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.

Endberichtkurzfassung

Das Projekt und die entsprechenden Schulungsmaßnahmen, haben gezeigt das das Erkennen von Bedrohungen, Angriffen, das Einfließen von Cyber Threat Intelligent Informationen und dann eine Auswertung im Sinne des Diamonds Models mit den

Fragen Wer hat mich angegriffen, welche Fähigkeiten wurden eingesetzt, wer ist das Opfer, welche Infrastruktur steht, dahinter und letztendlich das Warum aufzuzeigen, ein wesentlicher Faktor für Lagebild Informationen für eine Organisation sind. Dies wir in Zukunft die Aktivitäten wie NIS2, das neue RKEG und die digitale Souveränität unterstützen. Ebenso wurde auch die Bedeutung von Open Source in diesem Umfeld aufgezeigt, da erheblich Plattformen die von der EU auch entsprechend unterstützt werden, nicht mit Closed Source alternativen belegt sind, um so wichtiger ist es die Open Source Aktivitäten entsprechend zu supporten. Um ein vollständiges Bild als Schulungsteilnehmer zur erlangen, hat sich die länge der Schulungsmaßnahmen von 8 Tagen mit geringen Vorkenntnissen in den Thematiken SOC und CTI als ein minimaler Durchführungszeitraum herausgestellt. Es wäre nötig in Zukunft ein so komplexes Themenfeld weiter innerhalb von Organisationen zu fördern, auch wenn die Dauer dieser Schulungsmaßnahmen, entsprechende Zeit in Anspruch nehmen.

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