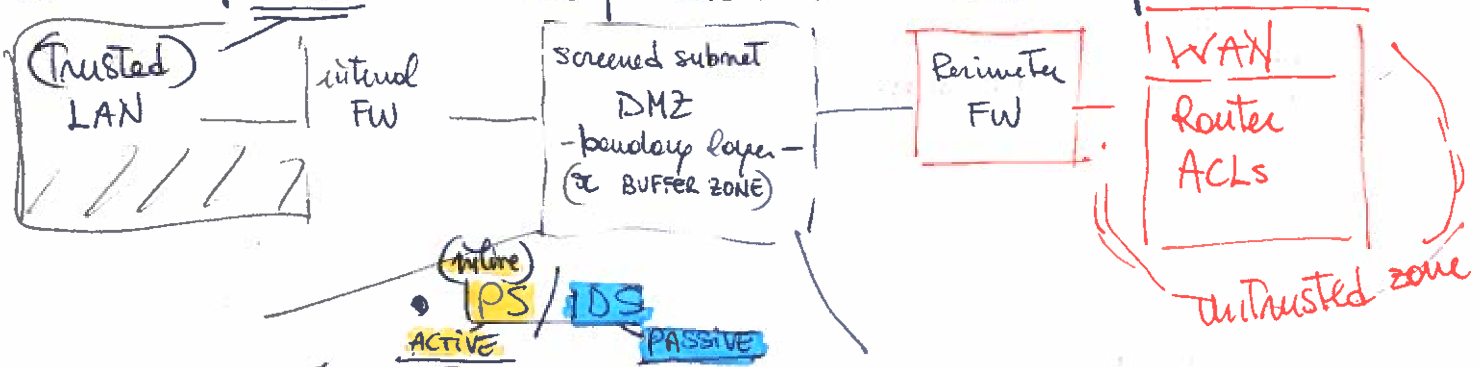
Comptia 701

D3- ArchiTecture

Cap. 11 /28

Sec. Principles

The creation of Sec. ZONES to ensure all of our data is not in the same area of the network.



- Jump Server : intermediary devices for the remote administration and management of critical components. Via SSH or RDP (Remote DeskTop Protocol)

- Proxy Server: (forward) internal ⟶ external [URL filtering, Content filtering, Web caching...]

- Reverse Proxy : internal ⟵ external performs the Authentication and decryption of a secure session to enable it to filter the incoming traffic.

- Load Balancer : balance the load when there is high volume of Traffic coming into the network.
  - ⟶ L4 : only forwards The Traffic by using The packet header (dest. addr. and port number)
  - ⟶ L7 : based on content-based routing . web apps, APIs... Application Level.
  - ⟶ method : least utilized host, DNS Round Robin, Sensors (IDS) ...

- Data Protection ⟶ all the data should be FDE (Full Disk Encryption).
  - ⟶ data backup ⟶ GZRS (Geo-Zone Redundant Storage).
  - ⟶ DLP is a must
  - ⟶ VPN can be used To access data

Port Security ⟶ Ethernet cable "restrict access To the switch"

- STICKY MAC : by storing the MAC addr. of authorized devices
- 802.1X auth. = authentication via RADIUS server before a connection is established: using CERTIFICATES.

- Extensible Auth. Protoc. (EAP)
  ↓
  makes 802.1X auth. INTEROPERABLE across various devices
  - EAP- TLS
  - EAP- PEAP (protected extensible Auth. Protocol)

1/2

FW

1° first Generation
FW = simple packet filters

2000s : stateful FW (L4) TCP/IP = able to track the state of network connections by monitoring a state table. → RECORDED ALL PACKETS

2°

→ UTM - Unified Threat Manag. - stateful FW + GW antivirus, IDS, spam filtering ...

Application level

→ VPN

concept of "All in one"

3°

2008 : Palo Alto : NGFW (L7) capable of deeper inspection = IPS
—FULL STACK VISIBILITY—

- new dimension of FW policies
- block malicious content
- Capable of SSL/TLS decryption

2020 : 4° Gen. : ML powered NGFWs.

Remember that SSH is the most secure and versatile remote access protocol and can be enhanced by implementing SSH keys. → Linux : > ssh keygen -t rsa → ~/.ssh/ directory

TUNNELING = Technique used to secure and encrypt data over potentially untrusted network.

IPSec (1996) → it's used in VPN : IPsec is security over IP protocol = is a L3 OSI model = RETE

TLS → Transport (L4)
SSH → Appl. L7

IPSec PACKET is formed of two portions :

1- Auth. Header (AH) : which provide data integrity → hashing alg.

2- Encapsulated Sec. Payload (ESP) : in which the data is stored and encrypted using symm. alg. (3DES, AES...)

The Internet Key Exchange (IKE) (first phase) is the session uses DH over UDP port 500 to create what is known as 'quick mode'.

Second phase the data is encrypted (BDES, AES).

There are three different IPSec modes :

1 Tunnel : a user create a VPN session from a remote location. There is the Authentication (certificates, kerberos...)
CIFRA = PROTEGGE TUTTO IL PACCHETTO IP

2 Always-on : creation of a site-To-site VPN (P2P) → the session is set to always-on, available all the time.

3 transport : using client/server communication.
PROTEGGE SOLO IL PAYLOAD!

Multifaceted challenge of data protection

DATA TYPES

much data is subject to specific LAWS and REGULATIONS => Regulated Data

- PII = email, driving license number, mobile phone number ...
- PHI = medical history, diseases, Treatments...

↳ IP - Intellectual Property: Trade secrets, patents, or copyright material

Non-Disclosure Agreements (NDAs)

EU → GDPR

USA → HIPAA (health)

California → CCPA (data rights and privacy)

UK → Data Protection Act

DATA CLASSIFICATIONS

they categorize data based on its sensitivity and the POTENTIAL RISKS ASSOCIATED with its EXPOSURE.

who should have access

BREACH

(1) Sensitive data: "privileged data"

(2) Confidential data: R&D (Research and Develop.) and legal data are classified as confidential.

(3) Public data: available to anyone.

