gefördert im Rahmen des österr. Verteidigungsforschungsprogramms FORTE des BMF

CYBER ATTACK DECISION AND SUPPORT PLATFORM (CADSP)

3. Fachtagung FORTISSIMO

DDr. Florian Skopik
Thematic Coordinator
Cyber Security
AIT Austrian Institute of Technology

Eisenstadt, 25. April 2023

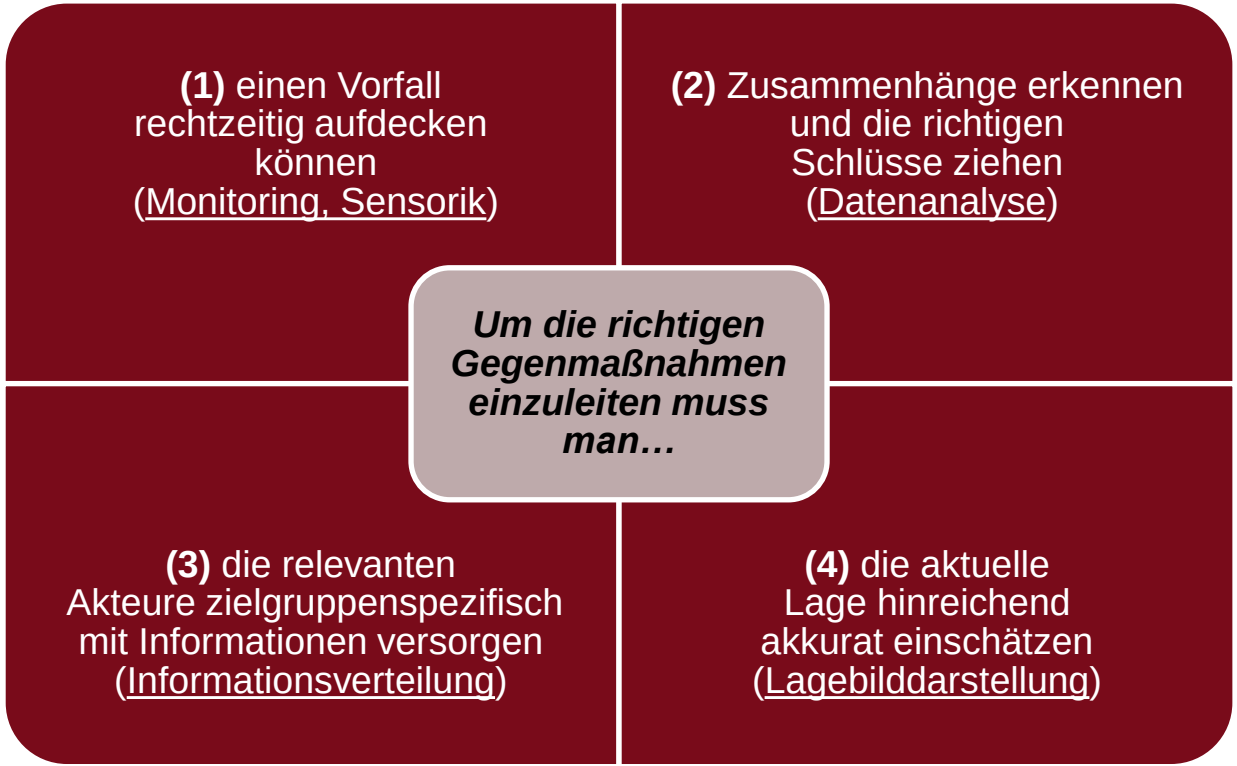
PROJEKTDATEN

- **FORTE** Projekt CADSP – Cyber Attack Decision and Support Platform
  - gefördert im Rahmen des österr. Verteidigungsforschungsprogramms FORTE des BMF
- **Laufzeit:** 01.11.2019 – 30.04.2022
- **Konsortialleitung:** Dr. Dr. Florian Skopik, AIT
- **Konsortium:**
  - AIT Austrian Institute of Technology
  - Frequentis AG
  - BMLV

