International Journal of Information Security (2026) 25:37
https://doi.org/10.1007/s10207-025-01165-2

REGULAR CONTRIBUTION

Share and benefit: incentives for cyber threat intelligence sharing

Tobias Reittinger[1] · **Johannes Grill**[1] · **Günther Pernul**[1]

Received: 30 July 2025 / Accepted: 17 November 2025

Abstract

Cyber threat intelligence (CTI) provides actionable insights into the threat landscape, helping organizations strengthen their defenses. Because commercial CTI is costly, inter-organizational sharing can reduce expenses, yet adoption remains limited. Still, the design of effective incentives for CTI sharing and their embedding in a sharing platform remains underexplored. We conducted 15 semi-structured interviews with security professionals to elicit incentive requirements and design options. We find that organizations prefer to share CTI with known recipients to build trust and support GDPR compliance. They also value mechanisms that lower coordination costs, such as a reputation system and price guidance to help prioritize scarce analyst time. Further, a major barrier is skepticism about the net benefits of sharing. To address this, we propose financial compensation for contributed CTI and a marketing label that signals proactive cybersecurity to partners and customers. We implemented these incentives in a platform prototype and assessed their effects in 14 hands-on sessions with security experts. Participants reported increased willingness to share, suggesting that well-designed incentives can catalyze CTI-sharing ecosystems. Put simply, organizations can share and benefit.

1 Introduction

As cyberattacks continue to increase [1], most organizations have encountered a cyber incident or breach [2]. However, the consequences of a cyberattack can be severe. In 2025, cyberattacks are expected to cause over 10 trillion US dollars in damage worldwide [3]. Beyond direct financial losses, these incidents undermine customer trust, disrupt critical operations, and often lead to declines in share price [2].

However, organizations can prevent cyberattacks by joining forces with other organizations [4]. The transition from individual to collaborative teamwork can occur through collaborative cybersecurity. A promising approach to joint cybersecurity is the sharing of cyber threat intelligence (CTI). In short, CTI are attack information that can be used to prevent, detect, and recover from cyberattacks in a timely manner [5]. CTI can be classified into three types:

- **Technical CTI**: Mainly indicators of compromise (IoCs) such as IP addresses or file hashes [6] that are used to sharpen security instruments and eliminate attack vectors.
- **Tactical CTI**: In-depth analyses of adversaries' tactics, techniques, and procedures (TTPs), enabling analysts to detect and defend against specific attack patterns [5].
- **Strategical CTI**: High-level information about attack trends and tailored for managerial decision-makers [6].

Organizations acquire CTI through both internal and external channels. Internally, they can analyze security logs and investigate incidents as they occur [6]. However, this reactive approach provides only a narrow, organization-specific perspective [7]. Externally, they can leverage open-source feeds, though these typically supply only IoCs [8, 9], or subscribe to commercial vendors, whose comprehensive intelligence often comes at a prohibitive cost [7]. Alternatively, by participating in CTI-sharing communities, organizations, especially small and medium-sized enterprises, gain affordable access to diverse CTI via platforms that integrate directly with their existing security infrastructures.

Despite its benefits, CTI sharing remains underutilized in practice due to several obstacles [5, 10]. First, the processing of internal security incidents requires effort and know-how. Second, organizations must trust recipients to handle shared intelligence confidentially and responsibly. Although early proposals have explored sharing communities [11] and technical implementations for CTI sharing [12], critical questions

✉ Tobias Reittinger
tobias.reittinger@ur.de

[1] University of Regensburg, Universitätsstr. 31, Regensburg, Germany

Published online: 22 January 2026

persist: It is unclear how to design incentives to effectively increase the motivation of organizations for CTI sharing [10]. Further, prior research lacks insights into how to integrate incentives into a CTI sharing platform. We address these gaps by answering the following research questions:

RQ1 *How to design incentives for CTI sharing?*
RQ2 *How can incentives be integrated into a CTI sharing platform?*

Our study comprised three phases: Phase 1 involved 15 semi-structured expert interviews to identify CTI-sharing incentives (RQ1). Phase 2 saw the design and implementation of a prototype platform embedding these motivators (RQ2). Phase 3 evaluated its impact via 14 hands-on interviews. We provide the following contributions:

- We identified three incentivizing features to increase the acceptance of the CTI sharing platform. First, we enable sharing CTI with known recipients to foster trust. Second, a reputation system designed for CTI sharing improves on traditional approaches. Third, a novel price suggestion mechanism offers valuable guidance on CTI pricing.
- We identified two incentive mechanisms that address increasing platform usage. First, financial payments integrate recurring deposits that simplify CTI sharing by preventing a lack of funds to purchase CTI records. Second, we highlight the participation in proactive cybersecurity to partners and customers with a novel marketing label.
- We implemented the incentives into an open-source CTI sharing platform,[1] exemplarily built atop a private permissioned blockchain.
- We evaluated the incentives with the industry professionals in hands-on interviews. We conclude that the identified incentives encourage an active sharing dynamic.

The paper is organized as follows. Section 2 reviews relevant background. Section 3 details our research method. Section 4 presents the incentives identified from the interviews. Section 5 integrates these incentives into a prototype CTI-sharing platform. Section 6 evaluates their impact, and Section 7 includes the discussion. We contrast our work with existing studies in Section 8, then conclude in Section 9.

2 Background

This section provides basic theoretical concepts. We present motivation and incentives, CTI sharing, and blockchain.

[1] Open-source code: https://github.com/techplus2024/Platform
Prototype instance to interact with: https://platform.uversy.com/

2.1 Motivation and incentives

We draw on three complementary behavioral theories to explain CTI sharing incentives: **Self-Determination Theory (SDT)** distinguishes intrinsic motivation, based on interest and sustained by autonomy, competence, and relatedness, from extrinsic motivation, driven by external rewards (financial or social) that trigger immediate but often short-lived action. Combining both can yield prompt behavior change with lasting engagement [13]. We operationalize intrinsic motivation by supporting *autonomy* through contributor control over what to share and with which community; enhancing *competence* via reputation insights, feedback, and automatic price suggestions that help allocate analyst time; and fostering *relatedness* through exchange within a trusted community. We leverage extrinsic motivation with financial payments to offset analyst effort and a marketing label that signals proactive cybersecurity to external stakeholders.

Institutional Theory (IT) suggests that organizations conform to coercive, normative, and mimetic pressures to gain legitimacy [14, 15]. We reflect these through sharing within a community and a marketing label that recognizes proactive cybersecurity behavior, including visible contribution metrics that enable benchmarking of CTI sharing.

Resource Dependence Theory (RDT) argues that firms exchange resources to reduce uncertainty and reliance on external actors [16, 17]. Price suggestions, financial payouts, and reputation-based indicators create a market that broadens access to high-quality CTI and lowers search/transaction costs, reducing dependence on commercial providers.

In summary, we apply SDT to explain *why* our identified incentives enhance individual and collective CTI-sharing motivation, IT to explain *how* normative pressures entrench these incentives within organizational fields, and RDT to demonstrate *how* they minimize reliance on outside providers.

We incorporate insights on cybersecurity incentives. Reittinger and Pernul [18] propose a taxonomy of positive incentives and catalogue diverse motivators for cybersecurity. Moreover, Reittinger et al. [19, 20] find that incentives are a viable means of shaping cybersecurity behavior. We also draw on incentive research from non-security domains. Kamenica [21] investigates incentives' economics and psychology, identifying that incentives are powerful but should be achievable, as too steep incentives diminish motivation. Bryson et al. [22] examine the effect of financial incentives on performance and discover that increased payment results in enhanced productivity and effort. Furthermore, Malaga [23] and Tadelis [24] conclude that reputation systems minimize fraudulent activity and suggest rewarding users who rate others. Jahn et al. [25] conclude that marketing labels can signal reputation. We transfer these insights to CTI sharing.

2.2 CTI sharing

To exchange CTI effectively between different organizations, several data formats have emerged [26]. A well-known and widely used open-source standard is Structured Threat Information Expression (STIX), which relies on semi-structured information in JavaScript Object Notation (JSON) [27]. A STIX document is a CTI record that contains STIX Domain Objects (SDOs). There are various SDOs, such as an attack pattern, which can document attacker behavior (TTPs). STIX Relationship Objects (SROs) can link different SDOs and show relationships between them. STIX enables a flexible representation of CTI, such as a threat report.

Furthermore, MITRE ATT&CK is well-known for describing attack patterns [28]. The framework categorizes attack techniques into individual phases of a cyberattack. 14 cyberattack phases describe a cyberattack's life cycle, such as initial access and impact. In this paper, we utilize STIX to exchange CTI on the platform and use MITRE ATT&CK to implement one of our interview findings.

2.3 Distributed ledger and blockchain

Distributed Ledger Technology (DLT) is a decentralized and replicated database with multiple nodes in which various participants can agree on the database state with consensus mechanisms [29]. DLT is best suited when participants do not fully trust each other or a centralized third party with their data and processing. The technology enables transparency by executing *Smart Contracts*, a program logic decentralized on all nodes, and the result is determined by a majority vote [30]. Thus, data integrity is ensured. The blockchain is the best-known DLT implementation.

In a blockchain, data is stored in a growing chain of coherent blocks, where a block contains several transactions. Each participant has a cryptographic key pair, representing the pseudonymous blockchain identity, to sign and verify transactions, thus ensuring data authenticity [30]. Blockchain can be distinguished into different types [31]. On *public permissionless* blockchains, anyone can create an identity, participate, and read all transactions. In contrast, on *private permissioned* blockchains, only selected participants can create an identity, conduct transactions, and read transactions. We use a private permissioned blockchain as an example architecture for implementing our CTI sharing platform, as it inherently supports some of the incentives we have identified.

3 Methodology

The study was conducted between October 2023 and May 2025 and comprised three sequential phases to uncover how to motivate professionals to share CTI, visualized in Figure 1. Our aim was to qualitatively explore effective incentives for CTI sharing, based on specific sharing impediments. In **Phase 1**, we identified sharing impediments and key incentives by interviewing industry experts. In **Phase 2**, we incorporated these incentives into a prototype CTI-sharing platform. Finally, in **Phase 3**, we evaluated the impact of the embedded incentives by conducting hands-on interviews. Participants represented unique organizations, except for P4 and P8, who were from the same organization.

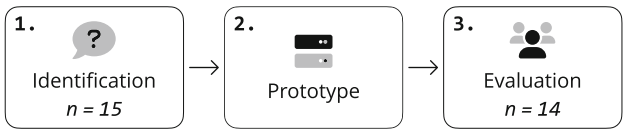

Fig. 1 Research method encompassing three phases

3.1 Identification (Phase 1)

We sought both strategic and operational insights by interviewing two stakeholder groups: business executives, who oversee CTI-sharing decisions, and cybersecurity practitioners, who execute and manage them. To uncover a full spectrum of barriers and motivations, we recruited participants from organizations that both do and do not currently share CTI, as well as from smaller security service providers that manage CTI exchange on behalf of larger clients. Leveraging professional networks (e.g., LinkedIn), industry contacts, and our institution's alumni network, we ultimately enlisted 15 participants during Phase 1. Despite time constraints and the sensitive nature of the topic, our sample spans multiple sectors, regions, regulatory regimes, roles, and organization sizes (see Table 1). Several participants from smaller organizations (e.g., P1, P6, P7, P9, P18) worked at security service providers responsible for cybersecurity across numerous client organizations, providing extensive cross-organizational insight.

