Google Cybersecurity Cert Notes

5/20

3 Task of Security Analyst

1.) Protect PC & network systems.
2.) Install prevention software.
3.) Conduct periodic sec audit.

6/3 – Brain virus & Morris worm – 2 early types of malware attacks that affected many PCs.

(86' Alvi Bros) Brain virus - created to detect illegal copies of medical sfw & infected every PC disk entered.

(88' Robert) Morris worm – program created to assess the number of PCs on the internet, installed itself on other PCs for headcount w/o tracking already compromised PCs re-installing itself until out of memory and crashed. **It led to the development of computer response teams. (CERTs)**

00' LoveLetter Attack – use social engineering by sending e-card saying "I love you", then scan all contacts by installing malware to get credentials and valuables

- **Watering hole attack:** A threat actor attacks a website frequently visited by a specific group of users.

8Domains:

1. security and risk management - focuses on defining security goals and objectives, risk mitigation, compliance, business continuity, and the law. Ex. Updating HIPPA compliancy.
2. asset security- focuses on securing digital and physical assets. It's also related to the storage, maintenance, retention, & destruction of data. Ex. Disposing of old equip properly.
3. security architecture and engineering - focuses on optimizing data security by ensuring effective tools, systems, and processes are in place. Ex. Configuring a firewall to help filter computer network traffic.
4. communication and network security - focuses on managing and securing physical networks and wireless communications. Ex. Analyze user behavior, any emps using hotspot, company data will be vulnerable.
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. Ex. Setting up employee access cards/key cards.
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. Ex. Routinely audit permissions to ensure only certain ppl see salaries.
7. security operations - focuses on conducting investigations and implementing preventative measures. Ex. Unknown device connects to internal network, must follow company procedure to 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. Ex. New app creation may be asked about password policies, on ensure any user's data is properly secured/managed.

APTs Advanced Persistent Threats – research their targets in advance tend to stay undetected for a while, and go after large corps and gov't entities, can do serious damage like power grid outage or spy to get trade secrets.

Threat actors are defined by their malicious intent and hackers are defined by their technical skills and motivations. Understanding their motivations and intentions will help you be better prepared to protect your organization and the people it serves from malicious attacks carried out by some of these individuals and groups.

Framework Core Components:

1.) **Identifying and documenting security goals** – Ex. Aligning with a gov't policy like HIPPA, analyst may be asked to identify and document areas that may be out of compliance.

2.) **Setting guidelines to achieve security goals** – Ex. When implementing guidelines to achieve HIPPA, the company may create new policies for how to handle data requests from individual users.
3.) **Implementing security processes** – Ex. Might help design procedures to ensure org complies with verified user data requests like when a user attempts to update/delete their profile info.
4.) **Monitoring and communicating results –** Ex. May monitor org's internal network and report a potential security issue affecting HIPPA to your mgr. or reg compliance officer.

National Institute of Standards and Technology: the Cybersecurity Framework (NIST CSF) – voluntary framework consisting of standards, guidelines, and best practices to manage cyber risk – (NIST RMF, FERC-NERC). **STUDY THESE**

Entry Level Analyst scenario – a high risk alert is received, you investigate and discover data has been transferred w/o authorization, working diligently to find the culprit to find it's a friend. Your obligation is to adhere to the policies and protocols you've been trained to follow.

Go back and study security ethical controls – Confidentiality,

1.) **privacy protections – the act of protecting PII from unauthorized use.**
2.) **Laws –the rules that are recognized by a community and enforced by a government entity.**

Network Protocol Analyzer (packet sniffer) – used to capture and analyze data traffic within a network. Ex. Tcpdump & Wireshark

Forensic investigations use - chain of custody & protecting and preserving evidence playbooks.

OWASP Top Ten | OWASP Foundation – link to stay up to date on most critical risks to web apps

Encoding – converts plaintext into secure ciphertext – uses a public conversion algo to enable systems that use different data representations to share info.

Personal Statement Notes:

1.) Strengths – Committed to developing Programming skills, and great at problem-solving.
2.) Values – Protecting the valuables of people and organizations alike, and treating others fairly, maintaining integrity.
3.) Interests? Having the opportunity to prevent people with malicious intent from compromising innocent hardworking everyday people.
4.) Statement for both: Cybersecurity and government employers.
5.) Having a problem-solving mindset aids me in helping protect people valuables, preventing thieves from taking advantage of them.

As an improving programmer with a strong commitment to developing my skills and a natural talent for problem-solving, I am dedicated and passionate about safeguarding the assets of both individuals and organizations. Upholding values of fairness, integrity, and the protection

of valuables, I strive to create secure environments that prevent malicious actors from compromising the hard work of everyday people and companies alike. My goal is to leverage my growing technical skills and ethical principles to contribute meaningfully to the world of cybersecurity, ensuring the safety and trust of all stakeholders.

Here are some suggestions you are encouraged to consider to help you continuously refine and strengthen your professional statement throughout the program:

1. Locate examples of current cybersecurity professionals' statements. Search for examples on GitHub or professional networking websites or apps. Compare your statement with statements you found online and determine ways you could improve your own statement.

2. Use a word processing spelling/grammar check or an online tool of your choice to make sure that your statement is free of errors.

3. Share your professional statement with trusted friends or colleagues and ask for their feedback. A second opinion is helpful to ensure that you are effectively conveying your ideas.

