Emerging Cyber Threat Identification and Profiling: An Automated Approach with NLP

[1]V.Sai Sri Keerthi, [2]N.Akshaya, [3]Y.Srija, [4]Dr. G. Jawaherlal Nehru
[1,2,3]UG Scholar, Department of Computer Science and Engineering, St. Martin's Engineering College,
Secunderabad, Telangana, India, 500100
[4]Associate Professor, Department of Computer Science and Engineering, St. Martin's Engineering College,
Secunderabad, Telangana, India, 500100
gjnehruceg33@gmail.com

Abstract:

Cyber threats continue to evolve, posing significant risks to organizations across various sectors. As attackers adopt more advanced tactics, traditional cybersecurity measures often fall short in effectively identifying and mitigating emerging threats. To proactively address these threats, we propose EMERGING CYBER THREAT IDENTIFICATION AND PROFILING which presents an automated approach to emerging cyber threat identification and profiling using Natural Language Processing (NLP) to analyze large volumes of open-source intelligence (OSINT) data from various sources, including social media platforms, online forums, news articles, and threat intelligence feeds. By employing advanced NLP techniques, the system can extract and categorize threat-related information, to detect potential threats, profile attackers, and provide actionable insights, enhancing the capabilities of cybersecurity teams to respond proactively to cyber incidents. Through the integration of machine learning algorithms, the system continuously learns from new data inputs, enhancing its accuracy and efficacy over time. This adaptive approach ensures that organizations can stay ahead of evolving threats, making informed decisions based on timely and actionable insights. Cyber threats continue to evolve, posing significant risks to organizations across various sectors. As attackers adopt more advanced tactics, traditional cybersecurity measures often fall short in effectively identifying and mitigating emerging threats. To proactively address these threats, we propose EMERGING CYBER THREAT IDENTIFICATION AND PROFILING which presents an automated approach to emerging cyber threat identification and profiling using Natural Language Processing (NLP) to analyze large volumes of open-source intelligence (OSINT) data from various sources, including social media platforms, online forums, news articles, and threat intelligence feeds.

Keywords: Cyber threats, threat identification, threat profiling, NLP, OSINT, machine learning, threat detection, cybersecurity, attacker profiling, actionable insights.

1. INTRODUCTION

With the increasing reliance on the Internet for business, governance, and social interactions, cybersecurity threats have become a critical concern. Cyberattacks pose significant risks to organizations, governments, and individuals, making it essential to develop strategies for identifying and mitigating these threats. Cyber threat intelligence is a key component in cybersecurity, aiming to provide organizations with timely and actionable insights to protect their systems and data. It involves the collection, analysis, and dissemination of threat information to help organizations proactively detect, prevent, and respond to cyber threats. The primary objective of cyber threat intelligence is to enhance security posture by reducing uncertainty and enabling informed decision-making. By leveraging intelligence from structured and unstructured sources, organizations can identify attack patterns, assess vulnerabilities, and implement effective defense mechanisms. This intelligence aids in the detection of indicators of compromise (IOCs), tactics, techniques, and procedures (TTPs) used by threat actors, and facilitates predictive threat analysis to preemptively counter cyber threats.

Additionally, cyber threat intelligence helps in understanding the motives, capabilities, and strategies of adversaries. This intelligence provides insights into different types of cyber threats, such as malware, phishing campaigns, ransomware attacks, and advanced persistent threats (APTs). By analyzing past incidents and tracking threat actor behavior, organizations can enhance their threat modeling and risk assessment methodologies, enabling a proactive security approach.

Threat intelligence platforms (TIPs) and frameworks like the MITRE ATT&CK and STIX/TAXII standards facilitate the structured exchange of threat intelligence, allowing security teams to coordinate efforts in real-time. Furthermore, cyber threat intelligence supports regulatory compliance and legal frameworks by providing the necessary data to meet cybersecurity mandates and standards, such as the General Data Protection Regulation (GDPR), National Institute of Standards and Technology (NIST) cybersecurity framework, and ISO 27001. Ensuring compliance with these regulations helps organizations maintain trust, mitigate legal risks, and prevent financial losses resulting from cyber incidents.

2. LITERATURE SURVEY

Cyber threat identification and profiling have become essential aspects of modern cybersecurity research. Automated systems utilizing artificial intelligence, machine learning, and natural language processing have proven effective in detecting, analyzing, and categorizing cyber threats. Several studies have explored methodologies for extracting intelligence from structured sources such as security databases and incident reports, while others have focused on unstructured sources like dark web forums and social media platforms. Integrating these intelligence sources enables organizations to develop a comprehensive understanding of cyber threats and fortify their defenses.

The use of behavioral analytics has significantly improved threat profiling. By examining patterns in cyberattack data, researchers have been able to categorize adversaries based on tactics, techniques, and procedures (TTPs). The MITRE ATT&CK framework has been widely adopted to classify adversary behaviors and predict potential attack vectors. Recent studies highlight the effectiveness of AI-driven cybersecurity tools in profiling cybercriminals, enhancing proactive defense strategies, and reducing response time to incidents.

