
SBA
Research


ASOC
Cyber Defense

Agenda

1. ASOC Übersicht
2. ASOC im Detail
3. Projektstatus
4. Weitere Projekte, Vorhaben und Schritte

1. ASOC Übersicht

ASOC Übersicht

- Ausgangssituation der Universitäten
- ASOC Projektdefinition
- Grundlegende Paradigmen
- Was ist ASOC?
- ASOC Ziele
- ASOC Nicht-Ziele

Ausgangssituation der Universitäten

- Große, heterogene Netzwerke
- Große Anzahl Studierender
- Führt zu hohen Lizenzkosten mit kommerziellen Lösungen
- Abgang erfahrener Mitarbeiter:innen im IT/ITSec – Bereich
  → Ressourcendefizit im Cybersecurity Bereich
- Zunahme von Angriffen / Erhöhung der Angriffsflächen durch neue Services und Digitalisierungsbemühungen

ASOC Projektdefinition

Das **Forschungsprojekt ASOC** untersucht einen **raschen und automatisierten Informationsaustausch** von Sicherheitsinformationen.

z.B. IOCs, Regeln, SOAR Workflows, Use Cases, Playbooks und Knowledge im akademischen Kontext

Dieser gemeinsame Ansatz soll die österreichischen Hochschulen durch **Nutzung von Synergieeffekten** bei der Aufgabe unterstützen, ihre digitale Infrastruktur zu schützen und die Cybersicherheit signifikant zu erhöhen sowie dabei proaktive Maßnahmen, Erkennung von Angriffen und Gegenmaßnahmen für alle teilnehmenden SOC zu entwickeln.

Grundlegende Paradigmen

1. Beitrag zur Erhaltung der digitalen Souveränität Europas
2. Auslotung des Open Source Potenzials
3. Einbindung von Forschung und Lehre
4. Begleitende Unterstützungsmaßnahmen

Was ist ASOC?

- Relativ grundlagennahes **Forschungsprojekt**
  - TRL 2 (Konzepte)
  - TRL 3 (Proof of Concept, Critical function experiments)
  - TRL 4 (Lab-Umgebung)
- Kein Umsetzungsprojekt
- Ergebnisse sollen Universitäten beim Thema sektorales SOC unterstützen.

ASOC Nicht-Ziele

- **Evaluierung** oder **Aufbau** eines Security Operation Centers (**SOC**)
- **Evaluierung** oder **Aufbau** eines Information Security Management Systems (**ISMS**).

ASOC - Ziele

- Entwicklung von Beiträgen zur Konzeptionierung eines **föderierten a**kademischen **SOC**s (**ASOC**), basierend auf Open Source Technologien.
- Aufbau eines **gemeinsamen Verständnisses** für SOC Themen / Kollab.
- Auslotung des **Open Source** Potenzials
- PoC einer **Laborumgebung** zum Testen der Methoden und Lösungen und zur weiteren Nutzung in der Forschung, Ausbildung und Lehre.
- Sichere und datenschutzkonforme föderale Datenspeicherung.
- Erprobung von Methoden zum AI-gestützten Threat Hunting.
- Klärung rechtlicher und sozialer Fragen.

Erste Erkenntnisse

- Open Source Lösungen sind vielversprechend
- Skalierung bislang kein Thema
- Größte Herausforderungen:
  - Politische Interessen
  - Fachkräftemangel
- Großes Interesse bei Ministerien in Österreich

2. ASOC im Detail

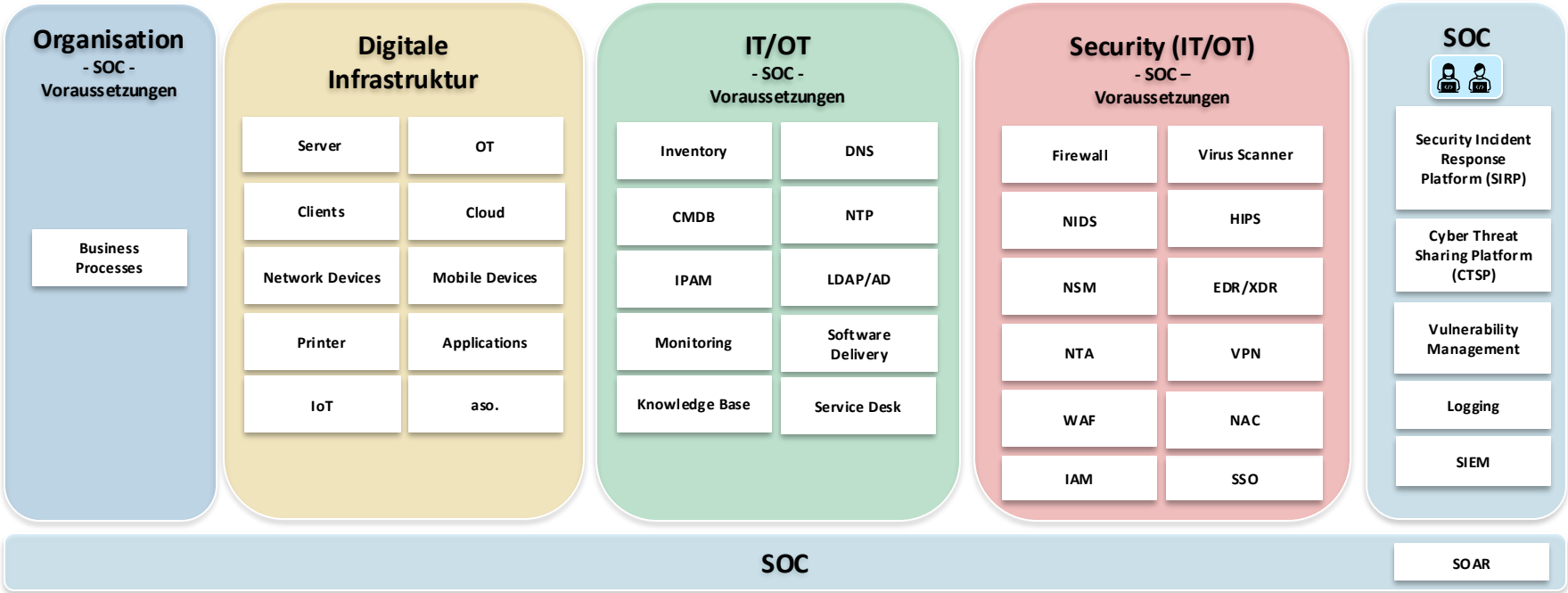
ASOC im Detail

- Arten von SOCs
- Fähigkeiten eines SOCs vs ASOCs
- Information Sharing and Analysis
- ASOC Szenarien
- Fähigkeiten eines ASOC