4. Research job postings and consider including key terms from the postings in your professional statement.

Link to cyber term glossary - 
Cyber Term Glossary.docx

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

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

3 Impacts of risks, threats, & vulnerabilities: Financial, Identity Theft, & Reputation

NIST RMF 7 Steps- Prepare, categorize, select, implement, Assess, Authorize & Monitor (NIST Risk Management Framework | CSRC)

The NIST CSF consists of five important core functions:

- **Identify** -mgmt of cyber risk and its effect on an org's ppl and assets.
- **Protect –** used to protect an org through implements of policies, procedures & trainings.
- **Detect –** Identify potential security incidents and improve monitoring capabilities.
- **Respond –** ensure proper procedures are used to contain, neutralize, and analyze incidents and implement improvement to the security process.
- **Recover** – process of returning affected systems back to normal operation.

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. NEED TO KNOW IF WORKING FOR GOVT.

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

Security Principles:

1. Minimize attack surface area
2. Principle of least privilege
3. Defense in depth
4. Separation of duties
5. Keep security simple
6. Fix security issues correctly
7. Establish secure defaults – the optimal security state is also the default state for users
8. Fail securely – if control fails, should default to most secure option. *Firewall stops all exploits
9. Don't trust services – if partnering with third-parties don't trust integrity
10. Avoid security by obscurity – security should focus on more critical factors other than source code secrecy.

CHECK OUT MEDIUM CYBER FORUM FOR TRENDS!!**

Elements of Internal Audits:

- Establishing the scope and goals
- Conducting risk assessment
- Completing a control assessment
- Assessing compliance
- Communicating Results

Questions to consider when planning an Audit: IF IN SR ROLE!! What is the audit meant to achieve? Which assets are most at risk? Are current controls sufficient to protect those assets? If not, what controls and compliance regulations need to be implemented?

Playbooks = Runbooks

Indicators of Compromise (IOCs) – suspicious domain names found in logs

Incident Response Playbook – orgs quick attempt to identify an attack, contain the damage, and correct the effects of a security breach | **6 phases**:

- Preparation – mitigate risk and impact of incidents by documenting procedures, est. staff plans and educating user.
- Detection & Analysis – detect and analyze events using defined process and tech
- Containment – goal is to prevent further damage and reduce immediate impact
- Eradication & Recovery – complete removal of an incidents artifacts to return to normal (aka IT restoration)
- Post-incident activity – document incident informing org leadership and applying lessons learned to ensure preparedness of future incidents
- Coordination -Report incidents and share information throughout the response process, based on established standards to ensure org meets compliance requirements

Cloud Service Provider (CSP) – companies that own large data centers that house millions of servers in location all over the globe and provide modern technology services, like PC storage, and networking thru the internet.

Software-Defined Networks (SDN) – an approach to network mgmt., enabling dynamic, programmatically efficient network configurations to improve net performance and monitoring.

The practice of using servers, applications, and network services that are hosted on the internet is called **CLOUD** computing.

Open Systems Interconnection (OSI) – 7-layer model that is a standardized concept that describes the layers computers use to communicate and send data over the net. 7. App layer, 6. Presentation Layer, 5. Session Layer, 4. Transport Layer, 3. Network Layer, 2. Data link layer, 1. Physical layer

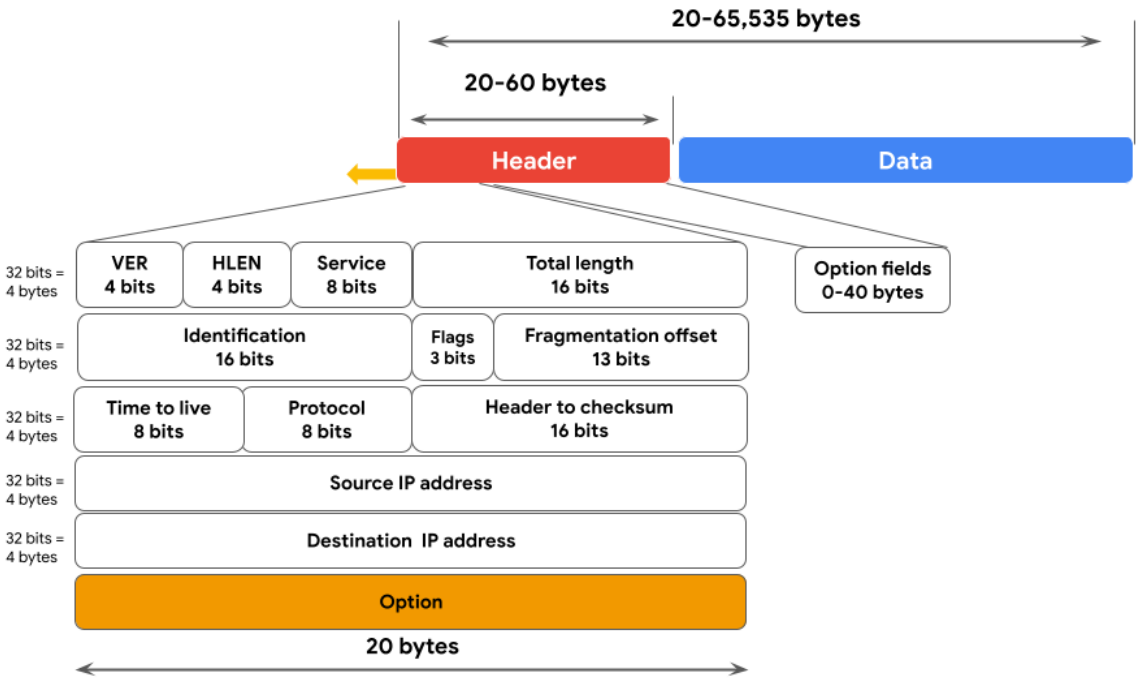
TCP/IP Transmission Control Protocol & Internet Protocol (N.I.T.A.)– 4-layer model (condensed vzn of the OSI) is a framework used to visualize how data is organized and transmitted across a network.

Protocol number -tells the receiving device what to do with the information in the packet.

