

## CONTAIN

Effiziente Reaktion auf IT-Sicherheitsvorfälle in transnationalen Lieferketten

<b>Programm / Ausschreibung</b>	KIRAS, Kooperative F&E-Projekte, KIRAS Kooperative F&E-Projekte 2021	<b>Status</b>	laufend
<b>Projektstart</b>	01.03.2023	<b>Projektende</b>	31.08.2025
<b>Zeitraum</b>	2023 - 2025	<b>Projektlaufzeit</b>	30 Monate
<b>Keywords</b>	Supply Chain Sicherheit, Cyber Sicherheit, Framework, Serious games und Simulationen		

### Projektbeschreibung

Die Resilienz von ICT-Infrastrukturen ist von zentraler Bedeutung für das Funktionieren von Supply Chains. Je verlässlicher diese kritischen Infrastrukturen sind, desto höher ist auch die Planbarkeit für Produktion und Lieferketten, aber auch für die Endkund:innen. Die Absicherung dieser Systeme gegen Bedrohungen aus dem Cyberraum ist somit zentral für das Funktionieren einer „Smart Economy“, die auf dem Prinzip „Just in Time“ aufbaut und möglichst ohne Zwischenlagerung auskommen und Transportwege optimieren will. Im Fall von Cyber-Angriffen ist es daher essentiell, auf erprobtes Incident Handling, ausreichende Früherkennung und entsprechende Entscheidungsmodelle zurückgreifen zu können, um die Beeinträchtigung der ICT-Systeme möglichst zu reduzieren.

Das Projekt CONTAIN zielt daher darauf ab, Bewusstsein für Themen des Incident Response und der nachfolgenden Prozesse zu steigern und Tools des Software Engineerings, sowie entsprechende Referenzprozesse zu definieren. Es zielt dabei auf die folgenden drei Hauptaspekte ab: (1) die Auswirkungen von Cyberangriffen zu reduzieren, (2) die Anzahl und Kritikalität erfolgreicher Cyberangriffe zu vermindern und (3) die Effizienz der Aufklärungsrate und dem Aufwand von Cyberangriffen zu steigern. CONTAIN fokussiert sich dabei auf Prozesse und Verfahren, die notwendig sind, um resilient auf IT-Sicherheitsvorfälle zu reagieren, deren Auswirkungen zu minimieren, Schwachstellen zu beheben, sowie die Robustheit und Souveränität der Systeme zu erhöhen. Für diesen Zweck plant CONTAIN Serious Games einzusetzen, um die Verhaltensweisen der Anwender:innen zu hinterfragen, Prozesse (operative Prozesse und Entscheidungsprozesse) zu analysieren, definieren und validieren, das Krisenmanagement zu definieren und validieren, sowie die Akteur:innen und ihre Verantwortlichkeit zu koordinieren. Das daraus entstehende Simulationsmodell dient schlussendlich der Identifizierung kritischer Prozesse, sowie etwaiger Ressourcen- und Kapazitätsengpässe, woraus relevante Möglichkeiten zur Optimierung von Prozessen abgeleitet werden, die insbesondere für Kleine- und Mittlere Unternehmen geeignet sind.

### Abstract

The resilience of ICT infrastructures is of central importance for the functioning of supply chains. The more reliable these critical infrastructures are, the greater the predictability for production and supply chains, but also for end customers. Securing these systems against threats from cyber space is therefore central to the functioning of a "smart economy" that is

based on the principle of "just in time" and wants to manage without intermediate storage and optimise transport routes as far as possible. In the case of cyber attacks, it is therefore essential to be able to fall back on proven incident handling, sufficient early detection and corresponding decision models in order to reduce the impairment of ICT systems as much as possible.

The CONTAIN project therefore aims to raise awareness of incident response issues and subsequent processes and to define software engineering tools and corresponding reference processes. It targets the following three main aspects: (1) reduce the impact of cyber-attacks, (2) reduce the number and criticality of successful cyber-attacks, and (3) increase the efficiency of cyber-attack detection rate and effort. CONTAIN focuses on processes and procedures necessary to respond resiliently to IT security incidents, minimise their impact, address vulnerabilities, and increase the robustness and sovereignty of systems. For this purpose, CONTAIN plans to use serious games to question the behaviour of the users, to analyse, define and validate processes (operational processes and decision-making processes), to define and validate crisis management, and to coordinate the actors and their responsibilities. The resulting simulation model ultimately serves to identify critical processes, as well as any resource and capacity bottlenecks, from which relevant options for optimising processes are derived that are particularly suitable for small and medium-sized enterprises.

### **Projektkoordinator**

- AIT Austrian Institute of Technology GmbH

### **Projektpartner**

- Universität Wien
- Roland Spedition GmbH
- team Technology Management GmbH
- Kwizda Holding GmbH
- Gartner KG.
- Bundesministerium für Landesverteidigung
- Universität für Bodenkultur Wien
- VICESSE Research GmbH