The American Journal of Engineering and Technology
ISSN 2689-0984 Volume 07 - 2025

Optimizing Threat Intelligence Sharing Across Multiple Security Platforms

[1]John Komarthi
[1]Independent Researcher, USA

Received: 11th Sep 2025 | Received Revised Version: 19th Oct 2025 | Accepted: 21th Nov 2025 | Published: 30th Nov 2025

Volume 07 Issue 11 2025 | Crossref DOI: 10.37547/tajet/v7i11-303

Abstract

Sharing of Cyber Threat Intelligence (CTI) has turned out to be an indispensable pillar of the modern cybersecurity landscape, it is enabling organizations to defend against the evolving threats. In this white paper, we will discuss the strategies to optimize the sharing of threat intelligence across multiple security platforms in the enterprise and community context. We will observe the current standards and practices, like Structured Threat Information eXpression (STIX) and trusted Automated Exchange of Indicator Information (TAXII) protocols, and also examine the role of these standards in integrating the Threat Intelligence Platforms (TIPs) with Security Information and Event Management (SIEM) systems. We will observe the impact of threat intelligence exchange through real-world case studies and how the cybersecurity attacks are mitigated, along with the challenges that are encountered (e.g., technical integration gaps, data overload, trust and privacy issues). We will also discuss the limitations in the current approaches, which include the inconsistent adoption of the standards, there is a prevalence of indicators with low context, and siloed systems that impede the information flow. The landscape of the emerging solutions, the future directions will be explored, machine learning prioritized to reduce the false positives, a decentralized sharing architecture by leveraging blockchain and federated learning for privacy, and also trust frameworks to incentivize collaboration. Through addressing the present challenges and leveraging the advanced technologies, organizations will be able to create a unified and effective threat intelligence sharing ecosystem that will strengthen the collective cyber defense.

Keywords: Cyber Threat Intelligence; Threat Information Sharing; STIX/TAXII (Structured Threat Information eXpression/Trusted Automated eXchange of Intelligence Information); Threat Intelligence Platform (TIP); Security Information and Event Management (SIEM); Machine Learning; Blockchain; Federated Learning; Information Sharing and Analysis Center (ISAC); Cybersecurity Collaboration.

Cite This Article: Komarthi, J. (2025). Optimizing threat intelligence sharing across multiple security platforms. The American Journal of Engineering and Technology, 7(11), 165–176. https://doi.org/10.37547/tajet/v7i11-303 .

1. Introduction

In the current threat landscape, cyberattacks are rising in numbers and in their sophistication. There has been an explosive growth in the incidents, for example, ransomware incidents have increased by 435 percent in just one year [1]. There have been high-profile breaches and exploits, such as the supply chain attack on SolarWinds, which caused an estimated 100 billion dollars in damages, proving that no organization is immune to attacks [2]. Smaller and independent organizations are struggling to keep up the pace with the fast-evolving tactics, procedures, and techniques (TTPs) of the attacked. Cyber Threat Intelligence has become a cornerstone of proactive defense. CTI consists of evidence-based knowledge of the adversarial threat indicators, context, TTPs, and remediation advice. This information, when shared and applied, enables earlier detection, mitigation, and prevention of the attacks. The 2022 SANS survey has indicated that almost 60 percent of the organizations are already using CTI in their security operations, and almost half of these maintain dedicated CTI analyst teams [3]. This highlights the recognition that the timely intelligence exchange can dramatically change the organization's risk posture. Optimizing threat intelligence and sharing across the security platforms in both small organizations and large enterprises is complex and challenging. Many enterprises deploy a mix of security tools that include firewalls, endpoint detection and response, intrusion prevention systems, SIEMS, and others, often from multiple vendors, each tool produces and consumes the threat data in their own formats. Integration of these heterogeneous systems into a cohesive intelligence-sharing workflow is important. The standardized schemas have been developed to facilitate interoperability, the OASIS STIX for the structured threat data and the TAXII transport mechanism for exchanging the CTI over HTTPS are now the default standards [4]. STIX has been designed to capture a wide range of threat information, which is in machine-readable format, right from simple indicators such as malicious IPs to complex adversary group profiles. TAXII enables organizations to share STIX-formatted data automatically in a secure manner. These standards are used in the modern Threat Intelligence Platforms, and allow separate tools to speak a common language of threat indicators. Even with all these advancements, there are significant gaps and limitations that affect intelligence sharing. Many organizations have reported that crucial intelligence, such as adversary TTPs, attack campaigns, is not being disseminated effectively in practice. The intelligence exchanges often depend on raw Indicators of Compromise (IoCs) such as hashes, IP addresses, URLs, which, without context, lead to alert fatigue and missing strategic insights. Not every security product supports STIX/TAXII or integration with TIPs, especially with the legacy systems, which may require custom connectors and manual processes for ingesting shared threat feeds. The organizational and human factors complicate the matter further; companies have to trust the reliability of the shared intelligence and handle the concerns over privacy, liability, and proprietary data while exchanging the data with external partners. Eventually, building an optimized threat intel sharing ecosystem needs more than just technology adoption, this requires addressing the policy, data management, and trust challenges as well [5].

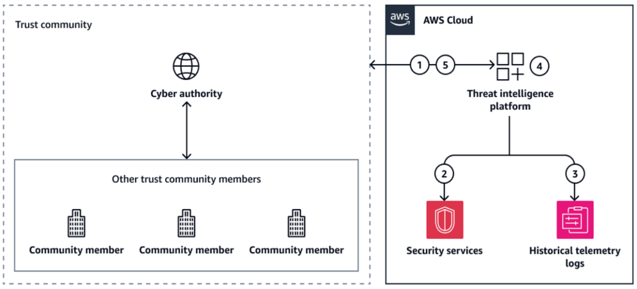

Figure 1: Generalized architecture for threat intelligence sharing.

