First, packets must be collected from the network via the **Network Interface Card (NIC)**, which is hardware that connects computers to a network, like a router. NICs receive and transmit network traffic, but by default they only listen to network traffic that's addressed to them. To capture all network traffic that is sent over the network, a NIC must be switched to a mode that has access to all visible network data packets. In wireless interfaces this is often referred to as monitoring mode, and in other systems it may be called promiscuous mode. This mode enables the NIC to have access to all visible network data packets, but it won't help analysts access all packets across a network. A network protocol analyzer must be positioned in an appropriate network segment to access all traffic between different hosts.
2. The network protocol analyzer collects the network traffic in raw binary format. Binary format consists of 0s and 1s and is not as easy for humans to interpret. The network protocol analyzer takes the binary and converts it so that it's displayed in a human-readable format, so analysts can easily read and understand the information.

Capturing packets

Packet sniffing is the practice of capturing and inspecting data packets across a network. A **packet capture (p-cap)** is a file containing data packets intercepted from an interface or network. Packet captures can be viewed and further analyzed using network protocol analyzers.

P-cap files can come in many formats depending on the packet capture library that's used. Each format has different uses and network tools may use or support specific packet capture file formats by default.

1. **Libpcap** is a packet capture library designed to be used by Unix-like systems, like Linux and MacOS®. Tools like tcpdump use Libpcap as the

default packet capture file format.

2. **WinPcap** is an open-source packet capture library designed for devices running Windows operating systems. It's considered an older file format and isn't predominantly used.
3. **Npcap** is a library designed by the port scanning tool Nmap that is commonly used in Windows operating systems.
4. **PCAPng** is a modern file format that can simultaneously capture packets and store data. Its ability to do both explains the "ng," which stands for "next generation."

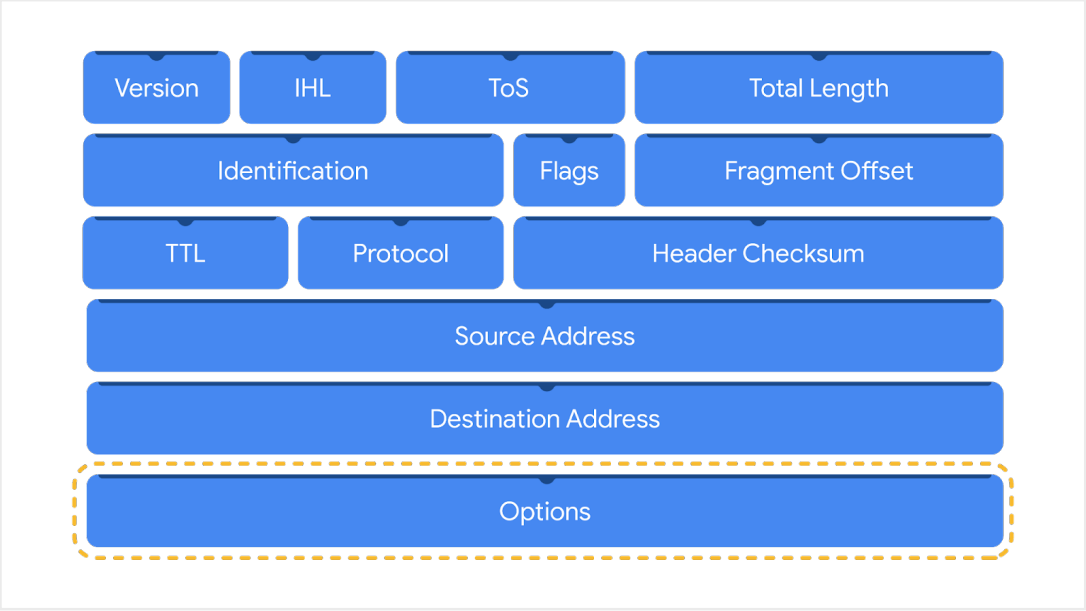
Internet Protocol (IP)

Packets form the foundation of data exchange over a network, which means that detection begins at the packet level. The **Internet Protocol (IP)** includes a set of standards used for routing and addressing data packets as they travel between devices on a network. IP operates as the foundation for all communications over the internet.

IP ensures that packets reach their destinations. There are two versions of IP that you will find in use today: IPv4 and IPv6. Both versions use different headers to structure packet information.

IPV4

IPv4 is the most commonly used version of IP. There are thirteen fields in the header:

