Google Cybersecurity Professional

Foundations of Cybersecurity - 01

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.
A **threat actor**, or malicious attacker, is any person or group who presents a security risk. This risk can relate to computers, applications, networks, and data.
An **internal threat** can be a current or former employee, an external vendor, or a trusted partner who poses a security risk. At times, an internal threat is accidental. For example, an employee who accidentally clicks on a malicious email link would be considered an accidental threat. Other times, the internal threat actor *intentionally* engages in risky activities, such as unauthorized data access.
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.
Programming is a process that can be used to create a specific set of instructions for a computer to execute tasks. These tasks can include:

- Automation of repetitive tasks (e.g., searching a list of malicious domains)
- Reviewing web traffic
- Alerting suspicious activity

Security Analyst Transferable skills- Communication, Collaboration,Analysis, Problem Solving

Security Analyst Technical skills - Programming languages, SIEM(security information and event management), digital forensics

Transferable skills

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

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

Technical skills

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

- **Programming languages:** By understanding how to use programming languages, cybersecurity analysts can automate tasks that would otherwise be very time consuming. Examples of tasks that programming can be used for include searching data to identify potential threats or organizing and analyzing information to identify patterns related to security issues.
- **Security information and event management (SIEM) tools:** SIEM tools collect and analyze log data, or records of events such as unusual login behavior, and support analysts' ability to monitor critical activities in an

organization. This helps cybersecurity professionals identify and analyze potential security threats, risks, and vulnerabilities more efficiently.

- **Intrusion detection systems (IDSs):** Cybersecurity analysts use IDSs to monitor system activity and alerts for possible intrusions. It's important to become familiar with IDSs because they're a key tool that every organization uses to protect assets and data. For example, you might use an IDS to monitor networks for signs of malicious activity, like unauthorized access to a network.
- **Threat landscape knowledge:** Being aware of current trends related to threat actors, malware, or threat methodologies is vital. This knowledge allows security teams to build stronger defenses against threat actor tactics and techniques. By staying up to date on attack trends and patterns, security professionals are better able to recognize when new types of threats emerge such as a new ransomware variant.
- **Incident response:** 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.

Phishing

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

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

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

Malware

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

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

- **Viruses:** Malicious code written to interfere with computer operations and cause damage to data and software. A virus needs to be initiated by a user (i.e., a threat actor), who transmits the virus via a malicious attachment or file download. When someone opens the malicious attachment or download, the virus hides itself in other files in the now infected system. When the infected files are opened, it allows the virus to insert its own code to damage and/or destroy data in the system.
- **Worms:** Malware that can duplicate and spread itself across systems on its own. In contrast to a virus, a worm does not need to be downloaded by a user. Instead, it self-replicates and spreads from an already infected computer to other devices on the same network.
- **Ransomware:** A malicious attack where threat actors encrypt an organization's data and demand payment to restore access.
- **Spyware:** Malware that's used to gather and sell information without consent. Spyware can be used to access devices. This allows threat actors to collect personal data, such as private emails, texts, voice and image recordings, and locations.

Social Engineering

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

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

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

Social engineering principles

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

Reasons why social engineering attacks are effective include:

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

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

Protected health information (PHI): Information that relates to the past, present, or future physical or mental health or condition of an individual
Security architecture: A type of security design composed of multiple components, such as tools and processes, that are used to protect an organization from risks and external threats
Security controls: Safeguards designed to reduce specific security risks
Security ethics: Guidelines for making appropriate decisions as a security professional
Security frameworks: Guidelines used for building plans to help mitigate risk and threats to data and privacy
Security governance: Practices that help support, define, and direct security efforts of an organization
Sensitive personally identifiable information (SPII): A specific type of PII that falls under stricter handling guidelines

A **playbook** is a manual that provides details about any operational action, such as how to respond to a security incident. Organizations usually have multiple playbooks documenting processes and procedures for their teams to follow. Playbooks vary from one organization to the next, but they all have a similar purpose: To guide analysts through a series of steps to complete specific security-related tasks.

