Session 2 - CIA Triad

1. What is the CIA Triad?

The CIA Triad is a foundational model in cybersecurity that defines the three key objectives of protecting information systems:

Confidentiality: Keeping data private and accessible only to authorized individuals.
Integrity: Ensuring data remains accurate, consistent, and unaltered by unauthorized parties.
Availability: Ensuring systems and data are accessible when needed by authorized users.

Every security control, tool, or policy in cybersecurity is designed to support at least one of these three pillars

2. Components of the CIA Triad

A. Confidentiality

Goal: Prevent unauthorized access to sensitive data.
How to Maintain:
Strong authentication (passwords, biometrics, security tokens).
Authorization and access control (role-based permissions).
Encryption (symmetric and asymmetric).
Network security controls (firewalls, VPNs, TLS/SSL).

Examples:

Using HTTPS to secure communication.
Encrypting customer data in a database.
Applying role-based access to company files.

B. Integrity

Goal: Ensure data is trustworthy and unaltered.
How to Maintain:
Hashing (SHA-256, SHA-3, MD5 – note: MD5 is weak).
Checksums to verify files during transfer.
Digital signatures to validate authenticity.
Version control systems like Git.
File integrity monitoring tools (Tripwire, Wazuh).

Examples:

Verifying file authenticity using a hash value.
Detecting unauthorized log changes in a SOC.
Using Git to track source code changes.

C. Availability

Goal: Ensure authorized users can access systems/data reliably.
How to Maintain:
DDoS protection (CDN, rate limiting).
Redundancy and failover mechanisms.
Regular backups and tested recovery plans.
System updates and patching.
Monitoring system performance and uptime.

Examples:

Using load balancers to keep a website online.
Restoring data after a ransomware attack.
Cloud-based disaster recovery systems.

3. Relevance to SOC Analysts

SOC Analysts often classify incidents based on which aspect of the CIA Triad is affected:

Confidentiality breach: Data exfiltration, credential theft.
Integrity breach: Log tampering, financial fraud.
Availability breach: DDoS attack, ransomware lockouts.

This classification helps analysts assess the impact of incidents and prioritize response.

4. Summary

The CIA Triad provides the foundation for all cybersecurity strategies:

Confidentiality → Keep data private.
Integrity → Keep data accurate.
Availability → Keep data accessible.

A strong SOC mindset means always asking: “Which part of the CIA Triad is under threat here?”