Cybersecurity Fundamentals

~Jithin Netticadan

CEH v12 | CAP | Qualys

5W1H of Security

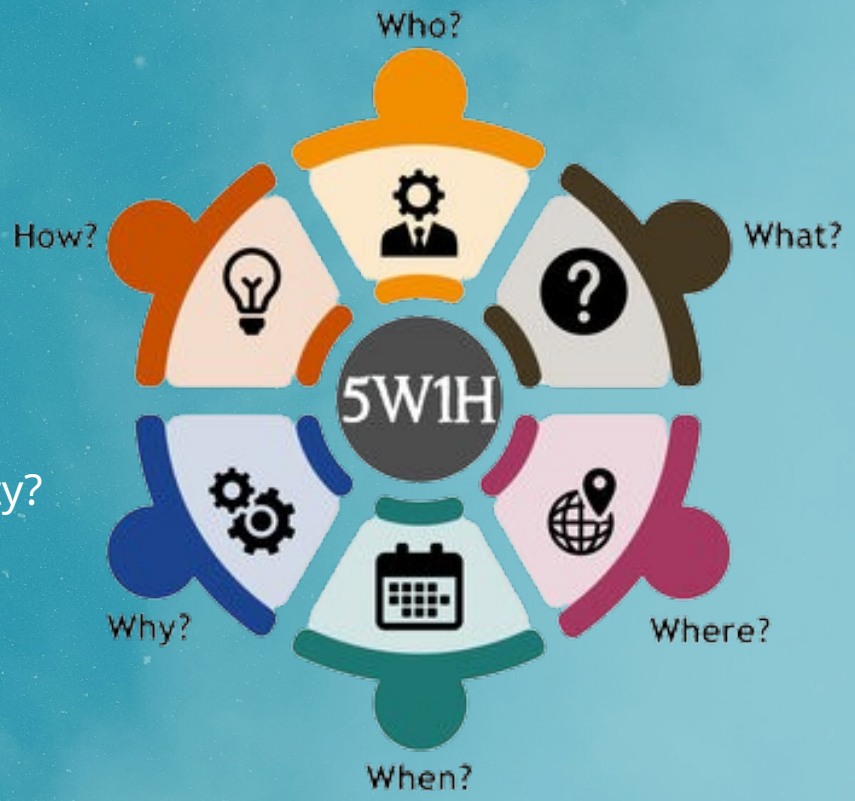
What is Information Security?

Why Do You Need Information Security?

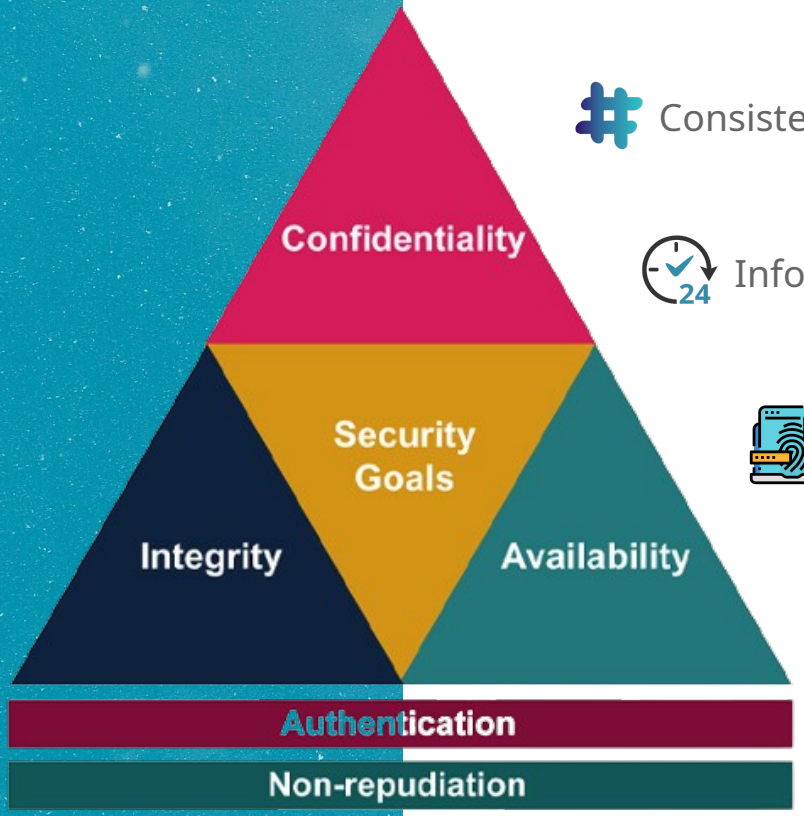
Who is responsible for information security?

When is the Right Time to Address Information Security?

Where Does Information Security Apply?



Pillars of Cybersecurity



Prevent sensitive information from unauthorized access attempts.