(4) Restricted data: should have limited access and necessitates heightened security measures.

(5) Private data: available to a restricted circle of Trust.

(6) Critical data: Backups or encrypted keys → could cause operation failure if corrupted or lost.

DATA STATES

The context in which data resides and how it's accessed.

at rest : is not being used -> it's static.

in transit : Traveling across networks => TLS, SSL, HTTPS

in use : in RAM - data in PROCESSING -

SOVEREIGNITY : any data that has been created is subject to the LAWS of the region in which is created

Methods to Secure Data

- MASKING : replacing / hiding information with fake... still preserving the data's original format and structure.

- TOKENIZATION : replacing 'patient names' with pseudonyms. Replacing sensitive data with TOKEN to preserve data integrity and ensures that individuals cannot be directly identified.
  -> it's commonly used ~~of the~~ card payment.

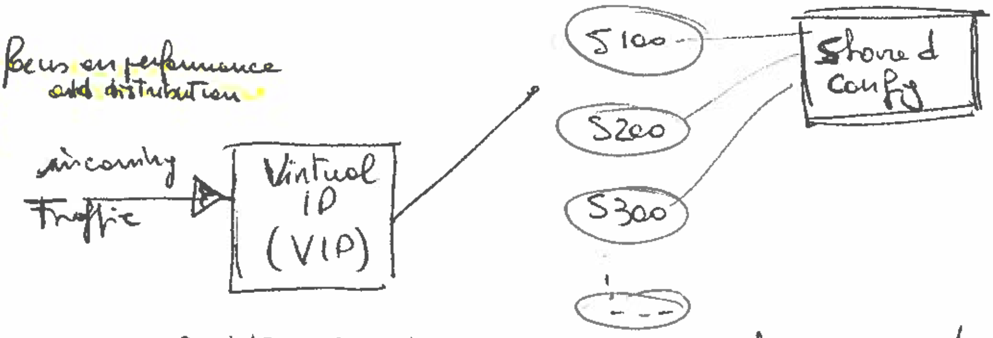
Comptia 701

Resilience and Recovery

DS ARCHITECTURE — Cap-13 1/2

HA - High availability

- network load balancer — focus on performance and distribution



type 1 : active/active there must be at least two, load balancers function together as a dynamic array.

type 2 : active/passive has one active and one passive (in standby mode).

- CLUSTERING — focus on RESILIENCE and HA — "failover", grouping multiple servers (or nodes) together to operate as a single system → they share a common QUORUM DISK

Site Considerations :

1 HOT SITE* : is the best for site recovery. IT's a fully operational site that mirrors your primary infrastructure. IT's the most expensive option to maintain.

2 WARM site : is fully functional, but data synchronization typically lags behind → delay of 3-4 hours compared to the primary site.

3 Cold site : is empty. You have power + water : no staff, equipment and data.

DATA (SOVRANITÀ) SOVEREIGNTY : Is an important consideration in disaster recovery planning, especially when choosing a recovery site, particularly HOT SITES* → Data stored and processed.

Multi-Cloud systems = Resilience against downtime => RESILIENCE + complexity.
multiple

COOP - Continuity of Operations

Is a strategy that enables organizations to continue essential functions and services during and after disruptive events.

1 Build RESILIENCE and REDUNDANCY
2 effective communication is vital during crisis
3 Training personnel to carry out their roles during disruptions.

Comptia 701

TEST

Cap 13/28

1) How to test a "Incident Response Procedures" (for a client):

- with least admin overhead: TableTop exercises are paper-based exercises in which the key stakeholders can evaluate each procedure with minimal setup.
- with enormous amount of admin overhead (to set up): SIMULATION is an effective evaluation method; IT mimics real events.

2) the CEO wants to determine the "staffing" requirements for the hot site, which BEST describes the CEO's primary objective in seeking this information?

- Capacity planning → to ensure the company's smooth transition and continued operation in the event of a disaster. — staffing needs —

3) A company has suffered power failures about once a week → affected BUSINESS OPERATION

it's now moving To Cloud because...

Geographic dispersion = spreading resources across various locations, which can be beneficial for a company experiencing frequent POWER FAILURES.

↓ IT provides REDUNDANCIES and ensures that BUSINESS OPERATION CAN CONTINUE FROM VARIOUS LOCATIONS, even if one faces a power outage.

Note. Cloud backup → DATA BACKUP

Redunt/backup power on-site → WOULD NOT IMPACT CLOUD OPERATIONS

4) intermittent power outages that last between 3-10 secs → UPS (Uninteruptable Power)

IT provides controlled power distr. to servers and networking equipment... protection against overloads → A managed PDU (Power Distributio)

5) Due to data compliance, we need to maintain a log of all incoming and outgoing EMAILS. This data must be retained for a period of three years.

Best Solution: JOURNALING

recording all incoming/outgoing emails in real time. This method is ideal for compliance, as it ensures that all email data is logged and retained for the mandated three-year period to meet the auditor's requirements.

other No solutions:
weekly/daily backups: would not provide real time logging of emails, they may lead to data gaps and compliance issues.

---

6) • Communication plan: is used to inform stakeholders discreetly during INCIDENTS.
- effective communication
- not using public channel such as WhatsApp which can be compromised.

• DISASTER RECOVERY plan: focuses on IT recovery strategies

• Incident Response plan: concentrates on responding to and MITIGATING incidents

• Business continuity plan: focuses on maintaining critical business operations.
- Focus: processi critici
BIA (Business Impact Analysis)

Identity and Access Management (IAM)

Provisioning user accounts: is the process of creating, managing and configuring user access rights.

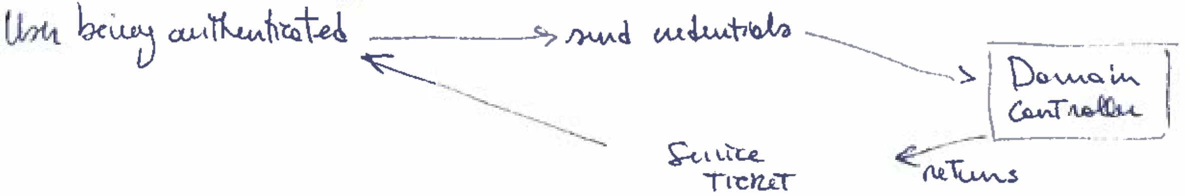
One of the most common types of user accounts is an account in Active Directory (defined as directory service)
it uses an authentication protocol called Kerberos.

ex. Microsoft's Active Directory ——→ uses a protocol LDAP (lightweight Directory Access Protocol)
to manage its objects.

