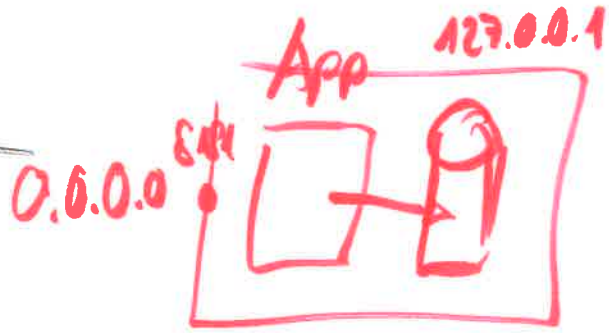
Cyber Defense

9.10.2024

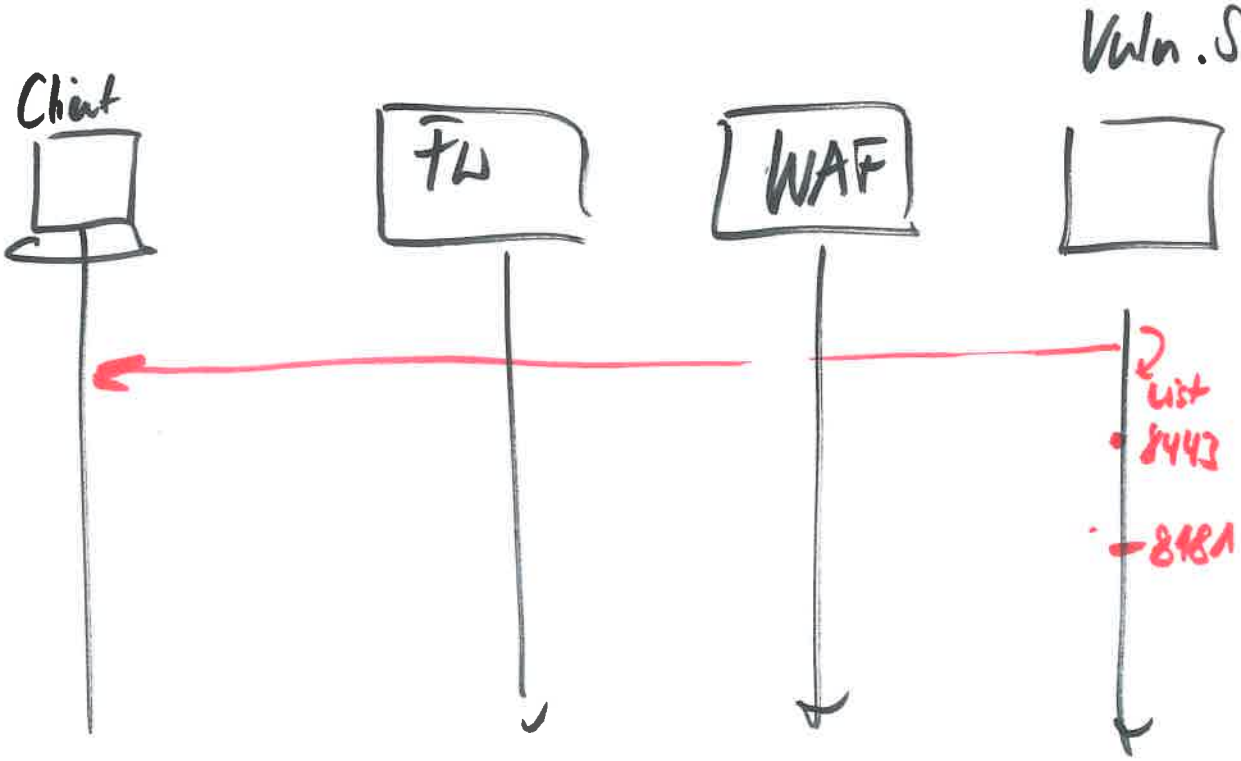
APT / Wazuh / SIEM / SOAR

Vuln. Metasploit Docker Challenge



2 Vulns

1) PHP → lösbar mit MS
2) Default Cred. Postgres → "



1) PHP
- Input Sanitization
- WAF
- FW Outbound Rule
- FW Inbound Rule 443

2) Postgres
- DB Hardening → DB Change
- Inbound FW
- Postgres Listen localhost

Es gibt 2 Lösungen für die Metasploit Challenge im HL, via PHP Exploit oder via Postgres Default Cred. Exploit

Begriffe

- SIEM
- SOAR
- EDR

Zuerst gab es SIEM und dann kam SOAR dazu.

Heute über Defender verbreitet sich EDR rasant (Defender und Azure Sentinel)