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:** IPv4 packets can be up to 65, 535 bytes, but most networks have a smaller limit. In these cases, 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.



A **network protocol** is a set of rules used by two or more devices on a network to describe the order of delivery and the structure of data. 3 types: Communication, Management, & Security.

Advanced Encryption Standard (AES) – used through Secure Shell (SSH) on TCP port 22 to ensure other type of unintended recipients can't intercept the transmissions.

Telnet – (used to connect with remote systems) can be used to connect to local or remote devices and uses TCP port 23.

SSH – (used to create a secure connection with a remote system) operates over the TCP port 22 and is a replacement for less secure protocols, such as Telnet.

DHCP servers operate on UDP port 67 while DHCP clients operate on UDP port 68

POP - (manage/retrieve email from mail server) 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.

IMAP – (for incoming mail) uses TCP port 143 for unencrypted email and TCP port 993 over the TLS protocol

SMTP – (for transmit and routing email from sender to recipient's address) uses TCP/UDP port 25 for unencrypted emails and TCP/UDP port 587 using TLS for encrypted emails.

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 25 (unencrypted)
SMTPS	TCP/UDP port 587 (encrypted, TLS)

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

Subnetting allows network professionals and analysts to create a network within their own network without requesting another network IP address from their internet service provider. This process uses network bandwidth more efficiently and improves network performance. Subnetting is one component of creating isolated subnetworks through physical isolation, routing configuration, and firewalls

- A forward proxy server regulates and restricts a person with access to the internet.

- A reverse proxy server regulates and restricts the internet access to an internal server.
- An email proxy server filters spam email by verifying whether a sender's address was forged.

Proxy servers utilize network address translation (NAT) to serve as a barrier between clients on the network and external threats

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

brute force attack is a trial-and-error process of discovering private information.

Some common measures to prevent brute force attacks include: hashing and salting, MFA and/or 2FA, CAPTCHA and reCAPTCHA, and password policies.

TCP Flag codes include:

Flags [S] - Connection Start

Flags [F] - Connection Finish

Flags [P] - Data Push

Flags [R] - Connection Reset

Flags [.] – Acknowledgment

- Trusted platform module (TPM). TPM is a computer chip that can securely store passwords, certificates, and encryption keys.
- Cloud hardware security module (CloudHSM). CloudHSM is a computing device that provides secure storage for cryptographic keys and processes cryptographic operations, such as encryption and decryption.
- **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 leverage different cloud resources.

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

Unified Extensible Firmware Interface (UEFI) is a microchip that contains loading instructions for the computer and replaces BIOS on more modern system

bootloader is a software program that boots the operating system.

Kernel-based Virtual Machine (KVM). KVM is an open-source hypervisor that is supported by most major Linux distributions.

Linux Architecture Map
User -> Application -> Shell -> FHS -> Kernel -> Hardware

Shell - a command line interpreter, it processes commands and outputs the results. Similar to the CLI

Filesystem Hierarchy Standard, or FHS. It's the component of the Linux OS that organizes data similar to a filing cabinet

Kernel - is a component of the Linux OS that manages processes and memory. helps ensure that the system allocates resources more efficiently and makes the system work faster

Package manager- a tool that helps users install, manage, and remove packages or applications.
Package - a piece of software that can be combined with other packages to form an application.

KALI LINUX PEN TESTING TOOLS:

- **Metaspoit** (find & exploit vulnerabilities on a machine)
- **Burp Suite** (test for weaknesses on web apps)
- **Jack The Ripper** (guess passwords)

KALI LINUX FORENSICS TOOLS:

- tcpdump (command line packet analyzer to capture net traffic
- Wireshark (GUI used to analyze live and captured net traffic)
- Autopsy (used to analyze hard drives and smartphones)

Other Linux Distributions

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

Parrot is an open-source distribution that is commonly used for security. Similar to KALI LINUX ™, Parrot comes with pre-installed tools related to penetration testing and digital forensics

Red Hat Enterprise Linux is a subscription-based distribution of Linux built for enterprise use, not free

CentOS is an open-source distribution that is closely related to Red Hat. It uses source code published by Red Hat to provide a similar platform. However, CentOS does not offer the same enterprise support that Red Hat provides and is supported through the community.

Advanced Package Tool (APT)

APT is a tool used with Debian-derived distributions. It is run from the command-line interface to manage, search, and install packages.

Yellowdog Updater Modified (YUM)

YUM is a tool used with Red Hat-derived distributions. It is run from the command-line interface to manage, search, and install packages. YUM works with `.rpm` files.

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)

Shell Commands:

pwd – prints the working directory on screen – returns the directory that you're currently in
ls – displays the names of files and directories in the current working directory
cd – navigates between directories – change directories
cat – displays the content of a file
head – displays just the beginning of a file, by default 10 lines (use **-n x(no**.) to return specified amt of lines Ex. [head -n 6 logs]
tail – opposite of head, returns last 10 lines by default – used to read the most recent info in log
less – returns the content of a file one page at a time – eases use of moving forward and back
whoami – to learn what your username is
Pro Tip: You can use the relative file path and enter **cd ..** to go up one level in the file structure. For example, if the current directory is **/home/analyst/projects**, entering **cd ..** would change your working directory to **/home/analyst**.