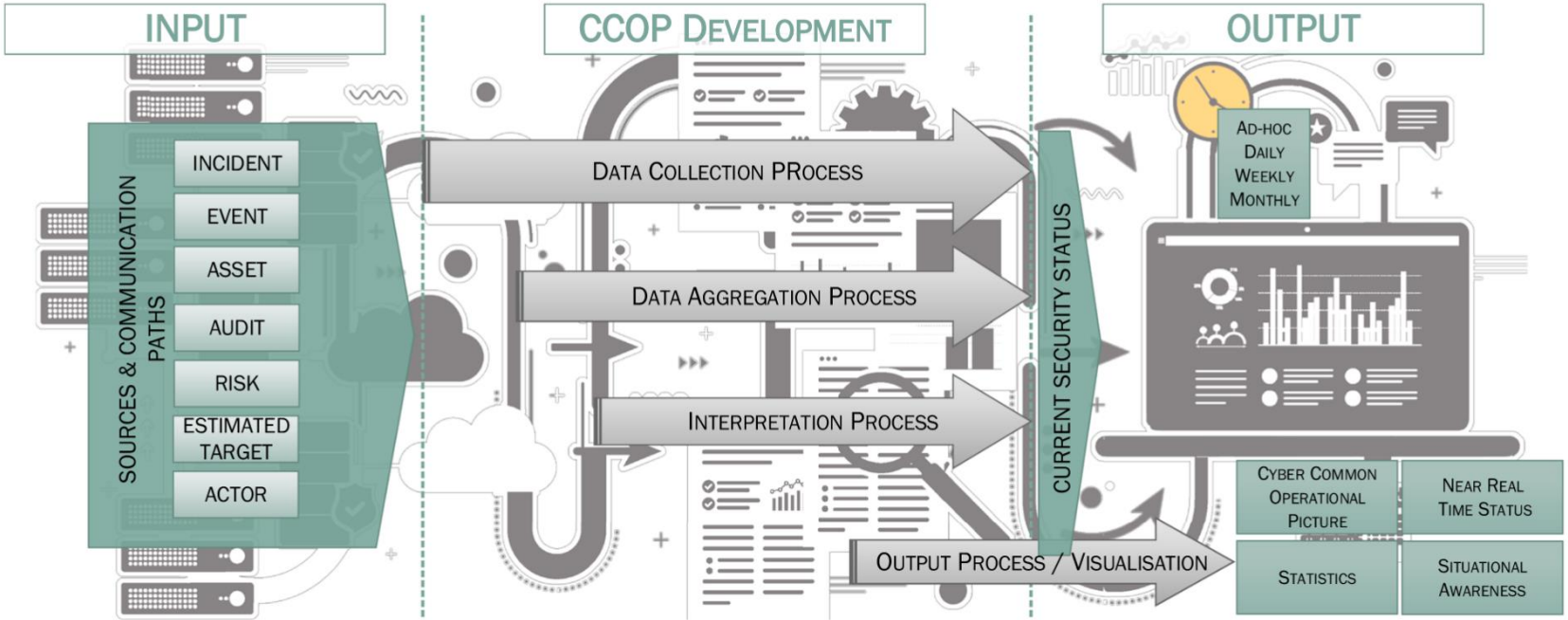
STATUS QUO IN DER CYBER ABWEHR

- Ständig ändernde **Bedrohungslage**
  - Neue Angriffstechniken
- Veränderte **Rahmenbedingungen**
  - Gesetzeslage: NIS(2), DSGVO, Cyber Security Gesetz
  - Neue Einrichtungen bei Behörden: CSC, CDZ
  - Neue Pflichten (Meldepflicht der BwDs, Audits, …)
  - Neue Technologien: Cloud, Mobile, (I)IoT, …
- Komplexe und fordernde Situationen bei „Ereignissen“
- Fundierte **Grundlage zur Entscheidungsfindung** notwendig!
  - Umgang mit Bedrohungen: Risikobewertung durch Trendanalysen
  - Umgang mit Vorfällen (Incidents)
    - Bewertung von Handlungsoptionen im konkreten Anlassfall

