Cybersecurit

security engineering
- designer system
- Building system
- Maintaining system

Defensive security (blue team)
Security operations centre
- trends and vulnerability awareness: up to date with the latest
- Policy violation: set of rules that outline how assets are to be protected
- Unauthorised and illegal activity: establish a baseline of acceptable behaviour and activity
- Intrusion and breach detection: detecting and responding to breaches

Digital forensics
File system
- system memory: holds active processes and information valuable for real-time evidence collection.
- System logs: recorded events and activities on a device that help investigators trace actions, changes, and security incidents.
- Network logs: records of network activities and communications that help trace connections, traffic, and potential security incidents.

Incident response
detecting, analyzing, and addressing security breaches or cyberattacks to minimize damage and recover quickly.

- Preparation – Establish policies, train staff, set up tools, and create response plans before incidents occur.

- Detection & Analysis – Monitor systems to identify potential security events, verify them, and assess their scope and impact.

- Containment, Eradication & Recovery – Isolate affected systems to prevent spread, remove malicious elements, and restore systems to normal operations.

- Post-Incident Activity – Review what happened, document lessons learned, and update plans or defenses to prevent future incidents.

Types of malware
- spyware: designed to spy on you, monitor your online activity
- Adware: install with done versions of software and automatically deliver advertisements to a user
- Back door: it's used to bypass authentication procedures to access a system
- Ransomeware: used to hold a system or data it contains captive until payment is made
- Scareware: it's a tactics ti trick user into taking a specific action

- Rootkit: used to modify the operating system to create backdoor which allows attackers to access your computer remotely.
- Virus: type of computer program that when executed, it replicates and attaches itself to files and programs by inserting its own codes
- Trojan horse: a malicious software that disguises itself as a legitimate or useful program to trick user into installing it, which makes the system opened to any form of attack
- Worms: type of malware that replicates itself in order to spread from one computer to another. Unlike virus that needs host to program
- It

Symptoms of malware
- increase in cpu usage which make device slow
- Computer freezing or crashing
- Decrease in web browsing speed
- Network connectivity issues
- Modified or deleted files
- Presence of unknown files
- Unknown processes running
- Programs turning off or reconfiguring themselves
- Emails being sent without user knowledge

Social engineering
Social engineering is the manipulation of people performing actions or divulging confidential information

Types of social engineering
- pretexting: attackers calls an individual and lies to them in order to gain access to privileged data. Eg financial data
- Tailgating: attackers quickly follows an authorised person into a secure, physical location
- Something for something (quid pro quo): attackers request for personal information in exchange for something

Denial of service DoS
Type of network attack that is relatively simple to carry out, even by an unskilled attacker.

Distributed DoS
Similar to DoS attack but originates from multiple, coordinated sources
Eg…
- An attacker builds a network (botnet) of infected hosts called zombies, which are controlled by handler systems.
- The zombie computers will constantly scan and infect more hosts, creating more and more zombies.
- When ready, the hacker will instruct the handler systems to make the botnet of zombies carry out a DDoS attack.

Search engines
Shadon
Censys
Virus total
Have I been pwned

Linux.die.net