

Cybersecurity Fundamentals

~Jithin Netticadan
CEH v12 | CAP | Qualys

5W1H of Security

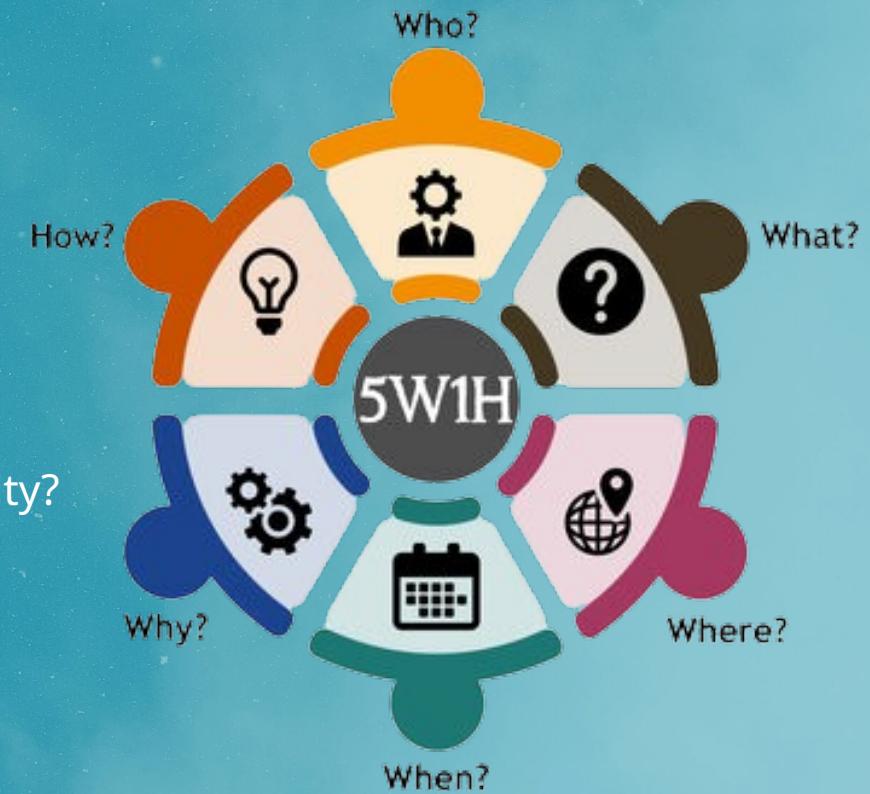
What is Information Security?

Why Do You Need Information Security?

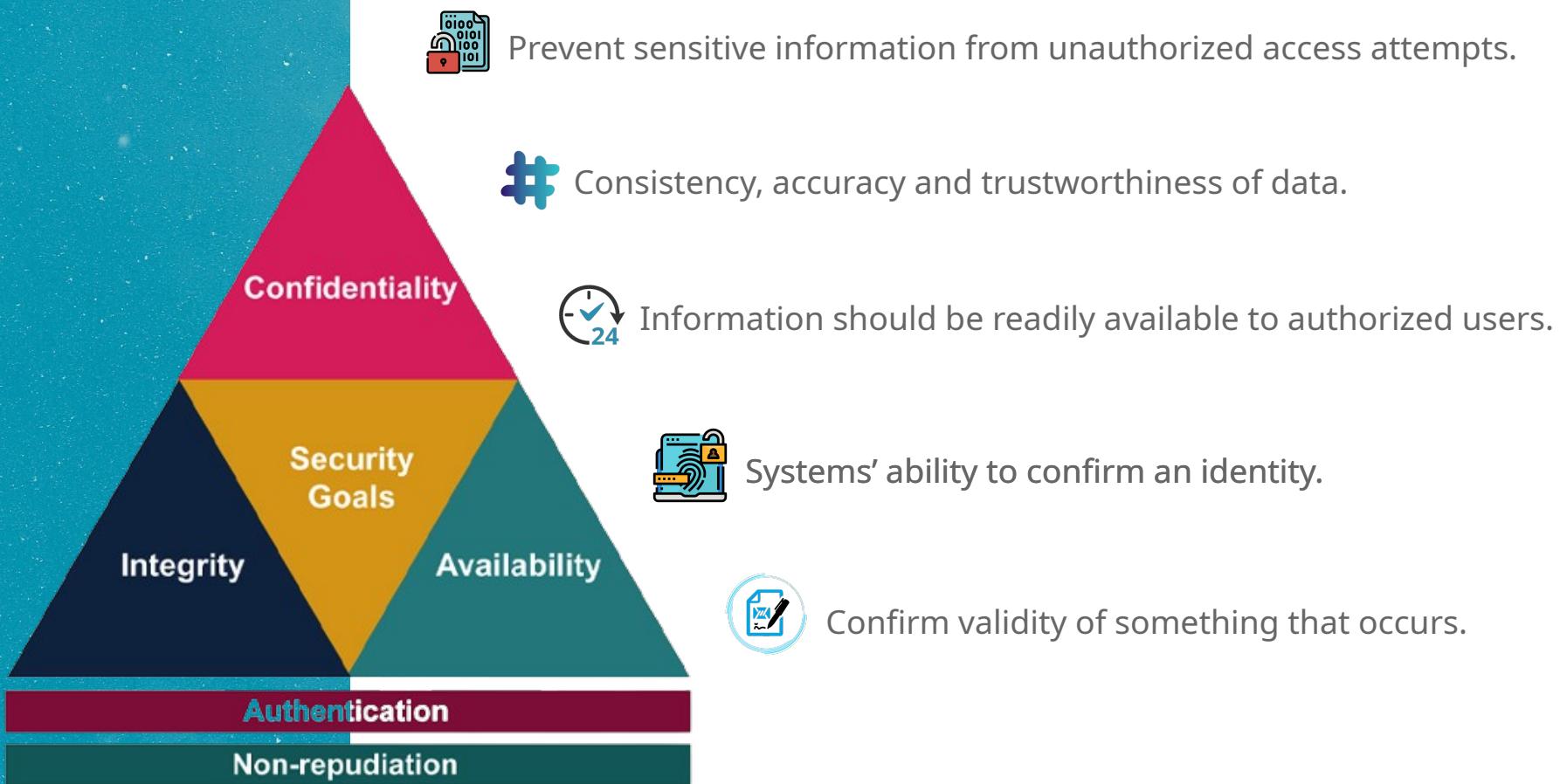
Who is responsible for information security?

