Notes on Cyber security.

As a security analyst my work is to protect people and organisations from attacks...

**Roles of an analyst**

Protection against external and internal threats...

Meets regulatory compliance...

Maintains and improves business productivity...

Reduce expenses...

Maintaining brand trust...

**Job titles**

1. security analyst of specialist
2. cyber security analyst or specialist
3. security operations centre analyst
4. Information security analyst...

**Responsibilities of a security analyst**

1. Protecting computer and network systems
2. Installing prevention software.
3. Conducting periodic audits…

Transferable skills that might be important in cyber security

1. Communication… often needs to describe the threats to people who do not have a tech background. Interpreting security procedures to employees or report findings to supervisors.
2. Collaboration. they often work together with teams of engineers etc…
3. Analysis… complex scenarios they may encounter… make recommendations as to how different tools can enhance security.
4. Problem solving… Understanding threat actors and identifying trends.

**Technical Skills**

1. Programming languages
2. Security information and event management (SIEM) tools… talls you that an unknown user has accessed the system.
3. Computer forensics…digital forensic investigators…

Historical attacks

1. The brain virus
2. The Morrison worm
3. The Equifax breach

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

My role is to identify and manage inappropriate use of tech that may place my org and uses at risk…

1. Conduct regular trainings. Which I may lead.

PHISHING

The use of digital communications to trick people into revealing sensitive data or deploying malicious software. Examples of phishing include spear phishing, smishing, vishing, whaling and Email something…

Malware – virus, worms,

CISSP

1. SECURITY AND RISK MANAGEMENT: here my job is to define security goals and obj, risk mitigations, compliance, business continuity and the law. Update policies made by the government.

2. ASSET SECURITY: MY Job here is to secure digital and physical assests. Storage retention, maintenance and destruction of data. For example, when old equipment is disposed, all confidential information is wiped completely.

3. SECURITY ARCHITECTURE AND ENGINEERING- optimises data security by ensuring that effective tools, systems, and processes are in place. For example, configuring a firewall.

4 COMMUNICATION AND NETWORK SECURITY – securing physical networks and wireless communications. E.g. discovering that users are connection to unsecure wireless hotspots. I will then produce a policy to mitigate risks and keep people and data safe.

1. IDRNTITY AND ACCESS MANAGEMENT – data security making sure users follow policies to control and manage physical assets. Documenting access roles. For example, setting up an employee’s key card access.
2. SECURITY ASSESSMENT AND TESTING – conducting security control testing, collecting, and analysing data and conducting security audit to monitor for risks threats and vulnerabilities. Just making sure that users have the correct access and only what they need. Make sure that no unauthorised person has access.
3. Security Operations – conducting investigations and implementing preventative measures.
4. SOFTWARE DEVELOPMENT SECURITY: uses secure coding practices which are a set of recommended guidelines that are used to create secure applications and services.

My job is to identify my orgs critical assets and risks. And them implement the necessary frameworks and controls…

SECURITY FRAMEWORKS ARE guidelines used for building plans to help mitigate risk and threats to data and privacy.

PUROOSE OF SEC FRAMEWORKS

1. Protecting PII
2. Securing financial information
3. Identifying security weaknesses
4. Managing organisational risks
5. Aligning security with business goals.

COMPONENTS OF FRAMEWORKS

1. Identifying and documenting security goals. GDPR. I may be asked to document areas where we aren’t compliant with GDPR
2. I will also have to set guidelines to achieve security goals.
3. Implementing strong security processes. Eg social media company… making sure policies are developed on the handling of data requests. For examples when
4. Monitoring and communicating results: monitor and report a certain sec issue affecting GDPR

SECURITY CONTROLS

Safeguards designs to reduce specific security risks…eg employees required to complete a privacy training. Using a software tool to know who has completed this training.

**CIA** = CONFIDENTIALITY- ONLY AUTHORISED USERS CAN ACCESS SPECIFIC DATA

INTEGRITY- DATA IS CORRECT, AUTHENTIC AND RELIABLE. For example using encryption

AVAILABILITY - DATA IS AVAILABLE TO THOSE WHO ARE AUTHORISED TO ACCESS IT.

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

**security lifecycle**: As a reminder, a security lifecycle is a constantly evolving set of policies and standards.

**The Federal Risk and Authorization Management Program (FedRAMP®)**

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

***Security ethics*** *are guidelines for making appropriate decisions as a security professional.*

**PRINCIPLES OF ETHICS**

**The first ethical principle, confidentiality**: For example, you may want to help out a coworker by providing computer system access outside of properly documented channels.

**The second ethical principle to consider is privacy protections.** Privacy protection means safeguarding personal information from unauthorized use. For example, imagine you receive a personal email after hours from your manager requesting a colleague's home phone number.

**A third important ethical principle we must discuss is the law.** Laws are rules that are recognized by a community and enforced by a governing entity. For example, consider a staff member at a hospital who has been trained to handle PII, and SPII for compliance. The staff member has files with confidential data that should never be left unsupervised, but the staff member is late for a meeting. Instead of locking the files in a designated area, the files are left on the staff member's desk, unsupervised.

Commonly Used Cyber Security Tools

Log - A log is a record of events that occur within an organization's systems. Examples of security-related logs include records of employees signing into their computers or accessing web-based services

**Security information and event management tools:** A SIEM tool is an application that collects and analyzes log data to monitor critical activities in an organization. It collects real time or instant information to identify potential breaches. SIEM tools reduce the amount of data an yanalyst must review by providing alerts for specific types of risks and threats.

Commonly used SIEM tools

1. **Splunk**: Splunk is a data analysis platform, and Splunk Enterprise provides SIEM solutions.  Splunk Enterprise is a self-hosted tool used to retain, analyse, and search an organization's log data.
2. **Chronicle**: Google’s Chronicle is a cloud-native SIEM tool that stores security data for search and analysis
3. **Playbooks**: A playbook is a manual that provides details about any operational action, such as how to respond to an incident including incident response, security or compliance reviews, access management, and many other organizational tasks that require a documented process from beginning to end. Playbooks, which vary from one organization to the next, guide analysts in how to handle a security incident before, during, and after it has occurred.
4. **Network protocol analyser** - Packet sniffer:  A packet sniffer is a tool designed to capture and analyze data traffic within a network. Common network protocol analyzers include ***tcpdump*** and **Wireshark**.

Types of playbook

1. Chain of custody playbook:  is the process of documenting evidence possession and control during an incident lifecycle
2. **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. 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.

Programming allows analysts to complete repetitive tasks and processes with a high degree of accuracy and efficiency. It also helps reduce the risk of human error, and can save hours or days compared to performing the work manually

**Linux Use case**

A common use of Linux for entry-level security analysts is examining logs to better understand what's occurring in a system. For example, you might find yourself using commands to review

an error log when investigating uncommonly high network traffic.

**SQL USE CASE**

SQL is a programming language used to create, interact with, and request information from a database. Filter through datapoints to filter information.

**PYTHON**

Security professionals can use Python to perform tasks that are repetitive and time-consuming and that require a high level of detail and accuracy.

**COURSE 2**

**Threat:** any circumstance or event that can negatively impact assets.

**RISK**: anything that can impact the confidentiality, integrity or availability of an asset.

**Vulnerability**: a weakness that can be exploited by a threat. Examples of vulnerabilities include: an outdated firewall, software, or application; weak passwords; or unprotected confidential data.

People can also be considered a vulnerability.

RANSOMEWARE: a malicious attack where threat actors encrypt an organisation’s data and demand payment to restore access.

**FINANCIAL CONSEQUENCES** can be significant—

* 1. interrupt production
  2. cost to correct the issue.
  3. and fines due to non-compliance.

**IDENTITY THEFT**- orgs must decide to store data and for how long. Including PII which can be sold in the dark web. **DAMAGE TO AN ORGS REPUTATION:**

Customers will seek new business relationships…result in legal penalties and fines…

NIST RISK’S MANAGEMENT FRAMEWORK (national institute of security and technology)

7 steps in the RMF

Prepare: activities that are necessary to manage security and privacy risks before a breach occurs.

Categorise: used to develop risk management processes and tasks…

Select: choose customise and capture documentation of the controls that protect an organisation. For example, keeping playbooks and other essential documents up to data.

Implement: implement security and privacy plans for the organisation.

Assess: determine if established controls are implemented correctly.

Authorise: being accountable for the security and privacy risks that may exist in an organisaition. Generating reports, developing plans of action and establishing project milestones that are related to my orgs sec goals.

Monitor: be aware of how systems are operating.

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

**Threats**

* **Insider threats:** Staff members or vendorsabuse their authorized access to obtain data that may harm an organization.
* **Advanced persistent threats (APTs):** A threat actor maintains unauthorized access to a system for an extended period of time.

**Risks**

* **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.

**Vulnerabilities**

A **vulnerability** is a weakness that can be exploited by a threat.

* **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.

SECURITY FRAMEWORKS

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

**Remember, people are the biggest threat to security!!**

Employee awareness and educate them about how they can protect the organization, their co-workers, and themselves. Educating employees about existing security challenges is

essential for minimizing the possibility of a breach.#

While frameworks are used to create plans to address security risks, threats, and vulnerabilities,

controls are used to reduce specific risks.

Security controls are safeguards designed to reduce specific security risks.

Types of Security controls

* Encryption - the process of encoding the data. Converting the data from plaintext to cypher text. Unreadable to humans and computers. Used to ensure confidentiality
* Authentication - the process of identifying who someone or something is. Example is logging in to a website with a username and password. More advance methods are MFA, challenge the user to demonstrate thy are who they claim to be.

VISHING- THIS is a social engineering attack. It is the exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source.

* Authorization - the concept of granting to specific resources in system. It is used to verify that someone has access to a specific resource.

**Examples of controls:**

Physical: Gates, fences and locks; security guards, CCVs, motion detectors, access cards or badges.

Technical: Firewalls, MFA, Antivirus

Administrative: separation of duties, authorisation, asset classification.

**THE CIA TRIAD**

This is a model that helps inform how organisation consider risk when setting up systems and security policies.

Confidentiality - only authorised users can access specific assess or data. Data should be available on a NEED-TO-KNOW basis.

Integrity - data is correct, authentic and reliable.

Availability - the data is accessible for those who are authorised to access it. Ensuring that systems and networks are functioning properly to ensure reliable access may be part of my everyday responsibilities.

NIST CYBERSECURITY FRAMEWORK - The CSF is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk.

5 CORE FUNCTIONS OF THE NIST CSF FRAMEWORK IDPRR

IDENTIFY - The first core function is identify, which is related to the management of cybersecurity risk and its effect on an organization's people and assets. The CSF identify function relates to monitoring systems and devices in an organization’s internal network to help security teams manage potential cybersecurity risks and their effects.

PROTECT - The second core function is protect, which is the strategy used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats. Coming up to unfamiliar threats and attakcks, studying historical data and making improvements to policies and procedures is essential.

DETECT - which means identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections.

RESPOND - The fourth function is respond, which means making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process.

RECOVER - which is the process of returning affected systems back to normal operation.

IPDRR

Open Worldwide Application Security Project SECURITY PRINCIPLES

1. MINIMISE THE ATTACK SURFACE AREA: An attack surface refers to all the potential vulnerabilities that a threat actor could exploit, like attack vectors, which are pathways attackers use to penetrate security defenses.

2. The principle of least privilege means making sure that users have the least amount of access required to perform their everyday tasks.

3. Defense in depth: Defense in depth means that an organization should have multiple security controls that address risks and threats in different ways.

4. Another principle is separation of duties:  can be used to prevent individuals from carrying out fraudulent or illegal activities. This principle means that no one should be given so many privileges that they can misuse the system.

5. Keep security simple: when implementing security controls, unnecessarily complicated solutions should be avoided because they can become unmanageable

6.  Fix security issues correctly: identify the root cause quickly

7. **Establish secure defaults: the optimal security state of an application is also its default state for users. It should take extra work to make the application insecure.**

**8. Fail Securely: when a control fails or stops, it should do so y 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.**

**9. Don’t trust devices: when woring with third party partners, be care of their own security policies which might be different from yours. Do not explicitly trust that a partner organisation is secure. Be careful that the balance is accurate before sharing data with third-party customers or vendors.**

**10. Avoid Security by Obscurity: let your method of keeping systems secure not just be by hiding things, like passwords or keeping the source code secret. Referencing OSWAP, the security of an application should not rely on keeping the source code secret. Its security should rely upon many factors, including reasonable password policies, defense in depth, business transaction limits, solid network architecture and fraud and audit controls.**

**PLANNING A SECURITY 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.

**This is a review of an orgs security controls, policies and procedures against a set of expectations.**

* 1. **Internal and external security audits.**
  2. **Internal sec audit is conducted by a team of people.**
  3. **It is used to help improve an orgs sec posture and help them avoid fines due to lack of compliance.**

**PURPOSES OF INTERNAL SECURITY AUDITS**

* 1. **Identify organisational risk.**
  2. **Assess controls.**
  3. **Correct compliance issues.**

Common elements of Internal audits

1. Establishing the scope and goals: scope is the specific criteria of an internal security audit. They identify people assets, policies, procedures and technologies that might impact the organisation’s security posture… Goals are an outline of the organisations security objectives.
2. Conducting a risk assessment: a risk assessment is focused on identifying potential threats, risks, and vulnerabilities. This helps organizations consider what security measures should be implemented and monitored to ensure the safety of assets.

Before completing these last three elements, you'll need to review the scope and goals,

as well as the risk assessment and ask yourself some questions. For example: What is the audit meant to achieve? Which assets are most at risk? Are current controls sufficient to protect those assets? If not, what controls and compliance regulations need to be implemented?

1. Completing a controls assessment: A controls assessment involves closely reviewing an organization's existing assets, then evaluating potential risks to those assets, to ensure internal controls and processes are effective. I might need to classify controls into administrative, physical and technical controls.

Administrative controls are related to the human component of cybersecurity. They include policies and procedures that define how an organization manages data, such as the implementation of password policies.

Technical controls are hardware and software solutions used to protect assets, such

as the use of intrusion detection systems, or IDS's, and encryption.

Physical controls refer to measures put in place to prevent physical

access to protected assets, such as surveillance cameras and locks.

1. Assessing compliance: compliance regulations are laws that organizations must follow to ensure private data remains secure. For example if they are doing business and are collecting credit card details from customers in the EU they must abide by the GDPR and the PCI DSS- payment card industry, data security standard
2. Communicating results. When the audit is complete, results and recommendations need to be communicated to stakeholders. It summarises the scope and goals of the audit, then it lists existing risks and note how quickly those risks need to be addressed. It also identifies compliance regulations the org needs to heed to and provides recommendation to improve the orgs security posture.

SECURITY INFORMATION AND EVENT MANAGEMENT DASHBOARDS.

Log: a record of events that occur within an orgs systems and networks.

Log sources: firewall logs, network logs, server logs.

Firewall logs: a record of attempted or established connections for incoming traffic from the internet. It also includes outbound requests to the internet from within the network.

Network log: a record of all computers and devices that enter and leave the network. It also records connections between devices and services on the network.

Server log: a record of events related to services such as websites emails or file shares. It includes actions such as login, password and username requests.

SIEM tool: is an application that collects and analyses log data to monitor critical activities in an organisation. Provides real time visibility, event monitoring and analysis, and automated alerts. Stores all data in a centralised location.

These tools can also be used to create dashboards. Provides information in an format that is easy to understand. Makes it easy to understand data. Siem dashboards help sec analysts to quickly access security analyst through, charts graphs or tables. It provides different metrics such as response time, availability and failure rate which are used to assess the performance of a software application.

**Security orchestration, automation, and response (SOAR)** is a collection of applications, tools, and workflows that uses automation to respond to security events.

**EXPLORING SECURITY INFORMATION AND EVENT MANAGEMENT TOOLS**

Splunk Enterprise, Splunk Cloud, and Chronicle are common SIEM tools that many organizations use to help protect their data and systems.

Splunk Enterprise is a self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time.

Splunk Cloud is a cloud-hosted tool used to collect, search, and monitor log data. Splunk Cloud is helpful for organizations running hybrid or cloud-only environments, where some or all of the organization's services are in the cloud.

Google's Chronicle. Chronicle is a cloud-native tool designed to retain, analyze, and search data. Chronicle provides log monitoring, data analysis, and data collection.

PHASES OF INCIDENT RESPONSE PLAYBOOKS

PLAYBOOK: this is a manual that provides details about any operational action.

They clarify what tools to use in response to a sec incident.

**Urgency, efficiency, and accuracy are necessary to quickly identify and mitigate a security threat to reduce potential risk.**

They ensure people follow a consistent list of actions in a prescribed way

regardless of who is working on the case.

INCIDENT RESPONSE PLAYBOOK

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

Phases of incident response

* 1. Preparation: organisation must be prepared to mitigate the likelihood of threats by documenting procedures, establishing staffing plans, and educating users.
  2. Detection and analysis: detect and analyse events using defined processes and technology.
  3. Containment: prevent further damage and reduce the immediate impact of a security incident. Helps prevent on going attack.
  4. Eradication and recovery: involves the complete removal of an incidents artifacts so that org can return to normal operation. Also known as IT restoration.
  5. Post incident activity: This phase includes documenting the incident, informing organizational leadership, and applying lessons learned to ensure that an organization is better prepared to handle future incidents.
  6. Coordination: Coordination involves reporting incidents and sharing information, throughout the incident response process.

the incident response process, based on the organization's established standards.

EXPLORE INCIDENT RESPONSE

Different playbooks are used for different attacks.

**WELCOME TO COURSE 3:**

Connect and Protect: Networks and Network Security

A NETWORK IS A GROUP OC CONNECTED DEVICES… devices can communicate through LAN or a WAN. A LAN is a network that spans a small area like an office building, a school or a home… for example, when my phone connects to my router it forms a LAN. A WAN is a wide area network that spans a large geographic area like a city, state or a country. The INTERNET IS one big WAN.

NETWORK TOOLS

HUB: a network device that broadcasts information to every device on the network, like a radio tower.

SWITCH: a device that makes connections between specific devices on a network by sending and receiving data between them. It is more intennigent than a hub by only sending data to the intended destination.

ROUTER: connects multiple networks together.

MODEM: a device that connects your router to the internet and brings internet access to the LAN.

VIRTUALIZATION TOOLS: these are pieces of software that perform network operations. They provide opportunities for cost saving and reliability/ scability

Network devices : these are devices that maintain information and services for users of a network

AWS Academy Mentor @ e-Careers | AWS Solutions Architect Pro

As an AWS Academy Mentor at e-Careers, I help learners achieve their cloud computing goals and prepare them for the AWS Solutions Architect Pro certification. I have over two years of experience in cloud services, cloud infrastructure, and AWS cloud migration, as well as multiple certifications in communication, marketing, and human resources. I am also passionate about language and culture, and I currently work as a Culture and Language Exchange Officer at the University of Hull, where I facilitate intercultural communication and learning among students and staff. Additionally, I have a six-month experience as a Pre-Sessional EAP Tutor at the same university, where I supported international students in developing their academic English skills. I hold a first-class honours degree in English Language and Literature from the University of Port Harcourt, and I am currently pursuing a master's degree in TESOL at the University of Hull. My core competencies include cloud services, cloud infrastructure, AWS cloud migration, language teaching, intercultural communication, and online learning. My mission is to empower learners and educators with the skills and knowledge they need to succeed in the digital and global world.

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

**Cloud network;** is a collection of servers of computers that stores resources and data in a remote data centres that can be accessed via the internet. They make it possible to use servers from anywhere in the world.

Cloud service offer on demand storage, processing power, business and analysitcs…

Companies can consume services in an elastic utility model…

NETWORK COMMUNICATION

A packet contains a header, body and footer

Header: contains the IP address, the MAC address an the protocol number.

Body: message that is to be transmitted to the receiving device.

Footer: signature on a letter. Tells the receiving device that the packet is finish.

BANDWIDTH: The amount of data that a device received per second. It is measured by dividing the quantity of data by the time in seconds. quantData/timepersec

SPEED: the rate at which the data packet is received or downloaded.

PACKET SNIFFING: the practice of capturing and inspecting data packets across a network.

TCP/IP MODEL - transmission control protocol and Internet protocol.

TCP- this protocol is an internet communication protocol that allows two devices to form a connection and stream data. It includes a set of instructions to organise data.

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

When data packets are sent or received via a network, they are assigned a port.

PORT: a software-based location that organises the sending and receiving of data between devices on a network. Port divide network traffic into SEGMENTS based on the service they function will perform between two devices.

PORT NUMBERS Port numbers allow computers to split the network traffic and prioritize the operations they will perform with the data.

PORT NUMBERS

25= email port

443 = internet comms=20 for large file transfers…

**NETWORK PROTOCOLS**

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

ADDRESS RESOLUTION PROTOCOL

This is a network protocol used to determine the MAC address of the next router or device on the path.

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

It can use PORT FILTERING to limit certain port numbers.

Types of firewalls

Hardware inspects each packet before it is allowed into the network. It is physical device as opposed to a software firewall.

Software firewalls are installed on a computer or on a server and they add some processing burden on the devices on which they are installed.

Instead of passing through all that hassle, companies may choose to use FAAS offered by cloud providers. CLOUD BASED firewalls. Organisations can configure these firewalls so that can access and analyse all network data before they are allowed into the orgs network.

STATEFUL FIREWALL: Stateful refers to a class of firewall that keeps track of information passing through it and proactively filters out threats. A stateful firewall analyses network traffic for characteristics and behaviour that appear suspicious and stops them from entering the network

STATELESS FIREWALL: Stateless refers to a class of firewall that operates based on predefined rules and does not keep track of information from data packets. A stateless firewall only acts according to preconfigured rules set by the firewall administrator.

Next GENERATION FIREWALL: provides even more security than a stateful firewall. Not only does an NGFW provide stateful inspection of incoming and outgoing traffic, but it also performs more in-depth security functions like deep packet inspection and intrusion protection. Some NGFWs connect to cloud-based threat intelligence services so they can quickly update to

protect against emerging cyber threats.

VIRTUAL NETWORKS

VPN, is a network security service that changes your public IP address and hides your virtual location so that you can keep your data private when you're using a public network like the internet.

SECURITY ZONES

These are segments of a network that protects the internal network from the internet.

NETWORK SEGMENTATION

This is a security technique that divides networks into segments with their separate permissions and security rules.

**An org can divide their networks into subnets.**

**Types of security zones:**

1. Uncontrolled zone: any network outside the organisations control.
2. Controlled zone: a subnet that protects the internal network from the uncontrolled zone.

DMZ: contains public facing services that can access the internet including web servers, proxy servers and DNS servers, email and file servers.

Restricted Zone: protects highly confidential information that is only accessible to certain employees with certain privileges.

PROXY SERVERS

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

It uses a different public IP address from that of the internal network. It hides the private network’s address and replaces that with a different IP address. It can also be used to block access to websites which are not allowed from within the organization. It also has temporary memory which it used to store data that is regularly requested for by internal networks. This reduces contact with the internal server.

TYPES OF PROXY SERVERS,

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

The goal is to hide a user's IP address and approve all outgoing requests. In the context of an organization, a forward proxy server receives outgoing traffic from an employee, approves it, and then forwards it on to the destination on the internet.

1. REVERSE PROXY SERVER: regulates and restricts the internet access to an internal server. The goal is to accept traffic from external parties, approve it and then forward it to the internal servers.
2. EMAIL PROXY SERVER. It filters spam email by verifying whether a senders address was forged. This reduces the risk of phishing attacks that impersonate people known to the organisation.

**INTRODUCTION TO NETWORK INTRUSION TACTICS**

Common network intrusion attacks include

Malware, spoofing, packet sniffing, packet flooding

They can harm an organization by

1. Leaking confidential information
2. Damaging an organisations reputation
3. Impacting customer retention
4. Costing money and time.

NETWORK INTERCEPTION ATTACKS

Packet sniffing is when a threat actor intercepts data in transit and captures some of the data or disrupts the transmission in some way. For example the threat actor can change the bank account to one he controls therefore diverting the money.

Backdoor Attacks.

Backdoors are weaknesses intentionally left by programmers or system and network administrators that bypass normal access control mechanisms. They use those back doors to troubleshoot or conduct administrative tasks. Byut they can also be isntalled by attackers after they have comprised an organisation to ensure they have persistent access.

**DDOS ATTACKS**

The objective of a denial of service attack, or a DoS attack, is to disrupt normal business operations by overloading an organization's network. The goal of the attack is to send so much information to a network device that it crashes or is unable to respond to legitimate users. This means that the organization won't be able to conduct their normal business operations, which can cost them money and time. A network crash can also leave them

vulnerable to other security threats and attacks.

TYPES OF DOS ATTACK

1. SYN FLOOD ATTACK: this type of attach simulates a TCP connection and floods a server with syn packets. This happens at the handshake process used to establish tcp connection.
2. ICMP attack: icmp is an internet protocol used by devices to tell each other about data transmission errors across a network. Like a request for a status update. This is a kind of attack in which an attacker repeatedly sends an ICMP requests. This uses up all the incoming bandwidth causing the server not to function.
3. The Ping of Death: tis is a type of DOS attach in which a server receives an oversized ICMP packet that is bigger than 64 kilobytes which is the actual max size for such a packet.

PACKET SNIFFING

Using software tools to observe data in as it moves across a network. I can use it to capture packets when debugging or investigating incidents.

Malicious actors can also do this. Their goal is fo find valuable information in the data packets they can use to their own advantage/ They can use a software or a hardware device to do this. They can make changes to the data.

They can make changes to the data by altering the recepients account number.

PASSIVE PACKET SNIFFING: here data is read in transit. Compare this to a post delivery person reading someone’s mail.

ACTIVE PACKET SNIFFING: manipulating the data in transit by injecting internet protocols to redirect it or changing the information the packet contains. It is like a neighbor telling a delivery person that they’d deliver the letter but read it before.

PREVENTION

1. Using a VPN to protect the network.
2. The website uses the HTTPS protocol. It uses the SSL/TLS
3. Avoiding unprotected WIFI. This means that anyone on the network can access all the data that flows through that network.

IP SPOOFING: here they change the source IP address of a packet to impersonate an authorized system and gain access to a network. They are just impersonating an authorized system to gain access. They are pretending to be someone they are not. They use this to bypass firewall rules that may have blocked them.

Types

1. On Path attack: here they place themselves in the middle of an authorized connection and intercepts or alters the data in transit. They put themselves between two devices to learn the Ip and mac addresses of the devices communicating with each other. They can then pretend to be any of the devices in the network.
2. Replay attack: this is when a malicious actor intercepts a data packet in transit and delays it or repeats it at another time. The delay can cause connection issues. The repeated packet may cause impersonation.
3. Smurf attack: this combines a DDOS attack and a spoofing attack. The attacker sniffs the IP addresses of the target and then floods it with requests.

PREVENTION

1. Encryption should always be enabled. This stops actors from reading the data in transit.
2. IP Spoofing: firewall can be configured to protect against IP spoofing. Make sure that the firewall is configured correctly by creating a rule to reject all incoming traffic that has the same IP address as the local network.

SECURITY HARDENING

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

ATTACK SURFACE

This are all the potential vulnerabilities that a threat actor could exploit. This is likened to a door and windows in a building.

Security hardening can be conducted on any system

Hardware, operating systems applications, computer networks and databsess.

Physical security is also part of hardening like guards and cameras.

It could be also in the form of patches. They are done to fix vulnerabilities.