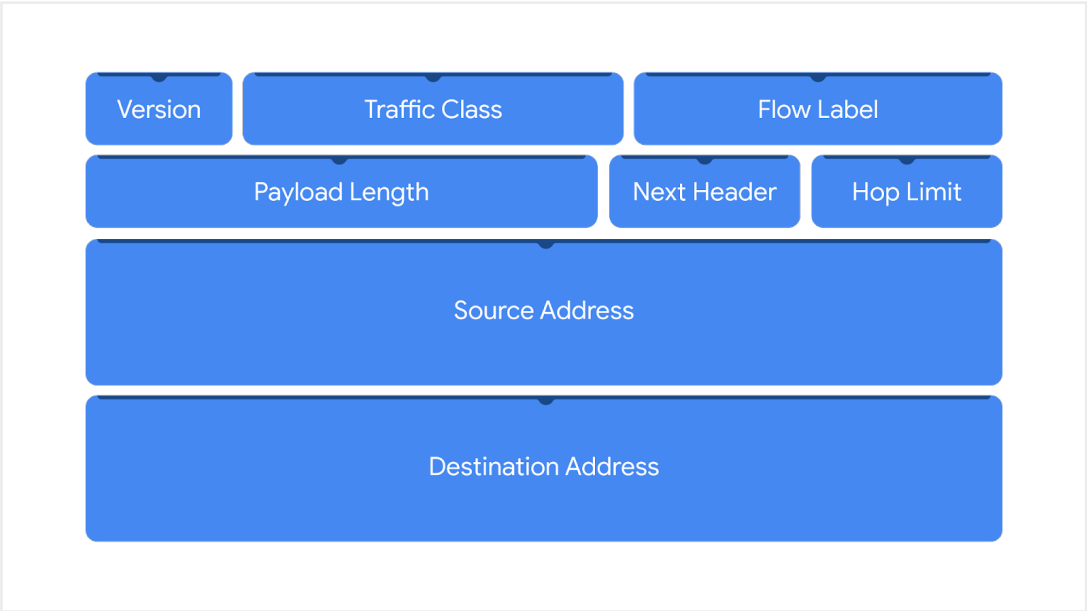


- **Version**: This field indicates the IP version. For an IPv4 header, IPv4 is used.

- **Internet Header Length (IHL)**: This field specifies the length of the IPv4 header including any Options.
- **Type of Service (ToS)**: This field provides information about packet priority for delivery.
- **Total Length**: This field specifies the total length of the entire IP packet including the header and the data.
- **Identification**: Packets that are too large to send are fragmented into smaller pieces. This field specifies a unique identifier for fragments of an original IP packet so that they can be reassembled once they reach their destination.
- **Flags**: This field provides information about packet fragmentation including whether the original packet has been fragmented and if there are more fragments in transit.
- **Fragment Offset**: This field is used to identify the correct sequence of fragments.
- **Time to Live (TTL)**: This field limits how long a packet can be circulated in a network, preventing packets from being forwarded by routers indefinitely.
- **Protocol**: This field specifies the protocol used for the data portion of the packet.
- **Header Checksum**: This field specifies a checksum value which is used for error-checking the header.
- **Source Address**: This field specifies the source address of the sender.
- **Destination Address**: This field specifies the destination address of the receiver.
- **Options**: This field is optional and can be used to apply security options to a packet.

IPV6

IPv6 adoption has been increasing because of its large address space. There are eight fields in the header:



- **Version**: This field indicates the IP version. For an IPv6 header, IPv6 is used.
- **Traffic Class**: This field is similar to the IPv4 Type of Service field. The Traffic Class field provides information about the packet's priority or class to help with packet delivery.
- **Flow Label**: This field identifies the packets of a flow. A flow is the sequence of packets sent from a specific source.
- **Payload Length**: This field specifies the length of the data portion of the packet.
- **Next Header**: This field indicates the type of header that follows the IPv6 header such as TCP.
- **Hop Limit**: This field is similar to the IPv4 Time to Live field. The Hop Limit limits how long a packet can travel in a network before being discarded.
- **Source Address**: This field specifies the source address of the sender.
- **Destination Address**: This field specifies the destination address of the receiver.

TCPdump

Tcpdump is a command-line network protocol analyzer. Recall that a **command-line interface (CLI)** is a text-based user interface that uses commands to interact with the computer.

Tcpdump is used to capture network traffic. This traffic can be saved to a **packet capture (p-cap)**, which is a file containing data packets intercepted from an interface or network. Analysts use tcpdump for a variety of reasons, from

troubleshooting network issues to identifying malicious activity. Tcpdump comes pre-installed in many Linux distributions and can also be installed on other Unix-based operating systems such as macOS®.

sudo tcpdump [-i interface] [option(s)] [expression(s)]

- The **sudo tcpdump** command begins running tcpdump using elevated permissions as sudo.
- The **-i** parameter specifies the network interface to capture network traffic. You must specify a network interface to capture from to begin capturing packets. For example, if you specify **-i any** you'll sniff traffic from all network interfaces on the system.
- The **option(s)** are optional and provide you with the ability to alter the execution of the command. The **expression(s)** are a way to further filter network traffic packets so that you can isolate network traffic. You'll learn more about **option(s)** and **expression(s)** in the next section.

-w

Using the **-w** flag, you can write or save the sniffed network packets to a packet capture file instead of just printing it out in the terminal. This is very useful because you can refer to this saved file for later analysis. In this command, tcpdump is capturing network traffic from all network interfaces and saving it to a packet capture file named **packetcapture.pcap**:

sudo tcpdump -i any -w packetcapture.pcap

-r

Using the **-r** flag, you can read a packet capture file by specifying the file name as a parameter. Here is an example of a tcpdump command that reads a file called **packetcapture.pcap**:

sudo tcpdump -r packetcapture.pcap

-v

As you've learned, packets contain a lot of information. By default, tcpdump will not print out all of a packet's information. This option, which stands for verbose, lets you control how much packet information you want tcpdump to print out. There are three levels of verbosity you can use depending on how much packet information you want tcpdump to print out. The levels are **-v**, **-vv**, and **-vvv**. The level of verbosity increases with each added v. The verbose option can be helpful if you're looking for packet information like the details of a packet's IP header fields. Here's an example of a tcpdump command that reads the **packetcapture.pcap** file with verbosity:

sudo tcpdump -r packetcapture.pcap -v

russ

-c

The **-c** option stands for count. This option lets you control how many packets tcpdump will capture. For example, specifying **-c 1** will only print out one single packet, whereas **-c 10** prints out 10 packets. This example is telling tcpdump to only capture the first three packets it sniffs from **any** network interface:

sudo tcpdump -i any -c 3

-n

By default, tcpdump will perform name resolution. This means that tcpdump automatically converts IP addresses to names. It will also resolve ports to commonly associated services that use these ports. This can be problematic because tcpdump isn't always accurate in name resolution. For example, tcpdump can capture traffic from port 80 and automatically translates port 80 to HTTP in the output. However, this is misleading because port 80 isn't always going to be using HTTP; it could be using a different protocol.