The picture above depicts a general threat intelligence platform of an organization and the environment that exchanges the CTI with peer community members and global authorities. In the above model, the platform ingests the threat feeds from external sources such as national CERTs, commercial providers, or industry ISACs and then distributes relevant indicators to the internal security controls, like intrusion prevention systems, to enable proactive defense. The platform also collects internal telemetry (incident reports, logs, alerts), curates the latest intelligence from this collected data (e.g., new attack indicators or tactics), and then shares the information back to the community. This creates a continuous feedback loop where each participant benefits and contributes to the collective knowledge base. This enables faster detection of any emerging threats and enables a more coordinated response across the participants of the network of defenders.

2. THREAT INTELLIGENCE LIFECYCLE NTEGRATION

Shared threat intelligence flows through all the phases of the organization's detection and response process, right from the initial collection of the data to the dissemination of the lessons learned. This forms a seamless cycle. Ensuring that the intelligence moves smoothly from the collection to action enables the defenders to react faster. Integrating CTI across the threat intelligence lifecycle with automated workflows and human oversight, the security teams can transform the raw data into actionable insights. This lifecycle encompasses the following key phases:

2.1 Collection and Ingestion:

The first phase is to gather threat intelligence from internal and external sources, which includes internal telemetry such as endpoint logs, network sensors, intrusion detection systems, and also endpoint external feeds. Sources range from industry communities like ISACs/ISAOs and government CERT alerts, commercial threat intel providers, and open-source intelligence (OSINT). Through the data aggregated from internal sensors and external partners, the organization builds a comprehensive view of the emerging threats. Many enterprises use automated ingestion pipelines to pull in indicators of compromise (IOC's), adversary tactics, and other threat data in real time. Continuous inflow of intelligence is ensured to keep the detection capabilities up-to-date, focusing on the intel relevant to critical assets and likely attackers, ensuring that the incoming data aligns with the overall defense strategy.

2.2 Normalization and Enrichment

Raw threat data comes in multiple formats and quality, the next step after data collection is to normalize and enrich the data. Normalization is converting and consolidating the indicators and observations into a standard format. Organizations adopt formats such as STIX for threat data and exchange protocols like TAXII to codify IOCs and TTPs in a machine-readable way. Enrichment adds the contextual metadata, which gives meaning to the raw indicators, by attaching the context to each indicator.

2.3 Analysis and correlation:

After the threat data is normalized and enriched, the data is moved to analyze and correlate it with the organization's internal telemetry. This is the phase where the raw data is turned into intelligence. Correlation involves linking the indicators and observations across different data sets, for instance, matching a malicious IP address against the internal log data if it appeared in any firewall or DNS logs. Present-day correlation engines and AI models can rapidly sift through the logs and alerts to identify the matches and anomalies that need attention. The analysis process has risk scoring and context evaluation to prioritize the threats, not every indicator is relevant, so the analysts assess the factors like relevance to the organization’s industry, criticality of the affected systems, or confidence level of the intel. Human machine teaming is important here, the automated correlation can handle the scale and speed, but the human analysts validate the findings, investigate complex patterns, and add strategic insight.

2.4 Operationalization:

After analyzing the threat data, the intelligence is moved from the reports into action. This intelligence is integrated across detection, prevention, and response systems. The curated intel feeds into SIEMs, IDS, EDRs, SOAR platforms, case management tools, and firewalls for real-time updates. After the integration, the detection improves as the rules and signatures update with the latest IoCs and TTPs. SOC analysts give instant context and enable faster triage. As a preventive measure, the intel indicators block threats proactively, the firewall drops the malicious traffic, and endpoints quarantine the flagged files. The threat hunters query the internal data for any new IoCs, and the incident response playbooks evolve based on the adversary tactics. Automation reduces the dwell time by triggering instant responses, such as blocking the IPs or isolating hosts. The operational use of CTI turns intelligence into immediate defense actions and continuously tunes the protection to emerging threats.

2.5 Feedback and Re-sharing:

Any mature program closes the loop through analyzing the outcomes and sharing insights. The teams review the incident data to assess the indicator accuracy, refine the rules, and prioritize new sources by providing feedback on detection models and making the CTI self-improving. Validated intel and findings are shared with ISACs, CERTs, and trusted partners, which reinforces the collective defense model. The dissemination is tailored to the roles; analysts receive the technical IoCs, and the executives get strategic summaries that are aligned with the business risk. The two-way flow ensures that the organizations consume and contribute the intelligence, thus raising overall community resilience.

2.6 Seamless workflows, human-machine teaming, and strategic alignment:

The success of the threat intel sharing relies on the automated, interconnected workflows where the collection, analysis, and dissemination flow without any manual delays. The machine handles the data at scale and finds the correlation, manual analysts apply judgment and contextual insight. Through tying the CTI goals to organizational priorities and critical assets, threat intel becomes a force driving proactive defense and risk management. Integrated CTI transforms organizations from reactive to resilient, providing situational awareness, faster response, and strategic decisions that strengthen both the internal and collective cyber defense posture.

3. REAL-WORLD IMPACT

Sharing threat intelligence effectively improves the cyber defense outcomes dramatically and enables the organizations to anticipate and be prepared to face the attacks that would have otherwise propagated unabated. When a new threat is detected by an entity that is part of the community can swiftly share the indicators and patterns, and others in the community can protect themselves from the shared intelligence. This turns a potentially severe threat incident into a non-event. The early warning system has proven its value in real-world scenarios, for example, analysis of the major ransomware incidents has shown that the malware families often reuse similar tactics [6]. Through sharing information about the initial attack, defenders somewhere else can be prepared for copycat attacks. A study has noted that the “Locky” and “WannaCry” ransomware campaigns, which are a year apart, have employed similar delivery vectors through phishing emails with malicious attachments, and they even leveraged the same anonymization network (Tor) for the command and controls [7]. If the threat indicators and TTPs from Locky were circulated in the community or shared through Threat Intelligence Platforms on time, other organizations could have fortified their networks through proper email filters, Tor network blocking etc., and potentially could have mitigated WannaCry’s impact. This shows how timely sharing of CTI can preemptively shield other organizations from a related but later attack.