This could also mean changing the password policies to make them longer. Or more frequent password changes. It could also mean updating the encruption status. Keeping encryption up to date.

If you have unused applications and ports, you can disable them. you can also reduce device access permissions. It reduces the overall attack surface. It can make device monitoring more efficient and reduce the attack surface.

Another important way to increase hardening is to run frequent penetrate testing.

**PENETRATION TESTING:** this is a simulated attack that helps identify vulnerabilities in systems networks websites applications and processes. These findings are documented in a report. The org can review these vulnerabilities and come up with a plan to fix them.

**OPERATING SYSTEM HARDENING**

The operating system is the interface between the hardware and the user. It is the first program loaded when the computer turns on.

Regular OS hardening tasks

1. Updates
2. Backups
3. Keeping an up to date of devices and authorized users.

PATCH UPDATE

A patch update is a software and operating system, or OS, update that addresses security vulnerabilities within a program or product. IT IS Important to run patch updates as soon as they are released because malicious actors would know right away where the vulnerability is in the out-of-date OS.

BASELINE CONFIGURATION

This is a documented set of specifications within a system that is used as a basis for future builds releases and updates.

HARDWARE AND SOFTWARE DISPOSAL

This ensures that all old hardware is properly wiped and disposed of. It's also a good idea to delete any unused software applications since some popular programming languages have known vulnerabilities. Removing this software makes sure there is no unnecessary vulnerability.

STRONG PASSWORD POLICIES.

This means that passwords follow specific rules. For example it might require a min of 8 characters, etc.

MFA also allows a user to identify their identity using 3 things: something you know, something you have, something unique about you.

## Brute force attacks

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

Types

1. Simple brute force attack: here they simply try to guess the username and password by entering a combination of usernames and passwords until they can find one that works.
2. Dictionary attack: here they use a list oc commonly used passwords maybe those compromised in an earlier breach. Or even using words from a dictionary.

Virtual machines and sandboxes can be used to test suspicious files, check for vulnerabilities before an event occurs or to simulate a cybersecurity incident.

Prevention measures for Brute Force attack.

1. Salting and Hashing: hashing is a process that converts information into unique value that can be then used to determine its integrity. You can no longer decrypt the original text. But salting adds random characters to hashed passwords increasing the length and complexity of hash values.
2. MFA- a two or more way identity verification procedure.
3. CAPTCHA and reCAPTCHA: completely automated turing public test is used to tell computers from humans.
4. Password policies: standardised password policies help prevent attacks. For example stating how many times a password can be tried before being locked out of an account is a good step. Others include password complexity, reusing passwords and frequency of password updates.

NETWORK HARDENING

Network hardening is focused on network related hardening such as port filtering, network access privileges and encryption over networks.

Regular updates

1. Firewall rule maintenance
2. Etwork log analysis
3. Patch updates and
4. Server backups.

NETWORK LOG ANALYSIS

This is the process of examining network logs to identify events of interest. This can be done using log analyzer tool or a SIEM tool to conduct network log analysis.

SIEM TOOL gathers security data from different sources and presents it on a single dashboard. It is an application that collects and analyses log data to monitor critical activities in an organisation.

TASKS PERFORMED ONCE

1. Port filtering on firewalls: this is a firewall function that blocks or allows certain port numbers to limit unwanted communication. ONLY ALLOW PORTS THAT ARE NEEDED. DISALLOW ALL OTHERS. Networks should be set up with the most up to date wireless protocols and all others disabled.
2. Network access privileges: here network segmentation is created for different departments in an organisation. This helps you with configuring least privilege access.
3. Encryption for communication: all communication should be encrypted using the latest encryption standards. Data in restricted zones should have much higher encryption standards.

Intrusion detection systems are there to detect commonly known attacks or obvious anomalies in network traffic. It does this through packet sniffing. But it does not stop the attack when it detects anything off with the traffic. It simply reports it.

Intrusion prevention systems monitors the system for any intrusive activity and takes action to stop the activity. It also reports findings to security analysts and administrators. It is said to be INLINE meaning that if anything happens to it, eg it breaks, the private network loses connection to the internet. It detects false positives and may block legitimate connection.

FULL PACKET CAPTURE DEVICES

SIEM – SECURITY INFORMATION AND EVENT MANAGEMENT

This collects and analyses log data to monitor critical activities in an organisation. It works in real time to report anything suspicious through a centralised dashboard. It also analyses network data from IDS, IPS, firewalls and VPNs, proxies and DNS logs. It is referred to as A SINGLE PANE OF GLASS. Google’s Chronicle and Splunk are two common SIEM tools. There are many others, And you have to research the different available tools and determine which is best for your organisation.

CLOUD HARDENING

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

They require proper maintenance through hardening techniques. Hosting in the cloud does not mean that the cloud service provider prevents intrusion.

One distinction between cloud network hardening and traditional hardening is the use of a server baseline image for all server instances stored in the cloud. You can use this to compare data in the cloud servers to the baseline image to make sure that there has not been any changes.

Keep applications separate. For example, older applications should be kept separate from newer applications and software that deals with internal functions should be kept separate from front end applications seen by users.

COURSE 4: TOOLS OF THE TRADE: LINUX AND SQL

INTRODUCTION TO OPERATING SYSTEMS



The OS is the interface between the computer hardware and the user. It makes the computer run but makes it run efficiently as possible.

LEGACY OPERATING SYSTEMS

This is an OS that is outdated but still being used. Some organisations still use them because software they rely on is no compatible with newer operating systems. And it is more common in industries that use a lot of equipment that requires embedded software, that OS one that’s placed inside the components of the equipment.

HOW OPERATING SYSTEMS WORK

The job of an OS is to help other computer systems run efficiently. You don’t have to control the computer hardware. The bootloader starts up the operating system.

A user uses an application. An application is a program that performs a specific task. The app sends the request to the OS. The OS interprets the request and directs to the appropriate component of the computer’s hardware. This information is returned to the OS and it then forwards to the application.

A yellow and red sign with arrows

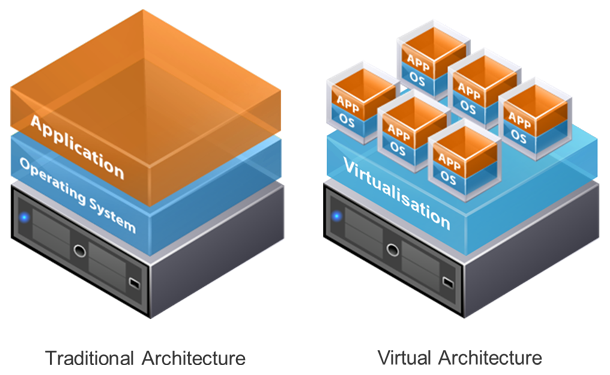
Description automatically generated

In a computer. The OS is the conductor. It handles resource and memory management to ensure the limited capacity of the computer system is used where it is needed most.

It is important that an analyst understands where the resources are uised. Understanding this usage of resource can help me respond to an incident and troubleshoot applications in the system.

VIRTUALISATION TECHNOLOGY

This is the process of using a software to create virtual representations of a physical machine or various physical machines. You can create multiple virtual machines from one physical server. So if the physical machine has 16 gb of ram for example, you can create 3 more virtual machines and allocate them 4gb of ram each. They also have their separate CPUs, storage and network. Theya re just code basically. The resources are usually allocated using a hypervisor which sits just above the hardware.



BENEFITS OF VIRTUALISATION

1. Security: VMs make it possible to isolate systems. The virtual machines are independent of the host machine and other virtual machines relying on the host machine. This makes it possible to isolate a system when it has become infected with malware. Security analysts can also intentionally place malware on a virtual machine and examine its behaviour in a more secure environment. But they are not completely safe, and the malware can still in coms cases escape virtualisation and spread to the host machine.
2. Efficiency: you can switch easily between VMs. Therefore you can streamline security tasks like testing and exploring applications.

GUI VS CLI

User interface is a programme that allows the user to control the functions of the operating system.

GuI graphical user interface: it is a user interface that uses icons on the screen to manage different tasks on the computer.

Basic components: start menu, task bar, desktop. It helps you search for applications from the start window.

CLI or command line interface: this is a text based user interface that uses commands to interact with the computer. The commands comm with the OS and exe tasks. There are no icons on the screen. It uses text languages. It is more powerful than the GUI. The CLI allows for customisation.

James remember that the user communicates with the OS through a user interface.

MODULE TWO (2)

Linux OS

WHAT MAKES LINUX UNIQUE?

It is open source which means anyone can have access to the source code. You can modify the source code. It allows developers to collaborate. It is used in many sec programmes. There are over 600 distributions of Linux.

USES CASES.

1. I will use it in examining different logs to identify what is happening in a system, eg, error logs.
2. Verify access auth in an IAM system.

THE LINUX ARCHITECTURE

1. User: the person interacting with the computer. The user initiates the tasks or the commands. More than one user can use the system’s resources at the same time.
2. Applications: this is a programme that performs a specific task. Nano is a text editor. It helps us keep notes on the screen.
3. Shell: it is how we communicate with the system. It processes the commands and outputs the results. The shell can be thought of as the CLI.
4. File system hierarchy standard: it is the component that organises data. It is like the cabinet of data. It is how data is stored in a system. It is used to organise data so that it can be found when the data is accessed by the system. It shows where the data is stored on a system. A directory is a file that organises where other files are stored.
5. Kernel: the kernel manages processes and memory. It communicates with the hardware to exe commands sent by the shell. It helps for efficient allocation of resources and makes the system work faster.
6. Hardware: this is the physical components of a computer.
7. Nano is a text based system used to store files on the screen…or something like that./..verify the information

Package manager is a tool that helps users install manage and remove packages or applications.

Different versions of linux are called distributions or distros.

Different distributions all have different reasons why they are used. The kernel is the most important part of the Linux operating system. Diff distros have diff pre-installed programmes.

KALI LINUX

It should be used on a virtual machine to prevent damage in case its tolls are improperly used.

Kali has many tools to use for pen testing.

Examples

1. METASPLOIT: used to look for vulnerabilities in a machine and exploit them
2. BURP SUITE: helps test for weaknesses in web apps
3. JOHN THE RIPPER: used in guessing passwords/ brute force attack maybe

Digital forensics is a process of collecting data and analusing it to determine what happened after an attack.

THE LINUX SHELL

The shell is the command line interpreter. The shell provides the CLI for you to interact with the OS. You have to enter the commands in the inface. The shell interacts with the kernel to exe commands. It helps you to connect application to each other.

Standard input

This consists of information received by the OS via the command line. This is like asking a friend a question during a conversation. If it can understnand the command it comms with the OS.

ECHO… this is a linux command that outputs a specified string of text.

String data is data consisting of an ordered sequence of characters.

Standard output is a specified information returned through the shell. Just like a friend gives an answer to a question.

Standard error contains messages returned by the OS through the shell. Just like someone cannot answer a question. This might occur when we misspell a command or when the system does not understand the command.

Linux commands learnt so far

1. sudo apt install suricata
2. sudo apt install tcpdump
3. sudo apt remove suricate
4. sudo apt remove tcpdump
5. apt list --installed
6. echo
7. expr for calculations. But there must be a space between the command and he numbers including between the signs and the numbers
8. clear: used to clear the bash screen

BASH SHELL: this is the most popular shell.

How to write in bash.

Command is an instruction telling the computer to do something. The dollar sign is found in Bash.

ARGUMENT: this is a specific information needed by a command. For example: echo “you are doing great”.

NOTE: ALL COMMANDS AND ARGUMENTS ARE CASE SENSITIVE

ROOT DIRECTORY: this is the highest directory in Linux. It is shown by a single slash. Sub directories branch out from the root directory.

1. Pwd: this prints the working directory on to the screen.
2. Ls: displays the names of files and directories in the current working directory
3. Cd: navigates between directories. Used when youy want to change directories
4. Cat: displays the content of a file
5. Head: used if you don’t want to display the full content of a large file. displays just the beginning of a file by default 10 lines

Standard FHS directories are those that branch out of the root directory. Some of them are:

1. /home
2. /bin: this stands for binary where binary files and other executables are stored. These executable files contain a series of commands a computer needs to follow to run programs and perform other functions.
3. /etc – this is the dir that stores system config files.
4. /tmp – used to store temporary files. /tmp dir is commonly used by attackers because anyone in the system can modify data in these files.
5. /mnt – stands for mount and stores media such as usb drivers and hard drives.
6. The “man hier” command is used to learn more about the FHS and its standard directories.
7. The “..” is used to represent the parent of the current directory. For example, “../projects”
8. The “whoami” command is used to learn what your username is. It returns the username of the current user.
9. “cd..” will take you up one level in the file structure.
10. Head -n 4 updates.txt. This modification will help us specify the number of lines. only done by adding
11. “Tail updates.txt” this is used to retrieve the last 10 minutes. You can use the command to read the most recent information in a log file.
12. The “less” command is used to treat the contact of a file or page one step at a time.

ABSOLUTE FILE PATHS VS RELATIVE FILE PATHS

Absolute file paths always start with the root dir and provide the full path to the file or directory. Whereas relative file paths is the path to a file relative to the current dir. Absolute file paths always point to the same location regardless of the current dir whereas relative paths may point to the different locations depending on the current dir.

Filtering meaning searching the system to find specific information that ca help you solve complex problems.

Advanced commands

1. “grep” searches a specified file and returns all lines in the file containing a specified string. This can be used when investigating an malware in files containing a specified string. For example, “grep OS updates.txt”

NB: remember that for grep to interpret a string of two or more words correctly I must enclose them using inverted comas or quotes.

1. Piping: sends the standard output of one command as the standard input to another command for further processing. Represented as ||. It involves redirection. It takes the output of one command and uses it as the input of another command for further action/ processing. For example: ls /home/analyst/projects | grep users

FILTERING: This simply mean selecting a file that matches a certain condition.

1. “find” this command searches for directories and files that meet specified criteria. You can use a wide range of criteria with the “find” command. You can search for files and directories that contain a specific string in the name, are a certain size or were last modified within a certain time frame. Eg find /home/analyst/projects (specify search criteria)

**Options** modify the behaviour of a command and commonly begins with a hyphen. For example -name (this is case sensitive) and -iname (not case sensitive)

**Find /home/analyst/projects -name “\*log\*”**

**In order to return all files where log is present regardless of the case, you would use the -iname, for example: find /home/analyst/projects**

**-iname “\*logs\*”**

The asterisk \* is used as a wildcard to represent zero or more unknown characters.

**-mtime option.**  This option is used to find files that were modified within sometime in the past. And the numbers indicate days not minutes or hours. For example you might have find /home/administrator/documents -mtime -6 this command is going to find the files in the documents folder that have been modified within the past 6 days. But if the number is +6 it is going to find the files that were modified over the past 6 days.

**NB:** the three most important commands used in filtering and sorting files in Linux are the grep, piping |and find commands. We use them to navigate and filter for information in the file system. 

When it comes to security the organisation of information is key. This is because you will always know where you kept something and can always reach it whenever you need it.

COMMANDS FOR DIRECTORIES

1. mkdir -creates a new dir
2. rmdir – removes a dir
3. touch – used to create a new file

There is an inbuilt command to warn you when a dir is not empty.

1. rm -is used to remove or delete a file.
2. mv – moves a file or dir to a new location
3. cp -copies a file or a dir to a new location.

Examples

rmdir oldreports

mkdir drafts

cd drafts = changes to the drafts dir

touch email\_patches.txt; touch OS\_patches.txt

moving and copying

cd /home/analyst/reports = move to the dir

ls= know the files in it

mv email\_policy.txt(first argument that tell us the file that is being moved) /home/analyst/drafts (second argument that tells us where to move the file)

cp vulnerabilities.txt /home/analyst/projects (copies the file into the projects dir and leaves it in its original location)

As a security analyst, file editors are used for writing or editing reports. A popular one is Nano and it can be accessed through the Nano command

NANO

Cd /home/analyst/drafts

Nano OS\_patches.txt

Ctrl+0 to save

Enter = save the file name

Ctrl+X to exit

You can use the mv command to rename a file. Use the new name as the second argument instead of using a location. Something like mv permissions.txt report.txt

Nano can also be used to create a new file by entering nano and the file name. It creates a new file and opens it. Vim and Emacs are also other popular text editors

N.B: The > and >> can also be used to send the output of one command to another command for processing. Using > overwrites the existing file whereas using >> adds content to the end of the existing file instead of overwriting it.

PERMISSIONS: the type of access granted for a file or directory. They are related to auth.

Authorisation is the process of granting access to a specific resource in a system. Allows you to limit access.

Data access should be on a NEED TO KNOW BASIS.

Types of permissions in linux.

1. READ: contents on the file can be read. On a dir it means you can read all files in that dir.
2. WRITE: you can create files in that dir.
3. EXECUTE PERMISSIONS: it allows users to exe the file. It allows users to enter the dir and access its files.

The user is the owner of a file if they are the ones who created it.

Group: a group is a collection of users

Other: this can be other users in the system. Anyone else can be put in this group.

File permissions in linux is represented with a 10 character string which are drwxrwxrwx

The first character “d” indicates the file type, in this case a dir. If it contains a hyphen it is a regular file type.

Second third and fourth indicate permissions for the user. In this example r means read, w means write, and x means the user has execute permissions. If one of them was missing there would be a hyphen.

The fifth sixth and seventh indicate permissions for the next owner type “group.” This means this group has read write and execute permissions. No hyphen.

The eight to 10th indicate permission for the next owner type “other”. In this case it means that they also have the same permissions.

A word writable file is a file where every owner type can write to and make changes to the file or directory. It can pose significant security concerns.

OPTIONS modify the behaviour of the command.it can be a single letter or a full word.

Ls -l displays permissions to files and directories.

Ls -a displays hidden files

Entering ls -la displays file permissions and hidden files.

CHANGING PERMISSIONS

REASONS TO CHANGE PERMISSIONS – changed department or not working on the same project.

Commands that help control access.

Chmod - changes permissions on files or directories.

There are two modes that focus on permissions. Both focus on symbolic.

Chmod g+w , o–r access.txt (symbolic mode)

U=user

G=-group

O-other

G means making some changes to the group permissions, O means making changes to other. In this example it means that we are adding the write permission to the group type owner while taking away the read permission from the other type owner.

ADDING AND DELETING USERS ON LINUX

Authentication is the process of a user proving they are who they say they are in the system. New users can be new to the org or new to a group.

It is important to delete a user when they leave the organisation. If they change groups they should also be deleted .

ROOT USER: this is the user with elevated privileges to modify the system. Individuals who need to perform specific tasks can be temporarily added as root users. They can create modify or delete any file or run any programme. Only root users can add new users.

NB: RUNNING COMMANDS IN LINUX USING ROOT USER PRIVILEGES IS BAD PRACTICE. WHY?

This could be problematic.

1. SECURITY: Malicious try to breach the root account. Therefore, IT SHOULD HAVE its LOGINS DISABLED.
2. IRREVERSIBLE MISTAKES: IT IS VERY EASY TO MAKE IRREVERSIBLE MISTAKES LIKE PERMANENTLY DELETING A DIR
3. ACCOUNTABILITY: IF A USER IS RUNNING AS ROOT, THERE IS NO WAY TO TRACK THEM.

Sudo: this is a command that grants temp elevated permissions to specific users. This provides more of a controlled approach compared to root. It comes from superuserdo.

Not everyone can become a super user. They have to be granted access through the configuration file called SUDOERS FILE.

MORE COMMANDS:

1. Useradd: adds users to the system. For example: sudo useradd salesrep7
2. Userdel: deletes a user from a system. For example sudo userdel salesrep7

SUDO privileges must be used carefully to ensure the safety of the system.

RESPONSIBLE USE OF SUDO

**Note**: Be aware of **sudo** if copying commands from an online source. It’s important you don’t use **sudo** accidentally.

There are options you can use along with sudo. For example if you want to set the user’s default group, you run the sudo command using the -g (lowercase)option. Sudo useradd -g architects James. This will automatically add the new user, James and assign their primary group to be that of architects.

But if you want to add the user to additional groups or supplemental or secondary groups, you use the -G option (upper case). Another example. When you type sudo adduser -G security James this will create a new user and add them to the existing group or groups. You can add a user to more than one groups.

1. Usermod: this command modifies existing user accounts. The -g and -G options can also be used with the usermod command if the user already exists. For example if you want to change the primary group of an existing user, you have to use the -g option. For example, sudo usermod -g human\_resources James| sudo usermod -g executive fgarcia would change fgarcia’s primary group to the executive.
2. If I want to add another group to the existing user, I will have to use the -a option together with the -G option. This is to make sure that the previous groups are not overwritten with the new request. The -a option preserves the old groups. an example of this would be sudo usermod -a -G marketing James

Using usermod with a -d option changes the users main directory.

Using usermod with the -l option changes the user’s login name

Using usermod with -L locks the account so the user cannot log in. for example sudo usermod -d /home/billing/James sudo usermod -l AWSFALCONX James

Userdel can be used with options such as -r. This is because if a user is deleted without the option, the files stored in the users home dir are not delete and can be recovered. However when the -r option is used just after userdel, it removes all the files in the user’s home dir and delete the user also. So it is good practice to have the files backed up in case we might be need them in the future.

Instead of deleting the user, we can disable/ deactivate their account with usermod -L. They user will no longer be able to log in but you will still have their permissions.

CHOWN (lowercase) this command is used to change the ownership of a file or dir. You can use it to change user or group ownership. To change the ownership of a file named access.txt to ruth, you will have to run sudo chown ruth access.txt. this will change the ownership of the file to ruth.



But if you want to change the group ownership to a group you must use the colon (:) before the name of the group. For example

MOST OF THE OPTIONIS YOU CAN USE WITH COMMANDS

A screenshot of a computer screen

Description automatically generated



This response was received because when you create a new user in Linux, a group is automatically created with the user. So, when you delete the user you have to delete the group to clean up any such empty groups that may remain behind.

The command sudo userdel groupresearcher9 will delete the group that was created when the user was added.

groupdel and not userdel is used to delete the group that was created when a user was added to the system.

When it comes to changing ownership, the user comes before the file

When it comes to modifying the group of a user, the groups come before the user.

When it comes to changing the directory of a user or a file, the user will come before the dir or the file.

MAN PAGES WITHIN THE SHELL

The man command displays information on what other commands are and how they work. It comes from the word manual.

whatis is a command that displays a description of a command on a single line. For example, whatis tail

apropos. For we want to change a password, but I don’t know how to do it. With the apropos command, this will display a list of commands with the word. But using the -a option and an additional string will return the exact command with the string in it.

INTRODUCTION TO SQL

Databases: an organised collection of information or data.

Spreadsheets designed for a single user or a small team to store data.

Databases can be accessed by multiple people. It can contain information about login attempts, software and updates or machines and their owners.

HOW DBS ARE ORGANISED

1. Relational database: it contains tables that are related to each other. Tables contains rows or records. They often have multiple tables. We can connect two tables if they have a common column.

The columns that relate two tables to each other are called keys. We have a primary key which is the column where every row has a unique entry. It must not have a duplicate value or any null or empty values. For example employee id.

Foreign key is a column in a table that is a primary key in another table. They can have empty values and duplicates. They allow us to connect two tables together.

A table can only have one primary key but can have multiple foreign keys.

QUERY DATABASES

SQL – STRUCTURED QUERY LANGUAGE

This is a programming language used to create, interact with and reqest information from a db.

Query is a request for data from a DB or a combination of dbs.

Log is a record of events that occur with an orgs systems.

SQL can search through millions of datapoints to extract relevant rows of data using one query using one command. You can use sql filtering to gather data. For example, you can use sql to determine which machines have not received the latest patch. You can also use it to determine the best time to update a machine based on when it is rarely used.

Security analysts commonly use SQL to find relevant information to support cybersecurity related decisions.

SQL FILTERING VS LINUS FILTERING

One way to access sql is through the linux command line.

**Differences between Linux and SQL filtering**

**Purpose**

Linux filters data in the context of files and directories on a computer system. It’s used for tasks like searching for specific files, manipulating file permissions, or managing processes.

SQL is used to filter data within a database management system. It’s used for querying and manipulating data stored in tables and retrieving specific information based on defined criteria.

**Syntax**

Linux uses various commands and command-line options specific to each filtering tool. Syntax varies depending on the tool and purpose. Some examples of Linux commands are find, sed, cut, e grep

SQL uses the Structured Query Language (SQL), a standardized language with specific keywords and clauses for filtering data across different SQL databases. Some examples of SQL keywords and clauses are WHERE, SELECT, JOIN

**Structure**

SQL offers a lot more structure than Linux, which is more free-form and not as tidy.

For example, if you wanted to access a log of employee log-in attempts, SQL would have each record separated into columns. Linux would print the data as a line of text without this organization. As a result, selecting a specific column to analyze would be easier and more efficient in SQL.

In terms of structure, SQL provides results that are more easily readable and that can be adjusted more quickly than when using Linux.

**Joining tables**

Some security-related decisions require information from different tables. SQL allows the analyst to join multiple tables together when returning data. Linux doesn’t have that same functionality; it doesn’t allow data to be connected to other information on your computer. This is more restrictive for an analyst going through security logs.

SQL is also used to find data to support security related decisions and analysis.

Example of sql queries

1. We want to determine which computer has been assigned to an employee.
2. We will write a query that returns only the columns we need from the table.
3. The two keywords we need are SELECT: indicates which columns to return and FROM: which indicates which table to query. Using them is common to everyday language. For example asking a friend to select some fruits from a basket.
4. We begin by typing the SQL statement
5. mysql > SELECT employee\_id, device\_id,
   1. -> FROM employees;

SYNTAX: the rules that dermine what is correctly structured in computing language.

Sql is not case sensitive.

A semi colon; is placed after the syntax

If we want to print out all the columns from the table we will run

SELECT\*

FROM employees;

**ORDER BY**

Database tables are often very complicated, and this is where other SQL keywords come in handy. ORDER BY is an important keyword for organizing the data you extract from a table.

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.

NB: using only order by will produce the query results in ascending order.

Sorting in descending order

You can also use the ORDER BY with the DESC keyword to sort in descending order. The DESC keyword is short for "descending" and tells SQL to sort numbers from largest to smallest, or alphabetically from Z to A. This can be done by following ORDER BY with the DESC keyword. For example,

SQL FILTERS

Filtering is selecting data that match a certain condition. This of filtering of only choosing the data we want for example we want to select an apple from a fruit cart. For example we can say choose only apples that are fresh.

OPERATOR: this is a symbol or keyword that represents an operation.

For example, if we want to find only those from USA, we will write something like country=”USA”

We will add an extra line that uses a **WHERE** clause. In SQL **WHERE** indicates a condition for a filter. An example syntax would be

mysql> SELECT \*

-> FROM log\_in\_attempts

-> WHERE country = ‘USA’ ; This command will return all the log in attempts coming from the united states.

What if we want to search for a pattern? For example, if we have a column for office, what if we want to search for a certain pattern? We will use use a WILDCARD % to search for unspecified characters.

For example

The ‘EAST%’ will return all records that start with EAST

LIKE is used with WHERE to search for a pattern in a column.

JAMES, YOU CANNOT USE THE = OPERATOR WITH THE % OPERATOR TO SEARCH FOR PATTERNS. YOU MUST USE THE LIKE OPERATOR TOGETHER WITH **WHERE** IN THE SYNTAX.