Standard FHS directories:

- **/home**: Each user in the system gets their own home directory.
- **/bin**: This directory stands for "binary" and contains binary files and other executables. Executables are files that contain a series of commands a computer needs to follow to run programs and perform other functions.
- **/etc**: This directory stores the system's configuration files.
- **/tmp**: This directory stores many temporary files. The **/tmp** directory is commonly used by attackers because anyone in the system can modify data in these files.
- **/mnt**: This directory stands for "mount" and stores media, such as USB drives and hard drives.
- **`man hier`** command to learn more about the FHS and its standard directories

Filtering Commands:

- **grep** – searches a specified file and returns all lines in the file containing a specified string Ex. [grep Cookies updates.txt]
- **piping (|)** – sends a standard output of 1 command as standard input into another command for further processing
- **find** - command searches for directories and files that meet specified criteria

There's a wide range of criteria that can be specified with **`find`**. For example, you can search for files and directories that

Some examples of Linux filtering commands are **find, sed, cut, e grep**

- Contain a specific string in the name,
- Are a certain file size, or
- Were last modified within a certain time frame.

Options – modify the behavior of a command and commonly begin with a hyphen (-)

- **-name (case-sensitive)**
- **-iname (not case-sensitive)** Ex. [find /home/analyst/projects -name "*log*"]
- **-mtime** last modified files/dir. in days Ex [find /home/analyst/projects -mtime -3]
  - -mtime +1 (last modified > 1 day ago
  - -mtime -1 (last modified < 1 day ago
  - -mmin (search based on minutes)

Note: An asterisk (*) is used as a wildcard to represent zero or more unknown characters.

More Directory Commands:

- mkdir – creates a new directory
- rmdir – removes, or deletes a directory
- touch – creates new file
- rm – removes or deletes a file
- mv – moves a file/directory to a new location
- cp – copies a file or directory into a new location
- nano - is a command-line file editor that's available by default in many Linux distros
  - To save a file in nano, use the keyboard shortcut Ctrl + O. You'll be prompted to confirm the file name before saving. To exit out of nano, use the keyboard shortcut Ctrl + X.
  - Note: Vim and Emacs are also popular command-line text editors.
- echo - the > and >> operators can be used to send the output of echo to a specified file rather than the screen.
  - The difference between the two is that > overwrites your existing file, and >> adds your content to the end of the existing file instead of overwriting it

File Permissions & User Modification Commands:

- ls -l – displays permissions to files and directories
- ls -a – displays hidden files
- ls -la – displays permissions to files and directories including hidden files
- chmod – changes permissions on files and directories

Note: When there are permission changes to more than one owner type, commas are needed to separate changes for each owner type. You should not add spaces after those commas.

Principle of least privilege – only a certain person need access to a file and no one else

Root User, or superuser - is a user with elevated privileges to modify the system

- sudo - is a command that temporarily grants elevated permissions to specific users
  - -g – sets the user's primary group Ex. sudo useradd -g security cmalone
  - -G – able to add > 1 secondary group Ex. sudo useradd -G hr, admin cmalone
- useradd - adds a user to the system
- groupdel – deletes the group an intended user to be deleted is in Ex. sudo groupdel cmalone
- userdel - deletes a user from the system sudo userdel cmalone
  - -r – deletes a user and all files in their home directory sudo userdel -r cmalone
- usermod – modifies existing user accounts Ex. sudo usermod -g procurement cmalone (changes primary group to procurement of existing acct)
  - -a – option that appends the user to an existing group and only used with -G option Ex. sudo usermod -a -G finance cmalone (would add the existing user to the finance group).
  - -d – changes the user's home directory sudo usermod -d /home/garcia_f fgarcia
  - -l – changes the users login name
  - -L – locks the acct so the user can't login sudo usermod -L cmalone (deactivates the acct from the user while given you access to their account & permissions where ownership can be moved to other users).
- chown – changes ownership of a file or directory, for a user or group Ex. sudo chown cmalone access.txt
  - (:) – to designate it as a group name Ex. sudo chown :procurement access.txt

Getting help in Linux with commands:

- man (short for manual) – displays info on other commands and how they work man tail
- whatis – displays a description of a command on a single line whatis head
- apropos – searches the manual page descriptions for a spec. string
  - -a – to search for multiple words apropos -a change password

https://unix.stackexchange.com/ (use for troubleshooting Linux issues)

SQL & Databases

Relational database - a structured database containing tables that are related to each other.

Keys – the columns that relate two tables to each other

Primary key – a column where every row has a unique entry (mustn't have duplicate/null/empty values)

Foreign key – a column in a table that is a primary key in another table (can have empty/duplicate values)

- SELECT - indicates which columns to return. Select employee_id, device_id -> From employees;
    - SELECT * - asterisk will return all columns from the table
- FROM - indicates which table to query
- ORDER BY – sorts in ascending order, written at the end of a query specifying a column Ex. ORDER BY city;
- DESC – short for descending tells SQL to sort numbers from largest to smaller or from Z to A.

Filtering in SQL

- WHERE – indicates the condition for a filter Ex. WHERE country = 'USA';
    - % sign – act as a wildcard for any number of other characters Ex. 'East%' (will return all records that start with East)

Filtering for patterns

- LIKE – an operator used with WHERE to search for a pattern in a column Ex. username LIKE 'a%';
- _ (underscore) - wildcard symbol that only subs for one other char. Ex. 'a_' returns as, an, a7, etc.

