Short Notes

12/08/2025

Some Basic Concepts:

1. ApexaiQ score –

credit rating for your entire **IT estate**-----including every device on your network.

It **computes all your risks and security gaps** into a single score----obsolescence and compliance

Calculated based on:

1. **IT Environment**
2. **Asset Hygiene** - Obsolescence, Maintenance, Vulnerabilities
3. **IT Gaps**

ranges between **60 (poor) to 160 (genius).**

2. IT asset management

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 it's lifecycle.

use:

make strategic decisions

to ensure that IT resources are used efficiently and effectively.

optimize costs

audit presentation

3. Vulnerabilities

weaknesses in a system

that gives threats the opportunity to compromise assets.

weaknesses in an organization’s technological system

that an attacker can use to

infiltrate, steal data, or shut down an organization.

4. Obsolescence

process of becoming out of date, or no longer useful, or the condition of being in such a state.

Outdated interfaces.

Technology obsolescence occurs when hardware and software have been superseded by more advanced versions.

5. Compliance

guidelines developed by regulatory bodies

following all legal requirements, standards, industry regulations, government policies, security frameworks and customer terms of agreement

to ensure software security, safeguard customer data and appropriate usage in business.

6.Maintenance

-making sure it performs at a level where it can provide the most value for its users.

-to keep the system reliable and up-to-date.

7. End of Life, End of Support, End of Maintenance

- **End of Life (EOL):** The product is officially retired and no longer sold or developed.
- **End of Support (EOS):** The company stops providing **technical help or customer service** for the product.

- **End of Maintenance (EOM):** The company stops releasing updates, bug fixes, or patches.

Basic difference:
EOL means the product's lifecycle is over, EOS means no help is available even if you still use it, and EOM means you'll get no new fixes/updates but may still get help until EOS.

Example:
Windows 7 —

- **EOM:** No new updates after January 14, 2020.
- **EOS:** Microsoft stopped giving any tech support after January 14, 2020.
- **EOL:** Microsoft declared Windows 7 officially retired on the same date, ending its lifecycle.

8.Asset Hygiene

maintaining up-to-date software, ensuring proper management and security of assets, and addressing vulnerabilities.

9. Crown Jewel

are a company's most prized and valuable assets.

Ex. physical assets or intangibles like patents or intellectual property and trade secrets.

10. Inventory

process of identifying, tracking, and managing all **hardware and software assets** an organization owns or uses

Ex. servers, laptops, mobile devices, printers, network devices, software licenses, and other technology-related items

11.NVD

National Vulnerability Database (**NVD**) is the U.S. government repository of standards-based vulnerability management

data represented using the Security Content Automation Protocol (SCAP).

12. Patch Management

Patch management is the process of distributing and applying updates to software.

These patches are often necessary to correct errors (also referred to as “vulnerabilities” or “bugs”) in the software

13. Data Breaches

release of confidential, private, or otherwise sensitive information into an **unsecured environment.**

14. MSP

A managed service provider (MSP) is a third-party company that remotely manages a customer's (IT) infrastructure and end-user systems

perform a defined set of day-to-day management services

15. Device Types

information about a class of devices, including properties that apply to all devices of a type.

16. True Saas

A fully cloud-based software service delivered and maintained by the provider, accessible via the internet.

17. Inbound/Outbound Integration

the processes of receiving and sending data between systems.

Inbound integration involves external systems sending data to ApexAIQ.

Outbound integration involves ApexAIQ sending data to external systems.

18. Compliance Standards - eg. CISA, CISO, HIPPA, ISO 27001

CISA – *Cybersecurity and Infrastructure Security Agency* – a U.S. government agency focused on protecting critical infrastructure from cyber threats.

CISO – *Chief Information Security Officer* – the executive responsible for an organization's information security strategy and programs.

HIPAA – *Health Insurance Portability and Accountability Act* – a U.S. law that protects sensitive patient health information.

ISO 27001 – An international standard for managing information security through best-practice frameworks and controls.

19. Perimeter

The network boundary separating internal resources from external threats.

20. ROI (Return on Investment)

tries to directly measure the amount of return on a particular investment, relative to the investment's cost.

21. KPI (Key Performance Indicators)

(key) indicators of progress toward an intended result.

22. Auto-remidiation

Automated processes that fix detected security or operational issues without manual intervention.

23. Network protocols

HTTP (Hypertext Transfer Protocol) – Transfers web pages between browsers and web servers.

HTTPS (HTTP Secure) – HTTP over TLS/SSL, encrypting web communication.

FTP (File Transfer Protocol) – Transfers files between computers over a network.

SMTP (Simple Mail Transfer Protocol) – Sends email messages between mail servers.

IMAP (Internet Message Access Protocol) – Retrieves and manages emails from a server.

POP3 (Post Office Protocol v3) – Downloads emails from a server to a local device.

DNS (Domain Name System) – Translates domain names into IP addresses.

DHCP (Dynamic Host Configuration Protocol) – Automatically assigns IP addresses to devices.

TCP (Transmission Control Protocol) – Ensures reliable, ordered data delivery between devices.

UDP (User Datagram Protocol) – Sends data without reliability checks, for speed-sensitive applications.

IP (Internet Protocol) – Routes packets of data from source to destination.

ICMP (Internet Control Message Protocol) – Sends error messages and operational information (e.g., ping).

ARP (Address Resolution Protocol) – Maps IP addresses to physical MAC addresses.

SSH (Secure Shell) – Secure remote login and command execution on devices.

24. Due-diligence

way to analyze and mitigate risk from a business or investment decision.

25. SOAR (Security Orchestration, Automation, and Response)

technology helps coordinate, execute and automate tasks between various people and tools all within a single platform.

This allows organizations to quickly respond to cybersecurity attacks, observe, understand and prevent future incidents, thus improving their overall security posture.

Tools and processes that automate and coordinate security incident response.

26. Role of ITAM in Zero Trust Security Models

Zero Trust is a cybersecurity strategy- Everyone and everything is read as a threat until proven otherwise.

27. Cyber Asset Attack Surface Management (CAASM)

Continuous monitoring and management of all cyber assets to **reduce potential attack entry points.**