Maximizing Cyber Threat Intelligence (CTI) in the Financial Sector: Benefits and Implementation Challenges

Abdullah bin Mohd Aziz

Department of Computer Science, Universiti Malaysia Kelantan, Bachok Campus, Kelantan, Malaysia

Abstract

Due to the critical importance of financial infrastructures, they are prime targets for cybercriminals, highlighting the necessity for robust security measures. This study explores the role of Cyber Threat Intelligence (CTI) in enhancing the security frameworks of financial institutions and identifies key challenges that could impede its effective adoption. CTI offers numerous benefits to the financial sector, including real-time threat awareness, allowing institutions to proactively address cyber-attacks. It significantly enhances the efficiency of incident response teams by providing contextual information about attacks. Additionally, CTI is crucial for strategic planning by offering insights into emerging threats and helps institutions comply with regulatory frameworks such as GDPR and CCPA. Other applications include improving fraud detection through data correlation, assessing and managing vendor risks, and optimizing resource allocation to address the most critical cyber threats. However, the adoption of CTI technologies faces several challenges. A major issue is data overload, as the vast amount of information generated can overwhelm institutions and lead to alert fatigue. Interoperability is another significant challenge; different systems within the financial sector often use incompatible data formats, complicating CTI integration. Cost constraints can also inhibit the adoption of advanced CTI tools, especially for smaller institutions. A lack of specialized skills required to interpret CTI data exacerbates the problem. The effectiveness of CTI depends on its accuracy, and false positives and negatives can have detrimental impacts. The rapidly evolving nature of cyber threats necessitates real-time updates, posing another challenge for effective CTI implementation. Furthermore, sharing threat intelligence among entities, often competitors, is hindered by mistrust and regulatory complications. This research aims to provide a detailed understanding of the applicability and limitations of CTI within the financial sector, encouraging institutions to adopt it with a thorough awareness of the associated challenges.

Keywords: Cyber Threat Intelligence, Financial Infrastructure, Fraud Detection, Incident Response, Interoperability, Regulatory Compliance, Skill Gap, Threat Awareness, Vendor Risk Management

Introduction

Computing technology has fundamentally altered the way in which modern society operates, offering a range of benefits that are both extensive and transformative. Within the private and public sectors, organizations have adopted complex information systems (IS) to facilitate and enhance a variety of operations. For instance, in the case of critical infrastructure—such as electrical grids, water supply, and telecommunications—information systems are employed to monitor system health, coordinate resource allocation, and facilitate repairs. These systems enable the centralized monitoring of vital metrics, allowing for real-time decision-making and predictive analysis that can preempt failures or disruptions. Furthermore, they permit the

integration of different data sources, providing a holistic view that can lead to improved efficiency and safety measures.

Figure 1. Major cybersecurity challenges faced by financial institutions

Source: Author

The rising trend in cyberattacks has led to an increasing urgency for collaborative efforts in combating cybercriminal activities. The sheer volume of attacks, coupled with their growing complexity, poses significant risks for organizations across various sectors. The variety of attacks, ranging from basic phishing attempts to sophisticated state-sponsored cyber espionage, has outpaced the capabilities of individual organizations to handle them alone. The risks associated with successful intrusions have escalated over time, often resulting in debilitating security breaches that could compromise sensitive data, financial assets, or even critical infrastructure. This increasing threat landscape has made it imperative for organizations to pool their resources and knowledge. One widely-adopted practice for fostering collective defense is the sharing of cyber threat intelligence (CTI), which encompasses data and insights about existing and emerging threats [1], [2].

Cyber threat intelligence (CTI) serves as a cornerstone in the collaborative approach to cybersecurity [3], [4]. CTI provides organizations with valuable information on the tactics, techniques, and procedures employed by cyber adversaries. By sharing this kind of intelligence, organizations can better anticipate potential vulnerabilities and enhance their defensive measures accordingly [5]. Moreover, shared intelligence can contribute to more effective responses to ongoing attacks, as organizations can quickly adapt their defenses based on real-time insights from other affected parties. This communal sharing of information serves as an augmentative force, effectively broadening the scope and enhancing the efficacy of individual cybersecurity operations. Various platforms and organizations, such as Information Sharing and Analysis Centers (ISACs) and governmental cybersecurity agencies, serve as facilitators for the dissemination of CTI.The cycle is designed to be iterative, meaning that the Dissemination stage feeds back into the Direction stage, allowing for continuous refinement and improvement of the intelligence process [6], [7].

Financial institutions serve as the backbone of modern economies, providing a range of services from savings and loans to investment opportunities [8]. Their role is so integral that any disruption in their operations can have a cascading effect on various sectors, affecting not just businesses but also the daily lives of average citizens. The stability of these institutions is therefore of paramount importance, and any form of vulnerability can have far-reaching implications. For instance, during economic downturns, the failure of a single major bank can trigger a domino effect that jeopardizes the financial stability of other banks and, by extension, the economy as a whole. This interconnectedness makes the financial sector highly susceptible to systemic risks, which can be exacerbated by external shocks such as natural disasters, geopolitical tensions, or significant policy changes [9], [10].

Table 1. Intelligent life cycle

Stage	Description
Direction	- Defines intelligence requirements and priorities. - Identifies stakeholders' questions and information needs. - Determines types of information needed and sources to obtain it. - Sets the course for subsequent phases.
Collection	- Employs various agencies and sources for information gathering. - May require specialized skills and extended timeframes. - Requires effective management to meet requirements or address limitations.
Processing	- Involves sub-processes like collating, evaluating, and analyzing gathered information. - Ensures trustworthiness of information. - Integrates it with existing intelligence. - Confirms relevance to initial requirements [11].
Dissemination	- Prepares synthesized intelligence in an accurate, usable format. - Dispatches the material to relevant parties. - Enables informed decision-making based on the intelligence.

In recent years, the threat for financial institutions has evolved to include sophisticated cyber-attacks. These attacks are perpetrated by a variety of malicious actors, ranging from state-sponsored hackers aiming to destabilize a country's economy to individual criminals looking for financial gain [12]–[14]. The methods employed can vary widely, from advanced persistent threats that aim to infiltrate systems over a long period to ransomware attacks that seek immediate financial returns. One common form of cyber-attack is the data breach, where sensitive customer information is stolen, often leading to identity theft and financial fraud. The consequences of such breaches are not just financial; they also erode the trust that customers place in these institutions [15], [16].