Arten von SOCs

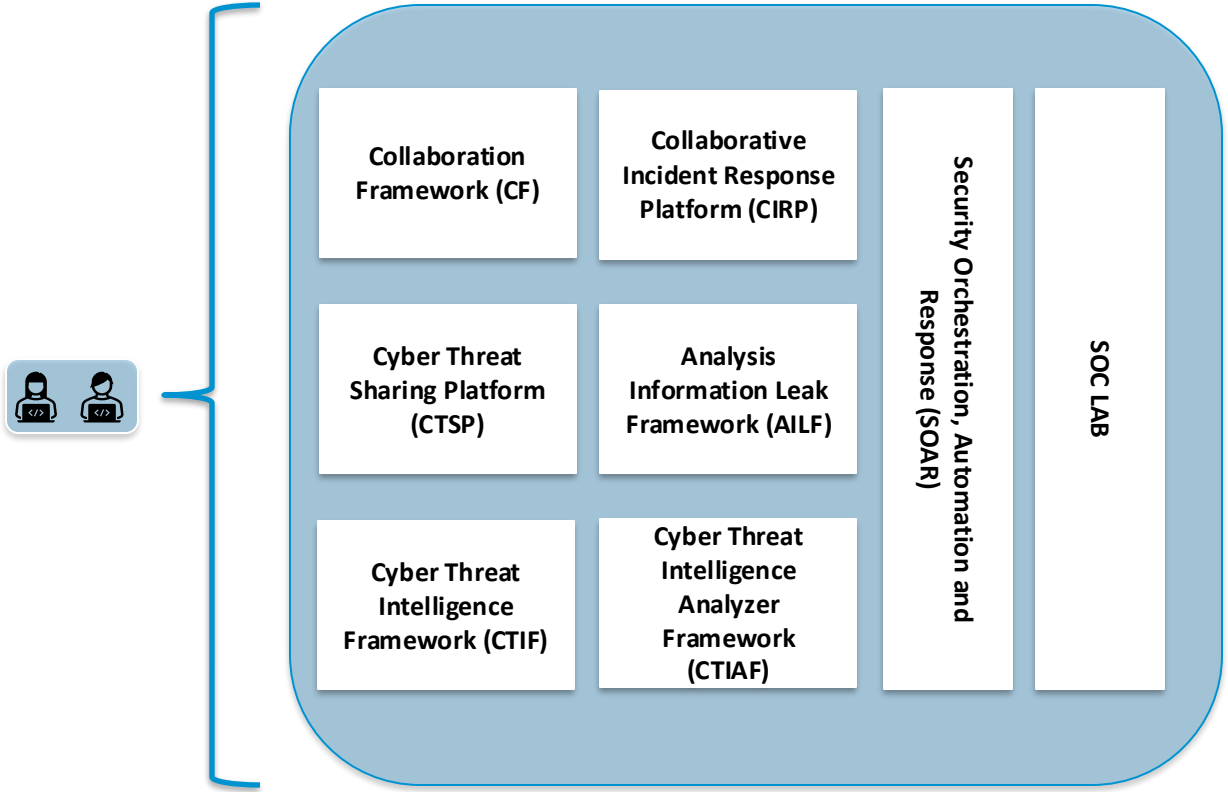
- **SOC as a Service** (full-fledged?)
  - (outsourced SOC)
- **Co-managed SOC** (up to a full-fleshed SOC controlled by the Owner)
  - (Hybrid SOC, in-house and outsourced Model (MSSP))
- **SOC/NOC** (up to a full-fleshed SOC)
  - (Combines internal Organizations (Security Operation and Network Operation))
- **Dedicated SOC** (full-fleshed SOC)
  - (meets all cybersecurity needs)
- **Command SOC** (ASOC, Sektor-CERT, CSIRT, ISAC (Information Sharing and Analysis Centers), etc.)
  - (Lagebild, Information Sharing, etc.)

Fähigkeiten* eines SOCs



*Mindestanforderungen der Fähigkeiten

Fähigkeiten* eines ASOCs



*Mindestanforderungen der Fähigkeiten

Universitäre sektorale Architektur

Information Sharing and Analysis

- Security Incident Informationen
- Indicators of Compromise (IOCs)
- Rules
- SOAR Workflows
- Cases/Use Cases
- Playbooks
- Fachexpertise, z.B. Tipps zu **Security Automation** Themen

ASOC Information Sharing Szenarien

Übersicht

Szenario 1: Eine Universität erkennt ein merkwürdiges Verhalten in ihrer digitalen Infrastruktur.

Szenario 2: Eine Universität hat einen Security Incident.

Szenario 3: Das ASOC hat wichtige Informationen zu neuen, bestehenden und erkannten oder abgeschlossenen Security Incidents.

ASOC Information Sharing Szenarien

Szenario 1

Szenario 1: Eine Universität erkennt ein merkwürdiges Verhalten in ihrer digitalen Infrastruktur.

Möchte IOCs beim ASOC abklären lassen.

Sollte das ASOC Hinweise zu den IOCs haben, wird die Information sofort an alle ASOC-Teilnehmende automatisiert weitergeleitet.

