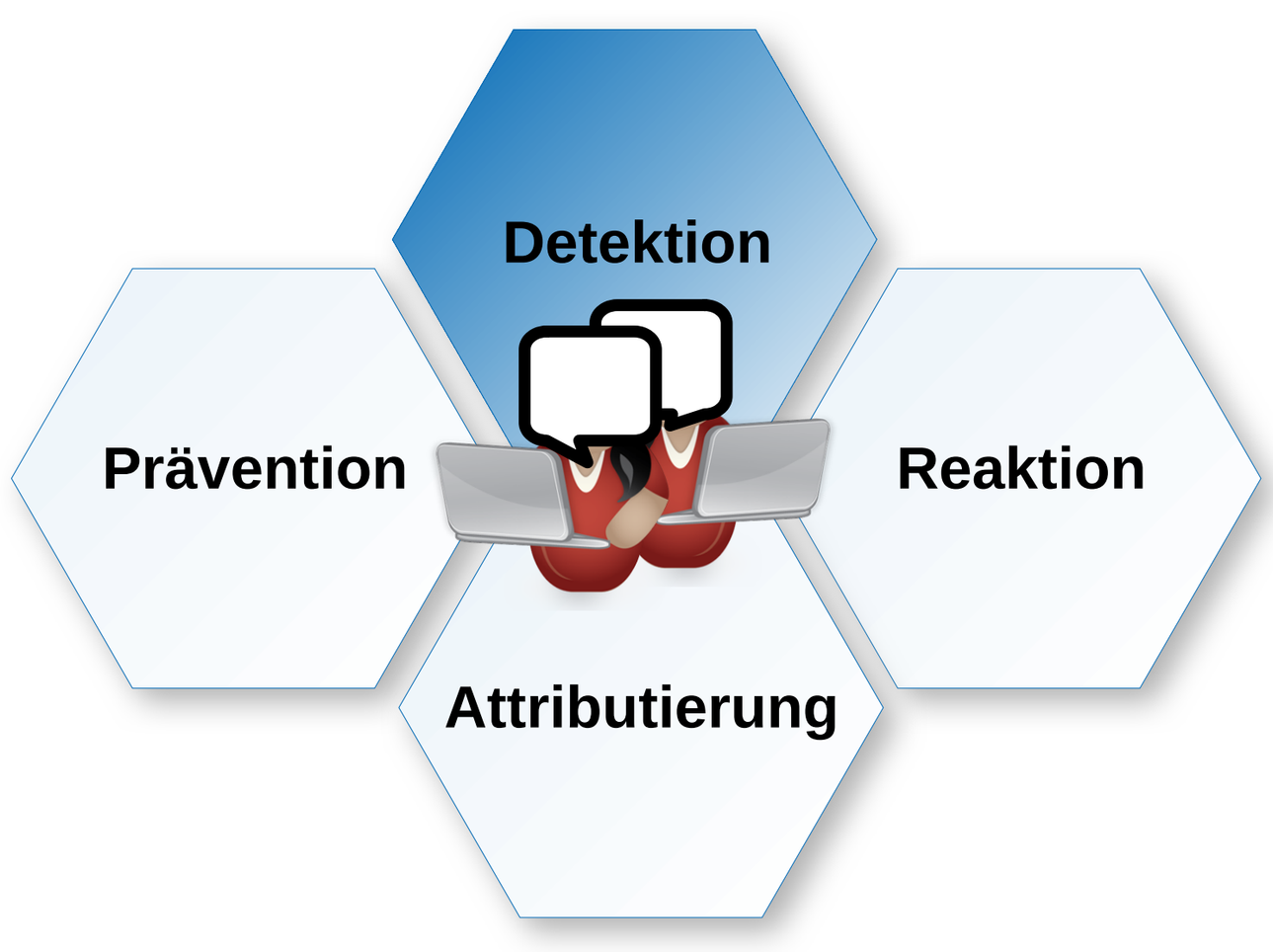
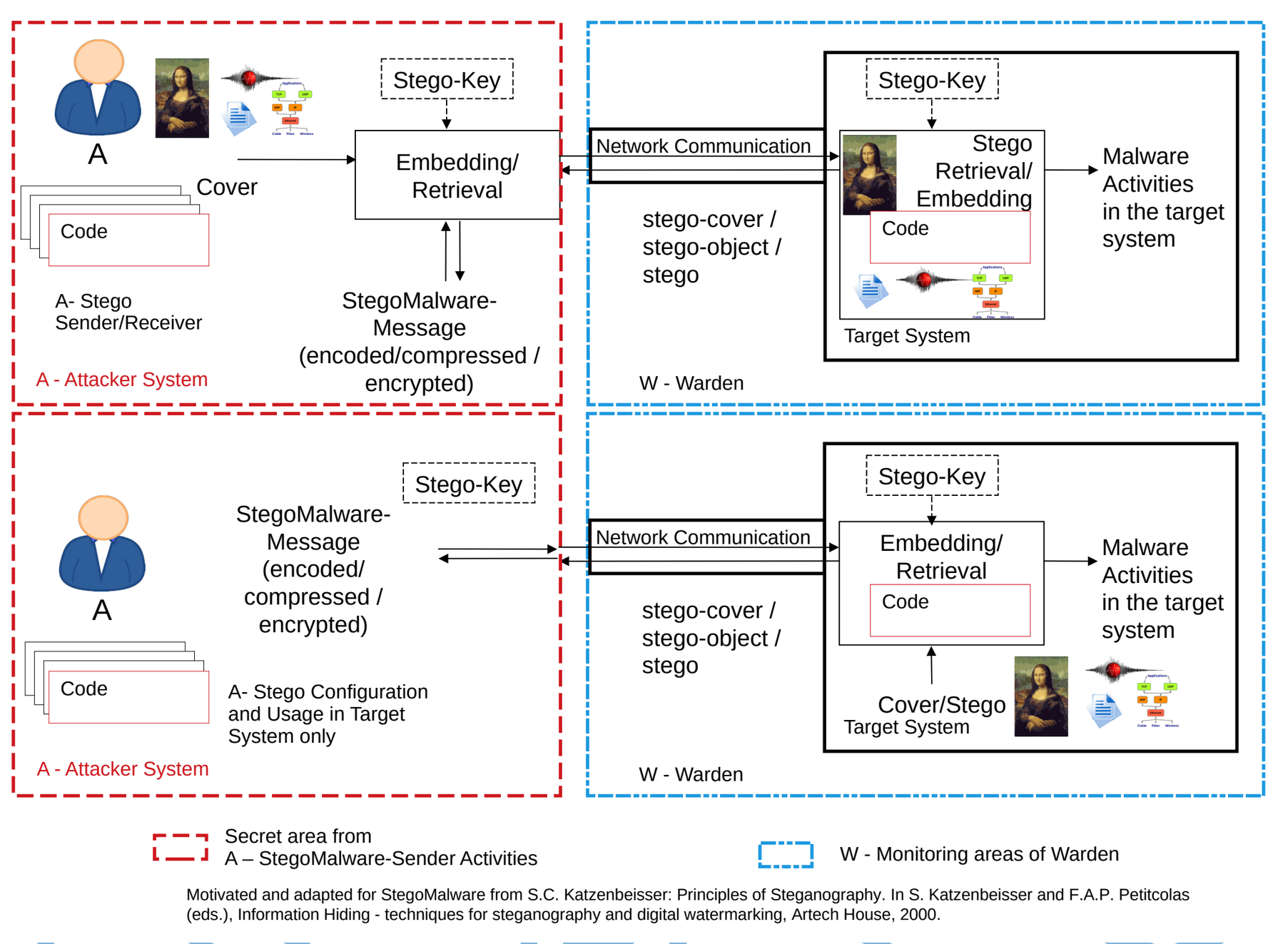
Attribution von verdeckten (Informations-)Kanälen im Bereich kritischer Infrastrukturen und Potentiale für Prävention und Reaktion

