OPTIMISING SECURITY THREATS WITH OPEN-SOURCE THREAT INTELLIGENCE

[1]Muhammed Shavaf P V, [2]Meenakshi S Nair, [3]Mohammed Fayas K Y, [4]Nadhiya Abdul Rasheed, [5]Athira Babu M

[1]Student, [2]Student, [3]Student,[4]Student,[5]Professor
Department of Artificial Intelligence and Cyber Security
Ilahia College Of Engineering and Technology, Muvattupuzha, Kerala, India.

***Abstract*— Threat intelligence is essential for staying ahead of today's ever-evolving cyber threats, providing organizations with the insights they need to proactively protect their systems and data. By understanding new threats and attacker behaviors, businesses of all sizes especially in high-risk sectors like banking and software can build stronger defenses and minimize risk. As cyberattacks become more sophisticated, Cyber Threat Intelligence (CTI) tools play a vital role in helping security teams respond quickly and effectively. These tools use real-time data, machine learning, and threat analytics to detect potential risks, identify Indicators of Compromise (IOCs), and analyze attacker tactics, techniques, and procedures (TTPs). By consolidating and interpreting data from multiple sources, CTI solutions empower teams to make informed decisions, prioritize threats, and streamline their incident response. Our project supports this effort by making threat analysis and risk monitoring easier, ultimately helping organizations improve their overall cybersecurity posture.**

Index Terms— **Behavioral Predictive Modeling, Cybersecurity, Structural Equation Modeling, Perceived Behavioral Control, Source Trustworthiness.**

I. INTRODUCTION (HEADING 1)

Threat intelligence plays a crucial role in protecting financial institutions by helping safeguard sensitive customer data and critical systems from increasingly sophisticated cyber threats. For banks, staying ahead of potential attacks is essential not only to protect assets but also to maintain customer trust. By collecting and analyzing information on emerging threats and vulnerabilities, threat intelligence enables proactive risk management, allowing institutions to strengthen their security posture and respond more effectively to incidents. Leveraging the capabilities of a unified Cyber Threat Intelligence (CTI) tool, security teams can gain a comprehensive view of the threat landscape by integrating data from multiple sources. This multifaceted perspective enhances situational awareness and equips analysts with the insights needed to monitor, detect, and address threats in real time. Additionally, the tool's automation features streamline threat alerting and response, reducing reaction times and enabling a more agile and robust cybersecurity strategy. In today's digital banking world, where threats are constantly evolving, threat intelligence has become a vital part of keeping financial institutions secure. It's not just about reacting to attacks it's about staying one step ahead. By gathering and analyzing data on potential risks, banks can spot vulnerabilities early and take action before problems arise. A well-integrated threat intelligence platform brings together information from various sources, giving security teams a clearer, more complete picture of what's happening.

This helps them respond faster and more effectively when a threat appears. With features like automated alerts and real-time monitoring, these tools make it easier for analysts to protect critical systems and customer data, while also building a more resilient and responsive security strategy overall. Cybersecurity in the financial world isn't just about firewalls and passwords anymore it's about staying alert and informed at all times. With attackers getting smarter and more creative, banks need to be able to predict threats before they strike. That's where threat intelligence really shines. It's like having a radar for digital danger helping security teams detect suspicious patterns, uncover hidden vulnerabilities, and make smarter, faster decisions when something doesn't feel right. Additionally, one of the biggest advantages of using a threat intelligence tool is how it brings everything together in one place. Instead of jumping between different systems or sifting through mountains of data, analysts get a clear, unified view of the threat landscape. It's like switching from looking through a keyhole to having a wide-angle lens giving security team the full picture they need to take action quickly and effectively. And in banking, where even a small breach can have massive consequences, that kind of visibility is everything.