To develop the questionnaire, we followed the established methodology of cognitive interviewing [32]. Before interviewing the participants, we conducted a pretest with two fellow researchers to improve the clarity and structure. The interview questionnaire was structured into four parts. *(1) Demographic Questions* characterize the background and experience of the participants. Subsequently, we explore the participants' current *(2) CTI Sharing*. Based on these insights, we ask about *(3) Incentives for CTI Sharing (Open Questions)*. Our open questions encourage participants to suggest unbiased ideas for incentives and their design. Finally, we ask about *(4) Incentives for CTI Sharing (Specific Questions)* that participants did not previously address. We added the interview structure in the Appendix A.

All interviews were conducted in German and English, using Zoom and Microsoft Teams. First, we informed participants that we would record the audio to transcribe quotes and use them anonymously in this paper. After the participants had consented, we began recording and asked them to repeat their consent to document it. We then started with demographic questions, ensuring all participants matched the target population. Subsequently, the remaining three parts of the interview guide were asked. As new ideas for incentives and their design were suggested by participants throughout the interviews, not all incentives were discussed with every participant in the interview because these suggestions were not yet available at the time of their interview. We contacted these participants by email and asked them about the incentives that had not yet been discussed. All participants responded to our message, thus ensuring that each participant addressed every question. The duration of the interviews ranged from one hour to two hours.

We transcribed the audio recordings using Microsoft Word after the interviews. Following the flexible coding approach [33], two authors of this paper independently performed the coding process and then jointly merged the individual codings into the final coding scheme. This final coding scheme was then jointly applied to assign the coding to the corresponding themes of the interview structure using thematic analysis [34].

3.2 Prototype development (Phase 2)

Based on our interviews, we identified the key incentives for organizational CTI sharing. To test feasibility, we built a prototype CTI-sharing platform that embeds these incentives. Leveraging insights from the interviews, we first designed the system architecture and selected appropriate technologies. Next, we implemented each incentive mechanism within the prototype. Finally, we published the source code as an open-source artifact and deployed the platform. Thus, our prototype can be fully interacted with as a website in the browser without coding experience or hardware requirements.

3.3 Hands-on evaluation (Phase 3)

To evaluate how the implemented incentives shaped sharing dynamics, we deployed the prototype platform. Our initial plan was to monitor a community's sharing activity over several months, yet this proved infeasible due to privacy constraints (see Section 4.2.1). Instead, we conducted hands-on interviews in which participants explored the live prototype and experienced its incentive mechanisms firsthand. Mirroring our Phase 1 approach, we enlisted fourteen participants in total: three new experts and eleven individuals who had taken part in Phase 1. The questionnaire of the evaluation is listed in Appendix A.

3.4 Ethics

Ethical considerations are a crucial part of our research. Thus, before conducting our study, we received approval for our research approach from the German Association for Experimental Economic Research e.V. [2] and obtained an Institutional Review Board certificate. The certificate has the number "1gpKGsYr" and can be viewed online. Our study design minimizes the collection of personal information, which is used only to characterize the participants' demographics. Furthermore, we obtained informed consent for the participation and audio recording at the beginning of the interview, and participants could withdraw their consent at any time during and after the interview. After the transcription and coding, the audio recordings were deleted to safeguard the participants' privacy. Additionally, we removed any characteristics that identified the participants or their affiliations from the collected transcripts. Thus, quotes are anonymized, and the number of employees is given as a range in the demographics summary (Table 1). To mitigate inaccuracies, we gave participants the opportunity to review and correct the citations they used.

3.5 Limitations

Our results should be interpreted in light of the following limitations. First, the data are self-reported and thus subject to recall inaccuracies. Second, recruitment was nonrandom and likely overrepresents European organizations. Regional and cultural differences, such as GDPR-driven privacy guidelines, regulatory breach-disclosure requirements, or social norms around reciprocity, may impact generalizability and shape which incentives resonate across regions. The sample may also overrepresent organizations that already share CTI, which helped us learn from their experiences but may bias the results. Third, many participants took part in both the identification and evaluation phases, introducing possible commitment bias, though this enabled a deeper assessment of the prototype. Nevertheless, as Table 1 shows, our sample spans diverse regulations, organizations, and backgrounds. We conducted 15 interviews in Phase 1 and 14 hands-on interviews in Phase 3, numbers comparable to similar qualitative studies [35]. Finally, because a long-term community deployment was infeasible, we approximated real-world impact through hands-on, task-based interviews, which may not capture longitudinal dynamics.

[2] Link: https://gfew.de/ethik/1gpKGsYr

Table 1 Summary of interview participants' characteristics.

ID	Phase 1	Phase 3	Job title	Sector	Employees	Gen.	Exp.	Org. Location	Sharing CTI
P1	✓		IT Security Consultant	Penetration testing	1-9	M	4	EU	
P2	✓	✓	Security Analyst	Software development	10-99	F	20	EU	
P3	✓	✓	IT Security Consultant	Consulting	100-999	M	12	EU	✓
P4	✓	✓	CISO	Software development	1,000-9,999	M	8	EU, NA, SA, AS	✓
P5	✓	✓	Security Architect	Automotive	+10,000	M	11	EU, NA, SA, AS	
P6	✓	✓	CEO	IT service provider	1-9	M	14	EU	✓
P7		✓	IT Security Consultant	Penetration testing	1-9	F	7	EU	✓
P8	✓	✓	ISO	Software development	1,000-9,999	M	3	EU, NA, SA, AS	✓
P9	✓	✓	Director of Cybersecurity	IT service provider	10-99	M	25	EU	
P10	✓		CEO	Automotive	10-99	F	15	EU	
P11		✓	Cybersecurity Engineer	Penetration testing	100-999	M	7	EU, NA, AS	✓
P12	✓		ISO	Consulting	10-99	M	10	EU	
P13		✓	Senior Incident Handler	Security services	100-999	M	24	EU	✓
P14	✓	✓	Cybersecurity Engineer	Manufacturing	1,000-9,999	M	4	EU	
P15	✓	✓	Security Manager	Pharmaceuticals	1,000-9,999	M	11	EU, NA, SA	
P16	✓		CISO	Manufacturing services	+10,000	M	9	EU	
P17	✓	✓	CEO	Retail	10-99	M	35	EU	✓
P18	✓	✓	CEO	Penetration testing	1-9	M	23	EU	

CISO: Chief Information Security Officer. ISO: Information Security Officer. CEO: Chief Executive Officer. Gen.: Gender. Exp.: Experience. Org: Organization. EU: Europe. NA: North America. SA: South America. AS: Asia

Table 2 Summary of interview findings with identified problems and solutions of CTI sharing

Identified Problems		Identified Solutions	
Occurrence	Impediments (4.1)	Incentives (4.2, 4.3)	Platform Architecture (4.4)
14 / 15	Distrusting recipients	Community Sharing, Reputation System	Decentralized Platform, Pseudonymous Payments
13 / 15	Doubtful benefit	Reputation System, Price Suggestion, Financial Payments, Marketing Label	Decentralized Platform, Pseudonymous Payments
4 / 15	Time constraints	Reputation System, Price Suggestion	
2 / 15	GDPR	Community Sharing	

4 Incentives identification

In this section, we outline the interview results, summarized in Table 2. First, we describe participants' prior *Sharing Experiences and Impediments* to CTI sharing. Next, we cover *Incentivizing Features* to increase the platform's acceptance and *Incentive Mechanisms* to address enhancing the platform's usage. Finally, *Platform Architecture* outlines the foundational architecture of the platform. "Members" refer to general participants within a CTI sharing community, and "participants" refer to our 18 interview participants.

4.1 Sharing experience and impediments

Eight participants have prior sharing experience, which we outline as follows. Participants primarily share IoCs, in particular IP addresses, and brief threat reports, such as exploitable vulnerabilities. IoCs are typically put on block lists, and the system administrators read threat reports. Most participants from small organizations can often only capture "*high-level insights in 90% of incidents*" ($P12$) due to fewer security systems in place. In contrast, participants from larger organizations with their own cybersecurity departments can create sophisticated threat reports: "*We document root cause, mitigation measures, and preventive measures as part of our incident response processes*" ($P4$) . Yet, these participants only rarely do so. Participants P4, P7, and P8 share self-collected CTI data within closed groups. This exchange primarily occurs via email, Slack, or Telegram, and in one case through a CTI sharing platform. However, they emphasize that the lack of anonymity options and the limited amount of data received in return often slow down the exchange. Consequently, they refrain from sharing more sensitive information. Participants P6, P13, and P17 are either security service providers themselves or use such services. These providers analyze their clients' threat IoCs, store them in proprietary databases, and distribute them across the security systems of their own client base. As a result, information sharing is limited to the provider's customer network, with no exchange taking place between different service providers. In contrast, participants P3 and P11 engage in informal exchanges about current threat developments through personal workshops or regular discussion groups. Overall, our participants offer insights into diverse sharing experiences.

Furthermore, we identified impediments to CTI sharing, displayed in Table 2 with the number of interview occurrences. The most important obstacle to CTI sharing is distrusting recipients (14 / 15 participants). Most participants refrain from sharing CTI records, which are sensitive data for them, with unknown or untrustworthy recipients. They fear an incident could be made public, resulting in a loss of reputation. One participant describes this impediment "*is mainly due to human concerns and less to organizational obstacles*" ($P3$)3. In addition, many participants see only doubtful benefits in CTI sharing (13 / 15), as "*there is no incentive to take on the work*" ($P5$) or they "*cannot assess the impact for their own organization*" ($P18$). In contrast, time constraints are a minor impediment for participants (4 / 15). The processing and sharing of CTI records require efforts that, combined with a doubtful benefit, are perceived as not beneficial by some participants. Finally, the General Data Protection Regulation (GDPR) is the least important impediment to CTI sharing (2 / 15). Here, the participants' organizations lack legal expertise and are concerned about "*which data in CTI records are personal data that fall under regulation*" ($P1$). Nevertheless, GDPR allows the processing and sharing of CTI as a legitimate interest while minimizing personal data [36].

In the following, we discuss each identified incentive and indicate which participant-reported impediment it helps to mitigate (see Table 2 for an overview).

4.2 Incentivizing features

We identified three incentivizing features. While a CTI sharing platform requires a basic set of functionalities, such as an engaging user interface, the incentivizing features are requirements that go beyond and increase the motivation to

share CTI. We present *Community Sharing*, *Reputation System*, and *Price Suggestion*.

4.2.1 Community sharing

Participant P2 explains the reasoning for community sharing: "*We do not want our own CTI records to end up on servers of unknown third parties. We only want to share CTI with a known group.*" (*P*2) A community can be grouped by sector, location, or interest. In Germany, every company is required by law to join one of 79 Chambers of Industry and Commerce [37]. These chambers are local groupings and offer free workshops on cyberattacks. Thus, "*every organization is already in a community suitable for CTI sharing.*" (*P*17) In addition, most participants are in one or more additional communities. Thus, organizations can conveniently participate in the CTI sharing community. The member-restricted communities mitigate the impediments of *trusting unknown parties* and *GDPR*, as this regulation requires measures to minimize the data protection incident risk, according to Article 32 of GDPR [38]. Following SDT, this feature increases relatedness to the community and facilitates intrinsic motivation; it also supports *autonomy* by letting contributors choose the audience and scope of disclosure. From an IT perspective, it taps into *normative* and *coercive* pressures of established communities to legitimize CTI exchange, and adds a *mimetic* channel as organizations emulate respected peers' sharing practices. In line with RDT, this feature reduces uncertainty and dependence on external actors by pooling critical intelligence, lowering search/transaction costs, and increasing collective resilience and bargaining power.