Additionally, name resolution uses what's known as a reverse DNS lookup. A reverse DNS lookup is a query that looks for the domain name associated with an IP address. If you perform a reverse DNS lookup on an attacker's system, they might be alerted that you are investigating them through their DNS records. Using the **-n** flag disables this automatic mapping of numbers to names and is considered to be best practice when sniffing or analyzing traffic. Using **-n** will not resolve hostnames, whereas **-nn** will not resolve *both* hostnames or ports. Here's an example of a tcpdump command that reads the **packetcapture.pcap** file with verbosity and disables name resolution:

sudo tcpdump -r packetcapture.pcap -v -n

Role of Incident Response

Triage is the prioritizing of incidents according to their level of importance or urgency. The triage process helps security teams evaluate and prioritize security alerts and allocate resources effectively so that the most critical issues are addressed first.

The triage process consists of three steps:

1. Receive and assess
2. Assign priority
3. Collect and analyze

Receive and Access

This involves gathering as much information as possible about the alert, including details about the activity that triggered the alert, the systems and assets involved,

and more.

Assign priority
Incidents differ in their impact, size, and scope, which affects the response efforts. To manage time and resources, security teams must prioritize how they respond to various incidents because not all incidents are equal.

Collect and analyze
performing a comprehensive analysis of the incident. Analysis involves gathering evidence from different sources, conducting external research, and documenting the investigative process. The goal of this step is to gather enough information to make an informed decision to address it.

Business continuity planning

Security teams must be prepared to minimize the impact that security incidents can have on their normal business operations. When an incident occurs, organizations might experience significant disruptions to the functionality of their systems and services. Prolonged disruption to systems and services can have serious effects, causing legal, financial, and reputational damages. Organizations can use business continuity planning so that they can remain operational during any major disruptions.

a **business continuity plan (BCP)** is a document that outlines the procedures to sustain business operations during and after a significant disruption. A BCP helps organizations ensure that critical business functions can resume or can be quickly restored when an incident occurs.

BCPs help to minimize interruptions to operations so that essential services can be accessed.

Site resilience, which is used to ensure the availability of networks, data centers, or other infrastructure when a disruption happens. There are three types of recovery sites used for site resilience:

- **Hot sites**: A fully operational facility that is a duplicate of an organization's primary environment. Hot sites can be activated immediately when an organization's primary site experiences failure or disruption.
- **Warm sites**: A facility that contains a fully updated and configured version of the hot site. Unlike hot sites, warm sites are not fully operational and available for immediate use but can quickly be made operational when a failure or disruption occurs.

- **Cold sites**: A backup facility equipped with some of the necessary infrastructure required to operate an organization's site. When a disruption or failure occurs, cold sites might not be ready for immediate use and might need additional work to be operational.

Overview of Logs

A **log** is a record of events that occur within an organization's systems. Logs contain log entries and each entry details information corresponding to a single event that happened on a device or system. Originally, logs served the sole purpose of troubleshooting common technology issues. For example, error logs provide information about why an unexpected error occurred and help to identify the root cause of the error so that it can be fixed. Today, virtually all computing devices produce some form of logs that provide valuable insights beyond troubleshooting.

Security teams access logs from logging receivers like SIEM tools which consolidate logs to provide a central repository for log data. Security professionals use logs to perform **log analysis**, which is the process of examining logs to identify events of interest. Logs help uncover the details surrounding the 5 W's of incident investigation: *who* triggered the incident, *what* happened, *when* the incident took place, *where* the incident took place, and *why* the incident occurred.

Types of logs

Depending on the data source, different log types can be produced. Here’s a list of some common log types that organizations should record:

- **Network**: Network logs are generated by network devices like firewalls, routers, or switches.
- **System**: System logs are generated by operating systems like Chrome OS™, Windows, Linux, or macOS®.
- **Application**: Application logs are generated by software applications and contain information relating to the events occurring within the application such as a smartphone app.
- **Security**: Security logs are generated by various devices or systems such as antivirus software and intrusion detection systems. Security logs contain security-related information such as file deletion.
- **Authentication**: Authentication logs are generated whenever authentication occurs such as a successful login attempt into a computer.

Log Details

Generally, logs contain a date, time, location, action, and author of the action

Login Event [05:45:15] User1 Authenticated successfully

Logs contain information and can be adjusted to contain even more information. Verbose logging records additional, detailed information beyond the default log recording. Here is an example of the same log above but logged as verbose.
Login Event [2022/11/16 05:45:15.892673] auth_performer.cc:470 User1 Authenticated successfully from device1 (192.168.1.2)

Log management is the process of collecting, storing, analyzing, and disposing of log data.

What to log?
The most important aspect of log management is choosing what to log. Organizations are different, and their logging requirements can differ too. It's important to consider which log sources are most likely to contain the most useful information depending on your event of interest.

Organizations that operate in the following industries might need to modify their log management policy to meet regulatory requirements:

- Public sector industries, like the Federal Information Security Modernization Act (FISMA)
- Healthcare industries, like the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Financial services industries, such as the Payment Card Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act (GLBA), and the Sarbanes-Oxley Act of 2002 (SOX)

JavaScript Object Notation (JSON)

JavaScript Object Notation (JSON) is a file format that is used to store and transmit data. JSON is known for being lightweight and easy to read and write. It is used for transmitting data in web technologies and is also commonly used in cloud environments. JSON syntax is derived from JavaScript syntax. If you are familiar with JavaScript, you might recognize that JSON contains components from JavaScript including:

A **key-value pair** is a set of data that represents two linked items: a key and its corresponding value. A key-value pair consists of a key followed by a colon, and then followed by a value. An example of a key-value pair is **"Alert": "Malware"**.
Note: For readability, it is recommended that key-value pairs contain a space before or after the colon that separates the key and value.
Commas
Commas are used to separate data. For example: **"Alert": "Malware", "Alert code": 1090, "severity": 10**.

