Session 3- Threats, Vulnerabilities, and Risks – Basics

1. Threats

Definition: Anything with the potential to exploit a vulnerability and cause harm.
Examples:

- Hackers attempting data theft
- Malware (viruses, ransomware)
- Insider attacks
- Natural disasters (fire, flood, earthquake)

Think of a threat as the bad thing that could happen.

2. Vulnerabilities

Definition: Weakness or flaw in a system that can be exploited by a threat.
Examples:

- Weak passwords
- Unpatched software
- Misconfigured firewalls
- Lack of encryption
- Human error (phishing clicks)

A vulnerability is like an open door or crack in the wall.

3. Risks

Definition: The likelihood that a threat will exploit a vulnerability, and the impact it would cause.
Formula:Risk = Threat × Vulnerability × Impact

Examples:
Weak password (vulnerability) + brute-force attacker (threat) → high risk of compromise.
Unpatched server (vulnerability) + ransomware actors (threat) → high risk of attack.

Risk is the chance and damage if the bad thing happens.

4. Connection to CIA Triad

Confidentiality: Threat exploits vulnerability → Data leak.
Integrity: Threat exploits vulnerability → Records tampered.
Availability: Threat exploits vulnerability → Service downtime.

5. Impact = Loss
    - If risks materialize, they result in:
        - Financial loss
        - Reputation loss
        - Legal/regulatory loss
        - Operational downtime
    - Threats exploit vulnerabilities → create risks → impact CIA triad → cause loss.

This is the foundation for SOC analysis: Identify threats, fix vulnerabilities, reduce risks, and prevent losses.