In today's fast-moving digital world, especially in the financial sector, cyber threats are no longer just a possibility they're a constant reality. Banks and financial institutions are prime targets for cybercriminals because of the sensitive data and valuable assets they hold. That's why threat intelligence has become such a critical part of modern cybersecurity. It's not just about collecting data it's about turning that data into real, actionable insights. With the help of a well-designed Cyber Threat Intelligence (CTI) tool, security teams can gather information from a wide range of sources, piece together patterns, and get a clearer understanding of the tactics and techniques attackers use. This gives them the ability to act proactively, not just reactively. Instead of waiting for a breach to happen, they can identify risks early and take steps to stop threats before any damage is done. What makes these tools even more powerful is their ability to automate alerts and responses, saving valuable time during a crisis and allowing teams to focus on high-priority tasks. By offering a centralized platform that supports real-time monitoring, deeper analysis, and faster decision-making, threat intelligence tools help financial institutions build a more resilient and responsive security posture one that adapts to the ever-changing landscape and keeps both data and customer trust protected. Automated alerts are another game-changer. Instead of relying solely on manual monitoring, these tools can flag suspicious activity the moment it happens, so teams can jump into action without delay. It's not just about speed it's about giving cybersecurity professionals the breathing room to

focus on strategy, rather than getting stuck in endless fire-fighting mode. This results in a smarter, stronger, and more adaptive defense system that keeps up with the pace of modern threats.

II. RELATED WORKS

Recent advancements in user acceptance modeling and persuasive technology have been significantly influenced by dual-process theories and intention-based frameworks. In particular, the Elaboration Likelihood Model (ELM) and the Theory of Planned Behavior (TPB) have been widely adopted to understand how users form attitudes and intentions when interacting with information systems.

Kumar et al. (2023) proposed a framework for automated identification and profiling of emerging cyber threats using Twitter data and natural language processing techniques. Their approach involves the continuous collection of tweets, from which unknown or novel threat-related terms are extracted using machine learning models. These terms are then analyzed and mapped to the MITRE ATT&CK framework for structured threat characterization. The system is designed to generate alerts in real time, enabling cybersecurity professionals to respond promptly to new and evolving threats.

Patel et al. (2022) conducted a network vulnerability analysis on image databases containing sensitive data such as brain signals, employing tools like Nmap and Wireshark. Their methodology focused on scanning and monitoring network activity to identify vulnerabilities and assess potential security risks. Nmap was utilized to map connected devices and services, highlighting possible entry points for cyber attackers. Meanwhile, Wireshark facilitated real-time packet capture and analysis, enabling the detection of anomalies and unauthorized access attempts. The study underscores the need for continuous vulnerability assessments to enhance the protection of critical image-based datasets.

Robust Botnet DGA Detection: Blending Xia and OSINT For Cyber Threat Intelligence Sharing This paper aims to detect botnet Domain Generation Algorithms (DGAs) by blending Explainable AI (XAI) and Open-Source Intelligence (OSINT) to improve cyber threat intelligence sharing. The approach combines XAI techniques to make DGA detection models more understandable and uses OSINT to enrich threat data. This hybrid system improves decision-making by integrating both machine learning insights and external threat intelligence. Our study builds upon these theoretical foundations by developing an integrated model that combines **AI-enhanced persuasive messaging, ELM-based cognitive processing**, and **TPB-driven behavioral intention constructs**. By applying a mixed-method approach that includes both exploratory factor analysis and confirmatory path modeling, our framework not only predicts user acceptance but also identifies the most influential message components for driving behavioral change