Organizations are tapping into numerous threat feeds and intelligence sources on a daily basis. Over 10 million STIX-formatted threat objects were shared publicly via open feeds and repositories. This information is as of 2023, and that is an average of 3,300 new indicators published every day [8]. These threat indicators range from malware file hashes, malicious IP/domain addresses, to discovered vulnerabilities and attack signatures. The rapid distribution of actionable intelligence enables the defenders in the organizations to mitigate the vulnerabilities or block the malicious infrastructure in near real-time and sometimes even before the threats can penetrate the system. For instance, a financial institution shares a threat indicator that is related to a phishing domain that is targeting its customers, then other financial institutions can preemptively add that phishing domain to their block lists, thus preventing the threat from spreading further. Multiple industry sectors have formalized this cooperation through Information Sharing and Analysis Centers (ISACs) and alliances [9]. ISAC of the financial services, for example, circulates daily threat indicators and attack briefs to its member banks globally. Cyber Threat Alliance (CTA) is a consortium of cybersecurity vendors that pool their threat intelligence and rapidly propagate the updates to the customers using their products. CTA members have significantly cut the time taken to deploy the countermeasures against new malware outbreaks [10]. A case study with cloud provider DigitalOcean has demonstrated that participating in the intel sharing community and feeding those insights into an automated blocking mechanism has reduced the cases of network abuse by 40 percent and also sped up the incident response times [11].

This has been achieved through leveraging the shared indicators, such as DDoS, intrusion attempts, to proactively filter the traffic and through learning from other providers' experiences to harden their own systems against any novel attack techniques. There was not only a drop in successful attacks but also an increase in customer trust and an overall strong security posture. These examples reinforce that the threat intelligence is more than just data sharing and is a force multiplier for an organization's defense. The combined intelligence of multiple organizations is far greater than the contribution of what a single entity could amass on its own.

Apart from preventing attacks, the shared threat intelligence has a deterrence and resiliency effect. The attackers operate globally, and they often reuse the infrastructure, tactics across the targets [12]. Defenders colluding and sharing the information at speed raises the cost and complexity for the attackers. The attackers can no longer count on a single exploit or using a malware variant for long in multiple places, as the first sighting triggers immunization across the network. At the time of large-scale incidents and fast spreading works or state-sponsored campaigns, the organization's ability to coordinate through real-time intel exchanges can be critical to contain. For example, during the 2022–2023 cyberattacks related to geopolitical conflicts, the government agencies and private sector partners have shared indicators of state-backed phishing and the wiper malware attacks in real time, which enabled the targets in other countries to secure the systems in advance [13]. The real-world impact of optimized threat intelligence sharing is that of a safer digital ecosystem where there is faster detection, coordinated response, and mitigation of attacks at scale. This makes it increasingly difficult for the malicious actors to achieve their objectives without being discovered and thwarted by the united defense community.

4. CASE STUDIES

4.1 Collaborative Intelligence Sharing in Defense of Ukraine's Infrastructure (CDAC Initiative):

During 2022-2023, there has been an escalation in cyber conflict in Eastern Europe, and Ukraine's critical infrastructure was under a barrage of cyberattacks. Cyber Defense Assistance Collaborative (CDAC) has stepped in to bolster Ukraine's cyber defenses by improving the threat intelligence sharing to its critical sectors [14]. CDAC has identified that one of the challenges that the Ukrainian defenders face is dealing with the threat intel that comes from disparate sources. There were large volumes of indicators from international allies and vendors coming in, but they faced difficulty in prioritizing, deduplicating, and parsing the information flood. Starting in early 2023, in response to this, CDAC has convened a partnership that includes a major threat intelligence platform vendor (ThreatQuotient), leading threat intel providers (Recorded Future and Mandiant), and the global Cyber Threat Alliance. In partnership, they have developed a centralized aggregator and distribution platform specifically for Ukraine's threat data. Using this platform, CTI is collected automatically from multiple streams, normalized into a common format using STIX, eliminating any duplicates, and highlighting the relevant alerts for Ukrainian networks. The system then redistributes the curated intelligence out to the critical infrastructure operators and the defense organizations in near real time. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) provides support and expertise to this effort and underscores the importance. According to the CISA officials, the collaborative platform has catalyzed information sharing and brought together the best capabilities of government and the industry in a unified defense of Ukraine's digital ecosystem. There is a broader significance to this case as it demonstrates the solution to intel overload, through a feedback approach. Multiple stakeholders have pooled their data to create an integrated threat picture in a high-risk environment. This system was envisioned for deployment across multiple regions. This showcases how the model can coordinate CTO across nations and organizations through a central hub in crisis situations. This also highlights the value of public-private collaboration, the government agencies have provided the authority and urgency, while the private cybersecurity firms provided the technology and threat expertise, and they both collectively achieved a level of protection that the individual entities could not provide alone.

