CTI

Cyber Threat Intelligence Qualifizierungsnetzwerk

Programm / Ausschreibung	Digitale Technologien, Digitale Technologien, Digitale Schlüsseltechnologien: Ausschreibung 2023	**Status**	abgeschlossen
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.

Endberichtkurzfassung

Das CTI-Qualifizierungsnetzwerk hat gezeigt, dass der systematische Einsatz von Cyber Threat Intelligence (CTI) einen entscheidenden Beitrag zur frühzeitigen Erkennung, Einordnung und Bewältigung moderner Cyberbedrohungen leistet.

Durch die Kombination aus methodischer Analyse, praxisnahen Übungen und realitätsnahen Szenarien konnten die Teilnehmenden ein belastbares Verständnis für den Aufbau eines konsistenten Cyber-Lagebildes entwickeln.

Zentraler Erfolgsfaktor war die strukturierte Analyse von Angriffen entlang etablierter Modelle wie dem Diamond Model und MITRE ATT&CK. Diese Ansätze ermöglichen es, Bedrohungen nicht nur technisch zu erkennen, sondern sie auch hinsichtlich Akteuren, Motiven, eingesetzten Fähigkeiten und betroffener Infrastrukturen einzuordnen und daraus fundierte strategische, taktische und operative Entscheidungen abzuleiten.

Die im Projekt aufgebauten Kompetenzen bilden eine wesentliche Grundlage zur Unterstützung regulatorischer und strategischer Initiativen wie NIS2 , dem Cyber Resilience Act (CRA), dem neuen RKEG sowie zur Stärkung der digitalen und technologischen Souveränität . Insbesondere Organisationen aus kritischen Infrastrukturen, dem Bildungs- und Forschungsbereich sowie IT-Dienstleister konnten die gewonnenen Erkenntnisse unmittelbar in den Aufbau oder die Weiterentwicklung eigener Security-Operations- und CTI-Strukturen überführen.

Ein zentrales Projektergebnis ist zudem die bestätigte hohe Relevanz von Open-Source-Lösungen im Bereich Cyber Security und Cyber Threat Intelligence. Viele von der Europäischen Union geförderte Plattformen verfügen derzeit über keine gleichwertigen Closed-Source-Alternativen. Das Projekt hat gezeigt, dass Open Source nicht nur wirtschaftlich attraktiv ist, sondern auch Innovationsfähigkeit, Transparenz und Unabhängigkeit fördert. Eine gezielte Weiterentwicklung und nachhaltige Nutzung dieser Ökosysteme ist daher essenziell.

Die Schulungsmaßnahme hat darüber hinaus verdeutlicht, dass bei geringen Vorkenntnissen ein Umfang von mindestens acht Präsenztagen erforderlich ist, um ein ganzheitliches und praxisnahes Verständnis von SOC- und CTI-Konzepten zu vermitteln. Trotz des erhöhten zeitlichen Aufwands sind derartige Qualifizierungsmaßnahmen unerlässlich, um langfristig belastbare Fähigkeiten im Umgang mit komplexen und dynamischen Cyberbedrohungen aufzubauen.

Insgesamt leistet das Projekt einen nachhaltigen Beitrag zur Stärkung der Cybersecurity-Kompetenzen in Österreich und schafft eine tragfähige Basis für weitere Kooperationen, Qualifizierungsangebote und Verwertungsaktivitäten über die Projektlaufzeit hinaus.

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