IBM CySec Architecture Series

[Tuesday, 1st July 2025]

▼ Video 1: CySec Architecture Principles

Principles to FOLLOW [5]:

1. **Defense in Depth principle :**
   → Defense in Depth is all about not relying on any SINGLE security mechanism to keep the system secure.

EDR - EndPoint Detection and Response [capabilities].

SPOF - Single Point of Failure.

---

2. **Least Privilege Principle :**

   → Granting ACCESS rights ONLY to people that require them, and are authorized to do so- inorder to carry out their duties and justify it, however, even so, only for as long as they require those rights [NOT indefinitely].→ Granting ACCESS rights ONLY to people that require them, and are authorized to do so- in order to carry out their duties and justify it, however, even so, only for as long as they require those rights [NOT indefinitely].

3. **Principle of Separation of Duties :**

   → No Single point of Control [Administrative Rights / Access Control].

4. **Principle of Security by Design :**

   → Security must be a foundation and key characteristics of architectural design right from requirement gatherings and designing till testing and in-production, and ***NOT*** just a garnishing at the very end for the sake of it.

5. **KISS [keep it simple stupid!] Principle :**

   → The job is not make it complex and hard unnecessarily, because that makes it easier for BAD guys to break in and harder for GOOD guys to work around.

   If bothered unnecessarily, people often are frustrated and by-pass all the security mechanisms, altogether just to download a time management software for example.

Principles to AVOID :

- **Security by Obscurity :**

  → **Security != Secrecy/Secret.** Absolutely be terrified and run away as soon as you see a BLACK BOX *[can only see the output and not the mechanism of its working]* mechanism or thing of security. Always instead prefer GLASS BOX *[Can see how the mechanism works but the confidentiality is preserved because of the secrecy of key and not the secrecy of operations]* philosophy of security mechanism.

▼ Video 2: CIA Triad

THE CIA TRIAD stands for ;

▼ Confidentiality

Ensuring information is accessible only to authorized individuals and preventing unauthorized disclosure.

→ Two important areas of concern:

i. Access Control [Authorization / Authentication]

ii. Encryption

▼ **Integrity**

Maintaining the accuracy and completeness of data, ensuring it hasn't been altered or corrupted without authorization.

▼ **Availability**

Ensuring information and systems are accessible and functional when needed by authorized users.

▼ Video 3: CySec Architect

▼ ROLE & MINDSET

> 💡 Normal IT Architect thinks about how a system will work. v/s CySec Architect thinks about a how a system will fail.

Cybersecurity Architect has to first understand how the system is going to work or they don't know how it might fail.

If thinking Cybersecurity architect, think *whiteboard* rather than keyboard, also *how would such 'xyz' system might fail and what could be done to prevent that.* [It's never gonna be 100% though].

▼ TOOLS

Some of the important diagrams that CySec architects use, in particular are three:

- Business Context Diagram:

  → Illustrate relationships among different entities in the business environment/system.

  eg. interdependent-relationships between entities such as Buyer, Trader, marketer, building etc.

- SYS (System) Context Diagram:

  → Business Context diagram is decomposed further into how it would look like in a SYSTEM [actually just a part of the system] illustrated via SYS Context diagram.

  eg. Project management, financial management, blueprints, permitting system, GUI etc.

- ARCH (Architecture) Overview Diagram:

  → A further decomposition of how Systems [illustrated via SYS Context] would be further enabled and implemented in a micro sense.

  eg. Project Database, Scheduler, Report generators, Alerts etc.

> 💡 All the 3 Diagrams mentioned are in a *lingua franca* among CySec architectures.

> 💡 Frameworks: **NIST CSF**, try reading about it.

▼ DOMAINS

Seven Domains (to be further discussed entirely in depth) are namely :

1. User
2. Endpoint device
3. Network
4. Application
5. Database
6. Monitor
7. Response

▼ Video 4: Identity & Access Management [I AM]

→ *DOMAIN 1 : "USER"*

▼ BASE [Foundational layer]

- **DIRECTORY** [DIR] - stores user information, containing some sort of database, schema and protocol that allows data retrieval and data writes.

  → Generally in real world scenarios there are no single directories (database) for an entire enterprise, there are multiple databases and thus- to be able to navigate the interdependencies among each of those sub-directories we need *SYNCHRONIZATION* (protocol/approach).

- **LDAP** - Lightweight Directory Access Protocol.

▼ 4 A's [of identity and access management]

▼ ADMINISTRATION

Purpose: Identity Management / Identity Governance.

> 💡 To create a system that efficiently grants access rights is great, but now it is required to create a system more efficient at removing those access rights , because that's where the security exposure exists.