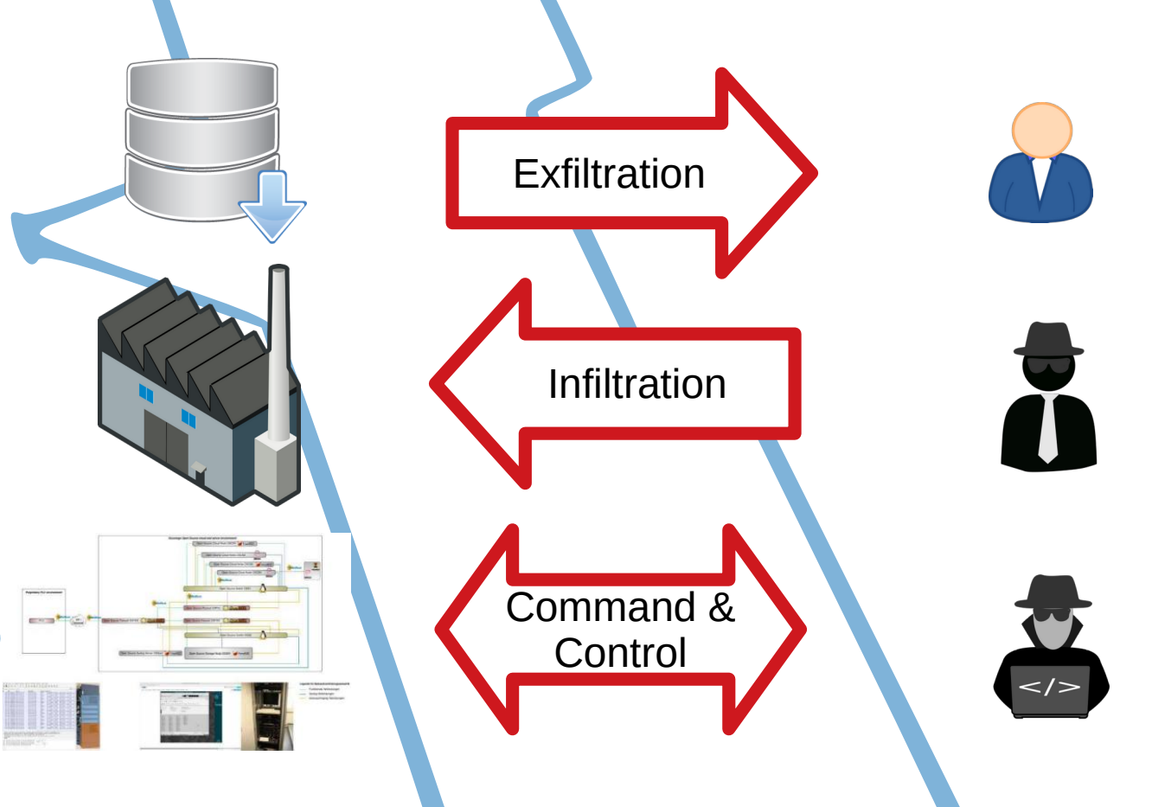
Akronym: **ATTRIBUT** (Phase 3)
Laufzeit: 01.09.2024 bis 31.08.2027