Pattern	Results that could be returned
'a%'	apple123, art, a
'a_'	as, an, a7
'a__'	ant, add, a1c
'%a'	pizza, Z6ra, a
'_a'	ma, 1a, Ha
'%a%'	Again, back, a
'_a_'	Car, ban, ea7

- BETWEEN – an operator that filters for numbers or dates within a range
    - Ex. WHERE OS_patch_date BETWEEN '2024-01-01' AND '2024-03-01';

Comparison operators:

operator	use
<	less than
>	greater than
=	equal to

operator	use
<=	less than or equal to
>=	greater than or equal to
<>	not equal to

Filters with AND, OR, and NOT

- AND – joins one column to another column, meeting 2 conditions at once Ex.
  - where operating_system = ‘OS 1’ and Email_client = ‘Email Client 1’;
- OR – specifies that either condition can be met (returns where conditions are met)
  - where operating_system = ‘OS 1’ or operating_ system = ‘OS 3’;
- NOT – negates a condition (returns all records that don’t match the condition)
  - where not operating_system = ‘OS 3’; (returns all machines that aren’t running OS 3 and needs to be updated).
  - Can also combine logical operators e.g. WHERE NOT country = 'Canada' AND NOT country = 'USA';

Join tables in SQL

- INNER JOIN – returns rows matching on a specified column that exists in more than one table
  - Ex. INNER JOIN machines ON employees.employee_id = machines.employee_id
- LEFT JOIN - returns all of the records of the first table, but only returns rows of the second table that match on a specified column.
- RIGHT JOIN
- FULL OUTER JOIN - combine two tables together; however, they don't necessarily need a match between columns to return a row.

**INNER JOIN tells SQL to perform the INNER JOIN. Then, we name the second table we want to combine with the first. This is called the right table. In this case, we want to join machines with the employees table that was already identified after FROM. Lastly, we tell SQL what column to base the join on. In our case, we're using the employee_id column. Since we're using two tables, we must identify the table and follow that with the column name. So, we have employees.employee_id. And machines.employee_id.

Aggregate Functions

aggregate functions - functions that perform a calculation over multiple data points and return the result of the calculation. The actual data is not returned.

- **COUNT** - returns a single number that represents the number of rows returned from your query.
  - **SELECT COUNT (firstname) From customers;**

- **AVG -** returns a single number that represents the average of the numerical data in a column.
- **SUM -** returns a single number that represents the sum of the numerical data in a column

Asset Inventory – a catalog of assets that need to be protected

Asset Classification – the practice of labeling assets based on the sensitivity and importance to an org.

Cloud security challenges

All service providers do their best to deliver secure products to their customers. Much of their success depends on preventing breaches and how well they can protect sensitive information. However, since data is stored in the cloud and accessed over the internet, several challenges arise:

- **Misconfiguration** is one of the biggest concerns. Customers of cloud-based services are responsible for configuring their own security environment. Oftentimes, they use out-of-the-box configurations that fail to address their specific security objectives.
- **Cloud-native breaches** are more likely to occur due to misconfigured services.
- **Monitoring access might be difficult** depending on the client and level of service.
- **Meeting regulatory standards** is also a concern, particularly in industries that are required by law to follow specific requirements such as HIPAA, PCI DSS, and GDPR.

Data lifecycle

5 stages of data lifecycle:

1. Collect
2. Store
3. Use
4. Archive
5. Destroy

- **Data owner:** the person that decides who can access, edit, use, or destroy their information.
- **Data custodian**: anyone or anything that's responsible for the safe handling, transport, and storage of information.
- **Data steward**: the person or group that maintains and implements data governance policies set by an organization.

3 of the most influential industry regulations that every security professional should know about are:

- General Data Protection Regulation (GDPR)

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)

Public Key Infrastructure (PKI).- an encryption framework that secures the exchange of online information

1. The PKI process involves the exchange of encrypted information and the establishment of trust using digital certificates.
2. Then, a digital certificate binds the data's public key to the verified identity of a website, individual, organization, device, or server.

** In PKI, data can be encrypted using asymmetric encryption, symmetric encryption, or both.

- **Asymmetric encryption** - involves the use of a public and private key pair for encryption and decryption of data.
- **Symmetric encryption** - involves the use of a single secret key to exchange information.
- tr - command translates text from one set of characters to another, using a mapping.
  - The first parameter to the tr command represents the input set of characters
  - the second represents the output set of characters
  - Ex. cat .leftShift3 | tr "d-za-cD-ZA-C" "a-zA-Z"

Ex. openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute

** the **`openssl`** command reverses the encryption of the file with a secure symmetric cipher, as indicated by **`AES-256-CBC`**. The **`-pbkdf2`** option is used to add extra security to the key, and **`-a`** indicates the desired encoding for the output. The **`-d`** indicates decrypting, while **`-in`** specifies the input file and **`-out`** specifies the output file. The **`-k`** specifies the password, which in this example is **`ettubrute`**.

- **sha256sum** – a command used for hashing a file using (a hashing algorithm)
  - sha256sum file1hash (hashes/encrypts the file)
- **cmp** – command used to compare files Ex. cmp file1hash file2hash

Five functions make up the Secure Hashing Algorithms (SHA) family of algorithms:

- SHA-1
- SHA-224
- SHA-256
- SHA-384

- SHA-512

AAA Framework

- Authentication –
  - knowledge, something the user knows (password)
  - ownership, something the user possesses (one-time passcode OTP)
  - characteristic, something the user is (biometric – fingerprint scan)
  - Single-sign on (SSO) – combines several diff logins into one
  - MFA – multifactor authentication – verifies identity by two or more ways
- Authorization –
  - Principle of least privilege
  - Separation of duties – principle that no user is given access that will allow misuse of systems
  - Open-Standard Auth Protocol (OAuth) – shares designated access between apps like telling Google it's okay to have another website access your profile
- Accounting – the practice of monitoring the access logs of a system

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

- https://idpro.org/ - stay up-to-date on IAM mgmt

User provisioning/deprovisioning is the process of creating/removing and maintaining a user's digital identity.

Defense in Depth - layered approach to vulnerability management that reduces risk

1. **Perimeter layer**, like authentication systems that validate user access
2. **Network layer**, which is made up of technologies like network firewalls and others
3. **Endpoint layer**, which describes devices on a network, like laptops, desktops, or servers
4. **Application layer**, which involves the software that users interact with
5. **Data layer**, which includes any information that's stored, in transit, or in use

Common Vulnerabilities and Exposures list, or (CVE) list - an openly accessible dictionary of known vulnerabilities and exposures.