4.2 Reducing Cloud Abuse via ISP threat Feed Sharing:

The Internet Service Providers (ISPs) and the cloud hosting companies often are faced with large-scale abuse of their infrastructure from threat actors (botnets, scanning, spam etc.,). A notable example is of DigitalOcean, which is a global cloud provider, and it sought to curb malicious activities that are originating from its networks [11]. Through partnering with an anti-abuse threat intelligence service (Abusix) and actively exchanging threat intel with other ISPs, DigitalOcean has significantly improved its incident prevention. The providers were receiving real time real-time feeds of the bad IP addresses, phishing URLs, and other indicators that were observed by the industry authorities and peers. The automated blacklisting and flagging of the traffic associated with the indicators in their own environment. The network abuse cases have dropped by 40 percent after implementing the threat sharing and response loop. Apart from this, the customer satisfaction has improved as there were fewer security incidents affecting the tenants, and the security team could respond faster as they had advance warning from the intel feeds. This case displays how competitively neutral data, such as the IPs of botnet nodes, are shared between the infrastructure providers and can yield mutual benefits. Through collaboratively maintaining the up-to-date threat picture, the entire system becomes more secure. Automation is key, the speed and volume of the events in ISP environments demand that the threat intelligence sharing be tightly integrated with the security controls. DigitalOcean has achieved this through platform APIs and scripting rather the manual intervention. This result shows that other infrastructure operators to participate in threat intel exchanges as part of the threat sharing process, as the positives clearly outweigh the effort when performed correctly.

4.3 Government Industry collaboration: JCDC and Log4j response (2021-2022):

One of the significant examples of public-private partnership for threat intelligence sharing is the response to the critical Log4j (‘Log4Shell’) vulnerability in late 2021 [15]. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) launched a Joint Cyber Defense Collaborative (JCDC) in August 2021. It was an operational coordination body that united both the federal agencies and major tech, security companies. The JCDC moved quickly when the Log4j was on zero day and facilitated real-time intelligence sharing and guidance across sectors. Big tech, finance, and telecom shared the detection methods, techniques, procedures, attacker tactics, and indicators of compromise that are related to the Log4j exploitation. CISA consolidated and redistributed the information as guidance to thousands of organizations. JCDC leveraged a hybrid model, there was a trusted Slack channel and regular briefings for real-time exchange, combined with the structured indicator sharing through CISA’s Automated Indicator Sharing (AIS) system. Through this human context sharing, and machine speed distribution of IoCs to the network defenders is facilitated. Companies such as Microsoft, Cisco, Palo Alto Networks, and Google rapidly consumed the threat feeds and internalized them into their security products and operations. Collaborative sharing via JCDC sped up the response times across the board, according to Cisco’s Chief Security and Trust Officer. JCDC helped them develop and deploy patches for the affected products within 10 days. Log4j vulnerability has highlighted how the coordinated intelligence model led by the government can give real-time actionable guidance on a zero-day crisis and reduce the window of exposure.

4.4 Financial Services FS-ISAC Global Intelligence Sharing (2020-2022):

The financial services sector has an established culture of information sharing through ISAC. The Financial Services ISAC (FS-ISAC) connects the banks, insurers, payment processors, and others in a global intel sharing community [9]. Between 2020 and 2022, the community faced an increasing number of attacks of ransomware attacks, state-sponsored hacking attacks, and supply chain attacks. The member institutions have scaled up their sharing of threat intelligence, contributing indicators and attack patterns through FS-ISAC’s platforms. FS-ISAC has reported that the sharing of cyber intelligence among its members between August 2020 and August 2021 has increased by 60 percent. FS-ISAC has a secure member portal and Threat Intelligence Exchange (IntelEx) platforms where institutions can post and consume alerts. Intelligence is shared via both machine-to-machine feeds and human-readable formats. It provides STIX/TAXII feeds and MISP repositories for automated indicator sharing. These feeds have been integrated into banks' SOC tools, so newly shared IoCs are automatically ingested into SIEMs and intrusion detection systems. FS-ISAC also runs regular threat briefing calls and trust groups to facilitate peer-to-peer exchange beyond automated feeds. Banco Falabella in Chile credits the cross-border threat intel for helping thwart cyberattacks through monitoring reports of attacks on banks in Argentina and Brazil shared through FS-ISAC. Falabella’s team anticipated a similar attack vector and strengthened its defenses in advance.

4.5 *Healthcare Sector: H-ISAC and Ransomware Threat Sharing (2021-2023)*

The healthcare and public health sector is a prime target for cyber adversaries and ransomware gangs, as hospitals hold sensitive patient data, making them susceptible to extortion [16]. There was a 42 percent increase in ransomware attacks in 2022 alone, compared to the previous year. Health-ISAC shares threat intelligence to strengthen the sector's resilience and protect patient safety. H-ISAC provides a trusted forum and technical infrastructure for real-time cyber intel sharing. The sharing model includes a secure portal where the members post intel, alerts on incidents, vulnerabilities, and threat actor activities targeting healthcare. By 2022, H-ISAC was reaching over eight thousand healthcare security professionals with timely threat indicators, reports, and best practices. The community leverages the structured formats and automated indicator threat sharing tool to facilitate rapid exchange of IoCs through member organizations. Situational awareness and incident response have been improved across the sector through enhanced intelligence sharing. With an increase in ransomware attacks, H-ISAC's alerts have enabled many hospitals to proactively implement safeguards before an attack hits. When faced with a wave of ransomware and nation-state threats, the healthcare sector's intensified CTI sharing has markedly improved readiness, and by extension, ensured greater patient safety and continuity of care.

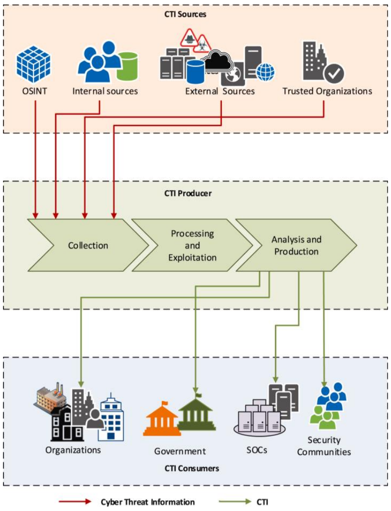

Figure 2: A conceptual overview of a CTI sharing platform model

5. LIMITATIONS

Sharing of threat intelligence according to the current approaches faces significant limitations, which will hamper their effectiveness. Data overload and noise are one major issue, and with thousands of IoCs being shared continuously, the security teams will be inundated with alerts, of which many may not be relevant to the environment and might be low-quality indicators [17]. Shared feeds can overwhelm the Security Operations Center (SOC) analysts with false positives and irrelevant information if not carefully prioritized, and divert attention from true threats. The quality and context problem where many shared IoCs lack the contextual information, such as how the indicators are being observed, recommended response actions, or associated threat actor tactics [18]. IP addresses or hashes on their own are often used limitedly without knowing it's part in the ransomware campaign, a minor malware, or an espionage threat, but even today, much of the CTO remains at the basic level. There is a wide gap between the simple indicators that are commonly shared and the high-level intelligence analysts actually need (TTPs and attack patterns). This is a limitation of the current sharing practices.