Given the high stakes involved, it is not surprising that the financial industry is one of the largest spenders on cybersecurity measures. Investment in cybersecurity goes beyond mere compliance with regulatory requirements; it is a critical business imperative. Financial institutions employ a multi-layered approach to security, incorporating not just technological solutions but also rigorous employee training and public awareness campaigns. Despite these efforts, the evolving nature of cyber threats means that cybersecurity remains a moving target. Financial institutions must continually adapt and innovate to stay ahead of malicious actors, making cybersecurity a continual and significant operational concern.

The financial sector faces an array of cyber threats that are both diverse and increasingly sophisticated. These threats emanate from a variety of sources, including state-sponsored hackers aiming to compromise national security, as well as individual actors motivated by financial gain. The methods employed in these cyber-attacks can range from phishing schemes to more advanced techniques like ransomware and distributed denial of service (DDoS) attacks. Some malicious actors focus on immediate financial gain, targeting customer accounts or manipulating transactions. Others may have more insidious goals, such as causing systemic disruptions that can lead to widespread chaos. For instance, an attack on a major financial exchange could not only halt trading but also undermine confidence in the financial system at large.

Data breaches are a particularly concerning form of cyber-attack for financial institutions. These breaches often result in the unauthorized access to sensitive customer information, including account numbers, passwords, and personal identification details. The ramifications of such breaches are twofold. First, they expose customers to the risk of identity theft and financial fraud, which can have long-lasting effects on their financial well-being. Second, data breaches can severely damage the reputation of the affected financial institution, leading to a loss of customer trust and, in some cases, legal repercussions. The cost of addressing these breaches—both in terms of financial loss and reputational damage—can be substantial [17], [18].

In response to the escalating threats, the financial industry has significantly ramped up its investment in cybersecurity measures, surpassing even governmental spending in this area [19]. This investment is directed towards a variety of initiatives, including but not limited to,

advanced firewall systems, intrusion detection systems, and secure data storage solutions. Employee training programs are also implemented to educate staff on the best practices for identifying and mitigating potential threats. Additionally, many financial institutions are collaborating with cybersecurity firms and governmental agencies to share information and resources, aiming to create a more robust defense mechanism against cyber threats. Despite these efforts, the dynamic nature of cyber threats necessitates ongoing vigilance and adaptation of cybersecurity strategies.

Applications

1. Threat Awareness:

In the past, cybersecurity strategies in financial institutions primarily focused on reactive measures, responding to threats and incidents as they occurred. This approach left organizations always one step behind cybercriminals, who are continually evolving their tactics and methods. Reactive cybersecurity essentially meant that financial institutions were exposed to greater risks because they only took action after an attack had occurred, which often led to significant financial losses and reputational damage. It was like a game of catch-up, where the organization had to constantly deal with the consequences of successful attacks, thereby diverting resources away from other critical business functions [20], [21].

The advent of Cyber Threat Intelligence (CTI) marks a pivotal shift toward a more proactive approach in cybersecurity. Financial institutions that employ CTI receive up-to-date information on global cyber threats, vulnerabilities, and potential attack methods. With this intelligence, these organizations can anticipate the types of attacks that may target their systems and implement countermeasures in advance. By analyzing trends and patterns in cyberattacks, financial institutions can adjust their security protocols accordingly, strengthening their defenses and potentially thwarting attacks before they occur. This proactive stance provides an added layer of security that goes beyond merely responding to attacks, making it a significant improvement over older, reactive approaches.

The shift towards a proactive approach through the employment of CTI brings about an enhanced level of security for financial institutions. Unlike older, reactive models of cybersecurity that prioritized incident response, a proactive stance aims to prevent incidents from occurring in the first place. By staying ahead of potential threats, organizations reduce the likelihood of successful attacks, thereby safeguarding both their assets and their reputation [22], [23]. This is particularly vital for financial institutions where breaches can result in not only significant financial losses but also erosion of customer trust.

2. Incident Response:

The significance of Cyber Threat Intelligence (CTI) in enhancing the capabilities of an incident response team is paramount. CTI provides data that is both current and relevant to the cybersecurity environment, allowing analysts to draw correlations between different indicators of compromise (IoCs) and tactics, techniques, and procedures (TTPs) employed by threat actors. By evaluating this information, an incident response team gains a situational awareness that is

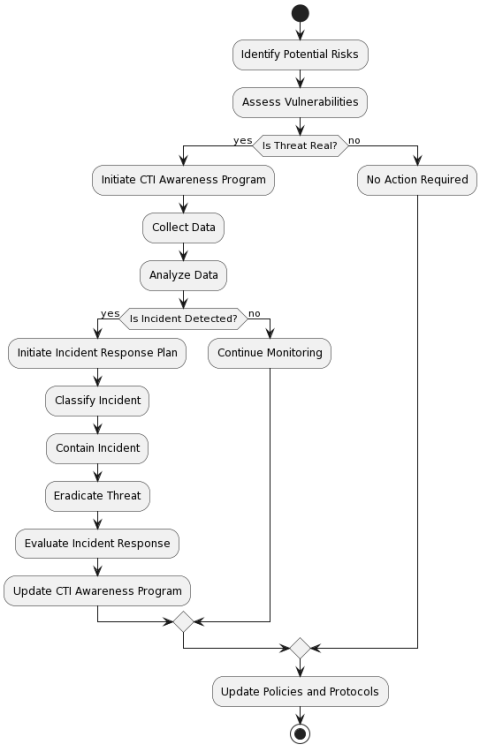
essential for assessing the severity of a threat. The context provided by CTI also assists the team in determining the most appropriate countermeasures to implement. For instance, understanding that an attack is part of a larger, coordinated campaign by a state-sponsored actor could prompt a different response compared to an isolated incident perpetuated by an individual.

Utilizing CTI streamlines the decision-making process, allowing for quicker responses to incidents. When an incident response team has information about the types of malware, the vectors of attack, and the vulnerabilities being exploited in real-time, they can act more effectively to contain and eradicate the threat. Knowledge of prior incidents involving similar TTPs could aid in predicting the attacker's next moves, thereby enabling proactive measures rather than merely reactive ones. This could range from patching vulnerable systems to altering network configurations to better isolate affected systems [24], [25].

CTI allows for targeted allocation of both human and computational resources by providing insights into the severity and complexity of an attack. The incident response team can prioritize tasks based on threat intelligence, ensuring that high-severity incidents receive immediate attention. This enables better time management and could significantly reduce the financial and operational impact of a cybersecurity incident.