▼ AUTHENTICATION

' WHO ARE YOU? ' - we can determine so based upon:

- something you **KNOW:** Password or PIN [lesser regard in modern times].
- something you **HAVE:** Access Card or Mobile Phone.
- something you **ARE:** **Facial** Recognition or Biometrics.

→ Best is to use MFA - *Multiple Factor Authentication* or TFA - *Two Factor Authentication.*

→ Trends seem to shift towards *password-LESS* authentication.

▼ **AUTHO**RI**Z**ATION

' WHAT ARE YOU ALLOWED TO DO? ' - we can determine so based upon:

→ RBA - Risk Based Authorization.

→ AA - Adaptive Access, meaning its NOT simple in or out, rather you can perform actions under certain *circumstances only* and not others. for eg. location, request type, request nature/amount, frequency etc.

PAM - PRIVILEGE ACCESS MANAGEMENT ***[special case]*** :

Course of Problem:

People with super, root or sudo privileges such as ROOT Admin, SYSAdmin, DBMSAdmin NetworkAdmin etc. who are responsible for management and maintaining the *CIA triad* of the organization in a sense can actually translate to *huge vulnerabilities* from being the protectors of sought. That's exact where **PAM** comes into picture.

How it works (helps) :

All the varying, different admins have to log in into PAM system and only remember their own credentials for the system, all the other actual DBs, NWs, or Repos can have different credentials known to PAM system, which are only granted to the ADMINs if they are once verified using MFA or TFA or other reliable methodologies. After each use by the admin the password and username are changed. VOILA!!!

Solves **4** major problems:

1. Know exactly who did the wrong if multiple people can access DIRs [Accountability].
2. Termination/ Leaving of ADMIN from enterprise doesn't matter, and is not a potential security threat.
3. Password change after each use.

4. Constant monitoring of each ADMIN.

▼ **AUDIT**ING

Here we go back and check i we actually did the previous 3A's correctly.

Logging each activity, touch, modification, access, each key stroke and cursor movement essentially. To trace back and replay exactly what had happened in what order by whom, under suspicion, analysis, or *worse*- post incident identification.

UBA - User Behavior Analytics.

UEBA - User Entity Behavior Analytics *[capability]*.

What if some members of one organization have to access info/resources of other cloud provider, SaaS, or another Business Client etc.?

→ The BASE + 4A's can be extended into other identity domains, can be achieved by **FEDERATION CAPABILITY.** ***Federation capability*** would all those members to log into the *Organizational* system, which would then as an identity provider for the members be able to access the external systems as maybe service providers for example. All of this can be achieved in an industry standard way and there are protocols defined to achieve the same.

▼ Video 5: EndPoint Device Security

→ DOMAIN 2 : "ENDPOINT SECURITY"

> 💡 **Visibility** and **Controls** are keys to security, if you can do both of those, you have a sincere fighting chance.

▼ What are EndPoint Devices?

Mobile Phones, Smart Watches, Server Stations, Proxy Servers, IoTs, basically any electronic device with computing prowess *[Hardware]- Expands the size of attack surface (potent).*

▼ EndPoint Management Systems [Controls].

- ▼ Inventory [Hardware/Software]

  eg. track of all registered/access granted *to* **devices** and their OS and the OS versions as well.

- ▼ Security Policy

  eg. must have current ‘n’ or ‘n-1’ security/update patch installed.

- ▼ Patching

  eg. must apply all the security patches released till day.

- ▼ Encryption

  All devices with access to organizational network must have some or the other data encryption algorithm as means of primary security to theft/misplacement.

- ▼ Remote Wipe

  If device is stolen or misplaced, all the data on the compromised device can be remotely wiped out to preserve confidentiality.

- ▼ Location Tracking

  Finding out/ Tracking the location of devices that have been lost or misplaced.

- ▼ Anti-Virus / Endpoint Detection Response [EDR]

  Ensuring no malware/virus on the devices connected to the network.

- ▼ Disposal

  What would be the security provisions made off of disposing these devices.

▼ BYOD - Bring Your Own Device.

→ Only 2 types of organizations:

1. Either POORLY defined Programs
2. Or Well defined programs

REQUIREMENTS:

- **CONSENT**
- **SOFTWARE** [version, requirements, must not have *'xyz'* apps etc.]
- **HARDWARE** [Types of Devices allowed and when not allowed]
- **SERVICES** [for eg. *must* use organization cloud , another eg. not allowed to access internet through mobile phone, use organization Wi-Fi *only* etc.]

▼ Video 6: Network Security

→ *DOMAIN 3: "NETWORK SECURITY"*

▼ Firewall

For protection purpose 2 firewalls are sometimes recommended, one is internet facing and one that is *internal* facing. With strictly defined explicit rules and parameters.

▼ Packet Filtering

Based upon certain rules and protocols we filter out data packets.