Falls möglich und notwendig werden entsprechende Regeln erstellt, getestet und automatisiert übermittelt.

ASOC Information Sharing Szenarien

Szenario 2

Szenario 2: Eine Universität hat einen Security Incident.

Möchte Inhalte eines laufenden Security Incidents mit dem ASOC abstimmen.

Sollten sich im Zuge des laufenden Security Incidents Informationen ergeben, wie zum Beispiel IOCs, werden diese Information sofort an alle ASOC-Teilnehmenden automatisiert weitergeleitet.

Falls möglich und notwendig werden entsprechende Regeln erstellt, getestet und automatisiert übermittelt.

Übermittelt die Universität gesammelten Daten eines geschlossen Security Incidents an das ASOC, damit diese entsprechende Regel UseCases, SOAR-Workflows und Playbooks prüfen bzw. erstellen kann, um diese allen ASOC-Teilnehmenden im Anschluss zur Verfügung zur stellen.

ASOC Information Sharing Szenarien

Szenario 3

Szenario 3: Das ASOC hat wichtige Informationen zu neuen, bestehenden und erkannten oder abgeschlossenen Security Incidents.

Möchte Information über die Security Incidents an die Universitäten automatisiert verteilen.

Möchte IOC-Informationen an die Universitäten automatisiert verteilen.

Möchte entsprechende Regeln basierend auf den IOC-Informationen automatisiert verteilen.

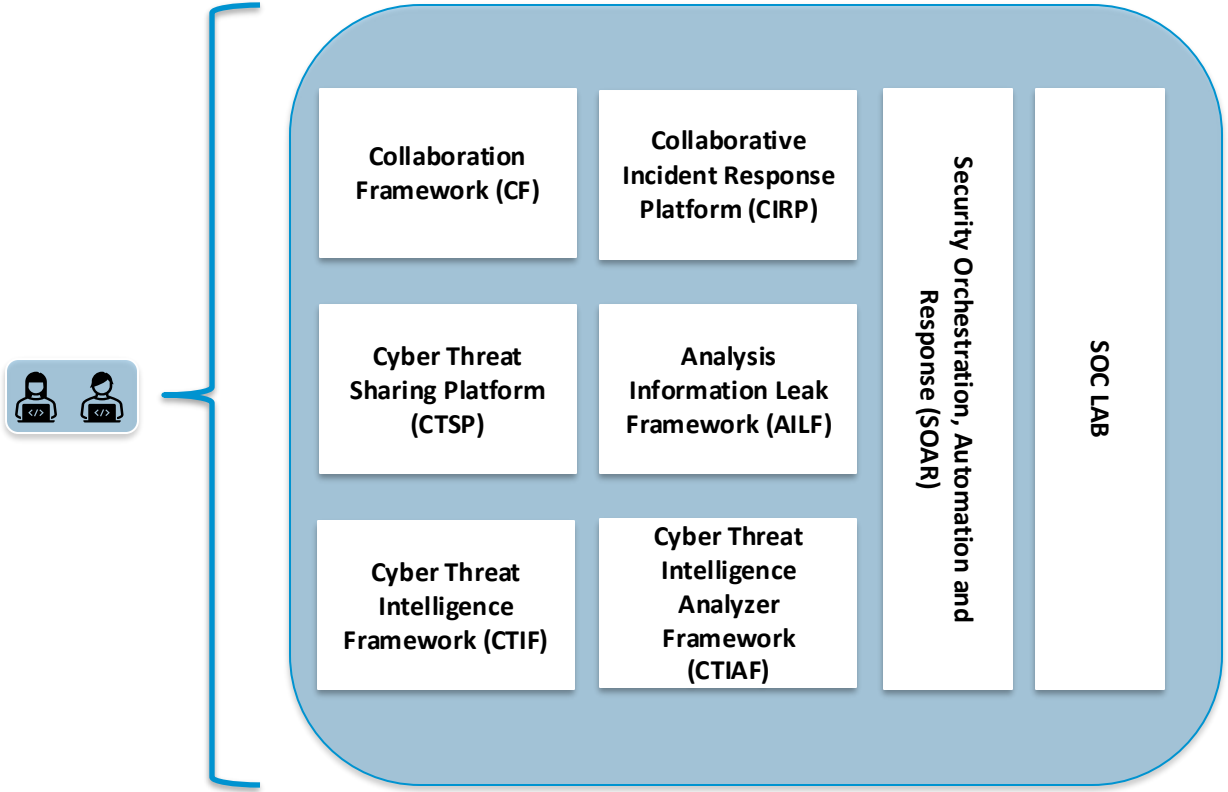
Möchte entwickelte Regeln an die Universitäten automatisiert verteilen.

Möchte entwickelte SOAR-Workflows an die Universitäten automatisiert verteilen.

Möchte entwickelte UseCases an die Universitäten automatisiert verteilen.

