SOCaaS Design

1. Customer Profile

Industry: Law Firm (Mid-sized, Lebanon-based, 50+ employees)

Size & Infrastructure:

- HQ with on-prem endpoints (PCs, laptops)
- Cloud-hosted Windows Domain Controller (Google Cloud)
- Remote access secured with Tailscale VPN
- Mix of local and remote staff handling sensitive case data

Top Threats

Credential Theft & Brute Force on Remote Access

- Context: Lebanese law firms rely heavily on VPN and O365 for remote work. Attackers frequently target weak or reused credentials to gain access. A successful brute-force attack could expose confidential case data.

Privilege Escalation in Active Directory

- Context: Once inside, adversaries may escalate privileges by adding themselves to Domain Admins or modifying Group Policies. For a law firm, this means attackers could disable logging, alter evidence storage, or maintain persistence.

Insider Threats Driven by Economic Crisis & Bribery

- Context: Due to Lebanon's financial instability, employees under economic pressure may be bribed to create shadow accounts or exfiltrate sensitive client files. This risk is heightened in law firms where case data carries financial and political value.

Email Spoofing & Legal Document Fraud

- Context: Attackers in Lebanon frequently spoof domains of law firms or courts to trick attorneys into opening fake subpoenas, settlement notices, or client instructions. Such fraud can lead to disclosure of sensitive case data or unauthorized fund transfers.

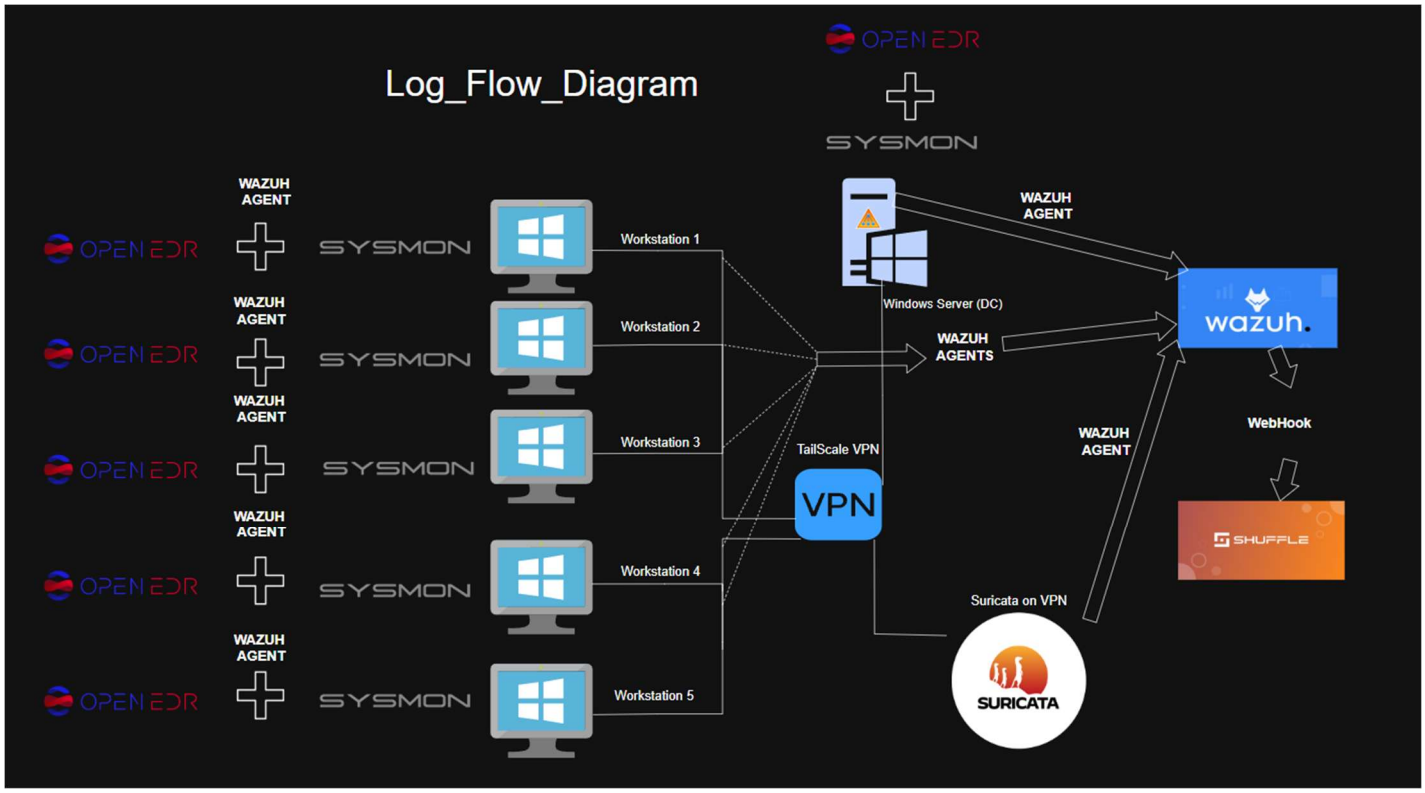
Ransomware & Persistence Mechanisms

- Context: Regional ransomware campaigns (LockBit, ALPHV) have targeted SMBs and legal entities in MENA. For a law firm, ransomware downtime can halt trials, breach client confidentiality, and cause reputational collapse.

2. Log Source List

Device	Log Types	Collection Method
5 Windows Endpoints	Windows Security Event Sysmon OpenEDR	Wazuh Agent
Windows Server (DC)	Windows Security Event Sysmon OpenEDR	Wazuh Agent
Suricata IDS	Network Alerts	Wazuh Agent
Shuffle SOAR	Playbooks	API Logs
Wazuh SIEM	Correlated Alerts	Webhook to Shuffle

3. Log Flow Diagram



Note: Diagram can be found on drawio file in deliverables within “Customer_Topolgy.drawio”