Design. It is crucial to organizations that they "*know it is a well-known or trusted community. [They] don't need to know all members personally [...]. Still, the restriction to a closed community is crucial.*" (*P*10) Within a community, organizations "*do not want to know who is explicitly providing and receiving CTI because when it is possible to pinpoint a CTI record to a specific organization, [they] are concerned about a loss of reputation.*" (*P*5) Organizations only "*want to know that [they] delegate CTI to and from a trusted community, but not who exactly is providing or receiving it.*" (*P*17) Thus, organizations require pseudonymity within a community. Such a closed and trusted community also ensures that attackers cannot access the shared CTI data. In contrast, an open-access platform could allow attackers to realize that their IoCs are being tracked and their attack patterns detected, enabling them to adapt their approaches accordingly.

As our interview participants come from different sectors and company sizes, their communities differ regarding the number of community members, the average number of employees, and activity. To address the different needs of the communities, we introduce community properties. These properties, described in Section 5.4, allow communities to set individual parameters that precisely align with the features and incentives.

Threat Modeling. However, merging into a community has potential drawbacks for pseudonymity. Outliers, e.g., organizations smaller or larger than average, could be identified based on their distinctive activity. Thus, a community must maintain a certain member size and homogeneity. This ensures that an individual organization cannot be identified by combining the community's external context with a limited member size and available metadata. Nevertheless, community sharing suits all organization sizes, combining large organizations' offerings and purchasing capabilities alongside small organizations' domain insights.

4.2.2 Reputation system

When utilizing CTI, organizations want to ensure that it "*provides value and strengthens cybersecurity*" (*P*18). To evaluate the quality of a CTI before obtaining it, participants want a "*reputation system that rates individual CTI records*" (*P*2). Thus, organizations have a higher level of trust in the platform and are more willing to use CTI from the platform. The reputation system thus mitigates the impediments *doubtful benefit*, *time constraint*, and *distrusting unknown participants*. Following SDT, reputation systems build *competence* via feedback and transparent impact and foster *relatedness* through peer recognition. From an IT view, reputation sets *normative* quality expectations, enables *mimetic* benchmarking, and meets *coercive* pressures from standards and regulators. In RDT terms, community-vetted scores reduce uncertainty and information asymmetry and lower search and transaction costs.

Design. There are three approaches to determining CTI quality. First, external experts evaluate each record before publication, but participants "*don't want to pay experts to evaluate [their] CTI*" (*P*1) and "*want to keep [their] CTI inside the community*" (*P*10). Second, expert members within the community assess records proactively, though security analysts "*would prefer not to spend time proactively assessing masses of CTI records that might not even be purchased.*" (*P*2) Third, members rate CTI after receiving it. While "*members must actually rate CTI records for the reputation system to work*" (*P*8), most organizations (13/15) "*are willing to adopt a mandatory rating system because [they] recognize that this helps everyone*" (*P*8).

A reputation system based on individual ratings is thus introduced. Communities can adjust two properties: the time horizon for submitting ratings and the rating percentage, i.e., the minimum share of received CTI that must be evaluated. Before these "*requirements are met, members should not be able to further participate in the platform.*" (*P*4) Ratings can be updated if a CTI record improves. For new, unrated records, "*the average rating of all CTI records of a member*

should be displayed as a substitute" (*P*2), which "*motivates [organizations] to be well rated and to offer CTI in the long term.*" (*P*17)
Threat Modeling. The reputation system could be exploited if two organizations collaborate and give each other positive ratings, creating a zero-sum incentive. Monitoring can help detect such behavior, for example, by flagging above-average frequencies of mutual ratings, allowing the community to investigate and potentially exclude bad actors. However, collaborating to exploit the system has significant downsides: organizations lose pseudonymity with their collaborators, and past or future CTI sales could be exposed, damaging their reputation. Therefore, legitimate users are unlikely to engage in such collusion.

4.2.3 Price suggestion

As organizations lack CTI sharing experience, participants noted that they "*don't know what a reasonable price per CTI record is*" (*P*2). Because external experts are not supposed to assess quality, they cannot determine the value of a CTI record. Thus, organizations must set the price of CTI themselves. However, the value of CTI varies greatly, as an IoC provides a value different from that of a threat report. Thus, organizations "*want a recommendation on how to price individual CTI records.*" (*P*17) Additionally, analysts who share CTI "*don't want to spend [their] time considering a price, as time is short*" (*P*2). There is no concrete approach to pricing CTI, so we introduce price suggestions to automate this process. P17 highlights the advantages of the price suggestion: "*It allows us to upload CTI faster and requires less prior knowledge. It can also increase sales as prices are set realistically.*" (*P*17) In sum, price suggestion lowers the entry barrier of CTI sharing and supports the platform economy. Hence, it addresses the impediment of *time constraints* and *doubtful benefits*, as it finds suitable prices and maximizes sales and revenue. Following SDT, price suggestions bolster *competence* through clear guidance and feedback on market fit while preserving *autonomy* by allowing contributors to accept or adjust suggested prices. According to IT, it codifies community-wide pricing norms that legitimize the CTI exchange. In RDT terms, they reduce uncertainty and transaction costs, lessen dependence on external pricing advisors or dominant vendors.
Design. To enable realistic suggestions, we define a minimum number of purchases as a community property to determine which existing CTI records are included in the calculation. This ensures that only reasonably priced records are considered, taking into account any price changes. Organizations want the price suggestion implemented in two parts: a quick summary of the average price and an in-depth comparison of previous sales. We identify three factors for comparing a new CTI record with similar records on the platform:

- **Size:** "*How many elements are in it*" (*P*4), for example the number of IoC and attack patterns
- **Content:** "*What elements are included*" (*P*2), for example an IoC or attack pattern
- **Attack Phases:** "*What phases of the attack lifecycle the CTI record covers*" (*P*3), e.g., initial access or execution

Participants find it "*challenging to determine how the factors should be specifically designed and weighted.*" (*P*17) Thus, the price suggestion offers guidance rather than a perfect solution. At the platform's launch, the feature may suffer from a cold start, providing limited value to sellers due to a small database. Novel CTI records may yield inaccurate suggestions, which can be flagged to indicate a small sample size and potential bias. Over time, as the database grows, the suggestions become more accurate, supporting the platform's longevity and benefits for all members. This initial design "*helps especially small and medium-sized organizations, as [they] have little experience in CTI pricing.*" (*P*17)
Threat Modeling. If multiple members collude to trade CTI at unrealistically high or low prices, this could bias the price suggestion. The impact is limited by using numerous purchases in the calculation and applying monitoring from Section 4.2.2. Indicators such as mutually excessive purchases can flag potential collusion. Additionally, collaborators would lose pseudonymity.

4.3 Incentive mechanisms

In addition to incentivizing features, we identified two incentive mechanisms. They encompass rewards for active participation in CTI sharing. We introduce *Financial Payments* and *Marketing Label*.

4.3.1 Financial payments

Financial payments are "*compensation for the time spent providing CTI [...] and for potential damages caused by the security incident.*" (*P*5) Additionally, "*the revenue from the sales can be used to increase the security department by covering the salaries.*" (*P*5) Organizations would prefer not to give away their CTI for free, thereby not allowing free riding and addressing the impediment *doubtful benefit*. Following SDT, financial payments increase extrinsic motivation, and the design of this incentive enhances autonomy, thus maintaining intrinsic motivation. From an IT perspective, payments formalize fair-reward norms, satisfy coercive accounting expectations, and create mimetic pressure as peers adopt compensated sharing. According to RDT, they reduce uncertainty and dependence on external funding by creating self-sustaining, internal revenue streams.
Design. Organizations must first deposit capital on the platform to purchase CTI, and participants prefer a pay-per-use

subscription. As P4 explains, "*It is easier to pay in periodic amounts automatically [...] as the funds are on the platform when you need them.*" (*P*4) This enables rapid CTI purchases in response to threats, and participants note they are "*clearly more willing to buy CTI because there is always a balance available.*" (*P*8) Periodic subscriptions should be tailored to each organization, with unused balances "*accumulating over several periods.*" (*P*4) Each CTI record should have an individual price and be purchasable directly from the balance. Manual deposits must be possible once the periodic funds are exhausted. Although participants consider "*a subscription with unlimited CTI access is convenient, the platform economy is likely not sustainable.*" (*P*5) Finally, deposits and sales revenues "*should be possible to be withdrawn at any time.*" (*P*17)

Threat Modeling. One disadvantage of financial payments is that the buyer must make the payment first and only knows whether the CTI record provides value afterward. We counteract this issue with the reputation system to give a strong indicator of the expected quality and value. Even if a CTI record has not yet been rated, a seller's average rating of all CTI records is displayed.

4.3.2 Marketing label

The marketing label is an "*excellent way to show customers and business partners that [an organization is] proactively increasing cybersecurity*" (*P*3), thus mitigating the impediment *doubtful benefit*. Additionally, the marketing label enhances the activity within the platform because, as we explain in the following, organizations have to fulfill requirements to obtain the label, which results in more purchases and sales. Furthermore, the marketing presentation increases awareness within the community and on the platform. Beyond serving as a social reward that increases extrinsic motivation, this mechanism strengthens relatedness due to peer recognition and, thus, intrinsic motivation, according to SDT. From an IT standpoint, marketing labels leverage normative and mimetic pressures to legitimize and normalize CTI sharing. In accordance with RDT, they also reduce reliance on external trust signals by creating a community-endorsed marker of quality and reliability.

Design. The marketing label is issued per community, allowing organizations to hold multiple labels from different communities. Each label displays the community name for distinction. For the label, it is "*accepted that people outside the community get limited insight to verify the label.*" (*P*9) To ensure its value, the "*issuance should be linked to requirements, specifically a minimum number of sales, purchases, or membership duration.*" (*P*1) As "*the marketing label would be worthless if the requirements are too low,*" (*P*6) each community must define appropriate thresholds that are challenging yet attainable for active members. This, in turn, increases supply, demand, and overall engagement on the platform. As a result, "*the popularity and reputation of the marketing label and the community will also increase.*" (*P*10)

To maintain long-term value, "*the requirements must be verified periodically. Thus, the marketing label is only valid for a limited period.*" (*P*17) After each validity phase, it should be renewed or withdrawn. A "*verified since*" field further incentivizes members to remain active across periods.

Organizations are "*reluctant to publish the specific sales thresholds required to earn the marketing label, since doing so could indirectly reveal that a security incident has occurred.*" (*P*2) However, they agree that sharing aggregated metrics–such as total purchases or average rating scores–can enhance transparency. To foster trust, each label receives a unique identifier and can be publicly verified through an external service.

Threat Modeling. Organizations joining forces could attempt to exploit the marketing label through coordinated trading to fulfill the requirements or transfer it to members who have not met the requirements. Such behavior can be detected using the monitoring described in Section 4.2.2, for example, by identifying mutually above-average purchase patterns. Yet, exploiting the system would require collaborators to give up pseudonymity between each other. As participant P4 concludes: "*[The proposed design] is the best you can do, most members will be honest and have a major incentive to sell and buy more CTI.*" (*P*4)

4.4 Platform architecture

In addition to incentivizing features and incentive mechanisms, we identified two requirements for the platform's design, which are crucial for the willingness to engage in CTI sharing. They determine the underlying architecture of the platform for the subsequent implementation of incentivizing features and incentive mechanisms. We present *Decentralized Platform* and *Pseudonymous Payment System*.

4.4.1 Decentralized platform

We described in Section 4.1 that for participants, the most significant impediment to organizational CTI sharing is trusting recipients (14/15 participants). Thus, they not only want to restrict the number of platform members (addressed by community sharing) but also distrust centralized platform providers holding their data: "*We don't want to hand over our sensitive data to a platform provider, only to buyers*" (*P*4). Participants are concerned about a single entity controlling the CTI platform and misusing their data: "*Centralized providers might analyze or use my CTI data for their own purposes, which is what large platform providers usually do*" (*P*12). These concerns reflect challenges already observed in

the field of cloud computing, particularly regarding security, as well as the limited transparency and control over stored sensitive data [39, 40].