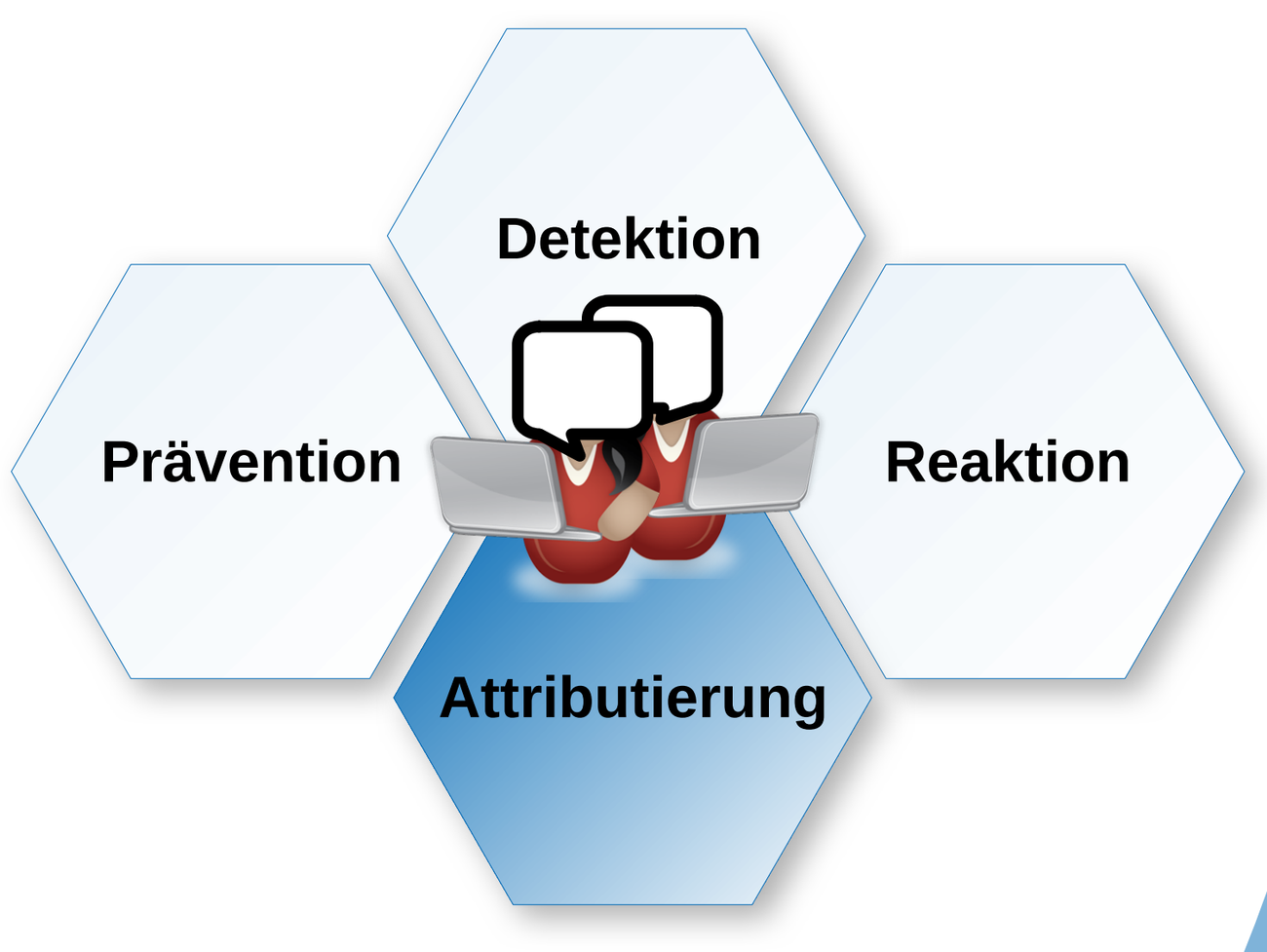
ATTRIBUT

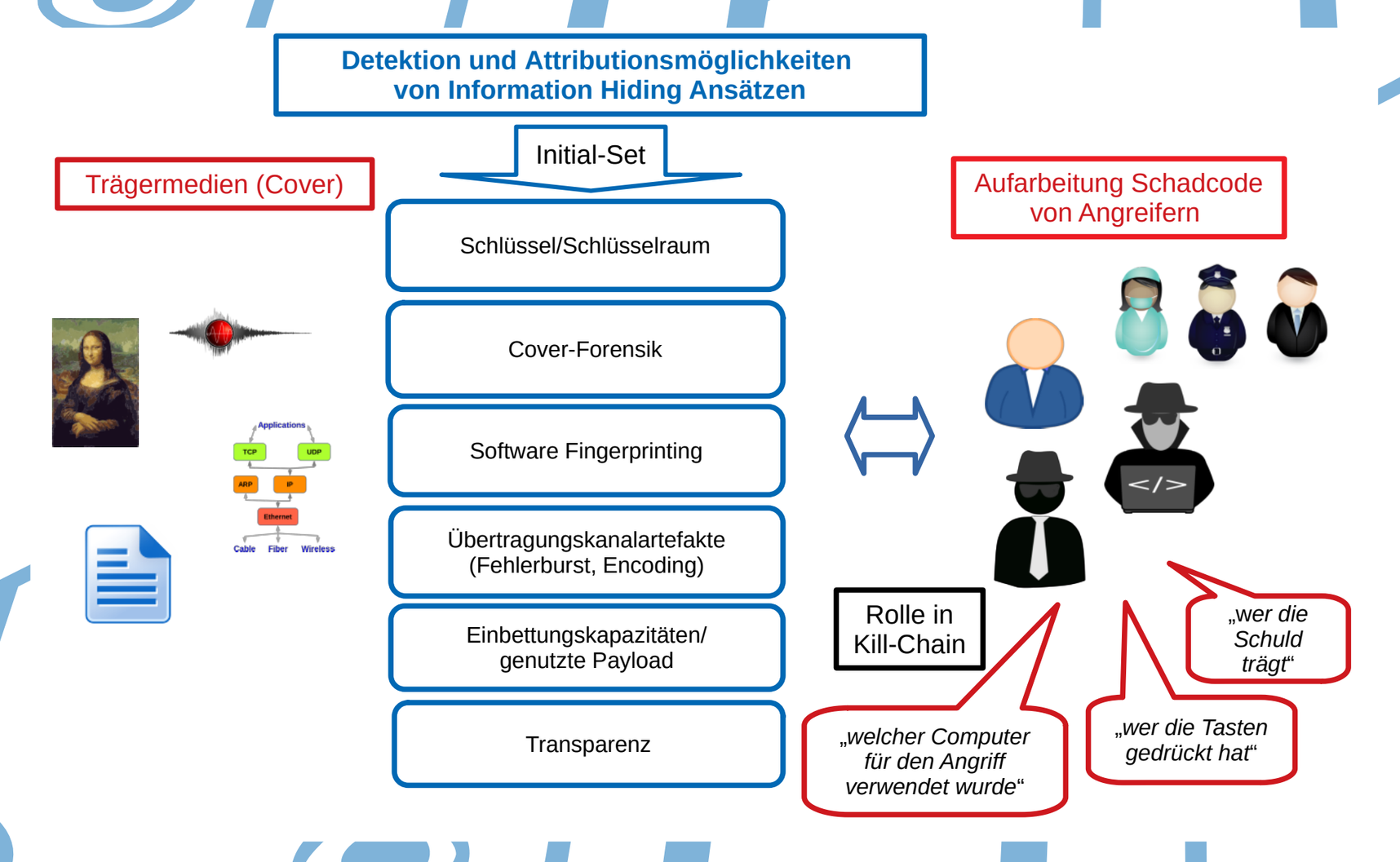


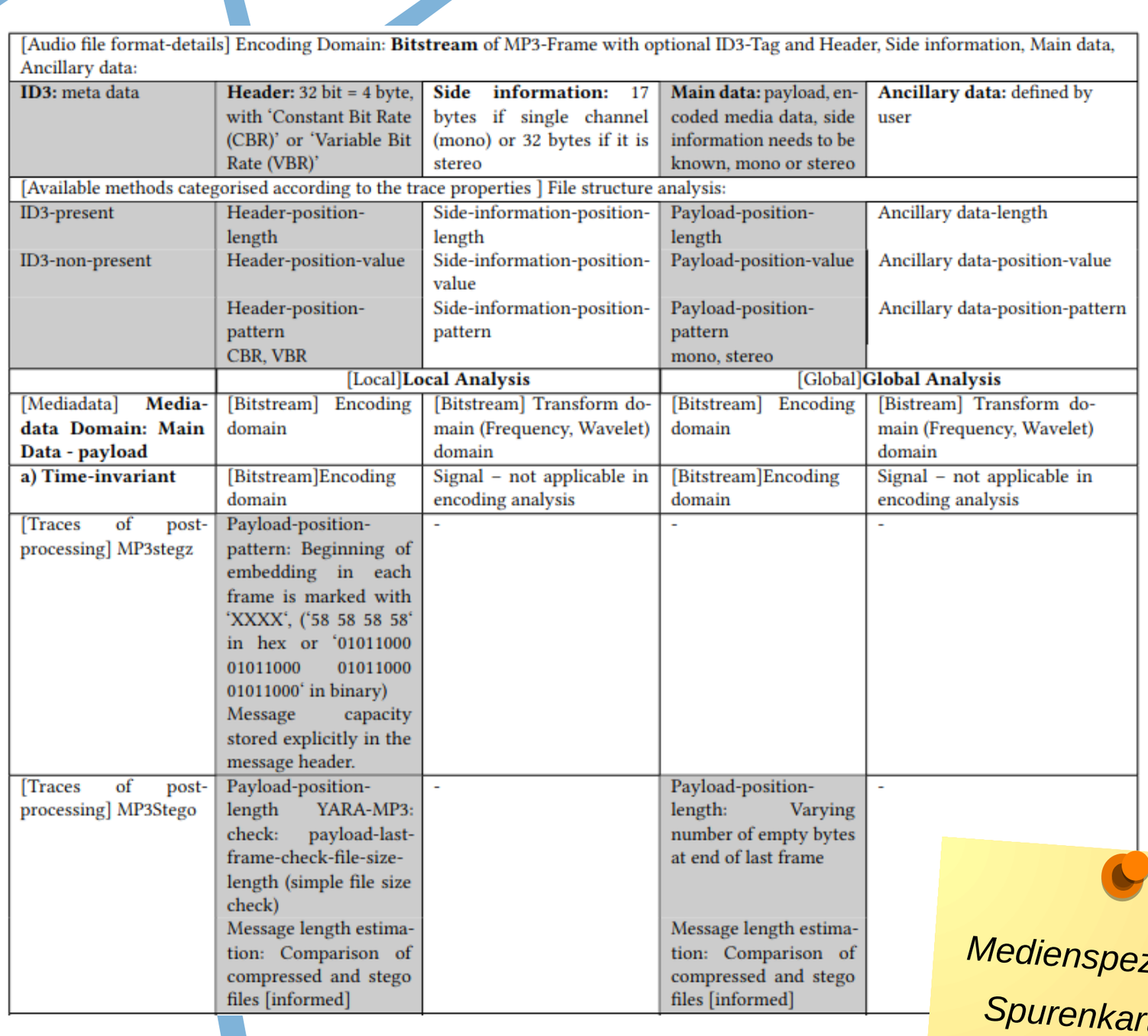