SELECT \*

FROM log\_in\_attempts

WHERE country LIKE ‘US%’ ;

MORE SQL QUERIES

DATA TYPES IN DATABASES

1. STRING: this is a data consisting of an ordered sequence of characters. They can be numbers, letters or symbols. Analyst90 for example.
2. NUMERIC: these are data consisting of numbers. Such as account of login attempts. Mathematical operations can be used on numeric data.
3. DATE AND TIME DATA: this is data representing a date and or time.

COMMON OPERATORS FOR WORKING WITH NUMERICAL DATA TYPES

1. = equal to
2. > greater than
3. < less than
4. <> not greater or less then
5. >= greater than or equal to
6. <= less than or equal to

mysql> SELECT \*

-> FROM log\_in\_attempts

WHERE time > ‘18:00:00’;

Between operator: this is an operator that filters for number or dates within a range. For example when looking for all patches installed within a range

SELECT \*

-> FROM machines

-> WHERE OS\_patch\_date BETWEEN ‘2021-03-01’ AND ‘2021-19-01’ ;

!= is often used as an alternative to not equal to.

INCLUSIVE VS EXCLUSIVE OPERATORS. An exclusive operator is one that does not include the value of the comparison. An inclusive operator includes the value of the comparison.

The BETWEEN operator is inclusive.

USING MULTIPLE OPERATORS.

For example when we want to find out which machines are using a particular email client and operating system, we have to use the AND operator.

AND as an operator specifies that both conditions must be met simultaneously. This is more like telling someone to select a fruit from a basket that is large and fresh. This limits the person to only selecting a fruit that is not large and rotten or small and fresh. It just has to be the specification they have been told.

We need to run a query to return the machines that run on OS1 and email client 1.

First try

mysql > SELECT \*

-> FROM machines

WHERE operating\_system = ‘OS 1’ AND email\_client = ‘Email Client 1’;

OR – this specifies that either condition can be met.

SELECT \*

FROM machines

WHERE operating-system = ‘OS 1’ OR operating\_system = ‘OS 3’;

this command will return answers to any of the queries above. Just satisfying one of the commands is fine. If it gets both, no problem.

USING NOT

This operator NEGATES a condition.

SELECT \*

FROM machines

-> WHERE NOT operating\_system = ‘OS 3’;

JOINING TABLES WHEN QUERYING A DATABASE

If we are trying to query two columns, dql needs to know which column we are referrung ti. We resolve this by writing the name of the table followed by the name of the column. For example employees.employee\_id is the ID eolumn for the employee column and machines.employee\_id is the ID column for the machines table.

If we want to get a deeper understanding of something, we might need to join different tables stored in our database.

We have to identify the shared column that we will use to connect the two tables. To do this, we use a primary key in one table to connect to another table where it’s a foreign table.

employee\_id is a primary key in the employees table because it has a unique value for every row in the employees table, and no empty values.

INNER JOIN: this returns rows matching on a specified column that exists in more than one table.

The results of the join is the two rows that have 1188 and 1189 and all columns from both tables.

In SQL, NULL represents a missing value due to any reason. This might mean machines that are not assigned to any employee.

OUTER JOINS

TYPES:

1. LEFT JOIN: This returns all of the records of the first table but only returns rows of the second table that match on a specified column.
2. RIGHT JOIN: this returns all of the records on the second table but only row on the first table that match on a specified column.
3. FULL OUTER JOIN: this query returns all records from both tables.

MariaDB [organization]> SELECT \* FROM machines LEFT JOIN employees ON machines.employee\_id = employees.employee\_id;

AGGREGATE FUNCTIONS

These are functions that perform a calculation over multiple data points and return the result of the calculation. The actual data is not returned. There are various aggregate functions that perform different calculations.

1. COUNT: returns a single number that represents the number or rows returned from you query.
2. AVG returns a single number that represents the average of the numerical data in a column.
3. SUM returns a single number that represents the sum of the numerical data in a column.

To use an aggregate function, I have to place the key word after the SELECT keyword, and then in parenthesis, indicate the column I want to perform the calculation on. For example, instead of SELECT \* or any other column name, I would type in SELECT COUNT (login\_times) FROM log\_in\_attempts…

Paralinguistics: tone of voice, speed of voice, pitch of voice…

Proxemics: distance between people when they are communicating…

What, why and how of asset security.

Risk is anything that can impact the confidentiality, integrity or availability of an asset..

The process of security risk planning is the first step toward protecting these cornerstones.

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

Asset: an item having value to a company, building equipment, people and data are all assets a company would want to protect.

With so many types of assets to think of, security plans need to prioritize resources. After all, no matter how large a security team is, it would be impossible to monitor every single asset at all hours of the day.

Security teams can prioritize their efforts based on threats.

Threats: In security, a threat is any circumstance or event that can negatively impact assets.

Vulnerabilities: In security, a vulnerability is a weakness that can be exploited by a threat. For example, a weak lock can be exploited by a burglar. They are flaws within an asset. Assets can have many diff types of vulnerabilities.

One way to interpret risk is to consider the potential effects that negative events can have on a business. Another way to present this idea is with this calculation:

Likelihood x Impact = Risk

n general, we calculate risk in this field to help:

Prevent costly and disruptive events

Identify improvements that can be made to systems and processes.

Determine which risks can be tolerated.

Prioritize the critical assets that require attention..

Threats are of two types.

1. Intentional threat: this might be a malicious hacker who gains access to sensitive information by targeting a misconfigured application.
2. Unintentional threat: this might be an employee who holds the door open for an unknown person and grants them access to restricted area. Either one can cause an event that must be responded to.

Categories of vulnerability

These are weaknesses that can be exploited by threats. But they are also grouped into two categories.

1. Technical vulnerability: this can be a misconfigured software that might give an unauthorised person access to important data.
2. Human vulnerability can be a forgetful employee who loses their access card in a parking lot.

Security starts with asset classification.

Asset management is the process of tracking assets and the risks that affect them.

Asset inventory is a catalog of assets that need to be protected. Asset inventory is like a shepherd protecting sheep. He must always have to know the number of sheep he has. It will be easier to allocate resources. You might also be able to know when one of them go missing.

ASSET CLASSIFICATION: this is the practice of labelling assets based on the sensitivity and importance to an organisation. Scheme- public, internal only, confidential and restricted. Public is shared with anyone, internal only is only for those who are working in the company. Confidential is for thos working on a specific project only. Restricted is only shared on a need-to-know basis. For example this may be payment information.

Asset classification requires knowing the following,

What you have; where it is; who owns it; and how important it is.

ASSETS IN A DIGITAL WORLD

Security teams classify assets based on value. But what exactly is valuable?

Data: this is information translated processed or stored by a computer. Protecting data is dependent on where that data is and what it’s doing.

States of data

1. In use: this is the data being accessed by one or more users. For example when you are using your email.
2. Data in transit: this is data travelling from one point to another.
3. Data at rest: data not currently being accessed. In this state, it is stored on a local device.

Information security is the practice of keeping data in all states away from unauthorised users. Information security is a serious problem. It can harm the organisation. We are currently adapting our understanding of data at rest.

RISK AND ASSET SECURITY

Placing a focus on people leads to the most effective security plans. Consider diverse backgrounds to ensure no one is left behind. Most sec plans break risks down into categories and factors.

Types of risk categories

1. Damage
2. Disclosure
3. Loss of information

Elements of a security plan: policies, standards and procedures.

Policies are a set of rules that reduce risk and protects information. They give everyone guidance on what’s being protected and why. It identifies the objectives, scope and limitations of security plans.

Standards: references that inform how to set policies. For example when a company states that a password must be 8 characters long.

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

THE NIST CYBERSECURITY FRAMEWORK

**Compliance** is the process of adhering to internal standards and external regulations. It helps companies maintain customer trust.

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

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

THE THREE MAIN COMPONENTS

1. CORE: a simplified version of the functions or duties of a security plan. It has 5 major broad functions. The CSF core is a set of desired cybersecurity outcomes that help organizations customize their security plan
   1. Identify
   2. Protect
   3. Detect
   4. Respond
   5. recover
2. TIERS: this provides security teams with a way to measure performance across each of the 5 functions of the core. They aren’t a yes or no proposition. It is just a way of showing companies what is or isn’t working with their security plan.
   1. Level 1 or passive Indicates reaching a minimum standard.
   2. Level 4 indicates a function is performed at exemplary standards.
3. PROFILES: they provide useful insight into the current state of a security plan. It is like photos capturing a moment in time. Comparing photos of a different subject at different times can provide useful insights.

CISA recommendations

1. Create a current profile of the security operations and outline the specific needs of your business.
2. Perform a risk assessment to identify which of your current operations are meeting business and regulatory standards.
3. Analyze and prioritize existing gaps in security operations that place the businesses assets at risk.
4. Implement a plan of action to achieve your organization’s goals and objectives.

Pro tip: Always consider current risk, threat, and vulnerability trends when using the NIST CSF.

A **risk register** is a central record of potential risks to an organization's assets, information systems, and data. Security teams commonly use risk registers when conducting a risk assessment.

Likelihood of occurrence

Impact in terms of severity

Calculate a score for the severity

Compare scores across all risks…



SECURITY CONTROLS

These are safeguards designed to reduce specific security risks.

Types of security controls

1. Technical: includes the many tech used to protect assets, for example, encryption and authentication.
2. Operational: maintaining the day to day environment: incident response.
3. Managerial: policies , standards and procedures.

INFORMATION PRIVACY

This is the protection of unauthorised access and distribution of data. Information privacy is about the right to choose. People can decide to how information about them is shared.

PRINCIPLE OF LEAST PRIVILEGE

This is the concept of granting only the minimal access and authorisation required to complete a task or function. This is related to the zero-trust architecture. Security controls should be designed with the principle of least privilege in mind. When they are they rely on differentiating between data owners and data custodian.

DATA OWNER: this is the person who decided who can access, edit, use or destroy their information. The idea is straightforward. The intellectual property can have multiple owners.

DATA CUSTODIAN: this is anyone or anything that is responsible for the safe handling, transport and storage of information. Organisations and systems are also custodians of people’s information. Data is an asset hence, information privacy requires proper classification and handling.

**Separation of duties—**a security concept that divides tasks and responsibilities among different users to prevent giving a single user complete control over critical business functions

Pro tip: Passwords play an important role when implementing the principle of least privilege. Even if user accounts are assigned appropriately, an insecure password can compromise your systems.

Privilege creep: when a user accumulates more access privileges than what they need over time. This might happen when an employee receives a promotion or switches teams and their job duties change.

There are 3 main approaches to auding user accounts

1. Usage audits: here the analyst checks to see the resources the user is accessing and what they are doing with it. It can help teams know if the users are acting in accordance with an organisation's security policies and procedures,
2. Privilege audits: this checks to see if a user has accumulated more access privileges than they need to perform a particular job function.
3. Account change audits: account director service skeep records and logs associated with each user. Changes to an account are usually saved aand can be used to audit the directory for suspicious activity like multiple attempts to change an account password. These services can be configured to alert system admis of suspicious activity.

THE DATA LIFECYCLE

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:

1. A diagram of data lifecycle

   Description automatically generatedCollect
2. Store
3. Use
4. Archive
5. Destroy

DATA GOVERNANCE

This is the processes that define how an organisation manages information. Governance often includes policies that specify how to keep data private, accurate, available and secure throughout its lifecycle.

Effective data governance is a collaborative activity that relies on people. Data governance policies commonly categorise individuals into specific role.

**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.

**Data governance policy:**  this is a specific policy that outlines how information will be managed across an organisation. The document clearly defines procedures that shou dbe followed to participate in keeping data safe. They also place limits oh who or what can access data.

**N/B**: As a security professional, protecting a person's data privacy decisions must always be respected.

**Information privacy vs information security**

Information privacy is the protection of unauthorised access and distribution of data.

Information security is the practice of keeping data in all states away from unauthorised users.

The key difference between information privacy and information security is that in privacy people are provided with control over their personal information and how it is shared. But in security the choices people have made about protecting their data are upheld and their information is kept safe from potential threats.

For example, if a company wants to collect customer data, they should first inform them how their data will be used allowing them the opportunity to decide if they want their data to be shared or not. Once they have collected consent, they will then implement specific security controls in order to protect the private data from unauthorised access, use or disclosure.

Note: Privacy and security are both essential for maintaining customer trust and brand reputation.

Note: the more data is collected, stored and used, the more vulnerable it is to breaches and threats.

3 security regulations I must know as a security analyst.

1. GDPR: general data protection regulation
2. PCI DSS: Payment card industry data security standard
3. HIPAA: health insurance portability and accountability act

Security audit vs security assessment

**Security audit** is the process of checking an organisation's security controls, policies and procedures against a set of expectations.

**Security assessment** is checking to determine how resilient current security implementations are against threats.

Note: Compliance with legal regulations, such as GDPR, can be determined during audits. That explains why it is important to have such audits.

A diagram of a security system

Description automatically generated with medium confidence

FUNDAMENTALS OF CRYPTOGRAPHY

PII: is any information that can be used to inform an individual’s identity. Maintaining the privacy is difficult. One of the main controls used is **cryptography — this is the process of transforming information into a form that unintended readers can’t understand.**

2 STEP PROCESS

1. Encryption: it scrambles plaintext to cyphertext.
2. Decryption: returning the cypher text into plain text.

**Ceasar’s cypher**

Algorithm is a set of rules that solves a problem.

**Cypher** is an algorithm that encrypts information.

**Cryptographic key** is a mechanism that decrypts cypher text. A cypher and key is mainly used together.

**Brute force attack: this is a trial-and-error process of discovering private information.**

**Keys are not stored in public places and ensured they are shared separately from the information they decrypt.**

Public key infrastructure

PKI is an encryption framework that secures the exchange of information online. It is a broad system that makes accessing systems seure.

PKI process

1. A diagram of a computer virus

   Description automatically generatedExchange of encrypted information. It can be asymmetric encryption or symmetric encryption. Asymmetric encryption involves the use of public and private key pair for encryption and decryption. The public key can only be used to encrypt whereas the private key is used for decryption. The disadvantage is that it slows down the encryption and decryption process.

In symmetric encryption, a single key is used for encryption and decryption. It is like a box which requires only one key. It makes communication faster but maybe less secure. It all depends on the use case, ie, if speed or security is the priority. For example, with mobile applications use asymmetric to establish communication. But when speed is the priority, symmetric takes over.

Common vulnerability: establishing trust between sender and receiver. Both rely on sharing keys that can be misused, lost or stolen.

1. Establish trust using a system of digital certificates between computers and networks.

Digital certificate: this is a file that verifies the identity of a public key holder.

Obscurity is not security.

Pro tip: A cryptographic system should not be considered secure if it requires secrecy around how it works. For example, you can access all the details about how AES works online and yet it is still unbreakable.

FIPS 140-3 (federal information processing standards) along with GDPR outline how data should be collected used and handled.

HASH FUNCTION

This is an algorithm that produces a code that can’t be decrypted. They produce a hash value or digest.

In security hashes are usually used to determine the integrity of files and applications.

A diagram of a block diagram

Description automatically generated

Data integrity relates to the accuracy and integrity of information. This is known as non-repudiation.

NON-REPUDIATION: the concept that the authenticity of information can’t be denied.

One way analysts use hashing functions is to find the has value of files or applications and comparing them against known malicious files.

**Hash Collision**, an instance when different inputs produce the same hash value. Because hashes are used for authentication, a hash collision is similar to copying someone’s identity. Attackers can carry out collision attacks to fraudulently impersonate authentic data.

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

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

A green and orange container with white text

Description automatically generated

Sha256sum is the linux command used to generate hash values for files. Prolyl for the SHA algorithm

**Access controls**

These are security controls that manage access, authorisation and accountability of information.

AAA FRAMEWORK

1. Authentication: these are systems that ask anything that attempts to access information “who are you?”

Factors of authentication

* 1. Knowledge: something the user knows
  2. Ownership: something the user possesses
  3. Characteristic: something the user is.

1. Authorisation
2. Accounting

SINGLE SIGN ON

This is a technology that combines several different technologies into one. Instead of requiring a user to authenticate many times, they do it just once. But vulnerable when used alone.

MFA combines two or more independent credentials.

HOW SSO WORKS

SSO works by automating how trust is established between a user and a service provider. Rather than placing the responsibility on an employee or customer, SSO solutions use trusted third-parties to prove that a user is who they claim to be.

A diagram of a cloud network

Description automatically generated

**AUTHORISATION**

Authorisation is linked to the idea that access to information lasts as long as it is need, it is related to the least privilege principle. It is also related to the separation of duties principle which states that users should not be given levels of authorisation that would allow them to misuse a system.

**Securing data over network**

**http**: hypertext transfer protocol. It uses the basic auth tech which is used to establish a user’s request to access a server.it sends an identifier every time a user communicates with a webpage. https does not expose data when it’s travelling over a network.

**OAuth**: this is an open standard authorisation protocol that shares designated access between applications. For example, another website can use my google profile. It uses api tokens which is a small block of encrypted code that contains information about the user.

WHY WE AUDIT USER ACTIVITY - ACCOUNTING

This is the practice of monitoring the access logs of a system. Sec analyst use it a lot. It helps identify trends. We use it to unconver hackers who have gained access into a system.

It is often the first thing to do when you are investigating an event.

SESSION: this is a sequence of network HTTP basic auth requests and responses associated with he same user. When a user communicates with a webpage or a db two things happen. The first is the creation of a sessionID.

SESSION ID: this is a unique token that identifies a user and their device while accessing the system.

The second thing that happens is that the system and the user’s computer exchange session cookies.

SESSION COOKIE: this is a token that websites use to validate a session and determine how long that session should last.

SESSION HIJACKING: an event when attackers obtain a legitimate user’s session ID.

**USER PROVISIONING**

This is the process of creating and maintaining a user’s digital identity. For example, a college might create a new user account when a new instructor is hired. The new account will be configured to provide access to instructor only resources while they are still teaching.

Another role analysts have is to deprovision users. This means removing a user’s access rights when they should no longer have them.

GRANTING AUTHORISATION

1. Mandatory access control. This is based on a strict need to know basis. Access to information must be granted manually by a central authority or system admin. It is non-discretionary control because access isn’t given at the discretion of the data owner. A diagram of a computer system

   Description automatically generated
2. Discretionary access control: this happens when the data owner decides appropriate levels of access. An example is with google drive when an owner of a file shares a google drive folder with editor, viewer, or commentator access with someone else.

A diagram of a group of people

Description automatically generated

1. Role based access control. Role based access or authorisation is determined by a user’s role within an organisation. For example, a user in the marketing department may have access to user analytics but not network administration.

A diagram of a role-based access control

Description automatically generated

VULNERABILITY MANAGEMENT

A vulnerability is a weakness that can be exploited by a threat.

Exploit: this is a way of taking advantage of a vulnerability.

Vulnerability management is the process of finding and patching vulnerabilities. It helps keep assets safe. It has a 4 stage process

1. Identify vulnerabilities
2. Consider potential exploits.
3. Prepare defences against threats,
4. Evaluate those defences.

Zero day

This is an exploit that was previously unknown. It means that the exploit is happening in real time with no day to fix it. It has not been planned for yet. This are things that don’t generally come to mind.

Défense in depth strategy

This is a security model that takes a layered approach to vulnerability management that reduces risk. It is commonly referred to as the castle approach. It has a 5 layer approach.

1. The perimeter layer: this is like a username and password. it is a user authentication layer that filters external access. The function is to only allow trusted partners to reach the next layer of defence.
2. Network layer: this is made up of firewalls. It is closely aligned with authorisation.
3. End point layer: endpoints are devices that have access to a network or linked to a network. Laptops, etc. antivruses are found here.
4. Application layer: this refers to all the interfaces the ae used to interact with technology. Here security measures they are programmed with the technology. One example is the MFA.
5. Data layer: here is where personally identifiable information resides. One important security control here is assets classification.

Common vulnerabilities and exposures.

Exposure are mistakes that can be exploited by a threat. It is more like misplacing an important document.

The CVE (common vulnerabilities list) list is an openly accessible dictionary of known vulnerabilities and exposures. The main goal of the CVE list is to offer a standard way of identifying and categorising known vulnerabilities and exposures.

CAN (CVE Numbering Authority): this is an organisation that volunteers to analyse and distribute information on eligible CVEs.

A vulnerability must meet 4 criteria

1. It must be independent of other issues: this means that it must be fixed on its own and not as a result of fixing something else.
2. It must be recognised as a potential security risk.
3. It must be submitted with supporting evidence
4. The report of a vulnerability must affect only one code base.

Other orgs also review this list.

The NIST National Vulnerabilities Database

They use the common vulnerability scoring system. This scores the severity of a vulnerability. They use it to calculate the impact and how quickly it should be patched.

CVSS of 4 or below is low risk

Anything above 9 is critical and must be patched right away.

In this reading, you’ll learn about open-source intelligence, commonly known as **OSINT**. OSINT is the collection and analysis of information from publicly available sources to generate usable intelligence. It's commonly used to support cybersecurity activities, like identifying potential threats and vulnerabilities.

In other words, intelligence is derived from information through the process of analysis, interpretation, and integration. Gathering information and intelligence are both important aspects of cybersecurity.

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

To provide insights into cyber attacks

To detect potential data exposures

To evaluate existing defences

To identify unknown vulnerabilities

ATTACK SURFACE

This is all the potential vulnerabilities that a threat actor could exploit.

This could mean that the organisation understand the digital and physical attack surface. The physical is made up of people and their devices. This can be attacked from both inside and outside the organisation. For example, when someone leaves the sensitive information on a laptop left on a public coffee shop. Someone in another company might see the sensitive information and capture it.

The physical attack surface should be filled with obstacles that prevent attacks from happening. This process is called security hardening.

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

**HARDENING** means minimising the attack surface by reducing the points of entry of an attack. The smaller the attack surface the easier it is it to protect.

**THE DIGITAL ATTACK SURFACE** is everything behind an organisation’s firewall. It includes anything that connects to an organisation online. A person sitting at a computer

Description automatically generated

Approaching cybersecurity with an attacker mindset.

**Vulnerability assessments** are the internal review process of an organisation’s security systems.

Applying an attacker mindset is about causing problems in a controlled environment and evaluating the outcome to gain insights.

Simulating threats

**Proactive simulations** assume the role of an attacker by exploiting vulnerabilities and breaking through defences. This is sometimes called a red team exercise.

**Reactive simulation** assumes the role of a defender responding to an attack. This is sometimes called a blue team exercise.

**Vulnerability scanner** is software that automatically compares existing common vulnerabilities and exposures against the technologies on the network.

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

Types of threat actors

Attack surfaces are all the potential vulnerabilities that a threat actor could exploit.

Theya re normally divided into five categories based on their motivations

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

Hacker

This is an person who uses computers to gain unauthorised access to computer systems networks or data.

There are three types - unauthorised hackers, authorised or ethical hackers and semi authorised hackers.

Advanced persistent threats

An advanced persistent threat (APT) refers to instances when a threat actor maintains unauthorized access to a system for an extended period of time. The term is mostly associated with nation states and state-sponsored actors. Typically, an APT is concerned with surveilling a target to gather information. They then use the intel to manipulate government, defense, financial, and telecom services.

APTs will often target private organizations first as a step towards gaining access to larger entities.

**Pathways through defenses**

**Attack vectors**: these are the pathways attackers use to penetrate security defenses. For example usb drives.

**Practicing an attacker mindset**

1. Identify a target… this can be a specific information, a system, person or group or an organisation itself.
2. Determine how the target can be accessed. What information is available.
3. Evaluate attack vectors that can be exploited.
4. Find the tools and methods of attack. What would the attackers use to carry this out?

Defending attack vectors

1. Educating users about security vulnerabilities
2. Applying the principle of least privilege: limit access rights to what is needed to perform a role.
3. Using the right security controls and tools.
4. Building a diverse security team: the unique perspectives matter a lot.

**Fortifying against Brute Force Cyber-attacks.**

This is a kind of attack where an attacker uses a trial-and-error process of discovering private information like user passwords.

There are varieties of tactics to find their way into a system.

1. Simple brute force attacks. Here the attacker is entering a combination of passwords they think might be the right one hoping the find the one that works.
2. Dictionary attacks: they use a list of commonly used credentials to access a system. It is like matching a definition to a word in the dictionary.
3. Reverse brute force attacks are similar to dictionary attacks except they start with a single credential and try it in various systems until a match is found.
4. Credential stuffing is a tactic in which attackers use stolen login credentials from previous data breaches to access user accounts at another organisation. A special type of is called *pass the hash*. They reuse stolen unsalted hashed credentials to trick an authentication system from creating a new authenticated user session on the network.
5. Exhaustive Key Search.

Tools used in hacking

1. Aircrack-ng: this is used to hack into wifi networks. It is also used to sniff the data packets transmitted through a network.
2. Hashcat: this is a tool for cracking passwords using the power of the computer’s graphics processor unit computation power.
3. John the Ripper: is is also used for password cracking.
4. Ophcrack
5. THC Hydra

How to prevent Brute force attacks

1. Hashing and salting
2. Multi factor authentication.
3. CAPTCHA : completely automated public turing test used to tell computers and humans apart. It is known as a challenge-response authentication.
4. Password policies

**ACTIVITY –**

USB baiting is an attack in which a threat actor strategically leaves a malware USB for an employee to find and install to unknowingly infect a network. It relies on curious people to plug in an unfamiliar flash drive they find.

**The Criminal Art Of Persuasion**

SOCIAL ENGINEERING: this is a manipulation technique that explouts human error to gain private information, access or valuables.

They trick people to break normal security procedures on the attackers behalf. It can happen anywhere.

**Stages of social engineering**

1. Prepare: gathering information about the target.
2. Establishing trust also called pretexting. Tricking their target into a false sense of trust.
3. Persuasion tactics: manipulating targets to volunteer information.
4. Disconnect from the target: they break communication with the target to cover their tracks.

**Preventing social engineering attack**

1. Implementing managerial controls like policies, standards, and procedures. Theya re used for updating operating systems and applications that can be exploited.
2. Staying informed of trends.
3. Sharing what you know with others. They play on our natural curiosity to help others. Their hope is that targets won’t think too hard about what is going on.

**Types of social engineering**

**Baiting**: this is the type that relies on people compromising their own security like in USB baiting. Finding an infected usb drive and plugging it into your own system.

**Phishing**: tricking people into revealing sensitive information through digital communication like through emails. It is the most common type of social engineering.

**Quid pro quo**: tricking someone into believing that they will receive some benefit if they provided some information, shared some form of access or money.

**Tailgating**: this is when an unauthorised person follows an authorised person into a restricted area. Also called piggybacking.

**Watering hole**: this is an type of attack when an attacker compromise a website frequently visited by a specific group of suers often a religious, charity or volunteer website.

**Encouraging caution** by doing the following:

**Staying alert:** be wary of suspicious communication from unknown people. Be care when it come to replying and clicking on links found in emails. Check for spelling errors and double check the sender’s name and email address.

**Be cautious** about sharing information especially over social media.

**Control curiosity** especially when something seems too good to be true. This includes clicking on attachments or links in emails and advertisements.

**PHISHING**

This is the use of digital communications to trick people into revealing sensitive data or deploying malicious software. They don’t just affect people they also harm organisations. One person can give a threat actor credentials that can be harmful to the whole organisation.

**PHISHING KIT**

This is a collection of software tools needed to launch a phishing campaign. People without technical backgrounds can use these kits. I will need to know the tools inside a phishing kit.

1. Malicious attachments: files that are infected and can cause harm.
2. Fake data collection forms. They ask for sensitive information.
3. Fraudulent web links. They are built to steal login credentials.