Also, the participants consider centralized data storage and processing to be unnecessary, as the acquired CTI must be directly integrated into their own security systems. "*We integrate malicious indicators into local systems such as firewalls, and use threat reports to enrich our own threat knowledge bases*" (*P*8). This leads to the conclusion that a peer-to-peer exchange model is more efficient: "*A direct transfer of CTI data between participants makes sense, as it eliminates the unnecessary middleman*" (*P*8).

Furthermore, the sharing community wants to "*define [its] properties and approve members collectively*" (*P*2), rather than entrusting a single entity with administrative control. This approach prevents the risk of unauthorized participants being registered by a sole administrator without notice.

As a result, we consider a decentralized architecture for the platform, as it enables organizations to administer the platform themselves and to store their CTI records physically on their own infrastructure within their security domain. Thus, they do not have to transfer their CTI records to a central instance to offer them on the platform. Organizations only have to give buyers access to their purchased CTI records.

4.4.2 Pseudonymous payment system

The identified incentives have shown that the network must be limited to selected participants and that these can operate pseudonymously within the network (Section 4.2.1). In addition, monetary rewards increase the motivation to share one's own CTI data records (Section 4.3.1). To enable this process, it must also be possible to carry out such transactions pseudonymously between the participants. A crucial aspect is that there "*must be no invoice documents that reveal the names of the buyer and seller organizations*" (*P*5). At the same time, it is essential for the long-term participation of the organizations in the platform that this "*pseudonymous payment system is both trustworthy and compliant with regulations*" (*P*16). Traditional payment service providers for online marketplaces, such as PayPal, therefore cannot be integrated into the platform architecture.

5 Prototype

We integrate the findings in Section 4 into a newly developed prototype. First, we describe the implementation of the *Platform Architecture*, then we present the *Incentivizing Features* and *Incentive Mechanisms* building on it.

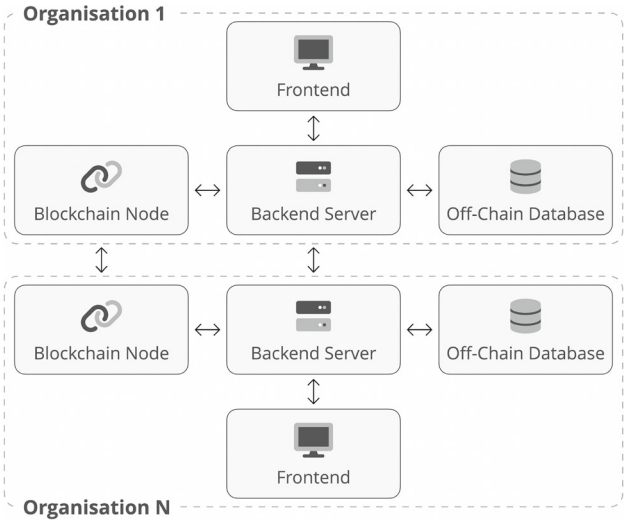

Fig. 2 Overview of the architectural components

5.1 Implementation of platform architecture

In order to implement *Decentralized Platform* and *Pseudonymous Payment System*, the architecture of the prototype is based on the four components *Blockchain*, *Off-Chain Database*, *Backend Server*, and *Frontend*. Figure 2 visualizes the components and their data flow between multiple organizations. Every organization hosts all components. We selected open-source technologies based on their maintenance activities, as well as their suitability for our requirements.

5.1.1 Blockchain

To implement the envisioned decentralized sharing platform, we adopted a blockchain-based approach. The primary motivation is that blockchain technology inherently provides a mature framework for implementing a pseudonymous payment system (as identified in Section 4.4.2), which is essential to enable monetary incentives for the exchange of CTI data within the platform. However, a public permissionless blockchain is not suitable for this purpose. Such networks do not restrict participation, and our CTI marketplace and all its transactions would be publicly visible worldwide, compromising the confidentiality required for CTI sharing. Furthermore, public blockchains fail to meet the expectations of our participants regarding a stable and trustworthy payment environment, as they are subject to significant volatility in token value and transaction fees, have experienced cases of fraud, and remain affected by regulatory uncertainty [41].

Instead, we selected Hyperledger Besu [42] as the underlying blockchain framework. It enables the creation of a private permissioned blockchain network with selected members, supports pseudonymity, and, being self-hosted, can be flexibly adapted to comply with local regulatory require-

ments. In addition, it offers scalability for high-volume data exchange and enables the creation and transfer of monetary tokens without transaction fees. This design allows us to support pseudonymous payments while maintaining control over membership and data access in a trusted community environment.

We save CTI record's metadata on the blockchain, such as the ratings. Thus, the necessary information is transparent for all members to buy a CTI record, but the record itself remains at the organization until it is purchased.

5.1.2 Off-Chain database

CTI records are stored in an off-chain database to allow each member control over their data. The records are stored in STIX format, a JSON document, enabling a standardized CTI exchange on the platform. Thus, we leverage the document-oriented NoSQL database Couchbase [43].

5.1.3 Backend server and frontend

The backend server hosts the frontend for an organization to interact with the sharing platform. Additionally, the server listens to the activity on the blockchain node, delegating purchased and sold CTI records to and from the off-chain database. For the backend server, we select Node.js [44] to interact with the blockchain node and PHP Laravel [45] to process the communication with the HTML frontend and the off-chain database.

5.1.4 Platform registration and token deposit

To enable initial onboarding and the issuance of pseudonymously usable tokens on the platform (see Figure 6 in Appendix E), we use a payment trustee that can be chosen by the platform members – e.g., a locally regulated provider operating within the same legal framework as the members. The underlying private permissioned blockchain (Hyperledger Besu) supports private transactions, allowing certain data and transactions to be accessible only to authorized members. Although the trustee is part of the platform, their access is technically limited to specific smart contracts for member registration and token deposit/withdrawal. The trustee has no visibility into the actual CTI sharing marketplace. As a result, they cannot infer the transaction behavior of participating organizations – in particular, their purchases or sales of CTI data.

An organization seeking to join the CTI sharing community must first apply for membership. Existing members review whether the applicant meets the criteria defined by the community, for example, being a registered entity from an approved country or operating in a specific industry sector. Once a consensus on the organization's admission is recorded on the blockchain, the new member generates a cryptographic key pair and submits the public key to the payment trustee. The trustee then verifies the organization's identity and confirms the recorded admission decision on the blockchain. Upon successful verification, the trustee registers the public key via the member registration smart contract. The organization can then deposit fiat currency with the trustee, who issues an equivalent amount of pseudonymous tokens using the token deposit smart contract and assigns them to the submitted public key. At this point, the new member is authorized to pseudonymously purchase or offer CTI data on the marketplace via the marketplace smart contract.

This design ensures that the platform is compliant with the regulation for identity verification of all members [46], before issuing pseudonymous tokens. The system maintains pseudonymity while disallowing anonymity (in line with the prohibition of anonymous crypto-asset accounts [46]). Authorized regulatory authorities may request access to both blockchain transaction records and token deposit/withdrawal data from the trustee in the context of a fraud investigation.

5.2 Implementation of incentivizing features

We outline the implementation of *Community Sharing*, *Reputation System*, and *Price Suggestion* as follows.

5.2.1 Community sharing

Initially, organizations have to form a closed CTI sharing community of trustworthy participants. Subsequently, they can deploy the sharing platform and generate their cryptographic key pairs. The platform stores each member's backend server's IP address and port. As the members communicate directly with each other in this decentralized system, they must take additional measures to maintain their pseudonymity. A member should not use an IP address that can be used to identify their organization. IP anonymization services, such as a VPN, can be utilized for this purpose.

5.2.2 Reputation system

o ensure the quality of CTI on the platform, members can rate a CTI record they purchased from one to five stars. Optionally, buyers can add a text-based comment to their review. We store the rating tamper-proof and transparently on the blockchain as part of the metadata of CTI records. For new and unrated CTI records, we display the average rating of a seller based on all their prior CTI records in such cases. This approach helps reduce the subjectivity of individual CTI ratings. To further minimize subjective bias, we complement member ratings with objective CTI quality metrics [47]. For instance, the *Relevancy* metric utilizes contextual information to enable potential consumers to assess

the usefulness of CTI for their specific environment. It compares characteristics such as the industry sector (e.g., finance or retail) and technologies in use (e.g., specific Linux distributions) between the publishing and consuming members. These attributes can be voluntarily provided by each member without compromising their pseudonymity within the platform.

Furthermore, to increase the number of ratings, organizations are willing to be compelled to rate purchased CTI records. If members fall below the required rating percentage or exceed the mandatory rating period, the smart contract disables further uploads or purchases of CTI records until the requirements are met. After each login, we highlight pending ratings and inform members early that they must provide additional ratings for a seamless experience without disruptions.

5.2.3 Price suggestion

As outlined in Section 4.2.3, we identified three factors in the interviews that should be integrated into the price suggestion: *Size*, *Content*, and *Attack Phases*. As the prototype utilizes CTI records in STIX format, we use the STIX elements to calculate the factors. To suggest a price for a new CTI record, we identify the similarity to prior CTI purchases based on these factors and outline their purchase prices. Thus, members get an overview of the prices of similar CTI. We describe each factor as follows.

First, *Size* counts the number of elements in a CTI record, indicating the amount of threat intelligence information stored within it. The elements are either an SDO, representing the actual content in a CTI record, or an SRO, describing the relationships between the SDOs. In addition, SDO elements such as attack patterns can define which attack phase (e.g., initial access) they are used for and which specific technique (e.g., phishing) is applied. As MITRE ATT&CK defines 14 attack phases, the number of occurring phases in a CTI record can be counted and compared to the number of phases in the new CTI record.

Second, *Content* describes the elements of a CTI record. As a record can represent IoCs or threat reports, many potential SDO elements enable a flexible composition. Thus, we can differentiate the content of CTI records based on three components: SDO, SRO, and attack phases. If SDOs of CTI records match, they offer similar content. SROs provide an additional content-related context. Two CTI records with identical SDOs can still have different SRO relationships, resulting in different content. CTI records can address the same attack phases, thus representing similar content.

Third, the factor *Attack Phases* is incorporated into *Size* as the count of attack phases and included in *Content* by addressing the attack phases of CTI records.

Using these factors, we compute a total difference delta between the new CTI record and each previously purchased record. We present the most similar CTI records and their prices, along with the average price across them. We formally define the calculation of the price suggestion in Appenidx C and demonstrate it with a specific example.

5.3 Implementation of incentive mechanisms

In the following, we describe the implementation of the *Financial Payments* and the *Marketing Label*.

5.3.1 Financial payments

We create two processes to implement Financial Payments into a CTI sharing platform, allowing an organization to sell its CTI to other interested organizations on the platform. The first process enables offering a CTI record on the platform, displayed in Figure 7 in the Appendix E. The seller (S) creates a STIX-compliant CTI record and can further specify metadata like description or type (IoC or threat report) in the frontend. The backend server performs the price suggestion by retrieving the metadata of all other CTI records from the blockchain and calculating the similarity to the new CTI record. The seller selects the final price, and the CTI record is stored locally in the seller's off-chain database. In addition, the backend signs the CTI offer, which includes the metadata of the CTI record, with the seller's private key $PrivKey_{ShareS}$. This signed offer is then published on the blockchain so all other members can view it.

