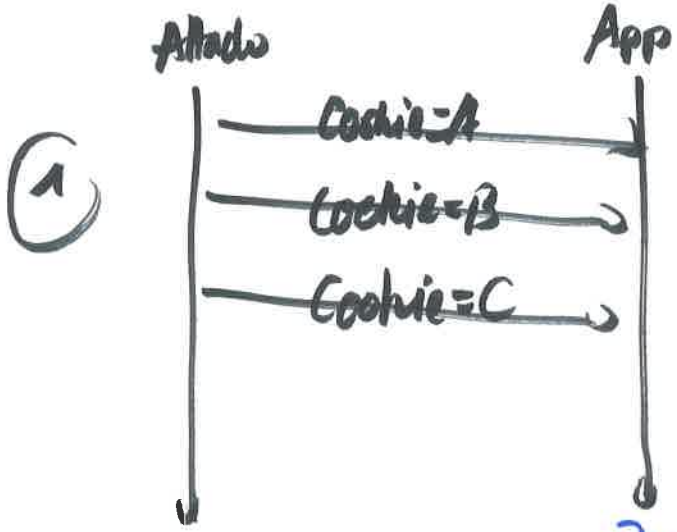
Cyber Defense
20.11.24

Heute reden wir über MISP

Security Advisory 1.1 Sielco

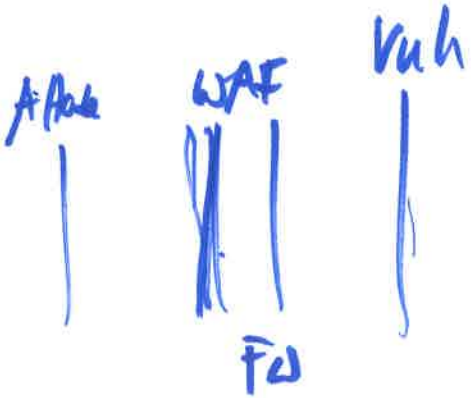


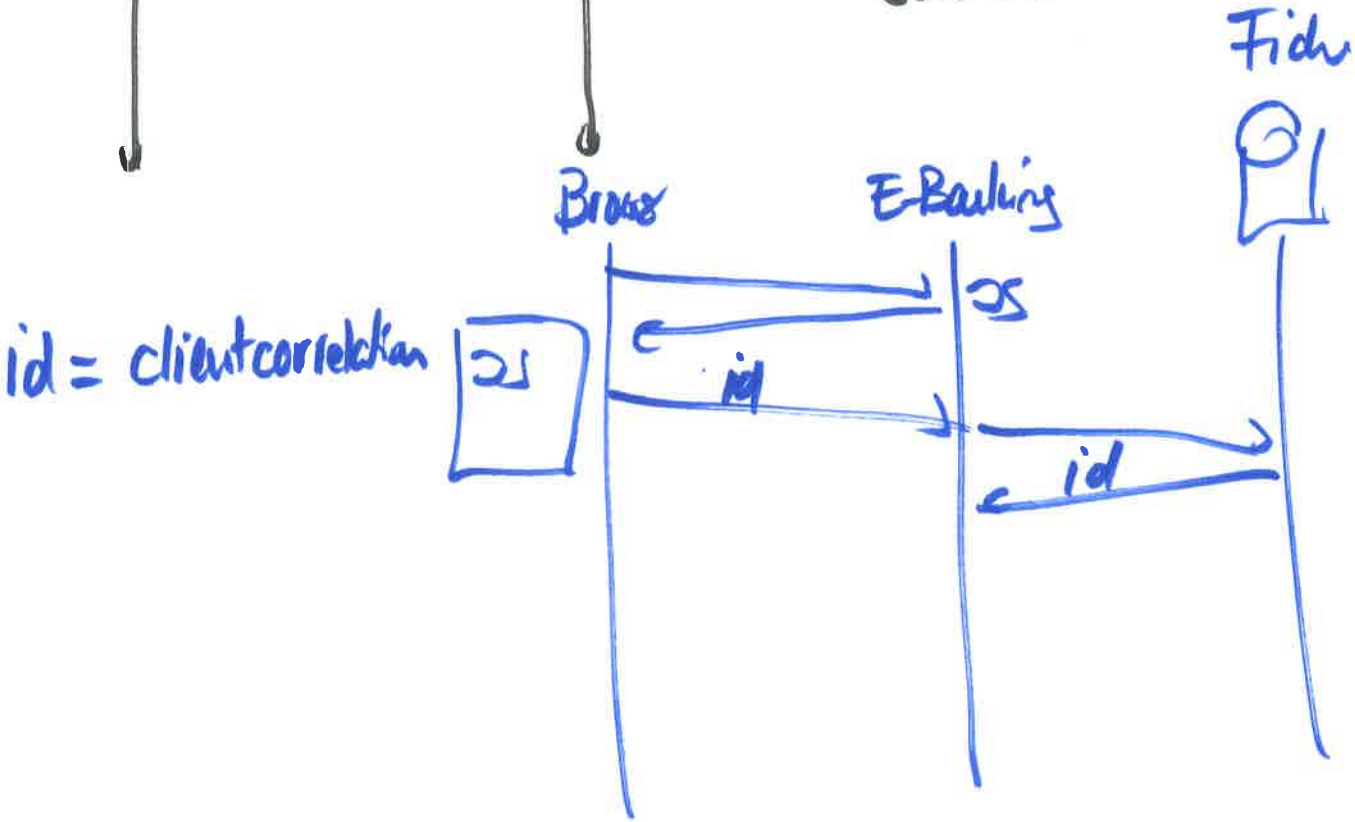
1