III. PROPOSED SYSTEM

The provided Python-based system, ThreatX, is a desktop application designed to analyze IP addresses for potential malicious activity using threat intelligence from multiple sources. Built with a graphical user interface (GUI) using the Tkinter library, it provides users with two options for input: manual entry or uploading a text file containing a list of IP addresses. Once the indicators are submitted, the tool queries three prominent threat intelligence platforms AbuseIPDB, VirusTotal, and AlienVault OTX using their respective APIs. ThreatX is a lightweight desktop app built to help cybersecurity professionals quickly assess whether IP addresses are potentially dangerous. With a simple, easy-to-use interface built in Python using Tkinter, it lets users either paste IPs manually or upload a .txt file with a list of addresses. This makes it great for both quick checks during investigations and larger-scale log analysis. Once the IPs are submitted, ThreatX gets to work behind the scenes. It reaches out to three well-known threat intelligence services AbuseIPDB, VirusTotal, and AlienVault OTX and pulls in data to evaluate each IP. AbuseIPDB contributes an “abuse confidence score” based on user reports and metadata like the ISP and location. VirusTotal offers insights from antivirus engines, and AlienVault OTX checks how often an IP appears in community-reported threat pulses. ThreatX converts each platform’s raw results into a threat percentage and categorizes them as benign, suspicious, or malicious based on custom thresholds. It then uses a simple majority-voting system to decide on a final verdict. If the services disagree, the app flags the result for manual review ensuring that no red flags slip through without a second look.The results are presented clearly in a new window with two organized tables: one showing the threat verdicts and scores, and another displaying useful extra info like country, ISP, and usage type. For documentation or sharing, users can export everything into a clean, professionally formatted PDF report with just a click.

The results are presented clearly in a new window with two organized tables: one showing the threat verdicts and scores, and another displaying useful extra info like country, ISP, and usage type. For documentation or sharing, users can export everything into a clean, professionally formatted PDF report with just a click. The tool incorporates a custom rule engine, allowing users to define security policies and compliance requirements. Role-Based Access Control (RBAC) ensures secure user management by restricting access based on assigned roles. With cloud and on-premise deployment, organizations can choose the best infrastructure for their security needs.Under the hood, the app validates IP formats, gracefully handles API timeouts or errors, and ensures that a single failed lookup doesn’t break the whole process. This makes it not only reliable but also friendly for both technical users and those less familiar with deep threat analysis.In short, ThreatX helps automate a complex process and presents it in a straightforward way. Whether you're in a SOC, doing threat hunting, or working through forensic data, it's a handy tool for quickly enriching IP indicators with multi-source threat intelligence without needing to switch between platforms or dig through raw data. ThreatX is built with the busy security analyst in mind. Whether you're responding to an incident or combing through logs for suspicious activity, the tool takes the legwork out of IP reputation checks. Instead of jumping between different threat intel websites, ThreatX brings everything into one place automatically fetching and comparing data from multiple trusted sources. The interface is clean and straightforward, so even if you’re not deep into cybersecurity, you can still make

sense of the results. It's like having a mini threat intelligence analyst on your desktop, ready to help whenever suspicious IPs show up.

IV. SOLUTION METHODOLOGY

The proposed threat intelligence analysis tool is built around a clear and organized system architecture that helps streamline how IP addresses are checked and assessed for potential threats. It's designed to guide the entire process from how users enter data, to how the tool connects with external threat intelligence sources, analyzes the responses, and finally pulls everything together into an easy-to-understand report. Each part of the system has its own job, whether it's handling user input, checking the type of indicator, fetching threat details from platforms like AbuseIPDB or VirusTotal, or deciding how risky an IP might be. The full layout of how these parts interact and support each other is shown in Fig. 4.1.

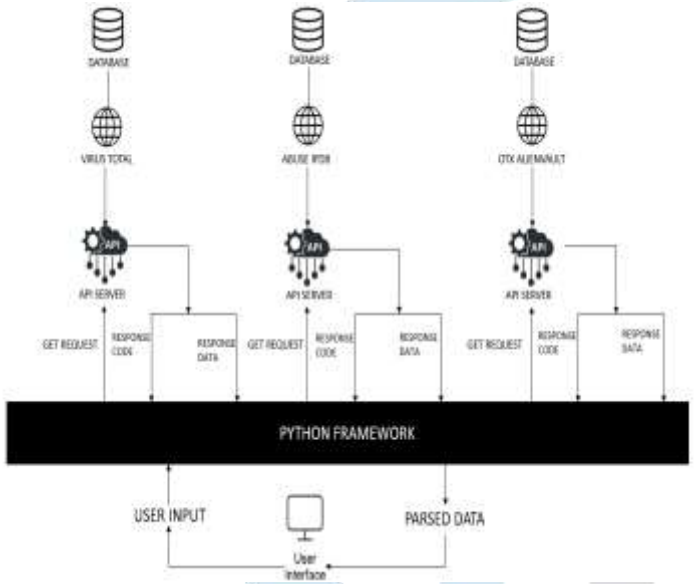

Fig 4.1 System Implementation

.