- The first type of playbook you might consult is called the **chain of custody** playbook. Chain of custody is the process of documenting evidence possession and control during an incident lifecycle. As a security analyst involved in a forensic analysis, you will work with the computer data that was breached. You and the forensic team will also need to document who, what, where, and why you have the collected evidence. The evidence is your responsibility while it is in your possession. Evidence must be kept safe and tracked. Every time evidence is moved, it should be reported. This allows all parties involved to know exactly where the evidence is at all times.
- The second playbook your team might use is called the **protecting and preserving evidence** playbook. Protecting and preserving evidence is the process of properly working with fragile and volatile digital evidence. As a security analyst, understanding what fragile and volatile digital evidence is, along with why there is a procedure, is critical. As you follow this playbook, you will consult the **order of volatility**, which is a sequence outlining the order of data that must be preserved from first to last. It prioritizes volatile data, which is data that may be lost if the device in question powers off, regardless of the reason. While conducting an investigation, improper management of digital evidence can compromise and alter that evidence. When evidence is improperly managed during an investigation, it can no longer be used. For this reason, the first priority in any investigation is to properly preserve the data. You can preserve the data by making copies and conducting your investigation using those copies.

Antivirus software: A software program used to prevent, detect, and eliminate malware and viruses
Database: An organized collection of information or data
Data point: A specific piece of information
Intrusion detection system (IDS): An application that monitors system activity and alerts on possible intrusions
Linux: An open-source operating system
Log: A record of events that occur within an organization's systems
Network protocol analyzer (packet sniffer): A tool designed to capture and analyze data traffic within a network
Order of volatility: A sequence outlining the order of data that must be preserved from first to last
Programming: A process that can be used to create a specific set of instructions for a computer to execute tasks
Protecting and preserving evidence: The process of properly working with fragile and volatile digital evidence
Security information and event management (SIEM): An application that collects and analyzes log data to monitor critical activities in an organization
SQL (Structured Query Language): A programming language used to create, interact with, and request information from a database

PLAY IT SAFE: MANAGE RISKS -02

Domain one: Security and risk management

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

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

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

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

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

Domain two: Asset security

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

Domain three: Security architecture and engineering

This domain focuses on managing data security. Ensuring effective tools, systems, and processes are in place helps protect an organization’s assets and data. Security architects and engineers create these processes.
One important aspect of this domain is the concept of shared responsibility. Shared responsibility means all individuals involved take an active role in lowering risk during the design of a security system. Additional design principles related to this domain, which are discussed later in the program, include:

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

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

Domain four: Communication and network security

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

Domain five: Identity and access management

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

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

Domain six: Security assessment and testing

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

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

Domain seven: Security operations

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

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

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

Domain eight: Software development security

The software development security domain is focused on using secure programming practices and guidelines to create secure applications. Having secure applications helps deliver secure and reliable services, which helps protect organizations and their users. Security must be incorporated into each element of the software development life cycle, from design and development to testing and release. To achieve security, the software development process must have security in mind at each step. Security cannot be an afterthought.

Performing application security tests can help ensure vulnerabilities are identified and mitigated accordingly. Having a system in place to test the programming conventions, software executables, and security measures embedded in the software is necessary. Having quality assurance and pen tester professionals ensure the software has met security and performance standards is also an essential part of the software development process. For example, an entry-level analyst working for a pharmaceutical company might be asked to make sure encryption is properly configured for a new medical device that will store private patient data.

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

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

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

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

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

- **ProxyLogon:** A pre-authenticated vulnerability that affects the Microsoft Exchange server. This means a threat actor can complete a user authentication process to deploy malicious code from a remote location.

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

NIST CSF(Cybersecurity framework) focuses on 5 core functions:

1) Identify
2) Protect
3) Detect
4) Respond
5) Recover

OWASP Security Principles:

- **Minimize attack surface area**: Attack surface refers to all the potential vulnerabilities a threat actor could exploit.
- **Principle of least privilege**: Users have the least amount of access required to perform their everyday tasks.
- **Defense in depth**: Organizations should have varying security controls that mitigate risks and threats.
- **Separation of duties**: Critical actions should rely on multiple people, each of whom follow the principle of least privilege.
- **Keep security simple**: Avoid unnecessarily complicated solutions. Complexity makes security difficult.
- **Fix security issues correctly**: When security incidents occur, identify the root cause, contain the impact, identify vulnerabilities, and conduct tests to ensure that remediation is successful.

Additional OWASP security principles

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.

Elements of Internal Audit:

1) Establishing the scope and goals
2) Conducting a risk assessment
3) Completing a controls assessment
4) Assessing compliance
5) Communicating results

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

Goals and objectives of an audit

The goal of an audit is to ensure an organization's information technology (IT) practices are meeting industry and organizational standards. The objective is to identify and address areas of remediation and growth. Audits provide direction and clarity by identifying what the current failures are and developing a plan to correct them.
Security audits must be performed to safeguard data and avoid penalties and fines from governmental agencies. The frequency of audits is dependent on local laws and federal compliance regulations.

