



## Sachbericht zum Verwendungsnachweis Teil II

**Verbundprojekt:** Datentreuhänder Plattform zum dezentralen Austausch von IT-Sicherheitsvorfällen (DEFENSIVE)

**Laufzeit:** 01.07.2022 – 31.12.2025

**Förderkennzeichen:** 16KIS1568K

Januar 2026

Universität Regensburg (IFS)

## 1. Ausführliche Darstellung der im Rahmen des Vorhabens durchgeführten Arbeiten und Vergleich zur ursprünglichen Vorhabenbeschreibung

Im Teilvorhaben IFS wurden die in der Vorhabenbeschreibung formulierten Ziele im Wesentlichen erreicht. Im Mittelpunkt stand die Konzeption und prototypische Realisierung einer Datentreuhänder-Plattform für Cyber Threat Intelligence (CTI) sowie die Untersuchung geeigneter Anreizmechanismen für den sicheren und nachhaltigen Austausch von Sicherheitsinformationen. Im Folgenden werden die einzelnen Arbeitspakete in ihrem geplanten Umfang (SOLL) und der tatsächlichen Umsetzung (IST) dargestellt.

### **AP1: Koordination und Monitoring**

Für AP1 war vorgesehen, dass IFS die Koordination des Teilvorhabens sowie die Mitwirkung an der Verbundkoordination übernimmt. Dies umfasste den Aufbau und die Pflege einer gemeinsamen virtuellen Arbeitsumgebung, die Organisation von Projekt- und Arbeitstreffen, die fortlaufende Dokumentation des Projektfortschritts sowie die Kommunikation mit den Verbundpartnern und dem Projektträger.

Diese Aufgaben wurden vollständig umgesetzt. Zu Projektbeginn wurde eine einheitliche Kollaborationsinfrastruktur etabliert, die aus einer Nextcloud-Instanz für den Austausch von Dokumenten, einem GitLab-System für die gemeinsame Entwicklung und Versionierung von Quellcode sowie mehreren Videokonferenz- und Kommunikationskanälen bestand. Auf dieser Basis konnten alle Projektbeteiligten kontinuierlich auf aktuelle Dokumente, Zwischenergebnisse und Softwarestände zugreifen.

IFS organisierte und protokollierte die regelmäßigen Verbundtreffen, die einmal jährlich in Präsenz stattfanden. Zusätzlich wurden in einem ca. vierwöchentlichen Rhythmus Online-Statusmeetings durchgeführt, um den Fortschritt der einzelnen Arbeitspakete eng zu begleiten, Schnittstellen zu klären und Abstimmungen mit den Partnern zu erleichtern. Die entstandenen Protokolle und Entscheidungsvorlagen wurden im Projektlauf strukturiert abgelegt und standen allen Projektbeteiligten zur Verfügung.

Die Koordinationstätigkeiten umfassten außerdem die Vorbereitung der Zwischenberichte und die Abstimmung notwendiger Anpassungen im Arbeitsplan. Durch die kontinuierliche Koordination und die transparente Kommunikation mit dem Projektträger konnten die Ziele des Teilvorhabens gleichwohl vollständig erreicht werden.

### **AP2: Anforderungserhebung**

In AP2 sollte ein fundierter Anforderungskatalog für eine Datentreuhänder-gestützte CTI-Sharing-Plattform erarbeitet werden. Die ursprüngliche Planung sah eine umfassende Literaturrecherche zu bestehenden CTI-Sharing-Plattformen und einschlägigen Standards vor, ergänzt um die Analyse von Anreizmechanismen in der Cybersicherheit. Auf dieser Grundlage sollten Anforderungen formuliert, in Form eines Katalogs

strukturiert und mit Hilfe von Experteninterviews, insbesondere mit KMU und weiteren Organisationen, validiert und priorisiert werden.

Die Umsetzung entsprach diesem Plan in vollem Umfang. Zu Beginn des Arbeitspakets wurde eine systematische Literaturanalyse durchgeführt, in deren Rahmen wissenschaftliche Publikationen, Branchenberichte und technische Dokumentationen zu CTI-Sharing-Plattformen ausgewertet wurden. Besonderes Augenmerk lag auf etablierten Lösungen wie MISP, Facebook ThreatExchange, IBM X-Force, Open Threat Exchange, OpenCTI und ThreatConnect. Für jede dieser Plattformen wurden Funktionsumfang, Datenmodelle, Governance-Ansätze sowie Sicherheits- und Datenschutzmechanismen untersucht und mit Blick auf das im Projekt verfolgte Datentreuhänder-Konzept bewertet.