Double quotes
Double quotes are used to enclose *text* data, which is also known as a string, for example: **"Alert": "Malware"**. Data that contains numbers *is not* enclosed in quotes, like this: **"Alert code": 1090**.
Curly brackets
Curly brackets enclose an **object**, which is a data type that stores data in a comma-separated list of key-value pairs. Objects are often used to describe multiple properties for a given key. JSON log entries start and end with a curly bracket. In this example, **User** is the object that contains multiple properties:

```
"User"
{
  "id": "1234",
  "name": "user",
  "role": "engineer"
}
```

Square brackets
Square brackets are used to enclose an **array**, which is a data type that stores data in a comma-separated ordered list. Arrays are useful when you want to store data as an ordered collection, for example: **["Administrators", "Users", "Engineering"]**.

Syslog

Syslog is a standard for logging and transmitting data. It can be used to refer to any of its three different capabilities:

1. **Protocol**: The syslog protocol is used to transport logs to a centralized log server for log management. It uses port 514 for plaintext logs and port 6514 for encrypted logs.
2. **Service**: The syslog service acts as a log forwarding service that consolidates logs from multiple sources into a single location. The service works by receiving and then forwarding any syslog log entries to a remote server.
3. **Log format**: The syslog log format is one of the most commonly used log formats that you will be focusing on. It is the native logging format used in Unix® systems. It consists of three components: a header, structured-data, and a message.

```
<236>1 2022-03-21T01:11:11.003Z virtual.machine.com evntslog - ID01
[user@32473 iut="1" eventSource="Application" eventID="9999"]
This is a log entry!
```

Header
The header contains details like the timestamp; the hostname, which is the name of the machine that sends the log; the application name; and the message ID.

- **Timestamp**: The timestamp in this example is **2022-03-21T01:11:11.003Z**, where **2022-03-21** is the date in YYYY-MM-DD format. **T** is used to separate the date and the time. **01:11:11.003** is the 24-hour format of the time and includes the number of milliseconds **003**. **Z** indicates the timezone, which is Coordinated Universal Time (UTC).
- **Hostname**: **virtual.machine.com**
- **Application**: **evntslog**
- **Message ID**: **ID01**

Structured-data

The structured-data portion of the log entry contains additional logging information. This information is enclosed in square brackets and structured in key-value pairs. Here, there are three keys with corresponding values: **[user@32473 iut="1" eventSource="Application" eventID="9999"]**.

Message

The message contains a detailed log message about the event. Here, the message is **This is a log entry!**.

Priority (PRI)

The priority (PRI) field indicates the urgency of the logged event and is contained with angle brackets. In this example, the priority value is **<236>** . Generally, the lower the priority level, the more urgent the event is.

Note: Syslog headers can be combined with JSON, and XML formats. Custom log formats also exist.

XML (eXtensible Markup Language)

XML (eXtensible Markup Language) is a language and a format used for storing and transmitting data. XML is a native file format used in Windows systems. XML syntax uses the following:

- Tags
- Elements
- Attributes

Tags

XML uses tags to store and identify data. Tags are pairs that must contain a start tag and an end tag. The start tag encloses data with angle brackets, for example **<tag>**, whereas the end of a tag encloses data with angle brackets and a forward slash like this: **</tag>**.

Elements

XML elements include *both* the data contained inside of a tag and the tags itself. All XML entries must contain at least one root element. Root elements contain other elements that sit underneath them, known as child elements.

Here is an example:

<Event>

<EventID>4688</EventID>
<Version>5</Version>
</Event>
In this example, **<Event>** is the root element and contains two child elements **<EventID>** and **<Version>**. There is data contained in each respective child element.

Attributes
XML elements can also contain attributes. Attributes are used to provide additional information about elements. Attributes are included as the second part of the tag itself and must always be quoted using either single or double quotes.
For example:
<EventData>
<Data Name='SubjectUserSid'>S-2-3-11-160321</Data>
<Data Name='SubjectUserName'>JSMITH</Data>
<Data Name='SubjectDomainName'>ADCOMP</Data>
<Data Name='SubjectLogonId'>0x1cf1c12</Data>
<Data Name='NewProcessId'>0x1404</Data>
</EventData>
In the first line for this example, the tag is **<Data>** and it uses the attribute **Name='SubjectUserSid'** to describe the data enclosed in the tag **S-2-3-11-160321**.

CSV (Comma Separated Value)
CSV (Comma Separated Value) uses commas to separate data values. In CSV logs, the position of the data corresponds to its field name, but the field names themselves might not be included in the log. It's critical to understand what fields the source device (like an IPS, firewall, scanner, etc.) is including in the log.