Consistency, accuracy and trustworthiness of data.

Information should be readily available to authorized users.

Systems' ability to confirm an identity.

Confirm validity of something that occurs.

Encrypt vs Hash vs Encode

Technique that makes your data unreadable and hard to decode for an unauthorized user.

One-way summary of data that cannot be reversed and is used to validate the integrity of data.

Reversible transformation of data format, used to preserve the usability of data.

Type of Cyber Attacks

Malware

Any type of malicious software designed to cause harm or damage to a computer, server, client or computer network and/or infrastructure without end-user knowledge.

Phishing

Trick users into divulging sensitive data, downloading malware, and exposing themselves or their organizations to cybercrime.

Social Engineering

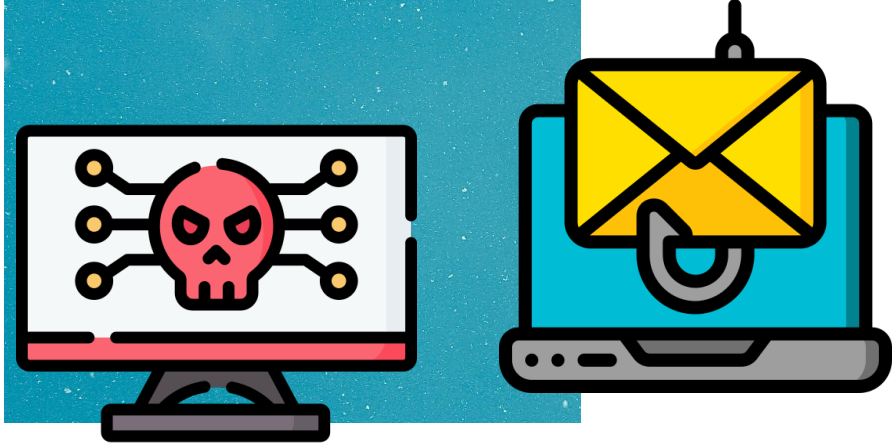
Set of tactics used to manipulate, influence, or deceive a victim into divulging sensitive information or performing ill-advised actions

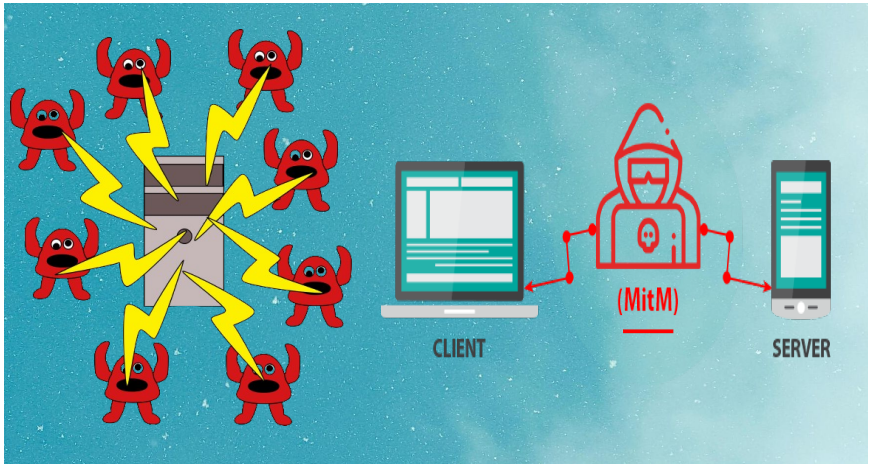
DoS/DDoS

Disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

MitM

Allow attackers to eavesdrop on the communication between two targets.





Cybersecurity Domains

Identity & Access Management (IAM)

Policies, processes, and technologies used to manage and control access to digital assets within an organization. IAM encompasses user authentication, authorization, identity provisioning, and access governance.

Digital Forensics

Collecting, preserving, analyzing, and presenting digital evidence in a legal investigation or dispute. Digital forensics professionals examine digital devices, networks, and data to uncover evidence of malicious activities and support legal proceedings.

Governance, Risk & Compliance (GRC)

Establish policies, procedures, and controls to ensure organizational objectives are met. Identify, assess, and mitigate risks that could impact the organization. Adhere to relevant laws, regulations, and industry standards.

Security Operations Center (SOC)

Centralized unit within an organization responsible for monitoring, detecting, analyzing, and responding to cybersecurity threats and incidents.

Cybersecurity Domains

Vulnerability Assessment & Penetration Testing (VAPT)

Vulnerability management involves identifying, assessing, prioritizing, and mitigating vulnerabilities in an organization's IT infrastructure.

Penetration testing also known as ethical hacking, is the practice of simulating cyber attacks against an organization's IT infrastructure, applications, and systems to identify security vulnerabilities.

Thank you