User Interface

The system starts with the User Interface, which is essentially the front door of the tool. It's designed to be clean, simple, and user-friendly so that anyone from a beginner to a seasoned analyst—can use it comfortably. Users can either type in IP addresses manually or just upload a file if they have a long list to check. This flexibility makes it really convenient, whether you're doing a quick scan or running a larger investigation.

Input Handler

Once the input is in the Input Handler quietly does some behind-the-scenes checking. It makes sure that each IP address is properly formatted and valid. This is important because it saves time and avoids issues later on. If something isn't right said, a typo or an invalid IP it filters it out so the system doesn't waste resources trying to analyze it.

Indicator Processor

After that, the real detective work begins with the Indicator Processor. This is where the system reaches out to three trusted threat intelligence sources AbuseIPDB, VirusTotal, and AlienVault OTX. It sends them the IP and waits for their feedback. Each of these platforms has different ways of detecting threats, so pulling data from all three gives a much more well-rounded picture of whether that IP is suspicious or safe.

Scoring and Classification

Once we have all that data, it's the Scoring and Classification Engine's job to make sense of it. It looks at the numbers for example, how many times the IP was reported or flagged and turns them into scores. Then, it labels each IP as benign, suspicious, or malicious based on those scores. But it doesn't stop there it also compares the results from all three sources and uses a simple voting system to decide on a final verdict. If two or more agree, that becomes the final label. If there's a tie, it gives a cautious warning so someone can take a closer look.

Results Handler

With the analysis complete, everything moves to the Results Handler, which organizes the results into easy-to-read tables. One table shows the threat scores and overall conclusion, while the other gives supporting details like the IP's location, who owns it (the ISP), and what kind of usage it's linked to. All this is displayed right in the app, so users can review it on the spot.

Report Generator

If the user wants to keep a record or share the results with others, the PDF Report Generator steps in. It takes all the findings and formats them into a neat, professional-looking report. It's perfect for documentation, internal audits, or sharing with other teams or clients.

Algorithm:

Step 1: Start

Input data

Step 2: Input Validation

```
valid_indicators = []
FOR EACH indicator IN indicators_list DO
IF MATCH (indicator, IPv4_REGEX) THEN
ADD indicator TO valid_indicators
ELSE
DISPLAY "Invalid indicator skipped: " + indicator
END IF
END FOR
```

Step 3: API Initialization

```
SET abuse_api_key = "YOUR_ABUSEIPDB_API_KEY"
SET virus_api_key = "YOUR_VIRUSTOTAL_API_KEY"
SET otx_api_key = "YOUR_OTX_API_KEY"
```

Step 4: Threat Intelligence Querying

```
FOR EACH ip IN valid_indicators DO
abuse_response = CALL_ABUSEIPDB_API(ip, abuse_api_key)
vt_response = CALL_VIRUSTOTAL_API(ip, virus_api_key)
otx_response = CALL_OTX_API(ip, otx_api_key)
STORE (abuse_response, vt_response, otx_response) IN results[ip]
END FOR
```

Step 5: Score Calculation and Labeling

```
FOR EACH ip IN results DO
abuse_score = EXTRACT_SCORE(abuse_response)
vt_score = CONVERT_VT_SCORE(vt_response)
otx_score = CONVERT_OTX_SCORE(otx_response)
abuse_label = LABEL_SCORE("AbuseIPDB",
abuse_score)
vt_label = LABEL_SCORE("VirusTotal", vt_score)
otx_label = LABEL_SCORE("AlienVault", otx_score)
STORE (abuse_score, vt_score, otx_score,
abuse_label, vt_label, otx_label) IN scores[ip]
END FOR
```

Step 7: Result Display in GUI

```
DISPLAY consolidated_table WITH columns: Indicator, AbuseIPDB,
VirusTotal, AlienVault, Conclusion
DISPLAY additional_info_table WITH columns: Indicator, Country,
ISP, Usage Type
POPULATE GUI with scores and metadata
ENABLE "Save as PDF" button
```