2 2FA nein, weil 'rote' eine gültige Session

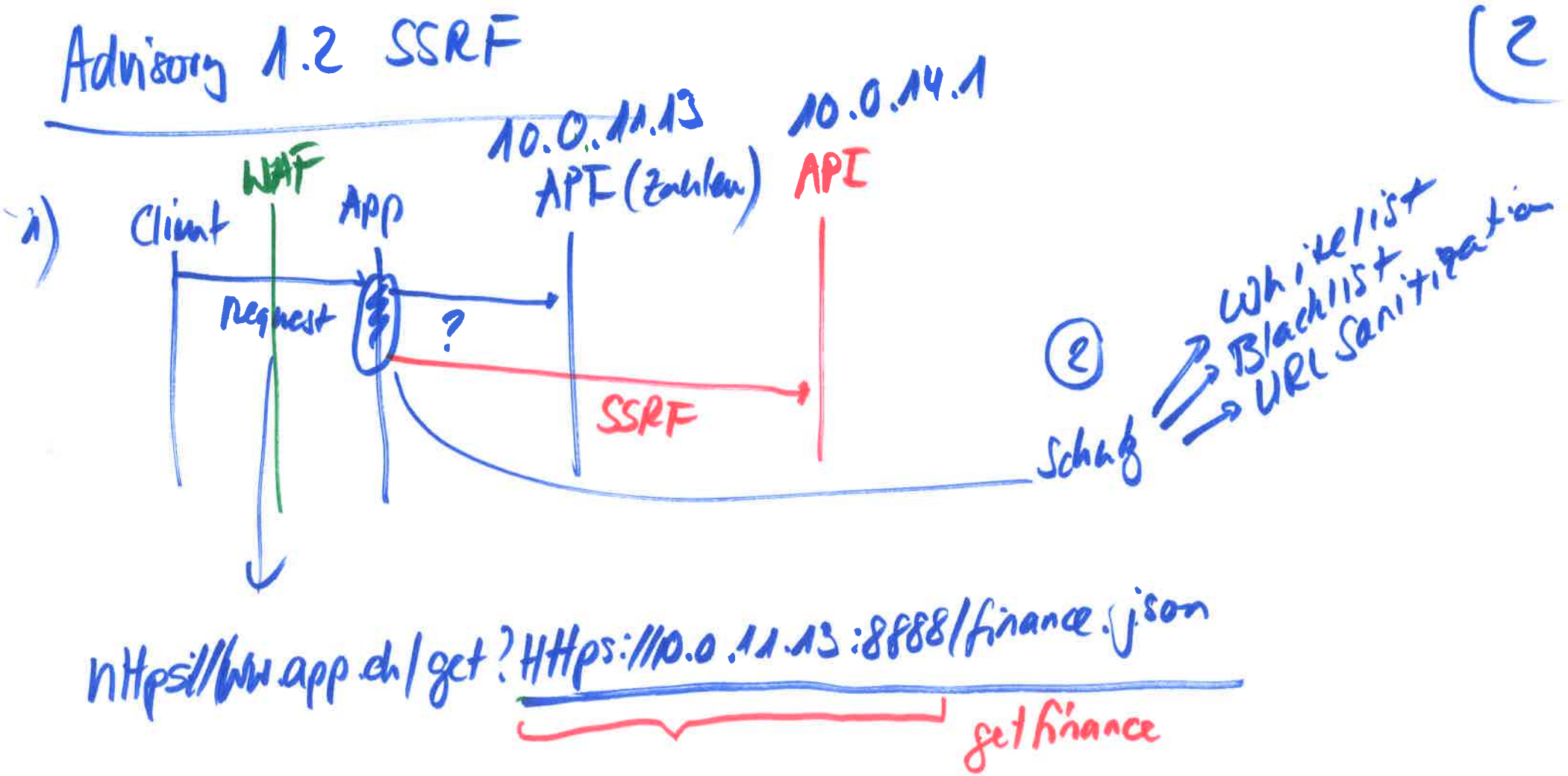
3 Fail2ban

IP sperren





Advisory 1.2 SSRF



3) WAF
- Whitelist im Request

XSRF ist dieser Angriff auf dem Client Computer