Gängige Basisangriffsformen

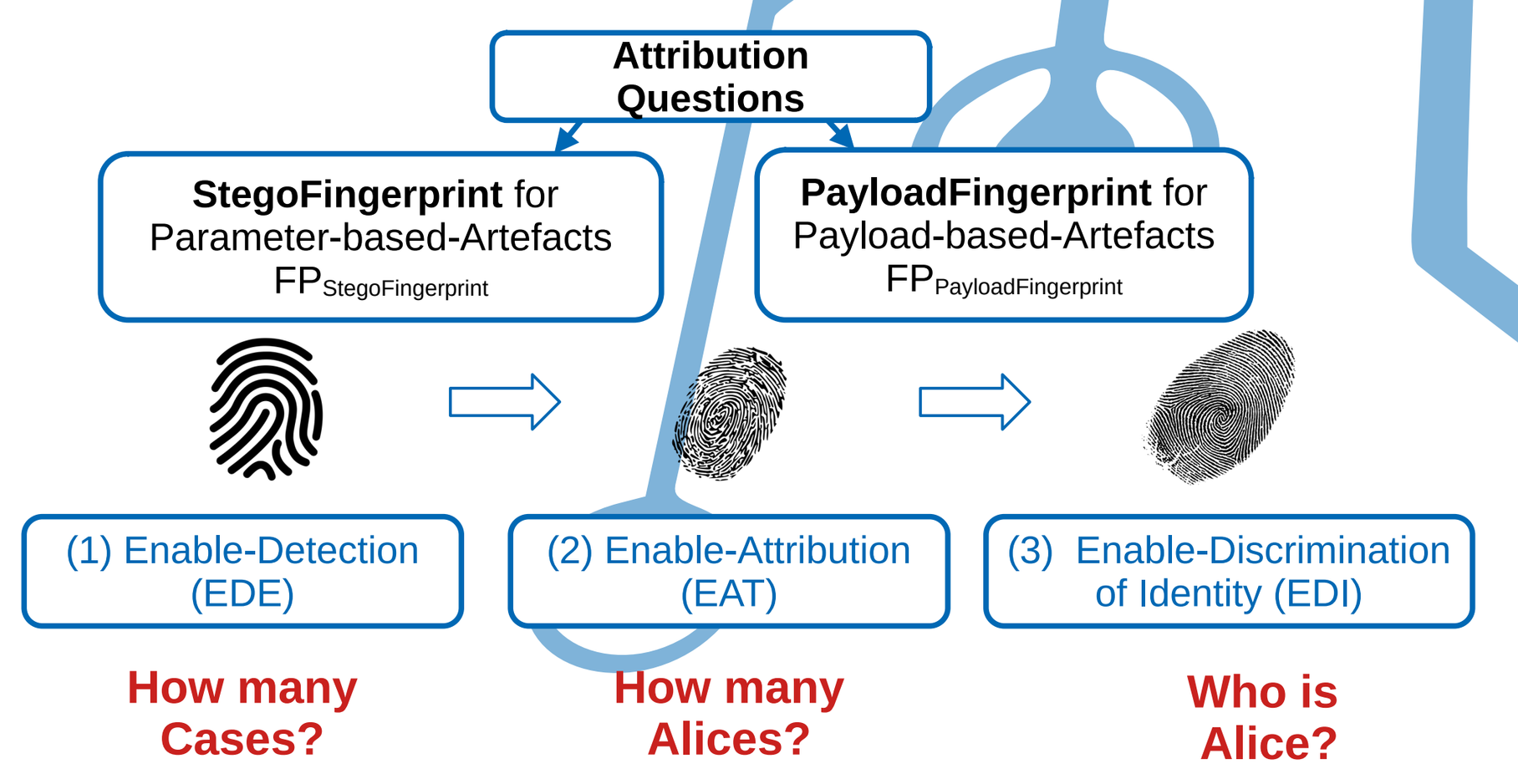




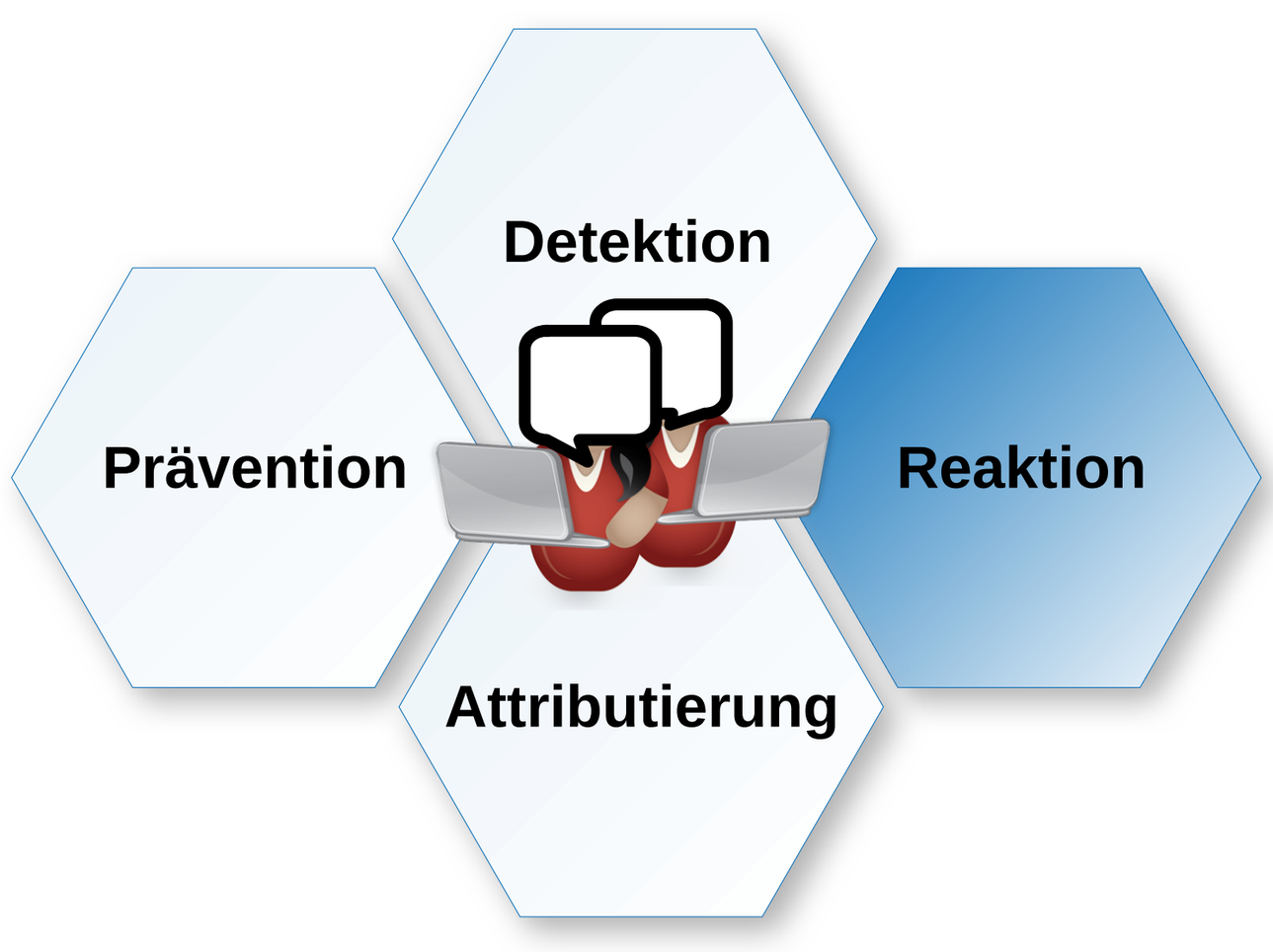