AUSPRÄGUNG VON VITALEN CYBER INCIDENT RESPONSE FÄHIGKEITEN

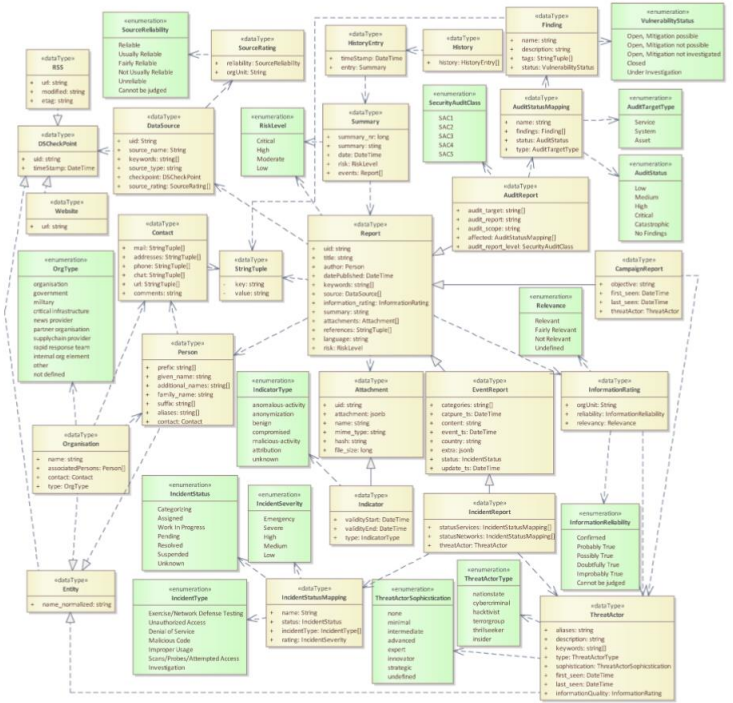


GESAMTANSATZ IN CADSP



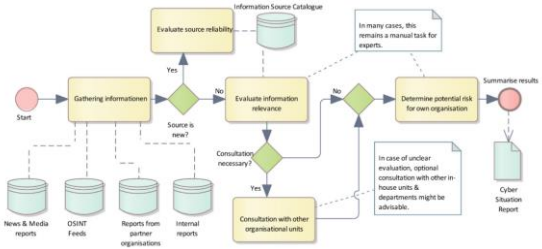
HARMONISIERTES DATENMODELL

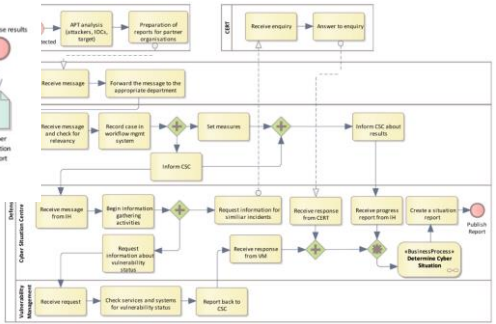
- Zusammenführen aller relevanten Informationen zur Beurteilung der Lage
  - Incident Handling, Risiko Management, Service Delivery, Vulnerability Management
- Anbindung div. Datenquellen
  - Asset Mgmt, CMDB, Service Catalog, Monitoring Systeme, SecReports, Audits…
- Wiederverwendung vieler Formate/Standards
  - CVE, CVSS, CPE, STIX, …
- Balance zwischen Flexibilität und Struktur

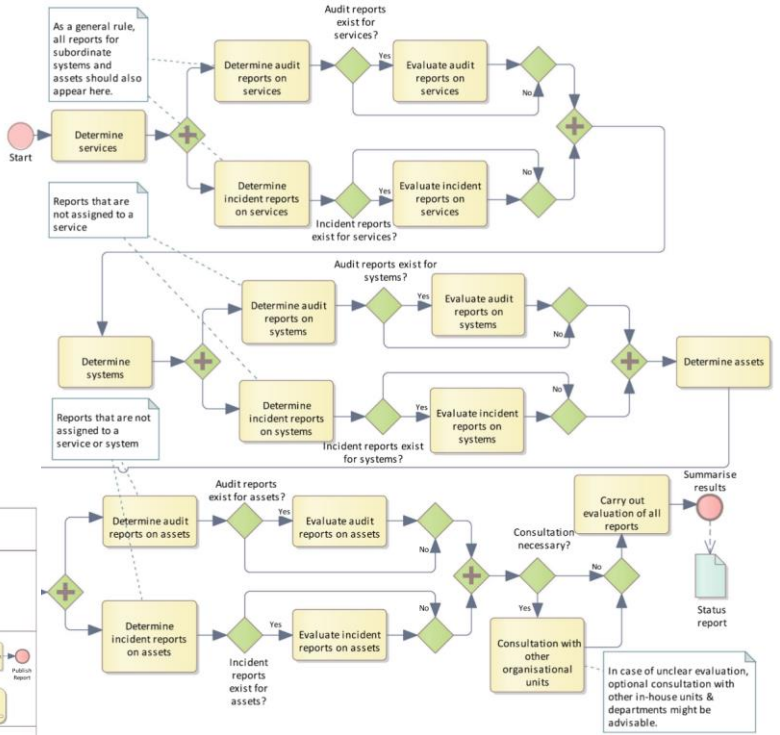


CONOPS - PROZESSMODELLE

- BPMN Workflows für die wichtigsten Prozesse
- Lfd. Sammeln der Daten
- Dateninterpretation und Erhebung der Lage
- Anfertigen der Lageberichte
- Reaktion auf Vorfälle
  - Interaktionen, Informationsflüsse