SSRF ist dieser Angriff auf einem Server (Facade Service)

SOC Fragen

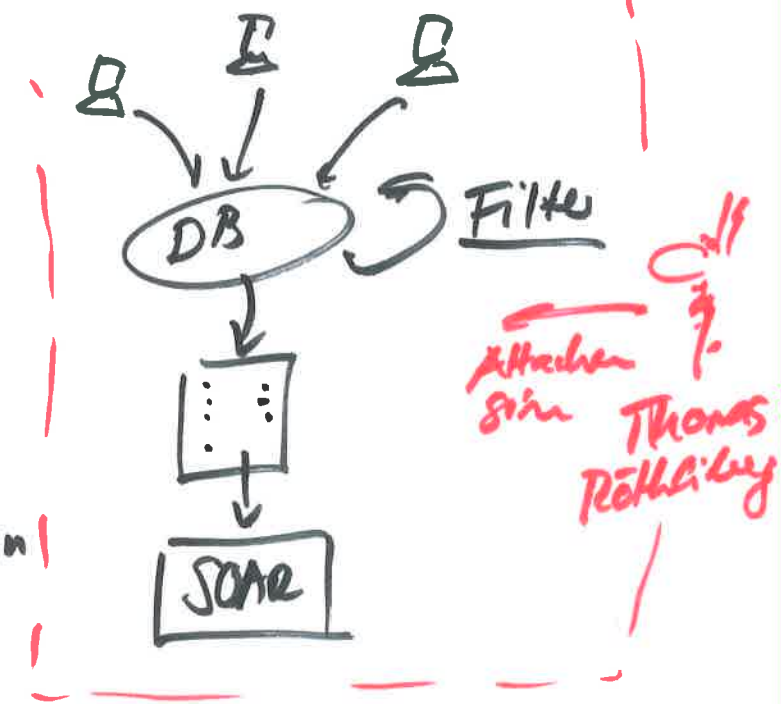
- Scope SOC → Was überwachen ← BYOD, OS, Devices
  - → Wie überwachen

- Anzahl Incidents → true positive
- Ablauf wenn man was findet.