Parallel dazu wurde eine eigenständige Literaturstudie zu Anreizen in der Cybersicherheit durchgeführt. Ziel war es, systematisch zu erfassen, welche Arten von positiven Anreizen, etwa Reputationsgewinne, Zugang zu hochwertigen Daten, Markt- und Marketingeffekte oder auch monetäre und tokenbasierte Modelle, in der Praxis eingesetzt und in der Forschung untersucht werden. Diese Arbeiten mündeten in eine Taxonomie positiver Anreize, die die unterschiedlichen Anreizarten und ihre Wirkmechanismen in einem strukturierten Modell zusammenführt. Ein zentraler Ausschnitt dieser Ergebnisse wurde in der HICSS-Publikation „A Taxonomy of Positive Incentives to Motivate Cybersecurity Behaviors“ wissenschaftlich veröffentlicht und bildet zugleich die theoretische Grundlage für die im Projekt betrachteten Anreizmechanismen.

Auf Basis der Literaturanalysen wurden insgesamt 33 Kernanforderungen an eine CTI-Sharing-Plattform formuliert. Diese betreffen unter anderem Datenschutz und Informationssicherheit, Interoperabilität, Skalierbarkeit, Rollen- und Rechtemodelle, Transparenz und Nachvollziehbarkeit, Anreiz- und Governance-Mechanismen sowie Anforderungen aus Sicht von KMU und öffentlichen Einrichtungen. Um die Anforderungsliste zu validieren und stärker zu praxisorientieren, wurden Interviews mit Vertretern aus KMU, weiteren Unternehmen und Organisationen geführt. In diesen Gesprächen wurden die Anforderungen diskutiert, konkretisiert und hinsichtlich ihrer Relevanz sowie Umsetzbarkeit bewertet.

Die Ergebnisse dieser Interviews flossen direkt in den finalen Anforderungskatalog ein. Dabei zeigte sich, dass insbesondere eine klare Governance-Struktur, ein ressourcenschonender Zugang für kleinere Organisationen sowie transparente und faire Anreizmechanismen von hoher Bedeutung sind. Der resultierende Anforderungskatalog diente im weiteren Projektverlauf als zentrale Referenz für die Architektur- und Plattformentwicklung in AP3 und AP4.

### **AP3: Entwicklung der Plattform**

AP3 hatte die Aufgabe, auf Grundlage der in AP2 erhobenen Anforderungen die Systemarchitektur der Datentreuhänder-Plattform zu entwerfen und einen prototypischen Demonstrator zu implementieren. Darüber hinaus sollten Fragen des

Identitäts- und Zugriffsmanagements sowie der Multi-Tenancy adressiert und die Plattform auf ein späteres Deployment vorbereitet werden.

Im Sinne der SOLL-Planung wurde zunächst ein Architekturentwurf ausgearbeitet, der eine modulare Struktur vorsieht. Kernpunkte dieser Architektur sind der Einsatz einer Distributed-Ledger-Technologie als vertrauensbildende Infrastruktur, klar abgegrenzte Dienste für Identitäts- und Zugriffsverwaltung sowie ein flexibles Datenhaltungskonzept, das sowohl die Speicherung von CTI-Artefakten als auch deren Metadaten und Zugriffsregeln abbilden kann. Das Datentreuhänder-Konzept spiegelt sich in der Trennung von Datenhoheit und technischer Betriebsverantwortung wider: Die Plattform stellt die Infrastruktur und die Governance-Mechanismen bereit, während die teilnehmenden Organisationen selbstbestimmt über die Einbringung, Freigabe und Nutzung ihrer Daten entscheiden.