Here is an example:
2009-11-24T21:27:09.534255,ALERT,192.168.2.7,1041,x.x.250.50,80,TCP,ALLOWED,1:2001999:9,"ET MALWARE BTGrab.com Spyware Downloading Ads",1

CEF (Common Event Format)
Common Event Format (CEF) is a log format that uses key-value pairs to structure data and identify fields and their corresponding values. The CEF syntax is defined as containing the following fields:
CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Fields are all separated with a pipe character **|**. However, anything in the

Extension part of the CEF log entry must be written in a key-value format. Syslog is a common method used to transport logs like CEF. When Syslog is used a timestamp and hostname will be prepended to the CEF message. Here is an example of a CEF log entry that details malicious activity relating to a worm infection:
Sep 29 08:26:10 host CEF:1|Security|threatmanager|1.0|100|worm successfully stopped|10|src=10.0.0.2 dst=2.1.2.2 spt=1232

Here is a breakdown of the fields:

- **Syslog Timestamp**: **Sep 29 08:26:10**
- **Syslog Hostname**: **host**
- **Version**: **CEF:1**
- **Device Vendor**: **Security**
- **Device Product**: **threatmanager**
- **Device Version**: **1.0**
- **Signature ID**: **100**
- **Name**: **worm successfully stopped**
- **Severity**: **10**
- **Extension**: This field contains data written as key-value pairs. There are two IP addresses, **src=10.0.0.2** and **dst=2.1.2.2**, and a source port number **spt=1232**. Extensions are not required and are optional to add.

This log entry contains details about a **Security** application called **threatmanager** that **successfully stopped a worm** from spreading from the internal network at **10.0.0.2** to the external network **2.1.2.2** through the port **1232**. A high severity level of **10** is reported.
Note: Extensions and syslog prefix are optional to add to a CEF log.

Detection Tools and Techniques

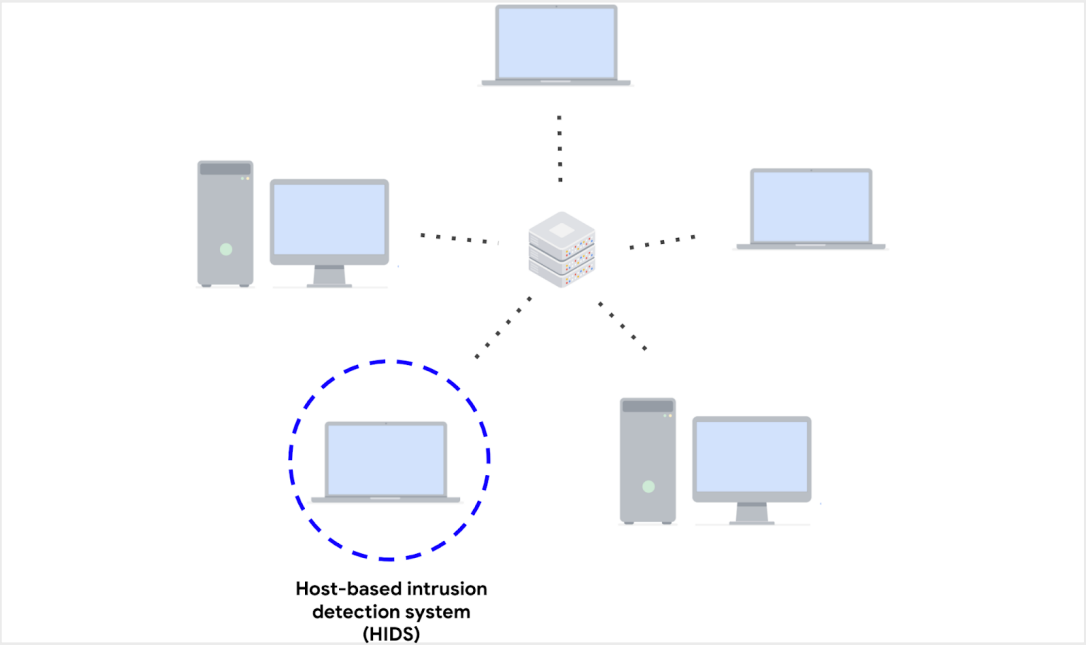
As you've learned, an **intrusion detection system (IDS)** is an application that monitors system activity and alerts on possible intrusions. IDS technologies help organizations monitor the activity that happens on their systems and networks to identify indications of malicious activity. Depending on the location you choose to set up an IDS, it can be either host-based or network-based.

Host-based intrusion detection system

A host-based intrusion detection system (HIDS) is an application that monitors the activity of the host on which it's installed. A HIDS is installed as an agent on a host. A host is also known as an endpoint, which is any device connected to a network like a computer or a server.

Typically, HIDS agents are installed on all endpoints and used to monitor and detect security threats. A HIDS monitors internal activity happening on the host to

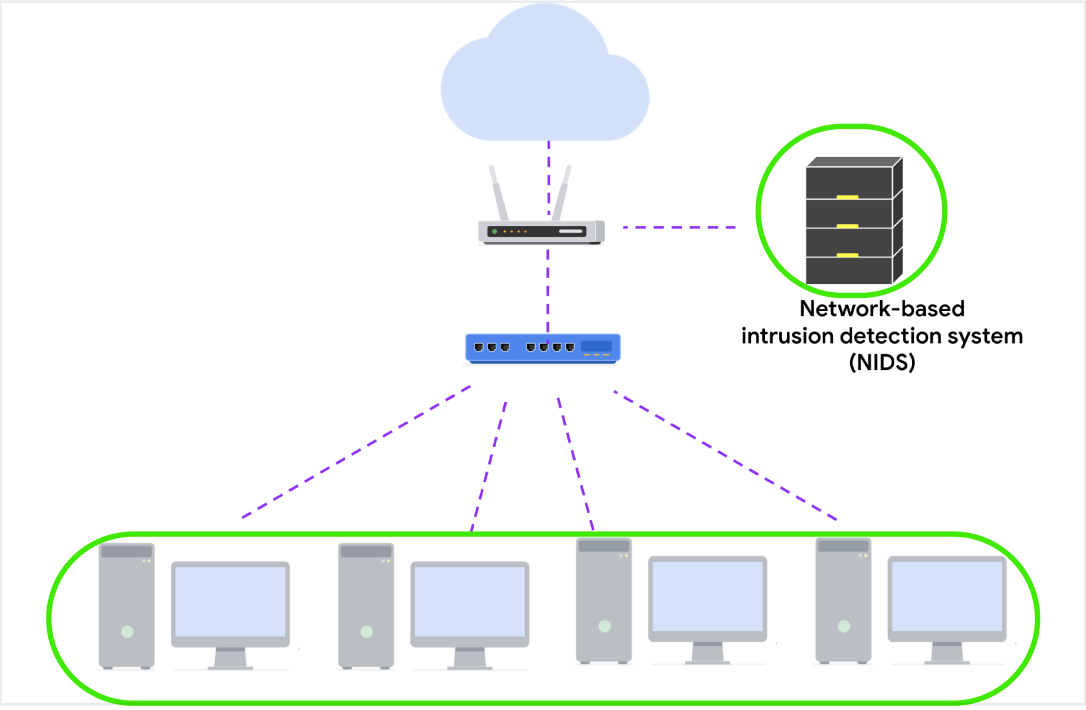
identify any unauthorized or abnormal behavior. If anything unusual is detected, such as the installation of an unauthorized application, the HIDS logs it and sends out an alert.