- Active Directory objects are stored in X.500 format:
  We can have three values in X.500 objects:
  - DC (domain component)
  - OU (organization unit)
  - CN (common name) for any other object

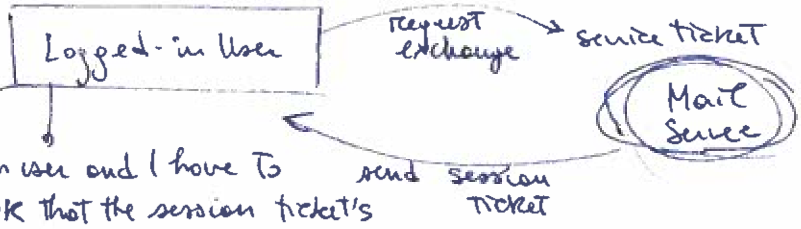
Each time an object is created in Active Directory, it gets an identifier called Sec. Ident. (SID), the next Updated Sequence Number (USN), and a timestamp.

Once a user account has been created, Active Directory authenticates via Kerberos protocol, which uses a process called a Ticket Granting Ticket (TGT) session.



- if Kerberos authentication fails, this is normally down to the user's computer time clock being out of sync with the domain controller by five minutes or more.
  - A NTP server can be placed on your LAN.

— Kerberos provides single sign-on (SSO) authentication, log in only once.
Then MUTUAL AUTHENTICATION (service ticket) process:



I'm user and I have to check that the session ticket's timestamp is within five minutes of that of the domain controller.

The user exchange their service ticket with the resource (mail server); it is called mutual auth. as both parties exchange tickets.

Single Sign-On (SSO)

. it's an authentication process. It's designed to simplify user experience by reducing the number of times users must log in to relevant applications.

Three authentication types that uses SSO are :

1 Kerberos → TGT to obtain "service ticket"

2 OAuth (Open Auth) : is an open standard for access delegation. ex. logging in AirBnb website using Google/Facebook platform.

OAuth via OpenID Connect ensure a seamless and secure user experience.

3 Security Assertions Markup Language (SAML) : XML-based standard used to exchange authentication and authorization data between third parties.

Access Control

is a framework used to ensure that only authenticated and authorized users can access the resources pertinent to their roles within an organization.

- Mandatory AC (MAC) : based on the sensitivity of data and the user's clearance level (Top secret, secret, confidential and restricted).

- RBAC : It is often employed within department where specfic role require access to resources, helping to minimize the risk of unauthorized access to sensitive information.

- Attribute-base AC (ABAC)
  based on user attributes. For example, a sw developer might have different Active Directory attributes such as job title, department, security clearance level, location, and access time.

- Discretionary-based AC (DAC)
  it's an AC model in which the owner of the object determines who is allowed to access it, the permissions are generally assigned via AC Lists (ACLs)

○ the principle of "Least Privilege" is a fundamental security strategy in which individuals are granted only the bare minimum level of access (or permissions) essential to fulfilling their job responsibilities.

Multi-Factor Authentication (MFA)

MFA elevates security protocols by necessitating the presentation of multiple verification factors:

# → Something
- you know: secret knowledge (PIN)
- you have: physical items ([illegible] Secure Tokens...)
- you are: personal traits (retina, fingerprints...)
- Somewhere you are: location-based factors

Hard authentication: tokens that are always in the user's possession and are never transmitted.
= physical

- smart cards
- Fobs/key fobs = NFC or RFID devices
- security USB keys
- SSH keys: it's an encrypted remote access protocol used by admin. (ex. To gain passwordless access to Linux server

Soft authentication: SW-based mechanisms, such as PIN, password... may be susceptible to phishing, keylogging attacks...

- One time Password (OTP): ex when you make online purchase, time expiry ~ 30-60 sec.
- Biometric auth
- Knowledge-based Auth (KBA) such as security questions...

Password Concepts

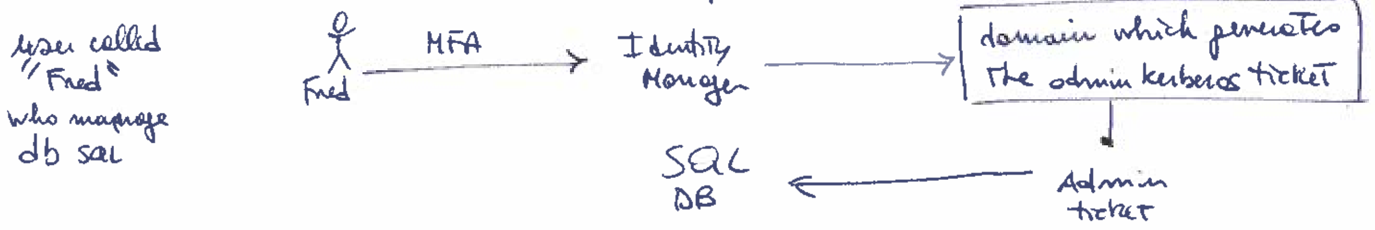
CompTia requires familiarity with all of these:

\ NIST recommends using passphrases (longer combinations of words) instead of short

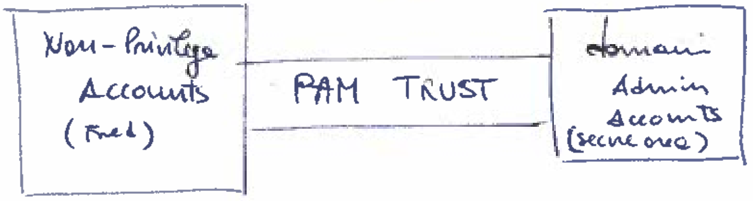
- password length = against brute-force attacks
- " complexity: lowercase, uppercase, numbers, special characters...
- " reuse / password history: prevent the recycling of old passwords
- expiry: requires users to change their password after a set period.
- age
  - min = Too frequently is not good
  - max = The milestone, the maximum period after which a user's password must be changed.
- account lockout: how many incorrect attempt a user can make (3-5)

PAM - Privileged Access Management

it's a practice that restricts and protects admin rights for root account.
With PAM, user accounts are given the equivalent of Temporary ticket with limited admin rights.


user called "Fred" who manage db sql
Fred
MFA
Identity Manager
domain which generates the admin kerberos ticket
Admin ticket
SQL DB

Once Fred has finished his admin Tasks or his Ticket expires, his admin privileges evaporate.