Data and tool integration is another limitation; not all the security platforms communicate in the same language, even though STIX/TAXII do provide a common format, many legacy systems do not support it [19]. Many organizations find that their intrusion detection systems, firewalls, or SIEM solutions lack native connectors for STIX and TAXII feeds, thus they are left with no other option but to build custom pipelines or use middleware to translate and import the threat data. The usage of middleware or custom pipelines can introduce delays and errors, or may lead to partial adoption where only selected intel sources are integrated. Data schemas that are incompatible and formatting the inconsistencies across the feeds also pose challenges, for example, a feed may use slightly different indicator definitions and cause confusion when correlating the information from multiple sources [20]. The efforts put into sharing the intelligence can be undermined by the fragmentation of security tooling and the data standards.

Legal constraints and trust form another serious limitation; effective sharing requires a high level of trust between the participants, so that the intelligence is accurate and that it will be used responsibly [21]. When it comes to practice, many organizations are hesitant to share the detailed incident data because of concerns of exposing proprietary information or violating any privacy regulations. For instance, the threat intel derived from the internal logs may include personal data such as email addresses, IP addresses tied to individuals, etc. This raises compliance issues under laws such as GDPR [22]. If proper anonymization and safe harbor frameworks are not followed, companies fear of liability that comes from sharing such data. There can be trust deficits even within established sharing groups, smaller organizations may doubt the quality of intelligence from others, and there may be reluctance to act on the data from unproven sources [23]. It is found that among dozens of CTI sharing platforms, the majority lacked a transparent trust and reputation mechanism, which means the consumers of the intel have no means to judge the reliability [24]. Also, newer members struggle to gain trust in these networks, the absence of robust trust frameworks limits the depth of the information that is shared, as organizations may only share low-sensitive indicators and hold back on valuable insights, and this can slow the collective responses.

Resource and skill limitations especially affect smaller entities, consuming and operationalizing threat intelligence needs skilled analysts and automated tooling [25]. Many organizations do not have dedicated CTI teams to process the incoming intel continuously. Smaller organizations also may lack the infrastructure needed to rapidly deploy the threat updates to all their security controls. This leads to the creation of an uneven playing field, where the larger organizations fully benefit from sharing, while others struggle to keep up with them. Current CTI sharing is limited by the volume overload, integration gaps, variable data quality, disparities in resources, and trust & privacy concerns. These limitations have to be addressed to unlock the full potential of the sharing of CTI across multiple platforms.

6. FUTURE DIRECTIONS:

To achieve a truly optimized threat intelligence sharing ecosystem needs evolution on multiple fronts. Recent research and industry initiatives are pointing the way ahead.

6.1 Enhanced Standardization and Interoperability:

Efforts are being made to universally adopt standards such as STIX/TAXII and to reduce the integration friction [19]. In future iterations, STIX is expected to improve the support for conveying the context, such as the kill chain phases or attack campaigns. Vendors are also increasingly building native STIX/TAXII support for their products under the pressure of the industry. A European technical report and standards body (ETSI) has recently emphasized that threat intelligence sharing needs to be considered as an essential component of an organization's security architecture, and called for tool interoperability as a top priority [26]. The emergence of open source translators and middleware, which can bridge the legacy systems with CTI feeds, will ease the integration challenge. For instance, connectors will automatically convert STIX into formats such as CSV, syslog for tools that need it, or cloud services that will act as the aggregator, converting various feed formats into one standardized output for the organization. Interoperability also translates into common data models for the reputational data, so that the confidence levels can be shared consistently. The standardization efforts aim to make sharing a plug-and-play process, where joining a new threat intel community will be as simple as an API key, and data will start flowing into all relevant internal systems. Achieving this will significantly optimize multi-platform CTI utilization.

6.2 AI-Driven Intelligence Processing and Prioritization:

AI and Machine learning have been playing an increasingly important role in making the threat intelligence more digestible and actionable [27]. ML techniques, from clustering to deep neural networks, help identify the patterns in a large threat data set and predict the vulnerability that is most likely to be exploited. AI assistants in SOCs automatically triage incoming threat intelligence, for example, filtering out the indicators that are duplicates, grouping indicators into likely incidents, and highlighting the indicators that match the organization's industry or the technology stack. The challenges of false positives can also be addressed using machine learning with the help of the organization's feedback. Some systems use multi-stage validation where ML-detected anomalies are cross-checked against rule-based systems to continuously improve the accuracy. AI is also being used for threat intel generation. Natural Language Processing (NLP) models can scan through the unstructured sources, such as malware research reports, hacker forums, to extract any new threat intel automatically. The models, as they mature, can feed into sharing platforms in real-time and expand the intelligence collected. ML models generally need large and up-to-date training data, as the threats evolve, models degrade over time if not trained over fresh data. To avoid this degradation, researchers are considering semi-supervised and online learning approaches, so the models are enabled to learn continuously with new telemetry and minimal human labeling. Through automatic analysis and prioritization, AI can reduce the workload on human analysts and ensure that the critical intel is acted upon first, which is especially vital in fast-moving attack scenarios.

