Day 1:03/02/2025

Task 1:-

Find information about following:-

1. IT Asset Management
2. Vulnerability
3. Obsolescence
4. Vulnerability
5. Compliance
6. Maintenance
7. End of Life
8. End of Support
9. End of Maintenance
10. Asset Hygiene
11. Crown Jewel
12. Inventory
13. NVD

IT Asset Management:-

IT asset management (ITAM) is the end-to-end tracking and management of IT assets to ensure that every asset is properly used, maintained, upgraded and disposed of at the end of its lifecycle.

What is IT Asset?

An information technology (IT) asset is any piece of information, software or hardware that an organization uses in the course of its business activities. Hardware assets include physical computing equipment like physical servers in data centers, desktop computers, mobile devices, laptops, keyboards and printers. Software assets, on the other hand, include applications for which licenses are typically issued per user or machine, as well as software systems and databases built using open-source resources. Software assets also include cloud-based assets, such as Software-as-a-Service (SaaS) applications.

Vulnerability:-

A vulnerability is a weakness in an IT system that can be exploited(used) by an attacker to deliver a successful attack. Or to gain unauthorized access to system. When any system get exploit to any vulnerability attacker install malware and can steel sensitive information.

Vulnerabilities can be exploited (to be use) by variety of methods such as SQL injection, buffer overflow and many more.

There are different types of vulnerability

1) Hardware:-
2) Software:-
3) Network:- Insecure network , lack of authentication , man in middle attacks leads to network vulnerability,

Obsolescence:-

It is a process of something becoming out date, no longer useful, or discarded. According to technology point of view A product hardware/software become out date due to rapid technological Development. For example:- windows 7 or intel core processor get out date due to advancement in technology.

Compliance

Compliance is the act of following rules , regulations or standards set by government or by any organization. Compliance are necessary to ensure ethical conduct , data security and prevent companies from violation of rules. Types of compliance are:

1) Legal
2) Financial
3) Data Compliance :- It follows laws , regulations and industry standards to handle data. It involve data protection , Access Management , Encryption

Maintenance:-

Maintenance is process of keeping data accurate , up to date and to keep relevant data i.e. it involves updating and correcting data.

End of Life:-

End-of-Life (EoL) refers to the **point in a product's lifecycle when it no longer receives support or updates from the manufacturer**. After this phase, the product is considered obsolete, meaning it won't have new features, bug fixes, security updates, or customer support. EoL is a critical milestone in a product's lifecycle, signaling to users that they should start planning to upgrade or replace the product.

EOL for software:- It pauses updates . patches , and direct support from developer.

EOL for hardware:- For hardware EOL reaches when manufracture discontinues production , sales and support services.

End of Support:-

EOS is often come before EOL. End-of-Support (EoS), also known as End-of-Service Life (EoSL), **marks a specific point in a product's lifecycle when the manufacturer stops providing technical support**, including bug fixes, patches, and updates.

Crown Jewel:-

It refer to most important and sensitive data of any organization. It required high level of protection. In point of view of business it is highest value(price) asset of any organization. For example:- Company's employee personal data are important and sensitive data.

Inventory:-

Inventory is asset that can clearly seen exist or difficult to describe or measure, An assets that can be realize for revenue generation or has value for exchange.

NVD(National Vulnerability Database):-

The NVD is the U.S. government repository of standards based vulnerability data represented using the security content automation protocol(SCAP:- is multi purpose framework of specification that supports automated configuration , vulnerability and patch checking, and security measurement.).This data enable automation of vulnerability management , security measurement , and compliance. The NVD include database of security related software flaws , product names and impact metrics.

Patch Management:-

It is process of applying updates to software to protect against vulnerabilities

Three common types of patches are:

1) Security Patches:
2) Bug fixing Patches:
3) Performance And Feature patches:

End of Maintenance:-

When any product reach EOM then no more patches(Set of program that fixes bug , improve security or adds new features) will released for that version but it will be providing support for that version.

Similar to ApexaiQ:-

1) Asset Panda:-
2) SolarWinds
3) Cloud wize