The second process facilitates the purchase of a CTI record for the required amount of tokens. This process is shown in Figure 8 in the Appendix E. Based on metadata such as the rating, the buyer (B) can initiate an informed purchase. The buyer's backend then utilizes the private key $PrivKey_{ShareB}$ to create and sign the purchase transaction. The backend sends the signed transaction to the blockchain, validating and storing the transaction. This means that all members agree that the buyer's pseudonym $PubKey_{ShareB}$ has transferred the tokens required by the purchase price to the pseudonym $PubKey_{ShareS}$ of the seller and has therefore made a valid purchase. The seller's backend listens for events from the blockchain and is notified of the purchase. The seller's backend initiates an encrypted communication with the buyer's backend and sends the purchased CTI record to the buyer. The buyer's backend validates the integrity of the CTI record by comparing its hash with the one stored on the blockchain. The backend saves the CTI record in the off-chain database, and the buyer is now authorized to submit a rating using the reputation system.

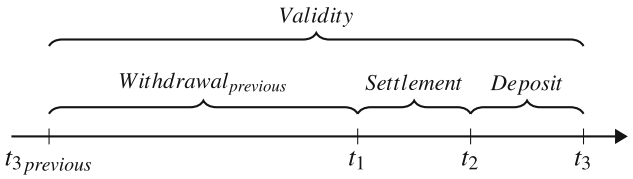

Fig. 3 Timeline of Quality Label Issuance

5.3.2 Marketing label

The **Marketing Label (ML)** is issued for a pre-defined validity period for each community member who fulfills the defined requirements. The validity period and the requirements for issuance can be specified in the community properties. The process of the marketing label issuance is displayed in Figure 9 in Appendix E and consists of multiple phases. We visualize the phases in Figure 3 and describe them as follows.

Settlement. The community defines a recurring issuance date for the ML in its properties. When this date t_1 is reached, the smart contract iterates through all the trading wallets ($PubKey_{,Share}$) and verifies whether each member meets the ML requirements. For eligible wallets, the contract issues and transfers a new ML token. In addition to the trading token representing monetary value, the ML token serves solely to prove the validity of the marketing label for the defined period.

Deposit. As the trading wallet represents only a pseudonymous identity, the marketing label cannot be directly linked to an identifiable organization. To associate it, the member transfers the marketing label token from the trading wallet to their marketing label wallet that stores the member's name. To preserve pseudonymity, this transfer is conducted through a mixer smart contract that uses Zero-Knowledge Proofs (ZKPs). Each member deposits a hashed secret together with the token into the mixer, and later proves ownership of one of the deposits without revealing which one [48, 49].

Withdrawal. During the subsequent withdrawal phase, members can reclaim an ML token to their registered marketing label wallet. To do so, they generate a Zero-Knowledge Proof demonstrating that they previously deposited a valid token without revealing which specific deposit was theirs. The mixer smart contract verifies this proof and, if valid, issues a new ML token to the member's ML wallet. This process ensures that no link between the trading and marketing label wallets can be established while maintaining continuous token validity across periods.

Validity. After withdrawal, members can display the marketing label on their website. We outline the validation of the ML in Figure 10 in Appendix E. External partners or customers can verify its authenticity through a backend verification service, which queries the associated ML wallet and retrieves the stored tokens from the blockchain. Based on the number of valid tokens, the service confirms the member's current and past validity periods. To ensure trust in the decentralized community, verification can also be performed across multiple backend servers. An example of the marketing label is shown in Figure 5 in Appendix D.

5.4 Community properties

As CTI sharing communities differ, we implement community properties to individually adjust each community's configuration of the incentivizing features and incentive mechanisms. Community properties are global variables that each community can set and modify as needs change over time. Each member can propose a new set of community properties, and other members can approve or reject the proposal. If a proposal receives a majority of approval on the blockchain, the new community properties are put in place. We describe all community properties in Appendix B.

5.5 Open-source artifact and live prototype

We publish our prototype as an open-source artifact on GitHub.[3] Thus, the community can adopt and extend our prototype with additional functionality. We deployed a running instance as a live prototype that everyone in the browser can use.[4] Thereby, the incentives and CTI sharing platform can be fully interacted with.

6 Evaluation

Below, we summarize key findings from blockchain network performance and hands-on interviews evaluating the embedded incentive mechanisms. Overall, managers prioritized incentives that increase the net benefits of CTI sharing, whereas security practitioners emphasized features that alleviate required time, effort, and coordination costs.

6.1 Performance and latency

In contrast to public blockchains such as Bitcoin or Ethereum, the private blockchain Besu employs proof-of-authority consensus mechanisms like QBFT or IBFT [42]. These protocols enable significantly higher transaction throughput and lower latency within private networks. A comprehensive performance analysis demonstrated that Besu, under high load, achieves an average transaction throughput of approximately 400 transactions per second with an average transaction latency of 1–2 seconds [50].

[3] Open-source code: https://github.com/techplus2024/Platform

[4] Prototype instance to interact with: https://platform.uversy.com/

In our platform, the actual data exchange occurs off-chain, meaning that on-chain transactions primarily consist of metadata and purchase records. Moreover, members do not trade individual IoCs, which are typically high-volume CTI data. Instead, a single transaction usually represents the purchase of a large bundle or a continuous stream of IoCs. Given that the platform is also restricted to approved members, feedback from our interview participants confirmed that their expected transaction volume would remain well below this threshold, indicating that the platform can readily sustain an active and scalable sharing community.

6.2 Community sharing

Participants emphasized that community-based sharing is essential for platform adoption: "*It builds trust and fosters sharing motivation*" ($P2$). They also predicted greater engagement if the platform served as a "*[...] one-stop store [...]*" ($P11$) for all their cybersecurity needs.

6.3 Reputation system

The feedback about the reputation system was positive. Participants find the rating with giving stars and a brief comment justifiable in terms of the time required, "*more complex rating systems with additional entries would be pointless as people would not do this*" ($P2$).

Participants expected the description for threat reports to be more extensive and frequent than for IoCs due to the scope and complexity, as "*there are more opportunities for feedback*" ($P5$). They also agreed that a minimum of 50-70% of purchased datasets should be rated, which is recognized as a "*balanced threshold between time and value*" ($P9$). Participants noted that only 2-3 ratings per dataset could be sufficient to obtain a first quality indicator, and a description would be particularly insightful. "*There are thousands of reviews on Amazon, but with such a complex topic, just a few reviews are enough*" ($P11$) because "*quality is more important than quantity''* ($P3$).

The method of soliciting feedback also gained insights. Pop-up notifications on the platform would interrupt users at inopportune moments. In contrast, email notifications were considered the most effective reminder mechanism for evaluations, catching users at more convenient times. It was recommended that "*emails should be sent within two weeks after purchase to prompt timely reviews*" ($P6$).

Furthermore, the feedback in the evaluation indicated that "*mandatory descriptions are more beneficial, even if it resulted in slightly more effort*" ($P18$). Additionally, integrating marketing labels into the review overlay was suggested to "*highlight the competence of the reviewers*" ($P11$). Finally, the average rating of sellers would help assess new datasets that had not yet accumulated ratings, and could "*provide an initial quality indicator*" ($P9$).

6.4 Price suggestion

In the hands-on interviews, participants noted that they "*have no idea what price to set*" ($P14$) for a CTI record. Thus, the price suggestion was perceived as "*beneficial and helpful*" ($P4$). While participants argued that the price suggestions could have a limited initial impact due to the few reference records available (cold start problem), they expect the suggestions to improve with usage.

We discovered that not all CTI records should be included in calculating the price suggestion, as outdated CTI records with lower values could bias the results. Participants recommended applying type-specific time windows for including them in the calculation of the price suggestion: IoCs are usually relevant for "*90 days because they can change quickly*" ($P11$), and threat reports have a "*lifespan of about 6 to 12 months*" ($P18$) according to the participants. Thus, we suggest minimizing the weighting of the current value of older CTI records that no longer reflect a comparable value in the calculation. The three used factors (size, content, and attack phases) were emphasized as "*optimal for distinguishing one record from another*" ($P3$).

6.5 Financial payments

Participants explained that "*financial payments are a major driver for activity*" ($P17$). One participant elaborated that this incentive does add enormously to the perceived value of CTI sharing: "*Financial payments demonstrate sharing's worth to management, and I could participate actively.*" ($P2$) The pay-per-use subscription model received positive feedback, allowing organizations to pre-plan their budgets for accessing the platform. Participants expected the prices of threat reports to top those of IoCs, due to the expected complexity and depth of the reports. As one participant observed, "*a more sophisticated report justifies a higher price to compensate for the effort involved*" ($P11$). Our evaluation also uncovered strong demand for a subscription model, enabling organizations to subscribe to a CTI provider and automatically purchase and receive all new data records via an API.

6.6 Marketing label

Participants acknowledged that the "*marketing label is a bigger incentive than you [initially] think*" ($P8$). They "*feel confirmed in their intention, the achievement is there*" ($P11$). To ensure the marketing label remains meaningful and achievable, we identified reasonable thresholds for achieving it. Participants agreed that the validity of the marketing label should last one year, analog "*as an ISO 27001*

doesn't last forever either" (*P*6). According to the participants, further requirements regarding purchase and sale volumes should be determined individually per community. We suggest keeping the sales requirement low to ensure organizations can acquire the label, as they have limited control over their sales volume. Additionally, participants suggested incorporating the rating of CTI records into the requirements, further incentivizing active participation and engagement within the CTI sharing community. Participants find 10 ratings as a practicable threshold.

7 Discussion

In this section, we discuss our findings and future work.

7.1 Community sharing

In a CTI sharing community, large and small organizations are complementary. Large organizations contribute curated datasets and mature analytics backed by sophisticated tooling and greater budgets, while small organizations add niche, regional, and early-warning signals that broaden coverage. In turn, large organizations gain richer telemetry and real-world validation, which reduces blind spots and false positives, while small organizations gain affordable access to high-quality CTI that they couldn't produce alone. The proposed incentives help balance contribution asymmetries and distribute curation costs through financial compensation, raising the security baseline for all.

Community sharing currently requires multiple participants to register simultaneously to preserve pseudonymity. To enable independent onboarding, we propose the use of a Self-Sovereign Identity (SSI) [51]: a trusted authority (e.g., a public institution or EU body) issues a verifiable credential with basic attributes (legal name, sector, location). Applicants then selectively disclose only eligibility attributes (e.g., finance sector, Germany) for peer validation, thereby cryptographically proving eligibility while maintaining pseudonymity; an external payment trustee still performs full identity verification. This approach allows organizations to join at any time without compromising pseudonymity.

Currently, a payment trustee, also referred to as a broker in public blockchain systems, remains a crucial component of all blockchain-based payment mechanisms, as it verifies identities and manages fiat funds, thereby bridging decentralized ledgers and the banking system. As regulations evolve, verification could be distributed across multiple independent entities that must agree on the outcome, thereby reducing reliance on a single intermediary.

7.2 Reputation system

The incentive model helps mitigate analysts' time constraints, for example, through automatic price suggestions and periodic payouts. Still, some components, notably the reputation system, introduce overhead. Future work should streamline these mechanisms, for instance, by developing an automated reputation system that leverages large language models to infer CTI quality dimensions [47] from contributed records.

7.3 Price suggestion

We identified three criteria for the price suggestion in the interviews. As our concept is a first approach, we demonstrated the demand for a price suggestion. Future work could expand this feature by researching possible additional criteria. For example, the size or sector of the organization could be considered to refine the price suggestion. Additionally, the cold start problem could be tackled by developing general guidelines or pricing standards for CTI. Therefore, the price difference between CTI types can be investigated to enhance the price suggestion. Furthermore, sellers would benefit from continued price suggestions for already offered CTI, as the value can change over time. Moreover, future work could explore digital nudges to encourage adoption of the price suggestion, given prior findings that nudges influence behavior in other cybersecurity contexts [57]. Thus, the CTI prices could be improved, increasing sharing activity.