6.3 Privacy preservation and Decentralized sharing architectures:

Trust and privacy barriers are being addressed through innovations in data sharing technology, which are enabling organizations to collaborate without fully exposing the sensitive data [28]. Blockchain and distributed ledger technology (DLT) are being used in threat intel platforms. Blockchain can provide an immutable log of shared intelligence and ensure untampered data. This incentivized the sharing of high-quality intel through a reputation mechanism. For example, a CTI based on blockchain can award reputation points or tokens to the contributors whenever the indicators prove to be useful and use consensus to validate the submissions [29]. A recent study of the emerging platforms revealed that the blockchain can eliminate single points of failure and add transparency, the current implementations suffer from scalability and latency issues, which make them less suitable for real-time sharing needs. Federated learning and secure multiparty computation are being explored to enable collective threat intelligence analysis without sharing the raw data [30]. In the case of federated learning, organizations can collaboratively train an ML by sharing model parameters or gradients and not the actual log data. Through this, each participant benefits from a robust model that has been trained on broader data, and no one has to reveal the internal logs or incidents. In a platform, LUUNU has demonstrated this concept by integrating a blockchain with the federated learning setup on top of the open source MISP threat sharing instance. LUUNU allows organizations to train models for detecting threats while using smart contracts to ensure data integrity and privacy. This combines trust, privacy, and intelligence sharing in a single framework. As these privacy-preserving techniques mature, there will be a wider adoption in sectors like finance and healthcare, where the regulations strongly restrict data sharing. This could also alleviate the reluctance from the organizations that are still doubtful of sharing their data due to privacy reasons.

6.4 Robust Trust and Reputation Systems:

In order to strengthen the shared intelligence, the future platforms will incorporate source validation, reputation scoring, and attribution features [31]. Present-day exchanges are relatively opaque, but the future CTI sharing communities may operate much like professional social networks and marketplaces, the contributors can earn a reputation score based on accuracy and value of their submissions, and consumers can filter or weight intel based on those scores. Academic work proposes models such as Proof of Reputation (PoR) consensus in blockchain CTI systems, the only sources with a certain reputation can add a new intelligence block [32]. Apart from the scoring, there has been a push for automated validation of shared intel. This involves cross-referencing of the submitted indicators against multiple independent data sources. Some of the sharing groups even have a peer review process, where the initial intel has been shared as unverified and then vetted by other members, along with validation feedback looping into the contributor's reputation. The metadata boosts the confidence levels, and the sightings count will become the standard part of the threat intel; the recipients know how the suggested indicator has been observed. A well-calibrated trust system will deter the injection of bad intelligence over time, as such entries will be quickly downgraded in reputation and filtered out. Formal sharing agreements and governance will improve trust as more sectors adapt to the structured information sharing agreements. The goal is to have a virtuous cycle where the quality intel sharing begets trust, in turn begets more sharing of quality intel.

6.5 Integrated Threat Intelligence Ecosystems and Automation:

The future points towards a deeper integration between CTI sharing platforms with the day-to-day security operations and a culture of collaboration [33]. Fusion centers or unified threat intel hubs are increasing, these platforms, apart from aggregating the intel from external and internal alert feeds, also integrate the incident response workflows, orchestration playbooks, and ticketing systems. In this ecosystem, when new threat intel comes in, this may automatically trigger proactive actions such as updating the firewall rules, scanning the archives for retroactive matches, and alerting the asset owners. Many forward-leaning organizations are moving towards real-time CTO, where the intelligence sharing is coming in a live stream that is feeding directly into the detection engines with minimal human involvement. This requires a high level of trust in the system and an extremely low false positive rate, which can be achieved by employing techniques such as AI curation and reputation scoring. There will be cross-sectoral partnerships and collaborations between public and private entities to deepen. Government CERTs and national cyber centers are heavily investing in platforms to share intel with industry. For example, the US DHS's Automated Indicator Sharing initiative has been evolving to STIX/TAXII-based automation. [34] Industry groups are also widening their range, and there are regional and international cybersecurity exchanges that connect ISACs from different sectors and recognizing the threats that often travel laterally across sector boundaries (A technique that has been used to attack a bank can be later used to target a hospital). There will be increased trust between the communities in the future. Companies might be simultaneously plugged into multiple threat intel communities, the sectoral ISAC, global malware exchange, and a local law enforcement partnership, all through a single unified platform that de-conflicts and synthesizes the intel flow. There has been a cultural shift towards openness and collaboration. A 2025 study on phishing defense concluded that success in using threat intelligence relies on complex approaches combining real-time intelligence sharing, constant technical innovation, and continuous user education [35]. This shows that human factors have to advance in tandem, and the cybersecurity leaders are increasingly viewing the participation in intel sharing as an essential part of their own risk management, which bodes well for the resource commitments that are needed to implement these future directions.

The next generation of threat intelligence sharing will be faster, smarter, and have data processing through AI, more secure and decentralized data exchange through blockchain and federated learning, have strong trust and incentive models, and a seamlessly integrated fabric of security tools and communities. The advancements are aiming towards mitigating the present-day pain points and ensuring that the intel is timely, relevant, and easily consumable by any security platform, while preserving the confidentiality concerns of the parties sharing the intel. The result is aimed to achieve a significantly fortified collective defense where the information flows unimpeded to wherever it is needed, and every organization, large or small, can act on the latest intel with confidence.

7. Conclusion

Sharing of threat intelligence across multiple security platforms has become a necessity in the face of increasingly aggressive and agile cyber adversaries. In this white paper, we have examined how optimized CTI sharing can empower organizations to move from an isolated, reactive security posture to a more collaborative, proactive defense model. Standards such as STIX/TAXII have laid the foundation for interoperability and enabled the integration of threat feeds with tools such as SIEM and firewalls to automate protective measures. The real-world cases highlight the tangible benefits that come through threat intel sharing, which results in faster incident detection, preventing attacks, and a reduction in damage. The current limitations have also been discussed, ranging from data overload and false positives to trust barriers and integration gaps, these can blunt the effectiveness of threat sharing if these are not addressed.