- https://owasp.org/www-project-top-ten/ - stay up to date of top vulnerabilities

Types of **Vulnerability Scans** – software that automatically compares known vulnerabilities and exposures against the technologies on the network.

- External v Internal – scan outside net area like firewall v inside net are like app software for weaknesses

- Authenticated v Unauthenticated – scan with login credentials v scan internal only file w no access
- Limited v Comprehensive – scan specific devices like misconfiguration on a firewall v scan all devices including OS, databases etc.

Steps:

- **Identification:** A vulnerable server is flagged because it's running an outdated operating system (OS).
- **Vulnerability analysis:** Research is done on the outdated OS and its vulnerabilities.
- **Risk assessment:** After doing your due diligence, the severity of each vulnerability is scored and the impact of not fixing it is evaluated.
- **Remediation**: Finally, the information that you've gathered can be used to address the issue.

OSINT tools – open-source intelligence - the collection and analysis of information from publicly available sources to generate usable intelligence.

- https://www.virustotal.com/gui/home/upload (service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content)
- https://attack.mitre.org/ (knowledge base of adversary tactics and techniques observed IRT)
- https://osintframework.com/ (find OSINT tools for any kind of source or platform)
- https://haveibeenpwned.com/ (search for breach email accounts)

Bug-bounty-programs (if ever interested in Pen Testing)

- https://hackerone.com/bug-bounty-programs

National Vulnerability Database (remain current on common vulnerabilities)

- https://nvd.nist.gov/

Applying an attacker mindset:

- Identify a target
- Determine how the target can be accessed
- Evaluate attack vectors that can be exploited
- Find the tools and methods of attack

Types of Brute force Software tools:	Prevention Measures – Brute Force Attacks
• Aircrack-ng • Hashcat	• Hashing and salting • Multi-factor authentication (MFA)

• John the Ripper • Ophcrack • THC Hydra	• CAPTCHA • Password policies

Caution with USB Drives – security tips

- https://www.cisa.gov/news-events/news/using-caution-usb-drives

Preventing Social Engineering Attacks

- Implementing managerial controls
- Staying informed of trends

Social engineering trends and security practice:

- https://www.sans.org/newsletters/ouch/ (free newsletter on social engineering trends
- https://www.scamwatch.gov.au/ (resource for news & tools on reporting, avoid, recognize, SE scams)

Phishing resources:

- https://www.phishing.org/
- https://apwg.org/

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.

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.

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.

dropper is a type of malware that comes packed with malicious code which is delivered and installed onto a target system.

loader is a type of malware that downloads strains of malicious code from an external source and installs them onto a target system

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."

Cryptojacking is a form of malware that installs software to illegally mine cryptocurrencies.

intrusion detection system, or IDS, is an application that monitors system activity and alerts some possible intrusions.

Web-based Exploits

I**njection attacks** is malicious code inserted into a vulnerable application

Cross site scripting, or XSS, is an injection attack that inserts code into a vulnerable website or web application. 3 main types:

- *Reflected* - XSS attack is an instance where a malicious script is sent to the server and activated during the server's response.
- *Stored* - XSS attack is an instance when malicious script is injected directly on the server. Here, attackers target elements of a site that are served to the user.
- *DOM-based* - XSS attack is an instance when malicious script exists in the web page a browser loads. Malicious script can be seen in the URL.

SQL injection is an attack that executes unexpected queries on a database. Occurs due to the lack of sanitized inputs. 3 main categories of SQL injections:

- In-band - uses the same communication channel to launch the attack & gather the results
- Out-of-band – use a diff. comm. channel to launch the attack & gather the results.
- Inferential - occurs when an attacker is unable to directly see the results of their attack and analyzes the behavior of the system

Injection Prevention - escape user inputs—preventing someone from inserting any code that a program isn't expecting. Can do it by:

- **Prepared statement** is a coding technique that executes SQL statements before passing them on to the 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.

Resource: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection

Threat modeling is a process of identifying assets, their vulnerabilities, and how each is exposed to threats. Generally, 6 steps:

1. Define the scope – determine what to build by creating inv of assets and classifying them
2. Identify threats – define all potential threat actors internal/external (employee or hacker)
3. Characterize the environment – attacker mindset to the business

4. Analyze threats – examine existing protection & identify gaps, ranking threats accord to risks
5. Mitigate risks – plan for defending against threats avoid, transfer, reduce, or accept it
6. Evaluate findings – document all steps and make note of any success and record lessons learned

Attack tree – a diagram that maps threats to assets

Process for Attack Simulation and Threat Analysis (**PASTA**) is a popular threat modeling framework that's used across many industries. **7 stages**:

1. Define business & security objectives
2. Define technical scope – identify app components that need to be evaluated
3. Decompose the application – identify existing controls to protect user data from threats
4. Perform a threat analysis – research on the type of attack that could be used
5. Perform a vulnerability analysis – investigate vulnerabilities by considering the root issue
6. Conduct attack modeling – tests vulnerabilities analyzed in stage 5 by simulating attacks
7. Analyze risk and impact – makes risk mgmt. recommendations based on the compiled analyzed data from all previous steps.

Common Frameworks for Threat Modeling

Stride	Trike:	VAST:
• Spoofing • Tampering • Repudiation • Information disclosure • Denial of service • Elevation of privilege	an open-source methodology & tool that takes a security-centric approach to threat modeling. It's commonly used to focus on security permissions, application use cases, privilege models, & other elements that support a secure environment.	Visual, Agile, & Simple Threat (VAST) Modeling framework is part of an automated threat-modeling platform called ThreatModeler®. Many teams use VAST to automate & streamline threat modeling assessments.