Collaboration is another critical aspect where CTI plays a vital role. Sharing intelligence within a community, be it an industry-specific consortium or a broader platform, amplifies the capabilities of individual incident response teams. For example, if one organization detects a new type of malware, sharing this information enables others to adjust their defensive mechanisms accordingly. Such collaborative efforts, fueled by shared CTI, facilitate a more robust collective defense against cyber threats.

Figure 2. awareness and incidence activity flow under CTI in financial institutions



Source: Author

Lessons learned from analyzing threat intelligence can be integrated into an organization's security policies, training programs, and even into the development of new security tools. For example, if CTI indicates a rising trend in phishing attacks exploiting a particular human behavior, the organization can implement educational programs to mitigate this specific risk [26], [27].

3. Strategic Planning:

Information on emerging threats is crucial for the strategic planning of cybersecurity infrastructure at a higher level. Knowledge of new attack vectors, vulnerabilities, and tactics, techniques, and procedures (TTPs) provides organizations with valuable foresight that can shape long-term security policies. Planning based on this predictive intelligence allows organizations to prioritize investments in technologies and solutions that are most relevant to the anticipated threat environment. For example, if an organization is aware of an increasing prevalence of advanced persistent threats (APTs) targeting their industry, they may opt to invest in more robust endpoint detection and response (EDR) solutions and multi-factor authentication technologies [28], [29].

By incorporating information on emerging threats into strategic planning, organizations can also prepare their personnel more effectively. Skill sets and training programs can be designed to equip staff with the capabilities required to combat the types of threats that are anticipated. For instance, if ransomware attacks are on the rise, cybersecurity training can be updated to include simulations that mimic these specific types of incidents. This leads to a workforce that is better prepared to deal with real-world scenarios, thereby enhancing the organization's resilience against such attacks.

In addition to technology and personnel, information on emerging threats can guide the modification of governance structures and procedures. Updating incident response plans, communication protocols, and escalation procedures based on the anticipated threat landscape ensures that the organization can respond in a coordinated and timely manner. This strategic alignment of governance mechanisms can also facilitate compliance with regulatory requirements that are becoming increasingly stringent, especially in sectors like finance and healthcare which are frequent targets of cyberattacks.

The role of emerging threat information is also salient in the development of partnerships and collaborative initiatives. Organizations can forge alliances with entities that possess complementary capabilities, thereby strengthening collective cybersecurity defenses [30]. For example, a financial institution, aware of an upsurge in attacks targeting mobile banking applications, might partner with technology firms specializing in mobile security solutions. Such strategic collaborations are often facilitated by shared threat intelligence platforms and can significantly enhance the capacity to prevent, detect, and respond to cyber threats.

Emerging threat information also aids in risk assessment and management activities. Comprehensive risk models can be developed, which consider the probable impacts of anticipated threats. This enables organizations to make data-driven decisions around cyber insurance, budget allocations, and other financial aspects of cybersecurity. By aligning their risk management strategies with information on emerging threats, organizations can more accurately predict and thus better prepare for the financial implications of cybersecurity incidents. This long-term approach, informed by timely and relevant data, thereby contributes significantly to the resilience and sustainability of an organization's cybersecurity infrastructure.

4. Fraud Detection:

Cyber Threat Intelligence (CTI) serves as a vital component in enhancing fraud detection capabilities, particularly through the correlation of transactional data with known indicators of fraudulent activity. In financial and e-commerce sectors, transactional data is abundant, but its sheer volume can be overwhelming for traditional fraud detection systems. The integration of CTI allows these systems to prioritize transactions that match or resemble known fraud patterns, thereby enabling a more focused and effective detection strategy. By flagging transactions that exhibit traits or patterns common to previously identified fraudulent activities, organizations can take preventive actions to either halt or scrutinize the transactions in real-time [31], [32].

This targeted approach to fraud detection facilitated by CTI is advantageous for optimizing resource allocation. Traditional fraud detection systems that operate without the benefit of CTI may generate a high number of false positives, which require manual verification and thereby consume valuable manpower and time. By utilizing CTI to correlate transactional data with proven indicators of fraud, organizations can fine-tune their algorithms to reduce false positives and focus their resources more effectively. This targeted scrutiny is particularly beneficial in high-frequency trading environments or large e-commerce platforms where the scale of transactions makes manual verification impractical.

Table 2. Implementing a fraud detection system with Cyber Threat Intelligence (CTI) in financial institutions

```
Initialize:
  Initialize ML_Model
  Configure CTI_API
  Initialize Database
  Set Threshold for Fraud_Score
Function Train_Model():
  Retrieve Historical_Transactions
  Retrieve Historical_CTI
  Preprocess and Clean Historical_Transactions
  Map Historical_CTI to relevant features
  Merge Historical_Transactions and Historical_CTI -> Training_Dataset
  Normalize Training_Dataset
  Train ML_Model using Training_Dataset
  Validate and Tune ML_Model
  Return ML_Model
Function Get_Real_Time_CTI():
  Fetch data from CTI_API
  Return Real_Time_CTI
Function Score_Transaction(Transaction, Real_Time_CTI, ML_Model):
  Preprocess and Clean Transaction
  Map Real_Time_CTI to relevant features
  Merge Transaction and Real_Time_CTI -> Processed_Transaction
  Normalize Processed_Transaction
  Fraud_Score = ML_Model.predict(Processed_Transaction)
  Adjust Fraud_Score based on Real_Time_CTI
  Return Fraud_Score
Train_Model()
Main Loop:
  While True:
    Transaction = Get_New_Transaction()
    Real_Time_CTI = Get_Real_Time_CTI()
    Fraud_Score = Score_Transaction(Transaction, Real_Time_CTI, ML_Model)
    If Fraud_Score > Threshold:
      Flag Transaction for manual review
    Update Transaction_DB with Transaction and Fraud_Score
    Update CTI_DB with Real_Time_CTI

    Feedback = Get_Manual_Review_Outcome()
If Feedback is not Null:
  Update Labeled_Fraud_DB with Transaction and Feedback
  ML_Model = Train_Model()
Update Real_Time_CTI = Get_Real_Time_CTI()
```

Furthermore, CTI can contribute to the dynamic evolution of fraud detection models. Threat actors continually adapt their tactics to circumvent existing security measures. CTI provides timely intelligence on these changing tactics, enabling organizations to update their fraud detection algorithms accordingly. For example, if a new type of credit card skimming technique is identified, CTI can inform the necessary changes in fraud detection algorithms to recognize transactions that may be affected by this technique [33]. This adaptability is essential for staying ahead of sophisticated and evolving fraud schemes.

