Threat DetectX – Day 3

1. Difference between IT Security, Information Security, Cyber Security, Operational Security

Security Domain	Definition & Focus	Example Scope
IT Security	Protects digital information and IT systems (hardware, software, networks) from threats and attacks	Servers, computers, networks, databases
Information Security	Safeguards all forms of information (digital, physical, verbal) ensuring confidentiality, integrity, availability	Paper records, digital files, verbal communications
Cyber Security	Defends digital assets and cyberspace (networks, systems, data) from cyber threats and attacks	Internet, cloud, endpoints, online applications
Operational Security	Process to identify and protect critical operational information and activities from adversaries	Business operations, industrial control systems

IT Security:

Focuses on protecting information processed, stored, or transmitted by IT systems such as computers, servers, and networks.

Scope: Encompasses technical controls like firewalls, antivirus, access controls, and patch management.

Objective: Ensure the confidentiality, integrity, and availability of digital information and IT assets.

Example: Preventing unauthorized access to a company's internal network or database.

Information Security:

Broader than IT security; protects all types of information, whether digital, physical, or spoken, from unauthorized access, disclosure, alteration, or destruction.

Scope: Includes policies, procedures, and controls for both digital and non-digital information (e.g., paper documents, verbal communication).

Objective: Uphold the CIA triad—Confidentiality, Integrity, and Availability—across all information assets.

Example: Securing confidential paper contracts as well as digital records.

Cyber Security:

A subset of information security focused specifically on protecting digital environments (cyberspace), including networks, computers, and data, from cyber threats such as hacking, malware, and phishing.

Scope: Involves technical measures like intrusion detection systems, encryption, and incident response for digital assets.

Objective: Defend against cyberattacks targeting digital infrastructure and data.

Example: Implementing measures to prevent ransomware attacks on cloud services or online platforms.

Operational Security (OPSEC):

A risk management process that identifies critical operational information, analyzes threats, assesses vulnerabilities, and implements countermeasures to prevent adversaries from exploiting sensitive data or processes.

Scope: Focuses on protecting the integrity of business operations, industrial processes, and critical infrastructure—often in real-time environments.

Objective: Prevent leakage of sensitive operational details that could be exploited by attackers.

Example: Restricting access to production schedules or industrial control systems to prevent sabotage or espionage.

2. Data Life-cycle

Data exists in three primary states during its life-cycle, each with distinct characteristics and security considerations:

Data at Rest
This refers to data that is stored and not actively being accessed or moved. Examples include files saved on hard drives, databases, backups, or cloud storage. Data at rest is considered stable but must be protected against unauthorized access through encryption, access controls, and physical security measures.

Data in Transit (or Data in Motion)
Data in transit is data actively moving between locations, such as across networks, between devices, or within systems. Examples include data sent over the internet, emails, or data transferred between cloud and local storage. Because it is exposed during transmission, encryption (like TLS/SSL) is critical to prevent interception or tampering.

Data in Use
Data in use is data currently being processed, accessed, or modified by applications or users. This state is the most vulnerable because data is exposed in memory or CPU registers. Protection methods include strong authentication, strict access controls, encryption when possible, and user agreements to prevent unauthorized disclosure.

3. Assets

Assets are valuable resources owned or controlled by an individual, business, or organization that contribute to its operations, productivity, and future economic benefits

They can be broadly classified into:

Physical (Tangible) Assets: These are tangible items you can see and touch, such as buildings, machinery, equipment, inventory, vehicles, and office furniture. They form the physical foundation of a business and are essential for day-to-day operations

Digital Assets: Intangible electronic resources like data, software, websites, digital documents, and intellectual property stored or transmitted in digital form. These require protection against unauthorized access and loss.

People Assets: The human resources of an organization, including employees and contractors, whose skills, knowledge, and access rights are critical to business success.

Paper Assets: Physical documents such as contracts, reports, and records that hold sensitive or proprietary information needing secure management.

Services: Intangible assets including outsourced operations, cloud services, IT support, and other business functions that support continuity and efficiency.

Software: Programs and applications used by an organization, including operating systems, productivity tools, and security software, which must be maintained and protected from vulnerabilities.

4. Frameworks and Regulations

Frameworks and regulations collectively help organizations secure sensitive data, protect privacy, and comply with legal and industry requirements.

PCI DSS (Payment Card Industry Data Security Standard): A set of security requirements designed to protect payment card data during storage, processing, and transmission. It aims to prevent credit card fraud by enforcing technical and operational controls like encryption, access control, and network security for organizations handling cardholder data.

ISO 27001: An international standard specifying requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). It provides a risk-based approach to managing sensitive company information, ensuring confidentiality, integrity, and availability.

GDPR (General Data Protection Regulation): A European Union regulation that governs the collection, processing, and storage of personal data of EU residents. It emphasizes data privacy, user consent, data protection rights, and strict penalties for non-compliance to protect individuals' personal information.

DPDPA (Data Protection and Digital Privacy Act): Generally refers to national or regional laws aimed at protecting personal data and digital privacy rights in India. Specifics vary by jurisdiction, but the focus is on regulating data collection, usage, and safeguarding individual privacy.

HIPAA (Health Insurance Portability and Accountability Act): A U.S. law that sets standards for protecting sensitive patient health information. It mandates safeguards for electronic health records, privacy rules, and security measures to ensure the confidentiality and security of healthcare data.

Standard / Regulation	Purpose	Primary Focus Area	Region/Scope
PCI DSS	Protect cardholder data	Payment card security	Global (card processing entities)
ISO 27001	Manage information security risks	ISMS, risk assessment, controls	Global (all organizations)
GDPR	Protect personal data of EU citizens	Privacy rights, data processing, breach reporting	European Union (affects global entities handling EU data)
DPDPA	Protect personal digital data in India	Consent, processing limitations, fiduciary duties	India
HIPAA	Protect health information (PHI)	Health data privacy and security	USA (healthcare sector)