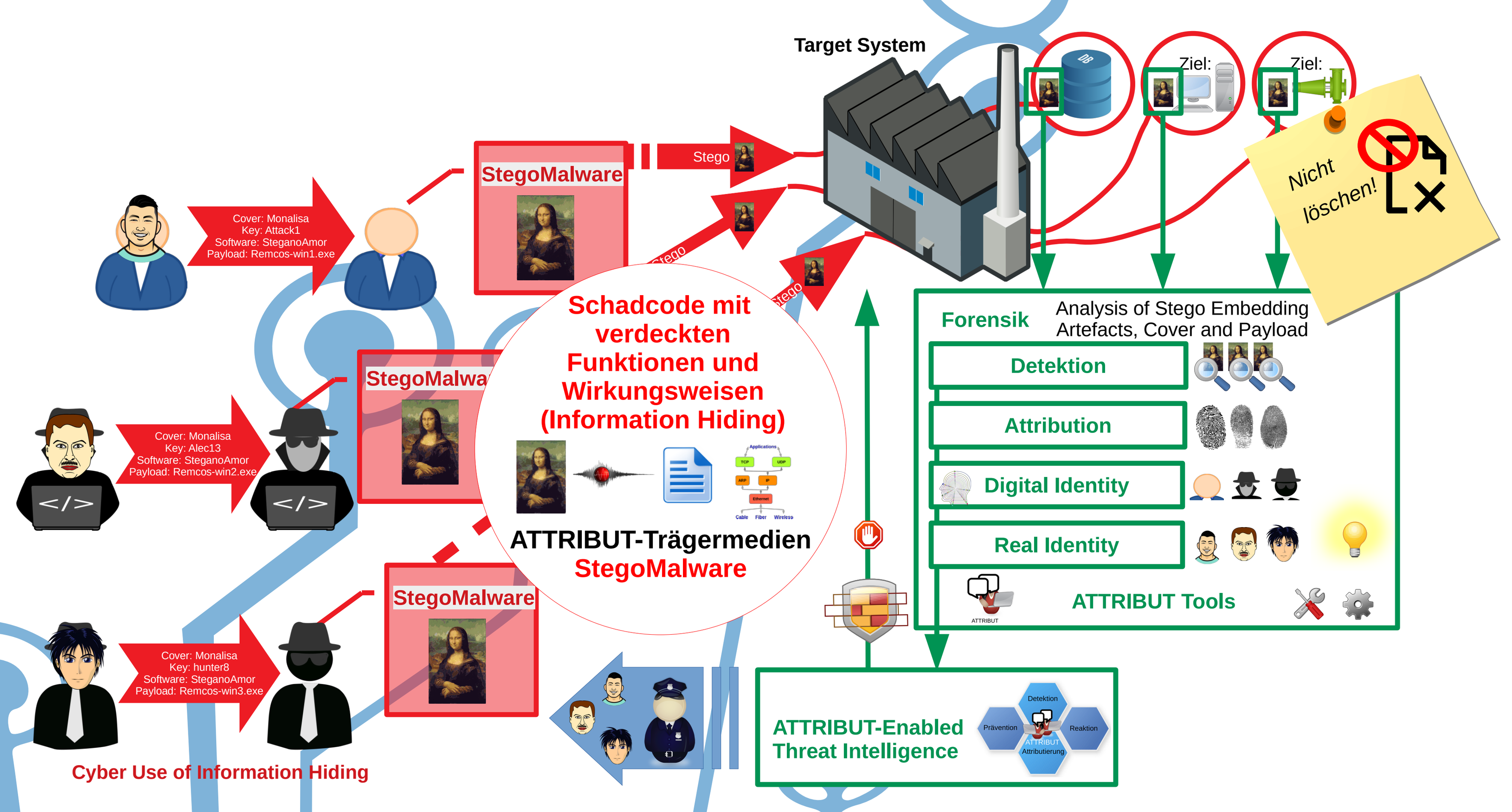


Medienspezifische Spurenkarten als *Open Educational Resources* (OER)