Continuous innovation and collaboration are needed to overcome these challenges. Advances in machine learning are being trained to filter and prioritize the threat data intelligently, addressing the noise problem, and help the analysts to focus on the actual problem. Latest sharing architectures employ blockchain, federated analytics, and distributed trust are helping to tackle the privacy and trust issues. This allows the organizations to contribute and consume intelligence with greater confidence that their data and reputations are safeguarded. There has been a cultural shift as organizations started to recognize that hoarding information can be self-defeating in an interconnected world; organizations are safer when the intelligence is shared. Industry bodies and governments are encouraging threat intel sharing through structured programs, grants, and even regulatory expectations for critical sectors to participate in the information sharing.

To ensure success in the optimization of threat intelligence sharing is hinged on the following factors, agility-threat intel processes and platforms have to be able to adapt quickly to latest threat types and data sources, trust & transparency - the more that the sharing platforms can demonstrate the integrity through audits, cryptographic assurances, or reputational feedback loops and protect the sensitive contributor data, the more organizations will be willing to share their own intelligence instead of just the low-level insights. Integration and automation- CTI has to be seamlessly fed into the prevention, detection, and response engines across the stack. This means a close coupling of TIPs with the SOAR platforms, security vendors agreeing on standard APIs for threat data exchange in real-time. Community and skill building - a collaborative ecosystem needs to be fostered, in which the organizations with limited security, staff can plug in and benefit from it. This may involve more managed services and user-friendly tools that will lower the barrier of entry for consuming and contributing to the threat intel.

Optimizing the threat intelligence sharing is a continuous process, it involves continuous improvement of the technology and processes, and also nurturing the spirit of collective defense. The future directions and trends that were outlined indicate that the community is moving forward in the right direction. If the community can leverage on implementing ML-driven threat intel analytics, establishing privacy-preserving sharing frameworks, enforcing interoperability standards, and strengthening the trust networks, the payoff will be a cyber defense capability that will keep up the pace with the threats and even outstrip them. In the era of fast-moving and sophisticated cyberattacks, an optimized, multi-platform threat intelligence sharing strategy is what will help defenders to anticipate, withstand, and counter the attackers. Through sharing the intelligence effectively, organizations worldwide can ensure that when one organization is attacked, others worldwide can defend it immediately and contribute to a secure digital environment for everyone.

8. Acknowledgments

The authors would like to express their gratitude for the academic support received during the preparation of this work. No external funding or institutional financial assistance was involved in this study. The authors also declare that there is no conflict of interest related to this article. All data used in this research are fully available within the article, and no additional datasets were generated or sourced externally.

References

1. Sophos, The State of Ransomware 2022. Sophos Group plc, 2022.
2. U.S. Government Accountability Office (GAO), Federal Response to the SolarWinds Cyberattack, GAO-22-104746, 2022.
3. SANS Institute, Cyber Threat Intelligence Survey Report 2022. SANS Press, 2022.
4. OASIS, STIX™ Version 2.1. Structured Threat Information Expression and TAXII™ Version 2.1. Trusted Automated Exchange of Indicator Information. OASIS Standard, 2021.
5. European Union Agency for Cybersecurity (ENISA), Guidelines on Threat Intelligence Sharing, 2021.
6. Europol, Internet Organised Crime Threat Assessment (IOCTA) 2022. Europol, 2022.
7. Symantec, Lessons from Locky and WannaCry Ransomware Campaigns. Symantec Threat Intelligence Report, 2018.
8. MISP Project, MISP Threat Sharing Platform Statistics 2023. Open Threat Intelligence Repository, 2023.

9. Financial Services Information Sharing and Analysis Center (FS-ISAC), Annual Global Intelligence Report 2022, 2022.
10. Cyber Threat Alliance (CTA), Annual Threat Sharing Report 2023, 2023.
11. Abusix and DigitalOcean, Collaborative Threat Intelligence Sharing to Reduce Cloud Abuse: Case Study, 2023.
12. MITRE Corporation, Global Adversary Behavior and Technique Reuse Study, 2021.
13. Cybersecurity and Infrastructure Security Agency (CISA), Cybersecurity Advisory on State-Backed Wiper Malware Activity, U.S. Department of Homeland Security, 2023.
14. Cyber Defense Assistance Collaborative (CDAC), Threat Intelligence Integration for Ukraine, 2023.
15. Cybersecurity and Infrastructure Security Agency (CISA), Joint Cyber Defense Collaborative (JCDC) and Log4j Response Report, 2022.
16. Health Information Sharing and Analysis Center (H-ISAC), Healthcare Threat Intelligence Sharing Report 2023, 2023.
17. Gartner, Threat Intelligence Overload: Managing Volume and Relevance in SOC Operations, 2023.
18. MITRE Engenuity, Contextualizing Indicators for Operational Threat Intelligence, 2022.
19. OASIS CTI Technical Committee, STIX™ and TAXII™ Interoperability Challenges Report, 2022.
20. European Union Agency for Cybersecurity (ENISA), Interoperability of Threat Intelligence Platforms, 2021.
21. Forum of Incident Response and Security Teams (FIRST), Traffic Light Protocol (TLP) v2.0 and Information Sharing Ethics, 2022.
22. European Commission, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, 2016.
23. Organisation for Economic Co-operation and Development (OECD), Trust Frameworks for Cross-Border Cyber Threat Information Sharing, OECD Digital Economy Papers, 2022.
24. Ponemon Institute, Challenges in Establishing Trusted CTI Sharing Networks, 2023.
25. SANS Institute, Threat Intelligence Operations Survey: Staffing and Capability Gaps, 2022.
26. European Telecommunications Standards Institute (ETSI), Technical Report TR 103 838: Cyber Threat Intelligence Standardization Landscape, 2023.
27. IBM Security X-Force, AI and Machine Learning in Threat Intelligence, 2023.
28. IEEE Access, Privacy-Preserving Collaborative Threat Intelligence Sharing Frameworks, IEEE, 2023.
29. N. Kshetri, “Blockchain-Based Threat Intelligence Sharing Systems: A Review,” Computers & Security, Elsevier, 2023.
30. LUUNU Consortium, Federated Learning Meets CTI: Secure Collaborative Detection, 2023.
31. NATO CCDCOE, Trust Models for Collaborative Threat Intelligence Sharing, 2022.
32. Z. Zhang et al., “Proof of Reputation in Blockchain-Enabled Threat Intelligence,” IEEE Transactions on Information Forensics and Security, 2023.
33. Cybersecurity and Infrastructure Security Agency (CISA), Integrated Threat Intelligence Operations: The Future of CTI Sharing, 2024.
34. U.S. Department of Homeland Security (DHS), Automated Indicator Sharing (AIS) Program Overview, 2023.
35. **Figure 1.** “Generalized architecture for threat intelligence sharing,” AWS Prescriptive Guidance, Amazon Web Services. [Online]. Available: https://docs.aws.amazon.com/prescriptive-guidance/latest/cyber-threat-intelligence-sharing/architecture.html