Beyond immediate fraud detection, CTI contributes to strategic planning and policy formulation. Data on emerging fraud tactics can inform long-term countermeasures, such as updates to customer authentication protocols, revisions in transaction approval workflows, or investments in new types of monitoring technology. Senior management can utilize CTI insights for making data-driven decisions regarding the allocation of budgets and resources for fraud prevention. For instance, if CTI indicates a rising trend in identity theft cases through social engineering, organizations may prioritize employee training and customer education on this specific threat vector [34]. CTI also promotes collaboration among different organizations and even across industries. Fraud indicators and tactics often cut across organizational and sectoral boundaries; an attack vector employed in one industry could very well be applied to another. Through information-sharing consortia or platforms, organizations can collectively benefit from the CTI gathered by individual entities. This collaborative approach enhances the collective fraud detection capabilities of participating organizations. Shared CTI allows for faster dissemination of new fraud indicators, thereby creating a more resilient and adaptive defense network against fraudulent activities.

5. Vendor Risk Management:

Financial institutions often operate within intricate supply chain networks that present a multitude of cybersecurity challenges. Cyber Threat Intelligence (CTI) is increasingly recognized as a crucial tool for evaluating the security postures of vendors within these supply chains. Vendors often have varying levels of cybersecurity maturity, and a weak link can expose the entire supply chain to potential risks. Utilizing CTI, financial institutions can assess the risk profiles of their vendors by examining data on previous security incidents, known vulnerabilities, and the overall cybersecurity practices followed by these entities. By correlating this information with intelligence on current threat landscapes, CTI can provide financial institutions with actionable insights to make informed decisions on vendor selection, management, and monitoring.

The value of CTI in this context extends to real-time risk mitigation. Financial institutions often rely on third-party services for a multitude of functions, ranging from payment processing to customer relationship management. Any breach or vulnerability in these third-party services could directly impact the financial institution's security posture. CTI provides ongoing, updated information on threats that could affect these vendors. When a new threat is identified, such as a specific malware targeting a software commonly used in the financial sector, CTI can warn

institutions of the risk in real-time, enabling them to take immediate preventive actions such as temporarily isolating connections to the affected vendor or applying additional security controls.

Another benefit of CTI in managing vendor-related risks in financial institutions is the standardization of security assessments. Vendor risk assessments often vary in their scope and depth, depending on the internal practices of each financial institution. CTI can provide a standardized set of metrics and key performance indicators (KPIs) that enable a consistent and rigorous assessment. This is particularly useful for financial institutions operating in multiple jurisdictions or those that have merged with or acquired other entities. Standardized assessments based on CTI can facilitate compliance with regulatory requirements related to vendor management and cybersecurity, making the process more efficient and less prone to errors.

Furthermore, the integration of CTI within vendor risk management processes enables financial institutions to prioritize their resources more effectively. Understanding the risk profile of each vendor allows institutions to focus their efforts where they are most needed. For instance, a vendor providing a mission-critical service would require more stringent oversight than a vendor providing a non-essential service. By using CTI to differentiate between high-risk and low-risk vendors, financial institutions can allocate their cybersecurity resources more efficiently, thereby enhancing their overall risk management strategy.

CTI can also serve as a valuable instrument for promoting cybersecurity awareness and collaboration among vendors. Financial institutions can share aggregated, anonymized threat intelligence with their vendors to help them improve their security measures. This fosters a culture of collective cybersecurity responsibility and enhances the overall resilience of the supply chain. The institution and its vendors become mutually reinforcing entities in a network capable of resisting cyber threats more robustly, a significant advantage given the interconnectedness of financial services and the increasing sophistication of cyber threats.

6. Social Engineering and Phishing:

Real-time threat intelligence plays a critical role in providing information about ongoing phishing campaigns specifically targeting financial institutions or their customers. In the ever-evolving landscape of cyber threats, phishing remains a prevalent and effective tactic employed by adversaries to gain unauthorized access to sensitive information. Real-time Cyber Threat Intelligence (CTI) offers immediate insights into new phishing techniques, exploited vulnerabilities, and other related indicators of compromise (IoCs) that can help in the prompt identification and mitigation of such attacks [35], [36].

The immediacy of real-time CTI is invaluable in enabling a swift response to phishing attempts. Financial institutions often face high volumes of transactions and customer interactions, making them lucrative targets for phishing campaigns. Any delay in identifying and responding to a phishing attack could lead to significant financial losses and erosion of customer trust. Real-time CTI provides actionable information that can be rapidly disseminated to relevant departments, such as fraud detection units and customer service teams, enabling them to take

appropriate measures like blocking compromised accounts or notifying customers to avoid certain links or attachments.

In addition to its benefits for internal decision-making, real-time CTI can enhance customer protection mechanisms. Financial institutions can use the intelligence to update their customer-facing security features and to issue timely advisories. For example, if a new type of phishing email is identified that exploits a recently discovered vulnerability in a commonly used email client, the institution can immediately inform its customer base to apply necessary patches or to be cautious of specific types of emails. This proactive customer communication can significantly reduce the success rate of phishing campaigns and may prevent considerable financial and reputational damage.

Real-time CTI also facilitates a more efficient allocation of resources in combating phishing threats. When financial institutions are aware of the specifics of an ongoing phishing campaign, such as the email domains being spoofed or the type of malware being deployed, they can direct their monitoring efforts more precisely. This allows for more targeted threat hunting and reduces the strain on security personnel who are often tasked with reviewing vast amounts of data and alerts. By focusing on the most relevant threats, financial institutions can achieve a higher detection rate while utilizing fewer resources, thereby optimizing their cybersecurity operations.

Real-time CTI is instrumental in fostering inter-organizational collaboration and information sharing. Phishing campaigns often target multiple financial institutions simultaneously or sequentially. By sharing real-time threat intelligence, these institutions can collectively enhance their defenses against common adversaries. Many industry-specific information-sharing platforms and consortiums exist to facilitate such collaboration.

7. Resource Allocation:

The efficient allocation of resources is a crucial consideration for financial institutions aiming to maintain a robust cybersecurity posture. Better intelligence, specifically Cyber Threat Intelligence (CTI), plays a pivotal role in this process by enabling organizations to focus on the most pressing threats. High-quality CTI provides actionable insights into the tactics, techniques, and procedures (TTPs) employed by threat actors, as well as indicators of compromise (IoCs) that can serve as early warning signs of an attack. By understanding the nature and severity of different cyber threats, financial institutions can make more informed decisions regarding where to deploy their cybersecurity resources for maximum effectiveness.