When is the Right Time to Address Information Security?

Where Does Information Security Apply?



Pillars of Cybersecurity



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.

MitM

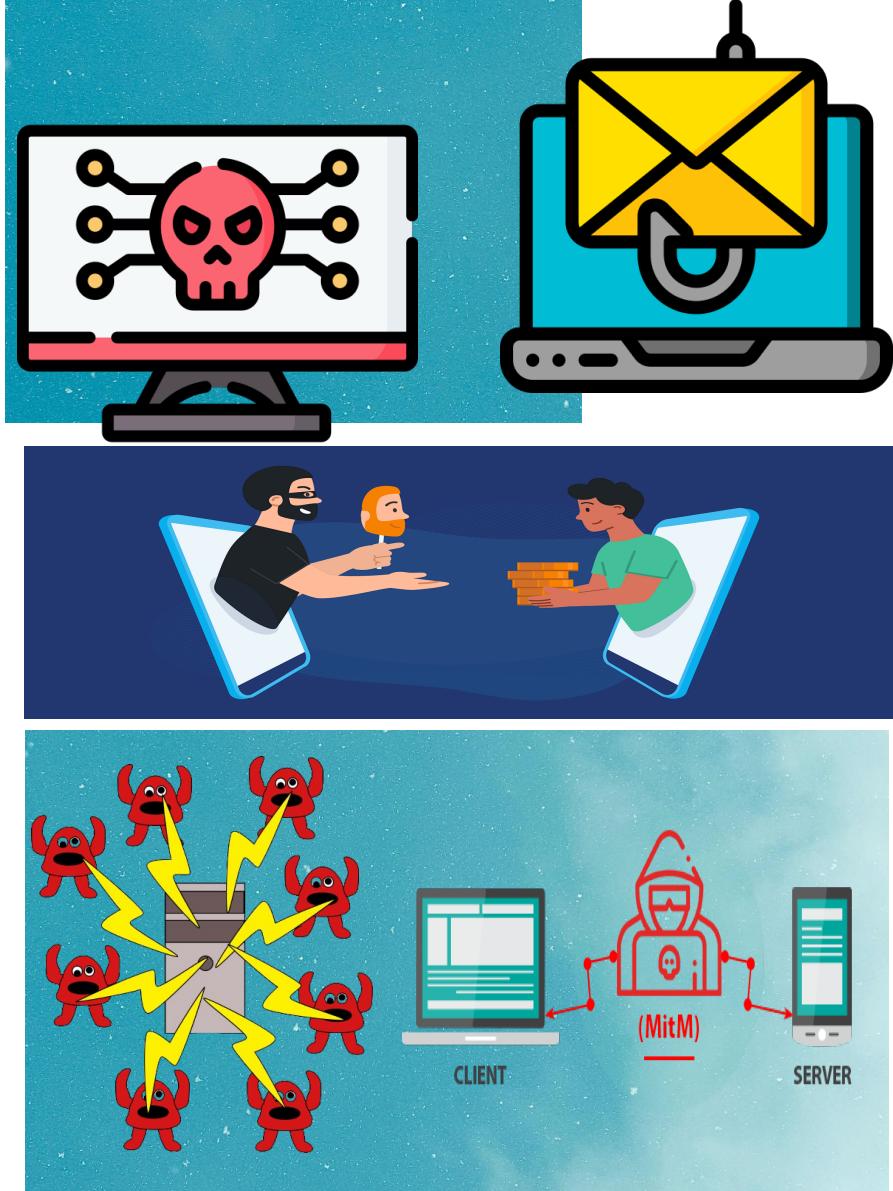
Allow attackers to eavesdrop on the communication between two targets.