Ein weiterer Aspekt waren Multi-Tenancy-Szenarien, da vor allem KMU auf gemeinsam genutzte Infrastrukturen angewiesen sind. Hierzu wurde ein Modell entwickelt, in dem mehrere Organisationen dieselbe technische Plattform nutzen können, ohne dass ihre jeweiligen Datenbestände miteinander vermischt werden oder unautorisiert zugänglich sind. Dies erforderte die Ausarbeitung eines differenzierten Rollen- und Rechtekonzepts sowie technischer Mechanismen zur Mandantentrennung, etwa über isolierte logische Bereiche, separate Identitätsdomänen oder entsprechende Konfigurationen der Zugriffsprüfungen.

Auf Basis des Architekturentwurfs wurde ein funktionaler Demonstrator umgesetzt. Dieser bildet zentrale Prozesse des CTI-Sharings ab: das Anlegen und Verwalten von Organisationen und Nutzerkonten, das Einbringen neuer CTI-Einträge, deren Speicherung und Verknüpfung mit Metadaten sowie das Suchen, Filtern und Abrufen vorhandener Informationen. Dabei wurden erste Ausprägungen von Anreizmechanismen berücksichtigt, etwa in Form von Transparenz über eigene Beiträge und deren Nutzung sowie der Möglichkeit, die Qualität von eingestellten Informationen zu bewerten.

Self-Sovereign Identity (SSI) wurde als vielversprechendes, aufstrebendes Identitätsmodell für den in zukünftigen Forschungsarbeiten einzusetzenden Demonstrator identifiziert. Obwohl sich SSI derzeit noch in einem frühen Stadium der technischen Entwicklung befindet, bietet der Ansatz das Potenzial, bestimmte Eigenschaften der Akteure unter Wahrung ihrer Anonymität kryptografisch nachweisbar zu machen und damit das Vertrauen in die Plattformteilnehmer zu stärken.

Der Projektpartner DFN-CERT hat die Ergebnisse des Code-Reviews mit uns geteilt. Die Erkenntnisse sind in einer Überarbeitung des Demonstrators eingeflossen.

## **AP4: Deployment**

In AP4 sollte der Demonstrator in einer geeigneten Umgebung deployt, mit Dokumentation versehen und gemeinsam mit Praxispartnern erprobt werden. Geplant war die Bereitstellung einer lauffähigen Instanz, die Dokumentation der Installations- und Konfigurationsschritte sowie die Einbindung von Interviewpartnern und weiteren

Experten, um Rückmeldungen zur Praxistauglichkeit, Benutzerfreundlichkeit und technischen Eignung zu erhalten.

Diese Ziele wurden im Wesentlichen erreicht. Zunächst wurde der Demonstrator in einer Test- und Demonstrationsumgebung aufgesetzt, die es erlaubte, die Plattform realitätsnah zu nutzen, ohne produktive Systeme zu berühren. Begleitend wurde eine Installations- und Konfigurationsanleitung erstellt, die die notwendigen technischen Voraussetzungen, die einzelnen Deploymentsschritte sowie Hinweise zur Administration und Nutzung beschreibt. Die bereitgestellte Anleitung ermöglicht es interessierten Dritten, den Demonstrator eigenständig aufzusetzen und zu testen.

Im nächsten Schritt wurden Industrieexperten und Interviewpartner, die bereits in der Anforderungserhebung eingebunden waren, eingeladen, den Demonstrator zu nutzen. In gemeinsamen Terminen wurden typische Nutzungsszenarien durchgespielt, etwa das Hinzufügen von CTI-Einträgen oder das Auffinden relevanter Informationen. Die Rückmeldungen der Teilnehmenden betrafen unter anderem die Verständlichkeit der Benutzeroberfläche, die Nachvollziehbarkeit der Zugriffsentscheidungen, den Aufwand für die Integration in bestehende Prozesse sowie die generelle Einschätzung des Mehrwerts einer solchen Plattform.

Die Rückmeldungen wurden ausgewertet und führten zu Anpassungen sowie Verbesserungsvorschlägen, etwa bei der Ausgestaltung der Benutzerführung. Eine längerfristige Pilotierung in produktiven Umgebungen mehrerer Organisationen war innerhalb der Projektlaufzeit nicht realisierbar, konnte jedoch durch die realitätsnahe Testumgebung und die Einbindung von Experten zumindest exemplarisch simuliert werden.