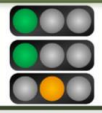




KONZEPT DES LAGEBILDES

- Zielgruppenspezifische Lagebilder
  - Rolle/Entscheidungen
  - Zeit: Tägl., wöchentl. Monatl.
- Grundaufbau
  - Generelle Lageübersicht (Ampel)
  - Zusätzl. textuelle Aufbereitung
  - Trends hinsichtlich festgelegter KPIs
  - Service Delivery Status
    - Nach Service-Klassen
    - Nach Abteilung

AD HOC SITUATIONAL REPORT 2021/11/11

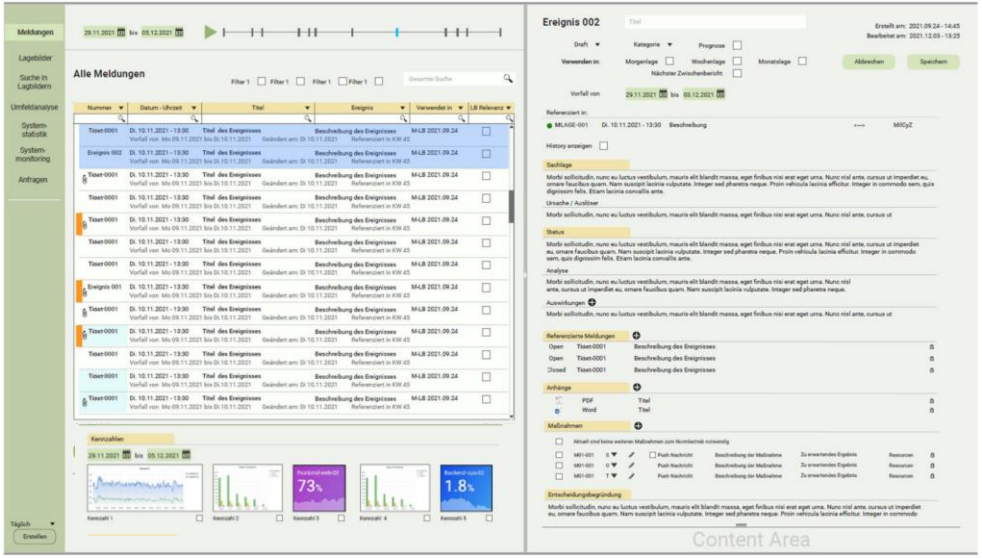
TOPICS	ASSESSMENT	EVENTS
General Status ICT | Domestic		No limitations on services at domestic and international level. Potential security incident.
General Status ICT | Abroad		
Cyber Security		

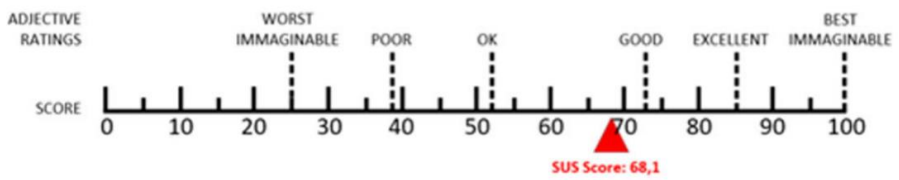
SUMMARY	ASSESSMENT
Based on PO's notification (received 11/11/2021), there was an APT security incident in PO's ICT infrastructure. The information provided by PO included indicators, vulnerabilities, as well as an initial attribution of the attacker. According to PO's experts, the adversary is a state-backed cyber espionage group from the state of Ostarrichi. CERT confirmed increased suspicious activities upon request that could also be attributed to Ostarrichi. IH confirmed the occurrence of traces (malware attachments) on Public Relations Department mail systems. VM confirmed that occurrence of vulnerabilities mentioned by PO during the suspected attack period. IH also initiated countermeasures. At this time, it cannot be ruled out that an APT is present. The Public Releation Department systems have been taken offline for the time being and are under forensic investigation. No traces of an attack have been found on critical systems at this time, and investigations are ongoing.	 Increased attention needed on mission critical services. Potential APT present!