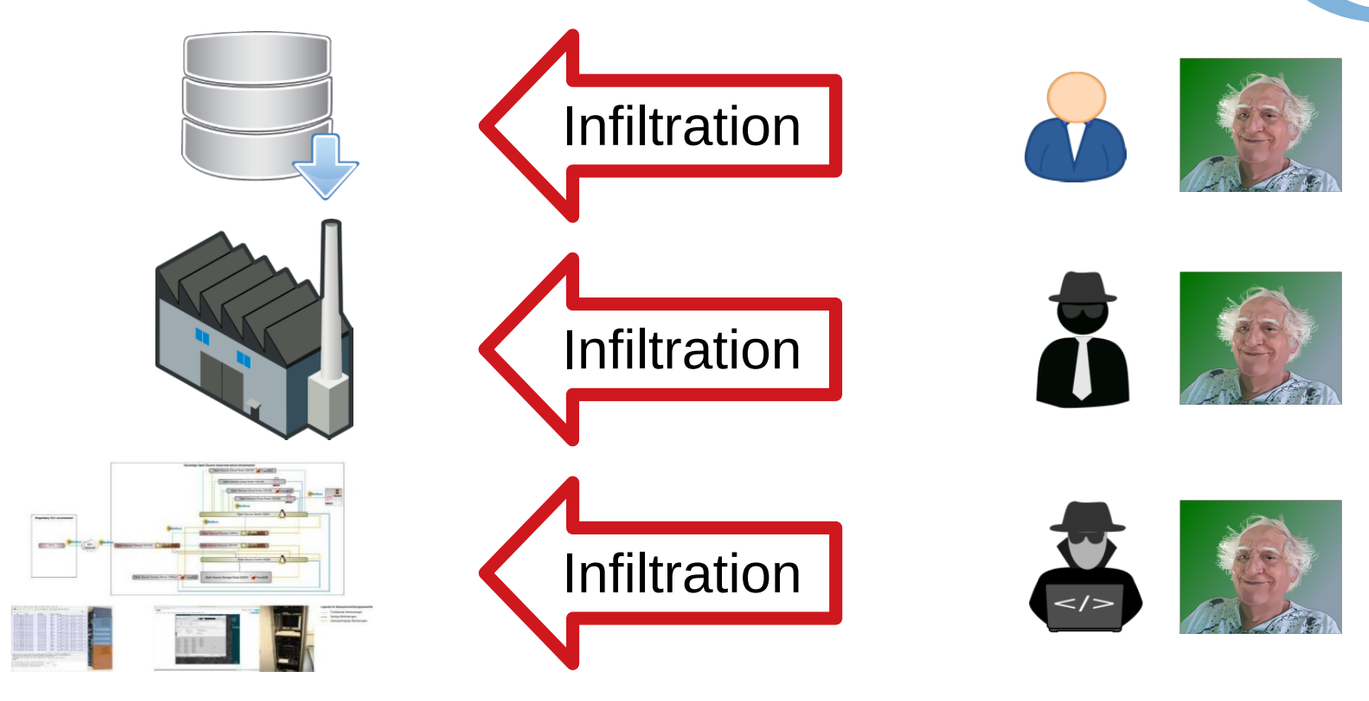


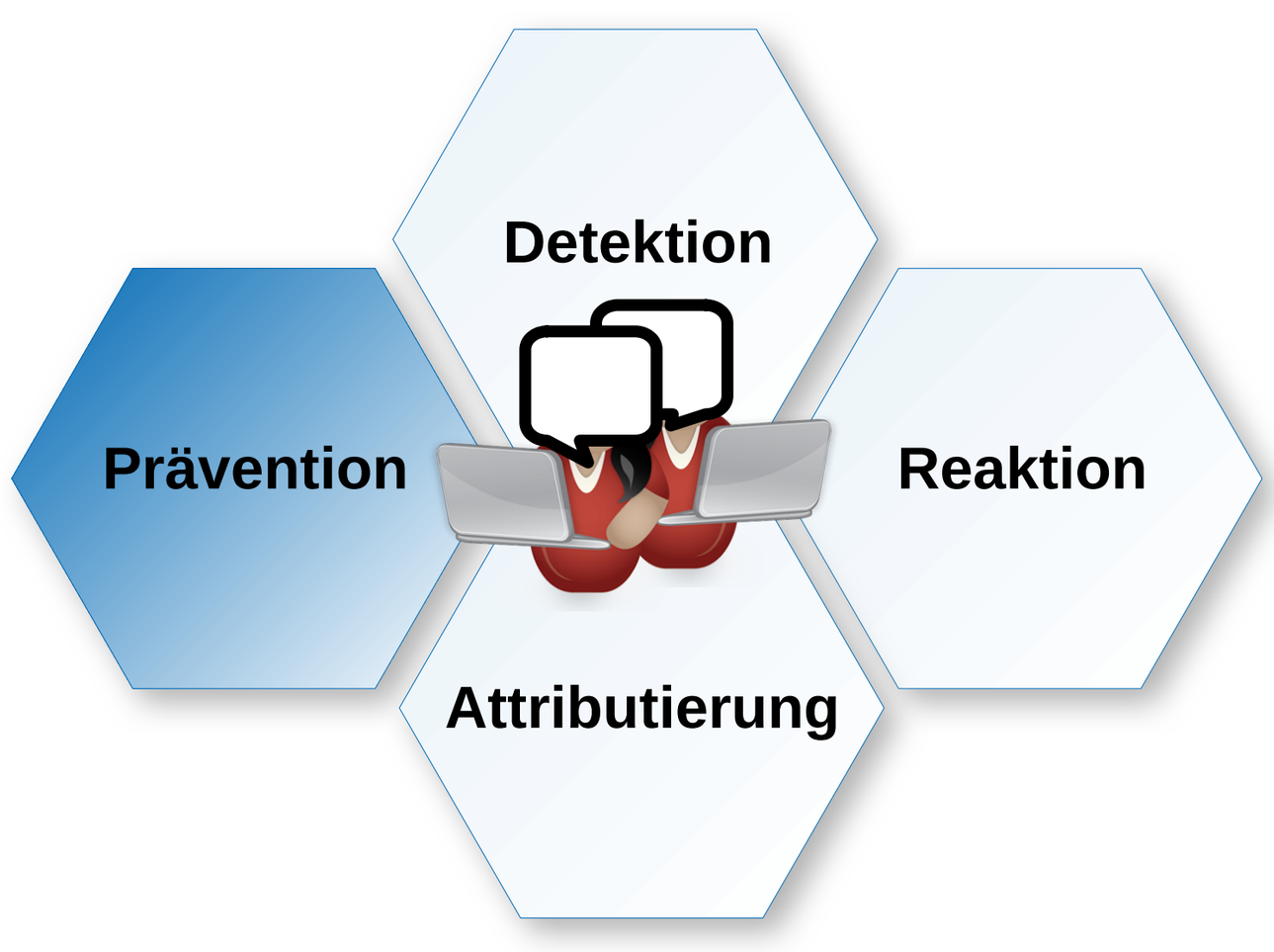
ATTRIBUT-Enabled Threat Intelligence

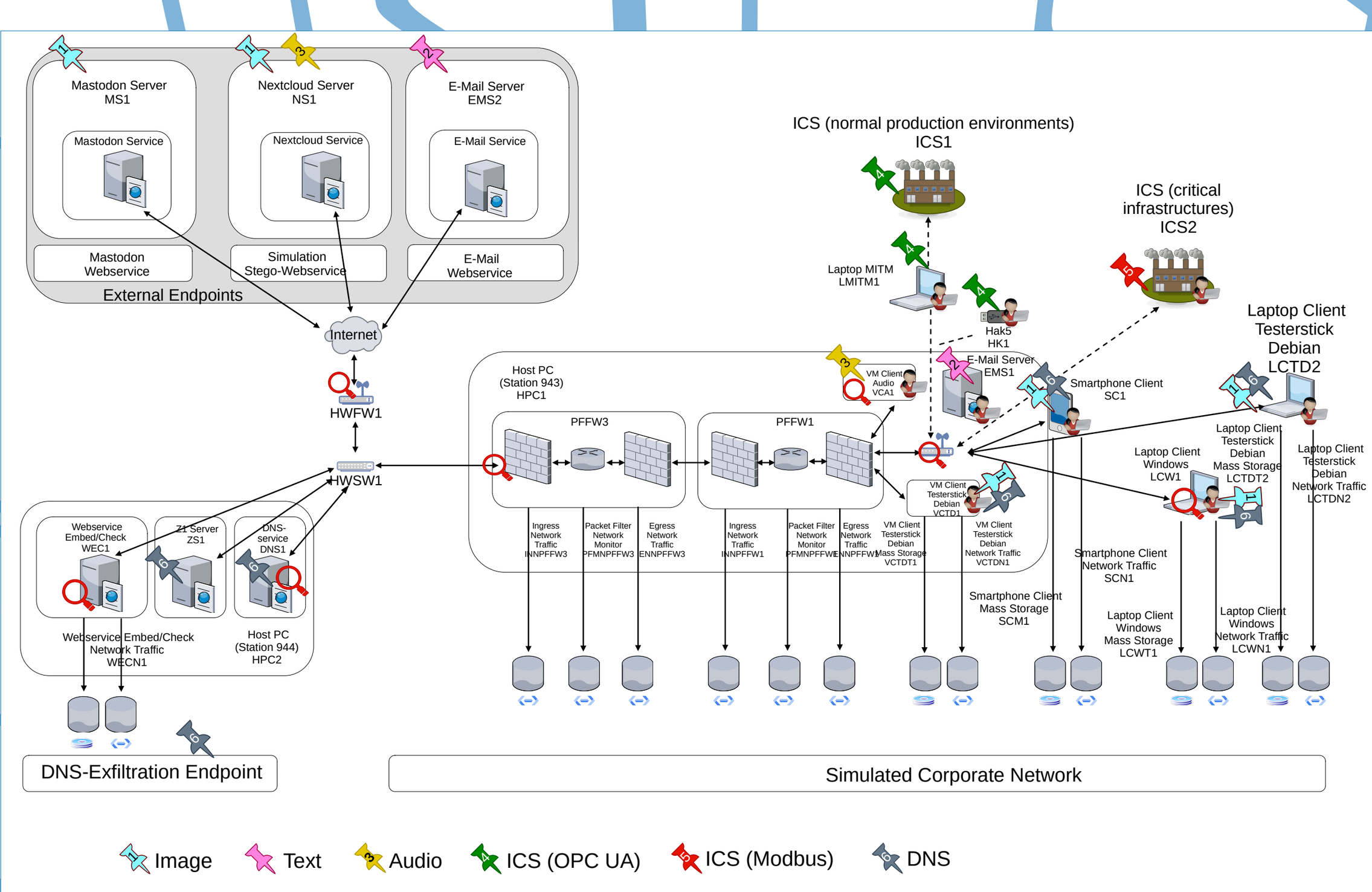


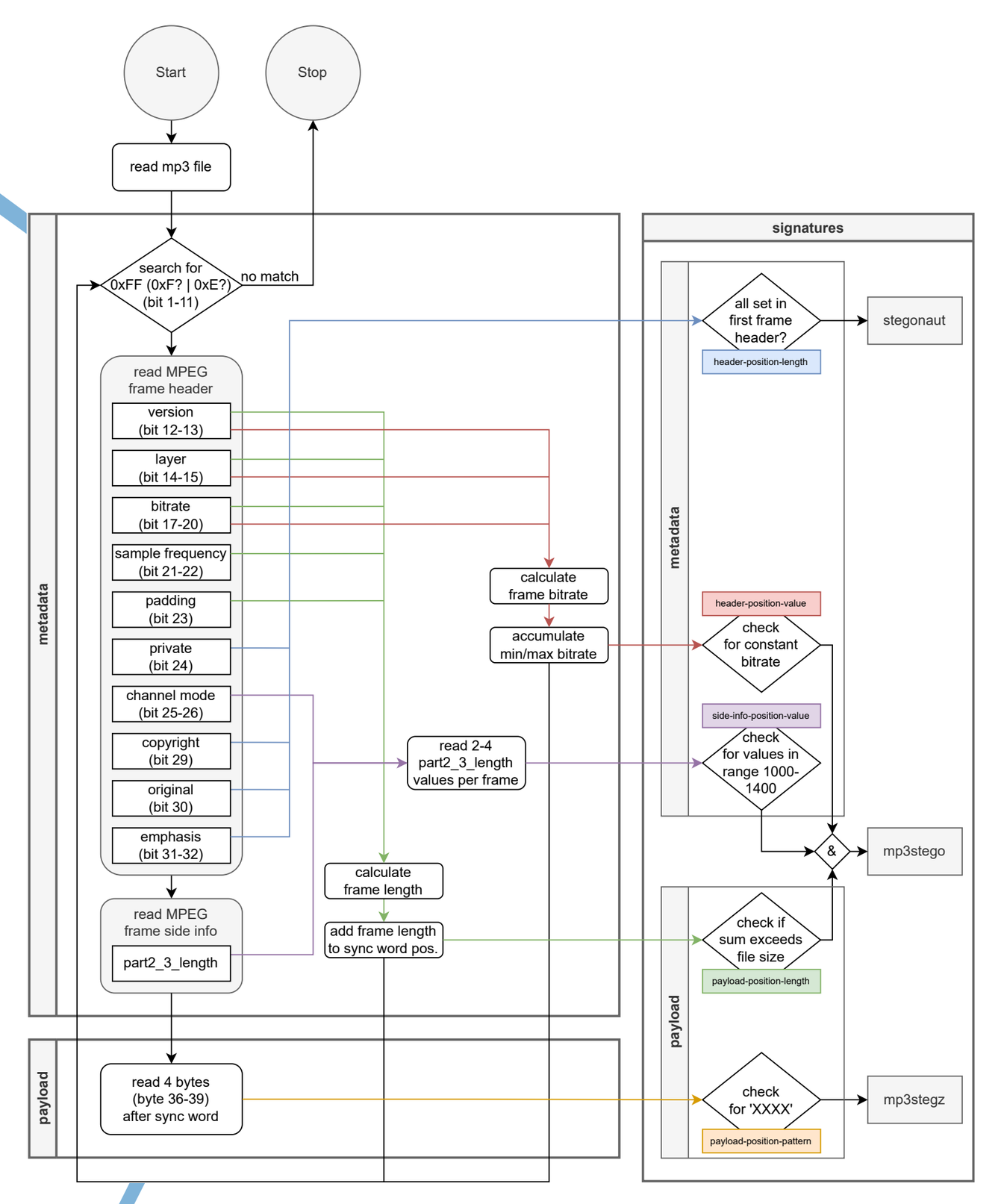


Basisangriffsformen: Kampagne SteganoAmor









Pin Nr.	FOSS demonstrators and generated datasets
1	THBRB Image Stego Tools v001 THBRB image cover and stego set 1
2	MLU Text Stego Tools v1.1.0 MLU text cover and stego set 1
3	OVGU Audio LSB Pattern and Parameter Simulator v001 OVGU audio cover dataset 1 OVGU audio stego datasets 1 to 5
4	THBRB OPC UA Network Traffic Simulator v001 THBRB Network Cover and Stego Pairs v002
5	OVGU Modbus Network Traffic Simulator v001 OVGU ICS-Modbus-Stego-Dataset 1
6	HSW DNS Network Traffic Simulator v001 HSW DNS-Stego-Dataset 1 v003 HSW DNS-Stego-Dataset 2 v001