## 2. Die wichtigsten Positionen des zahlenmäßigen Nachweises

Die Fördermittel des Teilvorhabens IFS wurden überwiegend für Personalaufwendungen im wissenschaftlichen Bereich verwendet. Die finanzierte Personalkapazität war maßgeblich für die Durchführung der Literaturrecherchen, die Konzeption der Anreizmechanismen, die Erhebung und Auswertung der Interviews sowie für die Entwicklung und Implementierung des Demonstrators. Die Mittel wurden entsprechend dem bewilligten Finanzierungsplan eingesetzt. Die beantragte kostenneutrale Verlängerung diente dazu, die vorhandenen Mittel über einen längeren Zeitraum abzurufen und damit die Kontinuität der wissenschaftlichen Arbeit sicherzustellen.

## 3. Notwendigkeit und Angemessenheit der geleisteten Projektarbeit

Die Kombination aus Datentreuhänder-Konzept, CTI-Sharing, Distributed-Ledger-Technologie und explizit gestalteten Anreizmechanismen stellt ein anspruchsvolles und in dieser Konstellation weitgehend unerforschtes Forschungs- und Entwicklungsfeld dar. Während einzelne Bausteine, etwa klassische CTI-Plattformen, Blockchain-basierte Anwendungen oder ökonomische Anreizmodelle, bereits in Literatur und Praxis beschrieben sind, lagen zu Projektbeginn keine belastbaren Referenzmodelle vor, in

denen diese Elemente zu einer gemeinsamen, datenschutzkonformen und zugleich praxistauglichen Plattformarchitektur zusammengeführt wurden. Hinzu kommt, dass der Austausch von Sicherheitsinformationen besonders sensiblen rechtlichen und organisatorischen Rahmenbedingungen unterliegt, etwa im Hinblick auf den Schutz von Geschäftsgeheimnissen, die Einhaltung datenschutzrechtlicher Vorgaben und die Vermeidung von Haftungsrisiken. Die Gestaltung einer Datentreuhänder-Plattform für CTI-Sharing musste daher nicht nur technische, sondern zugleich organisatorische, ökonomische und rechtliche Anforderungen in einem integrierten Ansatz berücksichtigen. Diese Ausgangslage führte dazu, dass zunächst grundlegende Vorarbeiten zu leisten waren, bevor eine prototypische Umsetzung zielgerichtet möglich war.

Vor diesem Hintergrund war eine mehrstufige Vorgehensweise erforderlich, die mit umfassenden Literaturstudien und Marktanalysen begann. In einem ersten Schritt wurden bestehende CTI-Plattformen und relevante Forschungsarbeiten systematisch ausgewertet, um funktionale Lücken, typische Schwachstellen und bewährte Praktiken zu identifizieren. Parallel wurden Konzepte positiver Anreize in der Cybersicherheit aufgearbeitet und in einer Taxonomie strukturiert, die sich auf das angestrebte Datentreuhänder-Szenario übertragen ließ. Darauf aufbauend wurden Anforderungsanalysen durchgeführt, in denen wissenschaftliche Erkenntnisse mit den konkreten Bedarfen von Unternehmen und weiteren Organisationen abgeglichen wurden. Die aus Interviews und Expertengesprächen gewonnenen Einsichten flossen in einen detaillierten Anforderungskatalog ein, der technische, organisatorische und Governance-Aspekte zusammenführt. Erst auf dieser Grundlage konnten belastbare Architekturentwürfe entwickelt werden, die sowohl die Besonderheiten von Distributed-Ledger-Technologien als auch die Anforderungen an Multi-Tenancy, Identitätsmanagement und Zugriffskontrolle angemessen berücksichtigen.