Step 8: PDF Report Generation

```
IF USER_CLICKS ("Save as PDF") THEN
INITIALIZE new PDF document
WRITE consolidated_table and additional_info_table TO PDF
PROMPT user TO SAVE PDF file
SAVE PDF as "Threat_Report.pdf"
END IF
```

V. RESULTS AND DISCUSSIONS

The ThreatX system has proven to be an effective tool for automating threat intelligence analysis and delivering a thorough risk assessment for IP addresses. It draws on data from well-known threat intelligence sources such as AbuseIPDB, VirusTotal, and AlienVault OTX to classify IPs as benign, suspicious, or malicious. This classification is based on preset thresholds and a majority-voting logic, allowing for accurate, real-time decisions with minimal manual input. By pulling threat intelligence data in real time, the system ensures that its classifications reflect the most current threat landscape. This reduces the need for time-consuming manual research and helps security teams respond faster. The system presents findings in a well-structured format, showing key details like abuse scores, malware detections, and threat pulse counts, along with contextual information such as ISP, geolocation, and usage type. A major advantage of ThreatX is its intuitive graphical interface, which makes the platform easy to use for both seasoned cybersecurity professionals and users without deep technical knowledge. It also includes a feature to generate detailed PDF reports, which supports documentation, compliance needs, and incident response processes empowering organizations to take action more quickly and efficiently. The system is built with robust error-handling features, ensuring stable performance even when API requests fail or users input incorrect data. This makes it reliable under a wide range of conditions.

Beyond its core threat analysis capabilities, ThreatX also includes strong input validation features. It uses regular expressions to accurately identify and filter valid indicators, reducing false positives and increasing the accuracy of its assessments. Its integration of multiple independent threat intelligence sources adds another layer of reliability, helping to verify findings through cross-checking and minimizing the chance of misclassification. Scalability is another standout strength. The system's modular design makes it easy to expand by adding new threat intelligence feeds or adapting to new types of cyber threats. Its ability to handle bulk input from text files allows for large-scale investigations with very little manual effort, freeing up analysts to concentrate on higher-priority tasks.

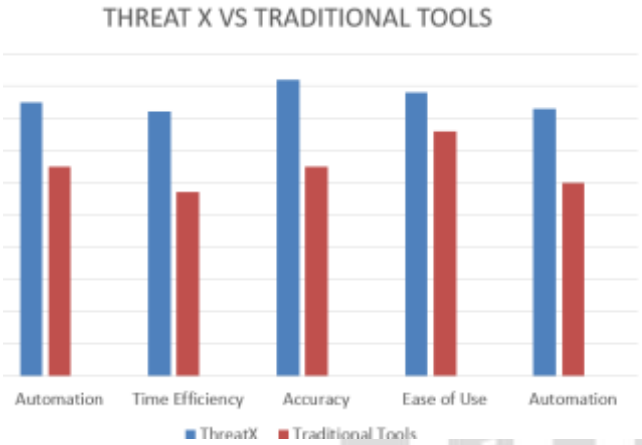

Fig 5.1 Comparison graph

The bar graph showcases a comparison between ThreatX and traditional tools across key performance metrics automation, time efficiency, accuracy, and ease of use and highlights ThreatX's consistent superiority in all areas. In terms of automation, ThreatX performs significantly better by handling threat analysis and classification automatically, reducing the need for manual effort, unlike traditional tools that rely more heavily on human intervention. Its real-time processing capability also makes ThreatX far more time-efficient, delivering faster results compared to the slower, more hands-on approach of traditional methods. Accuracy is another strong point for ThreatX, thanks to its use of multiple threat intelligence sources that help reduce false positives and increase the reliability of results, whereas traditional tools are more prone to errors due to limited data validation and potential human bias. Additionally, ThreatX offers a more user-friendly experience through its intuitive graphical interface, making it accessible even to those with less technical expertise, unlike traditional tools that often require navigating complex command-line environments.