Factors that affect audits

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

- Industry type

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

Control types include, but are not limited to:
1. Preventative
2. Corrective
3. Detective
4. Deterrent

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

Identify the scope of the audit

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

Complete a risk assessment

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

Conduct the audit

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

Create a mitigation plan

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

Communicate results to stakeholders

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

A **SIEM** tool is an application that collects and analyzes log data to monitor critical activities in an organization. SIEM tools offer real-time monitoring and tracking of

security event logs. The data is then used to conduct a thorough analysis of any potential security threat, risk, or vulnerability identified. SIEM tools have many dashboard options. Each dashboard option helps cybersecurity team members manage and monitor organizational data. However, currently, SIEM tools require human interaction for analysis of security events.

Security orchestration, automation, and response (SOAR) is a collection of applications, tools, and workflows that uses automation to respond to security events. Essentially, this means that handling common security-related incidents with the use of SIEM tools is expected to become a more streamlined process requiring less manual intervention.

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.

Security posture dashboard

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

Executive summary dashboard

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

Incident review dashboard

The incident review dashboard allows analysts to identify suspicious patterns that can occur in the event of an incident. It assists by highlighting higher risk items that

need immediate review by an analyst. This dashboard can be very helpful because it provides a visual timeline of the events leading up to an incident.

Risk analysis dashboard

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

Chronicle

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

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

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

Enterprise insights dashboard

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

Data ingestion and health dashboard

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

IOC matches dashboard

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

Main dashboard

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

Rule detections dashboard

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

User sign in overview dashboard

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

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

Incident and vulnerability response playbooks are commonly used by entry-level cybersecurity professionals. They are developed based on the goals outlined in an organization's business continuity plan. A business continuity plan is an established path forward allowing a business to recover and continue to operate as normal, despite a disruption like a security breach.

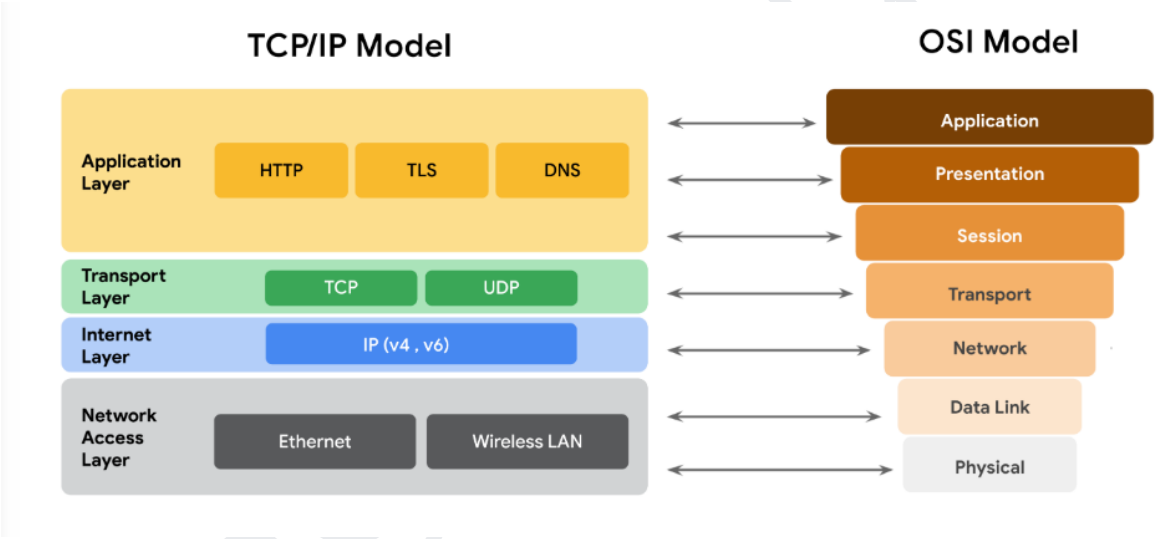
Common steps included in incident and vulnerability playbooks include:

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

NETWORKS & NETWORK SECURITY -03

4 layers of TCP/IP model are:

1) Network Access layer
2) Internet layer
3) Transport Layer
4) Application Layer



- **Internet Protocol (IP)**. 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.
- **Internet Control Message Protocol (ICMP)**. The ICMP shares error information and status updates of data packets. This is useful for detecting and troubleshooting network errors. The ICMP reports information about packets that were dropped or that disappeared in transit, issues with network connectivity, and packets redirected to other routers.

The **Transmission Control Protocol (TCP)** is an internet communication protocol that allows two devices to form a connection and stream data. It ensures that data is reliably transmitted to the destination service. TCP contains the port number of the intended destination service, which resides in the TCP header of a TCP/IP packet.