They use **smishing** which is the use of text messages to obtain sensitive information or to impersonate a known source.

**Vishing**: this is the exploitation of electronic voice communication to obtain sensitive information or impersonate a known source. For example, calling and pretending to be a company representative.

**PHISIHIG SECURITY MEASURES**

1. Anti-phishing policies spread awareness.
2. Employee training resources
3. Email filters – using allow lists to specify IP addresses approved to send mail to the company.

Intrusion prevention systems to look for unusual patterns in email traffic.

Spear phishing: targeting a small group of people, for example accountants within an organisation.

Whaling: targeting the executives of an organisation, or high-ranking executives.

Angler phishing is a technique where attackers impersonate customer service representatives on social media.

MALWARE

This is malicious software designed to harm devices or networks. They can be spread in many ways for example through a usb drive or they can be spread through online means.

A screenshot of a computer

Description automatically generated

Types of malware

1. Virus: this is a code written to interfere with computer operations and cause damage to data and software. They can hide within trusted applications. When the programme is launched, it clones itself and spreads to other applications.
2. Worm: this is a type of malware that can duplicate and spread on its own. They do not require activation to spread.
3. Trojan: this is a malware that looks like a legitimate programme. They look like useful application. They often then use the trojan to install another malware called ransomware.
4. Ransomware: this is a type of malware attack where attackers encrypt an organisation’s data and demand payment to restore access. A unique feature is that they make themselves known to their targets.
5. Spyware: malware used to gather and sell information without consent. This one is typically used to steal information.

Cryptojacking

This is a form of malware that install software to illegally mine cryptocurrencies.

Crypto mining is a process of obtaining new coins. Attackers hence use a crypto mining software to gain unauthorised access into systems to mine crypto. Began in 2017. When it lays hold of one server, it installs the software and devices that communicate with the infected server become infected themselves. The malicious code then ruins in the background mining for coins unknown to anyone.

**Intrusion detection systems** is al application that monitors system activity and alerts on possible intrusions. When it detects malware mining for coins it alerts the security personnel. The drawback is that new forms of malware can remain undetected.

**Signs that a device is infected**

1. **Slow down**
2. **Increased cpu usage**
3. **Sudden system crashes**
4. **Fast draining batteries**
5. **High electricity costs.**

Other measures

1. Using browser extensions designed to block malware
2. Using ad blockers
3. Disabling JavaScript
4. Staying on top of latest trends.
5. Education others on malware attacks.

WEB BASED EXPLOITS

These are malicious or bahaviour that’s used to take advantage of coding flaws in a web application. They used this to obtain sensitive information because web applications interact with multiple users across multiple networks. They often use an injection attack.

Injection attack: this is malicious code inserted into a vulnerable application. The infected application appears to run normally.

Cross-site scripting (XSS) this is a type of injection attack that inserts code into vulnerable website or web application. It is used by exploiting html and javascript.

Types of cross site scripting attacks

1. Reflected: this is an istance when malicious script is sent to a server and activated during the server’s response.
2. Stored: here the malicious code is directly injected into the web server.
3. Document object model (DOM)based attack is when an malicious script exists in the webpage a browser loads. A computer screen with a red skull and white text

   Description automatically generated

In this case the browser will process the html and execute the javescript. This method is used to steal sensitive information.

EXPLOITABLE GAPS IN DATABASES

SQL INJECTION ATTACK: SQL is used by most web applications, for example shopping websites. This is an attack that executes unexpected queries on a database.

It occurs due to lack of sanitised input. It works on an area of website that accepts user’s input. It occurs when an attacker exploits input fields that aren’t programmed to filter out unwanted text. A diagram of a server

Description automatically generated

Types of SQL injection attacks.

1. In-band: this type uses the same communication channel to launch an attack and gather the results. For example a malicious code is run on the search bar of a web server and it returns sensitive data in the same search box.
2. Out-of-band: uses a different communication channel to launch the attack and gather the result. Like connecting the vulnerable server to a database they control allowing them to bypass all the security controls in place on the web server. But they are very uncommon except the target server has some features enabled.
3. Inferential: here they cannot see the direct results of the attack, they simply infer through the bahaviour of the system. For example, say an attacker knows certain gaps with particular dbs and craft a script that returns a certain error. With that error, they can infer the structure of the db and then craft a damaging query that will give them access to the system.

One way to prevent SQL injection attacks is to use code that would sanitise inputs.

1. Using prepared statements: this is a coding technique that executes SQL statements before passing them on to the database. This means that the code is validated before the query is run on the database. Having well-prepared code is a vital step.
2. Input sanitisation: programming that removes user input which could be interpreted as code.
3. Input validation: programming that ensures user input meets a system’s expectations.

**THREAT MODELLING – a proactive approach to security**

Anticipating attacks is a key to preparing for them. Threat modelling is the process of identifying assets, their vulnerabilities and how each is exposed to threats. This is a lengthy and detailed activity.

PASTA – the process of attack simulation and threat analysis.

Threat modelling steps

Diagram of a diagram of a threat modeling steps

Description automatically generated

1. Define the scope, by creating inventory of assets and classifying them.
2. Identify threats: the team identifies all threat actors. This could be an employee who exposes the system to harm intentionally. The team then puts together an attack tree - a diagram that maps threats to assets.
3. Characterise the environment - here an attacker mindset is applied to the business. They look how employees and customers interact with the environment.
4. Analyse threats: they work together to identify existing protection and identify any gaps. They then rank threats according to the risk score that they assign.
5. Mitigate risk: they create a plan for defending against threats.
6. Evaluate findings: here everything is documented, any fixed are applied and they make a record of any lessons they learned from the exercise. They might even document it in their play book. Just guessing.

Threat modelling should be performed before, during and after an application is developed. It must be incorporated into every stage of the software development lifecycle SDLC.

Frameworks have been developed to make the process of software analysis smoother.

Common frameworks

1. STRIDE
2. PASTA
3. TRIKE
4. VAST

**Glossary terms from module 4**

Terms and definitions from Course 5, Module 4

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

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

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

**Attack tree:** A diagram that maps threats to assets

**Baiting:** A social engineering tactic that tempts people into compromising their security

**Botnet:** A collection of computers infected by malware that are under the control of a single threat actor, known as the “bot-herder"

**Cross-site scripting (XSS):** An injection attack that inserts code into a vulnerable website or web application

**Cryptojacking:** A form of malware that installs software to illegally mine cryptocurrencies

**DOM-based XSS attack:** An instance when malicious script exists in the webpage a browser loads

**Dropper:** A type of malware that comes packed with malicious code which is delivered and installed onto a target system

**Fileless malware:** Malware that does not need to be installed by the user because it uses legitimate programs that are already installed to infect a computer

**Hacker:** Any person or group who uses computers to gain unauthorized access to data

**Identity and access management (IAM):** A collection of processes and technologies that helps organizations manage digital identities in their environment

**Injection attack:** Malicious code inserted into a vulnerable application

**Input validation:** Programming that validates inputs from users and other programs

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

**Loader:** A type of malware that downloads strains of malicious code from an external source and installs them onto a target system

**Malware:** Software designed to harm devices or networks

**Process of Attack Simulation and Threat Analysis (PASTA):** A popular threat modeling framework that’s used across many industries

**Phishing:** The use of digital communications to trick people into revealing sensitive data or deploying malicious software

**Phishing kit:** A collection of software tools needed to launch a phishing campaign

**Prepared statement:** A coding technique that executes SQL statements before passing them onto the database

**Potentially unwanted application (PUA):** A type of unwanted software that is bundled in with legitimate programs which might display ads, cause device slowdown, or install other software

**Quid pro quo:** A type of baiting used to trick someone into believing that they’ll be rewarded in return for sharing access, information, or money

**Ransomware:** Type of malicious attack where attackers encrypt an organization’s data and demand payment to restore access

**Reflected XSS attack:** An instance when malicious script is sent to a server and activated during the server’s response

**Rootkit:** Malware that provides remote, administrative access to a computer

**Scareware:** Malware that employs tactics to frighten users into infecting their device

**Smishing**: The use of text messages to trick users to obtain sensitive information or to impersonate a known source

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

**Spear phishing:** A malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source

**Spyware:** Malware that’s used to gather and sell information without consent

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

**SQL injection:** An attack that executes unexpected queries on a database

**Stored XSS attack:** An instance when malicious script is injected directly on the server

**Tailgating:** A social engineering tactic in which unauthorized people follow an authorized person into a restricted area

**Threat:** Any circumstance or event that can negatively impact assets

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

**Threat modeling:** The process of identifying assets, their vulnerabilities, and how each is exposed to threats

**Trojan horse:** Malware that looks like a legitimate file or program

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

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

**Whaling:** A category of spear phishing attempts that are aimed at high-ranking executives in an organization

**Web-based exploits:** Malicious code or behavior that’s used to take advantage of coding flaws in a web application.

**THE INCIDENT RESPONSE LIFECYCLE**

Incident lifecycle frameworks provide a structure to support incident response operations. The frameworks help organisations develop a standardised approach to their incident response process, so that incidents are managed in an effective and consistent way.

The NIST Incident Response Lifecycle is a cyclical process. This means that phases in the lifecycle can be revisited or repeated as incident investigations progress.

NIST INCIDENT RESPONSE LIFECYCLE

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, Recovery
4. Post – incident activity.

INCIDENT – this is an occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity or availability of information or an information system or constitutes a violation or imminent threat of violation of law, security policies, security procedures or acceptable use of policies.

All security incidents are events, but not all security events are incidents. An event is an observable occurrence on a network, system or device. For example, an employee can forget their password and request for a change in password. that event is logged but it is not an incident because it does not have any harmful undertones to it. However, if the same is done by an attacker, then it is both an incident and an event because it is a potentially dangerous to the organisation.

**5 Ws of an Incident**

1. Who triggered the incident?
2. What happened
3. When the incident took place
4. Where the incident took place
5. Why the incident occurred.

It is important to remember this and keep record of this. It comes in handy when writing an incident report. You can do this using an incident handling journal.

INCIDENT RESPONSE TEAMS

A successful response requires a team of both security and non-security professionals working together with defined roles.

CSIRT – computer security incident response teams

These are specialised group of security professionals that are trained in incident management and response. Their goal is to effectively manage incidents, provide services for response and recovery and prevent future incidents from occurring. They must work cross functionally. For example, they consult legal teams or public relations teams.

ROLES IN CSIRT

1. Security analyst: investigate alerts to determine if an incident has occurred and determine the criticality rating. If critical, they escalate it to the technical lead.
2. Technical lead: they provide technical leadership by guiding security incidents through their lifecycle.
3. Incident coordinator: tracks and manages the activity of the csirt. Their job is to ensure that incident response processes are followed and that teams are regularly updated on the incident status.

Security analyst

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

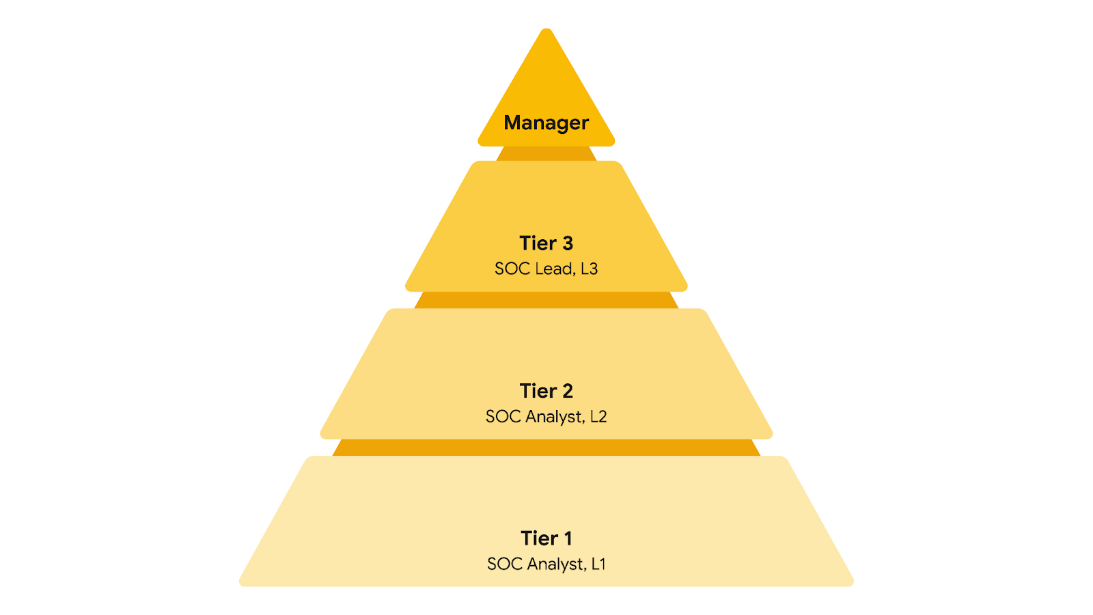
If a critical threat is identified, then analysts escalate it to the appropriate team lead, such as the technical lead.

**SECURITY OPERATIONS CENTER**

A security operations center (SOC) is an organizational unit dedicated to monitoring networks, systems, and devices for security threats or attacks. Structurally, a SOC (usually pronounced ed "sock") often exists as its own separate unit or within a CSIRT. You may be familiar with the term blue team, which refers to the security professionals who are responsible for defending against all security threats and attacks at an organization. A SOC is involved in various types of blue team activities, such as network monitoring, analysis, and response to incidents.

SOC organization

A SOC is composed of SOC analysts, SOC leads, and SOC managers. Each role has its own respective responsibilities. SOC analysts are grouped into three different tiers.



Tier 1 SOC analysts

These are responsible for monitoring, reviewing and prioritising alerts based on criticality or severity; creating and closing alerts using ticketing systems; and escalating alert tickets to tier 2 or tier 3.

Tier 2 SOC analysts

They are responsible for receiving escalated tickets from L1 and conducting deeper investigations; configuring and refining security tools; reporting to the SOC lead.

INCIDENT RESPONSE PLANS

An incident response plan is a document that outlines the steps to take in each step of incident response.

Response plans are not all the same. Organisations tailor them to meet their specific mission size, culture, industry and structure.

They share common elements like incident response procedures which are step by step instructions to respond to incidents. System information which are things like network diagrams, data flow diagrams, logging and asset inventory information. Other documents like contact lists, forms and templates.

Incident response plans must be reviewed regularly and tested through tabletops and simulations.

Security response teams must be prepared to respond quickly efficiently and effectively. This is because organisations have a certain time frame to report incidents.

Elements of a security plan

1. Policies
2. Standards
3. Procedures

INCIDENT RESPONSE TOOLS

Types of tools

1. Detection and management tools: monitor system activity to identify events that need investigation.
2. Documentation tools: to compile evidence.
3. Investigative tools: analysing the events like packet sniffers.

THE VALUE OF DOCUMENTATION

Documentation is any form of recorded content used for a specific purpose. It is meant to provide instruction and guidance on a specific topic.

**Types of documentation**

1. Playbooks
2. Incidents handler journal
3. Policies
4. Plans
5. Final reports

It differs from company to company. They may add some things or remove some things. Using documentation is like using a user’s manual when learning about a new product.

Playbook: this is a manual that provides details about any operational action.

It is important that the documentation I produce is clear, accurate and consistent so that my team and I can respond swiftly and decisively.

Google docs, one note, ever note, note pad++;

Ticketing systems like jira can be used for documentation.

Google sheets, cameras, recorders, etc can be used for documentation.

INTRUSION DETECTION AND PREVENTION SYSTEMS.

This is an application that monitors system and network activity and produces alerts on possible intrusions. This is like a home intrusion sensor. It collects information and sends out alert to personnel.

Intrusion prevention systems have all the same capabilities of an IDS, they in addition take action to stop and intrusion.; some popular tools are:

Snort, zeek, kismet, segan, suricata

Detection categories

1. A true positive is an alert that correctly detects the presence of an attack.
2. A true negative is a state where there is no detection of malicious activity. This is when no malicious activity exists and no alert is triggered.
3. A false positive is an alert that incorrectly detects the presence of a threat. This is when an IDS identifies an activity as malicious bit it isn’t. false positives are an inconvenience for security teams because they spend time and resources investigating an illegitimate alert.
4. A false negative is a state where the presence of a threat is not detected. This is when malicious activity happens, but an Ids fails to detect it. False negatives are dangerous because security teams are left unaware of legitimate attacks that they can be vulnerable to.

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

The tools monitor record and analyse endpoint system activity to identify alert and respond to suspicious activity. Unlike IDS or IPS, the tools collect endpoint activity data and perform behavioural analysis to identify threat patterns happening on an endpoint.

This uses machine learning and ai to analyse system behaviour to identify malicious or unusual activity. They also use automation to stop attacks without the manual intervention of security professionals. An example of an EDR running is to block a process from running if it notices that a user’s workstation is not normally used.

EDR tools include:

OpenEDR, Bitdefender, Endpoint Detection and Response and FortiEDR.

ALERT AND EVENT MANAGEMENT SIEM AND SOAR TOOLS

SIEM is an application that collects and analyses log data to monitor critical activities in an organisation. It provides a high level overview of what happens in a network.

This is similar to a dashboard. It provides information related to the car’s components. it notifies about the status of the car’s components.

In the same SIEM tools look at data flows between all systems and networks and anslyses them to provide a real time picture of any potential threat to the network. It does this by ingesting massive amounts of data and categorising this data so it is easily accessible through a centralised platform.

**SIEM PROCESS**

1. Collect and aggregate data: it can come from multiple sources like IDS, IPS, firewalls, databases, applications and more. Aggregation means all the data is centralised in one place. It can collect a huge volume of data.
2. Normalise data: it cleans up the data by removing non-essential attributes and keeps only what is relevant for security purposes. It creates consistency in log records when you are searching for specific log information.
3. Analyse data: it analyses the data according to configured rules to detect any possible security incident. It is then reported as an alert for security analysts to review.

SOAR - security orchestration, automation and response.

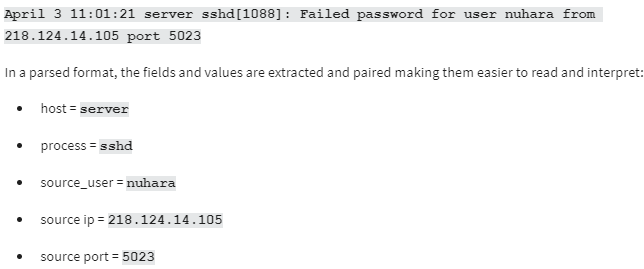
This is a collection of applications tools and workflows that uses automation to respond to security events. It can also be used to track and manage cases. Multiple events can form cases.

**Advantages of SIEM**

1. Access to event data: helps us know what is happening in a network, including real time activity. It can ingest millions of data so they can all be assessed all at once.
2. Monitoring, detecting and alerting. The contiuously monitor systems and networks in real time. They then analyse the collected data using detection rules to detect malicious activity. They can also send out alerts if an activity matches the rule.
3. Log storage: they also provide access to historical data. They can keep or delete them after a while depending on the organisation’s requirements.

Parsing can occur during the first step of the SIEM process. Parsing maps the data according to their fields and corresponding values.

It happens during the collection and aggregation process.



Normalising data.

This is where the tool transforms the data it receives from different sources into a single format that can be easily processed by the SIEM. Each data source is different, and data can be formatted in many different ways. Normalisation converts data in a standard structured format that is easily searchable.



Analyse data –

This is the process where the siem tool actually detects threat activity. They can be done with some type of detection logs such as a set of rules and conditions.

Note: a part of the analysis process includes correlation: CORRELATION involves the comparison of multiple log events to identify common patterns that indicate a potential security threat.

SIEM TOOLS

AlienVault, OSSIM, Chronicla, Elastic, Exabeam, IBM QRadar, Security Intelligence Platform, LogRhythm, Splunk.

**Glossary terms from module 1**

Terms and definitions from Course 6, Module 1

Computer security incident response teams (CSIRT): A specialized group of security professionals that are trained in incident management and response

Documentation: Any form of recorded content that is used for a specific purpose

Endpoint detection and response (EDR): An application that monitors an endpoint for malicious activity

Event: An observable occurrence on a network, system, or device

False negative: A state where the presence of a threat is not detected

False positive: An alert that incorrectly detects the presence of a threat

Incident: An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies

Incident handler’s journal: A form of documentation used in incident response

Incident response plan: A document that outlines the procedures to take in each step of incident response

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

Intrusion prevention system (IPS): An application that monitors system activity for intrusive activity and takes action to stop the activity

National Institute of Standards and Technology (NIST) Incident Response Lifecycle: A framework for incident response consisting of four phases: Preparation; Detection and Analysis; Containment, Eradication, and Recovery; and Post-incident activity

Playbook: A manual that provides details about any operational action

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

Security operations center (SOC): An organizational unit dedicated to monitoring networks, systems, and devices for security threats or attacks

Security orchestration, automation, and response (SOAR): A collection of applications, tools, and workflows that uses automation to respond to security events

True negative: A state where there is no detection of malicious activity

True positive An alert that correctly detects the presence of an attack

COURSE 6 – MODULE 2

LEAVE NO STONE UNTURNED IN CYBERSECURITY.

THE IMPORTANCE OF NETWORK TRAFFIC FLOWS.

Network traffic is the amount of data that moves across a network.

Network data is that’s transmitted between devices in a network.

By knowing what’s normal, it is easy to spot abnormalities.

We can detect abnormalities through observation to spot IOCs (indicators of compromise). These are observable evidence that suggests signs of a potential security incident.

A baseline is a reference point that’s used for comparison. In security baselines help establish a standard of expected or normal behaviour for systems, devices and networks. By knowing the baseline of a normal network, you’ll be better able to identify abnormal network behaviour.

Network components that can be monitored to detect malicious activity.

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

Command and control C2 – this is a technique used by malicious actors to maintain communications with a compromised system or systems. A malicious actor might be maintaining connection with a compromised host on https over port 8088 which is not normally associated with https (443). So organisations must know which ports should be open and approved for connections and watch out for any mismatches between ports and their associated protocols.

1. Packet Payload Information – information related to the transmission of a packet is contained in the network packet, for example the source and destination Ip addresses, the packet payload information which is the actual data that’s transmitted. Monitoring the payload information of packets can reveal when sensitive data is being transmitted outside of the network which could indicate a possible data exfiltration attack.
2. Temporal patterns – network packets containing information relating to time. It is useful in understanding time patterns. For example, if large volumes of traffic are suddenly outside of the normal hours of network activity, this is considered ***off baseline*** and should be investigated.

NETWORK OPERATIONS CENTRE – this is an organisational unit that monitors the performance of a network and responds to any network disruption such as a network outage. While DOC is focused on maintaining the security of an organisation through detection and response an NOC is responsible for maintaining network performance, availability and uptime.

Network Monitoring Tools

1. Intrusion detection systems: they monitor system activity and alert on possible intrusions. They are mostly on the lookout for unusual network activity based on the roles you have already configured. Most commonly they monitor the content of a packet payload to detect patterns associated with threats such as malware or phishing attempts.
2. Network protocol analysers. They are also called packet sniffers; they are designed to capture and analyse data traffic that traverses a network. They can be used for manual analysis of network traffic. Examples of these include TCPdump and Wireshark. They are used to record network communications through packet captures. Packet captures can then be investigated to identify potentially malicious activity.

DATA EXFILTRATION ATTACKS

Before data exfiltration can be carried out it means that the attacker already has access to the system. This can be done through social engineering like phishing. If they do, they proceed stealthily.

Lateral movement or pivoting: spending time exploring the network or expanding their access throughout the network. They scope the network out identifying sensitive data, like proprietary code, financial records, etc.

They will then need to collect, package and prepare the data for exfil. One way they do this is by reducing the data size. It helps them hide the data. One way they might exfil the data is by emailing it to themselves using the compromised email address.

HOW TO DEFEND AGAINST DATA EXFIL

1. Prevent attacker access. Requiring multi factor authentication.
2. Monitor network activity: multiple user logins coming from outside the network should be investigated.
3. Protect assets: all assets should be catalogued in an asset inventory.
4. Detect and stop the exfiltration: indicators of unusual data collection can be identified through network monitoring. This might include large internal file transfers. Large external uploads and unexpected file writes.

Ways to stop the attacker.

1. Block the IP address of the attacker by updating the firewall rule.

PACKET AND PACKET CAPTURES

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

Just like an addressed envelope in the mail, packets contain delivery information which is used to route it to its destination. This information includes a sender and receiver's IP address, the type of packet that's being sent, and more.

Components

1. Header – contains the type of network protocol and port being used. It is like the name and mailing address. Network protocols are a set of rules that determine the transmission of data between devices on a network. Ports are non-physical locations on a computer that organize data transmission between devices on a network. The header also contains the source and destination IP address.
2. Payload - this is the actual data that is being delivered. It is like the content of the letter inside an envelope.
3. Footer - the end of a packet.

Network protocol analysers - these are tools designed to capture and analyse data traffic within a network. I will need to ue them to inspect packets for indicators of compromise.

PACKET CAPTURE – PCAP

This is a file containing data packets intercepted from an interface or network. It is like intercepting an envelope in a mail. It helps you have access to communications between devices in a network.

PACKET ANALYSIS

Packet header: packets can have several headers depending on the protocols used such as ethernet header, an IP header, a TCP header and more. Headers provide information that’s used to route packets to their destinations this includes information about the source and destination IP addresses packet length, protocol, packet identification numbers and more.

A blue rectangular box with white text

Description automatically generated

PAYLOAD – this is the actual data being delivered. For example when uploading an image to a website, the payload would be the image itself.

FOOTER – it is also called the trailer, and it is located at the end of a packet. For the ethernet protocol, it used the footer to provide error checking information to determine if the data has been corrupted.

NB: the IP protocol does not use footers.

NETWORK PROTOCOL ANALYSERS

They are simp0ly tools designed to capture and analyse data traffic within a network. Examples are Tcpdump, Wireshark and Tshark. They can also be used to collect network statistics such a bandwidth or speed and troubleshoot network performance issues like slowdowns. A magnifying glass with a check mark and a green circle

Description automatically generated

How they work

1. The packets are collected from the network interface card. They only listen to network traffic that’s addressed to them by default. Enabling promiscuous or monitoring mode enables the NIC to capture all visible network data packets. But that alone doesn’t help, it must be positioned in an appropriate network segment to access all traffic between different hosts.

The data is collected in raw binary format. It then converts the data in human readable format so that analysts can understand the information.

P-CAP LIBRARIES / FORMATS

1. Libpcap – this is for Unix-like systems like Linux and MacOs. Tcpdump use libpcap as the default packet capture file format.
2. WinPcap - it is an opensource packet capture library designed for devices running the windows operating systems. It is the older file format which isn’t predominantly used.
3. Npcap is a library designed by the port scanning tool Nmap that is commonly iused in Windows operating systems.
4. PCAPng is a modern file format that can simultaneously capture packets and store data. Its ability to do both earns it the title “ng” or next generation.

PACKET CRAFTING – this is the art of creating a packet to carry out attacks and exploit the vulnerabilities in a network. It is used to penetrate a network’s structure. It is usually very difficult to detect and diagnose.

**Interpret network communications with packets.**

As you may know, networks are noisy. There's an enormous volume of communications happening between devices at any given time. And because of this, packet captures can contain large amounts of network communications, making analysis challenging and time-consuming.

REEXAMINE THE FIELDS OF AN IP HEADER

The TCP/IP model is a framework that is used to visualise how data is organised and transmitted across a network.

