logs file metadata Includes group of events Classified as event ID from machine send to SIEM
event: is any action or any click of the keyboard

Whit you do if you find Phishing email?

first see the sender is it legitimate or not and if email delivery to end user or dropped by security email

if email delivery to end user I will do further investigation what is the content of email "link or file" if file download or not

Then write ticket including all information I was collect and recommendations to reduce the risk

Scan destination user machine with AV and remove any unwanted program /software

Configuration email gateway and trend micro scan mail to proactively block similar behaviour conduct awareness training for employees to avoid phishing email

what is CIA?

Confidentiality that data and objects are protected from unauthorized viewing and other access.

Integrity means that data is protected from unauthorized changes.

Availability means that authorized users have access to the systems and the resources they need.

encryption and hashing?

encryption**: two-way process** There are two types of encryption algorithms, also known as ciphers: symmetric ciphers and asymmetric ciphers.

hash: one-way encryption uses to password safe and for integrity data

VPN: virtual private network secure connection to another network over internet all data encrypted

antivirus

software is designed to prevent, detect and remove malware infections on machine typically runs as a background process scanning computers, servers

who antivirus work

Typically, antivirus software uses all three scanning detection processes:

- **Specific Detection** – This works by looking for known malware by a specific set of characteristics.
- **Generic Detection** – This process looks for malware that are variants of known "families," or malware related by a common codebase.
- **Heuristic Detection** – This process scans for previously unknown viruses by looking for known suspicious behavior or file structures.

Although the detection tools are highly effective, no antivirus software is failsafe. If you suspect your device has been infected, you should take action to remedy the problem quickly.

WAF VS FW

Web application firewalls (WAFs) provide security at the 7th layer, protect against attacks data transmitted to your web applications.

WAFs protect against these attacks, and others, by examining HTTP traffic. They can filter traffic by whitelisting or blacklisting

FW layer 3 or 4 firewalls only have visibility into packet headers, and not packet data itself monitoring and control incoming and outcoming network traffic, between trusted internal network and untrusted external network

DNS

A DNS 53 service that translates human readable names like www.example.com into the numeric IP addresses like. phone book.

"A" This record refers to the actual IP address that's associated with the domain.

"CNAME" This record is used to indicate subdomains that might be listed under or associated with your current domain.

"MX" This refers to any mail servers that might be used in accordance with your domain.

"NS" This shows which nameservers are currently being used for your domain.

"SOA" This record has crucial information about your domain, like when your domain was last updated and relevant contact information.

"TXT" This can be edited to include any additional information about the domain that isn't currently listed.

Port RDP = 3389 windows terminal server

Port scanning in which step: Scanning step

HTTP&HTTPS

http: ***Hypertext Transfer Protocol***. allows for the communication between different systems **transfer data from a web server to a browser** in order to allow users to view web pages. It's the protocol that was used for basically all early websites. is not encrypted it can be *easily stolen*

Https: HTTPS protocols remedy this by using an **SSL (secure sockets layer) certificate**, which helps create a secure encrypted connection between the server and the browser, thereby protecting potentially sensitive information from being stolen as it is transferred between the server and the browser.

SSL certificate

SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser. Typically, SSL is used to secure credit card transactions, data transfer and logins, and more recently is becoming the norm when securing browsing of social media sites.

HTTP ERROR CODES

400 — Bad Request

A status code of 400 indicates that the server did not understand the request due to bad syntax.

404 — Not Found

415 — Unsupported Media Type

500 - Internal Server Error

429 Too Many Requests

SSL VS TLS

SSL (Secure Sockets Layers) old one and TLS (Transport Layer Security). **Update version from SSL**

both cryptographic protocols that provide authentication and data encryption between servers, machines, and applications operating over a network

Active directory VS domain controller

	ACTIVE DIRECTORY	DOMAIN CONTROLLER
DEFINITION	It is the directory service that keeps network related information in a structured organized.	It is controller that authenticates and is responsible for the security requests.
FUNCTIONALITY	Collect all the information related with the users.	They check the security by authenticating the users that are accessing the data.

Layers and protocol in each layer

1-Logical layer

2-data link (ARP Address Resolution Protocol, PPP)

3-network (IP, ICMP, IPsec 50, 51)

4-transport (TCP, UDP)

5-session (Layer 2 Tunnelling Protocol 1701 udp , Password Authentication Protocol)

6- presentation (TLS, SSL, SSH 22, FTP 21)

7-application (DNS 53, HTTP 80, HTTPS 443)

(TCP/IP, WANs, LANs)

transmission Control Protocol a 3-way handshake connection oriented and reliable acknowledgment

Internet Protocol (IP) IP is a connectionless protocol, which means that each unit of data is individually addressed and routed from the source device to the target device