Identify and Analyze Cyber Threats

Malware
Definition: Software that is intentionally designed to harm a computer or network, typically designed to steal data, damage systems, or gain unauthorized access.

Function: Malware typically enters a system through phishing emails, malicious downloads, or infected USB drives. Once inside, it can execute harmful actions such as stealing data, encrypting files, or creating backdoors for unauthorized access.

Real-World Example: The 2017 WannaCry ransomware attack used a vulnerability in outdated Windows systems to encrypt files and demanded Bitcoin payments for decryption.

Impact: Data loss, financial loss, disruption of systems.

Social Engineering
Definition: Social engineering manipulates individuals into giving up sensitive information.

Function: Using tactics like phishing, baiting or pretexting to gain access to confidential information by tricking users

Real-World Example: Twitter Bitcoin same used bots to social engineer employee credentials

Impact: Led to Unauthorized access to systems, data breaches, loss of reputation

Advanced Persistent Threats (APTs)
Definition: APTs are prolonged and targeted cyberattacks where attackers gain unauthorized access to a network and remain undetected to steal sensitive data over time.

Function: APTs use techniques, such as custom malware, spear-phishing, and exploiting system vulnerabilities. Attackers prioritize stealth to avoid detection while exfiltrating data or gaining persistent access.

Real-World Example: The SolarWinds attack (2020) was an APT where attackers inserted malicious code into a software update, compromising numerous organizations, including U.S. government agencies.

Impact: Data breaches, compromise of sensitive information

Insider Threats

Definition: Insider threats arise from individuals within an organization, such as employees, contractors, or business partners, who misuse their access to harm the organization.

Function: Insiders can intentionally or unintentionally compromise security by stealing data, leaking sensitive information, or damaging systems

Real-World Example: The 2013 Edward Snowden leaks revealed classified information about NSA surveillance programs, significantly impacting national security

Impact: Exposure of confidential data, loss of customer trust

Zero- Day Exploits
Definition: Zero-day exploits take advantage of vulnerabilities in software or hardware that are unknown to the vendor and unpatched.

Function: Attackers identify and exploit these flaws before they are discovered and patched, often using custom malware or scripts to infiltrate systems.

Real-World Example: The Stuxnet worm exploited zero-day vulnerabilities to sabotage Iran's nuclear centrifuges, highlighting its potential for cyber warfare.

Impact: Compromise of Infrastructure, Loss of System Control.

Apply Vulnerability Assessment Techniques