Bundesministerium
Finanzen

3. FORTISSIMO Fachtagung

CADSP – Cyber Attack Decision and Support Platform

Kontakt
Dr. Dr. Florian Skopik
E-Mail: florian.skopik@ait.ac.at
Web: https://www.ait.ac.at/cyber-security/

Projektziel

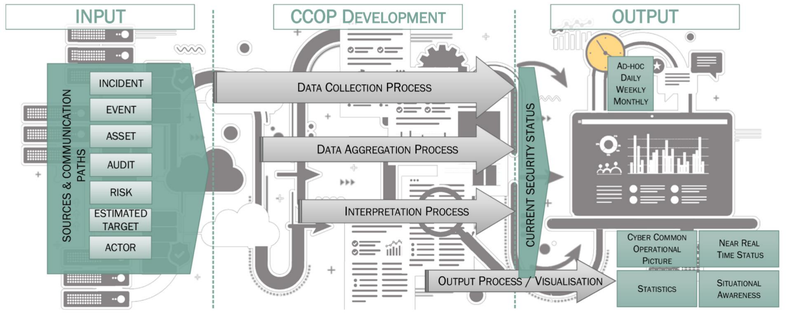
Das Ziel von CADSP ist die wissenschaftlich-fundierte Konzeption und prototypische Evaluierung einer Cyber Attack Decision and Support Plattform (CADSP) für ausgewählte BMLV (Bundesministerium für Landesverteidigung) Anwendungsfälle und definierte Prozesse für Cyber Incident Responses speziell im militärischen Umfeld. Dabei soll CADSP untersuchen, welche Datenquellen im gewählten Anwendungsfall geeignet sind, um hinreichend akkurate Informationen zur Lageeinschätzung in Bezug auf den aktuellen Sicherheitsstatus der eigenen Infrastruktur und stattfindender Cyber-Angriffe zu ermöglichen. Darauf aufbauend sollen eine passende Benutzeroberfläche und Lagebildvisualisierung generiert werden, die den Cyber Incident Response Prozess optimal unterstützen. Das Projekt soll sicherstellen, dass eine User-zentrierte Unterstützung in Form eines Software-Prototyp die Situational Awareness und dadurch die Handlungsfähigkeit der militärischen Nutzer nachweislich hebt. Es wird hierzu mit anerkannten qualitativen und quantitativen Methoden für Benutzertests gearbeitet.

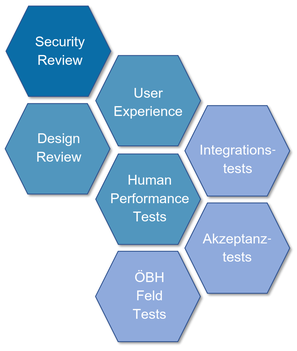
Projektlaufzeit: 01.11.2019 – 30.04.2022

AIT Austrian Institute of Technology · FREQUENTIS For a safer world · Bundesministerium Landesverteidigung

Concept of Operations und Grobkonzept

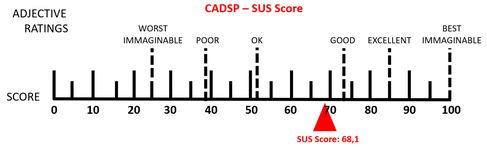
Zielsetzungen
- Definition des Lagebildbegriffs und Situationsbewusstseins des Bedarfsträgers
- Identifikation von Praxis-Anwendungsfällen
- Formulierung von funktionalen und nicht-funktionalen Anforderungen
- Komplettierung mit Anforderungen aus theoretischen Quellen
- Entwicklung des CONOPS

