

# Resume | ContiVA - Sec +

- 1) phishing email attack? yes/no? \_\_\_\_\_ it contains a "direct link" - <sup>phishing email</sup>
- 2) How To access "sensitive health record"?  
FIDO (phishing resistant) auth. + TOTP app. (for generating dynamic, time-sensitive passcodes).  
NOTE. LDAP is for directory services; EAP for Wi-Fi networks
- 3) OSINT requires "cross-referencing" and validating findings.
- 4) where is probable to have a MITM attack? (educating about) public Wi-Fi!
- 5) Secure COOKIES = HTTPS

Data exfiltration vs Blackmail (ransomware)  
↓  
unauthorized      ↓  
threatening 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:      ↓  
"why attackers successfully brought down..."      → time is different!

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

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

# Cloud

③ SaaS	ready to use : SW via Internet ex. SAP
② PaaS	you don't manage OS = DB, some SaaS, DevOps
① IaaS	you manage OS = containers (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 servers

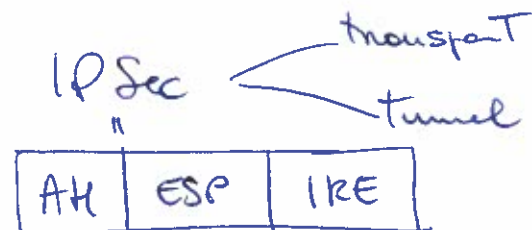
Alternative VPN solution: SASE = CASB + SWG (Secure Web Gateway)

SD-WAN is for improving network performance.

file-owner	←	ACL
file system	←	DAC
OS	←	MAC
Windows/Linux		

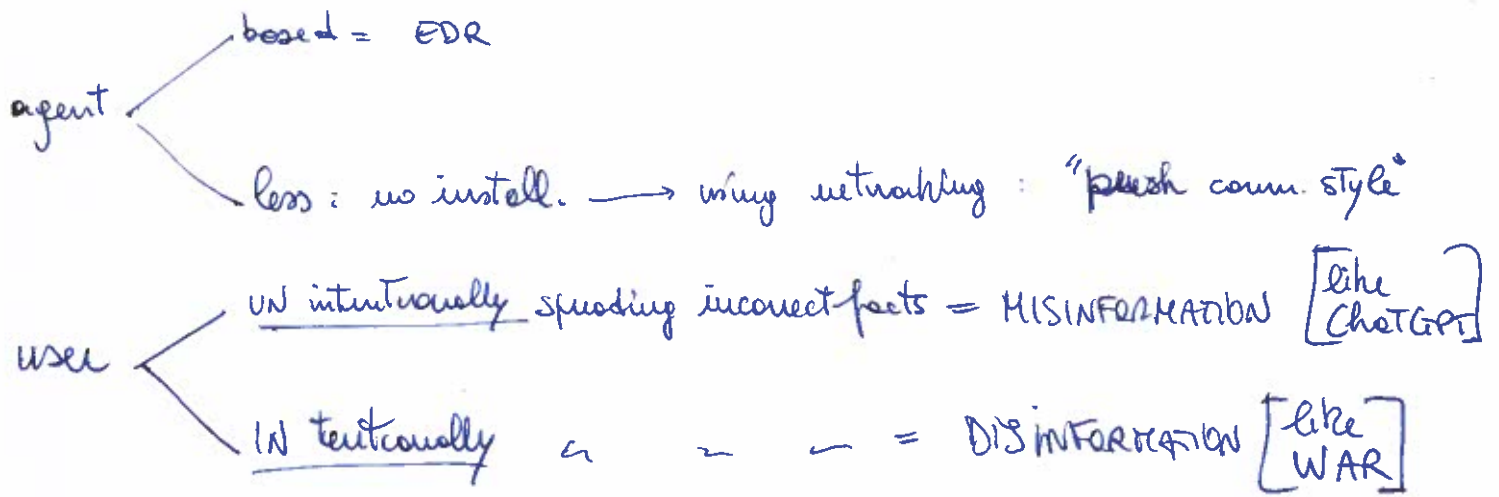
email:

SPF
DKIM
DMARC

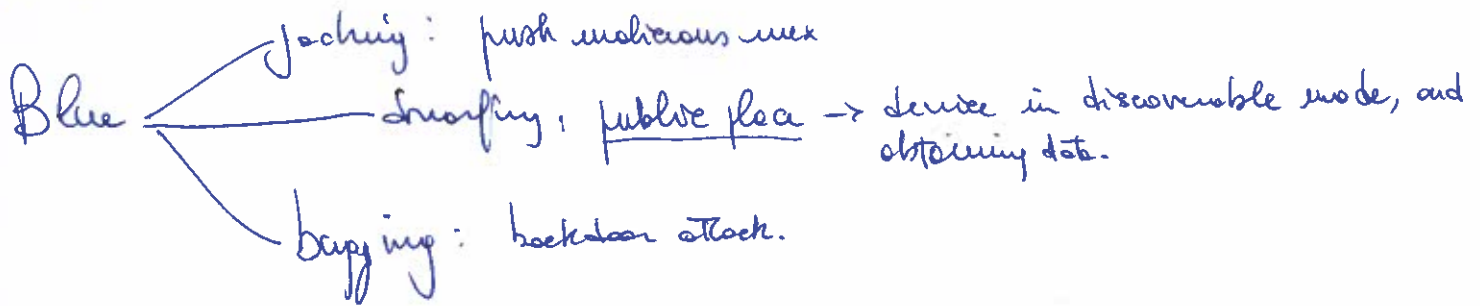


- ★ Playbook = SOC paperwork → "how to verify an incident".
- ★ Runbook = SOAR technology → "implement the playbook".

## Resume - Contra Sect



Bluetooth attack:



SNMP for monitor network devices → SNMP v3 profile: (encrypt credentials)

threat intelligence feeds:

- TAXII = machine readable format "how"
- STIX = defines "what" is shared