One of the keys to threat modeling is asking the right questions:

- What are we working on?
- What kinds of things can go wrong?
- What are we doing about it?
- Have we addressed everything?
- Did we do a good job?

Incident Detection & Response

NIST Incident Response Lifecycle:

Preparation:	Detection & Analysis:	Containment, eradication, & recovery:	Post-incident activity:
• Set up uniform company email conventions • Create a collaborative, ethical environment where employees feel comfortable asking questions • Provide cybersecurity training on a quarterly basis	• Identify signs of an incident • Filter external emails to flag messages containing attachments such as voicemails • Have an incident response plan to reference	• Communicate with sender to confirm the origin of the voice message • Provide employees with an easy way to report and contain suspicious messages	• Update the playbook to highlight additional red flags employees should be aware of • Review processes and workflows related to permissions and adjust oversight of those permissions

Computer security incident response teams, or (CSIRTs), are a specialized group of security professionals that are trained in incident management and response.

Suricata – tool with capabilities of an IDS & IPS (Intrusion Detection/Prevention Systems)

** Examples of IDS tools include Zeek, Suricata, Snort®, and Sagan.

Capability	IDS	IPS	EDR
Detects malicious activity	✓	✓	✓
Prevents intrusions	N/A	✓	✓
Logs activity	✓	✓	✓
Generates alerts	✓	✓	✓
Performs behavioral analysis	N/A	N/A	✓

Detection categories:

1. **A true positive** is an alert that correctly detects the presence of an attack.
2. **A true negative** is a state where there is no detection of malicious activity. This is when no malicious activity exists, and no alert is triggered.

3. **A false positive** is an alert that incorrectly detects the presence of a threat. This is when an IDS identifies an activity as malicious, but it isn't. False positives are an inconvenience for security teams because they spend time and resources investigating an illegitimate alert.
4. **A false negative** is a state where the presence of a threat is not detected. This is when malicious activity happens but an IDS fails to detect it. False negatives are dangerous because security teams are left unaware of legitimate attacks that they can be vulnerable to.

Endpoint detection and response (**EDR**) is an application that monitors an endpoint for malicious activity. EDR tools are installed on endpoints like end-user devices, PCs, phones, etc. Collects end point activity data for behavioral analysis to identify threat patterns using ML & AI to spot unusual or malicious activity.

** Tools like Open EDR®, Bitdefender™ Endpoint Detection and Response, and FortiEDR™ are examples of EDR tools.

** Other SIEM tools: AlienVault® OSSIM™, Chronicle, Elastic, Exabeam, IBM QRadar® Security Intelligence Platform, LogRhythm, Splunk

Monitoring Network Components Such as:

- Flow analysis –of packets, protocols and ports (ensuring associated combos match)
    - Command and control (C2) – when threat actors used protocols with ports that aren't associated with each other to maintain communication with the compromised system and their machine
- Packet Payload Information – source, dest IP, and packet info (monitor data being sent outside of the network, for potential data exfiltration attack)
- Temporal Patterns – packets relating to time (understand time patterns and baseline)

Net operations center (NOC) – an org'l unit that monitor the performance of a net & reponds to any net disruption, like net outages. Responsible for net performance, availability & uptime.

Learn other network components to monitor: https://attack.mitre.org/datasources/DS0029/

Data exfiltration attacks: https://attack.mitre.org/tactics/TA0010/

Packet Capture Libraries:

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."

Packet Analyzer Filtering (Using Wireshark):

Comparison Operators when using packet sniffers:

Operator type	Symbol	Abbreviation
Equal	==	eq
Not equal	!=	ne
Greater than	>	gt
Less than	<	lt
Greater than or equal to	>=	ge
Less than or equal to	<=	le

Contains – operator for filtering for an exact match of a string of text. Ex. http contains "moved"

Match – operator used to filter packets based on regular expression (regex) – characters that form a pattern

Filter for Protocols: (search in toolbar) dns, http, ftp, ssh, arp, telnet, icmp

Filter for IP address – EX. ip.addr == 172.21.224.2

Filter for source IP – EX ip.src == 10.10.10.10

Filter for destination IP – EX ip.dst == 4.4.4.4

Filter for MAC – EX eth.addr == 00:70:f4:23:18:c4

Filter for TCP or UDP – EX udp.port == 53 , tcp.port == 25

tcpdump command line:

    - **Ex: sudo tcpdump [-i interface] [option(s)] [expression(s)]**
- **-i any** you'll sniff traffic from all network interfaces on the system
- **option**(**s**) are optional & provide you with the ability to alter the execution of the command.

EXPRESSIONS

- **expression(s)** are a way to further filter network traffic packets so that you can isolate network traffic
    - **Ex: sudo tcpdump -r packetcapture.pcap -n 'ip and port 80'**

*****Parentheses can group or prioritize different expressions**, ex: ip and (port 80 or port 443) t**ells tcpdump to execute enclosed filters first before filtering for IPv4

OPTIONS

- **-i** parameter specifies the network interface to capture network traffic
- **-D** flag to list the network interfaces available on a system
- **-w** write/save sniffed net packs to a p-cap instead of in terminal saved to packetcap.pcap
    - **Ex: sudo tcpdump -i any -w packetcapture.pcap**
- **-r** read a pcap file by specifying the file name as a parameter
    - **Ex: sudo tcpdump -r packetcapture.pcap**
- **-v (-vv), (-vvv)** verbose control show much pack info you want to print out, increases with each added v.
    - **Ex: sudo tcpdump -r packetcapture.pcap -v**
- **-c** stands for count, controls number of packs to capture
    - **Ex: sudo tcpdump -i any -c 4**
- **-n, (-nn)** disables auto mapping of #s to names (will not resolve hostnames)(ports)
    - **Ex: sudo tcpdump -r packetcapture.pcap -v -n**
- **-X**: Display the hexadecimal and ASCII output format packet data. Security analysts can analyze hexadecimal and ASCII output to detect patterns or anomalies during malware analysis or forensic analysis.
- **&:** This is an instruction to the Bash shell to run the command in the background.