Beispiel: YARA-Regel für MP3-Stego-Tool *mp3stegz*

```
rule payload_position_pattern {
    strings:
        $mpeg_sync_word_with_pattern = { FF (F? | E?) [34] 58 58 58 58 }
    condition:
        #mpeg_sync_word_with_pattern > 0 }

rule mp3stegz : main {
    condition: payload_position_pattern
}
```

Cliparts: LibreOffice und openclipart.org
Abbildungen erstellt mit draw.io, QtQR und LibreOffice Draw
Hintergrundbild: Basierend auf "4464 Designed by Harryarts / Freepik"

ATTRIBUT Materialien:
- Erklärvideos
- Wissenschaftliche Publikationen
- Forschungsdatensätze
- OER Materialien (z.B. Spurenkarten)

ATTRIBUT Mastodon-Profil Englisch
https://sparrow.cs.uni-magdeburg.de/@AttributEnglish

ATTRIBUT Website
https://attribut.cs.uni-magdeburg.de/

ATTRIBUT Mastodon-Profil DE
https://sparrow.cs.uni-magdeburg.de/@ATTRIBUT

ATTRIBUT-Team:

Otto von Guericke Universität Magdeburg – Fakultät für Informatik
AMSL – Advanced Multimedia and Security Lab
Martin-Luther-Universität Halle-Wittenberg
Technische Hochschule Brandenburg – University of Applied Sciences
Hochschule Worms – University of Applied Sciences
Hochschule für den öffentlichen Dienst in Bayern – Fachbereich Polizei
universität ulm

Diese Forschungsarbeit wurde durch die Agentur für Innovation in der Cybersicherheit GmbH im Rahmen des Vorhabens Forschung zu „Existenzbedrohenden Risiken aus dem Cyber- und Informationsraum – Hochsicherheit in sicherheitskritischen und verteidigungsrelevanten Szenarien" (HSK) beauftragt und finanziert. Eine Einflussnahme der Agentur für Innovation in der Cybersicherheit GmbH auf die Ergebnisse fand nicht statt.

cyberagentur