This diagram shows a HIDS tool installed on a computer. The dotted circle around the host indicates that it is only monitoring the local activity on the single computer on which it's installed.

Network-based intrusion detection system

A network-based intrusion detection system (NIDS) is an application that collects and monitors network traffic and network data. NIDS software is installed on devices located at specific parts of the network that you want to monitor. The NIDS application inspects network traffic from different devices on the network. If any malicious network traffic is detected, the NIDS logs it and generates an alert.



This diagram shows a NIDS that is installed on a network. The highlighted circle around the server and computers indicates that the NIDS is installed on the server and is monitoring the activity of the computers.

Detection systems can use different techniques to detect threats and attacks. The two types of detection techniques that are commonly used by IDS technologies are signature-based analysis and anomaly-based analysis.

Signature-based analysis

Signature analysis, or signature-based analysis, is a detection method that is used to find events of interest. A **signature** is a pattern that is associated with malicious activity. Signatures can contain specific patterns like a sequence of binary numbers, bytes, or even specific data like an IP address.

Different types of signatures can be used depending on which type of threat or attack you want to detect. For example, an anti-malware signature contains patterns associated with malware. This can include malicious scripts that are used by the malware. IDS tools will monitor an environment for events that match the patterns defined in this malware signature. If an event matches the signature, the event gets logged and an alert is generated.

Advantages

- **Low rate of false positives:** Signature-based analysis is very efficient at detecting known threats because it is simply comparing activity to

signatures. This leads to fewer false positives. Remember that a **false positive** is an alert that incorrectly detects the presence of a threat.

Disadvantages

- **Signatures can be evaded:** Signatures are unique, and attackers can modify their attack behaviors to bypass the signatures. For example, attackers can make slight modifications to malware code to alter its signature and avoid detection.
- **Signatures require updates:** Signature-based analysis relies on a database of signatures to detect threats. Each time a new exploit or attack is discovered, new signatures must be created and added to the signature database.
- **Inability to detect unknown threats:** Signature-based analysis relies on detecting known threats through signatures. Unknown threats can't be detected, such as new malware families or **zero-day** attacks, which are exploits that were previously unknown.

Anomaly-based analysis

Anomaly-based analysis is a detection method that identifies abnormal behavior. There are two phases to anomaly-based analysis: a training phase and a detection phase. In the training phase, a baseline of normal or expected behavior must be established. Baselines are developed by collecting data that corresponds to normal system behavior. In the detection phase, the current system activity is compared against this baseline. Activity that happens outside of the baseline gets logged, and an alert is generated.

Advantages

- **Ability to detect new and evolving threats:** Unlike signature-based analysis, which uses known patterns to detect threats, anomaly-based analysis *can* detect unknown threats.

Disadvantages

- **High rate of false positives:** Any behavior that deviates from the baseline can be flagged as abnormal, including non-malicious behaviors. This leads to a high rate of false positives.
- **Pre-existing compromise:** The existence of an attacker during the training phase will include malicious behavior in the baseline. This can lead to missing a pre-existing attacker.

Intro to Suricata

Suricata is an open-source intrusion detection system, intrusion prevention system, and network analysis tool.

Suricata features

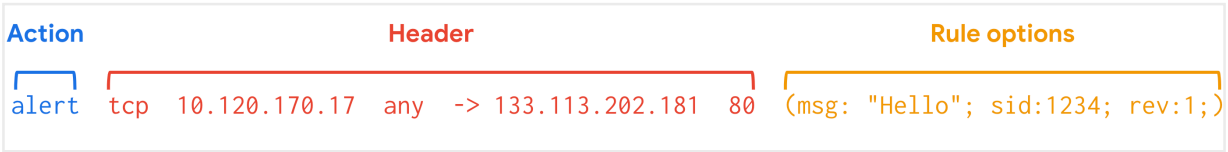
There are three main ways Suricata can be used:

- **Intrusion detection system** (**IDS**): As a network-based IDS, Suricata can monitor network traffic and alert on suspicious activities and intrusions. Suricata can also be set up as a host-based IDS to monitor the system and network activities of a single host like a computer.
- **Intrusion prevention system** (**IPS**): Suricata can also function as an intrusion prevention system (IPS) to detect and block malicious activity and traffic. Running Suricata in IPS mode requires additional configuration such as enabling IPS mode.
- **Network security monitoring** (**NSM**): In this mode, Suricata helps keep networks safe by producing and saving relevant network logs. Suricata can analyze live network traffic, existing packet capture files, and create and save full or conditional packet captures. This can be useful for forensics, incident response, and for testing signatures. For example, you can trigger an alert and capture the live network traffic to generate traffic logs, which you can then analyze to refine detection signatures.