7.4 Financial payments

We suggest initially filling the platform with some CTI records and making them available to participants free of charge. This addition would initiate the sharing dynamic, allowing participants to try out CTI records without risk. Thus, participants could be more willing to make financial payments and participate actively. A future analysis could investigate this effect.

7.5 Marketing label

It is essential that the requirements for obtaining a marketing label are achievable for the average member. Otherwise, the effect of the incentives could be diminished, and pseudonymity could be compromised as an outlier would be identifiable within a limited number of marketing labels. Hence, the requirements for the marketing label should be selected carefully and adjusted as the community evolves.

Table 3 Comparison of our findings to related platform proposals

	[52]	Blocis [53]	[54]	Trident [55]	Dealer [12]	MISP [56]	This Paper
Community Sharing	○	○	●	○	○	◑	●
Reputation System	◑	◑	◑	●	◑	◑	●
Price Suggestion	○	○	○	○	○	○	●
Financial Payments	●	●	◑	●	●	○	●
Marketing Label	○	○	○	○	○	○	●
Open-Source Code	○	○	○	○	●	●	●

Our findings are ● fully addressed, ◑ insufficiently addressed, ○ not addressed

7.6 Platform governance

The platform has been released as open source, enabling the community to extend and further develop its functionality in the future. The architecture components, backend services, off-chain databases, and the blockchain are operated by the participants themselves. The blockchain does not have to be maintained by all participants, but can also be managed by a subgroup of them. If desired, certain organizations, such as chambers of commerce or security service providers, can take over hosting of the entire infrastructure on behalf of their members or customers. In such a setup, a security service provider could assist a client in analyzing and mitigating an incident, and subsequently publish the related CTI information for sale on the platform. For the affected organization, it is acceptable that CTI data are processed within the backend and off-chain database of its trusted security provider, as long as the provider ensures responsible handling of the data and preserves the pseudonymity of the organization towards other platform participants. This approach reduces the infrastructure requirements for individual participants, who in turn may provide financial compensation to the entities operating the components.

8 Related work

We compare related approaches, including incentivized blockchain-based CTI sharing solutions and MISP [56], one of the most widely used threat intelligence sharing platforms [58], as summarized in Table 3.

Riesco et al. [52] use Ethereum to trade CTI records. They introduce a platform-specific CTI token and an additional member role, the investors, using the marketplace as an investment opportunity. The more trading takes place on the platform, the higher the price of the CTI token. The data producers are additionally incentivized to share data by being able to purchase CTI tokens at a reduced price, thus receiving a second income stream. A seller can be rated, although this is not explicitly addressed in the paper. Furthermore, individual CTI records cannot be evaluated based on quality.

Gong and Lee [53] leverage Ethereum for the CTI sharing Platform "Blocis". Consumers can store their evaluation function for data quality in a smart contract. The evaluation is automatically executed when a data producer uploads new CTI records to the blockchain. The feed pays the data producer with Ether tokens if the quality evaluation is positive. Although data quality is addressed in Blocis, there are no details of how this automated evaluation can be conducted, meaning that the reputation system remains abstract.

Nguyen et al. [54] propose a member-restricted community sharing architecture based on the Hyperledger Fabric permissioned blockchain for industrial control systems. A member must pay a periodic subscription fee to gain unlimited access to all data on the platform. However, according to our interview findings, consumers' unlimited access limits the monetary incentive for data producers. In addition, internal community verifiers have to check the quality of the data before it is uploaded to the platform. However, we find that members only want to evaluate CTI records that they have purchased and consider relevant for themselves.

Alexopoulos et al. [55] use the public blockchain Ethereum for the CTI marketplace "Trident", where subscribed IoC streams can be purchased and rated. A buyer must deposit tokens in the smart contract, which they can only receive again after submitting their rating. Thus, members are compelled to use the reputation system.

Menges et al. [12] propose the platform "Dealer" based on the public blockchain EOS, where members can sell their CTI pseudonymously and report a cyberattack to legal authorities based on reporting obligations. Random verifiers rate a CTI record independently before uploading. Despite this, these verifiers are unknown and require a fee to rate the CTI records. This contradicts our findings of the reputation system. Dealer offers the software code as open source.

While MISP [56, 59] is not based on blockchain technology, it still functions as a decentralized system. Participants can host their own MISP instances, which synchronize with each other through push and pull mechanisms. Threat data can be shared either with selected organizations within a sharing community or, for broader dissemination, with additional MISP instances. However, participating organizations

are registered in the system with their real names and are clearly identifiable. To avoid being directly associated with an incident, an organization can delegate its threat data to another organization, which then distributes the data on the platform. Nevertheless, the delegated organization still becomes aware of the security incident, meaning that true pseudonymity is not ensured within the platform. MISP also includes a sighting system that allows participants to provide feedback on shared CTI, particularly IoCs. They can confirm having observed the data or mark it as a false positive or expired. However, textual comments or ratings cannot be added, which is a limitation, especially for threat reports.

In summary, related publications primarily use public blockchain systems, thus not meeting organizations' requirements of a known and limited group of recipients. While related work implements a reputation system and financial payments, most papers insufficiently address organizations' needs. Furthermore, no work introduces a price suggestion or marketing label; only one publication presents a prototype as open-source. MISP offers only limited community sharing and reputation mechanisms and does not address the remainder of our incentives. Its primary focus is on sharing IoCs rather than the often more sensitive threat reports. Thus, our paper offers profound insights into incentives designed to encourage the sharing of all types of CTI.

9 Conclusion

In this paper, we investigated incentives for CTI sharing. Based on interviews with professionals, we identify that the acceptance of a CTI sharing platform can be enhanced by sharing with a known group of recipients and by obtaining crucial information about CTI records through a reputation system and a price suggestion. Furthermore, organizations' platform activity can be increased by financial payments for their CTI records and a marketing label to outline their proactive cybersecurity efforts to partners and customers. We implemented the identified incentives into an open-source prototype and evaluated their impact with hands-on interviews, indicating that they promote the sharing dynamic. Simply put, organizations can share and benefit.

Appendix A Interview questions

In the following, the questions from the semi-structured interviews are listed.

I. Demographic Questions

- What is your job title?
- In which sector is your organization?
- How many employees does your organization have?
- What is your gender?
- How many years of experience do you have in your field?

II. CTI Sharing

- Is your organization actively sharing CTI?
- In how many communities is your organization a member that are suitable for CTI sharing?

III. Incentives for CTI Sharing (Open Questions)

- Why does your organization share / not share CTI?
- What impediments did you encounter when sharing / trying to share CTI?
- What incentives increase your organization's motivation to start or increase CTI sharing?
- How should incentives be designed to motivate your organization to share CTI?
- How should the platform architecture for CTI sharing incentives be chosen?

IV. Incentives for CTI Sharing (Specific Questions)
The following questions were asked if they had not already been answered in the previous group of questions to ensure each participant addressed every question.

- How do financial payments influence your organization's motivation for CTI sharing?
- How does a marketing label influence your organization's motivation for CTI sharing?
- How does community sharing influence your organization's motivation for CTI sharing?
- How do anonymity and pseudonymity inside the community influence your organization's motivation for CTI sharing?
- How does a reputation system influence your organization's motivation for CTI sharing?
- How does a price suggestion for CTI records influence your organization's motivation for CTI sharing?
- How does a centralized or distributed platform influence your organization's motivation for CTI sharing?
- How does a transaction fee influence your organization's motivation for CTI sharing?
- How do a fee and external validators for the quality validation of offered CTI influence your organization's motivation for CTI sharing?

V. Evaluation
Following an introduction to the prototype, participants were given the opportunity for hands-on interaction. Subsequently, they were asked the following questions.

- What are your thoughts on the practicality of the community sharing, and what modifications would you recommend?
- What are your thoughts on the practicality of the proposed reputation system, and what modifications would you recommend?
- What are your thoughts on the practicality of the proposed price suggestion, and what modifications would you recommend?
- What are your thoughts on the practicality of the proposed financial incentives, and what modifications would you recommend?
- What are your thoughts on the practicality of the proposed marketing label, and what modifications would you recommend?
- What are your expectations or concerns regarding the platform's ability to handle the expected transaction volumes?
- Are there any additional features, incentives, or process changes you would suggest to further encourage active CTI sharing?

Appendix B Community properties

All community properties are listed as follows.

I. Reputation System

- **Evaluation quantity:** What percentage of purchases must be evaluated.
- **Evaluation period:** How much time a member has for the pending evaluations.

II. Price Suggestion

- **CTI Record Selection:** How many times the CTI record must be purchased before it is included in the price suggestion. This ensures that unsuitable records are filtered out and do not bias the price suggestion.

III. Marketing Label

- **Community Name:** Name of the community that will be displayed on the marketing label.
- **Requirements:** Which conditions must be met for issuing the marketing label.
- **Validity Period:** Validity period of an issued marketing label.
- **Deposit Period:** Period during which a newly issued marketing label token can be deposited in the mixer smart contract.
- **Mixer Size:** Minimum number of marketing label tokens stored in the mixer smart contract before withdrawal is permitted. A sufficiently large number of deposited tokens is necessary to ensure pseudonymity.

Appendix C Formal definition of price suggestion

The following explains how the price suggestion is calculated based on the identified criteria and uses an example to illustrate this. The size criterion for a CTI record is calculated from the sum of the number of STIX domain objects $\#SDO$, the number of STIX relationship objects $\#SRO$, and the number of represented attack phases $\#AP$. It should be noted that elements of the same type are also taken into account multiple times; for example, two or more SDO attack patterns in one record would be included in the calculation according to their quantity.

$$Size = \#SDO + \#SRO + \#AP \tag{1}$$

To examine two different CTI records A and B for the difference in the amount of information they contain, the delta $Size_{\Delta}$ is formed by the difference in the size of $Size_A$ and $Size_B$.

$$Size_{\Delta} = |Size_A - Size_B| \tag{2}$$

SDOs, SROs, and attack phases are considered to calculate the difference in content. For the content difference $C_{\Delta}SDO$ between A and B, the number of SDO matches found $\#Match_{AB}SDO$ between the two CTI records is subtracted from the total number of SDO elements. It is important to note that the total number of SDOs from the record with the smaller quantity of SDOs is used in the calculation. If the larger record were used, the difference in size would also be considered and thus evaluated twice, as this was already considered in the previous step.

$$C_{\Delta}SDO = min(\#SDO_A, \#SDO_B) - \#Match_{AB}SDO \tag{3}$$

$$C_{\Delta}SRO = min(\#SRO_A, \#SRO_B) - \#Match_{AB}SRO \tag{4}$$

$$C_{\Delta}AP = min(\#AP_A, \#AP_B) - \#Match_{AB}AP \tag{5}$$

Figure 4 shows an example to illustrate the content comparison. CTI record A has four SDOs, whereas record B only has three, which results in a difference in $Size_{\Delta} = 1$. However, both have one attack pattern and one course of action, which means there are two content matches. Subtracting the two matches from the smaller record B results in a difference

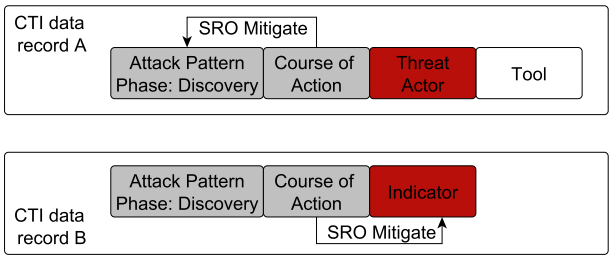

Fig. 4 Example of calculating the similarity of two CTI records A and B for the price suggestion

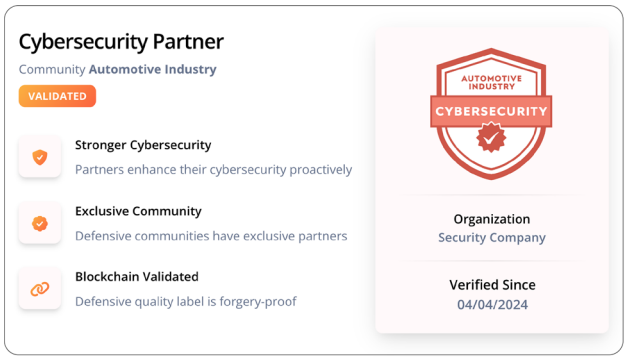

Fig. 5 Validation page of the marketing label

in the content of the SDO elements of $C_{\Delta}SDO = 3-2 = 1$ according to formula (3).