JIT - Just-in-Time permissions

\ Traditional privilege assignment often involves granting long-Term access right to users, which can become a liability.

\ JIT permissions are elevated on a Temporary basis:

1 I need permissions (privilege access), I'll ask a request To PAM system.

2 the request is routed to an approval workflow

3 once approved, The PAM Tool grants access for a predefined duration

4 after the Time limit for PAM expires, access is automatically revoked.

o password vaulting = privileged accounts are removed from The Active Directory and stored in password vaults (sw solution).

o ephemeral credentials = These are short-term, one-Time-use credentials. Any attacker must therefore not only discover these credentials; they must do so within this limited time frame.

THERE IS NO STORING PASSWORDS!

Test1: 66/90 - 26/03 - difficile, soprattutto lungo, studiare di più

In situations where *a user requires access to a specific resource that they lack permission to access*, which access control methodology:
-***Rule-based access control*** involves ~~applying a set of rules~~ to an access request, allowing a user to access a specific resource even if they were not explicitly granted permission.
-Unlike MAC, DAC, and role-based access control, rule-based access control does not strictly rely on explicit prior permissions for user access. SCADA

Eric wants to ascertain the *bandwidth consumption* and destination of traffic during a compromise. What technology can he deploy proactively to enable effective bandwidth monitoring?
-**NetFlow**.

User and entity behavior analytics (**UEBA**) tools are purpose-built for employing *behavior-based analytics*

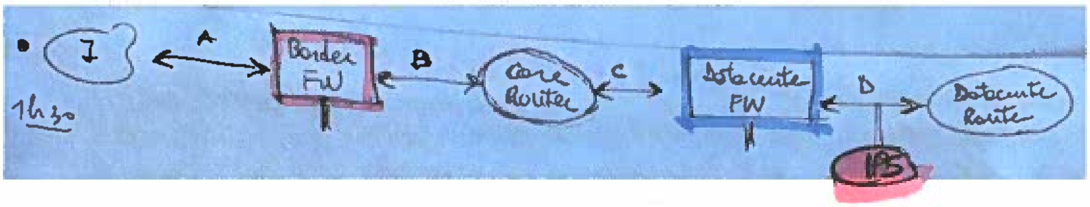
What are the required steps for John to transmit his Public key to another user?
The key can be easily shared using key servers or sent via email (including signature to ensure that belongs to the intended individual)

DS

As Alaina's company contemplates entering into a contract with a cloud service provider and seeks to evaluate the security of their services, which of the following methods is she likely to employ for the assessment?
-Review an existing SOC audit. Non è il SOC di Sicurezza Operativa !
Numerous cloud service providers typically restrict customer-initiated audits, whether conducted directly by the customer or by a third party. They frequently disallow vulnerability scans of their production environment to prevent service disruptions. Instead, many furnish third-party audit outcomes through a service organization controls (SOC) report or a similar audit artifact. *

DS

Among the following environments, which is the LEAST probable to permit the inclusion of a *right-to-audit clause* in a contract?
-A CSP.
In the realm of *datacenter co-location and facility rental contracts*, right-to-audit clauses are widely embraced as a standard practice, irrespective of the location.
Conversely, when dealing with cloud service providers, the likelihood of agreeing to a right-to-audit contract diminishes. Instead, these providers may furnish customers, and even prospective customers, with third-party audit data.



SCADA devices → (https and *TLS-enabled PROXY*) → Cloud Controller

During and extended power outages where generators are supplying power, common concerns include the **availability of fuel**, **maintenance** and ensuring **physical redundancy** (TO enable a second generator).

COOP = loss of **Facility**, **Personnel**, **Services**

* Upon completing an SOC 2, Type 2 (by Auditor) Audit ↦ org's posture = ATTESTATION

5	APPL.		
4	Trasp.	TCP/UDP	
3	rete	IP	
2	coll.	MAC	Datalink
1	fisico	ethernet	

L3 = IP
L4 = TCP = Transport

IPSec VPN = network level
TLS = Transport layer

race conditions scenario: TOC, TOU, *target-of-evaluation*

Cloud service providers have sec. tools → anti-DoS and enable logging

Bruce force = every combinations
Dictionary = commonly used *words*
Rainbow table = precomputed *hashes*

MAC = *users at a lower level should not be able to access files at a higher privilege level*
rule-based AC = rules, allowing a user to access resource even if they were not explicitly granted permission.
MAC = rely on explicit (admin) permission for user access
DAC = rely on explicit (admin) permission for user access;
DAC involves each data owner configuring their own security.
role-based AC (RBAC) = rely on explicit (admin) permission for user access

Cloud => **OAuth**: authorization service/protocol
OpenID: authentication protocol that verifies a user's identity; for Federated services (like SAML)
Kerberos: on-site authentication, commonly employed AAA protocols

fingerprint = something you ARE (not HAVE such as hw tokens, RFID cards…)

EDS: *behavior-based detection*
IPS: can identify network threats; they are not (ideally) designed for detecting behaviour on endpoint systems.

