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.

Endberichtkurzfassung

Übergeordnete Projektergebnisse

Das Projekt ASOC (Academic Security Operations Center) konnte insgesamt planmäßig erfolgreich abgeschlossen werden. Alle gesetzten Meilensteine wurden termingerecht erreicht, die Projektstruktur erwies sich von Beginn an als klar definiert und tragfähig. Die Zusammenarbeit zwischen den Projektpartnern gestaltete sich konstruktiv und zielorientiert, regelmäßige Workshops ermöglichten eine effektive Kommunikation sowie frühzeitige Identifikation potenzieller Herausforderungen.

Arbeitspaket 2: Konzepte und Grundlagen für ein universitätsübergreifendes SOC

SBA Research hat die konzeptionellen Grundlagen des Projekts maßgeblich erarbeitet. Ein umfassendes High-Level-Konzept für ein universitätsübergreifendes SOC wurde erstellt, das sich in 19 Hauptabschnitte gliedert und folgende Kernbereiche abdeckt:

SOC-Aufbau und -Architektur
Cyber Threat Sharing Platform (CTSP)
Security Information Feeds (SIF) und Indicators of Compromise (IoC)
Security Orchestration, Automation and Response (SOAR) Workflows
Use Cases und Playbooks für den universitären Umfeld
Wissensdatenbank (Knowledge Base)
Reifegradmodell mit Evaluierungsmethoden und Maßnahmenkatalog

Die Universität Innsbruck validierte die Konzepte aus praktischer Perspektive und überführte ausgewählte Komponenten in produktionsnahe Umgebungen.

ACOMarket evaluierte die potenziellen Kosten für kommerzielle IOC-Feeds. Die Analyse ergab ein Verhältnis von rund 70 % Open-Source-Feeds zu 30 % kommerziellen Feeds. Für kommerzielle Feeds sind Kosten zwischen 60.000 und 200.000 EUR pro Jahr (Mindestversion) zu veranschlagen.

Arbeitspaket 3: Sichere und datenschutzkonforme föderale Datenhaltung

AIT bewertete systematisch relevante Standards und Formate für den strukturierten Austausch von Sicherheits- und Risikoinformationen:

Format

Beschreibung

STIX 2.1

JSON-basiert, repräsentiert CTI-Objekte, Attack Patterns, Threat Actors

IODEF v2

XML/JSON für Incident-Informationen zwischen CERTs und CSIRTs

openXSAM

Offenes Format für Risikomanagementdaten (ISO/SAE 21434)

CSAF

Maschinenlesbare Sicherheitshinweise im EU-Kontext

Aufbauend auf dieser Analyse wurde ein Konzept für ein angepasstes Datenformat erarbeitet. AIT-Experten sind aktiv im ASRG OPENXSAM Technical Committee „Risk Data Exchange" eingebunden, um die erarbeiteten Anforderungen in die laufende Standardisierungsarbeit einzubringen.

Arbeitspaket 4: AI-unterstütztes Threat Hunting

Dieses Arbeitspaket bildet eines der technischen Kernresultate des Projekts und umfasst folgende wesentliche Entwicklungen:

DetectMate : AITs Anomalieerkennungslösung mit integrierten ML-Algorithmen zur frühzeitigen Erkennung von Angriffen
AlertBERT : Self-supervised Framework zur robusten Gruppierung von Alarmen, reduziert Alert-Fatigue und verbessert die Effizienz von Security-Analysten
CIDS (Collaborative Intrusion Detection System) : Prototypischer Ansatz für verteilte Netzwerke mit automatisierter Detektor-Auswahl
Taranis AI : Kontinuierliche Weiterentwicklung des Open-Source-CTI/OSINT-Analysetools mit neuen Funktionalitäten (Storyclustering, MISP-Integration, Named Entity Recognition)

Zusätzlich wurden folgende KI-basierte Methoden entwickelt und veröffentlicht:

SC4OSINT : Storyclustering-Algorithmus zur automatischen Gruppierung themenbezogener Artikel und Reports
CTI-Analyse-Pipeline : Pipeline zur Analyse und Enrichment von Cyber Threat Intelligence
AITSecNER : Named Entity Recognition für Cybersecurity
TTPFShot : Retrieval-basierter Few-Shot-Learning-Ansatz zur TTP-Labeling nach MITRE ATT&CK
Cybersecurity Text Classifier : Klassifizierung von Cybersecurity-Relevanz in News-Artikeln

Alle entwickelten Tools und Frameworks stehen als Open Source auf GitHub zur Verfügung, zahlreiche Publikationen wurden in internationalen Konferenzen (ARES, BigData) und Preprint-Repositorien (arXiv) veröffentlicht.

Arbeitspaket 5: Prototypische Ausbildungsumgebungen

SBA Research baute die SBALAB-Prototypumgebung auf. Dabei zeigte sich, dass viele Werkzeuge noch keine etablierten Schemata wie STIX II oder CACAO 2.0 unterstützen. Es wurde ein Interpreter entwickelt, der Informationen in das einheitliche STIX II-Format konvertiert – eine wichtige Grundlage für zukünftige Projekte mit standardisierten Daten.

Live-Demonstrationen von Übungsszenarien fanden im September 2025 für Partner und Bedarfsträger statt.

Im Bereich Lehre ermöglichte die Universität Wien unter der Leitung von Edgar Weippl die Integration von SOC- und CTI-Themen in den Bachelor-Lehrplan (Information Security, Semester 5 und 6). Rund 120 Studierende nahmen teil, die Zufriedenheit mit den Inhalten war hoch (83 % fanden SOC spannend, 80 % CTI).

AIT entwickelte Szenarien und Datensets sowie das AttackBed (Cyber-physisches Testbed) und AttackMate (Tool zur automatisierten Simulation und Orchestrierung von Angriffsszenarien) kontinuierlich weiter. Zwei Open Datasets wurden veröffentlicht (MITRE ATT&CK TTP-Datensatz, CyberSecNews DE/EN-Datensatz).

Arbeitspaket 6: Rechtliche und soziale Fragestellungen

Eine umfassende juristische Analyse der ASOC-Architektur wurde durchgeführt, einschließlich der Bewertung von DSGVO, NIS2-Richtlinie, Data Act, Privacy-by-Design-Konzepten und Urheberrecht im Kontext von Managed Security Service Providern.

Eine systematische PRISMA-Literaturübersicht untersuchte die Erfolgsfaktoren universitärer SOCs auf individueller, gruppenbezogener und organisationaler Ebene.

Wesentliche rechtliche Erkenntnis: Laut § 24 Abs. 6 des NISG-Entwurfs sind österreichische Hochschuleinrichtungen explizit vom Anwendungsbereich der NIS2-Richtlinie ausgeschlossen. Diese Erkenntnis hat erhebliche Relevanz für die weitere Planung von Cybersecurity-Initiativen im österreichischen Hochschulsektor.

Fazit

Alle sechs Arbeitspakete wurden erfolgreich abgeschlossen. Das Projekt lieferte umfassende konzeptionelle Grundlagen für ein universitätsübergreifendes SOC, entwickelte innovative AI-gestützte Lösungen für Threat Hunting und Alerting, etablierte Ausbildungsinfrastrukturen für Lehre und Forschung sowie fundierte rechtliche und sozialwissenschaftliche Analysen. Die erzielten Ergebnisse bilden eine tragfähige Basis für zukünftige Projekte und die praktische Implementierung eines föderierten Security Operations Centers im österreichischen Hochschulbereich.

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