Resource allocation based on enhanced CTI leads to a more targeted approach in cybersecurity measures. Traditional security mechanisms often employ a broad brush, attempting to safeguard against a wide range of threats but potentially lacking depth in any particular area. With better intelligence, a financial institution can focus its efforts on specific vulnerabilities that are more likely to be exploited, or on types of attacks that have been identified as imminent risks. For example, if CTI indicates that advanced persistent threats (APTs) are increasingly targeting financial sectors, the institution can prioritize the fortification of its network perimeters and internal controls to counteract these specific kinds of attacks.

Better intelligence also allows for more effective utilization of human resources. Cybersecurity personnel are often in high demand but limited supply. By having accurate and timely intelligence, these experts can be directed to work on the most critical aspects of the organization's cybersecurity, whether that be incident response, threat hunting, or vulnerability assessment. High-quality CTI can guide the team's focus, ensuring that they are working on issues that present the most significant risks to the organization, thereby making the best use of their expertise and time.

Effective resource allocation driven by high-quality intelligence is a key factor in achieving compliance with regulatory frameworks. Financial institutions are subject to numerous regulations that dictate specific security measures, and non-compliance can result in substantial fines and reputational damage. With better intelligence, an organization can prioritize the implementation of controls that are not only required for compliance but are also most relevant to the current threat environment. This dual focus ensures that compliance activities are aligned with actual security needs, thus optimizing the use of resources for both compliance and security.

Cybersecurity budgets are often constrained and must be distributed across a range of activities, including technology acquisition, personnel training, and incident response. By relying on quality intelligence, financial institutions can allocate their budgets more effectively, ensuring that funds are directed toward initiatives that offer the highest return on investment in terms of risk mitigation. This financially efficient approach to resource allocation ultimately enhances the institution's ability to protect its assets and maintain the trust of its customers and stakeholders.

Challenges in Adoption

In the current technological environment, organizations increasingly deploy Cyber Threat Intelligence (CTI) tools to safeguard against cybersecurity threats. These tools are designed to produce a wealth of data, including logs, alerts, and analytics, that pertain to various aspects of network security. While the primary objective is to keep organizations informed and prepared, the sheer volume of data generated can lead to a phenomenon known as 'alert fatigue.' In essence, alert fatigue occurs when the high frequency of alerts desensitizes the administrators or security analysts who monitor them. Overwhelmed by the constant influx of alerts—many of which may be false positives or low-priority items—the professionals responsible for network security may start ignoring or underestimating alerts. Consequently, this increases the likelihood that a genuine threat might go unnoticed or unaddressed, thereby potentially compromising the security infrastructure.

Moreover, the issue of data overload is not limited to alert fatigue; it also extends to data management and analysis. As CTI tools continue to generate copious amounts of data, storing and analyzing this information becomes increasingly complex and resource-intensive. Organizations often need to invest in additional storage solutions and data analytics platforms to manage the information effectively. Even with the appropriate resources in place, the

challenge remains in extracting actionable insights from the sea of data. Automated processes for data analysis are not infallible and often require human oversight for accurate interpretation. The complexity of correlating data points, recognizing patterns, and making data-driven decisions becomes significantly higher due to the sheer volume of information at hand.

Furthermore, data overload can have financial implications for organizations. The increased need for storage solutions and specialized staff to manage and interpret the data results in elevated operational costs. In an attempt to cope with the massive amounts of data, organizations might be tempted to over-provision resources, thus leading to inefficient resource allocation. Additionally, the time spent by highly-skilled cybersecurity professionals in sorting through a multitude of alerts and data points is time not spent on strategic planning or other value-generating activities.

In the financial sector, interoperability—or the lack thereof—poses a significant challenge when integrating Cyber Threat Intelligence (CTI) solutions into existing systems. Financial institutions often employ a myriad of technologies for various functions such as transaction processing, data storage, customer relationship management, and more. Each of these technologies may adhere to distinct formats or standards, established either by the institution itself or by third-party vendors. When introducing CTI tools into this complex environment, the incompatibility between systems can result in inefficiencies and gaps in the cybersecurity posture. Specifically, a CTI tool that is not fully compatible with existing systems may fail to ingest or interpret data correctly. The outcome is a fragmented security architecture where different elements function in silos, hindering the organization's ability to have a unified and coherent view of its security status [37].

This lack of interoperability also complicates the process of data sharing among different departments or even different entities within the financial ecosystem. Given that cybersecurity is a collective concern, the ability to share threat intelligence can significantly enhance an organization's defensive capabilities. However, if the CTI tools in use do not support common standards for data formatting and communication, the quality and speed of information sharing suffer. For instance, one department might detect an emerging threat but could find it difficult to disseminate this knowledge across other departments or allied organizations effectively. The latency in information sharing may provide attackers with a window of opportunity to exploit vulnerabilities, thereby posing a considerable risk.

Financial institutions may need to collaborate with CTI vendors to customize solutions that can integrate with their existing systems. Standardizing data formats and communication protocols is another step toward enhancing interoperability. Organizations like the Financial Services Information Sharing and Analysis Center (FS-ISAC) are working toward creating such standards to ease the integration of disparate systems. By solving interoperability issues, financial institutions not only streamline their internal operations but also strengthen their ability to collaborate on cybersecurity at an industry level. This, in turn, contributes to the robustness and resilience of the entire financial infrastructure.

In the financial sector, the adoption of advanced Cyber Threat Intelligence (CTI) solutions often comes with a considerable financial burden. While large financial institutions may have the capacity to invest in state-of-the-art CTI tools and dedicated cybersecurity teams, smaller entities like local banks, credit unions, or financial startups may find it challenging to allocate sufficient resources for such advanced solutions. High costs can arise from multiple areas: licensing fees for the CTI tools themselves, infrastructure costs for deploying and maintaining the tools, and human resource expenses for specialists capable of managing and interpreting the intelligence data. Due to these cost factors, smaller financial institutions may resort to using more rudimentary cybersecurity measures, potentially leaving them vulnerable to sophisticated cyber threats.

The issue of high costs extends beyond the initial financial outlay for procuring CTI solutions. There are additional, often hidden, costs related to training staff, ongoing maintenance, and updates. Even after the initial setup, CTI solutions require regular updates to stay effective against evolving cyber threats. This continual need for updates and maintenance further adds to the operational expenses. Also, the rapidly changing nature of cyber threats necessitates periodic training for cybersecurity staff, which is another cost that organizations have to bear. For smaller financial entities with limited resources, these recurrent costs may result in budget constraints, diverting funds away from other critical areas like business development or customer service [38].

