HS2024
Cyber Defense
13.11.2024

Heute sprechen wir primär über verschiedene Formate um IOC zwischen Organisationen zu sharen

Feedbach

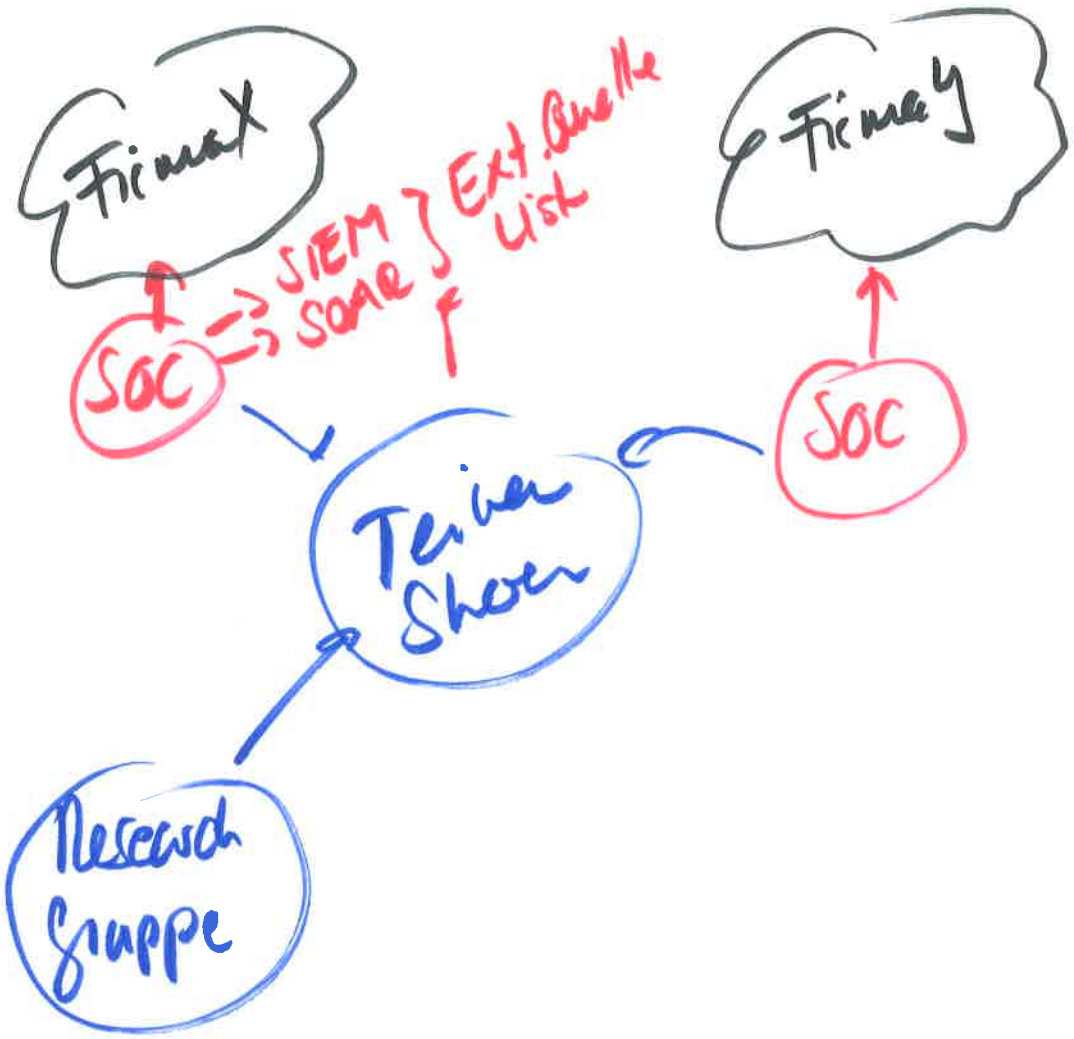
(2

a Advisories → gut → konsequente (Prüfung)
↳ alte Prüfungen abgeben

b) Besuch SOC

Swisscom SOC angefragt für Exkursion

* Mittwoch zwischen 08:00 und 10:00 Uhr in Zürich (Hardbrücke)
* Wer nicht an Exkursion teilnimmt, muss HL Aufgabe lösen



Wie?