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.



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.

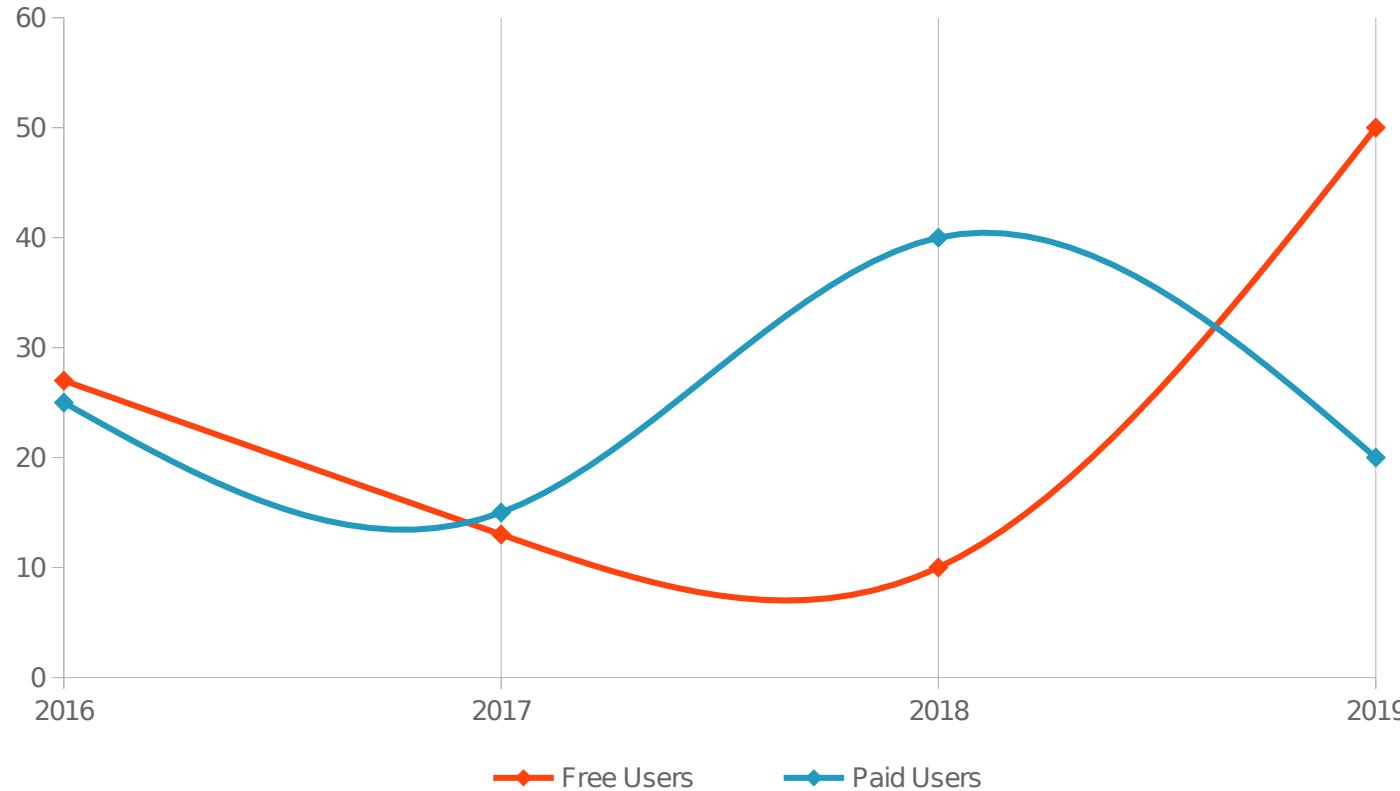
Cybersecurity Domains

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.

Lorem Ipsum



Lorem Ipsum Dolor Sit

*Lore ipsum dolor sit
amet, consectetur
adipiscing elit, sed do
eiusmod tempor
incididunt ut labore et
dolore magna aliqua.*

Lorem Ipsuum

LOREM

IPSUM

DOLOR

SIT AMET

CONSECTETUR

ADIPISCING

Lorem Ipsum

Lorem Ipsum Dolor 1	M 1,000	M 1,489	M 2,388
Lorem Ipsum Dolor 2	M 2,135	M 3,432	M 1,235
Lorem Ipsum Dolor 3	M 2,937	M 235	M 987
Lorem Ipsum Dolor 4	M 716	M 1,975	M 935
Lorem Ipsum Dolor 5	M 934	M 827	M 1,564
Sit	M 7,722	M 7,958	M 7,109

Lorem Ipsum



Lorem Ipsum

Lorem ipsum dolor sit amet,
consectetur adipiscing elit,
sed do eiusmod tempor
incididunt ut labore et dolore
magna aliqua.

Lorem ipsum



Lorem Ipsum

Lore ipsum dolor sit amet,
consectetur adipiscing elit,
sed do eiusmod tempor
incididunt ut labore et dolore
magna aliqua.

Thank you