UEBA (User and entity behaviour analytics) = tool built for behaviour-based analytics, machine learning

---

WiFi → WPA3 Enterprise → 802.1X authentication (sia per dispositivi wireless che cablati)
utente client-end: avvia la connessione intraprendendo una transazione EAP (Extensible Auth. Prot.)
access point o switch: Authenticator
Server di autenticazione (solitamente ***RADIUS***): riceve le richieste di accesso alla rete e risponde:
Se il processo di autenticazione riesce → l'autenticatore designa la porta come "autorizzata";
Altrimenti → la porta mantiene lo stato di "non autorizzato", comporta il blocco di tutto il traffico non EAP.

Una volta che l'utente si è registrato per un certificato di infrastruttura a chiave pubblica (PKI) o ha confermato la validità delle sue credenziali, è autorizzato ad accedere alla rete. RADIUS verifica che dispongano del certificato o delle credenziali necessarie ogni volta che si connettono. Ciò aiuta a impedire agli utenti illegittimi di accedere alla rete.

T2

-Circumstances in which a device should be removed from the network?
The device's *encryption level* cannot meet the company requirements/standards (data confidentiality); it poses a significant risk to the network.
For legacy devices removing them from the network may not always be the best immediate solution for critical operational reasons.

-a company is hit by a tornado that damages critical servers. which plans first?
DRP to restore IT systems and operations after a disaster (recovering data…)
Incident Response Plan outlines steps to take immediately to minimize damage and restore services, but will not address server (IT) damage caused by tornado.
BCP focuses on essential business functions can continue during and after a disaster.
Communication Plan how to comm. with stakeholders during and after a disaster, should be carried out only after a disaster plan is underway!

e-commerce website availability even if there is an environmental disaster:
→Cloud infrastructure/hosting = HA + redundancy across multiple datacenters
→Geographic dispersion = across multiple locations to mitigate the impact of region disasters.
RAID: provides redundancy and fault tolerance for storage, but does not address availability during environmental disaster.

-Phishing
when attackers infect a website (public forum) -targeted group are known to visit-
→ **Watering hole attack**

email "competition winner: you won a holiday", then click triggered a down of a virus
→ **Phishing**
Spear phishing: when targeting a specific group rather then generic such as this case.

-What type of device does a network admin need to install to control internal access to the network whilst maintaing security?
→ Bastion host: typically act as gw for access to the internal network.
A Jump Server/Host: control/manage access but *it's not for control internal access.
A Proxy Server: intermediary between client devices and the Internet and *.
A FW: incoming/outgoing traffic based on FW's rules; *

-how to privately access portions of the network remotely without using a VPN. Other traffic must not be mixed with his connection:
→ **Jump Server**: isolating traffic, allows remote access to specific portions
RDP: does not prevent other traffic on the connection.
Reverse Proxy is used to authenticate incoming users and the decryption of traffic.

-CISO enters the server room → **Threat Hunting**: proactively searching for and identifiyng potential security threats or vuln. within an org's environment
Active Reconnaissance: *gathering info about a target system or network -given scenario-
Passive Reconnaissance: * without directly interacting with the target

Doc containing the duration of pentest → **SOW** statement of work (scope, deliverables…)

Load Chart → breaking down task - *manpower capacity planning, workloads distribution*
Gantt Chart → assessing IT infrastructure (not people!) - *technology capacity planning, it represents the timeline of tasks and their dependencies.*

DS ex of **risk transference**: any form of insurance, outsourcing or migrating data (Cloud)

ensure you are informed if the sys32 files have been altered → **FIM** (File Integrity Monit.)

SDLS phases
Develop: writing,
Test: testing and fix before deployment
Staging: deploying sw to a staging environment before deployment to production
Production: deployment to live production env for end-users

-a company is transitioning to the cloud and needs to open ports on the fw…
→ it introduces **a supply chain risk**: that arise from third-party vendors, services or processes involved in the supply chain.

*block incoming SSH conn from IP addr 140.107.20.1 → **ACL***
access list inbound deny 140.107.20.1/32 0.0.0.0 port 22

MFA: gait(something you do) - retina(something you are) - username(something you have)

PCI DSS compliant be subject to an annual audit
→ driven by regulatory requirement

-several DNS queries that are bypassing network sec methods, what type of attack is this?
Data exfiltration (= unauthorized transfer data);
instead of DNS poisoning which corrupts DNS cache to redirect session to fake website.

reduce the threat scope for a major customer, which implement first?
→ Zero trust within Data Plane (in this way no entity is trusted!!)
Segmentation does not directly reduce the overall threat scope, it splitting a network into smaller isolated network.

DS *a company has a SLA for its printer. the support company notifies that will require the printers to be taken offline for 4hs over the weekend in order to apply a maintenance patch. it will not affect uptime. What is support company requesting?*
→ Scheduled Downtime - a planned period offline for maintenance/updates
no maintenance window: that's a predefined period.

best ways to control access to a datacenter:
mantrap, access control vestibule, visitor badges(who are authorized to be inside).
(note that logs are for tracking!)

script = automation + orchestration

-suffering latency with VPN concentrator while establishing , they are looking for Cloud-based solution that will improve performance and flexibility with traditional VPN solution.

→ we should implement **SASE** **a Cloud native sec architecture** that combines network sec functions with WAN capabilities for remote users and branch offices.

"day-to-day" *-who backs up, encrypts and stores data* → **(data) Custodian** → Heimdall (custode/guardiano del regno di Asgard e Bifrost) -THOR-

responsible for labeling and quality of data → **Steward** → ~~[illegible]~~ Stoow con nome STEWARD dietro le sistema

for determining the purposes and means of processing → **Controller**

processing data on behalf of data controller → **Processor**

DS

-which has an impact on risk manag. decision?

ARO -annualized rate of occurrence - estimated freq at which a specific threat will exploit a vuln within a given timeframe

SLE monetary loss expected from a single security incident.

- Zero-trust control plane components utilizes rules to determine access to a service based on factors such as the security status of users' systems:
→ Policy-driven AC = rules
follow the principle of "threat scope reduction".
- minimizing the potential of compromised credentials - = continuous verification.

- Zero-trust model (network) = All comm. is secured, regardless of the network security zone it occurs in.