The internet layer accepts and delivers packets for the network. It's also the layer where the Internet Protocol operates as the foundation for all communications on the internet. It's responsible for making sure packets reach their destinations.

Different protocols use different headers…

Version field – specifies which version of IP is being used. It is like the different classes of mail - priority, express or regular.

IHL (internet header length) – this specifies the length of the OP header plus any options.

ToS (type of service) – tells us if certain packets should be treated with special care. Like a fragile sticker on a delivery.

Total length – identifies the entire length of the packet including the headers and the data. it is compared to the dimensions and weigh of an envelope.

Identification; flags and Fragment Offset - deal with information related to fragmentation.

Fragmentation - is when the IP packet is broken up into chunks, transferred and reassembled. These three fields tell when a packet has been broken up or when fragmentation has been used and state how they should be reassembled in the correct order. Similar to how mail can travel through multiple routes.

TTL - how long a packet can live before they are dropped. Similar to how tracking information provides details about an envelop expected delivery day.

Protocol – specifies the protocol used by providing a value that corresponds to a protocol. TCP is represented by 6.

Header Checksum - it stores a value used to check if an error has occurred in the header.

Source address

Destination address

Options - not required but often used for network troubleshooting rather than regular network traffic. When used the header length increases. Like purchasing postal insurance for an envelope.

INVESTIGATING PACKET DETAILS

The Internet Protocol (IP) includes a set of standards used for routing and addressing data packets as they travel between devices on a network.

A white and black text on a white background

Description automatically generated

A white text on a white background

Description automatically generated

A screenshot of a computer screen

Description automatically generated

WIRESHARK

Contains a GUI for easy visualisation of network traffic.

**Display filters** help find information when inspecting packet captures with large volumes of information. You can find specific information that is most relevant to your investigation.

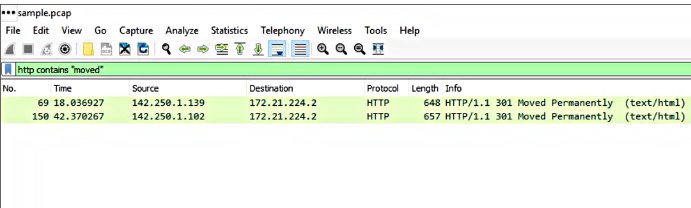
**Comparison operators** can be used to locate specific header fields and values. They can be expressed using either abbreviations or symbols. For example, this filter using the == equal symbol in this filter ip.src == 8.8.8.8 is identical to using the eq abbreviation in this filter ip.src eq 8.8.8.8. A screenshot of a computer

Description automatically generated

Pro tip: You can combine comparison operators with Boolean logical operators like **and** and **or** to create complex display filters. Parentheses can also be used to group expressions and to prioritize search terms.

**Contains operator.**

The contains operator is used to filter packets that contain an exact match of a string of text. Here is an example of a filter that displays all HTTP streams that match the keyword "moved".



Matches operator

The matches operator is used to filter packets based on the regular expression (regex) that's specified. Regular expression is a sequence of characters that forms a pattern. You'll explore more about regular expressions later in this program.

Filter toolbar

You can apply filters to a packet capture using Wireshark's filter toolbar. In this example, dns is the applied filter, which means Wireshark will only display packets containing the DNS protocol.

A screenshot of a computer

Description automatically generated

**Filter for an IP address**

You can use display filters to locate packets with a specific IP address.

For example, if you would like to filter packets that contain a specific IP address use **ip.addr**, followed by a space, the equal **==** comparison operator, and the IP address. Here is an example of a display filter that filters for the IP address **172.21.224.2**:

**ip.addr == 172.21.224.2**

To filter for packets originating from a specific source IP address, you can use the **ip.src** filter. Here is an example that looks for the **10.10.10.10** source IP address:

**ip.src == 10.10.10.10**

To filter for packets delivered to a specific destination IP address, you can use the **ip.dst** filter. Here is an example that searches for the **4.4.4.4** destination IP address:

**ip.dst == 4.4.4.4**

Filter for a MAC address

You can also filter packets according to the Media Access Control (MAC) address. As a refresher, a MAC address is a unique alphanumeric identifier that is assigned to each physical device on a network.

Here's an example:

eth.addr == 00:70:f4:23:18:c4

Filter for ports

Port filtering is used to filter packets based on port numbers. This is helpful when you want to isolate specific types of traffic. DNS traffic uses TCP or UDP port 53 so this will list traffic related to DNS queries and responses only.

For example, if you would like to filter for a UDP port:

udp.port == 53

Likewise, you can filter for TCP ports as well:

tcp.port == 25

**PACKET CAPTURES WITH TCPDUMP**

It is mostly pre-installed on Linux systems. It is a command line tool which does not have a GUI.

With tcpdump, you can apply options and flags to your commands to easily filter network traffic so that you can find exactly what you're looking for. You can filter for a specific IP address, protocol, or port number.

Note: It's common for network traffic to be encrypted, which means data is encoded and unreadable. Inspecting the network packets might require decrypting the data using the appropriate private keys.

Like many other packet sniffing tools, you’ll need to have administrator-level privileges to capture network traffic using tcpdump

The following is the tcp syntax for capturing packets:

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

The sudo tcpdump command begins running tcpdump using elevated permissions as sudo.

The -i parameter specifies the network interface to capture network traffic. You must specify a network interface to capture from to begin capturing packets. For example, if you specify -i any you’ll sniff traffic from all network interfaces on the system.

The option(s) are optional and provide you with the ability to alter the execution of the command. The expression(s) are a way to further filter network traffic packets so that you can isolate network traffic. You’ll learn more about option(s) and expression(s) in the next section.

**Note**: Before you can begin capturing network traffic, you must identify which network interface you'll want to use to capture packets from. You can use the -D flag to list the network interfaces available on a system.

Options are used at the end of commands to filter network traffic. Short options are abbreviated and represented by a hyphen and a single character like -i whereas long options are spelled out using a double hyphen like –interface.

**IMPORTANT**: options are case sensitive. A -w option is different from a -W option.

**Note**: tcpdump options that are written using short options can be written with or without a space between the option and its value. For example, sudo tcpdump -i any -c 3 and sudo tcpdump -iany -c3 are equivalent commands.

**The** -w flag is used to save tcp captures to a p-cap file instead of just having it printed out on the terminal. This way you can always go back to it for later analysis. For example

sudo tcpdump -i any -w packetcapture.pcap

**The** -r flag is used to read a particular file that has been captured. But the file name must be specified as a parameter. For example

Sudo tcpdump -r packetcapture.pcap

**The** -v flag means verbose. It allows you to control how much information tcpdump prints out for a packet because tcpdump by default does not print out all the packet’s information. The level of verbosity increases with each added v. so -vv will print out more than -v, whereas -vvv will print out more information than -vv. Using the -v flag shows you information about a packet’s IP header field. The command is

Sudo tcpdump-r packetcapture.pcap -v

**The** -c flag is used to specify how many of the packets tcpdump captured should be printed. It is usually followed by a number. For example -c 1 means that one packet will be captured. But if we specifiy -c 29 for example, it will capture and display 29 packets. The command would be

Sudo tcpdump -i any -c 10

The -n flag: it is important to know that tcpdump performs name resolution and often maps ports to the protocol that they are most associated with. But this can be misleading because for example port 80, although is most often associated with http, can use a different protocol. Tcpdump also converts IP addresses to names. Using the -n flag tells tcpdump not to resolve IP addresses to the domain names. It disables the automatic mapping of numbers tonames and is considered to be the best practice when sniffing or analysing traffic. Using the -nn will not resolve both hostname and ports. The command will be

sudo tcpdump -r packetcapture.pcap -v -n - not performing a reverse DNS lookup will prevent an attacker from being notified that they are being investigated.

**Pro tip**: only options that cannot accept parameters right after them can be combined. You cannot combine options that can accept parameters like the -r flag.

EXPRESSIONS

Using filter expressions are optional but knowing how to use them can be very important when trying to analyst a packet. For example they can help you to search network traffic by protocol only, like the **ipv6** protocol using the ip6 expression.

Boolean operators like and, or or not can also be used to filter network traffic for specific ip addresses, port and more.

sudo tcmdump -r packetcapture.pcap -n ‘ip and port 80’

**Pro tip:** You can use single or double quotes to ensure that tcpdump executes all of the expressions. You can also use parentheses to group and prioritize different expressions. Grouping expressions is helpful for complex or lengthy commands. For example, the command ip and (port 80 or port 443) tells tcpdump to prioritize executing the filters enclosed in the parentheses before filtering for IPv4.

Interpreting output.

A screenshot of a computer

Description automatically generated

**Glossary terms from module 2**

Terms and definitions from Course 6, Module 2

Command and control (C2): The techniques used by malicious actors to maintain communications with compromised systems

Command-line interface (CLI): A text-based user interface that uses commands to interact with the computer

Data exfiltration: Unauthorized transmission of data from a system

Data packet: A basic unit of information that travels from one device to another within a network

Indicators of compromise (IoC): Observable evidence that suggests signs of a potential security incident

Internet Protocol (IP): A set of standards used for routing and addressing data packets as they travel between devices on a network

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

Media Access Control (MAC) Address: A unique alphanumeric identifier that is assigned to each physical device on a network

National Institute of Standards and Technology (NIST) Incident Response Lifecycle: A framework for incident response consisting of four phases: Preparation; Detection and Analysis; Containment, Eradication and Recovery; and Post-incident activity

Network data: The data that’s transmitted between devices on a network

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

Network traffic: The amount of data that moves across a network

Network Interface Card (NIC): Hardware that connects computers to a network

Packet capture (p-cap): A file containing data packets intercepted from an interface or network

Packet sniffing: The practice of capturing and inspecting data packets across a network

Playbook: A manual that provides details about any operational action

Root user (or superuser): A user with elevated privileges to modify the system

Sudo: A command that temporarily grants elevated permissions to specific users

tcpdump: A command-line network protocol analyzer

Wireshark: An open-source network protocol analyzer

**Incident detection and Verification**

**The detection and analysis phase of the lifecycle.**

1. Detection: this is where the teams verify and analyse incidents. It allows for the prompt discovery of security events. Not all events are incidents but all incidents are events.

Challenges to detection

* 1. It is impossible to detect everything. Tools have limitations to how they work.
  2. High volumes of alerts. Alert rules that are too broad and not tuned to an organisation’s environment create false positives.

Some incidents are unavoidable, so it is vital for companies to have an incident response plan in place.

1. Analysis: this is the investigation and validation of an alert. During this process, they apply critical thinking. They examine indicators of compromise to determine if an incident has occurred.

READING: CYBERSECURITY INCIDENT DETECTION METHODS.

Threat hunting: this is the proactive search for threats on a network. Security professions use threat hunting to uncover malicious activity that was not identified by detection tools and as a way to do further analysis on detections.

They are used to detect threats before they cause damage.

Threat hunting specialist are known as threat hunters. They eagerly perform research on emerging threats and attacks and then determine the probability of an organisation being vulnerable to a particular attack. They use threat intelligence, indicators of compromise, indicators of attack and machine learning to search for threats in an organisation.

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

Cyber deception: this is the process of deliberately deceiving malicious actors with the goal of increasing detection and improving defensive strategies.

INDICATORS OF COMPROMISE.

These are observable evidence that suggests signs of a potential security incident. it does this by charting specific pieces of evidence that are associated with the attack, like a file name that is associated with a type of malware.

INDICATORS OF ATTACK

Are series of observed events that indicate a real-time incident. IOAs focus on identifying the behavioural evidence of an attacker including their methods and intentions.

IOCs help to identity the who and what of an attacker, while IOAs identify the why and how of an ongoing or unknown attacker.

Not every IOC means that an incident has happened. Sometimes it might be as a result of human error, a malfunction or other reasons unrelated to security.

PYRAMID OF PAIN

A diagram of a network structure

Description automatically generated

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.

Here’s a breakdown of the different types of indicators of compromise found in the Pyramid of Pain.

1. Hash values: Hashes that correspond to known malicious files. These are often used to provide unique references to specific samples of malware or to files involved in an intrusion.
2. IP addresses: An internet protocol address like 192.168.1.1
3. Domain names: A web address such as www.google.com
4. Network artifacts: Observable evidence created by malicious actors on a network. For example, information found in network protocols such as User-Agent strings.
5. Host artifacts: Observable evidence created by malicious actors on a host. A host is any device that’s connected on a network. For example, the name of a file created by malware.
6. Tools: Software that’s used by a malicious actor to achieve their goal. For example, attackers can use password cracking tools like John the Ripper to perform password attacks to gain access into an account.

7. Tactics, techniques, and procedures (TTPs): This is the behavior of a malicious actor. Tactics refer to the high-level overview of the behavior. Techniques provide detailed descriptions of the behavior relating to the tactic. Procedures are highly detailed descriptions of the technique. TTPs are the hardest to detect.

Screens screenshot of a screenshot of a computer error message

Description automatically generated

ANALYSE INDICATORS OF COMPROMISE WITH INVESTIGATIVE TOOLS.

For example, identifying and blocking a single IP address associated with malicious activity does not provide a broader insight on an attack, nor does it stop a malicious actor from continuing their activity. Focusing on a single piece of evidence is like fixating on a single section of a painting: You miss out on the bigger picture.

By adding context to an IoC—for instance, identifying other artifacts related to the suspicious IP address, such as suspicious network communications or unusual processes—security teams can start to develop a detailed picture of a security incident. This context can help security teams detect security incidents faster and take a more informed approach in their response.

CROWDSOURCING: this it the process of gathering information using public input and collaboration. If not an attacker can use the same tactic with multiple organisations. A person in a hoodie using a computer

Description automatically generated

With crowdsourcing, organizations harness the knowledge of millions of other cybersecurity professionals, including cybersecurity product vendors, government agencies, cloud providers, and more. Crowdsourcing allows people and organizations from the global cybersecurity community to openly share and access a collection of threat intelligence data, which helps to continuously improve detection technologies and methodologies.

A diagram of a security camera

Description automatically generated

THE BENEFITS OF DOCUMENTATION

If something was documented, then there is record of it happening. Relevant information can be access.

1. Transparency: this is useful as a source of evidence in legal proceedings, insurance claims, etc.
2. 2. Standardization: there is an est set of guidelines members of an organisation can follow to complete a task or workflow. Example is est an org sec polity. Helps maintain quality of work.
3. Clarity: it gives everyone clear understanding of their duties. It also provides info on how to get the job done. It eliminates uncertainty and confusion when there is an incident. it is important to review and update documentation regularly to keep up with the changes in the security landscape.

DOCUMENT EVIDENCE WITH CHAIN OF CUSTODY FORMS.

Evidence tracking is very important during an incident lifecycle or esp as part of any legal proceedings.

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

**Digital forensics** is the practice of collecting and analysing data to determine what has happened after an attack.

**Broken Chance Of Custody:** This occurs when there are inconsistencies in the collection and logging of evidence in the chain of custody.

**CHAIN OF CUSTODY ESTBALISHES**

1. Integrity
2. Reliability
3. Accuracy of evidence.

The forms are used to meet legal standards so they can use used in legal proceedings. They provide us with a methods of maintaining evidence so malicious actors can be held responsible for their actions.

Best practice for an effective documentation.

**Documentation** is any form of recorded content that is used for a specific purpose and is essential in the field of security. Security teams use documentations to support investigations, complete tasks and communicate findings.

Transparency

In security, transparency is critical for demonstrating compliance with regulations and internal processes, meeting insurance requirements, and for legal proceedings. 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.

Standardization

Standardization through repeatable processes and procedures supports continuous improvement efforts, helps with knowledge transfer, and facilitates the onboarding of new team members. Standards are references that inform how to set policies.

You have learned how NIST provides various security frameworks that are used to improve security measures. Likewise, organizations set up their own standards to meet their business needs. An example of documentation that establishes standardization is an incident response plan, which is a document that outlines the procedures to take in each step of incident response. Incident response plans standardize an organization’s response process by outlining procedures in advance of an incident. By documenting an organization’s incident response plan, you create a standard that people follow, maintaining consistency with repeatable processes and procedures.

Clarity

Ideally, all documentation provides clarity to its audience. Clear documentation helps people quickly access the information they need so they can take necessary action. Security analysts are required to document the reasoning behind any action they take so that it’s clear to their team why an alert was escalated or closed.

Best practices

As a security professional, you’ll need to apply documentation best practices in your career. Here are some general guidelines to remember:

Know your audience

Before you start creating documentation, consider your audience and their needs. For instance, an incident summary written for a security operations center (SOC) manager will be written differently than one that's drafted for a chief executive officer (CEO). The SOC manager can understand technical security language but a CEO might not. Tailor your document to meet your audience’s needs.

Be concise

You might be tasked with creating long documentation, such as a report. But when documentation is too long, people can be discouraged from using it. To ensure that your documentation is useful, establish the purpose immediately. This helps people quickly identify the objective of the document. For example, executive summaries outline the major facts of an incident at the beginning of a final report. This summary should be brief so that it can be easily skimmed to identify the key findings.

Update regularly

In security, new vulnerabilities are discovered and exploited constantly. Documentation must be regularly reviewed and updated to keep up with the evolving threat landscape. For example, after an incident has been resolved, a comprehensive review of the incident can identify gaps in processes and procedures that require changes and updates. By regularly updating documentation, security teams stay well informed and incident response plans stay updated.

THE VALUE OF CYBERSECURITY PLAYBOOKS – TRAVEL ITINERARY

Playbook - this is a manual that provides details about any operational action. It provides SA with instructions on what to do during an incident. playbooks clearly outline the actions to take during an incident. without playbooks an effective and swift response to an incident is nearly impossible.

Playbooks often contain checklists that can help sec teams perform effectively during stressful times by helping them complete steps in a specific order and actually remember the steps.

A diagram of a flowchart

Description automatically generated

TYPES OF PLAYBOOKS

1. Non automated: requires step by step action performed by an analysis.
2. Automated: automate tasks in incident response processes like categorising the severity of an incident or gathering evidence. They can help lower the resolution time during an incident. SOAR or SIEM tools can be configured to automate playbooks.
3. Semi-automated: this combines a person’s actions with automation. Tasks that are tedious, error prone or time-consuming tasks can be automated so that analysts focus on other tasks. They increase productivity and decrease time to resolution.

Playbooks must be updated and maintained regularly. It is good to introduce changes to playbooks during the post-incident phase.

THE ROLE OF TRIAGE IN INCIDENT RESPONSE

Hospitals determine the urgency of treatment using a process called TRIAGE: it is used to categorise patients by the urgency of their conditions. It helps to manage limited resources. Before an alert is escalated it goes through a TRIAGE process.

TRIAGE: is the prioritising of incidents according to their level of importance or urgency. Security teams have limited resoiurces for incident response. Incidents are triaged based on the threat they pose to the confidentiality, availability and integrity of systems. For example, ransomware requires immediate response. It is a higher priority than a phishing email.

TRIAGE begins when an alert is sent out. Sec need to identify the different types of alerts and prioritise them according to urgency.

TRIAGE PROCESS

1. Receive and assess - to see if it is a true positive.
2. Assign priority based on policy and guidelines.
3. Collect and analyse evidence.

Received an alert for a failed user login attempt. Asking pertinent questions might help determine if it is malicious. It describes the process of adding context.

1. Is there anything out of the ordinary?
2. Are there multiple failed login attempts?
3. Did the login happen outside of normal working hours?
4. Did the login happen outside the network?

This helps analysts avoid making conclusions.

THE TRIAGE PROCESS

It consists of 3 stages

1. Receive and assess: at the point the security analyst receives the alert from a SIEM tool or an IDS. They will have to take a closer look to see if it is a true positive because there can be multiple instances of false positives. Some questions I can ask myself to determine if it is worth responding to will be:
   1. Is it a false positive?
   2. Has this alert been triggered in the past. Knowing the history of the alert will help analysts determine if it is a new one or a recurring issue. I think this can even help with proper configuration of systems.
   3. Was it triggered by a known vulnerability? Having this knowledge will help me know how best to deal with the issue, in terms of how to respond to it and minimise the impact of the vulnerability.
   4. What is the severity of the alert? Helps determine the priority pf response.
2. Assign priority: this is very important because not all incidents have the same impact, are of the same size and require the same effort. Determining the priority of the incident will help security teams focus on the most critical incidents that can have more significant impact on the organization. There are three things to consider

* Functionality: if the incident will severely impact the ability of systems to function and provide unfettered services to end users like in a ransomware attack, it is worth escalating immediately. This is because data can be encrypted or even deleted.
* Information risk: alerts that indicate an ongoing data exfiltration attack have to be escalated immediately. This can affect the CIA of an organisation’s data and information negatively. It can have far reaching effects on the organisation.
* Recoverability: it might not be worth it allocating resources to information that cannot be recovered. Recovering from an incident depends on the size and scope of the incident and the amount of resources at the disposal of the organisation.

1. Collect and analyse: involves the comprehensive examination of the incident by collecting data from multiple sources and conducting external research. The whole investigative process must be carefully documented. Depending on the severity of the incident, it might be escalated to a level 2 security analyst or a manager.

BENEFITS OF TRIAGE

1. Resource management: triaging alerts allows security teams to focus their resources on threats that require urgent attention. This helps team members avoid dedicating time and resources to lower priority tasks and might also reduce response time.
2. Standardisation: triage provides a standardized approach to incident handling. Process documentation like playbooks help move alerts through an iterative process to ensure that alerts are properly assessed and validated. This ensures that only valid alerts are moved up to investigate.

**THE CONTAINMENT, ERADICATION AND RECOVERY PHASE OF THE INCIDENT LIFECYCLE**

CONTAINMENT: this is the act of limiting and preventing additional damage caused by an incident.

Containment strategies are contained in incident response plans. They provide detailed actions sec teams should take after an incident is detected.

For example, isolating a system from a network prevents further spread of the system in the network.

It is the first step of removing a threat from an environment.

ERADICATION: this is the complete removal of the incident elements from all the affected systems. For example, include performing vulnerability tests and applying patches related to the vulnerability.

RECOVERY: this is the returning of affected systems to normal operation. Recovery includes reimaging affected systems, resetting passwords, and adjusting network configuration rules like firewall rules.

**NOTE: THE INCIDENT RESPONSE LIFECYCLE IS CYCLICAL. MULTIPLE INCIDENTS CAN HAPPEN ACROSS TIME THAT ARE RELATED. YOU MAY HAVE TO CIRCLE BACK TO OTHER PHASES TO CONDUCT FURTHER INVESTIGATION.**

Business continuity considerations.

A business response plan is a document that outlines the procedures to sustain business operations during and after a significant disruption. A BCP helps organisations ensure that critical business functions can resume or can be quickly restored when an incident occurs.

This is important to consider because prolonged disruptions to the functionality of their systems can have serious effects like legal financial and reputational damages.

Site Resilience

Resilience is the ability to prepare for, respond to and recover from disruptions. Organisations can design their systems to be resilient so they can continue delivering services despite facing disruptions. An example is site resilience which is used to ensure the availability or networks, data centres or other infrastructure when a disruption happens. There are three types of recovery sites used for site resilience.

1. Hot sites: a fully operational facility that is a duplicate of an organisation’s primary environment. Hot sites can be activated immediately when an organisation’s primary site experiences failure or disruption.
2. 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 be quickly be made operational when a failure or disruption occurs.
3. Cold sites: a backup facility equipped with some of the necessary infrastructure required to operate an organisation’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.

THE POST INCIDENT ACTIVITY PHASE OF THE INCIDENT LIFECYCLE

This is the process of reviewing an incident to identify areas for improvement during incident handling.

Documentations get updated or created. One of the documents is the final report.

Final report: documentation that provides a comprehensive review of an incident. it includes times and details of the incident and recommendations for the future.

One way to improve processes is to hold a LESSONS Learnt meeting also known as POST MORTEM.

It is held two weeks after the incident. the final report is used as a reference document during the meeting, the goal is to share ideas about how to improve future efforts. Some questions are asked like

* 1. What happened?
  2. What time did it happen?
  3. Who discovered it?
  4. How did it get contained?
  5. What were the actions taken for recovery?
  6. What could have been done differently?

Incident reviews can review human errors before detection and during response. Blaming someone for an action they didn’t do should be avoided.

A diagram of a medical process

Description automatically generated

Pro tip: Before a team hosts a lessonS learned meeting, organizers should make sure all attendees come prepared. The meeting hosts typically develop and distribute a meeting agenda beforehand, which contains the topics of discussion and ensures that attendees are informed and prepared. Additionally, meeting roles should be assigned in advance, including a moderator to lead and facilitate discussion and a scribe to take meeting notes.

Lessons learned meetings provide opportunities for growth and improvement. For example, security teams can identify errors in response actions, gaps in processes and procedures, or ineffective security controls. A lessons learned meeting should result in a list of prioritized actions or actionable recommendations meant to improve an organization’s incident handling processes and overall security posture. This ensures that organizations are implementing the lessons they’ve learned after an incident so that they are not vulnerable to experiencing the same incident in the future. Examples of changes that can be implemented include updating and improving playbook instructions or implementing new security tools and technologies.

Common elements found in a final report:

* Executive summary. a high-level summary of the report including the key findings and essential facts related to the incident.
* Timeline: a detailed chronological timeline of the incident that includes timestamps dating the sequence of events that led to the incident.
* Investigation: a compilation of the actions taken during the detection and analysis of the incident. for example, analysis of a network artifact such as a packet capture reveals information about what activities happen on a network.
* A screenshot of a computer

  Description automatically generatedRecommendations: a list of suggested actions for future prevention.

Glossary terms from module 3

Terms and definitions from Course 6, Module 3

Analysis: The investigation and validation of alerts

Broken chain of custody: Inconsistencies in the collection and logging of evidence in the chain of custody

Business continuity plan (BCP): A document that outlines the procedures to sustain business operations during and after a significant disruption

Chain of custody: The process of documenting evidence possession and control during an incident lifecycle

Containment: The act of limiting and preventing additional damage caused by an incident

Crowdsourcing: The practice of gathering information using public input and collaboration

Detection: The prompt discovery of security events

Documentation: Any form of recorded content that is used for a specific purpose

Eradication: The complete removal of the incident elements from all affected systems

Final report: Documentation that provides a comprehensive review of an incident

Honeypot: A system or resource created as a decoy vulnerable to attacks with the purpose of attracting potential intruders

Incident response plan: A document that outlines the procedures to take in each step of incident response

Indicators of attack (IoA): The series of observed events that indicate a real-time incident

Indicators of compromise (IoC): Observable evidence that suggests signs of a potential security incident

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

Lessons learned meeting: A meeting that includes all involved parties after a major incident

Open-source intelligence (OSINT): The collection and analysis of information from publicly available sources to generate usable intelligence

Playbook: A manual that provides details about any operational action

Post-incident activity: The process of reviewing an incident to identify areas for improvement during incident handling

Recovery: The process of returning affected systems back to normal operations

Resilience: The ability to prepare for, respond to, and recover from disruptions

Standards: References that inform how to set policies

Threat hunting: The proactive search for threats on a network

Threat intelligence: Evidence-based threat information that provides context about existing or emerging threats

Triage: The prioritizing of incidents according to their level of importance or urgency

VirusTotal: A service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content.

COURSE 6, MODULE 4

OVERVIEW OF LOGS.

Logs support incident investigations. Events are a valuable data source. They help create context around an alert so you can interpret the actions that took place on a system.