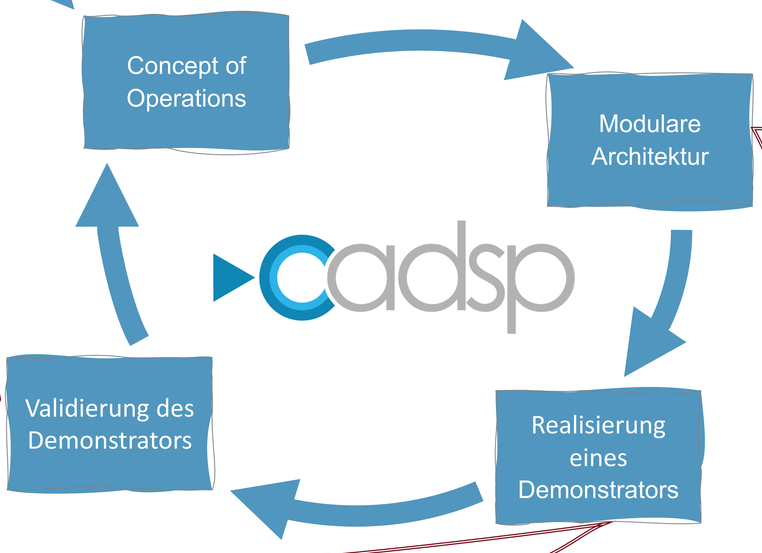




Validierung des Demonstrators

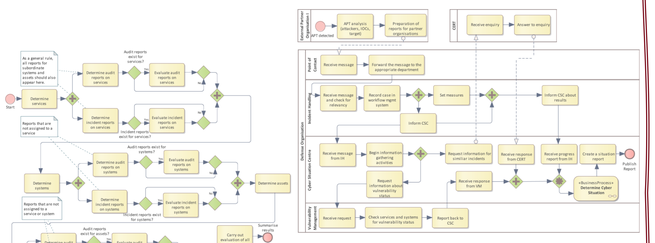
Zielsetzungen
- Technische Tests der Gesamtlösung
- Human Performance Tests
- Untersuchung der Einsetzbarkeit des finalen CADSP in einem realen Szenario
- Stakeholder Workshop und Feedback Sessions



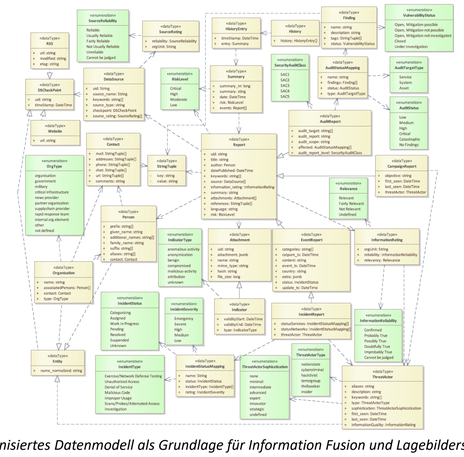


Modulare Architektur

Zielsetzungen
- Generelles Architekturdesign und Schnittstellen zu BMLV Tools
- Strategie und Techniken des Loggings und der Sensorik
- Normalisierung und Common Information Model
- Untersuchung der Möglichkeiten der Anomalieerkennung in Betriebsdaten



Beispielhafte Lagebildprozesse: „Erhebung der eigenen Lage“ (links); Behandlungsprozess für UC „Sicherheitsvorfall bei einer externen Partnerorganisation“ (oben)



Harmonisiertes Datenmodell als Grundlage für Information Fusion und Lagebilderstellung

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

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 Ostarrich. CERT confirmed increased suspicious activities upon request that could also be attributed to Ostarrich. 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 Relation 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.

ASSESSMENT

Increased attention needed on mission critical services. Potential APT present!

CYBER-SECURITY SITUATION OVERVIEW (LAST 30 DAYS)

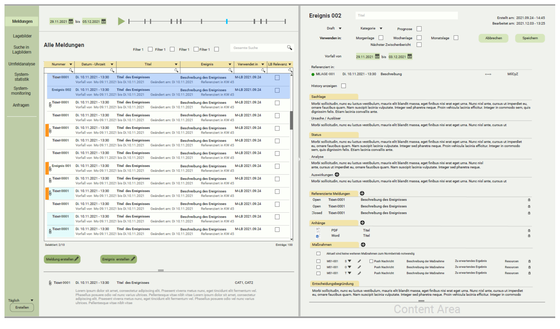
INDICATOR	#	T
Major Global Security Events	3	↘
Ext. Partner Incidents	2	↗
Internal Incident Reports	1	↗
Internal Vulnerability Reports	10	↗

RISK MGMT

INFO SEC MGMT

SERVICE SECURITY STATE

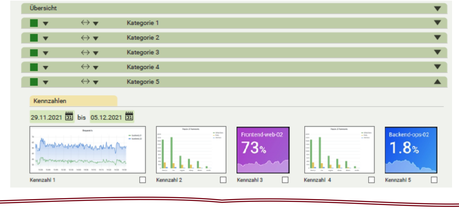
DEPARTMENT / SERVICES	MISSION-CRITICAL	EXISTENTIAL	OTHER
Public	DISRUPTED	n/a	DISRUPTED
Armed Forces	CAUTION	NO ISSUE	NO ISSUE
Intelligence	CAUTION	NO ISSUE	n/a
Command	CAUTION	NO ISSUE	n/a



Konzept-Lagebild (links) und implementierte Demonstratoren (oben, rechts)

Realisierung eines Demonstrators

Zielsetzungen
- Implementierung / Integration Cyber Security Sensorik und Anbindung an existierende Datenquellen
- Anbindung an BMLV Bestandstools
- Integration neuer Incident Response Tools
- Proof-of-Concept Lagebildvisualisierung für BMLV Anwendungsfälle



FFG Forschung wirkt. · FORTE · Bundesministerium Landesverteidigung