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.

The application layer in the TCP/IP model is similar to the application, presentation, and session layers of the OSI model. The application layer is responsible for making network requests or responding to requests. This layer defines which internet services and applications any user can access. Protocols in the application layer determine how the data packets will interact with receiving devices. 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)

Application layer protocols rely on underlying layers to transfer the data across the network.

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.

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.

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).

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.

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.

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.

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.

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.

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.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.

Network protocols can be divided into three main categories: communication protocols, management protocols, and security protocols.

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.
Communication Protocols - TCP, UDP, HTTP,DNS

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.

Note: The encryption protocols mentioned do not conceal the source or destination IP address of network traffic. This means a malicious actor can still learn some basic information about the network traffic if they intercept it.

NAT- Network Address Translation is responsible for communication by translating between the public IP address and private IP address.NAT is a part of layer 2 (internet layer) and layer 3 (transport layer) of the TCP/IP model.

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) 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 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 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 (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

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 (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.

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.The flaws with WEP were in the protocol itself and how the encryption was used. WPA addressed this weakness by using a protocol called Temporal Key Integrity Protocol (TKIP). WPA encryption algorithm uses larger secret keys than WEPs, making it more difficult to guess the key by trial and error.

WPA also includes a message integrity check that includes a message authentication tag with each transmission. If a malicious actor attempts to alter the transmission in any way or resend at another time, WPA's message integrity check will identify the attack and reject the transmission.

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. If they set the new key to all zeros, it is as if the transmission is not encrypted at all.Because of this significant vulnerability, WPA was replaced with an updated version of the protocol called WPA2.

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.

- 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.

Subnetting is the subdivision of a network into logical groups called subnets. It works like a network inside a network.Classless addressing replaces classful addressing. Classless Inter-Domain Routing (CIDR) is a method of assigning subnet masks to IP addresses to create a subnet. Classful addressing was used in the 1980s as a system of grouping IP addresses into classes (Class A to Class E). Each class included a limited number of IP addresses, which were depleted as the number of devices connecting to the internet outgrew the classful range in the 1990s. Classless CIDR addressing expanded the number of available IPv4 addresses.

Forward proxy server regulates and restricts a person's access to the internet. Reverse proxy server restricts the internet access to an internal server.

Next generation firewalls (NGFWs) are the most technologically advanced firewall protection. They exceed the security offered by stateful firewalls because they include deep packet inspection (a kind of packet sniffing that examines data packets and takes actions if threats exist) and intrusion prevention features that detect security threats and notify firewall administrators. NGFWs can inspect traffic at the application layer of the TCP/IP model and are typically application aware. Unlike traditional firewalls that block traffic based on IP address and ports, NGFWs rules can be configured to block or allow traffic based on the application. Some NGFWs have additional features like Malware Sandboxing, Network Anti-Virus, and URL and DNS Filtering.

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 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 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.

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.

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.

Passive packet sniffing - attack where packets are read in transit

Active packet sniffing - attack where packets are manipulated in transit

A **smurf attack** is a network attack that is performed when an attacker sniffs an authorized user's IP address and floods it with packets. Once the spoofed packet reaches the broadcast address, it is sent to all of the devices and servers on the network

Ping of death: A type of DoS attack caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64KB
Replay attack: A network attack performed when a malicious actor intercepts a data packet in transit and delays it or repeats it at another time

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.

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. An improperly configured user role increases risk by allowing unauthorized users to have access to critical cloud operations.

Modern encryption relies on keeping the encryption keys secure. Below are the measures you can take to further protect your data when using cloud applications:

- 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.

Tools of the Trade- SQL & Linux

The **Basic Input/Output System (BIOS)** is a microchip that contains loading instructions for the computer and is prevalent in older systems. The **Unified Extensible Firmware Interface (UEFI)** is a microchip that contains loading instructions for the computer and replaces BIOS on more modern systems.

Components of Linux:
1)User
2)Applications
3) Shell
4) Filesystem Hierarchy Standard
5)Kernel
6) Hardware

The **Filesystem Hierarchy Standard (FHS)** is the component of the Linux OS that organizes data. It specifies the location where data is stored in the operating system.

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

The kernel is the component of the Linux OS that manages processes and memory. It communicates with the applications to route commands. The Linux kernel is unique to the Linux OS and is critical for allocating resources in the system. The kernel controls all major functions of the hardware, which can help get tasks expedited more efficiently.

the Red Hat Package Manager (RPM) can be used for Linux distributions derived from Red Hat, and package managers such as dpkg can be used for Linux distributions derived from Debian.