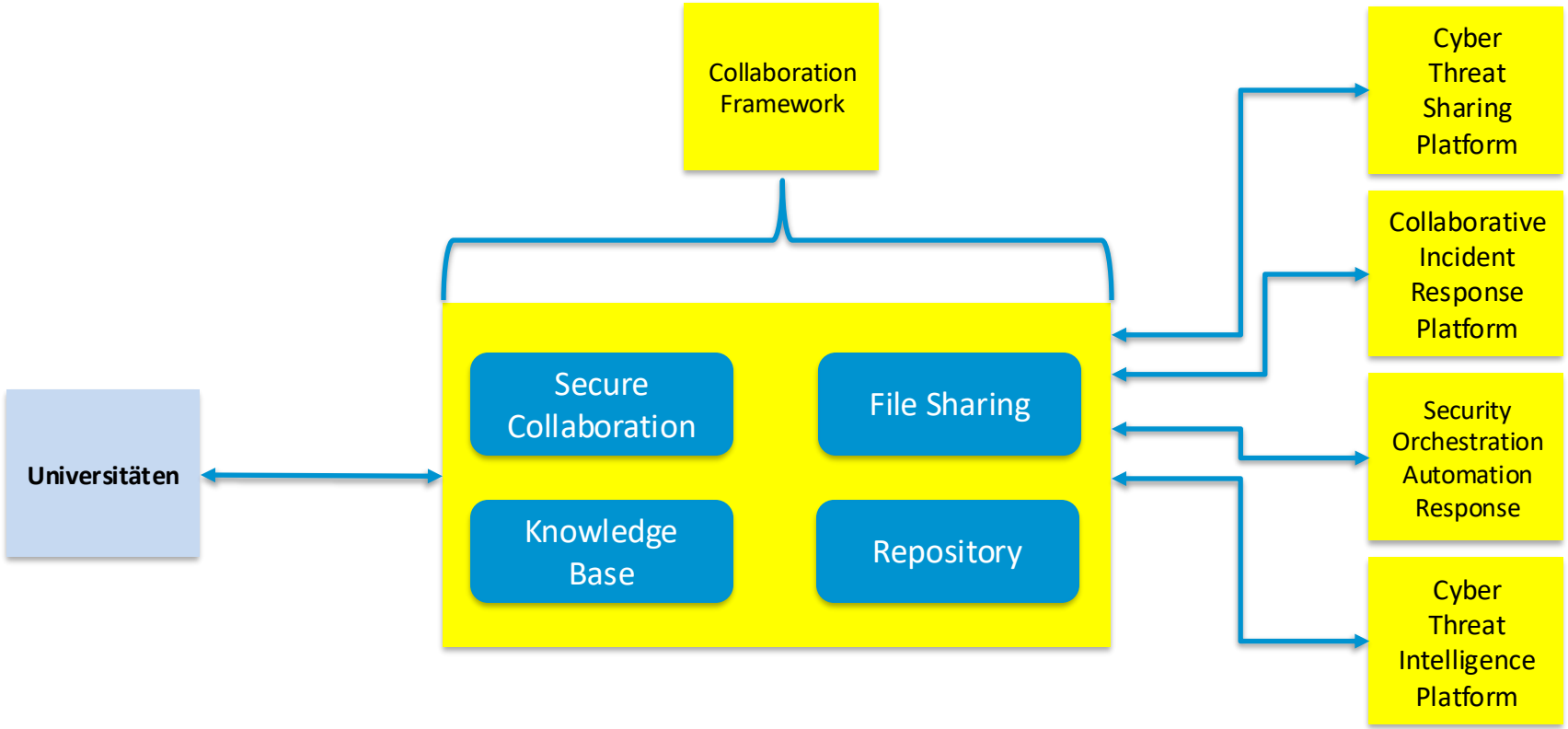
Möchte entwickelte Playbooks an die Universitäten automatisiert verteilen.