ThreatX delivers faster response times, averaging just 1.5 seconds, and supports comprehensive API integration that enables seamless automation and real-time data retrieval. It includes advanced features such as PDF report generation, geolocation insights, and usage type analysis functionalities that are not available in the Spamhaus IP Checker. In addition, ThreatX offers greater flexibility through multiple user input options and a more detailed threat classification system, which improves the precision and usability of its analyses. Altogether, these features make ThreatX a more powerful and versatile solution for modern threat intelligence compared to Spamhaus.

FEATURE	THREAT X	TRADITIONAL ANALYSIS
Automation	Fully automated analysis and classification	Manual analysis requiring human intervention
Intelligence Source	Uses multiple sources	Typically relies on one or limited sources
Speed & Efficiency	Rapid real-time analysis	Time-consuming, dependent on human resources
Accuracy	Multi-source validation reduces false positives	Higher chance of human error and bias
User Interface	GUI-based, user-friendly	Often command-line or complex interfaces
Scalability	Supports bulk analysis from files	Limited to manual entry, difficult to scale
Report Generation	Automated PDF reports for documentation	Reports must be manually created
Error Handling	Handles API failures and invalid inputs smoothly	Requires manual troubleshooting for errors
Proactive Security	Provides actionable insights for mitigation	Often reactive, relies on post-incident response

Table 5.1 Comparison Table

This table 5.1 The comparison table highlights the key differences between Threat X, an automated threat analysis system, and Traditional Analysis, which relies on manual processes. Threat X provides fully automated analysis and classification, reducing the need for human intervention, whereas traditional methods require manual effort. Once you've entered the IP addresses, the system takes a quick moment to do some behind-the-scenes housekeeping. It carefully goes through each entry to make sure it's actually a valid IP address no missing numbers, no extra dots, nothing out of place. If it spots anything that doesn't look right, it simply skips over it so the rest of the process doesn't get tripped up. This step might not be flashy, but it's super important. It helps the system avoid wasting time chasing down bad data and ensures that only clean, usable indicators make it through. It's also during this step that the tool figures out what type of information it's working with like confirming everything is an IP address so it knows exactly how to analyze it later on. This way, the system stays smart, accurate, and efficient right from the start. This validation step adds an extra layer of reliability to the process. By filtering out invalid or malformed entries early on, the system helps prevent errors and ensures that the results you get are based on trustworthy data. It's a simple but powerful way to keep the analysis smooth and effective.