CYBER-SECURITY SITUATION OVERVIEW (LAST 30 DAYS)			RISK MGMT	SERVICE SECURITY STATE			
INDICATOR	#	T		SERVICES / DEPARTMENT	MISSION-CRITICAL	EXISTENTIAL	OTHER
Major Global Security Events	3	↘		Public	DISRUPTED	n/a	DISRUPTED
Ext. Partner Incidents	2	↗	INFO SEC MGMT	Armed Forces	CAUTION	NO ISSUE	NO ISSUE
Internal Incident Reports	1	↗		Intelligence	CAUTION	NO ISSUE	n/a
Internal Vulnerability Reports	10	↗		Command	CAUTION	NO ISSUE	n/a

UMSETZUNG IM PROOF-OF-CONCEPT

- Sammlung von Meldungen/Reports aus Fachabteilungen
  - Neue Risikobewertungen
  - Neue Vulnerabilities
  - Neue Vorfälle
  - Neue Auditberichte
  - Allg. politische Lage
- Eingliedern strukturierter Informationen durch Anbindung an div. „real-time“ Datenquellen (OSINT)
- Teil-automatisierte Auswertung bzw. Aggregation mittels Machine Learning und NLP (Konzept)
- Berechnung von KPIs und visuelle Darstellung





RESULTATE DES PROJEKTS

Abbildung CONOPS für BMLV

- Bedarfsträgerprozesse
- Organigramm beteiligter Akteure und ihre Rollen/Profile
- Relevanz von Fachdaten für unterschiedliche Akteure

CADSP Architektur

- Modulare, offene, tragfähige und erweiterbare Architektur mit standarisierten Schnittstellen

Machine Learning zur Datensammlung u. Bewertung

- Konzepte und Modelle zur Datensammlung und Analyse
- Katalog möglicher Datenquellen
- Erarbeitung geeigneter Analyse-Algorithmen

Implementierung eines PoCs

- Funktionaler Prototyp kompatibel zu existierender Toollandschaft
- Für ausgewählte BMLV Szenarien und als Grundlage weiterführender Human Performance Tests

Validierung der PoCs

- Spezifische Testpläne und Testmethodik
- Human Performance Tests zur Bestimmung der Effizienzsteigerungen
- User Acceptance Tests

Wissenschaftlicher Diskurs

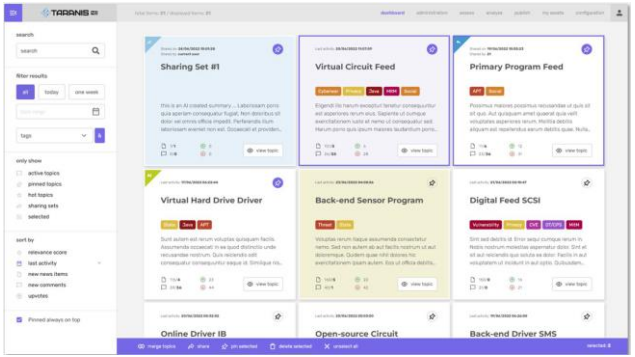
- Einbringung allg. Konzepte, losgelöst vom BMLV Kontext, in die wissenschaftl. Community
- Vernetzung mit Stakeholdern quer über Europa

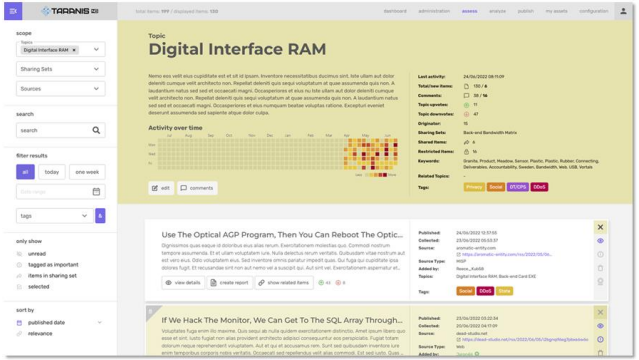
Skopik F., Bonitz A., Grantz V., Goehler G. (2022): From scattered data to actionable knowledge: flexible cyber security reporting in the military domain. International Journal of Information Security, Vol.21, pp. 1323-1347, Springer.

AUSBLICK: AWAKE (2021-2024)

- CEF Projekt mit CERT.at, BMI und BKA
- OSINT Collection und Clustering
- NLP Features (machine learning)
  - Keyword Extraction
  - Topic/Story Clustering
  - Erstellen von Zusammenfassungen
- Erstellen von Reports („Tagesberichte“)
- Zielgruppenspezifisches Teilen von Reports

- Erweiterungen von taranis-ng (CERT.sk)
  - Open Source: https://github.com/ait-cs-IaaS/Taranis-NG





DANKE FÜR IHRE AUFMERKSAMKEIT!

Florian Skopik
florian.skopik@ait.ac.at

25. April 2023