CADSP

Cyber Attack Decision and Support Platform – Technische Machbarkeitsstudie und Validierung

Programm / Ausschreibung	FORTE, FORTE, FORTE - Kooperative F&E-Projekte	**Status**	abgeschlossen
Projektstart	01.11.2019	**Projektende**	30.04.2022
Zeitraum	2019 - 2022	**Projektlaufzeit**	30 Monate
Keywords	Cyber Lagebild, Cyber Sensorik, Incident Response Prozesse		

Projektbeschreibung

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.

Abstract

The aim of CADSP is the scientifically founded conception and prototypical evaluation of a Cyber Attack Decision and Support Platform (CADSP) for selected BMLV (Federal Ministry of Defense) use cases and defined processes for Cyber Incident Responses especially in the military environment. In doing so, CADSP should investigate which data sources are suitable in the selected application scenario in order to provide sufficiently accurate information for assessing the current security status of an infrastructure and cyber attacks taking place. Building on this, a suitable user interface and situation visualization are to be generated that optimally support the Cyber Incident Response process. The project aims to en-sure that user-centered support in the form of a software prototype demonstrably enhances situational awareness and thereby the ability of military users to act. The project will apply recognized qualitative and quantitative methods for user testing.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Bundesministerium für Landesverteidigung
- FREQUENTIS AG