System activity is recorded on a log file. Logs are useful during investigation because they record detail like what where and why an event occurred. Date time location action and names of users who perform the action. They are used to build a story and timeline to identify what happened.

Log analysis - this is the process of examining logs to identify events of interest.

It is important to log efficiently. One must be selective in what is logged.

How logs get collected

* Log forwarders software collect logs from various and automatically forward them to a centralised log repository for storage.

Types of logs

* Network logs – proxies routers switches and firewalls
* System logs – operating systems
* Application logs – software applicaitons
* Security logs – IDS and IPS
* Authentication logs – records login attempts.

Best practices for log collection and management

Log details

Generally, logs contain a date, time, location, action, and author of the action. Here is an example of an authentication log:

Login Event [05:45:15] User1 Authenticated successfully.

Logs contain information and can be adjusted to contain even more information. Verbose logging records additional, detailed information beyond the default log recording. Here is an example of the same log above but logged as verbose.

Login Event [2022/11/16 05:45:15.892673] auth\_performer.cc:470 User1 Authenticated successfully from device1 (192.168.1.2)

Log management

Because all devices produce logs, it can quickly become overwhelming for organizations to keep track of all the logs that are generated. To get the most value from your logs, you need to choose exactly what to log, how to access it easily, and keep it secure using log management. Log management is the process of collecting, storing, analyzing, and disposing of log data.

What to log

The most important aspect of log management is choosing what to log. Organizations are different, and their logging requirements can differ too. It's important to consider which log sources are most likely to contain the most useful information depending on your event of interest. This might be configuring log sources to reduce the amount of data they record, such as excluding excessive verbosity. Some information, including but not limited to phone numbers, email addresses, and names, form personally identifiable information (PII), which requires special handling and, in some jurisdictions, might not be possible to be logged.

The issue with overlogging

From a security perspective, it can be tempting to log everything. This is the most common mistake organizations make. Just because it can be logged, doesn't mean it needs to be logged. Storing excessive amounts of logs can have many disadvantages with some SIEM tools. For example, overlogging can increase storage and maintenance costs. Additionally, overlogging can increase the load on systems, which can cause performance issues and affect usability, making it difficult to search for and identify important events.

Log protection.

Along with management and retention, the protection of logs is vital in maintaining log integrity. It’s not unusual for malicious actors to modify logs in attempts to mislead security teams and to even hide their activity.

Storing logs in a centralized log server is a way to maintain log integrity. When logs are generated, they get sent to a dedicated server instead of getting stored on a local machine. This makes it more difficult for attackers to access logs because there is a barrier between the attacker and the log location.

The primary purpose of logs during incident investigation is to provide a record of event details. Knowing what occurred on systems, networks, and devices helps security analysts identify unusual or malicious activity.

VARIATIONS OF LOGS – RECEIPTS IN A SHOP

Logs come in different formats but they contain the same thing like

1. Timestamps
2. System characteristics
3. Action taken and who performed it.

Logs are often generated from different data sources. Some are human readable while others are machine readable, some are verbose while others are short and simple.

Commonly used log formats

1. Syslogs. It is both a protocol and a log format. As a protocol, it transports and writes logs. As a log format it contains a header and a structured data and a message. 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. JSON – javascript object notation. It is known for simplicity and readability. It’s a text-based format designed to be easy to read and write. It also uses key-value pairs to structure data.
3. Extensible Markup Language (XML): Is used for storing and transmitting data. Instead of using key value formats, it uses tags and other keys to structure data.
4. Comma separated values (CSV).
5. CEF (Common Event Format)
6. Common Event Format (CEF) is a log format that uses key-value pairs to structure data and identify fields and their corresponding values. The CEF syntax is defined as containing the following fields:

CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

SECURITY MONITORING WITH DETECTION TOOLS

Telemetry: is the collection and transmission of data for analysis. While logs record events, telemetry describes the data itself like packet captures.

IDS is an application that monitors system activity and alerts on possible intrusions.

Endpoint is any device connected to a network. They are entry points making them key targets.

To monitor endpoints, a Host based intrusion detection system is used. It is an application that monitors the activity of the host on which it’s installed. A host is any device that comms with another device on a network.

A network based intrusion detection system is an application that collects and monitors network traffic and network data. Multiple IDS can be deployed at different points in the network to achieve adequate visibility. It logs unusual network activity and generates an alert.

IDS use diff detection methods of which one is signature analysis.

Signature analysis is a detection method used to find events of interest. A signature is the set of rules an ids refers to when it is monitoring network activity. If it matches, ids logs it and sends an alert. For example when a failed login attempt happens three times in a row.

The activity must be logged before an alert is generated. Ids tech records the information as ids logs. They can be sent stored and analysed in a central log repository.

The two types of detection techniques that are commonly used by IDS technologies are signature-based analysis and anomaly-based analysis.

Signature-based analysis

Signature analysis, or signature-based analysis, is a detection method that is used to find events of interest. A signature is a pattern that is associated with malicious activity. Signatures can contain specific patterns like a sequence of binary numbers, bytes, or even specific data like an IP address.

Previously, you explored the Pyramid of Pain, which is a concept that prioritizes the different types of indicators of compromise (IoCs) associated with an attack or threat, such as IP addresses, tools, tactics, techniques, and more. IoCs and other indicators of attack can be useful for creating targeted signatures to detect and block attacks.

Different types of signatures can be used depending on which type of threat or attack you want to detect. For example, an anti-malware signature contains patterns associated with malware. This can include malicious scripts that are used by the malware. IDS tools will monitor an environment for events that match the patterns defined in this malware signature. If an event matches the signature, the event gets logged and an alert is generated.

Anomaly-based analysis

Anomaly-based analysis is a detection method that identifies abnormal behavior. There are two phases to anomaly-based analysis: a training phase and a detection phase. In the training phase, a baseline of normal or expected behavior must be established. Baselines are developed by collecting data that corresponds to normal system behavior. In the detection phase, the current system activity is compared against this baseline. Activity that happens outside of the baseline gets logged, and an alert is generated.

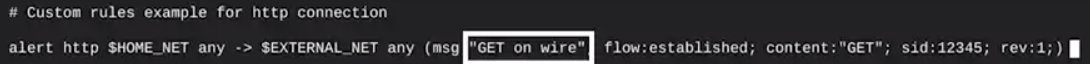
Components of a detection signature – examining signature syntax

Signatures are rules you want an IDS to connect for example configuring an ids to detect malicious traffic on a specific port.

Components of an NIDS rule

1. Action: determines what action to take if the rule criteria is met. Some common actions are allow, pass or reject.
2. Header: this defines the signature’s network traffic. Includes source and des tip addresses, source and destination ports, protocols and traffic direction. We can specify unusual IP addresses in the header.
3. Rule options: allows you customise signatures with additional parameters. For example, you can set options to match the contents of a malicious packet to detect malicious payloads which reside in the packets data. This helps in narrowing network traffic to find exactly what you are looking for. They are enclosed in parenthesis and separated by semicolons.
4. 

EXAMINE SIGNATURES WITH SURICATA



Suricata Format Type

Alerts and events are output in EVE – extensible event format JSON – JavaScript Object Notation

Suricata generates alert logs (these are the logs that are often related to security) and network telemetry logs (simply record what is happening across a network). However, both logs are used to build a story around what happened during an event.

Note: Rule order refers to the order in which rules are evaluated by Suricata. Rules are processed in the order in which they are defined in the configuration file. However, Suricata processes rules in a different default order: pass, drop, reject, and alert. Rule order affects the final verdict of a packet especially when conflicting actions such as a drop rule and an alert rule both match on the same packet.0

Although suricata comes with pre-written rules, it is highly recommended that you modify or customise the existing rules to meet your specific requirements. This is because each organization’s IT infrastructure is different. So security teams have to extensively test and modify detection signatures according to their needs. Custom roles helps to reduce the amount of false positives alerts that the security teams receive.

A configuration file is a file used to configure the settings of an application. Configuration files let you customise exactly how you want your IDS to interact with the rest of your environment.

Suricata’s config file is suricata.yaml. It uses YAML file syntax and structure.

LOG FILES

Suricata generates two types of log files:

1. eve.json. this file type is seen as more detailed and effective when conducting security investigations. It contains a unique identifier called flow\_id which is used to correlate related log files or alerts to a single network flow making it easier to analyse network traffic. It is the standard suricata log file.
2. fast.log: this is considered legacy and is not recommended for threat hunting or incident response efforts. It only records basic logs like ip address and port details about network traffic. Contains only minimal alert information.

Question 4

A security analyst creates a Suricata signature to identify and detect security threats based on the direction of network traffic. Which of the following rule options should they use?

They should use flow. The flow option matches the direction of network traffic flow. The content option is used to specify a specific string found in a network packet that the signature should match.

REEXAMINE SIEM TOOLS

A siem is an app that collects and analyses log data to monitor critical activities in an organisation. It does this by collecting analysing and reporting on sec data from multiple sources.

SIEM PROCESS

1. collect and analyse data from different sources.
2. Normalising data by including only relevant data. It represents the data using a standard format.
3. They index the data so that It can be accessed through search.

**Log forwarders.**

A common way that organizations collect log data is to use log forwarders. **Log forwarders are software that automate the process of collecting and sending log data.**

QUERY FOR EVENTS WITH SPLUNK

SPLUNK USES SPL – search processing language

CHRONICLE – default method is using udm – unified data model which searches through normalised data. You can then search through raw logs.

**Glossary terms from module 4**

Terms and definitions from Course 6, Module 4

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

Array: A data type that stores data in a comma-separated ordered list

Common Event Format (CEF): A log format that uses key-value pairs to structure data and identify fields and their corresponding values

Configuration file: A file used to configure the settings of an application

Endpoint: Any device connected on a network

Endpoint detection and response (EDR): An application that monitors an endpoint for malicious activity

False positive: An alert that incorrectly detects the presence of a threat

Host-based intrusion detection system (HIDS): An application that monitors the activity of the host on which it’s installed

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

Key-value pair: A set of data that represents two linked items: a key, and its corresponding value

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

Log analysis: The process of examining logs to identify events of interest

Log management: The process of collecting, storing, analyzing, and disposing of log data

Logging: The recording of events occurring on computer systems and networks

Network-based intrusion detection system (NIDS): An application that collects and monitors network traffic and network data

Object: A data type that stores data in a comma-separated list of key-value pairs

Search Processing Language (SPL): Splunk’s query language

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

Signature: A pattern that is associated with malicious activity

Signature analysis: A detection method used to find events interest

Suricata: An open-source intrusion detection system, intrusion prevention system, and network analysis tool

Telemetry: The collection and transmission of data for analysis

Wildcard: A special character that can be substituted with any other character.

YARA-L: A computer language used to create rules for searching through ingested log data.

Zero-day: An exploit that was previously unknown.

Glossary

Cybersecurity

Terms and definitions from Course 6

A

Advanced persistent threat (APT): An instance when a threat actor maintains

unauthorized access to a system for an extended period of time

Analysis: The investigation and validation of alerts

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

Array: A data type that stores data in a comma-separated ordered list

B

Broken chain of custody: Inconsistencies in the collection and logging of evidence in

the chain of custody

Business continuity plan (BCP): A document that outlines the procedures to sustain

business operations during and after a significant disruption

C

Chain of custody: The process of documenting evidence possession and control

during an incident lifecycle

Command and control (C2): The techniques used by malicious actors to maintain

communications with compromised systems

Command-line interface (CLI): A text-based user interface that uses commands to

interact with the computer

Common Event Format (CEF): A log format that uses key-value pairs to structure

data and identify fields and their corresponding values

Computer security incident response teams (CSIRT): A specialized group of

security professionals that are trained in incident management and response

Configuration file: A file used to configure the settings of an application

Containment: The act of limiting and preventing additional damage caused by an

incident

Crowdsourcing: The practice of gathering information using public collaboration

D

Data exfiltration: Unauthorized transmission of data from a system

Data packet: A basic unit of information that travels from one device to another within

a network

Detection: The prompt discovery of security events

Documentation: Any form of recorded content that is used for a specific purpose

E

Endpoint: Any device connected on a network

Endpoint detection and response (EDR): An application that monitors an endpoint

for malicious activity

Eradication: The complete removal of the incident elements from all affected systems

Event: An observable occurrence on a network, system, or device

F

False negative: A state where the presence of a threat is not detected

False positive: An alert that incorrectly detects the presence of a threat

Final report: Documentation that provides a comprehensive review of an incident

H

Honeypot: A system or resource created as a decoy vulnerable to attacks with the

purpose of attracting potential intruders

Host-based intrusion detection system (HIDS): An application that monitors the

activity of the host on which it’s installed

I

Incident: An occurrence that actually or imminently jeopardizes, without lawful

authority, the confidentiality, integrity, or availability of information or an information

system; or constitutes a violation or imminent threat of violation of law, security

policies, security procedures, or acceptable use policies

Incident handler’s journal: A form of documentation used in incident response

Incident response plan: A document that outlines the procedures to take in each step

of incident response

Indicators of attack (IoA): The series of observed events that indicate a real-time

incident

Indicators of compromise (IoC): Observable evidence that suggests signs of a

potential security incident

Internet Protocol (IP): A set of standards used for routing and addressing data

packets as they travel between devices on a network

Intrusion detection system (IDS): An application that monitors system activity and

alerts on possible intrusions

Intrusion prevention system (IPS): An application that monitors system activity for

intrusive activity and takes action to stop the activity

K

Key-value pair: A set of data that represents two linked items: a key, and its

corresponding value

L

Lessons learned meeting: A meeting that includes all involved parties after a major

incident

Log analysis: The process of examining logs to identify events of interest

Log management: The process of collecting, storing, analyzing, and disposing of log

data

Logging: The recording of events occurring on computer systems and networks

M

Media Access Control (MAC) Address: A unique alphanumeric identifier that is

assigned to each physical device on a network

N

National Institute of Standards and Technology (NIST) Incident Response

Lifecycle: A framework for incident response consisting of four phases: Preparation;

Detection and Analysis; Containment, Eradication, and Recovery; and Post-incident

activity

Network-based intrusion detection system (NIDS): An application that collects and

monitors network traffic and network data

Network data: The data that’s transmitted between devices on a network

Network Interface Card (NIC): Hardware that connects computers to a network

Network protocol analyzer (packet sniffer): A tool designed to capture and analyze

data traffic within a network

Network traffic: The amount of data that moves across a network

O

Object: A data type that stores data in a comma-separated list of key-value pairs

Open-source intelligence (OSINT): The collection and analysis of information from

publicly available sources to generate usable intelligence

P

Packet capture (p-cap): A file containing data packets intercepted from an interface

or network

Packet sniffing: The practice of capturing and inspecting data packets across a

network

Playbook: A manual that provides details about any operational action

Post-incident activity: The process of reviewing an incident to identify areas for

improvement during incident handling

R

Recovery: The process of returning affected systems back to normal operations

Resilience: The ability to prepare for, respond to, and recover from disruptions

Root user (or superuser): A user with elevated privileges to modify the system

S

Search Processing Language (SPL): Splunk’s query language

Security information and event management (SIEM): An application that collects

and analyzes log data to monitor critical activities in an organization

Security operations center (SOC): An organizational unit dedicated to monitoring

networks, systems, and devices for security threats or attacks

Security orchestration, automation, and response (SOAR): A collection of

applications, tools, and workflows that uses automation to respond to security events

Signature: A pattern that is associated with malicious activity

Signature analysis: A detection method used to find events interest

Standards: References that inform how to set policies

Sudo: A command that temporarily grants elevated permissions to specific users

Suricata: An open-source intrusion detection system and intrusion prevention system

T

tcpdump: A command-line network protocol analyzer

Telemetry: The collection and transmission of data for analysis

Threat hunting: The proactive search for threats on a network

Threat intelligence: Evidence-based threat information that provides context about

existing or emerging threats

Triage: The prioritizing of incidents according to their level of importance or urgency

True negative: A state where there is no detection of malicious activity

True positive An alert that correctly detects the presence of an attack

V

VirusTotal: A service that allows anyone to analyze suspicious files, domains, URLs,

and IP addresses for malicious content

W

Wildcard: A special character that can be substituted with any other character

Wireshark: An open-source network protocol analyzer

Y

YARA-L: A computer language used to create rules for searching through ingested log.

data

Zero-day: An exploit that was previously unknown.

PYTHON AND CYBER SECURITY

Programming is used to create a specific set of instructions for a computer to execute tasks.

Python is a general purpose language. It is not specialised in any sort of problems. It is used to perform data analysis but in security it is used to automate tasks.

AUTOMATION: the use of technology to reduce human and manual effort to perform common and repetitive tasks. You use it to automate short simple tasks.

For example a security analyst can use python to analyse logs for events of interest. Python can also be used to manage access control lists. The list of who can access systems and its resources. A python programme can periodically monitor this system. This is more or less like using Aws lambda.

Python can also be used to combine separate tasks into one workflow.

Advantages of python

1. Resembles human language.
2. Requires less code.
3. Easy to read.
4. Benefits of following standard guidelines
5. Online support
6. Built-in-code, libraries etc.

Programming languages are converted to binary numbers, which are a series of 0s and 1s that represent the operations that the computer's central processing unit (CPU) should perform. Each instruction corresponds to a specific operation, such as adding two numbers or loading a value from memory.

Python code must be converted through an interpreter before the computer can process it.

An **interpreter** is a computer program that translates Python code into runnable instructions line by line.

**Syntax** refers to the rules that determine what is correctly structured in a computing language.

**Specific areas python might be used to automate tasks.**

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

CREATING A PYTHON SCRIPT

A script is simply what we write in a code.

It is good practice to begin with a comment before writing the code. A comment is the note programmers make about the intention behind their code.

A # symbol is used to represent a comment

# Print Hello Python - comment

print “Hello python!” - code

Print outputs a specified object to the screen.

After using print, make sure what you want to output is in parenthesis.

The string data, or what we want to output must be enclosed in quotation marks. The quotation marks is one example of syntax.

Syntax - the rules that determine what is correctly structured in computing language.

Python Environments are varied. It can be run through IDEs, the command line also.

Notebooks are online interfaces for writing, storing and running code. They also allow you to document information about the code. Notebook content either appears in a code cell or markdown cell.

Code cell: these are meant for writing and running code. A notebook provides a mechanism for running code cells. Often this is a play button located within the cell. When you run the code, its output appears after the code.

Markdown cell: these are meant for describing the code. They allow you to format text in the markdown language. Markdown language is use for formatting plain text in text editors and code editors. For example you might indicate that a text should be in a certain header style.

Conditional Statements in Python

A conditional statement evaluates code to determine if it meets a specified set of conditions. The keyword is important in a conditional statement. IF starts a condition.

After IF we specify the condition that must be met and what will happen if it is.

For example:

If failed\_attempts > 5:

Print(“Account locked”)

The colon: signifies what we want to happen when the condition is met. In this case when the use has tried more than 5 times.

Note: the print statement must be indented so that it executes only when the condition is true.

The first line is called the header and the actions that happens when the condition is met is called the Body.

OPERATORS

1. >
2. <
3. >=
4. <=
5. == : this operator evaluates whether two objects match. It assigns a Boolean value of true when they match and a value of false if they don’t.
6. != not equal. This evaluates whether two objects are different. It assigns a Boolean value of true when they don’t match and false when they match.

Else – precedes a code section that only evaluates when all conditions that precede it within the conditional statement evaluate to False.

The header of an if statement

The first line of this code is the header. In the header of an if statement, the keyword if is followed by the condition. Here, the condition is that the status variable is equal to a value of 200. The condition can be placed in parentheses:

if (status == 200):

print("OK")

Note: You must always place a colon (:) at the end of the header. Without this syntax, the code will produce an error.

Note: For the body of the if statement to execute as intended, it must be indented further than the header. Additionally, if there are multiple lines of code within the body, they must all be indented consistently.

else statements

The keyword else precedes a code section that only evaluates when all conditions that precede it within the conditional statement evaluate to False.

In the following example, when the HTTP response status code is not equal to 200, it prints an alternative message of "check other status":

if status == 200:

print("OK")

else:

print("check other status")

Note: Like with if, a colon (:) is required after else, and the body that follows the else header is indented.

elif statements

In some cases, you might have multiple alternative actions that depend on new conditions. In that case, you can use elif. The elif keyword precedes a condition that is only evaluated when previous conditions evaluate to False. Unlike with else, there can be multiple elif statements following if.

For example, you might want to print one message if the HTTP response status code is 200, one message if it is 400, and one if it is 500. The following code demonstrates how you can use elif for this:

if status == 200:

print("OK")

elif status == 400:

print("Bad Request")

elif status == 500:

print("Internal Server Error")

**Note**: Python processes multiple elif statements differently than multiple if statements. When it reaches an elif statement that evaluates to True, it won’t check the following elif statements. On the other hand, Python will run all if statements.

Logical operators for multiple conditions

In some cases, you might want Python to perform an action based on a more complex condition. You might require two conditions to evaluate to True. Or, you might require only one of two conditions to evaluate to True. Or, you might want Python to perform an action when a condition evaluates to False. The operators and, or, and not can be used in these cases.

**and**

The and operator requires both conditions on either side of the operator to evaluate to True. For example, all HTTP status response codes between 200 and 226 relate to successful responses. You can use **and** to join a condition of being greater than or equal to 200 with another condition of being less than or equal to 226:

if status >= 200 and status <= 226:

print("successful response")

When both conditions are True, then the "successful response" message will print.

or

The or operator requires only one of the conditions on either side of the operator to evaluate to True. For example, both a status code of 100 and a status code of 102 are informational responses. Using or, you could ask Python to print an "informational response" message when the code is either 100 or 102:

if status == 100 or status == 102:

print("informational response")

Only one of these conditions needs to be met for Python to print the message.

not

The not operator negates a given condition so that it evaluates to False if the condition is True and to True if it is False. For example, if you want to indicate that Python should check the status code when it’s something outside of the successful range, you can use not:

if not(status >= 200 and status <= 226):

print("check status")

Note: In this case, the parentheses are necessary for the code to apply not to both conditions. Python will evaluate the conditions within the parentheses first. This means it will first evaluate the conditions on either side of the **and** operator and then apply **not** to both of them.

The in operator in Python can be used to determine whether a given value is an element of a sequence. Using the in operator in a condition can help you check whether a specific username is part of a list of approved usernames. For example, in the code below, username in approved\_list evaluates to True if the value of the username variable is included in approved\_list

Loops in Python.

An iterative statement is code that repeatedly executes a set of instructions.

**for loops : If you need to iterate through a specified sequence, you should use a for loop.**

**Loop variable:** The **loop variable** is a variable that is used to control the iterations of a loop.

**For i in [‘sycamore’, ‘jude’, ‘breckneck’]:**

**The body of the for loop might consist of multiple lines of code. In the body, you indicate what the loop should do with each iteration**

**Note:** When used in a **for** loop, the **in** operator precedes the sequence that the **for** loop will iterate through. When used in a conditional statement, the **in** operator is used to evaluate whether an object is part of a sequence.  The example **if "elarson" in ["tshah", "bmoreno", "elarson"]** evaluates to **True** because **"elarson"** is part of the sequence following **in**.

**You can declare assign a variable to a sequence so that you don’t have to do that within the for loop header.**

### ****Using  range()****

Another way to iterate through a **for** loop is based on a sequence of numbers, and this can be done with **range()**. The **range()** function generates a sequence of numbers. It accepts inputs for the start point, stop point, and increment in parentheses. For example, the following code indicates to start the sequence of numbers at **0**, stop at **5**, and increment each time by **1**:

**range(0, 5, 1)**

**Note:** The start point is inclusive, meaning that **0** will be included in the sequence of numbers, but the stop point is exclusive, meaning that **5** will be excluded from the sequence. It will conclude one integer before the stopping point.

**You should be aware that it's always necessary to include the stop point, but if the start point is the default value of 0 and the increment is the default value of 1, they don't have to be specified in the code.**

**Integers in the Loop condition**

**Often, as just demonstrated, the loop condition is based on integer values. For example, you might want to allow a user to log in as long as they've logged in less than five times. Then, your loop variable, login\_attempts, can be initialized to 0, incremented by 1 in the loop, and the loop condition can specify to iterate only when the variable is less than 5**

### Boolean values in the loop condition

Conditions in **while** loops can also depend on other data types, including comparisons of Boolean data. In Boolean data comparisons, your loop condition can check whether a loop variable equals a value like **True** or **False**. The loop iterates an indeterminate number of times until the Boolean condition is no longer **True.**

**Managing Loops**

you can use the **break** and **continue** keywords to further control your loop iterations. Both are incorporated into the conditional statement within the body of the loop. They can be inserted to execute when the condition in an if statement is True. The **break** keyword is used to break out of a loop. The **continue** keyword is used to skip an iteration and continue with the next one.

Python Concepts from Module 1 Course 6

Comments

The following syntax is used to create a comment. (A comment is a note programmers

make about the intention behind their code.)

#

Starts a line that contains a Python comment

# Print approved usernames

Contains a comment that indicates the purpose of the code that follows it is to

print approved usernames

Functions

The following functions are commonly used in Python.

print()

Outputs a specified object to the screen

print("login success")

Outputs the string "login success" to the screen

print(9 < 7)

Outputs the Boolean value of False to the screen after evaluating whether the

integer 9 is less than the integer 7

type()

Returns the data type of its input

print(type(51.1))

Returns the data type of float for the input of 51.1

print(type(True))

Returns the data type of Boolean for the input of True

range()

Generates a sequence of numbers

range(0, 5, 1)

Generates a sequence with a start point of 0, a stop point of 5, and an

increment of 1; because the start point is inclusive but the stop point is

exclusive, the generated sequence is 0, 1, 2, 3, and 4

range(5)

Generates a sequence with a stop point of 5; when the start point is not

specified, it is set at the default value of 0, and when the increment is not

specified, it is set at the default value of 1; the generated sequence is 0, 1, 2, 3,

and 4

Conditional statements

The following keywords and operators are used in conditional statements.

if

Starts a conditional statement

if device\_id != "la858zn":

Starts a conditional statement that evaluates whether the device\_id variable

contains a value that is not equal to "la858zn"

if user in approved\_list:

Starts a conditional statement that evaluates if the user variable contains a

value that is also found in the approved\_list variable

elif

Precedes a condition that is only evaluated when previous conditions evaluate to

False; previous conditions include the condition in the if statement, and when

applicable, conditions in other elif statements

elif status == 500:

When previous conditions evaluate to False, evaluates if the status variable

contains a value that is equal to 500

else

Precedes a code section that only evaluates when all conditions that precede it within

the conditional statement evaluate to False; this includes the condition in the if

statement, and when applicable, conditions in elif statements

else:

When previous conditions evaluate to False, Python evaluates this else

statement

and

Requires both conditions on either side of the operator to evaluate to True

if username == "bmoreno" and login\_attempts < 5:

Evaluates to True if the value in the username variable is equal to "bmoreno"

and the value in the login\_attempts variable is less than 5

or

Requires only one of the conditions on either side of the operator to evaluate to True

if status == 100 or status == 102:

Evaluates to True if the value in the status variable is equal to 100 or the value

in the status variable is equal to 102

not

Negates a given condition so that it evaluates to False if the condition is True and to

True if it is False

if not account\_status == "removed"

Evaluates to False if the value in the account\_status variable is equal to

"removed" and evaluates to True if the value is the account\_status variable

is not equal to "removed"

Iterative statements

The following keywords are used in iterative statements.

for

Signals the beginning of a for loop; used to iterate through a specified sequence

for username in ["bmoreno", "tshah", "elarson"]:

Signals the beginning of a for loop that iterates through the sequence of

elements in the list ["bmoreno", "tshah", "elarson"] using the loop

variable username

for i in range(10):

Signals the beginning of a for loop that iterates through a sequence of

numbers created by range(10) using the loop variable i

while

Signals the beginning of a while loop; used to iterate based on a condition

while login\_attempts < 5:

Signals the beginning of a while loop that will iterate as long as the condition

that the value of login\_attempts is less than 5 evaluates to True

break

Used to break out of a loop

continue

Used to skip a loop iteration and continue with the next one

Glossary terms from module 1

Terms and definitions from Course 7, Module 1

Automation: The use of technology to reduce human and manual effort to perform common and repetitive tasks

Boolean data: Data that can only be one of two values: either True or False

Command-line interface: A text-based user interface that uses commands to interact with the computer

Comment: A note programmers make about the intention behind their code

Conditional statement: A statement that evaluates code to determine if it meets a specified set of conditions

Data type: A category for a particular type of data item

Dictionary data: Data that consists of one or more key-value pairs

Float data: Data consisting of a number with a decimal point

Integer data: Data consisting of a number that does not include a decimal point

Integrated development environment (IDE): A software application for writing code that provides editing assistance and error correction tools

Interpreter: A computer program that translates Python code into runnable instructions line by line

Iterative statement: Code that repeatedly executes a set of instructions

List data: Data structure that consists of a collection of data in sequential form

Loop variable: A variable that is used to control the iterations of a loop

Notebook: An online interface for writing, storing, and running code

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

Set data: Data that consists of an unordered collection of unique values

String data: Data consisting of an ordered sequence of characters

Syntax: The rules that determine what is correctly structured in a computing language

Tuple data: Data structure that consists of a collection of data that cannot be changed

Type error: An error that results from using the wrong data type

Variable: A container that stores data

INTRODUCTION TO FUNCTIONS

Writing code multiple times is time consuming, but with the use of functions we can reuse codes. It is a section of code that can be reused during programming.