Fähigkeiten* eines ASOCs



*Mindestanforderungen der Fähigkeiten

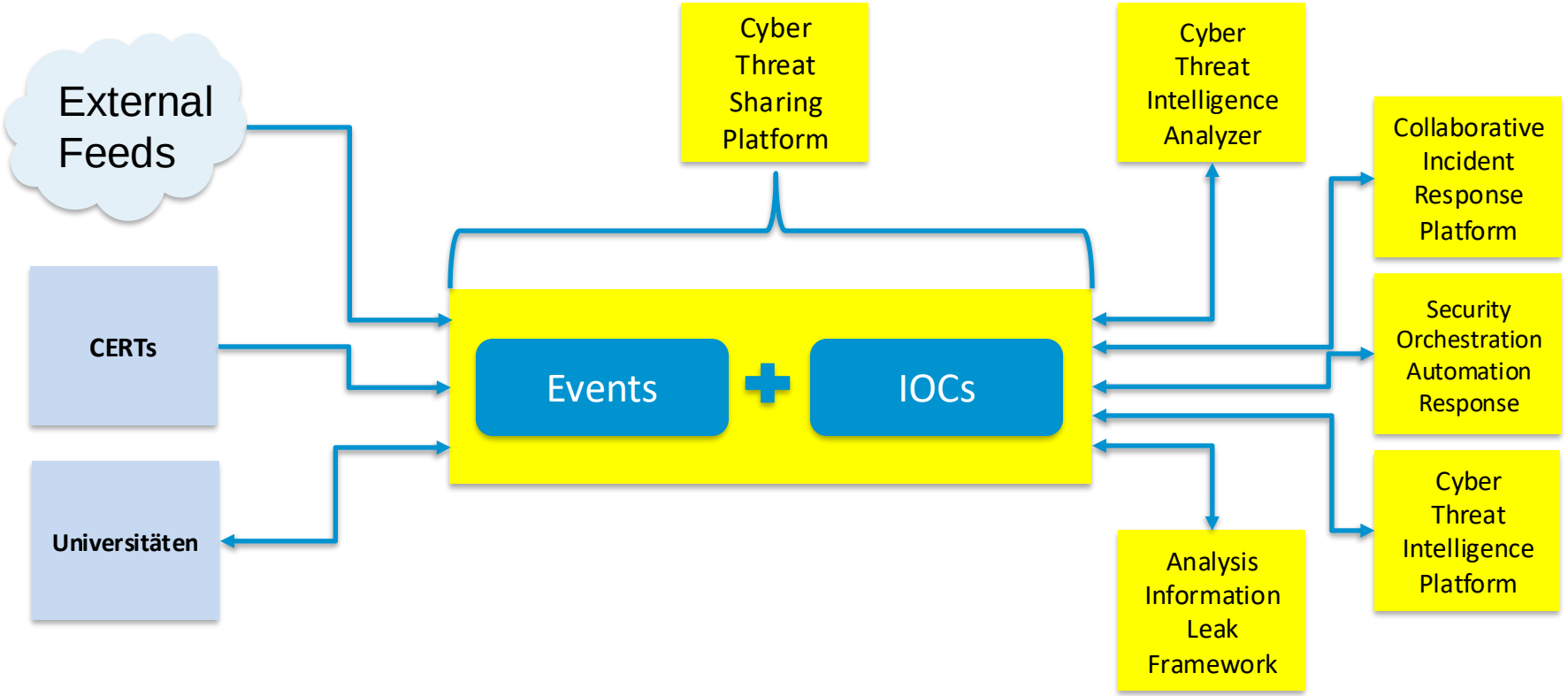
Collaboration Framework



Collaboration Framework

- Das Collaboration Framework gewährleistet gesamtheitlichen Informationsaustauch. Die Teilnehmer können sich per Chat Service austauschen.
- Beinhaltet ein Ticketing System, um Anfragen entgegenzunehmen und bearbeiten.
- Ebenso enthalten ist eine gemeinsame Wissensdatenbank und die Möglichkeit Files (Regeln, UseCases, etc.) zu teilen.

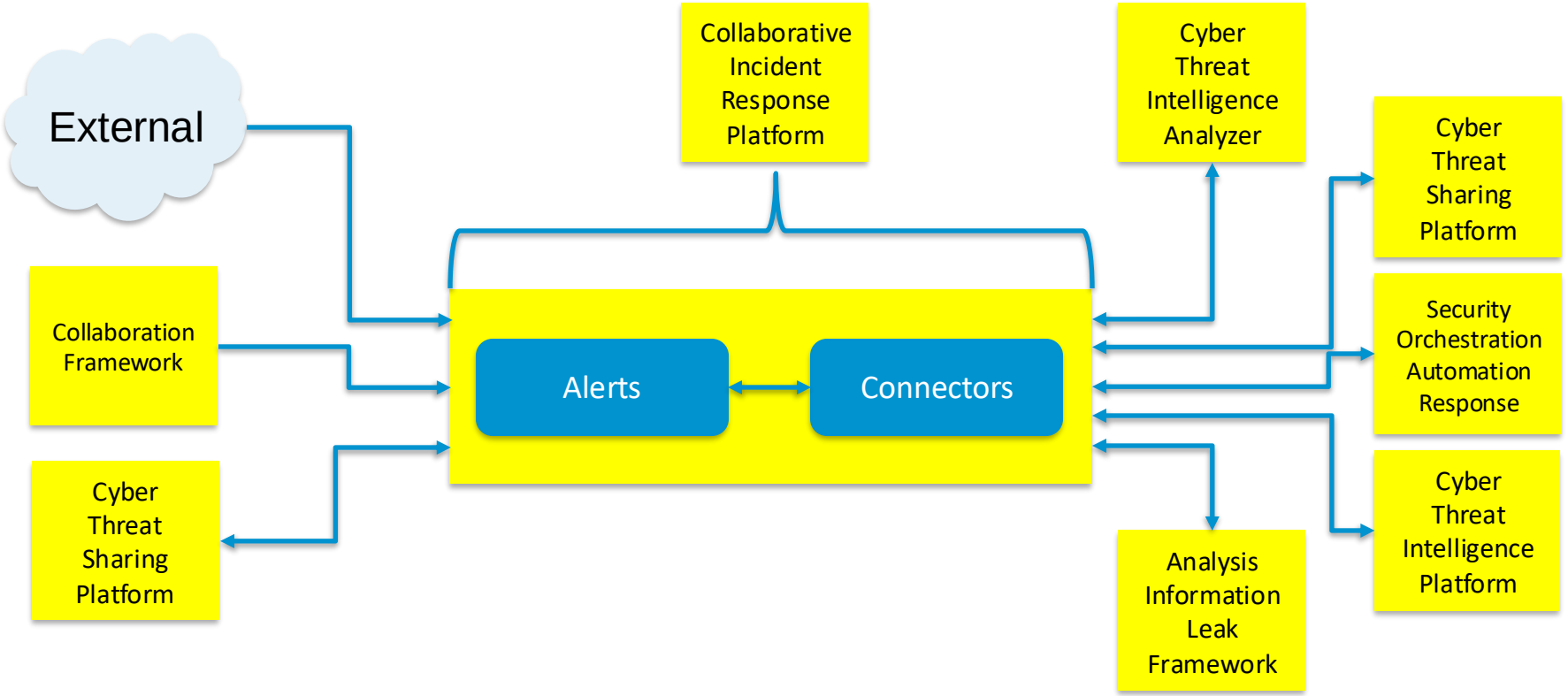
Cyber Threat Sharing Platform



Cyber Threat Sharing Platform

- Teilen, Speichern und Korrelieren von Kompromittierungsindikatoren
- von gezielten Angriffen, Threat Intelligence, Finanzbetrugsinformationen, Schwachstelleninformationen oder sogar Informationen zur Terrorismusbekämpfung.