Package management tools are sometimes utilized instead of package managers because they allow users to more easily perform basic tasks, such as installing a new package. Two notable tools are the Advanced Package Tool (APT) and Yellowdog Updater Modified (YUM).

cat- displays content of the file
Head - displays first 10 lines of the file
Tail - displays the last 10 lines of file
Pwd- gives the present working directory
Less -gives the content of 1 page at a time

For example, you might want to find all files in the **`projects`** directory that contain the word “log” in the file name. To do this, you’d enter **`find /home/analyst/projects -name "*log*"`**. You could also enter **`find /home/analyst/projects -iname "*log*"`**.
In these examples, the output would be all files in the **`projects`** directory that contain **`log`** surrounded by zero or more characters. The **`"*log*"`** portion of the command is the search criteria that indicates to search for the string “log”. When **`-name`** is the option, files with names that include **`Log`** or **`LOG`**, for example, wouldn’t be returned because this option is case-sensitive. However, they would be returned when **`-iname`** is the option.
Note: An asterisk (**`*`**) is used as a wildcard to represent zero or more unknown characters.

Security analysts might also use **`find`** to find files or directories last modified within a certain time frame. The **`-mtime`** option can be used for this search. For example, entering **`find /home/analyst/projects -mtime -3`** returns all files and directories in the **`projects`** directory that have been modified within the past three days.
The **`-mtime`** option search is based on days, so entering **`-mtime +1`** indicates all files or directories last modified more than one day ago, and entering **`-mtime -1`** indicates all files or directories last modified less than one day ago.

For example, **`ls /home/analyst/reports | grep users`** returns the file and directory names in the **`reports`** directory that contain **`users`**. Before the pipe, **`ls`** indicates to list the names of the files and directories in **`reports`**. Then, it sends this output to the command after the pipe. In this case, **`grep users`** returns all of the file or directory names containing **`users`** from the input it received.

The **`mkdir`** command creates a new directory.The **`rmdir`** command removes, or deletes, a directory.The **`touch`** command creates a new file.The **`rm`** command removes, or deletes, a file.The **`mv`** command moves a file or directory to a new location, and the **`cp`** command copies a file or directory into a new location. The first

argument after `mv` or `cp` is the file or directory you want to move or copy, and the second argument is the location you want to move or copy it to.

When used with `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. The **>** operator should be used carefully, because it's not easy to recover overwritten files.

Both the **>** and **>>** operators will create a new file if one doesn't already exist with your specified name.

In Linux, permissions are represented with a 10-character string. Permissions include:

- **read**: for files, this is the ability to read the file contents; for directories, this is the ability to read all contents in the directory including both files and subdirectories
- **write**: for files, this is the ability to make modifications on the file contents; for directories, this is the ability to create new files in the directory
- **execute**: for files, this is the ability to execute the file if it's a program; for directories, this is the ability to enter the directory and access its files

These permissions are given to these types of owners:

- **user**: the owner of the file
- **group**: a larger group that the owner is a part of
- **other**: all other users on the system
- `ls -a`: Displays hidden files. Hidden files start with a period (`.`) at the beginning.
- `ls -l`: Displays permissions to files and directories. Also displays other additional information, including owner name, group, file size, and the time of last modification.
- `ls -la`: Displays permissions to files and directories, including hidden files. This is a combination of the other two options.

```
chmod u+rwx,g+rwx,o+rwx login_sessions.txt
chmod u=r,g=r,o=r login_sessions.txt
```

`sudo useradd -g security fgarcia adds fgarcia as a new user and assigns their primary group to be security.`
`To use the -G option, the supplemental group must be passed into the command after -G. You can add more than one supplemental group at a time with the -G option. Entering sudo useradd -G finance,admin fgarcia adds fgarcia as a new user and adds them to the existing finance and admin groups.`

To change the primary group of an existing user, you need the `-g` option. For example, entering `sudo usermod -g executive fgarcia` would change `fgarcia`'s primary group to the `executive` group.
To add a supplemental group for an existing user, you need the `-G` option. You also need a `-a` option, which appends the user to an existing group and is only used with the `-G` option. For example, entering `sudo usermod -a -G marketing fgarcia` would add the existing `fgarcia` user to the supplemental `marketing` group.

When changing the supplemental group of an existing user, if you don't include the `-a` option, `-G` will replace any existing supplemental groups with the groups specified after `usermod`. Using `-a` with `-G` ensures that the new groups are added but existing groups are not replaced.
There are other options you can use with `usermod` to specify how you want to modify the user, including:

- `-d`: Changes the user's home directory.
- `-l`: Changes the user's login name.
- `-L`: Locks the account so the user can't log in.

