# ASOC

Towards an Academic Security Operations Center

| | | | |
|---|---|---|---|
| **Programm / Ausschreibung** | KIRAS, Kooperative F&E-Projekte, KIras Kooperative CS F&E Projekte (KFE CS_2022) | **Status** | laufend |
| **Projektstart** | 08.01.2024 | **Projektende** | 31.03.2026 |
| **Zeitraum** | 2024 - 2026 | **Projektlaufzeit** | 27 Monate |
| **Keywords** | SOC, Gaia-X, Künstliche Intelligenz | | |

## Projektbeschreibung

Österreichische Universitäten müssen sich den sicherheitstechnischen Herausforderungen stellen, die sich einerseits durch reale Bedrohungen von außen und andererseits durch regulatorische Anforderungen ergeben. Während viele Universitäten über exzellentes technisches Personal verfügen, deren Know-How über viele Jahre etwa im Zuge des Aufbaus des ACOnets gewonnen wurde, sind strategische, universitätsweite Maßnahmen aufgrund der förderalen Strukturen der Universitäten und der heterogenen IT-Systeme oftmals schwierig und mit vielen Hindernissen verbunden. Zusätzlich kämpfen die Universitäten um den Erhalt ihrer herausragenden Techniker:innen, da diese wegen des vorherrschenden Fachkräftemangels oftmals von großen Unternehmen erfolgreich abgeworben werden.
In vorliegenden Projekt wollen wir Universitäten auf dem Weg zu einer institutionsübergreifenden Struktur maßgeblich unterstützen, indem wir ein Vorgehensmodell für notwendige vorbereitende Maßnahmen konzipieren, relevante Komponenten auf Basis innovativer Ansätze wie Gaia-X und AI/Machine Learning entwickeln und begleitende Maßnahmen wie Cyberrange Trainingskonzepte sowie Methoden zur Selbstevaluierung der Reifegrade der Universitäten entwerfen. Eine zentrale Forschungsfrage ist, wie Universitäten aus der enormen Menge an Log- und Metadaten in annähernd Echtzeit Bedrohungen und Angriffe erkennen können, um zeitgerecht Gegen- und Schutzmaßnahmen einleiten zu können.
Eine weitere essentielle Frage ist, ob es technisch und organisatorisch machbar ist, Gesamtlösungen, die zwangsläufig tiefen Einblick in die IT-Systeme der beteiligten Organisationen benötigen, zu entwickeln, die die digitale Souveränität Österreichs und Europas in diesem systemkritischen Umfeld erhalten.

## Abstract

Austrian universities have to face the security challenges posed by real-world external threats on the one hand and regulatory requirements on the other. While many universities have excellent technical staff who gained know-how over many years (e.g. by establishing the ACOnet infrastructure), strategic, university-wide measures are often difficult and associated with many obstacles due to the universities' federated structure and heterogenous IT-systems. In addition, universities struggle to retain their outstanding technicians, who are often successfully poached by large companies due to the prevailing shortage of skilled workers.
In this project we want to significantly support universities on their way to a cross-institutional structure by designing a

process model for necessary preparatory measures, developing relevant components based on innovative approaches such as Gaia-X and AI/Machine Learning, and designing accompanying measures such as cyberrange training concepts as well as methods for self-evaluation of universities' maturity levels. A key research question is how universities can detect threats and attacks from the enormous amount of log and metadata in near real time in order to initiate timely countermeasures and protective measures.
Another essential question is whether it is technically and organizationally feasible to develop overall solutions, which inevitably require deep insight into the IT systems of the participating organizations and still preserve the digital sovereignty of Austria and Europe in this system-critical environment.

## Projektkoordinator

- SBA Research gemeinnützige GmbH

## Projektpartner

- AIT Austrian Institute of Technology GmbH
- ACOmarket GmbH
- Schoeller Network Control Datenverarbeitung GmbH
- Bundesministerium für Frauen, Wissenschaft und Forschung
- Universität Wien
- Universität für Weiterbildung Krems
- Taceo GmbH
- Universität Innsbruck
- Research Institute AG & Co KG
- EDV-Design Informationstechnologie GmbH
- CONDIGNUM GmbH