*****Options are case sensitive, can be written w or w/o a space between**. Ex sudo tcpdump -i any -c 3 | sudo tcpdump -iany -c3**

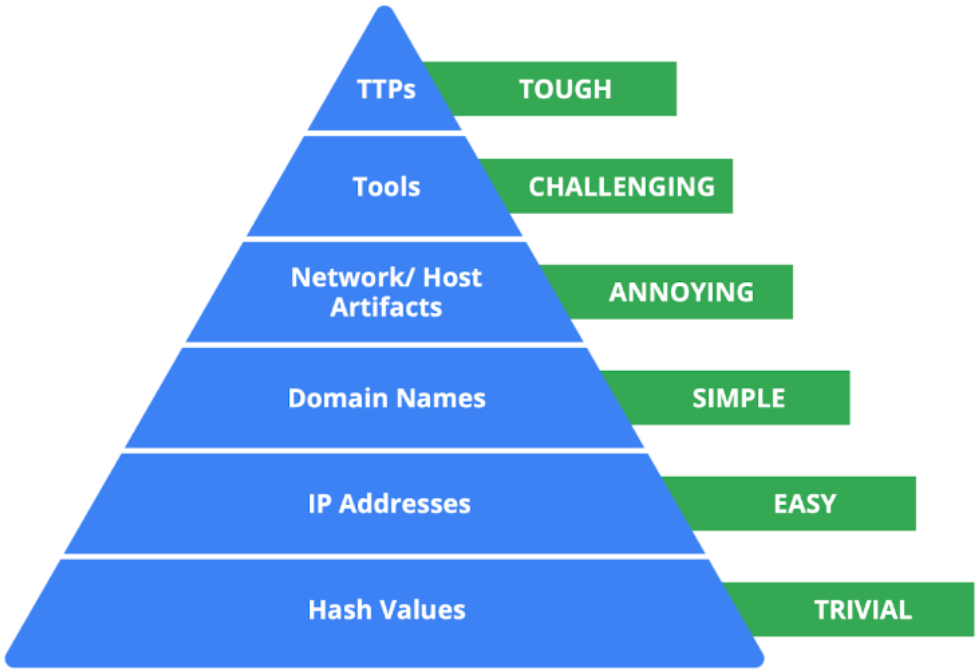
*****Options can be combined -v & -n = -vn, but if an option accepts a parameter right after it like -c 1 or -r capture.pcap then you can't combine other options.

**tcpdump resource https://www.tcpdump.org/manpages/tcpdump.1.html
https://www.tcpdump.org/ (tutorials & guides)

Threat intelligence is evidence-based threat information that provides context about existing or emerging threats

Threat intelligence platform **(TIP) -** which is an application that collects, centralizes, and analyzes threat intelligence from different sources.

Pyramid of Pain, with the goal of improving how indicators of compromise are used in incident detection.



*Analyze IoCs Resources:

- https://www.virustotal.com/gui/home/upload
- https://virusscan.jotti.org/
- https://urlscan.io/

Chain of custody - is the process of documenting evidence possession and control during an incident lifecycle.

- Custody Log (must be signed whenever a new user has possession)
- In the court of law, chain of custody documents help establish proof of the integrity, reliability, and accuracy of the evidence.

Documentation gives **Transparency, Standardization, & Clarity**

The triage process consists of three steps:

1. Receive and assess

Questions to ask when verifying the validity of an alert:

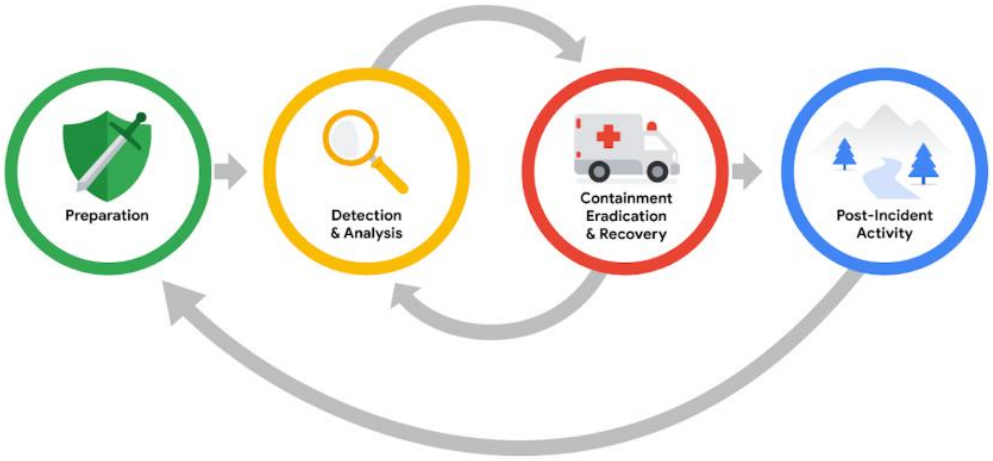
- Is the alert a false positive
- Was this alert triggered in the past
- Is the alert triggered by a known vulnerability
- What is the severity of the alert

2. Assign priority

- Functional impact – does it impact the services (ex. ransomware attack)
- Information impact – was sensitive data stolen or manipulated (exfiltration attack)
- Recoverability – can an org recover (ex. leaked PPI, or proprietary data)

3. Collect and analyze

- Comprehensive analysis of incident
- Gather evidence from diff sources
- Conduct external research
- Document investigative process



SIEM