Day 1 Data Analysis ASSIGNMENT

Prepare documentation in on

1. Cyber Security (covering everything related)
2. Asset Management
3. IT Asset Management
4. Cyber Security Asset Management
5. Similarities and differences between IT and Cyber Security Asset Management
6. Emerging trend in Cyber Security
7. One Case study on any Cyber attack

1. Cyber Security - Cyber security refers to the practice of protecting systems, networks, and data from cyber threats, such as hacking, malware, phishing, and ransomware attacks. It encompasses various domains, including network security, endpoint security, cloud security, and data protection.

Key Aspects of Cyber Security:

- **Network Security**: Protects computer networks from unauthorized access.
- **Endpoint Security**: Secures individual devices like laptops and smartphones.
- **Cloud Security**: Ensures safe usage of cloud-based services.
- **Application Security**: Focuses on protecting software applications from threats.
- **Data Protection**: Implements encryption and access controls to safeguard data.

Types of cyber attacks:

1. Hacking

- Unauthorized access to a system or network to steal, modify, or destroy data.
- **Example:** SQL injection, brute force attacks.

2. Malware (Malicious Software)

- Software designed to harm or exploit devices and networks.
- **Types:**
    - **Viruses** – Attaches to files and spreads when executed.
    - **Worms** – Self-replicating malware that spreads across networks.
    - **Trojans** – Disguised as legitimate software to trick users into installing them.
    - **Spyware** – Secretly monitors user activity and steals information.

3. Phishing

- Fraudulent attempts to obtain sensitive data by disguising as a trustworthy entity.
- **Example:** Fake emails from banks or service providers tricking users into providing login details.

4. Ransomware

- Encrypts files and demands payment (ransom) to restore access.
- **Example:** WannaCry, REvil ransomware attacks.

5. Denial-of-Service (DoS) & Distributed Denial-of-Service (DDoS) Attacks

- Overloads a network or website with excessive requests, causing service disruptions.
- **Example:** Botnet attacks.

6. Man-in-the-Middle (MitM) Attack

- Attackers intercept communication between two parties to steal or manipulate data.
- **Example:** Fake Wi-Fi hotspots capturing login credentials.

7. Zero-Day Exploits

- Attackers exploit unknown vulnerabilities before developers patch them.
- **Example:** Software security flaws used by hackers before an official update is released.

8. SQL Injection

- Injects malicious SQL queries into a database to steal or modify data.
- **Example:** Gaining admin access to a website by exploiting login forms.

9. Brute Force Attack

- Automated guessing of passwords using multiple combinations.
- **Example:** Cracking weak passwords on accounts or servers.

10. Credential Stuffing

- Using leaked usernames and passwords from data breaches to access other accounts.
- **Example:** Reusing passwords across multiple sites leads to account takeovers.

2. Asset Management - Asset management refers to the systematic process of acquiring, maintaining, and disposing of assets in a cost-effective manner. It is widely used in businesses to track physical and digital assets, optimize asset usage, and ensure compliance.

Types of Asset Management:

- **Financial Asset Management**: Manages investments and financial portfolios.
- **Physical Asset Management**: Deals with tangible assets like machinery and infrastructure.
- **Digital Asset Management**: Handles digital files and software.

3. IT Asset Management (ITAM) - IT Asset Management (ITAM) focuses on managing IT-related assets such as hardware, software, and network resources to optimize performance and reduce costs.

Key Components of ITAM:

- **Hardware Asset Management**: Tracking servers, computers, and other devices.
- **Software Asset Management**: Managing software licenses and compliance.
- **Lifecycle Management**: Monitoring the procurement, usage, and disposal of IT assets.

- **IT Governance and Compliance**: Ensuring adherence to IT policies and regulatory requirements.

4. Cyber Security Asset Management (CSAM) - Cyber Security Asset Management (CSAM) involves identifying, tracking, and securing all assets within an organization to minimize cybersecurity risks. It provides visibility into assets that may be vulnerable to cyber threats.