The `userdel` command deletes a user from the system. For example, entering `sudo userdel fgarcia` deletes `fgarcia` as a user. Be careful before you delete a user using this command.
The `userdel` command doesn't delete the files in the user's home directory unless you use the `-r` option. Entering `sudo userdel -r fgarcia` would delete `fgarcia` as a user and delete all files in their home directory.

Instead of deleting the user, you could consider deactivating their account with `usermod -L`. This prevents the user from logging in while still giving you access to their account and associated permissions. For example, if a user left an organization, this option would allow you to identify which files they have ownership over, so you could move this ownership to other users.

The `chown` command changes ownership of a file or directory. You can use `chown` to change user or group ownership. To change the user owner of the `access.txt` file to `fgarcia`, enter `sudo chown fgarcia access.txt`. To change the group owner of `access.txt` to `security`, enter `sudo chown :security access.txt`. You must enter a colon (`:`) before `security` to designate it as a group name.

Similar to `useradd`, `usermod`, and `userdel`, there are additional options that can be used with `chown`.

The `man` command displays information on other commands and how they work. It's short for "manual."

The `apropos` command searches the man page descriptions for a specified string. Man pages can be lengthy and difficult to search through if you're looking for a specific keyword. To use `apropos`, enter the keyword after `apropos`.
You can also include the `-a` option to search for multiple words. For example, entering `apropos -a graph editor` outputs man pages that contain both the words "graph" and "editor" in their descriptions.

The `whatis` command displays a description of a command on a single line. For example, entering `whatis nano` outputs the description of `nano`. This command is useful when you don't need a detailed description, just a general idea of the command.

Reference Guide Linux

The `SELECT` keyword indicates which columns to return.`FROM` indicates which table to query

`ORDER BY` sequences the records returned by a query based on a specified column or columns. This can be in either ascending or descending order.

```
'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
```

- **`COUNT` returns a single number that represents the number of rows returned from your query.**

- **`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.**

Reference Guide SQL

Assets, Threats & Vulnerabilities -05

Likelihood x Impact = Risk

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.

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.

Components of the CSF

As you might recall, the framework consists of three main components: the *core*, *tiers*, and *profiles*. In the following sections, you'll learn more about each of these CSF components.

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.

Note: The core, tiers, and profiles were each designed to help any business improve their security operations. Although there are only three components, the entire framework consists of a complex system of subcategories and processes.

Regulations are rules that *must* be followed, while frameworks are resources you can *choose* to use.

3 basic elements of a security plan are standards, policies, regulations

There are three common approaches to auditing user accounts:

- Usage audits
- Privilege audits
- Account change audits

As a security professional, you might be involved with any of these processes.

Usage audits

When conducting a usage audit, the security team will review which resources each account is accessing and what the user is doing with the resource. Usage audits can

help determine whether users are acting in accordance with an organization’s security policies. They can also help identify whether a user has permissions that can be revoked because they are no longer being used.

Privilege audits

Users tend to accumulate more access privileges than they need over time, an issue known as *privilege creep*. This might occur if an employee receives a promotion or switches teams and their job duties change. Privilege audits assess whether a user's role is in alignment with the resources they have access to.

Account change audits

Account directory services keep records and logs associated with each user. Changes to an account are usually saved and can be used to audit the directory for suspicious activity, like multiple attempts to change an account password. Performing account change audits helps to ensure that all account changes are made by authorized users.
Note: Most directory services can be configured to alert system administrators of suspicious activity.

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

- **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.

- **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.

- **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.(AES,DES,3DES)
- **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.(RSA, ECC)

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

  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.

  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.

  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.

  AAA framework - Authorization Authentication Accounting

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

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.

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.

The Cybersecurity and Infrastructure Security Agency (CISA) recommends using automatic updates

Advantage: An advantage to automatic updates is that the deployment process is simplified. It also keeps systems and software current with the latest, critical patches.

Disadvantage: A drawback to automatic updates is that instability issues can occur if the patches were not thoroughly tested by the vendor. This can result in performance problems and a poor user experience.

- *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.

- **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.

Angler phishing is a technique where attackers impersonate customer service representatives on social media. This tactic evolved from people's tendency to complain about businesses online. Threat actors intercept complaints from places like message boards or comment sections and contact the angry customer via social media. Like the AIM attacks of the 1990s, they use fraudulent accounts that appear similar to those of actual businesses. They then trick the angry customers into sharing sensitive information with the promise of fixing their problem.