    Figure 2. “Cyber threat intelligence sharing architecture,” ScienceDirect, Journal of Information Security and Applications, vol. 83, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212624000899

ALL Figures

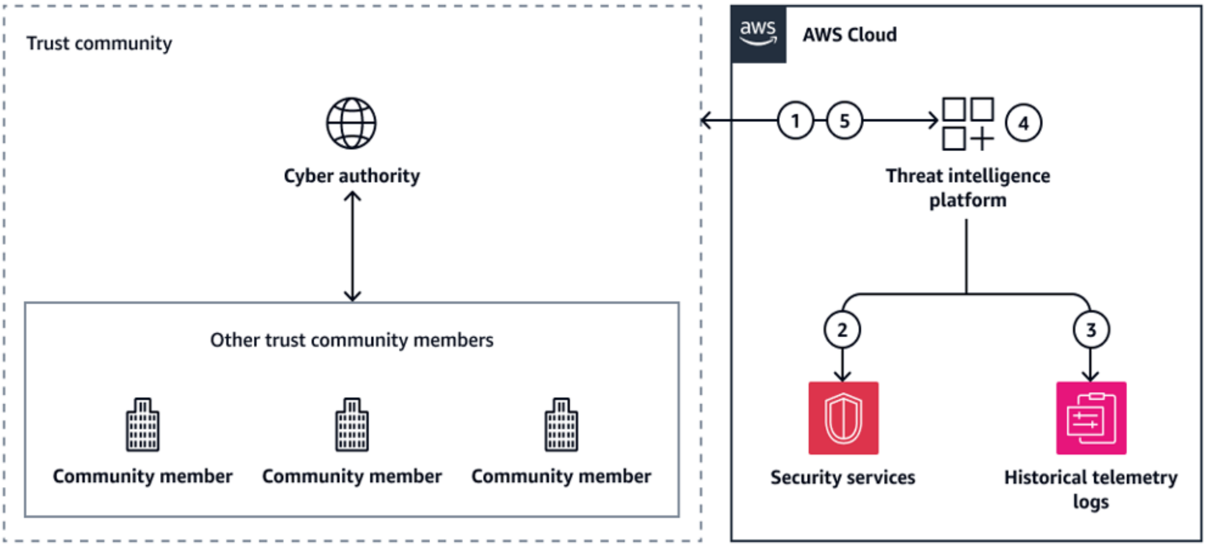

Figure 1: Generalized architecture for threat intelligence sharing.

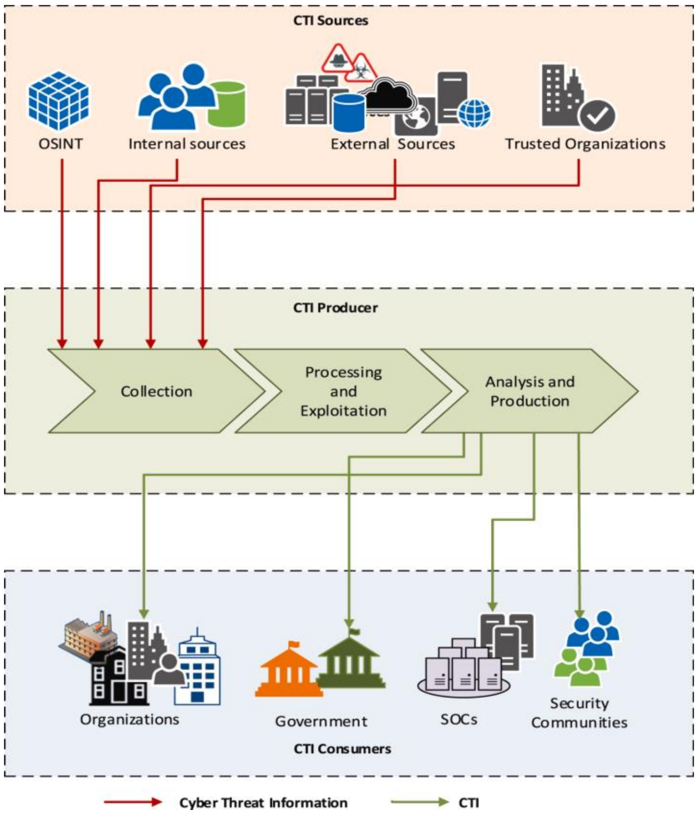

Figure 2: A conceptual overview of a CTI sharing platform model