Die geleistete Projektarbeit ist vor diesem Hintergrund als notwendig und in ihrem Umfang angemessen zu bewerten. Ohne die umfassende Anforderungserhebung und die systematische Betrachtung von Anreizmechanismen wäre ein zielgerichteter und praxisnaher Plattformentwurf nicht möglich gewesen; das Risiko, die tatsächlichen Bedürfnisse der Zielgruppen zu verfehlen, wäre erheblich gewesen. Ebenso war der beträchtliche Aufwand für die Implementierung und das Deployment des Demonstrators erforderlich, um die zuvor entwickelten Konzepte aus der Theorie in eine technisch lauffähige Form zu überführen. Erst durch den funktionsfähigen Demonstrator konnten Annahmen zur technischen Machbarkeit, zur Ausgestaltung von Rollen- und Rechtemodellen sowie zur Akzeptanz der Plattformidee im Austausch mit Experten überprüft und weiter geschärft werden. Die im Projekt gewonnenen wissenschaftlichen Erkenntnisse, die international sichtbare Publikationen zu Anreizmechanismen und dem entwickelten sowie evaluierten Demonstrator zeigen insgesamt, dass die eingesetzten Ressourcen zielgerichtet genutzt wurden, um die ambitionierte Zielsetzung des Teilvorhabens zu erreichen und eine belastbare Grundlage für weitere wissenschaftliche und praktische Verwertungsschritte zu schaffen.

#### 4. Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse

In diesem Abschnitt wird der Verwertungsstand der im Teilvorhaben IFS erzielten Ergebnisse dargestellt und aufgezeigt, in welcher Form diese nach Projektende in Wissenschaft und Praxis genutzt werden können. Dabei steht insbesondere die Frage im Vordergrund, welchen konkreten Beitrag die im Projekt entwickelten Konzepte (insbesondere der Anforderungskatalog, die Datentreuhänder-Architektur, die Anreizmodelle sowie der prototypische Demonstrator) zur Verbesserung des Umgangs mit Cyber Threat Intelligence (CTI) leisten und wie sich daraus längerfristig stabile, vertrauenswürdige Sharing-Ökosysteme entwickeln lassen.

Aus praktischer Sicht liegt der zentrale Nutzen der DEFENSIVE-Ergebnisse darin, dass Organisationen, insbesondere KMU und öffentliche Einrichtungen, eine klar strukturierte Orientierung für den Aufbau oder die Auswahl von CTI-Sharing-Plattformen erhalten. Der im Projekt erarbeitete Anforderungskatalog fasst technische, organisatorische und Governance-Anforderungen in einer Form zusammen, die sowohl für Sicherheitsverantwortliche als auch für IT-Architekten und Entscheidungsträger nachvollziehbar ist. Er kann beispielsweise als Checkliste bei der Bewertung bestehender Lösungen oder als Grundlage für Ausschreibungen und Architekturentscheidungen dienen. Gleichzeitig zeigt die im Projekt entwickelte Datentreuhänder-Architektur, wie ein vertrauenswürdiger, datenschutzkonformer Austausch von sicherheitsrelevanten Informationen technisch realisiert werden kann, ohne, dass die beteiligten Organisationen die Hoheit über ihre Daten gefährden.

Der prototypische Demonstrator macht diese Konzepte konkret nutzbar. Er demonstriert, wie CTI-Daten in einer gemeinsamen Infrastruktur verwaltet, mit Metadaten angereichert und über geeignete Rollen- und Rechtekonzepte geschützt werden können. Durch den Einsatz von Distributed-Ledger-Technologien werden Transparenz und Nachvollziehbarkeit von Transaktionen erhöht, was wiederum das Vertrauen der beteiligten Organisationen stärkt. Der Demonstrator kann von interessierten Akteuren als Referenz für eigene Pilotprojekte genutzt, technisch angepasst und schrittweise in bestehende Sicherheitslandschaften integriert werden. Auf diese Weise fungiert er als Brücke zwischen Forschungsprototyp und potenziell produktiven Lösungen.

Von besonderer Bedeutung ist zudem die systematische Betrachtung von Anreizmechanismen. Eine wesentliche Hürde für den Erfolg von CTI-Sharing-Initiativen besteht darin, dass Organisationen zwar von den Informationen anderer profitieren, gleichzeitig aber zögern, eigene Daten beizusteuern. Die im Projekt entwickelte Taxonomie positiver Anreize zeigt, welche Motivationsfaktoren, etwa Reputationsgewinne, Zugang zu höherwertigen Informationen, Community-Effekte oder marketingbezogene Vorteile, in einem Sharing-Ökosystem wirksam werden können und wie sie gestaltet sein sollten. Diese Erkenntnisse fließen sowohl in die Konzeption von Governance-Strukturen als auch in konkrete Plattformfunktionen ein und sind damit ein zentraler Baustein für die nachhaltige Verwertbarkeit der Projektergebnisse.