Faced with these financial constraints, smaller financial institutions are exploring various strategies to mitigate the impact of high costs associated with advanced CTI solutions. One approach is the use of shared platforms or collaborative models where multiple smaller entities pool resources to invest in a common CTI infrastructure. Industry organizations and regulatory bodies are also stepping in to offer standardized yet affordable CTI solutions specifically designed for smaller players in the financial market. While these alternatives may not entirely replicate the capabilities of high-end CTI solutions, they aim to offer a baseline level of cybersecurity that is both effective and financially feasible. This balancing act between cost and security effectiveness remains a crucial concern as cyber threats continue to evolve in complexity and scale.

The cybersecurity industry, and by extension the specialized field of Cyber Threat Intelligence (CTI), faces a pronounced skill gap that poses significant challenges for organizations, particularly in the financial sector. Properly interpreting and utilizing the data generated by CTI tools necessitates a skill set that combines technical acumen with analytical capabilities. Personnel must not only be proficient in various programming languages and network protocols, but they also need a nuanced understanding of the current threat landscape to distinguish between routine anomalies and potential security incidents. However, finding professionals who possess this blend of skills is a daunting task. Even when organizations do manage to recruit such talent, there is often a disparity between the complexities of the CTI data and the available skill level, leading to less-than-optimal utilization of the intelligence gathered.

The skill gap has repercussions that go beyond mere operational inefficiencies. For instance, when security analysts are not adequately equipped to interpret CTI data, there is an increased risk of overlooking critical threats or misclassifying the severity of alerts. In the worst-case scenario, this could lead to security breaches and financial losses. Furthermore, the skill gap often compels organizations to rely heavily on a small team of specialized professionals, creating a bottleneck in the threat detection and response process. This over-reliance on a limited workforce can result in fatigue and decreased productivity, which in turn can compromise the organization's cybersecurity posture.

To address the skill gap, organizations are exploring multiple avenues. Some are investing in comprehensive training programs aimed at upskilling their current workforce. Others are partnering with academic institutions to create specialized curricula that focus on CTI and cybersecurity at large. There is also a growing trend towards automation, where routine tasks are handled by algorithms, freeing up human experts to focus on more complex analyses. Despite these efforts, completely bridging the skill gap remains a long-term endeavor requiring coordinated action from industry stakeholders, educational institutions, and policy-makers. Until then, the skill gap will continue to be a significant hurdle in the effective deployment and utilization of CTI tools.

The effectiveness of Cyber Threat Intelligence (CTI) in safeguarding an organization's assets often hinges on the collective sharing of threat information among different entities. This is especially true in sectors like finance, where the interconnectedness of systems can lead to cascading vulnerabilities. A single compromised entity can pose risks to a wide array of participants in the financial ecosystem. Therefore, sharing CTI data across organizations, including competitors, is considered beneficial in preemptively identifying and mitigating threats. However, achieving this level of collaboration is fraught with challenges, primarily due to concerns over trust and the potential leakage of sensitive information. Organizations often hesitate to share crucial intelligence data for fear that it might expose their internal vulnerabilities or give competitors an undue advantage. This mistrust severely hampers the establishment of a cohesive defense against common threats.

The reluctance to share information is not unfounded, as the mishandling of shared CTI data can have dire consequences. For instance, the unauthorized dissemination of threat intelligence could potentially alert adversaries that their tactics have been discovered, thereby giving them the opportunity to adapt and become even more elusive. Additionally, CTI often contains information that is sensitive to business operations, including details on system architectures or internal protocols. Sharing such information indiscriminately could pose risks of corporate espionage or strategic disadvantage. Consequently, organizations face a complex dilemma: on one hand, collective intelligence can significantly bolster cybersecurity measures; on the other, sharing poses a myriad of risks that can be detrimental to individual entities.

Various mechanisms are being developed to facilitate secure and controlled information sharing. Initiatives such as Information Sharing and Analysis Centers (ISACs) are gaining

traction as trusted platforms where organizations can anonymously share and receive threat intelligence. Advanced cryptographic techniques are also being employed to allow for the secure exchange of sensitive information in a way that prevents unauthorized access. Additionally, legal frameworks and agreements are being explored to set the rules of engagement for CTI sharing, specifying the rights and responsibilities of each party involved. Despite these advancements, trust remains a critical factor that can only be built over time and through consistent, positive interactions among participating organizations.

Addressing Interoperability Challenges in CTI Adoption

Interoperability represents a significant barrier to the effective implementation of Cyber Threat Intelligence (CTI) within financial institutions, given the diversity of technologies and systems used across the sector. Overcoming this challenge requires a multi-faceted approach, starting with the adoption of standardized data formats and communication protocols. Financial institutions must align with global standards, such as Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII), which facilitate the seamless sharing of threat intelligence data. Moreover, leveraging Application Programming Interfaces (APIs) can enable better integration between disparate systems, allowing for real-time data flow and analysis across platforms. Middleware solutions, designed to bridge the gap between incompatible systems, can further enhance interoperability by enabling secure and efficient data exchange without the need for system overhauls. Collaborative industry-wide initiatives, such as those led by the Financial Services Information Sharing and Analysis Center (FS-ISAC), can also play a crucial role in addressing these challenges. By partnering with technology providers and participating in shared threat intelligence platforms, financial institutions can benefit from pooled resources and expertise. Case studies of successful interoperability implementations within the sector, such as the collaboration between major banks and cybersecurity firms, offer practical insights into how these solutions can be deployed effectively.

Balancing CTI Adoption Challenges with Mitigation Strategies

While the manuscript effectively highlights the challenges associated with CTI adoption, it is essential to balance these discussions by providing practical solutions to mitigate each issue. For instance, the problem of data overload can be addressed through the integration of advanced data analytics and machine learning technologies, which can automate the process of filtering and prioritizing alerts, thus reducing the risk of alert fatigue. These tools can distinguish between low-priority and critical threats, allowing cybersecurity teams to focus on the most pressing issues. Similarly, addressing the skill gap in CTI requires a combination of strategies, including developing internal training programs and forging partnerships with educational institutions to create specialized cybersecurity curricula. Automated tools, such as threat intelligence platforms (TIPs), can further augment human capabilities by streamlining the analysis and dissemination of threat data, thereby easing the burden on limited cybersecurity staff. Encouraging financial institutions to adopt a more collaborative approach, such as participating in joint training exercises and information-sharing networks, can also help mitigate these

challenges by fostering a community-driven defense against cyber threats. By providing clear, actionable recommendations, the manuscript can present a more optimistic outlook on the prospects of CTI adoption.