Suricata uses **signatures analysis**, which is a detection method used to find events of interest. Signatures consist of three components:

- **Action**: The first component of a signature. It describes the action to take if network or system activity matches the signature. Examples include: alert, pass, drop, or reject.
- **Header**: The header includes network traffic information like source and destination IP addresses, source and destination ports, protocol, and traffic direction.
- **Rule options:** The rule options provide you with different options to customize signatures.

Here's an example of a Suricata signature:



Configuration file

Before detection tools are deployed and can begin monitoring systems and networks, you must properly configure their settings so that they know what to do. A **configuration file** is a file used to configure the settings of an application. Configuration files let you customize exactly how you want your IDS to interact with the rest of your environment.

Suricata's configuration file is **suricata.yaml**, which uses the YAML file format for syntax and structure.

Log files

There are two log files that Suricata generates when alerts are triggered:

- **eve.json**: The eve.json file is the standard Suricata log file. This file contains detailed information and metadata about the events and alerts generated by Suricata stored in JSON format. For example, events in this file contain a unique identifier called flow_id which is used to correlate related logs or alerts to a single network flow, making it easier to analyze network traffic. The eve.json file is used for more detailed analysis and is considered to be a better file format for log parsing and SIEM log ingestion.
- **fast.log**: The fast.log file is used to record minimal alert information including basic IP address and port details about the network traffic. The fast.log file is used for basic logging and alerting and is considered a legacy file format and is not suitable for incident response or threat hunting tasks.

The main difference between the eve.json file and the fast.log file is the level of detail that is recorded in each. The fast.log file records basic information, whereas the eve.json file contains additional verbose information.

SIEM Log Sources and Log ingestion

Understanding how log sources are ingested into SIEM tools is important because it helps security analysts understand the types of data that are being collected, and can help analysts identify and prioritize security incidents.

SIEM process overview

Previously, you covered the SIEM process. As a refresher, the process consists of three steps:

1. **Collect and aggregate data**: SIEM tools collect event data from various data sources.
2. **Normalize data**: Event data that's been collected becomes normalized. Normalization converts data into a standard format so that data is structured in a consistent way and becomes easier to read and search. While data normalization is a common feature in many SIEM tools, it's important to note that SIEM tools vary in their data normalization capabilities.
3. **Analyze data**: After the data is collected and normalized, SIEM tools analyze and correlate the data to identify common patterns that indicate unusual activity.

This reading focuses on the first step of this process, the collection and aggregation of data.

Data is required for SIEM tools to work effectively. SIEM tools must first collect data using log ingestion. Log ingestion is the process of collecting and importing data from log sources into a SIEM tool. Data comes from any source that generates log data, like a server.

In log ingestion, the SIEM creates a copy of the event data it receives and retains it within its own storage. This copy allows the SIEM to analyze and process the data without directly modifying the original source logs. The collection of event data provides a centralized platform for security analysts to analyze the data and respond to incidents. This event data includes authentication attempts, network activity, and more.

Log forwarders

There are many ways SIEM tools can ingest log data. For instance, you can manually upload data or use software to help collect data for log ingestion. Manually uploading data may be inefficient and time-consuming because networks can contain thousands of systems and devices. Hence, it's easier to use software that helps collect data.

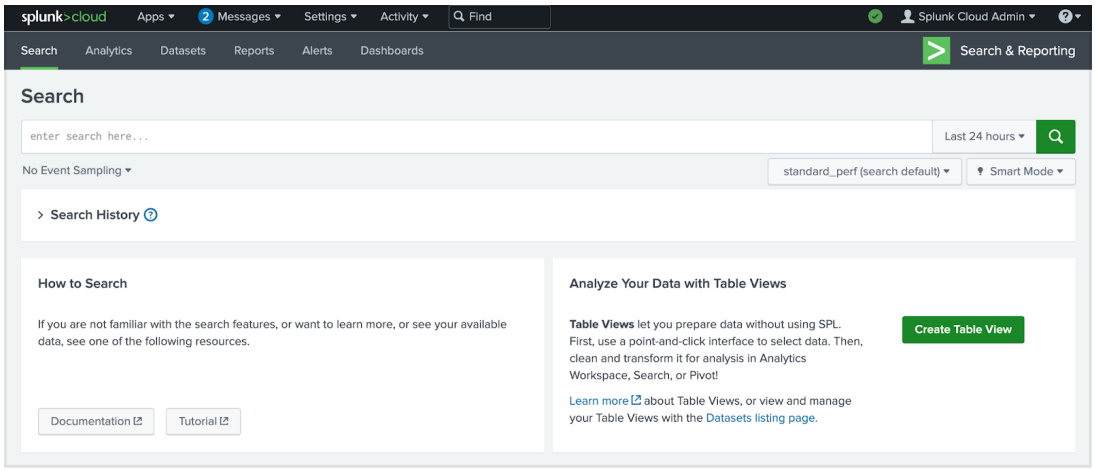
A common way that organizations collect log data is to use log forwarders. Log forwarders are software that automate the process of collecting and sending log data. Some operating systems have native log forwarders. If you are using an operating system that does not have a native log forwarder, you would need to install a third-party log forwarding software on a device.