The content difference of the SROs $C_{\Delta}SRO$ and the attack phases $C_{\Delta}AP$ are calculated according to the formulas (4) and (5). In the example in Figure 4, CTI records A and B both have a SRO "mitigate" but with different content, as different SDO elements are involved with Attack Pattern and Indicator. This results in no match and a deviation of $C_{\Delta}SRO = 1 - 0 = 1$. Both records also have an attack phase "Discovery" assigned to the attack pattern, which means that both CTI records describe the same phase of an attack, resulting in $C_{\Delta}AP = 1 - 1 = 0$.

After the deviations $C_{\Delta}SDO$ and $C_{\Delta}SRO$ have been calculated, they can be added to a CTI record structure deviation $C_{\Delta}Struct$.

$$C_{\Delta}Struct = C_{\Delta}SDO + C_{\Delta}SRO \tag{6}$$

Following the example results in $C_{\Delta}Struct = 1+1 = 2$. In contrast, the attack phases do not define a structure but are a special case of the content analysis of a CTI record. As requested by the interview participants, the difference between the provided attack phases is therefore included as a third factor in the final calculation of the total deviation $Total_{\Delta}$ in addition to the size and the content structure. All three factors have a weighting factor w in order to make their influence on the calculation of the total deviation adjustable. Nevertheless, whether certain factors are more important than others, and if so, which ones, has not yet been investigated, which is why each weighting factor has a default value of $w = 1$.

$$Total_{\Delta} = w_s * Size_{\Delta} + w_{st} * C_{\Delta}Struct + w_{ap} * C_{\Delta}AP \tag{7}$$

The final total deviation for the example is:
$Total_{\Delta} = 1 * 1 + 1 * 2 + 1 * 0 = 3$

Appendix D Validation of the marketing label

We outline an exemplary validation page of the marketing label.

Appendix E Prototype process diagrams

We describe the process of member registration and token deposit in Figure 6. We outline the process of uploading a new CTI record in Figure 7 and the purchase of a CTI record in Figure 8. Additionally, we display the process of the marketing label issuance in Figure 9 and the marketing label verification in Figure 10.

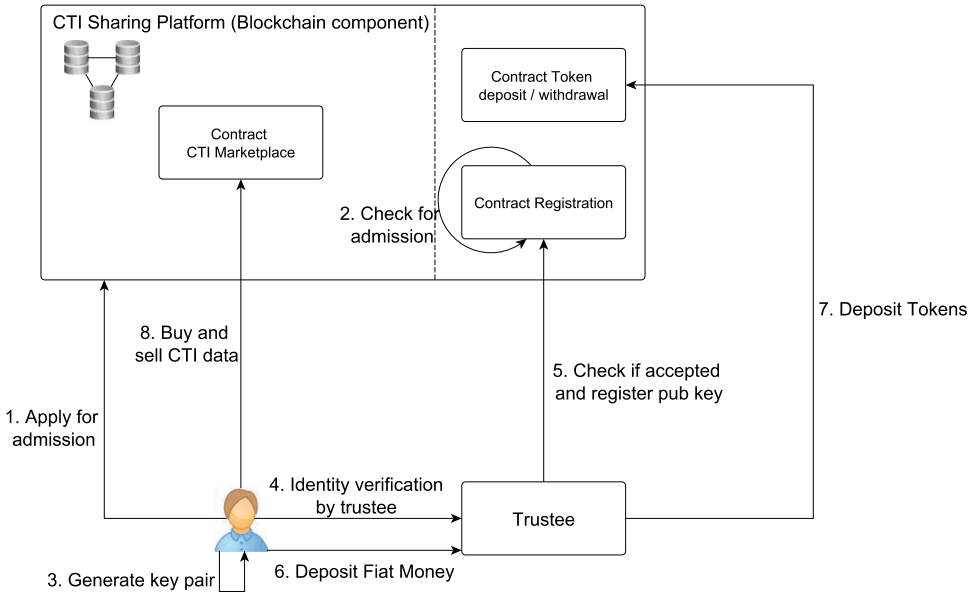

Fig. 6 Existing member registration and deposit of tokens on the sharing platform. The Trustee is only able to access and interact with the token deposit/withdrawal and registration contracts. The Trustee does not have access to the CTI Marketplace contract and therefore has no insight into member sharing behavior

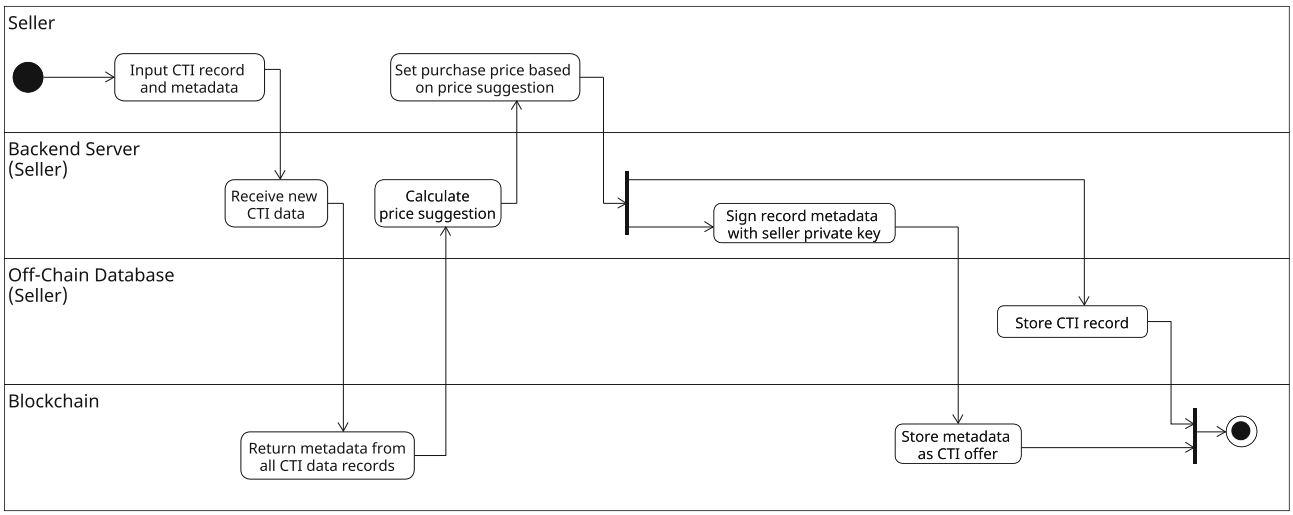

Fig. 7 Upload of a new CTI record for sale in the sharing platform

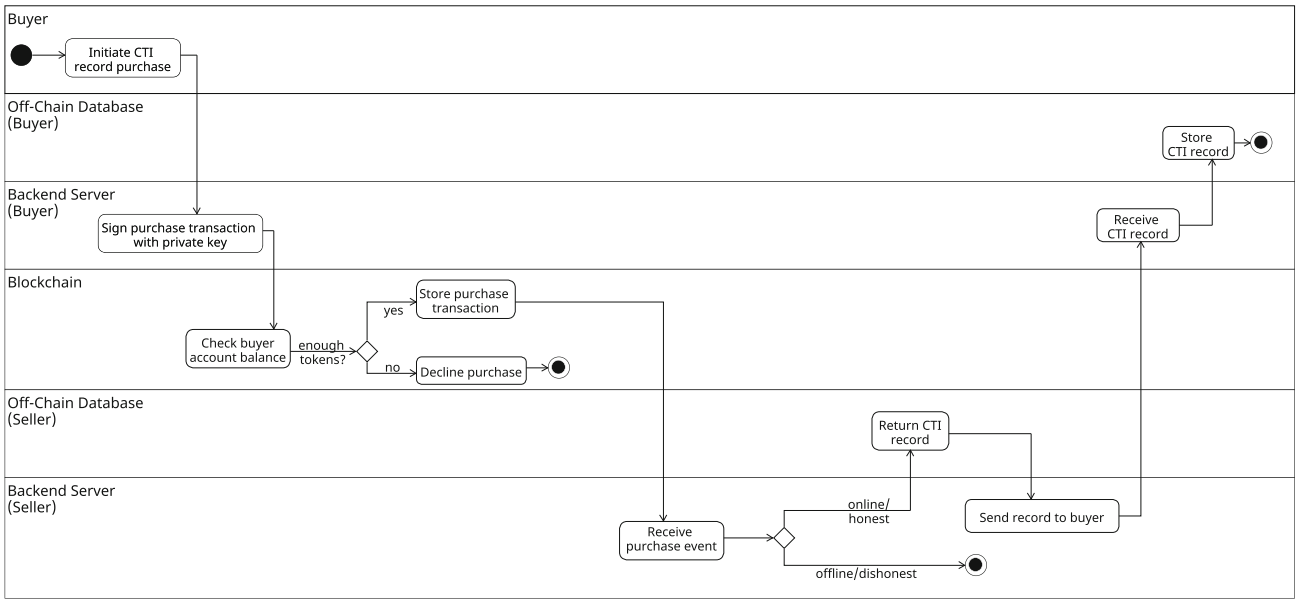

Fig. 8 Purchase of a CTI record in the sharing platform

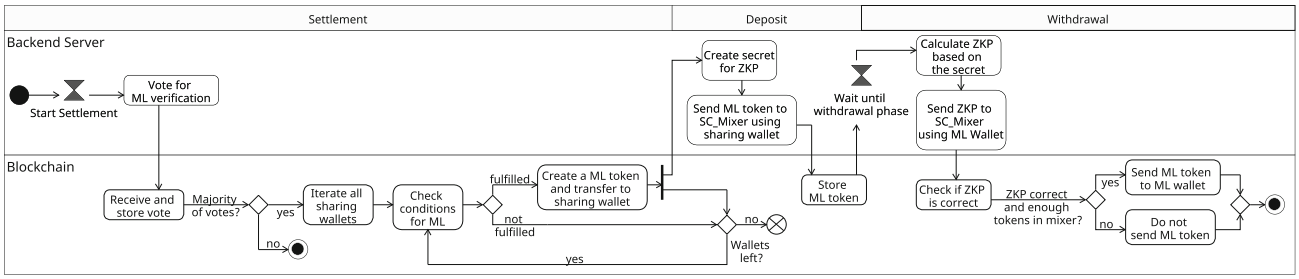

Fig. 9 Issuance of the marketing label (ML) for a new validity period

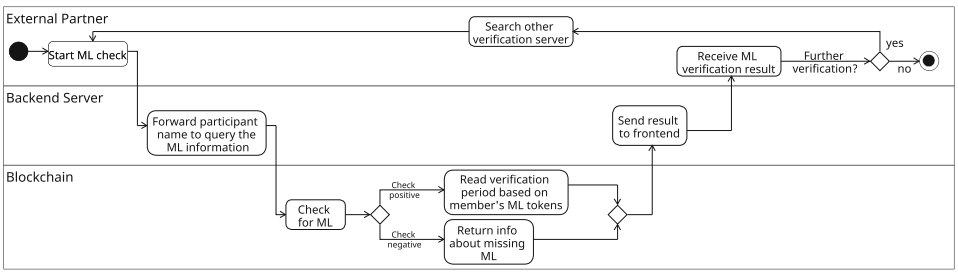

Fig. 10 Verification of the marketing label by an external partner

Author Contributions All authors contributed to the study conception and design. Material preparation, data collection, analysis, and first draft were performed by T.R. and J.G.. All authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding Open Access funding enabled and organized by Projekt DEAL. This research is part of the DEFENSIVE project, funded by the German Federal Ministry of Research, Technology, and Space (16KIS1568K).