Key Elements of CSAM:

- **Asset Discovery**: Identifying all assets in an organization's network.
- **Vulnerability Assessment**: Analysing security risks associated with assets.
- **Risk Management**: Implementing measures to protect critical assets.
- **Incident Response**: Quickly addressing security breaches and threats.

5. Similarities and Differences between ITAM and CSAM -

Feature	IT Asset Management (ITAM)	Cyber Security Asset Management (CSAM)
Focus	Optimizing asset utilization and cost	Protecting assets from cyber threats
Scope	IT resources (hardware, software, licenses)	IT resources with security risks (endpoints, applications, networks)
Objective	Cost efficiency and compliance	Security and risk mitigation
Monitoring	Tracks asset lifecycle and usage	Tracks vulnerabilities and threats
Compliance	Ensures software license compliance	Ensures security policy adherence

6. Emerging Trends in Cyber Security -

- **Zero Trust Security** – No user or device is trusted by default, requiring continuous verification.
    - **Example:** Google's **BeyondCorp** security model ensures employees access corporate data only after authentication, even from internal networks.

- **AI and Machine Learning in Security** – AI-powered systems detect and mitigate threats in real time.
    - **Example: Darktrace** uses AI to identify unusual network behaviour and prevent cyber threats before they escalate.

- **Cloud Security Enhancements** – Advanced security measures for protecting cloud-stored data.
    - **Example: Microsoft Defender for Cloud** provides threat protection across multi-cloud and hybrid environments.

- **Blockchain for Cyber Security** – Securing transactions and preventing data breaches with decentralized encryption.
    - **Example: IBM's Hyperledger Fabric** ensures tamper-proof data storage in supply chain management.

- **IoT Security** – Safeguarding interconnected devices from cyber threats.
    - **Example: Cisco IoT Threat Defense** secures IoT networks by segmenting traffic and detecting anomalies.

- **Cyber Resilience Strategies** – Ensuring business continuity despite cyberattacks.

- **Example: Maersk** implemented a robust cyber resilience plan after the 2017 NotPetya attack, restoring operations quickly and improving future security defenses.

7. Case Study: Cosmos Bank Cyber Attack (India's Biggest Bank Heist)

Overview of the Cosmos Bank Heist -

- On August 11, 2018, a cyber attack at Cosmos Bank in Pune led to a theft of approximately ₹94.42 crores (~$13 million).
- Hackers infiltrated the bank's server, compromising security systems in one of India's largest cyber heists.
- The attack initially appeared as a server malfunction, causing widespread concern among bank officials.

Methodology of the Attack -

- Over 5,000 cloned cards were used to withdraw funds across 32 countries in a single day.
- A sophisticated malware bypassed transaction verification protocols.
- Hackers manipulated the transaction approval system, enabling fraudulent withdrawals.

Investigation and Response -

- A Special Investigation Team (SIT) was formed, including cybersecurity experts.
- Initial investigations yielded limited leads, despite mobile data tracking and CCTV analysis.
- Pune Police arrested 18 individuals, primarily hired accomplices, lacking knowledge of the masterminds.

International Implications and Collaboration -

- The case exposed links to international cybercriminals, including potential North Korean connections.
- International cooperation was required for fund recovery and legal actions.
- ₹10 crores were frozen in foreign accounts, with ₹5.72 crores eventually returned to Cosmos Bank.

Security Insights and Future Precautions -

- The heist highlighted vulnerabilities in digital banking infrastructure.
- It emphasized the necessity of global cooperation in combating cybercrime.
- The case serves as a benchmark for cybersecurity measures and law enforcement strategies.

Conclusion -

Cyber security and asset management are critical to protecting financial and digital resources. The Cosmos Bank heist illustrates the evolving threats in the cyber landscape and underscores the need for robust security strategies, international collaboration, and continuous monitoring to prevent future cyber attacks.