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.

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 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.

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.

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.

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. If the search box is vulnerable to injection, an attacker could enter a malicious query that would be executed in the database, causing it to return sensitive information like user passwords. The data that's returned is displayed back in the search box where the attack was initiated.

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
Note: Out-of-band injection attacks are very uncommon because they'll only work when certain features are enabled on the target server.

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.

PASTA -Process for Attack Simulation and Threat Analysis

Threat modeling is the process of identifying assets, their vulnerabilities, and how each is exposed to threats. It is a strategic approach that combines various security activities, such as vulnerability management, threat analysis, and incident response. Security teams commonly perform these exercises to ensure their systems are adequately protected. Another use of threat modeling is to proactively find ways of reducing risks to any system or business process.

A typical threat modeling process is performed in a cycle:

- Define the scope
- Identify threats
- Characterize the environment
- Analyze threats
- Mitigate risks
- Evaluate findings

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.

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.

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.

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.

Sound the Alarm: Detection & Response -06

5 core functions of NIST CSF are:

1) Identify
2) Protect
3) Detect
4) Respond
5) Recover

National Institute of Standards and Technology (NIST) Incident Response Lifecycle, which is a framework for incident response consisting of four phases:

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-incident activity

The job of the **security analyst** is to continuously monitor an environment for any security threats. This includes:

- Analyzing and triaging alerts
- Performing root-cause investigations
- Escalating or resolving alerts

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

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

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

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

- **A true positive** is an alert that correctly detects the presence of an attack.
- **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.
- **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.
- **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.

Many IDS tools can also operate as an IPS. Tools like Suricata, Snort, and Sagan have both IDS and IPS capabilities.

Endpoint detection and response (**EDR**) is an application that monitors an endpoint for malicious activity. EDR tools are installed on endpoints. Remember that an **endpoint** is any device connected on a network. Examples include end-user devices, like computers, phones, tablets, and more.

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

The SIEM process consists of three critical steps:

1. **Collect and aggregate data**
2. **Normalize data**
3. **Analyze data**

The Ethernet protocol uses footers to provide error-checking information to determine if data has been corrupted. In addition, Ethernet network packets that are analyzed might not display footer information due to network configurations.
Note: Most protocols, such as the Internet Protocol (IP), *do not* use footers.

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."

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.

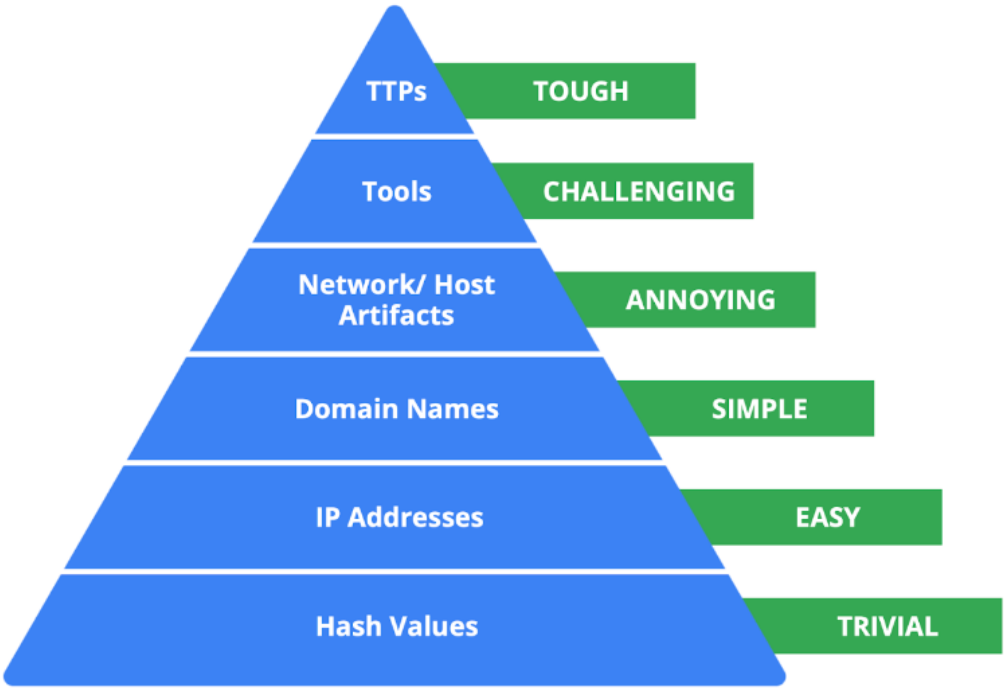
IPv6

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.