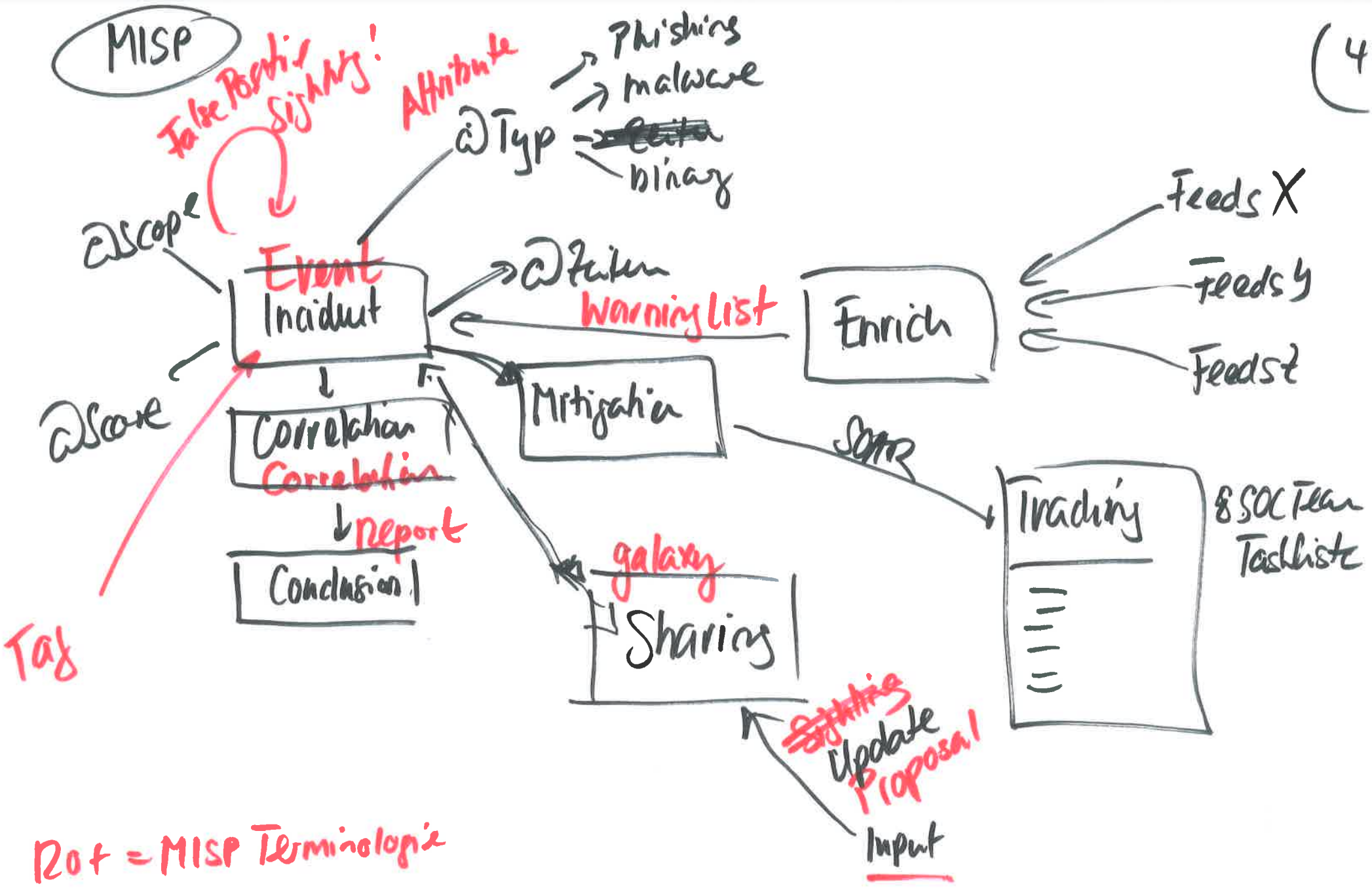
- Tools
  - Sammeln?
  - Erkennen?
  - Hunting?
- Kosten
  - Anzahl MA
- Kompetenzen?
  - Was muss man können
  -

- Freizeit
  - hat man noch Freizeit
- Know-How Pflege?
  - → wie up to date

SOC → Lorenz Inglin / Florian



Wir überlegen uns Fragen an die Leute von Swisscom bei der Exkursion



Wir überlegen uns die Entities wenn wir eine Incident Sharing Lösung bauen würden und rot sind die Begriffe von MISP (einfacherer Einstieg in MISP)