Conclusion

The application of Cyber Threat Intelligence (CTI) in financial institutions serves multiple purposes aimed at strengthening security measures and risk mitigation. One of the immediate benefits of utilizing CTI is threat awareness. Financial organizations have the capability to access real-time information concerning various types of cyber threats and attacks happening on a global scale. This empowers them to take pre-emptive measures to protect their systems and data, significantly reducing the probability of a successful attack. For instance, if there is a surge in ransomware attacks targeting similar institutions in another part of the world, local institutions can implement appropriate security measures before they become victims themselves.

In addition to real-time situational awareness, CTI proves invaluable in incident response protocols. When a cyber-attack occurs, the incident response team needs detailed information about the nature of the attack, the malware used, and the methods of intrusion [39], [40]. CTI provides this contextual information, aiding in faster and more accurate responses to cyber incidents. The intelligence gathered helps in understanding the tactics, techniques, and procedures (TTPs) used by the adversaries, which in turn aids in devising effective countermeasures. This is especially crucial in the financial sector where delays in resolving cyber incidents can lead to substantial financial losses and erode customer trust.

Strategic planning for future cybersecurity measures also benefits significantly from CTI. Intelligence on emerging threats and vulnerabilities enables financial institutions to plan and allocate resources wisely. These insights can be integrated into the broader risk management and strategic planning processes, leading to more informed decisions about investments in security technologies and human resources. For example, if the intelligence indicates an increase in advanced persistent threats (APTs) targeting financial applications, organizations can prioritize updating and fortifying those particular systems.

Compliance with regulations is another area where CTI provides an edge. Various regulatory frameworks such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States mandate proactive risk assessment and data protection measures. Industry-specific rules for the financial sector like the Payment Card Industry Data Security Standard (PCI DSS) also require rigorous cybersecurity protocols. CTI assists organizations in staying ahead of the regulatory requirements by identifying potential areas of non-compliance and suggesting improvements. In turn, this minimizes the risks of financial penalties and reputational damage resulting from regulatory violations.

The application of CTI extends even to specialized areas such as fraud detection and vendor risk management. By correlating transactional data with known indicators of fraud, CTI enhances

the ability of financial institutions to spot potentially fraudulent activities, thus safeguarding both institutional and customer assets. Moreover, financial institutions often rely on an intricate network of vendors for various services, ranging from cloud storage to payment processing. CTI can evaluate the security postures of these third-party vendors, helping institutions understand potential risks in their supply chain.

The utilization of Cyber Threat Intelligence (CTI) in financial institutions presents numerous challenges, each requiring careful consideration and strategic handling. A primary concern is data overload; the vast amount of data generated by CTI tools can be overwhelming for organizations. This often leads to "alert fatigue," where critical alerts may be ignored or overlooked due to the constant stream of notifications. This issue can be particularly pronounced in high-stakes environments like financial institutions, where missing a genuine alert can have significant economic and reputational ramifications.

Another notable challenge is interoperability among different systems within a financial organization's infrastructure. Financial institutions often use a multitude of systems and technologies, each with its own set of standards and formats. Integrating CTI solutions into such a heterogeneous environment can prove difficult. This complexity can impede the effective distribution and utilization of threat intelligence, thereby diminishing the potential security benefits. The issue is compounded when organizations want to share threat intelligence data across different platforms or with third parties, further complicating the already intricate architecture.

Financial constraints also pose a significant hurdle, particularly for smaller financial institutions. Advanced CTI solutions often come with a high price tag, both in terms of software and hardware requirements and ongoing maintenance. This can make the adoption of sophisticated CTI tools less feasible for smaller entities, leaving them potentially more vulnerable to cyber threats. Cost considerations can thus act as a deterrent to adopting CTI solutions, despite their obvious benefits in enhancing cybersecurity measures.

The challenge of a skills gap is a pervasive issue in the cybersecurity industry and is particularly relevant in the specialized field of CTI. Effective usage of CTI data requires a specific skill set that includes the ability to interpret complex datasets and make informed decisions based on them. The industry faces a shortage of professionals with these skills, and this gap can limit the effectiveness of CTI initiatives. Organizations may have access to advanced CTI tools but lack the in-house expertise to use them optimally, reducing the return on investment for such technologies.

Issues of accuracy and timeliness are essential to the effectiveness of CTI. False positives can lead to unnecessary allocation of resources and can desensitize security teams to alerts, whereas false negatives could result in ignored threats that materialize into actual attacks. Additionally, the rapid evolution of cyber threats necessitates that CTI be updated in real-time to retain its effectiveness. Alongside these operational challenges, there are broader concerns related to trust and information sharing among competing entities, and the potential regulatory issues

surrounding data sharing. Both trust and regulatory considerations add complexity to CTI adoption, sometimes acting as barriers to implementing a collaborative and efficient threat intelligence strategy.

References

[1] H. Jo, Y. Lee, and S. Shin, "Vulcan: Automatic extraction and analysis of cyber threat intelligence from unstructured text," *Comput. Secur.*, vol. 120, p. 102763, Sep. 2022.

[2] E. Kim, K. Kim, D. Shin, B. Jin, and H. Kim, "CyTIME: Cyber Threat Intelligence ManagEment framework for automatically generating security rules," *Proceedings of the 13th International*, 2018.

[3] D. Homan, I. Shiel, and C. Thorpe, "A New Network Model for Cyber Threat Intelligence Sharing using Blockchain Technology," in *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2019, pp. 1–6.

[4] J. Grisham, S. Samtani, M. Patton, and H. Chen, "Identifying mobile malware and key threat actors in online hacker forums for proactive cyber threat intelligence," in *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2017, pp. 13–18.

[5] Y. Kamat and S. Nasnodkar, "Advances in Technologies and Methods for Behavior, Emotion, and Health Monitoring in Pets," *Applied Research in Artificial Intelligence and Cloud Computing*, vol. 1, no. 1, pp. 38–57, 2018.

[6] H. Kure and S. Islam, "Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure," *J. Univers. Comput. Sci.*, 2019.

[7] F. Menges, C. Sperl, and G. Pernul, "Unifying Cyber Threat Intelligence," in *Trust, Privacy and Security in Digital Business*, 2019, pp. 161–175.

[8] H. M. Alzoubi *et al.*, "Cyber Security Threats on Digital Banking," in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, 2022, pp. 1–4.