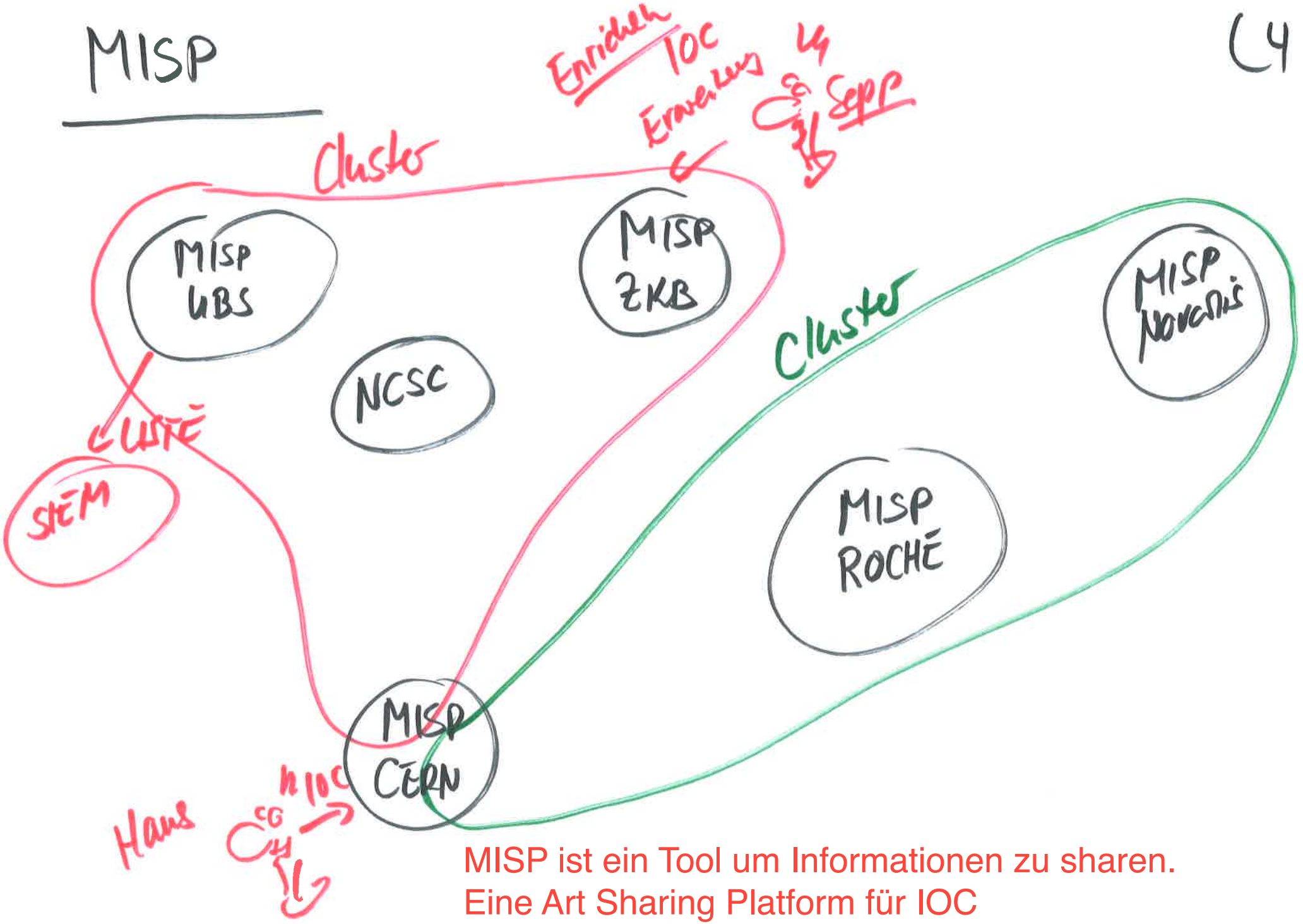
- Papers publizieren.