They consist of small instructions and can be called upon any number of times anywhere in our code.

We can make changes to the function and they are applied everywhere they occur in a code.

Built -in functions: these are functions that exist within Python and can be called directly. They are available by default.

User defined functions: these are functions that programmers design for their specific needs.

Functions make working in Python more effective and efficient.

USER DEFINED FUNCTION

def: this is a keyword placed before a function name to define a function.

User-defined functions are functions that programmers design for their specific needs. To define a function, you need to include a function header and the body of your function.

Function header

The function header is what tells Python that you are starting to define a function. For example, if you want to define a function that displays an "investigate activity" message, you can include this function header:

def display\_investigation\_message():

The def keyword is placed before a function name to define a function. In this case, the name of that function is display\_investigation\_message.

The parentheses that follow the name of the function and the colon (:) at the end of the function header are also essential parts of the syntax.

Function body

The body of the function is an indented block of code after the function header that defines what the function does. The indentation is very important when writing a function because it separates the definition of a function from the rest of the code.

To add a body to your definition of the display\_investigation\_message() function, add an indented line with the print() function. Your function definition becomes the following:

def display\_investigation\_message():

print("investigate activity")

PAREMETER IN PYTHON

A parameter is an object that is included in a function definition for use in that function.

They are accepted into a function through the parenthesis in the function name.

For example range(start, stop)

ARGUMENT (PYTHON)

This is the data brought into a function when it is called. For example range (3, 7) the 3 and 7 are arguments.

RETURN STATEMENTS

We can pass arguments into a function, but we can also send information out of a function. We do this using a RETURN STATEMENT.

A return statement is a python statement that executes inside a function and sends information back to the function call.

Use case

Checking if someone is allowed to access a particular file and returns a Boolean value of true or false to the larger program.

Another

Analysing log in attempts could come in the form of computing the percentage of failed login attempts and return this percentage to the program which can use this to determine if to lock an account.

RETURN

This keyword is used to return information from a function to the caller of the function.

It is important to remember that when Python encounters the return function, it executes the function and exits the function. It does not continue running any other code that follow the return statement. This is something I must keep in mind.

When defining and calling functions, you're working with local variables, which are different from the variables you define outside the scope of a function.

Global variables

A global variable is a variable that is available through the entire program. Global variables are assigned outside of a function definition. Whenever that variable is called, whether inside or outside a function, it will return the value it is assigned.

For example, you might assign the following variable at the beginning of your code:

device\_id = "7ad2130bd"

Throughout the rest of your code, you will be able to access and modify the device\_id variable in conditionals, loops, functions, and other syntax.

Local variables

A local variable is a variable assigned within a function. These variables cannot be called or accessed outside of the body of a function. Local variables include parameters as well as other variables assigned within a function definition.

In the following function definition, total\_string and name are local variables:

def greet\_employee(name):

total\_string = "Welcome" + name

return total\_string

The variable total\_string is a local variable because it's assigned inside of the function. The parameter name is a local variable because it is also created when the function is defined.

Whenever you call a function, Python creates these variables temporarily while the function is running and deletes them from memory after the function stops running.

This means that if you call the greet\_employee() function with an argument and then use the total\_string variable outside of this function, you'll get an error.

The function accesses the global variable. If you wanted the identify\_user() function to accommodate other usernames, you would have to reassign the global username variable outside of the function. This isn't good practice. A better way to pass different values into a function is to use a parameter instead of a global variable.

A screenshot of a computer program

Description automatically generated

EXPLORING PYTHON’S BUILT IN FUNCTIONS

They are functions that exist within python and can be called directly.

When functions are used together, it happens that the inner function is processed first and the value is passed to the outer function.

For example, print (type(“hello”)). In this, the type function is processed and passed to the print function.

It is important to note that some functions only accept specific data types and will return an error is the wrong type of data is fed into it. They also need a specific amount of parameters.

The print function outputs all data types and also accepts an unlimited number of parameters.

So before using a built-in function, we have to know how many parameters they require and the data type they accept. We also need to know what kind of output they produce.

max() - this returns the largest numeric input passed into it. It doesn’t have a defined number of parameters.

a= 3

b= 9

c= 6

print (max(a,b,c)) - this tells us that the highest value among those is 9.

sorted() this is a function that sorts the components of a list.

The sorted() function does not change the iterable that it sorts.

NB: you cannot have mixed data types in the sorted() function.

PSEUDOCODE: this is a simplified language that is a bit close to a programming language. It is often used to represent an algorithm.

LIBARIES IN PYTHON

To access additional functions, you can import a library.

Library: this is a collection of modules that provide code users can access in their programs.

Module: this is a python file that contains additional functions, variables, classes and any kind of runnable code.

PYTHON STANDARD LIBRARY:

This is an extensive collection of usable python code that comes packaged with python.

The re module in Python: this is used to search for patterns in log files. You will be using this as a security analyst.

The CSV module allows you to work efficiently with CSV files.

The glob and OS modules are used for interacting with the command line.

The time and datatime modules are used when working with time stamps.

External library websites are also available.

Examples include Beautiful Soup which is used for parsing website HTML files and NumPy for arrays and mathematical computations. They are useful in analysing network traffic, log file parsing and complex math.

CODE READABILITY

STYLE GUIDE: this is a manual that informs the writing, formatting and design of documents. They are intended to make programmers follow similar conventions.

PEP 8 STYLE GUIDE is a resource that provides stylistic guidelines for programmers working in Python. Python Enhanced Proposals.

It is used to create consistency among programmers. It is based on the principle that code is read more than it is written. It helps everyone be consistent with other programmers.

COMMENT: this is the note programmers make about their code.

Make comments clear and keep them up to date when the code changes.

Comments should be short and right to the point.

1. INDENTATION: this is the space added at the beginning of a line of code. It improves readability and ensures it is executed properly. For example, un-indented print statements would execute the command in isolation.

Another way of writing multi-line comments is by using documentation strings and not assigning them to a variable. Documentation strings, also called docstrings, are strings that are written over multiple lines and are used to document code. To create a documentation string, use triple quotation marks (""" """).

Glossary terms from module 2

Terms and definitions from Course 7, Module 2

Argument (Python): The data brought into a function when it is called

Built-in function: A function that exists within Python and can be called directly

Comment: A note programmers make about the intention behind their code

Function: A section of code that can be reused in a program

Global variable: A variable that is available through the entire program

Indentation: Space added at the beginning of a line of code

Library: A collection of modules that provide code users can access in their programs

Local variable: A variable assigned within a function

Module: A Python file that contains additional functions, variables, classes, and any kind of runnable code

Parameter (Python): An object that is included in a function definition for use in that function

PEP 8 style guide: A resource that provides stylistic guidelines for programmers working in Python

Python Standard Library: An extensive collection of Python code that often comes packaged with Python

Return statement: A Python statement that executes inside a function and sends information back to the function call.

Style guide: A manual that informs the writing, formatting, and design of documents.

User-defined function: A function that programmers design for their specific needs

WORKING WITH STRINGS – STRING OPERATION

String is a data that consists of an ordered sequence of characters. You can enclose strings in double or single quotation marks. A variable is a container for storing variables.

# convert an integer into a string

New\_string = str(123)

Print (type(new\_string))

Performing basic string operations.

The len() function returns the number of elements in an object. Tells us how many characters an object has

# print the length of a string “Hello”

Print (len(“Hello”))

STRING CONCATENATION

This is the process of joining two or more strings together.

For example,

#concatenate two strings

Print(“Hello” = “World”)

We cannot use the minus sign to subtract two strings.

STRING METHOD- this is a function that belongs to a specific data type. This means that we would not use the method used for strings for another data type as this would cause an error.

Methods appear after the string. Two common string methods are the.upper and the .lower methods.

The .upper method returns a copy of the string in all uppercase letters.

For example

#apply upper method to “Hello”

Print(“Hello”.upper())

STRING INDICES AND SLICES

INDEX - this is a number assigned to every element in a sequence that indicates its position.

EVERY CHARACTER IN A STRING IS ASSIGNED A NUMBER AND WE START COUNTING FROM ZERO.

For example IF WE RUN

“Hello” [4] this would return O as the output because 4 is assigned to O in that word.

But what if we want to return more than one character. We can extract a large part of a string by specifying a set of indices. This is called a SLICE.

When taking a slice from a string we specify where the slice starts and stops. For example

“HELLO” [1:4] – in this case while one is outputted, the final one which is 4 isn’t.

HOW TO SEARCH IN A STRING

Using the .index() method is used to find the first occurrence of the input in a string and return its location.

Using this method when there is multiple occurrence of the character we are looking for will return only the first instance of the character occurring in the string. In the word HELLO, it will return the first L and not the second L.

STRINGS ARE IMMUTABLE—this means that they cannot be changed after they are created and assigned a value. Even with index notation, they cannot be changed. This is not the case with lists. They can be altered using the index notation.

LISTS

This is a data type that allow you to store multiple pieces of data in a single variable. For example a list of Ip addresses or another list of applications that are blocked from running on a system.

For example- my\_list[,,,]

LIST CONCATENATION – this is combining two lists into one by placing the elements of the second list directly after the elements of the first list.

Unlike strings, LISTS are mutable. This means that you can change the elements in a list. The following command replaces or changes some element in the list.

my\_list = [1,2,3,4,5]

my\_list [1]=”GH”

There are two ways we can insert and remove elements from lists.

The first is the insert method represented by .insert(). It is used to add an element in a specific position inside a list. This method takes two arguments - the first is the position where we want the element to be in the list and the second is the element we want to add.

For example:

my\_list = [1,2,3,4,5]

my\_list.insert(1,”G”)

ALGORITHM

This is a set of rules that solve a problem. It is a set of steps that takes an input from a problem, uses this input to perform tasks and returns a solution as an output.

The .append() method adds input to the end of a list. For example my\_list.append(4)

List methods.

List methods are functions that are specific to the list data type. These include the .insert() , .remove(), .append() and .index().

.insert()

The .insert() method adds an element in a specific position inside a list. It has two parameters. The first is the index where you will insert the new element, and the second is the element you want to insert.

.remove()

The .remove() method removes the first occurrence of a specific element in a list. It has only one parameter, the element you want to remove.

.append()

The .append() method adds input to the end of a list. Its one parameter is the element you want to add to the end of the list.

Built-in functions

The following built-in functions are commonly used in Python.

str()

Converts the input object to a string

str(10)

Converts the integer 10 to the string "10"

len()

Returns the number of elements in an object

print(len("security"))

Returns and displays 8, the number of characters in the string "security"

String methods

The following methods can be applied to strings in Python.

.upper()

Returns a copy of the string in all uppercase letters

print("Security".upper())

Returns and displays a copy of the string "Security" as "SECURITY"

.lower()

Returns a copy of the string in all lowercase letters

print("Security".lower())

Returns and displays a copy of the string "Security" as "security"

.index()

Finds the first occurrence of the input in a string and returns its location

print("Security".index("c"))

Finds the first occurrence of the character "c" in the string "Security" and

returns and displays its index of 2

List methods

The following methods can be applied to lists in Python.

.insert()

Adds an element in a specific position inside the list

username\_list = ["elarson", "fgarcia", "tshah"]

username\_list.insert(2,"wjaffrey")

Adds the element "wjaffrey" at index 2 to the username\_list; the list

becomes ["elarson", "fgarcia", "wjaffrey", "tshah"]

.remove()

Removes the first occurrence of a specific element inside a list

username\_list = ["elarson", "bmoreno", "wjaffrey", "tshah"]

username\_list.remove("elarson")

Removes the element "elarson" from the username\_list; the list becomes

["fgarcia", "wjaffrey", "tshah"]

.append()

Adds input to the end of a list

username\_list = ["bmoreno", "wjaffrey", "tshah"]

username\_list.append("btang")

Adds the element "btang" to the end of the username\_list; the list

becomes ["fgarcia", "wjaffrey", "tshah", "btang"]

.index()

Finds the first occurrence of an element in a list and returns its index

username\_list = ["bmoreno", "wjaffrey", "tshah", "btang"]

print(username\_list.index("tshah"))

Finds the first occurrence of the element "tshah" in the username\_list and

returns and displays its index of 2

Additional syntax for working with strings and lists

The following syntax is useful when working with strings and lists.

+ (concatenation)

Combines two strings or lists together

device\_id = "IT"+"nwp12"

Combines the string "IT" with the string "nwp12" and assigns the combined

string of "ITnwp12" to the variable device\_id

users = ["elarson", "bmoreno"] + ["tshah", "btang"]

Combines the list ["elarson", "bmoreno"] with the list ["tshah",

"btang"] and assigns the combined list of ["elarson", "bmoreno",

"tshah", "btang"] to the variable users

[] (bracket notation)

Uses indices to extract parts of a string or list

print("h32rb17"[0])

Extracts the character at index 0, which is ("h"), from the string "h32rb17"

print("h32rb17"[0:3])

Extracts the slice [0:3], which is ("h32"), from the string "h32rb17"; the first

index in the slice (0) is included in the slice but the second index in the slice (3)

is excluded

username\_list = ["elarson", "fgarcia", "tshah"]

print(username\_list[2])

Extracts the element at index 2, which is ("tshah"), from the username\_list

Regular expressions

The following re module function and regular expression symbols are useful when

searching for patterns in strings.

re.findall()

Returns a list of matches to a regular expression

import re

re.findall("a53", "a53-32c .E")

Returns a list of matches to the regular expression pattern "a53" in the string

"a53-32c .E"; returns the list ["a53"]

\w

Matches with any alphanumeric character; also matches with the underscore (\_)

import re

re.findall("\w", "a53-32c .E")

Returns a list of matches to the regular expression pattern "\w" in the string

"a53-32c .E"; matches to any alphanumeric character and returns the list

["a", "5", "3", "3", "2", "c", "E"]

.

Matches to all characters, including symbols

import re

re.findall(".", "a53-32c .E")

Returns a list of matches to the regular expression pattern "." in the string

"a53-32c .E"; matches to all characters and returns the list ["a", "5",

"3", "-", "3", "2", "c", " ", ".", "E"]

\d

Matches to all single digits

import re

re.findall("\d", "a53-32c .E")

Returns a list of matches to the regular expression pattern "\d" in the string

"a53-32c .E"; matches to all single digits and returns the list ["5", "3",

"3", "2"]

\s

Matches to all single spaces

import re

re.findall("\d", "a53-32c .E")

Returns a list of matches to the regular expression pattern "\s" in the string

"a53-32c .E"; matches to all single spaces and returns the list [" "]

\.

Matches to the period character

import re

re.findall("\.", "a53-32c .E")

Returns a list of matches to the regular expression pattern "\." in the string

"a53-32c .E"; matches to all instances of the period character and returns

the list ["."]

+

Represents one or more occurrences of a specific character

import re

re.findall("\w+", "a53-32c .E")

Returns a list of matches to the regular expression pattern "\w+" in the string

"a53-32c .E"; matches to one or more occurrences of any alphanumeric

character and returns the list ["a53", "32c", "E"]

\*

Represents, zero, one or more occurrences of a specific character

import re

re.findall("\w\*", "a53-32c .E")

Returns a list of matches to the regular expression pattern "\w\*" in the string

"a53-32c .E"; matches to one or more occurrences of any alphanumeric

character and returns the list ["a53", " ", "32c", " ", " ", "E"]

{ }

Represents a specified number of occurrences of a specific character; the number is

specified within the curly brackets

import re

re.findall("\w{3}", "a53-32c .E")

Returns a list of matches to the regular expression pattern "\w{3}" in the string

"a53-32c .E"; matches to exactly three occurrences of any alphanumeric

character and returns the list ["a53","32c"]

ACCESSING A TEXT FILE IN PYTHON

All we need is the txt file, its location and the right python key words.

We begin by typing the with statement. The WITH keyword handles errors and manages external resources.

Using the WITH keyword tells Python to automatically close the file after reading it. For example,

with open(“login\_attempts.txt” “r”) as file:

with - tells python to close the file once it finishes reading from it.

open- tells python to open the file

file\_name = here the name of the file or a link to it on the internet is provided.

“r” - this tells python that you only want to read the file. If it were to write to the file, the r would be replaced with a w.

file- it contains the variable information as long as we insert the with statement.

: - the colon must end the with statement.

The .read() method converts files to strings.

The .write() method is used to create a new file or change the value in an existing file. But you have to indicate what needs to be changed in the subsequent lines.

PARSING

Parsing is the process of converting data into a more readable format.

The .split() method converts a string into a list. It does this through specified characters. But if no argument is passed, it separates the strings in the list using white spaces.

Note: Another way to separate elements when using the .join() method is to use "\n", which is the newline character. The "\n" character indicates to separate the elements by placing them on new lines.

DEBUGGING

This is the practice of identifying and fixing errors in code.

Types of errors

1. Syntax – invalid usage of the Python language. For example when you forget to add a colon. They are easy to fix because you can find where the error occurred. You get the INVALID SYNTAX error message.
2. Logic - they may not cause error messages but provide unintended results. It could be writing incorrect text within a print statement.

A logic error can be serious as in the case of excluding messages or alerts that ought to have been escalated.

To diagnose it, we have to use print statements throughout the code. It will describe the location in the code. The idea is to use the print statement to identify which section of the code that functions properly or not.

Another way to identify logic errors is to use a debugger. it allows you insert break points in your code. It allows you to segment your code in sections and run one section at a time.

1. EXCEPTIONS - this happens when the program doesn’t know how to execute code even though there are no problems with the syntax. They might happen for example when something is impossible in mathematics, like asking something to be divided by zero. They might also happen when you ask python to access index values that do not exist or when Python does not recognise variable or function names. They may occur when you use an invalid data type. A debugger can also be used to figure out a potential source of error.

Glossary terms from module 4

Terms and definitions from Course 7, Module 4

Automation: The use of technology to reduce human and manual effort to perform common and repetitive tasks

Conditional statement: A statement that evaluates code to determine if it meets a specified set of conditions

Debugger: A software tool that helps to locate the source of an error and assess its causes

Debugging: The practice of identifying and fixing errors in code

Exception: An error that involves code that cannot be executed even though it is syntactically correct

File path: The location of a file or directory

Function: A section of code that can be reused in a program

Integrated development environment (IDE): A software application for writing code that provides editing assistance and error correction tools

Iterative statement: Code that repeatedly executes a set of instructions

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

Logic error: An error that results when the logic used in code produces unintended results

Parsing: The process of converting data into a more readable format

Syntax error: An error that involves invalid usage of a programming language.

Variable: A container that stores data

INTRODUCTION TO COURSE 8 – PUT IT TO WORK

HAVING A SECURITY MINDSET:

You have to rec what you are defending but who you are defending against. You have to know the assets you are defending and the types of threats you are defending against.

A security mindset is the ability to evaluate risk and constantly seek out and identify the potential or actual breach of a system, application, or data.

Using our sec mindset, will help us stay up to date with the kind of attacks that is happening. Learn about the recent trends. Having a sec mindset helps analyst protect and defend against the constant pressure from attackers.

Entry level analyst can protect a wide range of assets.

Having a strong sec mindset can set you apart from other candidates from others. You can also reference it in future job interviews.

DATA AND ASSET CLASSIFICATION

Classifying for safety

Security professionals classify data types to help them properly protect an organization from cyber attacks that negatively impact business operations. Here is a review of the most common data types:

Public data

Private data

Sensitive data

Confidential data

Public data

This data classification does not need extra security protections. Public data is already accessible to the public and poses a minimal risk to the organization if viewed or shared by others. Although this data is open to the public, it still needs to be protected from security attacks. Examples of public data include press releases, job descriptions, and marketing materials.

Private data

This data classification type has a higher security level. Private data is information that should be kept from the public. If an individual gains unauthorized access to private data, that event has the potential to pose a serious risk to an organization.

Examples of private data can include company email addresses, employee identification numbers, and an organization’s research data.

Sensitive data

This information must be protected from everyone who does not have authorized access. Unauthorized access to sensitive data can cause significant damage to an organization’s finances and reputation.

Sensitive data includes personally identifiable information (PII), sensitive personally identifiable information (SPII), and protected health information (PHI). Examples of these types of sensitive data are banking account numbers, usernames and passwords, social security numbers (which U.S. citizens use to report their wages to the government), passwords, passport numbers, and medical information.

Confidential data

This data classification type is important for an organization’s ongoing business operations. Confidential data often has limits on the number of people who have access to it. Access to confidential data sometimes involves the signing of non-disclosure agreements (NDAs)— legal contracts that bind two or more parties to protect information—to further protect the confidentiality of the data.

Examples of confidential data include proprietary information such as trade secrets, financial records, and sensitive government data.

Asset classification

Asset classification means labeling assets based on sensitivity and importance to an organization. The classification of an organization's assets ranges from low- to high-level.

Public data is a low-level asset. It is readily available to the public and will not have a negative impact on an organization if compromised. Sensitive data and confidential data are high-level assets. They can have a significantly negative impact on an organization if leaked publicly. That negative impact can lead to the loss of a company’s competitive edge, reputation, and customer trust. A company’s website address is an example of a low-level asset. An internal email from that company discussing trade secrets is an example of a high-level asset.

DETECT AND PROTECT WITHOUT NEGLECT:

It is important to remember that the assets and data that you protect affect multiple levels of your organisation.

One of the most important considerations for a company is to protect customer data which includes credit card details, SSN, emails, usernames and passwords and etc. It is important to remember this when engaged in cybersec.

NB: understanding the importance of the data is important. It is also important to hand the sensitive data with care.

WHEN A SECURITY EVENT RESULTS IN A DATA BREACH, IT IS CATEGORISED AS A SECURITY INCIDENT. but if it is resolved without it resulting in a breach, it is not considered an incident.

It is better to be safe when taking a job in a security profession. For example, something small like an employee installing an app on their work device should be escalated to a supervisor. Cos this might be a potential vulnerability.

A bigger issue is noticing that a log may have malicious code executed in it. It can disrupt the operation of the company.

NO ISSUE IS TOO SMALL OR TOO BIG. ERR ON THE SIDE OF CAUTION!

DISASTER RECOVERY AND BUSINESS CONTINUITY.

Business continuity plan

The impact of successful security attacks on an organization can be significant. Loss of profits and customers are two possible outcomes that organizations never want to happen. A business continuity plan is a document that outlines the procedures to sustain business operations during and after a significant disruption. It is created alongside a disaster recovery plan to minimize the damage of a successful security attack. Here are four essential steps for business continuity plans:

Conduct a business impact analysis. The business impact analysis step focuses on the possible effects a disruption of business functions can have on an organization.

Identify, document, and implement steps to recover critical business functions and processes. This step helps the business continuity team create actionable steps toward responding to a security event.

Organize a business continuity team. This step brings various members of the organization together to help execute the business continuity plan, if it is needed. The members of this team are typically from the cybersecurity, IT, HR, communications, and operations departments.

Conduct training for the business continuity team. The team considers different risk scenarios and prepares for security threats during these training exercises.

Disaster recovery plan

A disaster recovery plan allows an organization’s security team to outline the steps needed to minimize the impact of a security incident, such as a successful ransomware attack that has stopped the manufacturing team from retrieving certain data. It also helps the security team resolve the security threat. A disaster recovery plan is typically created alongside a business continuity plan. Steps to create a disaster recovery plan should include:

Implementing recovery strategies to restore software

Implementing recovery strategies to restore hardware functionality

Identifying applications and data that might be impacted after a security incident has taken place.

Juliana's story: Asset protection

Meet Juliana Soto, who recently completed an online cybersecurity certificate program and was hired as a cybersecurity analyst for Right-On-Time Payment Solutions, a fictional payment processing company allowing individuals to transfer money to friends and family. Right-On-Time also allows companies to accept payments from customers or organizations.

In this reading, you will begin a three-part journey that follows Juliana as she takes on new roles and responsibilities within the cybersecurity team of her new company.

Juliana decides that one of her first objectives is to gain a better understanding of the most important assets to the company by reviewing various company reading materials that will help her learn what is most valuable to them. On her first day, she is given reading materials to help her familiarize herself with the company. She learns that customers must create unique usernames and passwords and provide their full name or company name to sign up for the service as an individual. Business customers can also sign up for the service if they provide their employee identification number (EIN). Finally, customers must enter their bank account information or debit card number for payments to be accepted.

Juliana discovers that this company handles a lot of personally identifiable information (PII) from its customers. This kind of information is considered sensitive data. Unauthorized access to it can lead to significant damage to the organization’s finances, its customers, and its reputation. Juliana realizes that the most important asset to this company is customer data.

After finishing the required onboarding materials, she decides to put together an information lifecycle strategy. She learned about this when completing her online cybersecurity certificate program.

Information lifecycle strategy

Juliana recalls the following steps of the information lifecycle:

The first step in the information lifecycle is to identify the important assets to the company, including sensitive customer information such as PII, financial information, social security numbers, and EINs.

The second step is to assess the security measures in place to protect the identified assets and review the company’s information security policies. There are different components to this step, ranging from vulnerability scanning to reviewing processes and procedures that are already in place. Juliana is new to the company and might not be ready to conduct vulnerability scans.

The third step of the information lifecycle is to protect the identified assets of the organization. Once again, this is only Juliana’s first day on the job. She asks her supervisor if she can observe a more senior security analyst for a day. This will give her the opportunity to learn how the security team monitors the company’s systems and network.