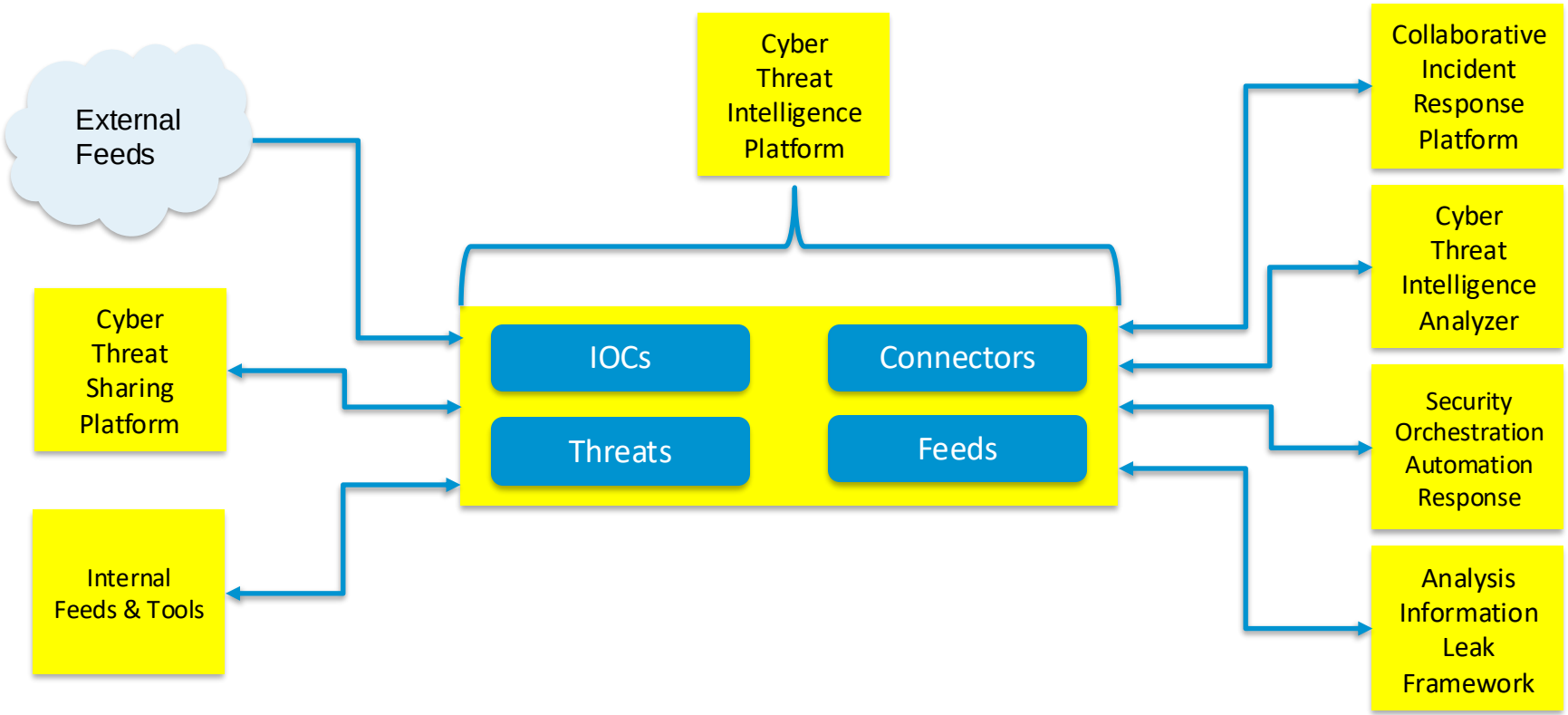
Collaborative Incident Response Platform



Collaborative Incident Response Platform

- Die Collaborative Incident Response Platform erfasst Informationen (z.B. Incident Anfragen, IOCs, etc) von den Teilnehmern, erstellt Cases, die individuell oder mit entsprechend vorbereiteten Use Cases im Sinne eines CERTs behandelt werden.
- Diese können automatisierte Informationen mit dem Cyber Threat Intelligence Framework abgleichen.
- Bei einer positiven Triage, sprich bei einem True Positive, und der Incident Behandlung, können im Anschluss die Threat Informationen der Cyber Threat Sharing Platform zur Verfügung gestellt werden und mit den Teilnehmern geteilt werden.