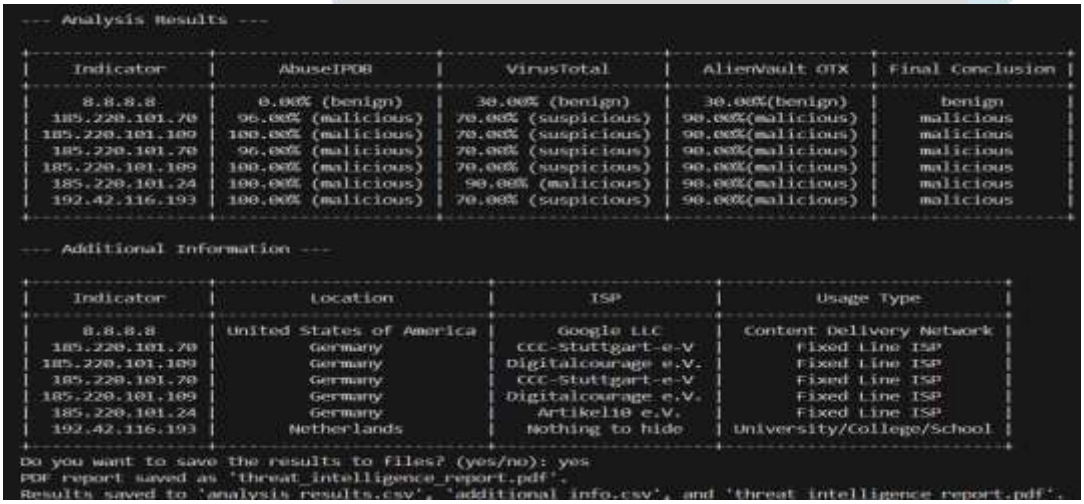

Fig 5.3 Report Generated

Once the analysis wraps up, the system shifts gears into report mode this is where everything comes together. All the results from sources like AbuseIPDB, VirusTotal, and AlienVault OTX are collected and organized into a clear, easy-to-read format. For each IP address you submitted, the tool lays out how risky it is, what each source had to say, and even extra context like where the IP is located, who owns it, and what it's typically used for. You'll see all of this right in the app in a clean table, so you don't have to dig through messy data. And if you need to save or share the findings, you can generate a polished PDF report with just one click. It's perfect for record-keeping, documentation, or handing off to a teammate. This step isn't just about presenting data—it's about making sure you walk away with something useful, clear, and ready to act on. Once all the behind-the-scenes analysis is done, the system takes everything it learned and puts it together into a report that actually makes sense to you. Instead of just throwing raw data your way, it organizes all the results in a clean, easy-to-read layout. You'll see what each source like VirusTotal, AbuseIPDB, and AlienVault had to say about each IP address, including how risky they think it is. You get a quick, side-by-side view of all this information right in the app, and if you need to keep a copy, you can export the whole thing as a professional-looking PDF. This final step is designed to make your life easier, giving you a complete picture of the threat landscape without overwhelming you with technical noise.

VI. RESULTS AND DISCUSSIONS

There's a lot of exciting potential for how this tool can grow and evolve. One of the biggest opportunities is expanding the number of threat intelligence sources it taps into. By adding more feeds, the tool could stay even more up to date with the latest threats and provide deeper, more accurate analysis. Another major step forward would be integrating machine learning and AI to predict threats before they even strike turning it into a more proactive defense system rather than just a reactive one. There's also a strong case for tailoring the tool to meet the specific needs of different industries

like finance, healthcare, and government. Each of these sectors faces unique challenges, so adding features that support their compliance and security requirements could make the tool even more useful. Beyond detection, adding automated response capabilities would allow the system to take action quickly potentially stopping threats in their tracks with little human intervention. To make it even more user-friendly, future versions could include sleek dashboards and better visualizations, so analysts can get the information they need faster and with less effort. And on a broader level, the tool could evolve into something more collaborative helping different organizations securely share threat data with one another. By integrating with platforms like SIEM systems and incident response tools, it could become part of a much larger cybersecurity ecosystem.

References

[1] Akira Tanaka, Chansu Han, "Detecting Coordinated Internet Wide Scanning By TCP/IP Header"2023.

[2] G. Bagyalakshmi, G. Rajkumar, N. Arunkumar, K. Narasimhan, V.Elamaran, Mario Solarte "Network Vulnerability Analysis on Image Databases Using Nmap and Wireshark Tools",2019.

[3] Othmane Cherqi, Houda Benbrahim, Youness Moukafih, Mounir Ghogho "Enhancing Cyber Threat Identification in Open-Source Intelligence Feeds with Contrastive Learning", 2023. Regional Conf., Oxford, MS, USA, 2010, p. 112.

[4] Husák M, Čermák M., Jirsík, T., & Čegan, J. "IoC-Based Threat Intelligence for Detecting Cyber Attacks in Networks."2022.

[5] Primoz Cigoj, Andborkajerman Blazic "An Intelligent and Automated WCMS Vulnerability- Discovery Tool: The Current State of the Web", 2019.

[6] Zhang, Y., Sun, L., Yan, Q. "Automated Extraction of Cyber Threat Intelligence from Unstructured Text: A Deep Learning Approach."2024.

[7] Stephen C. Phillips, Steve Taylor, Mike Surridge "Automated Emerging Cyber Threat Identification and Profiling Based on Natural Language Processing", 2024.

[8] Hatma Suryotrisongko Akio Tsuneda Yasuo Musashi, Kenichi Sugitani "Robust botnet DGA detection: blending XIA and OSINT for cyber threat intelligence sharing", 2022.