Resume | CompTIA - Sec+

1) phishing email attack ? yes/no? ——— it contains a "direct link" - phishing email

2) How to access "sensitive health record"?
FIDO (phishing resistant) auth. + TOTP alg. (for generating dynamic, time-sensitive passw).

NOTE. LDAP is for directory servers; EAP for Wi-Fi networks

3) OSINT requires "cross-referencing" and validating findings

4) where is possible to have a Hijack attack? (educating about) public WiFi!

5) Secure Cookies = HTTPS

Data exfiltration vs Blackmail (estorsione)
↓ unauthorised ↓ threating to release & expose sensitive information unless demands are met.

Root Cause Analysis vs Threat hunting = proactively searching for threats (OSINT, IoC...)
↓ ↓
reason behind an issue: time is different!
"Why attackers successfully brought down..." ⟶

- IoC vs. Predictive Analysis = analyzing dataset to identify threats] THREAT INTELLIGENCE
↓
various: outbound traffic, geo anomalies logins...

- Bug Bounty Program are not Pentest! : are Responsible Disclosure initiatives.

Cloud

SaaS	ready to use : SW via Internet ex. SAP
PaaS	you don't manage OS = DB dans SQL, DevOps
IaaS	you manage OS = container (Docker...)

Load balancing types:

1. weighted - least conn.
2. source IP hashing → same session server
3. resource based : CPU, network...
4. Round-Robin (RR) = list of predefined severs

Alternative VPN solution : SASE = CASB + SWG (Secure Web GW)

- SD-WAN is for improving network performance.

Pare-feu ← ACL
Filesystem ← DAC
OS ← MAC
Windows / Linux

email :

SPF
DKIM
DMARC

IPSec = transport / tunnel

AH	ESP	IKE

- Playbook* = SOC paperwork → "how to verify an incident".
- Runbook = SOAR technology → "implement the playbook*".

Resume 1 CompTIA Sect

agent
- based = EDR
- less : no install. → using networking : "pull comm. style"

user
- UN intentionally spreading incorrect facts = MISINFORMATION [like ChatGPT]
- IN tentionally " " " = DISINFORMATION [like WAR]

Bluetooth attack:

Blue
- Jacking : push malicious msg
- Snarfing : public place → device in discoverable mode, and obtaining data.
- Bugging : backdoor attack.

SNMP for monitor network devices → SNMP V3 Prefer : (encrypt credentials)

Threat intelligence feeds:
- TAXII = machine readable format "how"
- STIX = defines "what" is shared