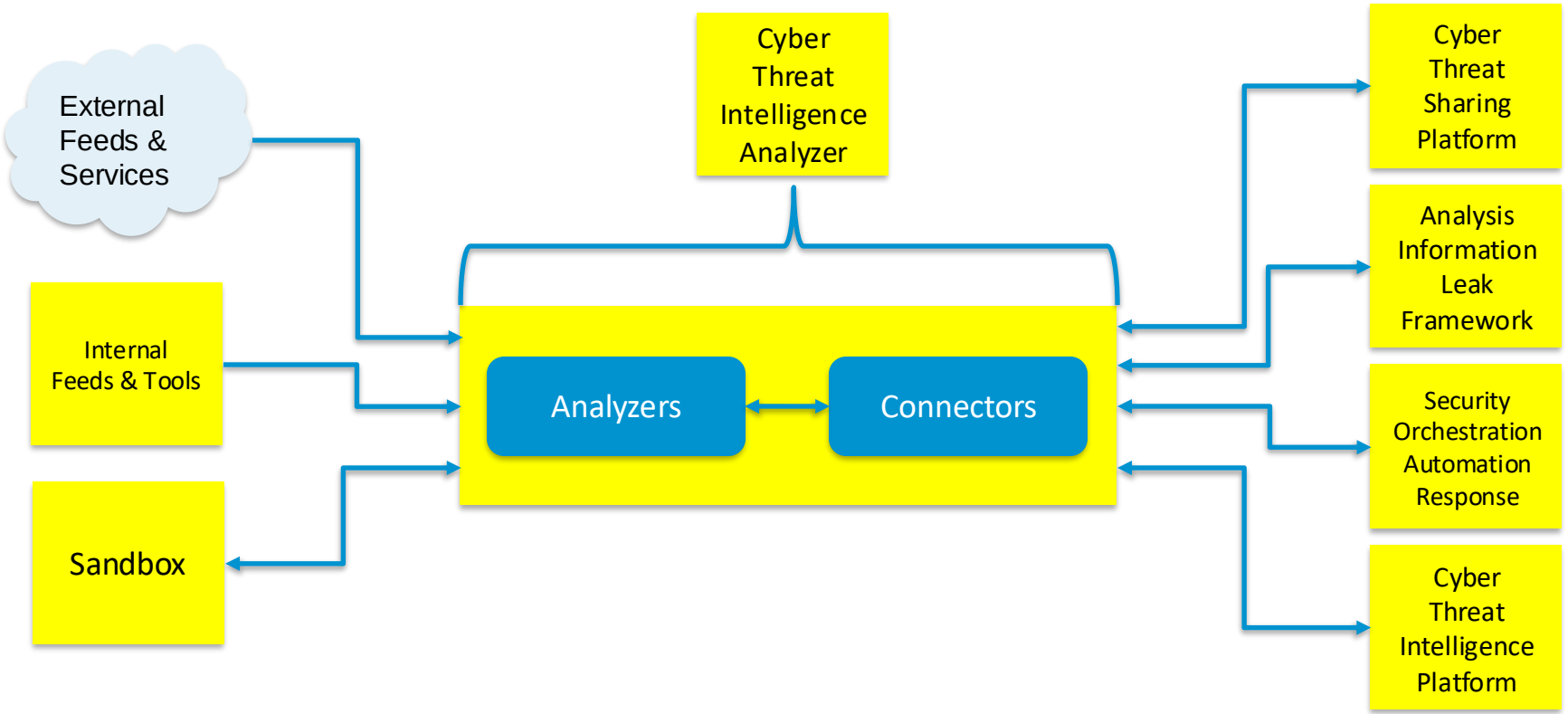
Cyber Threat Intelligence Framework



Cyber Threat Intelligence Framework

- Das Cyber Threat Intelligence Framework dient zur Verwaltung der Cyberbedrohungen.
- Technische und nichttechnische Cyberbedrohunginformationen.
- Ganzheitlicher Überblick zur Bedrohungslandschaft zur besseren Verfolgung und Überwachung.

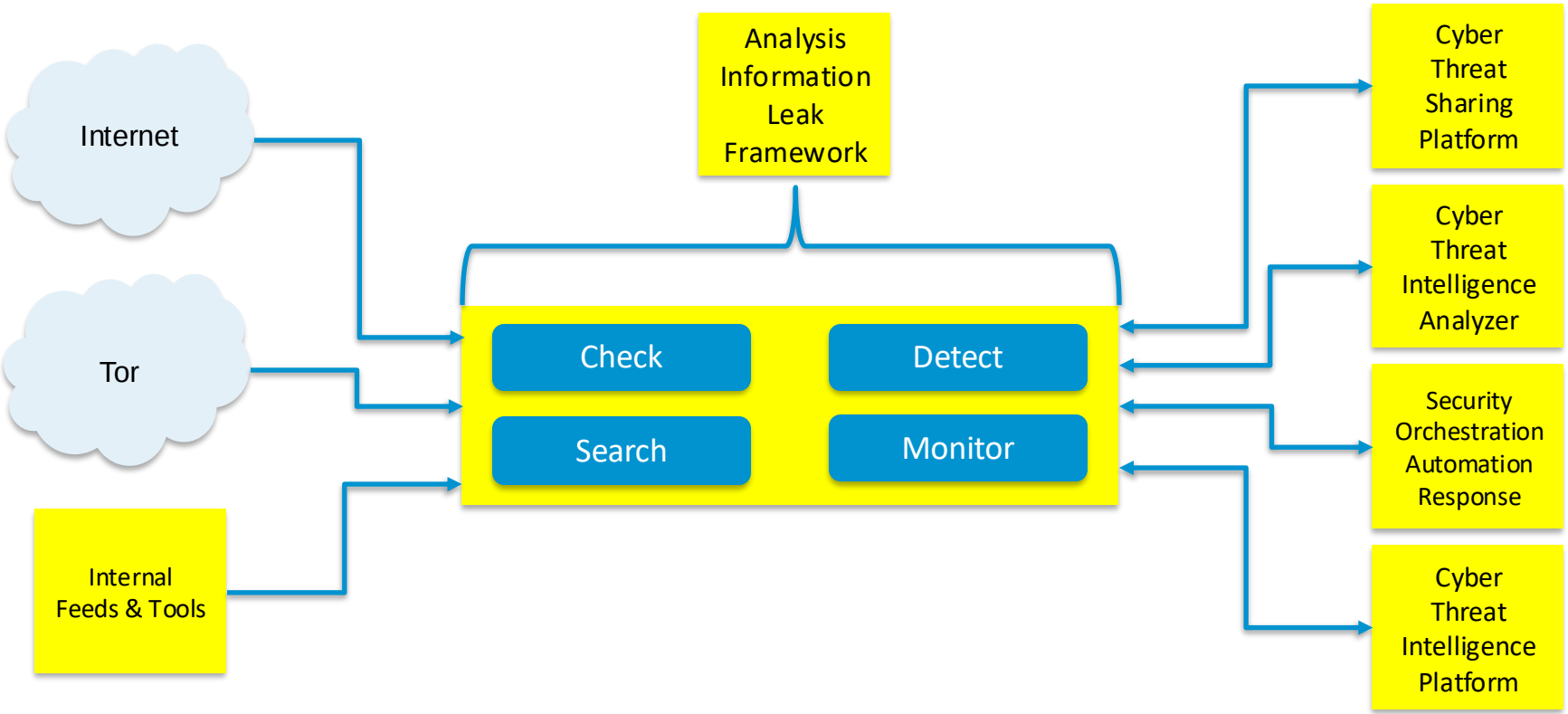
Cyber Threat Intel Analyzers Framework



Cyber Threat Intelligence Analyzer Framework

- Das Cyber Threat Intel Analyzers Framework ist Analyse- und Responseengine.
- Analyse von Observables wie IP- und E-Mail-Adressen, URLs, Domainnamen, Dateien oder Hashes, etc.
- Analysatoren, um Observables auf ihr Gefährdungspotenzial eines Sicherheitsvorfalles automatisiert prüfen zu können.