[9] Y. Gao, X. Li, H. Peng, B. Fang, and P. S. Yu, "HinCTI: A cyber threat intelligence modeling and identification system based on heterogeneous information network," *IEEE Trans. Knowl. Data Eng.*, vol. 34, no. 2, pp. 708–722, Feb. 2022.

[10] Z. Li, J. Zeng, Y. Chen, and Z. Liang, "AttacKG: Constructing Technique Knowledge Graph from Cyber Threat Intelligence Reports," in *Computer Security – ESORICS 2022*, 2022, pp. 589–609.

[11] S. Samtani, K. Chinn, C. Larson, and H. Chen, "AZSecure Hacker Assets Portal: Cyber threat intelligence and malware analysis," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 2016, pp. 19–24.

[12] V. Wang, H. Nnaji, and J. Jung, "Internet banking in Nigeria: Cyber security breaches, practices and capability," *International Journal of Law, Crime and Justice*, vol. 62, p. 100415, Sep. 2020.

[13] D. Ghelani, T. K. Hua, and S. K. R. Koduru, "Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking," *Authorea Preprints*, 2022.

[14] K. Najaf, M. I. Mostafiz, and R. Najaf, "Fintech firms and banks sustainability: Why cybersecurity risk matters?," *J. Finan. Eng.*, vol. 08, no. 02, p. 2150019, Jun. 2021.

[15] G. Husari, X. Niu, B. Chu, and E. Al-Shaer, "Using Entropy and Mutual Information to Extract Threat Actions from Cyber Threat Intelligence," in *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2018, pp. 1–6.

[16] S. Smys and W. Haoxiang, "Data elimination on repetition using a blockchain based cyber threat intelligence," *IRO Journal on Sustainable Wireless*, 2021.

[17] J. Zhao, Q. Yan, J. Li, M. Shao, Z. He, and B. Li, "TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data," *Comput. Secur.*, vol. 95, p. 101867, Aug. 2020.

[18] D. Shackleford, "Cyber threat intelligence uses, successes and failures: The sans 2017 cti survey," *SANS Institute*, 2017.

[19] A. Shah and S. Nasnodkar, "A Framework for Micro-Influencer Selection in Pet Product Marketing Using Social Media Performance Metrics and Natural Language Processing," *Journal of Computational Social Dynamics*, vol. 4, no. 4, pp. 1–16, 2019.

[20] S. Samtani, R. Chinn, H. Chen, and J. F. Nunamaker, "Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence," *Journal of Management Information Systems*, vol. 34, no. 4, pp. 1023–1053, Oct. 2017.

[21] J. Kotsias, A. Ahmad, and R. Scheepers, "Adopting and integrating cyber-threat intelligence in a commercial organisation," *European Journal of*, 2023.

[22] N. Arnold *et al.*, "Dark-Net Ecosystem Cyber-Threat Intelligence (CTI) Tool," in *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2019, pp. 92–97.

[23] R. Brown and R. M. Lee, "2021 SANS Cyber Threat Intelligence (CTI) Survey," *Tech. Rep*, 2021.

[24] P. Ranade, A. Piplai, S. Mittal, A. Joshi, and T. Finin, "Generating Fake Cyber Threat Intelligence Using Transformer-Based Models," in *2021 International Joint Conference on Neural Networks (IJCNN)*, 2021, pp. 1–9.

[25] Y. Zhou, Y. Tang, M. Yi, C. Xi, and H. Lu, "CTI View: APT Threat Intelligence Analysis System," *Security and Communication Networks*, vol. 2022, Jan. 2022.

[26] S. Ainslie, D. Thompson, S. Maynard, and A. Ahmad, "Cyber-threat intelligence for security decision-making: A review and research agenda for practice," *Comput. Secur.*, vol. 132, p. 103352, Sep. 2023.

[27] V. Mavroeidis and S. Bromander, "Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence," in *2017 European Intelligence and Security Informatics Conference (EISIC)*, 2017, pp. 91–98.

[28] R. Brown and R. M. Lee, "The evolution of cyber threat intelligence (cti): 2019 sans cti survey," 2019.

[29] I. Linkov and A. Kott, "Fundamental Concepts of Cyber Resilience: Introduction and Overview," in *Cyber Resilience of Systems and Networks*, A. Kott and I. Linkov, Eds. Cham: Springer International Publishing, 2019, pp. 1–25.

[30] H. Vijayakumar, "Unlocking Business Value with AI-Driven End User Experience Management (EUEM)," in *2023 5th International Conference on Management Science and Industrial Engineering*, 2023, pp. 129–135.

[31] N. Sun *et al.*, "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1748–1774, thirdquarter 2023.

[32] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions," *Comput. Secur.*, vol. 87, p. 101589, Nov. 2019.

[33] D. Schlette, F. Böhm, M. Caselli, and G. Pernul, "Measuring and visualizing cyber threat intelligence quality," *Int. J. Inf. Secur.*, vol. 20, no. 1, pp. 21–38, Feb. 2021.
[34] A. Shah and S. Nasnodkar, "The Impacts of User Experience Metrics on Click-Through Rate (CTR) in Digital Advertising: A Machine Learning Approach," *Sage Science Review of Applied Machine Learning*, vol. 4, no. 1, pp. 27–44, 2021.
[35] W. by R. Lee, "2020 SANS Cyber Threat Intelligence (CTI) Survey," *Tech. Rep*, 2020.
[36] M. Parmar and A. Domingo, "On the Use of Cyber Threat Intelligence (CTI) in Support of Developing the Commander's Understanding of the Adversary," in *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, 2019, pp. 1–6.
[37] Y. Kamat and S. Nasnodkar, "Empirical Investigation of the Impact of 3D Printing on Multiple Dimensions of Student Engagement in STEM Education," *Journal of Empirical Social Science Studies*, vol. 5, no. 1, pp. 48–73, 2021.
[38] H. Vijayakumar and A. Seetharaman, "Impact of AIServiceOps on Organizational Resilience," *2023 15th International*, 2023.
[39] S. Samtani, M. Abate, V. Benjamin, and W. Li, "Cybersecurity as an industry: A cyber threat intelligence perspective," *The Palgrave Handbook of*, 2020.
[40] G. Sakellariou, P. Fouliras, I. Mavridis, and P. Sarigiannidis, "A Reference Model for Cyber Threat Intelligence (CTI) Systems," *Electronics*, vol. 11, no. 9, p. 1401, Apr. 2022.