CTI

Cyber Threat Intelligence Qualifizierungsnetzwerk

Programm / Ausschreibung	Digitale Technologien, Digitale Technologien, Digitale Schlüsseltechnologien: Ausschreibung 2023	**Status**	laufend
Projektstart	01.08.2024	**Projektende**	31.07.2025
Zeitraum	2024 - 2025	**Projektlaufzeit**	12 Monate
Keywords	cybersecurity, threat intelligence, security operations		

Projektbeschreibung

Angesichts der rasanten digitalen Transformation und einem massiven Anstieg von Cyberangriffen ist es für Unternehmen unerlässlich, proaktiv gegen Cyberbedrohungen vorzugehen. Europäische Regulierungen wie NIS2 und der Cyber Resilience Act unterstreichen die Bedeutung entsprechender Maßnahmen. Cyber Threat Intelligence (CTI) spielt eine entscheidende Rolle, um Organisationen mit notwendigen Informationen zu versorgen und ihre Reaktionsfähigkeit zu verbessern. Fachkräftemangel und Ausbildungslücken behindern jedoch die Umsetzung effektiver Cybersicherheitsmaßnahmen.

Fundierte und praxisorientierte Cyber Threat Intelligence (CTI)-Schulungen sind entscheidend, um Sicherheitsteams mit den notwendigen Fähigkeiten und Kenntnissen auszustatten, damit sie potenzielle Bedrohungen effektiv identifizieren und darauf reagieren können. Das vorliegende Qualifizierungsnetz umfasst das Erlernen von Techniken zur Sammlung von Daten aus offenen Quellen, die Analyse dieser Daten, um relevante Bedrohungsindikatoren zu identifizieren, die Entwicklung von Strategien zur Verringerung dieser Bedrohungen und Maßnahmen zur Automatisierung von Arbeitsabläufen (SOAR). Durch die Teilnahme an den CTI-Trainings, die aus 6 technisch fundierten und praxisorientierten Modulen bestehen, werden Mitarbeiter:innen in Sicherheitspositionen nicht nur in die Lage versetzt, die Sicherheitslage ihrer Organisationen zu verbessern, sondern auch dazu beizutragen, dass ihre Organisationen den neuesten gesetzlichen und regulatorischen Anforderungen gerecht werden. Der Fokus auf Open Source wird dazu beitragen, die digitale Souveränität in diesem kritischen Bereich zu erhalten.

Ziel ist es, durch eine gezielte und praxisorientierte Schulungsmaßnahme ein umfassendes Verständnis der Bedrohungslandschaft zu entwickeln und die Resilienz gegenüber Cyber-Angriffen signifikant zu erhöhen. Durch den Transfer von CTI Know-how erhalten die Unternehmen zudem Impulse zur Erhöhung ihrer Forschungs-, Entwicklungs- und Innovationskompetenz.

Projektkoordinator

- SBA Research gemeinnützige GmbH

Projektpartner

- EDV-Design Informationstechnologie GmbH
- CONDIGNUM GmbH
- Universität Innsbruck
- GEKKO it-solutions GmbH
- Austrian Power Grid AG
- AIT Austrian Institute of Technology GmbH
- ACOmarket GmbH
- CERT.at GmbH
- cyan Security Group GmbH