- Adaptive Authentic. = examines aspects like login context, geographical location ... } multi-device usage ere

Zero-trust = verification + validate level of confidence

Sec. Audit: focus on compliance -> external auditor -> compliance yes/no

Sec. Assessment: focus on monitoring risks -> report identified risks

• ATTESTATION = is an independent verification of an org's adherence to control or standards.

: internal audit -> dedicated org team

External -> required by government or regulatory -> third-party firm

---

Social Eng. Attacks:

• email is the #1 for entering ransomware org.

↓

• phishing is the mechanism.

→ physical: tailgating (no badging), shoulder surfing, dumpster diving.

↗ gathering information from ~~the~~ trash -> secure shredding paper.

↳ virtual: phishing, spear phishing, whaling, vishing, hoax, watering hole attack.

spear ↓ specific group

whaling ↓ executives

vishing ↓ voice

• smishing ↓ (mobile) SMS/text

these should be included in Sec. Training program:

- policy / handbook -> phishing awareness
- situational awareness -> evolving threat landscape .. no open email from unknown senders
- insider threat
- password manag. : reuse, strong, use passw manager!
- removable media and cables -> authorized device
- Social eng. used -> "the 7 principals of social eng."
- OpSec -> operational security principles: no unsecure Wifi networks etc

D4 – Sec. Operations

Secure Baselines 3 phases:

ESTABLISH →

- Identify assets
- Threat Modeling
- Benchmarks (vendor and industry)
- Risk Assessment
- Tailoring (there is no one fits all)

DEPLOY →

(eliminate human error!)

- Config. Manag tool
- AD Group Policy
- MDM Tool
- DevOps : CI/CD and IaC (ex. terraform...)
- Change Manag.

MAINTAIN

- Vuln. Scan. (1x month)
- Patch Manag.
- Config. Monitoring
- Baseline review
- Auditing [compliance] (1x year)

Hardening:

- Mobile devices: strong passw, app manag, OS updates, Remote Wipe.
- Workstation: 〃, disable unneeded services, least privilege access, anti-malware, host FW.
- Network devices: 〃, 〃, firmware updates, ACLs, segmentation (VLAN).
- Cloud infrastructure: IAM, encryption, logging and monitoring and secure config.
  ⟷ the standard today are: DevOps, CI/CD, infrastr.-as-code (IaC).
- ICS/SCADA: critical functions ⇒ Physical security!

Server → VM image / VM Template } third-party, CSP defined (Cloud)

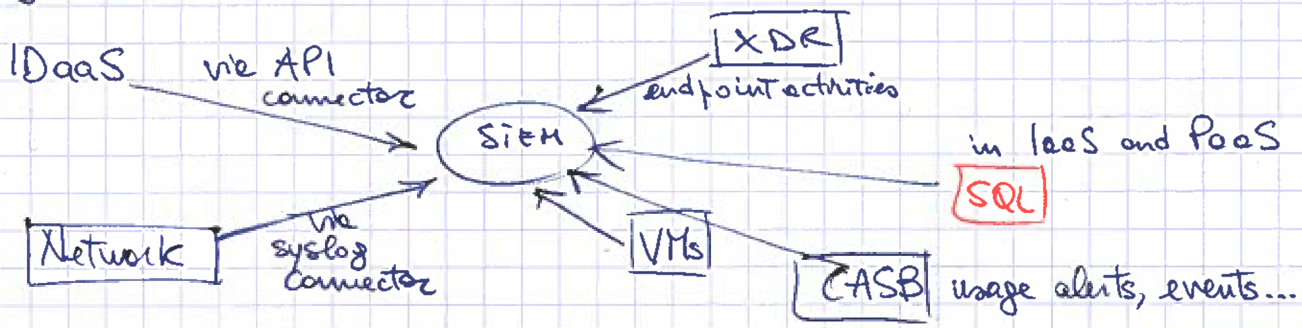
IaC is the manag. of Cloud infrastructure described in code.
↘ is a key DevOps practice used in CI/CD pipeline.

LEAP - Cisco proprietary (alternative to TKIP for WPA)

PEAP - encapsulated EAP within TLS Tunnel. "Protected".

EAP (802.1x) "extensible auth prot." - auth. framework for COMPATIBLE Wireless

Log ingestion process with a SIEM:



Asset Manag. Lifecycle: keeping track of your stuff, making sure it's secure

1) Acquisition/Procurement → e.g. checking for valid licenses to avoid pirated SW... (vendor's reputation)
- baseline configuration for HW (secure OS)

2) Assignment/Accounting → Who is responsible? person, department, Team...
- Classification (confidential financial data...)
- ensure appropriate "Access Controls" → lead to data breach.

3) Monitoring/Asset Tracking → inventory tracked in a config. manag. db (CMDB)
- enable tracking asset location, status...
- untracked asset can create blind spot?

→ maintain a uptodate Asset Register (periodic audit) via barcode or QR

4) Disposal/decommissioning → Sanitization

Destruction → securely destroy → prevent unnecessary exposure

- proof of... certification

Data Retention Policy → how long data is kept → Compliance

VA → requires running multiple Vuln. Scanners (network, weakness, passwords...)

Then whatever emerge - Vuln. reported - will be PRIORITIZED based on severity and relative likelihood.
(CVSS number score) and CVE

Remember that Static analysis requires access to source code;
Dynamic " not require access to " " ;

THREAT INTELL. SOURCES: → OSINT (free)
→ Closed/proprietary (vendor specific)
→ Vuln. DB - Shodan -, MITRE CVE list...
→ Dark Web (overlay to the existing internet)

IoC = "threat indicators" [pieces of forensic data]

What's a threat (intelligence) feed? a continuous stream of data about potential threats. (real-Time news)

- real-time exchange → AIS (autom. Indic. Sharing) a CISA (USA) capability (cisa.gov)
- TAXII = machine readable format, defines "how" STIX formatted messages are shared.
and
- STIX defines "what" is shared

→ SIEM, NGFW and IDPS solution may ingest Threat intelligence feeds

Pentest (is a more in-depth exam) requires special skills) is a "simulated" cyber attack → that's why it's intrusive.
↓
Footprinting (gather data)
ACTIVE: ping sweep, Tracert, nmap, extracting DNS info...
PASSIVE: browsing, google, whois lookup, social media...
What you can gather(?) → see OSINT framework website as map!

for logging and monitoring:
- AGENTS → server, endpoint endpoints → requires updates and consume resources!
- AGENTLESS → network (syslog data) without the need for a local agent

- Playbook (paperwork) a doc checklist → how to verify an incident : SOC
- Runbook (technology) → implements the playbook data into Automated tool : SOAR

SOC : Log Collector → SIEM → SOAR
SOC Analyst interprets SIEM and SOAR information.
Response automation via AI
→ reduce MTTD
- playbook + runbook
Rapid7
Splunk, QRadar...
DASHBOARDS

guarantee LOG non repudiation => hash the log and then digitally sign them

against copies verify consistency.