Insgesamt lässt sich festhalten, dass die Ergebnisse des Teilvorhabens IFS mehrere Ebenen der Verwertung adressieren: Auf konzeptioneller Ebene liefern Anforderungskatalog, Architektur und Anreizmodelle wiederverwendbare Bausteine für

zukünftige CTI-Sharing-Initiativen. Auf technischer Ebene bietet der Demonstrator eine erprobte Referenzimplementierung, anhand derer konkrete Umsetzungsschritte geplant und evaluiert werden können. Und auf organisatorischer Ebene schaffen die erarbeiteten Governance-Überlegungen und Anreizkonzepte die Grundlage für tragfähige, langfristig stabile Kooperationen zwischen den beteiligten Organisationen.

a. Erfindungen/Schutzrechtsanmeldungen und erteilte Schutzrechte

Dies trifft auf das DEFENSIVE-Projekt nicht zu.

b. Wirtschaftliche Erfolgsaussichten nach Projektende

Dies trifft auf das DEFENSIVE-Projekt nicht zu.

c. Wissenschaftliche Erfolgsaussichten nach Projektende

Die wissenschaftlichen Erfolgsaussichten des Teilvorhabens IFS sind als sehr gut einzuschätzen. Mit der im Projekt entstandenen und bereits publizierten Arbeit zur Taxonomie positiver Anreize in der Cybersicherheit liegt ein wissenschaftlich begutachtetes Ergebnis vor, das international anschlussfähig ist und in der Fachcommunity auf Resonanz stößt. Diese Publikation bildet ein theoretisches Fundament, auf dem weitere Forschungsarbeiten zu Anreizsystemen im Kontext von CTI-Sharing, Datentreuhändermodellen und kooperativen Sicherheitsökosystemen aufbauen können.

Darüber hinaus eröffnen die im Projekt erarbeiteten Konzepte und der Demonstrator vielfältige Möglichkeiten für weiterführende empirische und gestaltungsorientierte Forschung. So können beispielsweise unterschiedliche Anreizmodelle oder Governance-Strukturen auf Basis des Demonstrators experimentell untersucht werden, indem in kontrollierten Studien oder Pilotprojekten beobachtet wird, wie sich das Verhalten der teilnehmenden Organisationen verändert. Ebenso bietet die Architektur die Möglichkeit, Fragen der Skalierbarkeit, Interoperabilität mit bestehenden Sicherheitslösungen oder der Integration zusätzlicher Datenschutzmechanismen wissenschaftlich zu analysieren.

Die im Projekt gewonnenen Erkenntnisse werden in Qualifikationsarbeiten (z. B. Masterarbeiten, Dissertationen) weiter vertieft und tragen so langfristig zur wissenschaftlichen Profilbildung im Themenfeld Cyber-Security, CTI-Sharing und digitale Plattformen bei. Insgesamt ist zu erwarten, dass aus dem Projekt heraus weitere Veröffentlichungen entstehen, die sowohl die theoretische Fundierung als auch die praktischen Erfahrungen aus Architekturentwurf, Implementierung und Evaluation aufgreifen und in die internationale Forschungsdiskussion einbringen.

d. Wissenschaftliche und wirtschaftliche Anschlussfähigkeit für eine mögliche notwendige nächste Phase bzw. die nächsten innovatorischen Schritte zur erfolgreichen Umsetzung der Ergebnisse.

Die Ergebnisse des Teilvorhabens IFS weisen eine hohe Anschlussfähigkeit sowohl für wissenschaftliche als auch für wirtschaftliche Weiterentwicklungen auf. Auf wissenschaftlicher Ebene bieten sich insbesondere Verbundprojekte an, in denen die im Projekt entwickelten Konzepte in größeren, realitätsnahen Szenarien erprobt und

weiterentwickelt werden. Denkbar sind beispielsweise Projekte, in denen mehrere Branchen oder Sektoren (z. B. kritische Infrastrukturen, Industrie, öffentliche Verwaltung) gemeinsam CTI austauschen und dabei unterschiedliche regulatorische Rahmenbedingungen, Bedrohungslagen und Organisationsstrukturen berücksichtigen. Hier könnten insbesondere Fragen zur Governance, zu Haftungs- und Compliance-Aspekten sowie zur Akzeptanz von Datentreuhänder-Modellen vertieft untersucht werden.