Indicators of compromise (**IoCs**) are observable evidence that suggests signs of a potential security incident. IoCs chart specific pieces of evidence that are associated with an attack, like a file name associated with a type of malware.

Indicators of attack (**IoA**) are the series of observed events that indicate a real-time incident. IoAs focus on identifying the behavioral evidence of an attacker, including their methods and intentions.



The Pyramid of Pain captures the relationship between indicators of compromise and the level of difficulty that malicious actors experience when indicators of compromise are blocked by security teams. It lists the different types of indicators of compromise that security professionals use to identify malicious activity.

effective documentation has three benefits:

1. Transparency
2. Standardization
3. Clarity

Chain of custody is the process of documenting evidence possession and control during an incident lifecycle. Chain of custody is an example of how documentation produces transparency and an audit trail.

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

To manage time and resources, security teams must prioritize how they respond to various incidents because not all incidents are equal. Here are some factors to consider when determining the priority of an incident:

- **Functional impact:** Security incidents that target information technology systems impact the service that these systems provide to its users. For example, a ransomware incident can severely impact the confidentiality, availability, and integrity of systems. Data can be encrypted or deleted, making it completely inaccessible to users. Consider how an incident impacts the existing business functionality of the affected system.
- **Information impact:** Incidents can affect the confidentiality, integrity, and availability of an organization's data and information. In a data exfiltration attack, malicious actors can steal sensitive data. This data can belong to third party users or organizations. Consider the effects that information compromise can have beyond the organization.
- **Recoverability:** How an organization recovers from an incident depends on the size and scope of the incident and the amount of resources available. In some cases, recovery might not be possible, like when a malicious actor successfully steals proprietary data and shares it publicly. Spending time, effort, and resources on an incident with no recoverability can be wasteful. It's important to consider whether recovery is possible and consider whether it's worth the time and cost.

- **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.

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.

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.
Common Log formats:

- JSON
- Syslog
- XML
- CSV
- CEF(Common event format)

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.

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.

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 process:

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.

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. After installing it, you'd configure the software to specify which logs to forward and where to send them. For example, you can configure the logs to be sent to a SIEM tool. The SIEM tool would then process and normalize the data. This allows the data to be easily searched, explored, correlated, and analyzed.

There are two types of searches you can perform to find events in Chronicle, a Unified Data Mode (UDM) Search or a Raw Log Search.

Through a UDM Search, Chronicle searches security data that has been ingested, parsed, and normalized. A UDM Search retrieves search results faster than a Raw Log Search because it searches through indexed and structured data that’s normalized in UDM.

UDM events contain a set of common fields including:

- **Entities**: Entities are also known as nouns. All UDM events must contain at least one entity. This field provides additional context about a device, user, or process that’s involved in an event. For example, a UDM event that contains entity information includes the details of the origin of an event such as the hostname, the username, and IP address of the event.
- **Event metadata**: This field provides a basic description of an event, including what type of event it is, timestamps, and more.
- **Network metadata**: This field provides information about network-related events and protocol details.
- **Security results**: This field provides the security-related outcome of events. An example of a security result can be an antivirus software detecting and quarantining a malicious file by reporting "virus detected and quarantined."

Raw Log Search supports the use of regular expressions, which can help you narrow down a search to match on specific patterns.

Automate Tasks with Python-07

These are some specific areas of cybersecurity in which Python might be used to automate specific tasks:

- Log analysis
- Malware analysis
- Access control list management
- Intrusion detection
- Compliance checks
- Network scanning

Tuples are more memory efficient than lists, so they are useful when you are working with a large quantity of data.

range(0,10) prints from 0 to 9

The **Python Standard Library** is an extensive collection of Python code that often comes packaged with Python. It includes a variety of modules, each with pre-built code centered around a particular type of task.

- The `re` module, which provides functions used for searching for patterns in log files
- The `csv` module, which provides functions used when working with `.csv` files
- The `glob` and `os` modules, which provide functions used when interacting with the command line
- The `time` and `datetime` modules, which provide functions used when working with timestamps

You can use these additional symbols to match to specific kinds of characters:

- `.` matches to all characters, including symbols
- `\d` matches to all single digits [0-9]
- `\s` matches to all single spaces
- `\.` matches to the period character

Link

Put it to Work-08

Data custodians assign and remove access to software or hardware. Custodians are responsible for implementing security controls for the data they are responsible for, granting and revoking access to that data, creating policies regarding how that data is stored and transmitted, advising on potential threats to that data, and monitoring

the data. Data custodians are notified when data security controls need to be strengthened or have been compromised.