ATTESTATION = confirming / validating ownership : ex. driving license = Identity.

Before involving third-party vendor ← → address your technical issues?

↓ outsource its processes

trust?

transmitting your data?

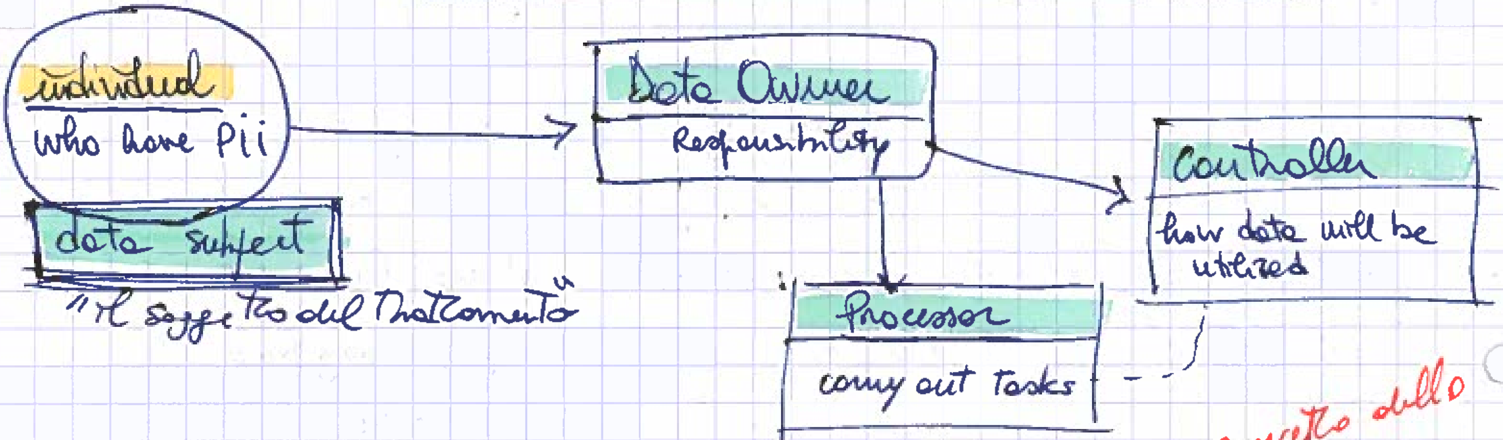
~~they~~ It may violate a NDA

Data RETENTION Policy → how long data should be kept

implemented WAF → against SQLi

AVOIDANCE → proactively thwart the RISK.

And preventing the attack.



"il soggetto del trattamento"

Thermostat device → "moving to a separate sec. zone"

~~over than "applying an industry standard baseline config."~~

concetto dello ISA 62443

CHANGE MANAG. PROC. = technical changes

- estimate the DOWNTIME → - all dependencies
  - all stakeholders (notification)

↓

Validate/test in testing env

BACKOUT plan is created by administrator and system owners.

it does not involve STAKEHOLDERS *

STAKEHOLDERS play a crucial role * in conducting IMPACT ANALYSIS, and determining the "maintenance window"

Allow list → difficult to manage

NOTE. "Scaling a cluster up or down" does not alter the system themselves, and it should not be restricted.

legacy apps → licensing costs is not considered because license is often unavailable!

(Architecture)

NIST Zero Trust Maturity Model :

assessments are conducted on identity, devices, networks, apps and workloads and data.
→ NO PHYSICAL SEC. sensors such as infrared data

Policy engine = determining access permissions to resources by evaluating policies established by admins along with data fro EDR tools, threat intelligence feeds...

↓

Policy enforcement point = no agent installed on client side / resource side

↓

authent. prompt to access a file server = Policy enforcement point [verify trust]

↓

Jack's laptop is considered a SUBJECT - including Users, Apps, devices.

- Audit => Operational ("day to day") Security Controls

Data Owner hold the most Senior position.

↑ subject

Processor

Controller

Risk Management Process

- risk exceptions : when an org accept a risk, even if it deviates from usual policies.
- risk AVOIDANCE : applying patches → eliminate a risk from the environment

if RTO = 4h and RPO = 1day → systems should be restored within 4h with a loss of 1 day's worth of data at most.

└ allowable duration before the potential data loss > org's Tolerance.

- Risk mitigation = minimize impact - ex. Segmentation for malware infection.
- to meet regulatory compliance req. → recurring (annual) Risk Ass.

(no "continuous" is too frequent?)

- Journaling facilitates db recovery transactions → affect the RPO (amount of data lost during trans.)

- masking in client-side code can lead to potential data exposures.

Credit card number ↳ MUST BE USED in server-side web application.

\ geofencing apps = determine location via GPS data and WiFi networks.

data obfuscation methods = masking, encryption, tokenization.

\ differential backup: all changes made since the most recent full backup.

\ incremental ↳ : " — " . the last incremental backup.

Path diversity is essential to ensure that connectivity to a facility does not rely on a single route. this measure is crucial in preventing the nightmare scenario that network managers fear, when a single accident or disruptive event, such as construction equipment in an unfortunate location, damages multiple fiber or copper paths...

Snapshot = VM disks, power state, VM's memory state... not the hypervisor's configuration

UPS + generator = best solution for longer outages occured. UPS systems backed up by generators.