The last step of the security lifecycle is to monitor the security processes that have been implemented to protect the organization’s assets. She contacts her supervisor and gives them a detailed report of what she has learned on her first day. She requests to finish her day by monitoring a few of the systems that are in place. Her supervisor is impressed with her initiative and prepares Juliana to monitor the security systems. What a great first day for Juliana!

Glossary terms from module 1

Terms and definitions from Course 8, Module 1

Business continuity plan (BCP): A document that outlines the procedures to sustain business operations during and after a significant disruption

Confidential data: Data that often has limits on the number of people who have access to it

Disaster recovery plan: A plan that allows an organization’s security team to outline the steps needed to minimize the impact of a security incident

Private data: Information that should be kept from the public

Public data: Data that is already accessible to the public and poses a minimal risk to the organization if viewed or shared by others

Security mindset: The ability to evaluate risk and constantly seek out and identify the potential or actual breach of a system, application, or data

Sensitive data: A type of data that includes personally identifiable information (PII), sensitive personally identifiable information (SPII), and protected health information (PHI)

Protecting the data and assets of an organization is the primary goal of a security team.

WHAT IS INCIDENT ESCALATION

This is the process of identifying a potential security incident, triaging it and handing it off to a more experienced team member.

ESSENTIAL SKILLS TO ESCALATE SECUTIY INCIDENTS

1. ATTENTION TO DETAIL – you can identify if something does not seem right in a network.
2. ABILITY TO FOLLOW AN ORGANISATION’S ESCALATION GUIDELINES OR PROCESSES. – this will help you escalate it properly.

Escalate with a purpose.

The escalation process

Every company has different protocols and procedures, including unique escalation policies. These policies detail who should be notified when a security alert is received and who should be contacted if the first responder is not available. The policy will also determine how someone should specifically escalate an incident, whether it’s via the IT desk, an incident management tool, or direct communication between security team members.

Prepare to escalate through security recognition. Incident classification types.

1. Malware infection - this is a case where a malicious software designed to disrupt a system infiltrates an organisation’s computers or network. They can come in various forms. One is a phishing attempt, ransomeware attack.

Malwares can cause the computer to run at unusually low speeds. Attackers can prevent information from viewing critical data unless they pay. Sometimes it is not guaranteed to gain access to the data even.

1. Unauthorised access - this is when an individual gains digital or physical access to a system or application without permission. Eg brute force attack is a trial and error method.

ALL UNAUTHORISED ACCESS MUST BE ESCALATED!

1. Improper usage - this happens when an employee violates the organisation’s acceptable use policies. It is complicated for example when an employee attempts to use company licenses for personal use or even trying to access a co-worker’s data.

Because it is sometimes difficult to determine if improper usage is accidental or intentional, IT MUST ALWAYS BE ESCALATED TO A SUPERVISOR!

REMEMBER it is important to escalate a suspicious activity even you are not very sure of the activity. This is called incident criticality. You can escalate with a medium level of criticality if you don’t have enough information to tag the incident or determine the amount of damage done to the org. a more experienced sec analyst can sort it out.

What is the best way to determine the urgency of a security incident?

It depends on the asset or assets the incident affects.

The impact of an attacker gaining unauthorised access to manufacturing application or PII is far greater than a forgotten password. So when you receive an alert informing you that something Is wrong with any of those sensitive assets, it is important to escalate them with high criticality.

WHEN AND HOW TO ESCALATE A SECURITY INCIDENT

WHAT ARE THE ACTUAL STEPS TO ACTUALLY ESCALATE AN INCIDENT? DEPENDS ON THE ORGANISATION.

GENERAL GUIDELINES.

ESCALATION POLICY - This is a set of actions that outline who should be notified when an incident alert occurs and how that incident should be handled. #

What if:

Your supervisor is out of office? You can escalate to someone else.

It is important to bookmark the escalation policy just in case the person you are supposed to escalate to is out of the office.

NB: attention to detail can make the difference between escalating an incident to the right or wrong person. It can also help you prioritise which incidents need to be escalated with more or less urgency.

ESCALATION TIMING

It is very important that I am confident in my decisions and bold when asking questions. I must be intentional about learning the organisation’s escalation policy.

Ask questions when necessary. It shows commitment to constantly learning the right way to do my job.

It is important that I can classify and proritise specific incident types especially as they relate to different assets. For example, an incident that affects assets that are essential to business operations must always take priority over incidents that do not directly impact business operations. For example, an incident where unauthorised access has been grained to a manufacturing application should take priority over an incident where malware has infected a legacy system that does not impact business operations.

Escalation tips:

1. Know the escalation policy of my organisation
2. Follow the policy at all times.
3. Ask questions.

STAKEHOLDERS, WHO ARE THEY AND WHY ARE THEY IMPORTANT.

This is an individual or group that has interest in the decisions or activities or an organisation.

1. Risk managers - they identify risks, manage the response to security incidents, notify the legal department and inform the organisation’s public relations team.
2. Chief executive officer – this is the highest ranking person in the org. they are responsible for the financial and managerial decisions in a company, manage operations and report to shareholders.
3. Chief financer officer – managing financial operations, cost of tools and strategies.
4. Chief information security officer – develop the orgs security architecture, conducting risk analysis and system audits, creating business security continuity plans.
5. Operation managers – they oversee security professions, work directly with analysts, (first line of defence), they are also responsible fo the daily maintenance of operations.

CLEAR AND CONCISE COMMUNICATION

Before communicating to a stakeholder, it is important to be mindful of what I communicate and who I am communicating to. Different stakeholders need to be informed of different issues.

It is important to have all the details on hand before communicating with stakeholders. Partially because they are very busy people. Comms should be precise, avoid unnecessary technical terms with a clear purpose.

They don’t have to guess the email o why it matters to them.

We can ask the immediate manager what the stakeholder needs to know.

Questions?

What data is the most important to be protected on a daily basis; what tools are the most effective.

EFFECTIVE COMMUNICATION here means relaying only what is important to stakeholders. My role is to help them obtain the information they need to make decisions.

Building blocks of cybersecurity communications.

When telling stakeholders about a security challenge, you must follow the following steps

* What the challenge is
* How it impacts the organisation
* And some proposed solutions.

Example - found malicious code exe

Steps: you need to communicate, what do you do?

Detail the issue – malicious code exe; next is to refer to the incidence playbook and mention the suggestion guidance about malicious codes, the final piece of the story is to provide a solution to the issue.

The incident can be communicated through:

* Email
* Document
* Visual representation - they are used to convey key details in the form of graphs, charts, videos or other visual effects. Allows them to see a pictorial representation of what is displayed.
* Incident management or ticketing systems

Communicate effectively with stakeholders

You previously learned about security stakeholders and their significance in an organization. In this reading, you’ll learn the importance of clearly communicating to stakeholders to ensure they have a thorough understanding of the information you’re sharing and why it’s meaningful to the organization.

Get to the point

Security stakeholders have roles and responsibilities that are time sensitive and impact the business. It’s important that any communications they receive, and the actions they need to take, are clear. To get to the point in your communications, ask yourself:

What do I want this person to know?

Why is it important for them to know it?

When do they need to take action?

How do I explain the situation in a nontechnical manner?

Follow the protocols

When you first join a security team, you’ll want to learn about the different protocols and procedures in place for communicating with stakeholders and other members of the organization. It’s important to make sure you know what applications and forms of communications are acceptable before you begin communicating with stakeholders, such as in-person meetings, video-conferencing, emails, or company chat applications.

Communicate with impact

You previously learned about the different stakeholders within an organization and what specific areas they’re focused on. When you first begin your career in the cybersecurity field, you're more likely to interact with lower-level stakeholders, like operations managers or security risk managers, who are interested in the day-to-day operations, such as logging. Senior-level stakeholders might be more interested in the underlying risks, such as the potential financial burden of a security incident—as opposed to the details around logs.

When you communicate with an operations manager, make sure you address relevant information that relates to their daily responsibilities, such as anomalies in data logs that you are escalating. Concentrating on a manager’s daily responsibilities will help you communicate the need-to-know information to that individual.

Communication methods

Your method of communication will vary, depending on the type of information you’re sharing. Knowing which communication channels are appropriate for different scenarios is a great skill to help you communicate effectively with stakeholders. Here are a few ways you might choose to communicate:

Instant messaging

Emailing

Video calling

Phone calls

Sharing a spreadsheet of data

Sharing a slideshow presentation

f your message is straightforward, an instant message or phone call might be the route to take. If you have to describe a complex situation with multiple layers, an email or in-person meeting might be the better option. If you’re providing a lot of data and numbers, sharing a graph might be the best solution. Each situation helps you determine the best means of communication.

VISUAL COMMUNICATION USING A DASHBOARD

The use of visuals to tell a security story can help you communicate impactful data and metrics. Charts and graphs are particularly helpful for this. They can be used to compare data points or show small parts of a larger issue. Using relevant and detailed graphics can help you develop the story you want to tell stakeholders, so they can make decisions that would help protect the organization.

Be mindful of when you are communicating with emails. Make sure you are sending the right person the email. Sometimes, when the issue is quite urgent, it might be best to send a simple instant message of placing a direct call. Stakeholders might not respond quickly to an urgent issue, so just ring the stakeholder.

It's important to stand out in the security profession, especially if you don't have previous experience in the industry. Visual representations, emails, and phone calls are great ways to showcase your written and verbal communication skills. Following up to someone who does not respond to your email in time shows initiative.

When to use visual communication

Security is often a team effort. Everyone must work together to ensure an organization is properly protected from bad actors. Knowing how to communicate with your colleagues is a big part of the team-focused aspect.

Sometimes it’s enough to send a simple email update. Other times you might want to include a document attachment that further elaborates on a specific topic. A simple phone call can also be valuable because it allows you to quickly communicate the necessary information without having to wait for a response to an email or message. Other times, the best way to communicate is through visuals.

For example, consider a situation where your supervisor has asked you to provide them with results from a recent internal audit of five different departments within the organization. The audit gathered data showing how many phishing emails each department clicked over the last five months. This is an ideal opportunity to tell this story using visualization tools. Instead of sending an email that simply describes what the findings are, a graph or chart will clearly illustrate those findings, making them easier for the stakeholder to understand quickly and easily.

MODULE 4

HELPFUL CYBERSECURITY RESOURCES

1. OWASP TOP 10 - a globally standard awareness document that lists the top 10 most critical security risks to web applications. Renewed every 3 to 4 years.

Security websites and blogs include

* CSO online – news and analysis on various security topics. Review the publication every now and then.
* Krebs on Security – covers security news and investigations
* Dark Reading – provides information about various security topics, many many many. provides information on analytics and application security, mobile and cloud security, and the Internet of Things (IoT)

HOW TO STAY ENGAGED WITH THE CYBERSECURITY COMMUNITY

Security organizations and conferences

Attending security conferences and joining organizations gives you the opportunity to gain knowledge from seasoned professionals who are constantly seeking out new ways to improve on their security strategies and techniques.

Find the right organization.

What security organization should you join? This question depends on your specific interest in security. Are you someone who wants to focus on reacting to security incidents or preventing them from happening? Are you interested in forensic security or data logging? Do you have aspirations of being a CISO one day? It’s important to have a clear understanding of what your interests are before you narrow down your search for a cybersecurity organization or conference.

Begin the search.

Once you understand what your interests are, do a web search for organizations or conferences in your area. For example, you can type in “incident response cybersecurity conferences in my area.” This search will give you a list of cybersecurity conferences focused on incident response. If you’re interested in forensic security, you can type “forensic security organizations in my area” or a similar phrase into your web search engine. No matter what your interests are, you can do a web search online to find a cybersecurity organization or conference focused on that area.

Use social media

Social media is another great way to find cybersecurity organizations or conferences.

LinkedIn

®, for example, is a social media platform that connects business professionals with one another. You can use LinkedIn® to find security groups or organizations to join. In the LinkedIn® search bar, you can try search queries such as:

“Incident response cybersecurity groups”

“Organizations for cybersecurity analysts”

Be aware of social engineering.

While social media is a good way to connect with other professionals in the security industry, it’s also important to be mindful that hackers use social media to trick users into giving up private information. You've previously learned that social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. To protect yourself from social engineering when using social media to find resources, always remember not to click on unexpected links or attachments sent from unfamiliar users on social media.

Mailing lists for security

Another great way to stay connected with the security industry is to sign up for different cybersecurity mailing lists. These mailing lists send out information periodically on various security topics. The Cybersecurity & Infrastructure Security Agency (CISA) offers two cybersecurity mailing lists for you to join:

A list focused on security threat information, best practices for cybersecurity, and analysis from CISA’s domestic and international security partners.

BUILD YOUR CYBERSECURITY NETWORK.

Social media is a great way to connect with other security professionals in the industry.

NB: it is important I be mindful of the information I share on my social media page or with the people I communicate with.

WAYS TO EFFECTIVELY ESTABLISH OR ADVANCE SECURITY CAREER

* Read the posts of leaders in the security industry. CISO’s for example.

CISOs, how? Research them on the internet, use LinkedIn to find them and connect with them.

* Specifically search for the following: cyber security analysts or people who talk about cybersecurity. The use social media filters to filter people and people who talk about what you’re interested in.

Send a connection request with a note “ Hi I’d like to connect to learn more about why you became interested in security and your experiences.”

* Joining different security associations. Search for “cybersecurity industry associations”

WHEN CONNECTING WITH OTHER SECURITY PROFESSIONALS ON Linkedin, it is very important to remember the following:

* Use a conversational tone.
* Provide a clear reason for wanting to connect.
* A screenshot of a white page

  Description automatically generatedAvoid spelling and grammatical errors.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Possible Entry Level Security Roles

1. Security Analyst

- monitoring networks

- Monitoring networks - Using SIEM tools and SOAR

- researching IT security trends

2. Information Security Analyst

- Creating plans - Controls and Frameworks used to develop plans and procedures.

- Implementing Security measures - using SIEMs and Packet sniffers to identify risks.

3. Security Operations Analyst role

- Ensuring security incidents are handled rapidly and efficiently – Security Playbooks and how they are unique

- Following established policies and procedure. - being able to follow the processes and guidelines in Playbooks.

JOB SITES

* ZIP recruiter.
* Indeed
* Monster Jobs

# IMPORTANT TIPS

1. DO YOUR RESEARCH BEFORE APPLYING TO ANY POSITION
2. GATHER PLENTY OF INFORMATION ANOUT THE COMPANY, THE JOB AS WELL AS ANY REQUIRED SKILLS,
3. KNOW EXACTLY WHAT THE EMPLOYER IS LOOKING FOR. ALIGN YOUR OWN VALUES AND PASSIONS TO THE ORGANISATION’S MISSION AND VISION.
4. CREATE A CATCHY RESUME.

WHAT IS A CAREER IDENTITY

This is who you are and what you have to offer professionally and guide you to navigate towards your goals.

It is the unique value you bring to the workforce based on who you are and what you have to offer, now and in the future.

It is informed by all your life and work experiences, and shaped by your strengths, motivations, and values.

It is something you cultivate based on your direction and goals.

It is IMPORTANT because the more you know about who you are and what makes you thrive and where you want to go the better equipped you are to choose a path that aligns with your strengths, values and goals. People would have a better understanding of what you have to offer.

NO MATTER WHAT YOUR EXPERIENCES ARE, WE HAVE VALUE TO OFFER.

REALISE WHAT WORKS FOR YOU, WHAT YOU LOVE DOING. For example, distilling complex ideas into simple language that would be understood by customers.

NB: one of the best ways to explore your career identify is to write your own career identity statement.

Key components of a CIS

Strengths – they are tasks and activities you do well. Skills knowledge and talents you have gained throughout your life and work experiences. Maybe you’re very detailed oriented, building relationships, repairing cars or patience, empathy, problem solving.

A strength is an activity that strengthens you. For something to be a strength, you have to be good at it and it has to make you feel stronger.

Motivations – motivations stem from your passion and purpose. Knowing what fuels you is important because it keeps you going. I am passionate about teaching language in general.

Values - they are what is most important to you, they guide your approach to decision making, developing relationships, overcoming challenges. For example, integrity, kindness, Honesty, and responsibility, efficiency and service to others. How can I make something more efficient?

BUILDING MY CAREER IDENTITY

ASSESSING MY STRENGTHS, MOTIVATION AND VALUES

1. What skills, knowledge and talents set me apart?

Effective verbal/ written communication, Empathy, leadership, responsibility, resilience, relationship building

1. What fuels and motivates me most?

A desire to help others, happiness, and fulfilment in what I do, being able to afford my needs and those of others.

1. What values guides me - integrity, Honesty, transparency, Love

A screenshot of a white paper

Description automatically generated

Interviewing your peers will help you find out your values.

How would you describe me to someone else?

What stands out about me?

Do I inspire you?

CAREER IDENTITY STATEMENT

Three or four sentences that go beyond mentioning your skills or qualifications. You want to reveal your passion and purpose.

“I am a…roles…. With …years… of experience doing…accomplishment…. My greatest strength is…strength…, and I have a talent for …strength… I am passionate about …motivation…, and I value …value…”

“I am a **content strategist** and **product marketer** with **over ten years** of helping **businesses use new technologies to drive success.**

My greatest strength is **collaborating and driving efficiencies across teams**, and I have a talent for **crafting stories** and **creating marketing programs to successfully launch technology products.**

I am passionate about **empowering brands to find and use solutions that work for them** and **helping builders of new technologies to develop even better, more effective products.**

And most importantly, I value **having fun** and **being collaborative**, **inclusive** and **authentic while I do it**!

**A white text with blue text

Description automatically generated**

What to add to my resume

1. Add everything I have learnt from the programme such as

* Programming languages
* Linux command line
* Security mindset
* Frameworks and controls
* Familiarity with SIEM tools and Packet sniffers.

1. Transferrable and Technical skills

* Detail oriented
* Collaborative
* Written and verbal communication skills

HOW TO STRUCTURE THE RESUME

Name

Job title

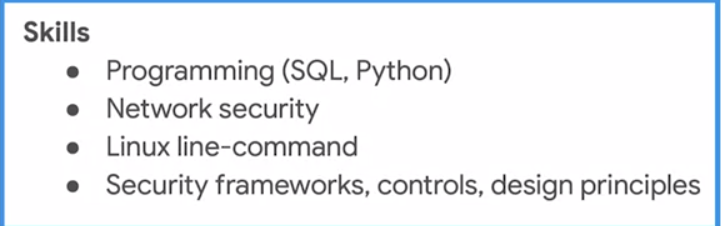
Phone number.

Email address.

Summary - this part should be brief, just one or two sentences, related to your strengths and relevant skills. Make sure it includes specific words from the responsibility section of the job description.

For example:

*I am a motivated security analyst seeking an entry level cybersecurity position to apply my skills in network security, security policy and organisational risk management.*

Skills section 

Work experience - list your work history. Provide a list of the skills and responsibilities you performed. It is good to begin with a very and quantifiable details of an accomplishment.

For example: collaborated with a team of six to develop training for more than 25 company employees.

* Try to highlight the security and technology related skills and knowledge you have based on previous experience on previous jobs and this security programme.

Education and certifications - begin with the most recent including certifications, trade school, online course or college experiences.

RESUME TIPS

* Make sure there are no grammatical errors.
* Two pages long
* 10 years or less of work experience.

You can use resume templates online. Replace all of the previous text with your qualifications.

Cover Letter tips.

A resume tells the facts, what you have done, but a cover letter tells who you are. Why cyber security, why the opportunity, have a reason for joining. Something that has affected you that makes you want to join cybersecurity.

How long should your cover letter be and structure?

1. Talk about yourself, family and hobbies.
2. Cut to what makes you unique, different from other applicants, how do you overcome adversity and how do you plan to do so, what does this job mean to you, soft skills you can bring to the role.
3. Since you are changing your career, in your cover letter you have to tell the employer why you are making this change and explan it in the most convincing way. Why does it excite.
4. Don’t standardise the cover letter and fire it off. Tailor it around the company’s mission, their purpose and their products and put that in your cover letter.
5. Capture their attention quickly. What is it about you that should be interesting. Be bold, but be loud! Be EXPRESSIVE!!!

THE INTERVIEW PROCESS

1. It begins with a pre-screening phone call - this is a 50 minute phone call with the hiring manager. The purpose is to verify you are who your resume says you are and you meet the minimum requirements for the role.

Following this, it might be an interview. Or one to one interview.

PREPARING FOR THE INTERVIEW

1. Review the job description and your resume.

2. Practice speaking about the skills and experiences the employer is looking for.

3. Consider practicing with a friend.

4. Dress professionally and feel comfortable.

5. Take a few deep breaths

6. Remind yourself of all the preparation you’ve done

7. Test your video and audio settings.

Interviews usually include two parts:

1. A background interview - include questions about education, work experience, skills, and abilities. Expect some unrelated personal questions.
2. A technical interview - ask you questions about technical skills related to the role. Expect to be asked scenario-based questions or explanation of technical concepts.

ANSWER THE QUESTIONS CONFIDENTLY AND CONCISELY.

It’s okay to say you don’t know the answer to a question or you need a moment to think about the question.

EMPLOYERS RESPECT HONESTY.

NB: don’t forget to ask questions that will help you decide if the team and the company culture are a good match for you.

EXAMPLES OF QUESTIONS I CAN ASK THE RECRUITER

1. What is the work culture like at the company?

2. What will my average day be like in this role?

SEND A THANK YOU EMAIL TO THE RECRUITER EXPRESSING GRATITUDE FOR THEIR TIME AND BRIEFLY RESTATE WHY YOU WOULD BE A GOOD FIT FOR THE POSITION.

TECHNICAL INTERVIEW TIPS

1. Show you understand the fundamentals and can explain it to the interviewer.

2. Splunk, Wireshark, understand their internals. If they didn’t exist, how would you solve a problem (TCP dump).

3. Network Security, Web application security knowledge, Operating system internals, Understanding and mastering security protocols.

4. Practice answering open-ended questions which can sometimes be difficult and ambiguous by design. They might be complex too. Begin by asking the interviewer for clarification to help you narrow down the focus of the question and lower the scope of the problem.

5. Organise your answers using the Star Method.

S -

T -

A -

R –

6. It is fine if you don’t know the answer to the question. But don’t LIE.

7. The ideal candidate is someone who loves to learn, someone who is honest, can manage ambiguity and complexity. Someone who runs towards a problem and not away from it. Leading and Mentoring others.

8. it is okay to be nervous during technical interviews. It means you care about the process.

9. Trust yourself, Trust your gut, don’t be afraid to Fail, But give it your most powerful shot!

Possible Technical Interview Questions

1. What is the TCP/IP model?

2. What is the OSI model?

3. What are SIEM tools and what are they used for?

CONDUCTING PRE-INTERVIEW RESEARCH

* RESEARCH THE ORGANISATION – they want to know you are a good match for the team and you value what is important to the company.
* You also have to decide if they match your values. SO make sure to know their vision, and mission. Understand their core values and company culture.
* Think about why these values are important to you and practice how to communicate them to the employers.
* Consider what sets you apart from other candidates. What about your skills, experience and work ethic make you a best match for this position.
* How do your goals align with the goals of the organisation? Highlight things that make you the best candidate for the role.
* Think about the employers perspective. They may have productivity or compliance goals or the team might be growing because they are expanding.
* Know what they are seeking for in a candidate then prepare yourself to state directly now you can meet their needs.
* Since they may have some reservations about your lack of experience, be prepared to address that by speaking about your strong work ethic.
* This includes ability to learn quickly based on feedback or ability to learn from others.
* Talk about your security mindset or problem solving skills you have developed from personal life, work or education.
* Talk about how you can add value to the team. This is essential.
* Write down questions about the organisation’s past accomplishments and future goals. This shows you have done your research and care about the organisation.

HOW TO BUILD RAPPORT WITH INTERVIEWERS.

Rapport is a friendly relationship in which the people involved understand each other’s ideas and communicate well with each other.

How do you build rapport?

1. Be professional but be polite and friendly, show appreciation for the interview opportunity.

2. On the phone interview, use a friendly and conversational tone of voice, try smiling while you talk. Smiling while you talk can make you sound friendlier.

3. During face-to-face interview, you can talk in a way that feels natural to you. That can mean saying “Hello, nice to meet you”. You can ask about their weekend or how their day is going.

4. Make eye contact while asking the questions, during in person interviews.

5. Look directly into the camera during video interviews. This shows them that you are engaged in the conversation.

6. These are some questions you can ask: What is the biggest challenge I will face coming into this role and how would I be expected to meet that challenge? What would you say is the best part about working for this company? What is the typical day like for an analyst? What is the potential for growth in this role.

7. Send a follow-up email a day or two thanking the interviewer for the opportunity to have had an interview with them. It is nice to mention something specific from the interview in the email. IT shows you were actively engaged in the conversation.

8. Sending a follow-up email reminds the interviewer about your discussion and sets you apart from others they are interviewing.

USING STRATEGIES TO ANSWER INTERVIEW QUESTIONS

1. Carefully consider each question before responding. STAR

The STAR method is used to answer behavioural and situational interview questions. Helps you understand each question and provide a thoughtful response.

S – SITUATION

T – TASK

A – ACTION

T – RESULT

The star method is used to answer open ended questions like:

Tell me about a time when you encountered a challenged in a job?

Situation

Two people needed to stay home because of an illness, and I was the only person left to attend to customers.

Task

I needed to answer phone calls from customers, while assisting shoppers in the store.

Action

I came up with a strategy that allowed me to assist customers as they entered the store while also ensuring that customers who called were helped or politely placed on hold until I was able to address their needs.

Result

I managed the in-store operations for the day without many mistakes and my manager complimented me during the next team meeting.

Answer questions with confidence:

You can do this by admitting that you don’t know something.

If they ask you to discuss a skill you don’t have, it is OKAY to admit that you don’t have it yet! HOWEVER

The trick is to confidently mention that you are quicl learner and eager to develop that skill. Treat it as an opportunity to emphasize your ability to learn and adapt on the job.

Another way to show confidence is to take the time to understand a question in order to provide the best solution possible. Don’t be afraid to ask them for some time to analyse the question. It shows you are interested in finding the right solution or answer to the problem.

Interview Tips

Break down the question into technical preparation and non-technical preparation.

Technical preparation

* Build up on networking fundamentals, information security fundamentals.
* Make sure you ask clarifying questions to get to the root of the problem and what the interviewer wants from you.
* Don’t dive into the problem. If you don’t know something, don’t be afraid to say, I don’t know. But inform them how you intend to become familiar with the question or the concept.

Non-technical

Practice with a friend and be kind to yourself. Bring your whole self to the interview. Showcase how you’ll work with the team. Bring up examples you have done with others and how you performed in the projects. Highlight your soft skills as those are very crucial to interviewers.

The main thing for new people is to show curiosity. People who are very driven to learn more about the field. Asking the right questions about figuring something out.

Don’t be afraid to apply even if you don’t meet the minimum qualifications.

Elevator Pitch

A brief summary of your experience skills and backgrounds. It must be short enough to say in 60 seconds or less.

You demonstrate who you are to potential employers. You can use them in networking conferences and on LinkedIn.

It must be:

* Short
* Persuasive
* Who you are
* Why you care
* Qualifications
* Skills related to cybersecurity - critical thinking, problem solving, building relationships. Mention technical skills you’ve learnt such as python, linux, SIEM.

AVOID

* RAMBLING OR SHARING IRRELEVANT DETAILS.
* DON’T SOUND INGENUINE RO ROBOTIC
* SPEAK NATURALLY
* SPEAKING TOO QUICKLY.

A white background with black text

Description automatically generatedSearch the internet for examples of elevator pitches.