Wirtschaftlich eröffnet der Demonstrator die Möglichkeit, in Kooperation mit Unternehmen und öffentlichen Einrichtungen Pilot- und Demonstrationsprojekte aufzusetzen, in denen die Plattform schrittweise an produktionsnahe Umgebungen herangeführt wird. In solchen Projekten könnten einzelne Komponenten, wie das Identitäts- und Rechtemanagement, die Multi-Tenancy-Architektur oder spezifische Anreizfunktionen, in bestehende Sicherheitslösungen integriert und hinsichtlich ihres Mehrwerts bewertet werden. Aus solchen Piloten können sich wiederum Geschäftsmodelle ergeben, etwa in Form von Managed Services für CTI-Sharing oder Beratungsleistungen zur Einführung von Datentreuhänder-Plattformen.

Für eine mögliche nächste Projektphase bieten sich zudem vertiefende technologische Innovationen an. Dazu zählen die Einbindung weiterer Datenquellen und Schnittstellen zu etablierten Sicherheitswerkzeugen (z. B. SIEM-Systeme, SOC-Plattformen), die Nutzung von Methoden der Künstlichen Intelligenz zur Auswertung und Priorisierung von CTI-Daten sowie die Weiterentwicklung der Plattform zu einem modularen Baukasten, der an unterschiedliche Einsatzszenarien angepasst werden kann. Die im Teilvorhaben IFS erarbeiteten Grundlagen, Anforderungskatalog, Architektur, Anreizmodelle und Demonstrator, bilden hierfür eine tragfähige Basis, auf der sowohl akademische als auch industrielle Partner aufbauen können, um die Ergebnisse von DEFENSIVE in Richtung produktreifer, breit einsetzbarer Lösungen weiterzuführen.

## 5. Bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen während der Durchführung des Vorhabens

Während der Durchführung wurden externe Arbeiten beobachtet, die thematisch angrenzen. Diese zeigen zunehmende Aufmerksamkeit für dezentrale CTI Sharing Systeme, erwiesen sich jedoch nur begrenzt direkt übertragbar auf die von DEFENSIVE angestrebten Ziele. Die Sichtung bestätigte die Relevanz des gewählten Ansatzes und lieferte vereinzelt Impulse.

- Abraham, C., Bélanger, F., & Daultrey, S. (2025). Promoting research on cyber threat intelligence sharing in ecosystems. *Journal of Cybersecurity*, 11(1).
- Chatziamanetoglou, D., & Rantos, K. (2024). Cyber threat intelligence on blockchain: A systematic literature review. *Computers*, 13(3), 60.
- Venčkauskas, A., Jusas, V., Barisas, D., & Misnevs, B. (2024). Blockchain-based model for incentivized cyber threat intelligence sharing. *Applied Sciences*, 14(16), 6872.

## 6. Erfolgte und geplante Veröffentlichungen der Ergebnisse

In diesem Abschnitt werden die veröffentlichten wissenschaftlichen Publikationen gelistet, die im Zusammenhang mit dem DEFENSIVE Vorhaben stehen. Dabei wurde das Anreizmodell untersucht und das Konzept zu einem Datentreuhändersystem auf Blockchain-Basis erstellt, welches den Austausch von Sicherheitsdaten ermöglicht. Zusätzlich wurde der Demonstrator entwickelt und evaluiert.

- Reitinger, T., & Pernul, G. (2025, January). A taxonomy of positive incentives to motivate cybersecurity behaviors. In *Proceedings of the 58th HI International Conference on System Sciences (HICSS-58)*.
- Baumer, T., Grill, J., Adan, J., & Pernul, G. (2024, July). A Trust and Reputation System for Examining Compliance with Access Control. In *Proceedings of the 19th International Conference on Availability, Reliability and Security* (pp. 1-10).
- Reitinger, T., Grill, J., & Pernul, G.. Share and benefit: Incentives for cyber threat intelligence sharing. *International Journal of Information Security*.