\ failover test ⟶ force a fail over using live network or other systems

COLD site = a location that can be activated during a disaster (ex: Renting spaces), but lacks the necessary systems.

WARM site = possesses some or all of the infrastructure and systems required

HOT = fully functional environment equipped with HW, SW, data

↘ if RPO = 6h ⟶ incremental backups = every 6 h
recovery point obj
(compliant with RPO)
implementing backup every 1h may impact performance and recovery time

COOP = loss of access to a facility, loss of personnel, and loss of servers.

[facility, personnel (Human), Servers]

DDoS attack → network → log sources: FWs, IDS/IPS logs ...

authentication log
- Debian, Ubuntu : /var/log/auth.log
- Red Hat /var/log/SECURE

Windows:
- Audit account logon events: - Success
  - Failure

} Having logs for both attempts is valuable for incident investigations, especially in cases such as stolen credentials!

Serverless architecture eliminate the need for a system admin as the provider assumes responsibility for managing the function-as-a-service (FAAS) capability.

good SCALABILITY up/down to meet demand (call freq. increases/decreases)!

they are not well-suited for complex apps ⇒ are more effective for MICROSERVICES !

SPAN ports = Mirrored ports = ACTIVE and monitor (they are not passive and not inline!)

Build Apps without managing the underlying infrastructure! Serverless = FAAS (organization) Acme.com —ϟ— CSP < third-party* provider

Contract

*The most effective way to ensure that * adhere to the standards is by establishing contracts directly with the primary suppliers.

- Acme can conduct AUDIT & VA on vendors, only if it have a contractual relationship.

*third-party support availability services as a RISK TRANSFERENCE, in which the support contract transfers the associated risk to the contractor.

- IPSec* [network layer] L3 (IP) = IKE (establishes the Sec. associations on both ends of a tunnel)
  - ESP (encrypt the packet) — confidentiality, integrity
  - AH (auth. the entire packet)

  } because AH does not encrypt, it's faster than ESP.

  } CONFIDENTIALITY + INTEGRITY + ~~AVAILABILITY~~

- Web Apps ⟶ TLS VPN (Transport L.) L4 (ease of use, it does not require client installation)

From SCADA devices to a Cloud based Controller → Set-up a TLS-enabled Proxy between the devices and the Server.

NGFW → no need to create specific rules for each attack → THREAT FEEDS, admin can leverage rules that automatically block emerging threat by utilizing services like "IP reputation".

UTM device = services like FW (1), IPS (2), antivirus/malware (3) ⟶ no SD-WAN service

Architecture Models

decentralized approaches : increase resilience by mitigating the impact of failures in a single location.

Hybrid Cloud Design : the challenge is an increased complexity (cost, regulatory, visibility ...)

↳ in Cloud computing aligning resources = ELASTICITY ;

And customer are always accountable for their Data and Accounts.

Serverless model (Cloud) → no need to patch infrastructure, reducing the maintenance burden. Adopting DevSecOps practices can help to improve security.

IaC model → code changes issue ⟶ Version Control

managing and provisioning pc datacenters though definition file.

SDN - SW defined Networking - SDN Controller manages all devices such as SW, routers...

SCADA / ICS • Always segregate/isolate (air gap) the SCADA system from the main network to decrease the likelihood of being affected (by malware).

- Req.: legitimate access to the SCADA system → implement ACCOUNT USAGE AUDITING.
- legacy devices = recoverability, patch availability ;
- big Issue → inability to patch/updates SCADA/ICS.

[illegible]

Create Sec. ZONES

by considering ROLES and User Identities = NAC (network access control) tools
+
VLANs

Jump Server intermediary from untrusted zone outside a FW

- network traffic analysis - ⟶ network TAP.
|
no critical security function
↓
failure mode = FAIL-OPEN

NIPS on network
|
a copy of all the traffic flowing to NIPS network segment for analysis purposes

\IPS = in-line -> actively block traffic
- fail-OPEN = risking potential attack
- fail-CLOSED : in case of IPS failure, prioritizes downtime over a lack of monitoring.

\IDS = TAP

\IPS-ANOMALY-based -> APTs (deviation from baseline) [vs. signature/hash detection]

implementing of 802.1x = enabled WiFi infrastructure -> EAP protocol

PEAP

uses server-side certificates and employs tunneling

EAP
eliminates the need for client-side certificates

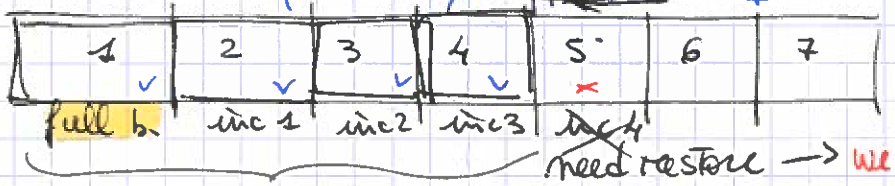
Replication as a strategy for resilience :

It creates a continuous copy of live data either asynchronously or synchr.
- It requires storage media that can keep pace with the rate of changes occurring.

Organizations ⟼ RPOs determine acceptable amount of data loss in the event of incident
⟼ RTOs, max. allowable duration for data recovery.
↳ play a crucial role in guiding Backup strategies.

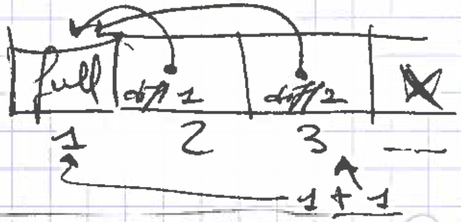
· Journaling (backup scheme) for a DB ⟼ by recording transactions in real-time as they take place. ⟼ Minimal data loss, only if the journal is not loss!

• Backup schedule = - generating a full backup once a week
- followed by incremental backup on the remaining days.



need restore → we need 3 + 1 (full) backups !

differential salva tutti i dati cambiati dall'ultimo full backup
ripristino : serve il full + l'ultimo differential



Incremental : salva solo i dati cambiati dall'ultimo backup (di qualsiasi tipo!).
ripristino : serve il full + tutti gli incremental successivi!