Analysis Information Leak Framework

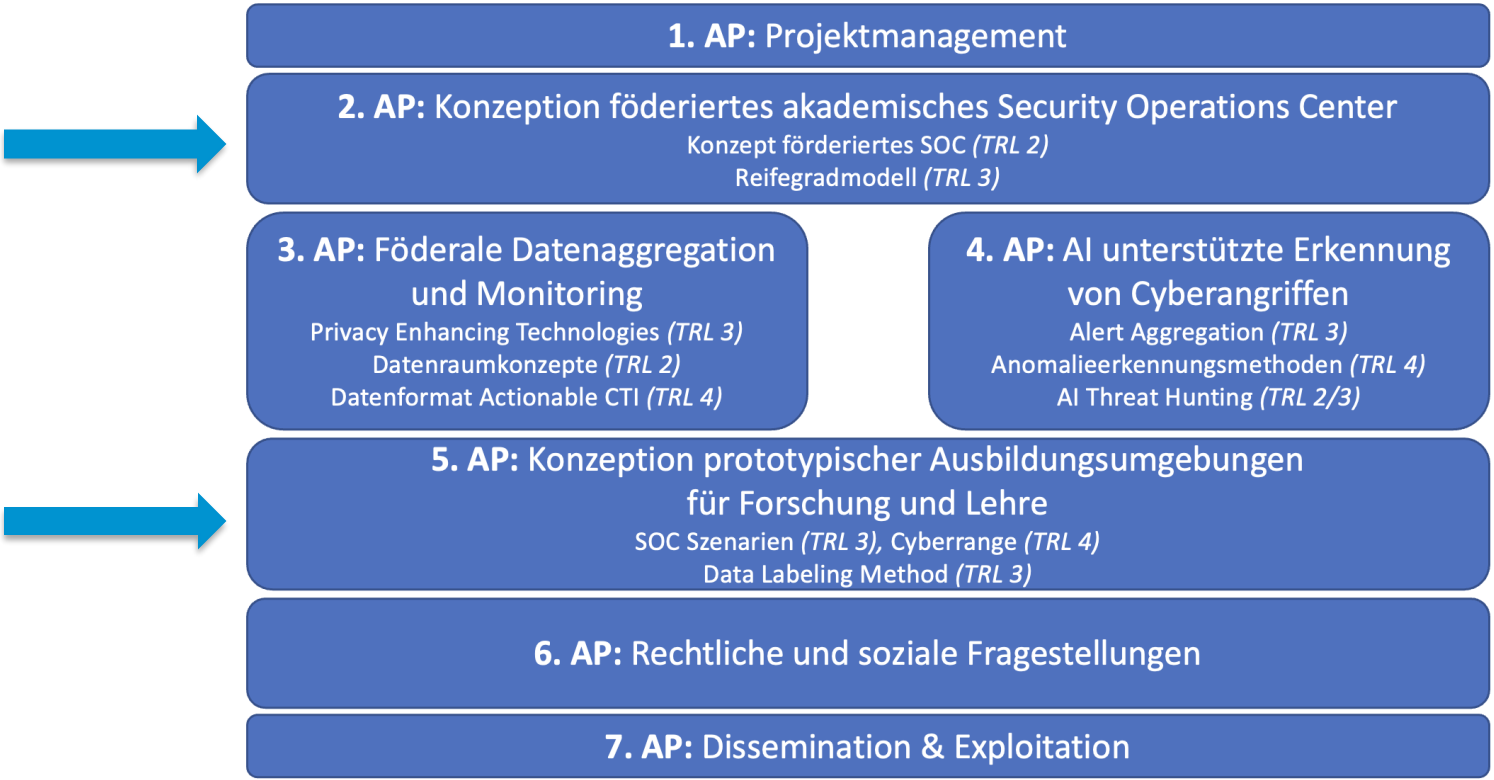


Analysis Information Leak Framework

- Das Analysis Information Leak Framework analysiert potenzielle Informationslecks und Open Source Intelligence Informationen (OSINT) aus unstrukturierten Datenquellen und Datenströmen.

3. Projektstatus ASOC

ASOC Arbeitspakete (AP)



Status ASOC Arbeitspakete

- AP2 Konzepte und Grundlagen für ein universitätsübergreifendes Security Operation Center
  - Erledigte Punkte:
    - Erstellung DraftV1 Dokument High Level Konzept
    - Factsheet
  - Derzeit in Arbeit:
    - Reifegradmodell Fragenkatalog Automatisierung
    - Liste Feeds
    - Evaluierung von relevanten Komponenten
    - Erstellung DraftV2 Dokument High Level Konzept
    - Präsentation Universitäten
- AP3 Sichere und datenschutzkonforme föderale Datenhaltung und übergreifende Analysen
  - Derzeit in Arbeit :
    - Erstellung Draft Dokument ASOC GAIA-X
- AP6 Rechtliche und soziale Fragestellungen
  - Derzeit in Arbeit :
    - Erstellung Evaluierungsplan
    - Erstellung Draft Dokument

4. Projektstatus ASOC

Weitere Projekte und Vorhaben im Umfeld von ASOC - genehmigt

- **CTI** Cyber Threat Intelligence Innovationslehrgang
  - Stärkung der Cybersicherheit in Österreich durch Qualifizierung von Mitarbeiter:innen im Bereich CTI.
- **LLM4CTI**: Exploratives Projekt
  - Untersuchung des Potenzials automatisierter Techniken auf Basis von Large Language Models (LLM)

Weitere Projekte und Vorhaben im Umfeld von ASOC - geplant

- Europäische Initiativen zur transnationalen Zusammenarbeit
  - Kooperation mit europäischen Stakeholdern
  - Z.B. DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT
- LLM4CTI Umsetzungsprojekt

Kontakte bei Interesse zur Zusammenarbeit:

Alexander Szönyi

aszoenyi@sba-research.org

Markus Klemen

mklemen@sba-research.org

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie

Bundesministerium Digitalisierung und Wirtschaftsstandort

FFG Forschung wirkt.

wirtschaftsagentur wien Ein Fonds der Stadt Wien

European Commission

FWF Der Wissenschaftsfonds.

netidee OPEN INNOVATIONS