Bedürfnis

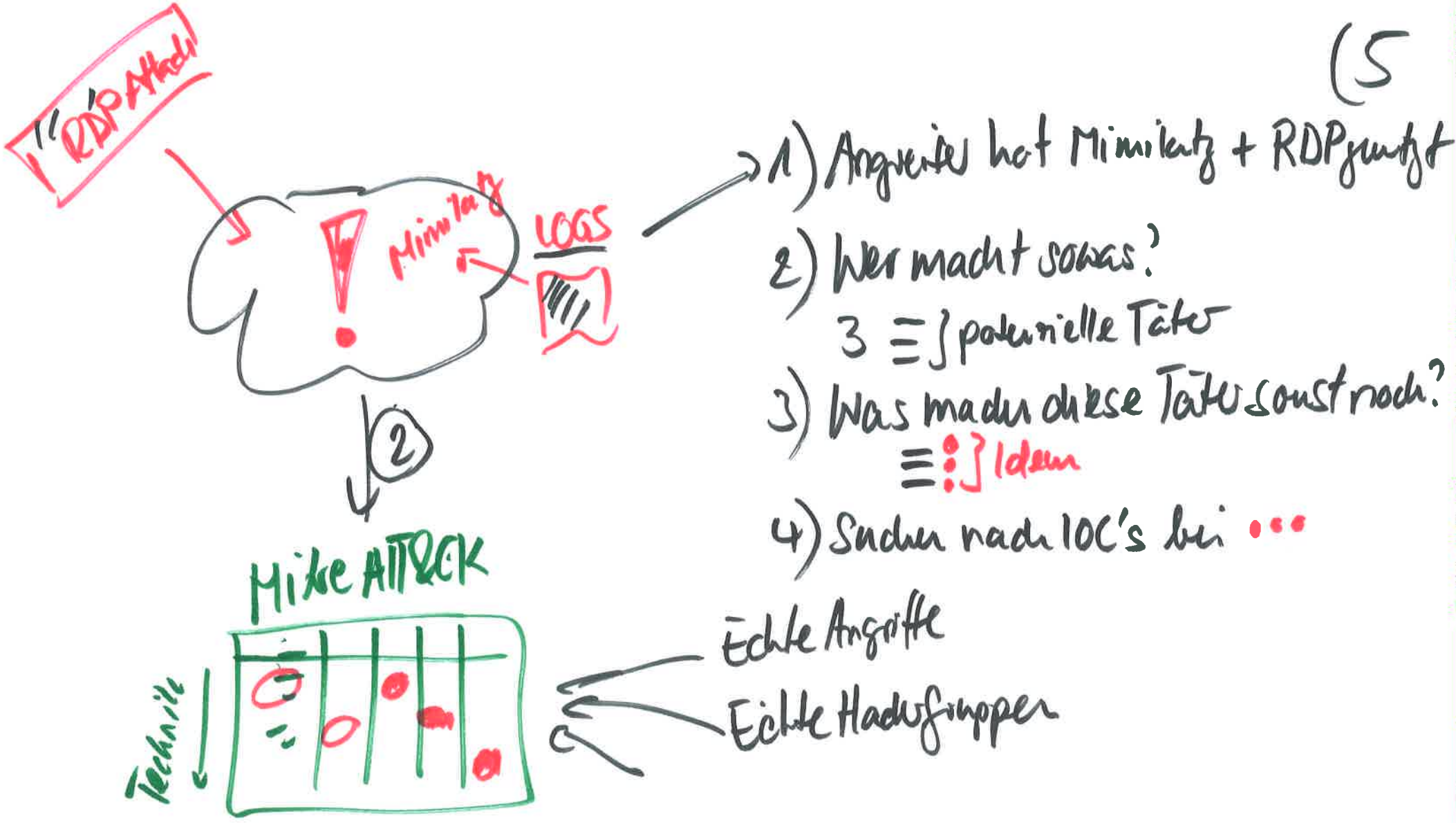
- Standard
  - Klassifizieren (Modell)
  - Strukturierte Daten (JSON)

Einführung ins Thema, warum sprechen wir überhaupt über Frameworks? Idee, einen Standard für den Austausch von Informationen zu haben

MISP



MISP ist ein Tool um Informationen zu sharen.
Eine Art Sharing Platform für IOC



Wir diskutieren über den Nutzen des Att&ck Framework. Idee ist es, anhand vom Framework Ideen zu erhalten, nach was man im eigenen Netzwerk suchen sollte (siehe 1) bis 4))