Data Availability The full source code of the developed CTI-sharing platform with incentives is published on GitHub: https://github.com/techplus2024/Platform

Declarations

Conflicts of Interest The authors declare no competing interests.

AI Acknowledgement During the preparation of this work, the authors used DeepL, Grammarly, and ChatGPT (Version 4o) in order to improve readability and language. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

Competing interests One of the authors, Günther Pernul, is a member of the editorial board.

References

1. Microsoft Corporation. Microsoft digital defense report 2024: The foundations and new frontiers of cybersecurity (2024). https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024. Accessed: 07/06/25
2. Deloitte Global. The promise of cyber: Global future of cyber survey (4th edition) (2024). https://www.deloitte.com/global/en/services/consulting-risk/research/global-future-of-cyber.html. Accessed: 07/06/25
3. Statista. Estimated cost of cybercrime worldwide 2018-2029 (2025). https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide. Accessed: 11/14/25
4. Hausken, K.: Security investment, hacking, and information sharing between firms and between hackers. Games **8**(2), 23 (2017)
5. Wagner, T.D., Mahbub, K., Palomar, E., Abdallah, A.E.: Cyber threat intelligence sharing: Survey and research directions. Computers & Security **87**, 101589 (2019)
6. Tounsi, W., Rais, H.: A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security **72**, 212 (2018)
7. Bouwman, X., Griffioen, H., Egbers, J., Doerr, C., Klievink, B., Van Eeten, M.: A different cup of ti the added value of commercial threat intelligence, In: 29th USENIX security symposium (USENIX security 20), pp. 433–450 (2020)
8. Liao, X., Yuan, K., Wang, X., Li, Z., Xing, L., Beyah, R.: Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence, In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, pp. 755–766 (2016)
9. Jin, B., Kim, E., Lee, H., Bertino, E., Kim, D., Kim, H.: Sharing cyber threat intelligence: Does it really help?, In: 31st Annual Network and Distributed System Security Symposium, NDSS 2024, San Diego, California, USA, February 26 - March 1, 2024 The Internet Society, (2024)
10. Alaeifar, P., Pal, S., Jadidi, Z., Hussain, M., Foo, E.: Current approaches and future directions for cyber threat intelligence sharing: A survey. Journal of Information Security and Applications **83**, 103786 (2024)
11. Geras, T., Schreck, T.: Sharing communities: The good, the bad, and the ugly, In: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, pp. 2755–2769 (2023)
12. Menges, F., Putz, B., Pernul, G.: Dealer: decentralized incentives for threat intelligence reporting and exchange. Int. J. Inf. Secur. **20**(5), 741 (2021)
13. Deci, E.L., Ryan, R.M.: Intrinsic motivation and self-determination in human behavior. Springer Science & Business Media, Berlin (2013)
14. DiMaggio, P.J., Powell, W.W., et al.: The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. Am. Sociol. Rev. **48**(2), 147 (1983)
15. PAMELA, S.T.: The institutionalization of institutional theory, Studying organization: Theory and method p. 169 (1999)
16. Hillman, A.J., Withers, M.C., Collins, B.J.: Resource dependence theory: A review. J. Manag. **35**(6), 1404 (2009)
17. Pfeffer, J., Salancik, G.: In: Organizational behavior 2 Routledge, pp. 355–370, (2015)
18. Reittinger, T., Pernul, G.: A taxonomy of positive incentives to motivate cybersecurity behaviors, In: Proceedings of the 58th HI International Conference on System Sciences (HICSS-58) (2025)
19. Reittinger, T., Glas, M., Aminzada, S., Pernul, G.: Employee motivation in organizational cybersecurity: Matching theory and reality, In: International Symposium on Human Aspects of Information Security and Assurance, Springer, pp. 3–16 (2024)
20. Reittinger, T., Glas, M., Aminzada, S., Pernul, G.: Motivational factors in cybersecurity: linking theory to organizational practice, Information & Computer Security (2025)
21. Kamenica, E.: Behavioral economics and psychology of incentives. Annu. Rev. Econ. **4**(1), 427 (2012)
22. Bryson, A., Freeman, R., Lucifora, C., Pellizzari, M., Perotin, V., et al.: Paying for performance: incentive pay schemes and employees' financial participation. CEP discussion paper **1112**, 52–75 (2012)
23. Malaga, R.A.: Web-based reputation management systems: Problems and suggested solutions. Electron. Commer. Res. **1**, 403 (2001)
24. Tadelis, S.: Reputation and feedback systems in online platform markets. Annual Review of Economics **8**, 321 (2016)
25. Jahn, G., Schramm, M., Spiller, A.: The reliability of certification: Quality labels as a consumer policy tool. J. Consum. Policy **28**, 53 (2005)
26. de Melo e Silva, A., Costa Gondim, J.J., de Oliveira Albuquerque, R., García Villalba, L.J.: A methodology to evaluate standards and

platforms within cyber threat intelligence. Future Internet **12**(6), 108 (2020). https://doi.org/10.3390/fi12060108
27. OASIS. Oasis stix documentation (2024). https://oasis-open.github.io/cti-documentation/stix/intro. Accessed: 07/06/25
28. Corporation, M.: Mitre ATT&CK website (2025). https://attack.mitre.org/. Accessed: 07/06/25
29. Sunyaev, A.: In: Internet Computing, vol. 2, ed. by A. Sunyaev Springer International Publishing, Cham, (2020), pp. 265–29. https://doi.org/10.1007/978-3-030-34957-8_9
30. El Ioini, N., Pahl, C.: A review of distributed ledger technologies, In: On the Move to Meaningful Internet Systems. OTM 2018 Conferences, ed. by H. Panetto, C. Debruyne, H.A. Proper, C.A. Ardagna, D. Roman, R. Meersman Springer International Publishing, Cham, pp. 277–288 (2018)
31. De Angelis, S., Zanfino, G., Aniello, L., Lombardi, F., Sassone, V.: Blockchain and cybersecurity: a taxonomic approach, In: Workshop. EU Blockchain Observatory (2019)
32. Willis, G.B.: Cognitive interviewing: A tool for improving questionnaire design, sage publications, (2004)
33. Deterding, N.M., Waters, M.C.: Flexible coding of in-depth interviews: A twenty-first-century approach. Sociological methods & research **50**(2), 708 (2021)
34. G.R. Gibbs, Thematic coding and categorizing, Analyzing qualitative data **703**(38-56) (2007)
35. Caine, K.: Local standards for sample size at chi, In: Proceedings of the 2016 CHI conference on human factors in computing systems (2016), pp. 981–992
36. Nweke, L.O., Wolthusen, S.: Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection, In: 2020 12th International Conference on Cyber Conflict (CyCon), vol. 1300 (IEEE, 2020), vol. 1300, pp. 63–78
37. DIHK. Industrie- und handelskammern (german trade associations). https://www.dihk.de/de/ueber-uns/die-ihk-organisation/industrie-und-handelskammern. Accessed: 07/06/25
38. European Union. General data protection regulation (gdpr) (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434. Accessed: 07/06/25
39. Netwrix. Netwrix cloud data security report (2019). https://www.netwrix.com/2019cloudsecurityreport.html. Accessed: 07/06/25
40. Capgemini. Capgemini cloud sovereignty: The road ahead (2022). https://www.capgemini.com/insights/research-library/cloud-sovereignty/. Accessed: 07/06/25
41. Federal Bureau of Investigation. 2023 cryptocurrency fraud report released (2024). https://www.fbi.gov/news/stories/2023-cryptocurrency-fraud-report-released. Accessed: 07/06/25
42. The Linux Foundation. Hyperledger besu (2025). https://github.com/hyperledger/besu. Accessed: 07/06/25
43. Couchbase, Inc. Couchbase (2025). https://github.com/couchbase. Accessed: 07/06/25
44. OpenJS Foundation. Node.js (2025). https://github.com/nodejs. Accessed: 07/06/25
45. Laravel Holdings Inc. Laravel (2025). https://github.com/laravel/framework. Accessed: 07/06/25
46. European Union. Regulation (eu) 2024/1624 of the european parliament and of the council of 31 may 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (2024). https://eur-lex.europa.eu/eli/reg/2024/1624/oj/eng. Accessed: 07/06/25
47. Schlette, D., Böhm, F., Caselli, M., Pernul, G.: Measuring and visualizing cyber threat intelligence quality. Int. J. Inf. Secur. **20**, 21 (2021)
48. Rinberg, R., Agarwal, N.: Privacy when everyone is watching: An sok on anonymity on the blockchain, Cryptology ePrint Archive (2022)
49. Petkus, M.: Why and how zk-snark works, arXiv preprint arXiv:1906.07221 (2019)
50. C. Fan, C. Lin, H. Khazaei, P. Musilek, Performance analysis of hyperledger besu in private blockchain, In: 2022 IEEE international conference on decentralized applications and infrastructures (DAPPS) (IEEE, 2022), pp. 64–73
51. Mühle, A., Grüner, A., Gayvoronskaya, T., Meinel, C.: A survey on essential components of a self-sovereign identity. Computer Science Review **30**, 80 (2018)
52. Riesco, R., Larriva-Novo, X., Villagrá, V.A.: Cybersecurity threat intelligence knowledge exchange based on blockchain: Proposal of a new incentive model based on blockchain and smart contracts to foster the cyber threat and risk intelligence exchange of information. Telecommun. Syst. **73**(2), 259 (2020)
53. Gong, S., Lee, C.: Blocis: blockchain-based cyber threat intelligence sharing framework for sybil-resistance. Electronics **9**(3), 521 (2020)
54. K. Nguyen, S. Pal, Z. Jadidi, A. Dorri, R. Jurdak, A blockchain-enabled incentivised framework for cyber threat intelligence sharing in ics, In: 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops) (IEEE, 2022), pp. 261–266
55. Alexopoulos, N., Vasilomanolakis, E., Roux, S.L., Rowe, S., Mühlhäuser, M.: Trident: towards a decentralized threat indicator marketplace, In: Proceedings of the 35th Annual ACM Symposium on Applied Computing (2020), pp. 332–341
56. Wagner, C., Dulaunoy, A., Wagener, G., Iklody, A.: MISP: the design and implementation of a collaborative threat intelligence sharing platform, In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, WISCS 2016, Vienna, Austria, October 24 - 28, 2016 (ACM, 2016), pp. 49–56
57. Baumer, T., Reittinger, T., Kern, S., Pernul, G.: Digital nudges for access reviews: Guiding deciders to revoke excessive authorizations, In: Twentieth Symposium on Usable Privacy and Security (SOUPS 2024) (2024), pp. 239–258
58. Fischer, D., Sauerwein, C., Werchan, M., Stelzer, D.: An exploratory study on the use of threat intelligence sharing platforms in germany, austria and switzerland, In: Proceedings of the 18th International Conference on Availability, Reliability and Security, ARES 2023, Benevento, Italy, 29 August 2023- 1 September 2023 (ACM, 2023), pp. 30:1–30:7
59. CIRCL. MISP documentation (2024). https://www.circl.lu/doc/misp/. Accessed: 07/06/25