[data packets include source address, destination address, port number etc. essentially filtering out based on certain parameters and rules on *Header Payload*]

▼ Stateful Packet Inspection

Inspecting the actual contents [data] of the data packets and not just the header payload which we did previously. It also has rules and criteria based upon which it accepts or declines.

▼ Proxy Server

Doesn't allow end to end communication between 2 endpoints, generally an *endpoint device* and a *server*. Rules and criteria can again be reinforced as well as data inspection can be carried out, for eg. avoid letting malware or SQL-injection queries be passed directly to the server. It can also be used for privacy concerns.

▼ NAT [Network Address Translation]

NAT translates local IP addresses to external IP addresses for single or multiple devices to maintain security as it looks all devices are on one single end point [IP address], it also allows seamless conversion or resolving of local IP to external [internet routable] IP address and vice-versa. Usually built-in all the modern home routers.

▼ Segmentation

It is about how firewall and other network architectures are used to achieve different levels of security?

Read about the following [when necessary, kinda helpful]:

- 1st Gen - Bastion Host
- TRI-Homed Network [Scalable + Cheap but Single-Point-of-Failure]
- Basic DMZ [De-militarized] (Costly + Complex but Defense in Depth)
- Multi-Tiered [Costly again, yet Defense in Depth]

▼ VPN

Basic idea: Secure Channel over an untrusted network like internet (zero control over), the same is accomplished by encrypting data, thus preserving confidentiality.

CON: Limited inspection of data packets.

There is a trend of moving from BROAD VPNs (Simple, catch all) towards → Application Specific VPN [Granularity, higher control]

▼ SASE [Secure Access Service Edge]

Relevant, modern and important aspect in consideration with subject of *Zero-trust*. It's some sort of secure capability that's delivered on the edge [near delivery point].

$$SASE = \frac{NETSEC + WAN}{CLOUD}$$

NETSEC - Network Security

WAN - Wide Area Network Capability (defined- software wise)

Why companies like it:

- Faster access to cloud apps
- Better security everywhere
- Easier to manage (one service vs. multiple tools)
- Scales with remote work

▼ Video 7: Application Security

→ DOMAIN 4: "APPLICATION SECURITY"

WHY?? *[Why to care about application security?]*

→ Essentially all relevant *CODE* has substantial level of complexity, which cause bugs and errors in code functionality, these bugs are access points to security vulnerabilities.

Statistical facts indicate that cost of resolving bugs from coding phase [beginning to code] towards testing phase in some cases tend to rise to 640x (times) the original cost of resolving the bug.

▼ DevSecOps [SDLC]

→ Shift Left Thinking [Security By Design, essentially introducing security layers/concerns at each step of DevOps or building/coding].

→ Collaboration, more automation and a lot of feedback loops to reduce potent costs incurred.

▼ Secure Coding Practices

→ OWASP.org [OWASP Top Ten List - give that a read]

→ Trusted Libraries [doesn't eliminate the risk, but helps immensely]

→ Standard Architectures

→ SBOM [Software Bill of Materials]

- Components being used,
- Libraries and Origins of the components and libraries used,

- Dependencies that exist among components and how do they translate and how are they spelled out,
- Versions of each component and interdependencies that exist.

▼ Vulnerability Testing

▼ SAST [Static Application Security Testing]

Referred to as 'WHITE BOX', allows to peek in the working of the source code [earlier on in SDLC].

▼ DAST [Dynamic Application Security Testing]

Referred to as 'BLACK BOX', instead of source code, it obscures [*hide*] the source code [later on in SDLC].

→ It's actually not either SAST ***OR*** DAST, instead think about it in sense of **BOTH/AND** to help minimize the cost/losses. Because each finds somewhat different individual set of vulnerabilities and not just the same or unary set of vulnerabilities.

▼ Video 8: DATAbase Security

→ *DOMAIN 5: "DATA SECURITY"*

WHY?? *[Why to care about data security?]*

According to Ponemon Institute;

→ Average cost of a data breach worldwide - $4.35 Million

→ Average cost of a data breach in USA - $9.44 Million

→ Number of organizations hit by *more than 1* data breach - 83%

▼ GOVERNANCE

Essential goal, Recovery and data protection plans.

→ Policy.

→ Classification criteria.

→ Catalog of data.

→ Building a resilience plan.

▼ DISCOVERY

Finding and *actually* Recovering data.

→ Structured data - Database

→ Unstructured data - files, excel sheets, emails etc. (often overseen)

→ Network [Data Loss Protection - DLP, real time across multiple data systems]

▼ PROTECTION & COMPLIANCE

▼ PROTECT

→ Encryption

→ Key Management [Quantum-safe cryptography]

→ Access Control

→ BACKUP

▼ COMPLY

→ Report audits and compliance acc. to law.