Search methods with SIEM tools

Splunk Searches

Splunk has its own querying language called **Search Processing Language (SPL)**. SPL is used to search and retrieve events from indexes using Splunk's

Search & Reporting app. An SPL search can contain many different commands and arguments. For example, you can use commands to transform your search results into a chart format or filter results for specific information.



Here is an example of a basic SPL search that is querying an index for a failed event:

index=main fail

- **index=main**: This is the beginning of the search command that tells Splunk to retrieve events from an **index** named **main**. An index stores event data that's been collected and processed by Splunk.
- **fail**: This is the search term. This tells Splunk to return any event that contains the term **fail**.

Splunk's Search Reference

Pipes

Previously, you might have learned about how piping is used in the Linux bash shell. As a refresher, piping sends the output of one command as the input to another command.

SPL also uses the pipe character **|** to separate the individual commands in the search. It's also used to chain commands together so that the output of one command combines into the next command. This is useful because you can refine data in various ways to get the results you need using a single command.

Here is an example of two commands that are piped together:

index=main fail| chart count by host

- **index=main fail**: This is the beginning of the search command that tells Splunk to retrieve events from an **index** named **main** for events containing the search term **fail**.
- **|**: The pipe character separates and chains the two commands **index=main** and **chart count by host**. This means that the output of the

first command **index=main** is used as the input of the second command **chart count by host**.
- **chart count by host**: This command tells Splunk to transform the search results by creating a **chart** according to the **count** or number of events. The argument **by host** tells Splunk to list the events by host, which are the names of the devices the events come from. This command can be helpful in identifying hosts with excessive failure counts in an environment.

Wildcard
A **wildcard** is a special character that can be substituted with any other character. A wildcard is usually symbolized by an asterisk character *****. Wildcards match characters in string values. In Splunk, the wildcard that you use depends on the command that you are using the wildcard with. Wildcards are useful because they can help find events that contain data that is similar but not entirely identical. Here is an example of using a wildcard to expand the search results for a search term:

index=main fail*
- **index=main**: This command retrieves events from an **index** named **main**.
- **fail***: The wildcard after **fail** represents any character. This tells Splunk to search for all possible endings that contain the term **fail**. This expands the search results to return any event that contains the term **fail** such as "failed" or "failure".

Course 8: Put It to Work: Prepare for Cybersecurity Jobs

Classifying for safety
Security professionals classify data types to help them properly protect an organization from cyber attacks that negatively business operations. Here is a review of the most common data types:
- **Public data**
- **Private data**
- **Sensitive data**
- **Confidential data**

Public data
This data classification does not need extra security protections. **Public data** is already accessible to the public and poses a minimal risk to the organization if viewed or shared by others. Although this data is open to the public, it still needs

to be protected from security attacks. Examples of public data include press releases, job descriptions, and marketing materials.

Private data
This data classification type has a higher security level. **Private data** is information that should be kept from the public. If an individual gains unauthorized access to private data, that event has the potential to pose a serious risk to an organization.
Examples of private data can include company email addresses, employee identification numbers, and an organization's research data.

Sensitive data
This information must be protected from everyone who does not have authorized access. Unauthorized access to sensitive data can cause significant damage to an organization's finances and reputation.
Sensitive data includes personally identifiable information (PII), sensitive personally identifiable information (SPII), and protected health information (PHI). Examples of these types of sensitive data are banking account numbers, usernames and passwords, social security numbers (which U.S. citizens use to report their wages to the government), passwords, passport numbers, and medical information.

Confidential data
This data classification type is important for an organization's ongoing business operations. **Confidential data** often has limits on the number of people who have access to it. Access to confidential data sometimes involves the signing of non-disclosure agreements (NDAs)— legal contracts that bind two or more parties to protect information—to further protect the confidentiality of the data.
Examples of confidential data include proprietary information such as trade secrets, financial records, and sensitive government data.

Disaster recovery and business continuity

Identify and protect
Creating business continuity and disaster recovery plans are the final steps of a four-part process that most security teams go through to help ensure the security of an organization.
First, the security team identifies the assets that must be protected in the organization. Next, they determine what potential threats could negatively impact those assets. After the threats have been determined, the security team implements tools and processes to detect potential threats to assets. Lastly, the IT or appropriate business function creates the business continuity and disaster recovery plans. These plans are created in conjunction with one another. The

plans help to minimize the impact of a security incident involving one of the organization's assets.
Business continuity plan

The impact of successful security attacks on an organization can be significant. Loss of profits and customers are two possible outcomes that organizations never want to happen. A **business continuity plan** is a document that outlines the procedures to sustain business operations during and after a significant disruption. It is created alongside a disaster recovery plan to minimize the damage of a successful security attack. Here are four essential steps for business continuity plans:

- **Conduct a business impact analysis.** The business impact analysis step focuses on the possible effects a disruption of business functions can have on an organization.
- **Identify, document, and implement steps to recover critical business functions and processes.** This step helps the business continuity team create actionable steps toward responding to a security event.
- **Organize a business continuity team.** This step brings various members of the organization together to help execute the business continuity plan, if it is needed. The members of this team are typically from the cybersecurity, IT, HR, communications, and operations departments.
- **Conduct training for the business continuity team**. The team considers different risk scenarios and prepares for security threats during these training exercises.

A **disaster recovery plan** allows an organization's security team to outline the steps needed to minimize the impact of a security incident, such as a successful ransomware attack that has stopped the manufacturing team from retrieving certain data. It also helps the security team resolve the security threat. A disaster recovery plan is typically created alongside a business continuity plan. Steps to create a disaster recovery plan should include:

- Implementing recovery strategies to restore software
- Implementing recovery strategies to restore hardware functionality
- Identifying applications and data that might be impacted after a security incident has taken place