→ Ability to retain record acc. to law

▼ DETECTION & RESPONSE

▼ DETECT

→ Monitoring system data and flow.

→ UBA [User Behavior Analytics].

→ Generating Alerts.

▼ RESPOND

→ Create and open a case.

→ DYN PB's [Dynamic Playbook].

→ Automation. [static]

→ Orchestration and Automation [Orchestration is *more* dynamic than automation]

According to CODB [Cost of Data Breach] Survey;

→ TOP 5 ***'things'*** that reduced the cost of data breach :

1. ML [Machine Learning]
2. DevSecOps
3. IR [Incident Response]
4. Cryptography
5. Ultimately, Employee Training [Humans are anyways [*commonly*] the weakest link in CySec]

▼ Video 9: Detection

→ DOMAIN 6: "DETECTION / MONITOR"

S = P + D + R

i.e. Security = Prevention + Detection + Response

[CIA Triad - WHAT we are trying to achieve?]

Above Eqn. is HOW we achieve the CIA Triad?

▼ SIEM [Security Information and Event Management System]

→ It is a type of software that helps organizations **monitor, detect, and respond to security threats** in their IT systems.

SIEM' functions [what it does]:

→ Analyze and co-relate information

→ Re-iterate rules and policies

→ Anomalies [ML/UBA]

→ Trends differentiation and analysis

→ Generate Reports

▼ XDR [Extended Detection and Response]

→ I**ntegrates and automates threat detection, investigation, and response across multiple security layers**—including endpoints, networks, email, cloud workloads, and servers—into a single, unified platform.

XDR is Up-Down approach as opposed to SIEM [Down-Up Approach].

Federated Search - searches local end-points and devices and scans them or asks them to raise alerts if specific or if any parametrized problems are generated among any based on certain rules or certain formulae or certain conditions that seem troublesome/bothersome. [High Quality Search - fetches data interrupts and analysis alerts *Just-In-Time*].

SIEMs tend to get more expensive as more data is feed into them.

XDRs need reasons to go out and search for certain parametrized problems in the 1st place.

Alarm coming in from SIEM might be a alert for XDR to then be skeptical and carry out an investigation of sorts.

It's NOT *XDR vs SIEM,* instead its more likely **XDR + SIEM.**

▼ HUNTING

RECONNAISANCE - gathering intel about a target system or network to find vulnerabilities that could be exploited. [1st Phase]

MTTI - Mean-Time-to-Identify [generally, *200 Days*]

MTTC - Mean-Time-to-Contain [generally, *70 Days*]

→ MTTI + MTTC = Since, when you were attacked until you finally recovered (*approx. 270 Days*).

If not able to prevent an attack, at least become aware of it sooner, the way to do so is by ***threat hunting***.

Investigation - *REACTION* to an incident.

Threat **HUNTING** - *PROACTIVE*

Threat HUNTING = EXPERIENCE + INSTINCT → HYPOTHESIS + TOOLS → ***EARLY DETECTION***

▼ Video 10: Response

→ *DOMAIN 7: "RESPONSE"*

S = P + D + R

i.e.. Security = Prevention + Detection + Response

[CIA Triad - WHAT we are trying to achieve?]

Above Eqn. is HOW we achieve the CIA Triad?

MTTC - Mean-Time-to-Contain [*Response* Portion i.e. try to **reduce** MTTC]

▼ INCIDENT RESPONSE [IR]

→ Traditionally, RESPONSE procedure is Called ***IR*** [Incident Response].

Traditionally, its also made to use largely a manual process, relying on *'heroes'* with GUT feelings and a way of getting things done their way. Although, that doesn't scale well and isn't repeatable.

They **TRIAGE** the alerts and then **REMEDIATE** them.

▼ Security Orchestration Automation and Response [SOAR]

→ MODERN, making use of automation scripts and conditional programming algorithms to allow replicability and scalability.

---

1. CREATE a CASE.
2. XDR and/or SIEM ***modify*** and ***assign*** the CASE to investigating officer/lead, they also attach indicators of compromise [artifacts].
3. TRACK the CASEs.
4. INVESTIAGTE [DYN PBs].
5. REMEDIATION steps.

Black Swan Events - Rarely occur or FOAK [First-of-a-kind] Events].

→ Requires partial or full ORCHESTRATION.

White Swan Events - Regular, easily automated and/or configured.

→ Requires AUTOMATION and little to NO human interference.

- **NOTIFY**
  - Type of DATA breach

    Names, Mobile Phone, Passwords etc.
  - Geography

    Where did the security breach occured from, Nation-State-City- Area... as close as possible.
  - Regulatory Authorities

    eg. GDPR [General Data Protection Regulation] part of EU.

> **Jeff Crem [Author of the 10 part Cybersecurity Architecture video series] *in collaboration* with IBM.**