Various automated threat detection systems, such as SIEM and SOAR platforms, leverage AI and ML models to streamline threat Despite these advancements, challenges remain in the automation of cyber threat intelligence. False positives, adversarial machine learning attacks, and data overload continue to hinder efficient threat detection. Studies have explored countermeasures such as adversarial resilience in AI models and enhanced filtering mechanisms to refine threat intelligence. Additionally, blockchain technology has been proposed as a solution for securing threat intelligence data exchanges and ensuring data integrity across distributed networks. The future of cyber threat intelligence lies in the continued refinement of automation techniques. Real-time intelligence sharing, federated learning, and enhanced data privacy measures are emerging as key focus areas for research. The integration of blockchain for decentralized threat intelligence sharing and homomorphic encryption

Through a review of these works, it is evident that automation plays a crucial role in cyber threat identification and profiling. Ongoing research in AI-driven cybersecurity solutions, integration of predictive analytics, and advancements in secure data-sharing mechanisms will be instrumental in strengthening cyber resilience. The development of dynamic and adaptive threat intelligence models remains a top priority for cybersecurity researchers, ensuring organizations remain well-equipped to handle evolving cyber threats.

The digital realm faces an ever-evolving barrage of cyber threats, necessitating increasingly sophisticated methods for identification and profiling. Central to this pursuit is the integration of machine learning, which has fundamentally reshaped the landscape of cyber defense. Traditional signature-based detection systems are proving inadequate against the polymorphic nature of modern attacks, leading researchers to explore the potential of statistical anomaly detection. Early efforts in this area laid the groundwork, but the sheer volume and complexity of contemporary network traffic demanded more robust solutions.

Consequently, supervised learning algorithms, such as Support Vector Machines and Random Forests, have become indispensable tools for classifying network activity as either benign or malicious. Complementing these techniques, unsupervised learning methods, including K-means and DBSCAN, enable the identification of anomalous behavior without relying on pre-labeled data. The advent of deep learning has further propelled the field forward, with Recurrent Neural Networks and Long Short-Term Memory networks demonstrating exceptional capabilities in capturing the temporal dependencies inherent in network traffic. This ability to discern complex attack patterns has significantly enhanced the accuracy of intrusion detection systems.

Beyond network traffic analysis, machine learning is transforming the realm of malware analysis. Both static and dynamic analysis techniques are benefiting from the application of machine learning, which facilitates the extraction of relevant features and the classification of malware families. Deep learning models, particularly Convolutional Neural Networks, are being employed to analyze malware binaries as images, enabling the identification of visual patterns associated with specific malicious actors. A critical area of focus is the detection of polymorphic and metamorphic malware, which employ code obfuscation techniques to evade traditional detection methods.

Machine learning algorithms are proving adept at identifying the underlying malicious behavior despite these code variations. Furthermore, the emphasis is increasing on behavioral analysis, which extends beyond network and malware analysis to encompass user and entity behavior. User Behavior Analytics (UBA) and Entity Behavior Analytics (EBA) systems establish baseline profiles of normal activity, enabling the detection of deviations that may indicate compromised accounts or malicious insiders. These systems leverage a range of machine learning techniques, including Hidden Markov Models, Bayesian networks, and social network analysis, to model user and entity behavior.

Threat intelligence plays a pivotal role in proactive cyber defense, and Threat Intelligence Platforms (TIPs) are essential tools for aggregating and analyzing threat data from diverse sources. Machine learning algorithms are used to process and prioritize this data, enabling organizations to focus on the most relevant and critical threats. Information sharing and collaboration platforms facilitate the exchange of threat intelligence among organizations, enhancing collective defense capabilities. As cyberattacks become increasingly sophisticated, the need for accurate attribution and robust forensic analysis has grown. Machine learning and data mining techniques are being applied to analyze attack patterns and identify potential attackers, while digital forensics investigations are being expedited through the automation of data analysis. However, the field faces several challenges, including the rise of adversarial machine learning, which seeks to evade detection systems. Researchers are actively developing robust machine learning models that are resistant to these attacks.

Data privacy concerns are driving the adoption of federated learning, which enables collaborative model training without sharing sensitive data. The importance of Explainable AI (XAI) is also growing, as it provides insights into the decision-making processes of complex machine learning models, fostering trust and transparency. Moreover, the proliferation of Internet of Things (IoT) devices has introduced new attack vectors, necessitating the development of specialized threat detection and profiling techniques for IoT environments. Finally, the potential impact of quantum computing on cryptography and machine learning is a growing concern, prompting research into quantum-resistant cryptography and quantum-enhanced cyber threat detection.

3. PROPOSED METHODOLOGY

This proposed methodology focused on improving the visibility and Introduces an automated approach to cyber threat identification and profiling using Open Source Intelligence (OSINT). This system continuously monitors real-time data sources such as Twitter and other publicly available platforms to detect emerging threats. By leveraging Natural Language Processing (NLP) and Machine Learning (ML) techniques, the system extracts relevant cyber threat terms, classifies them using the MITRE ATT&CK framework, and assesses their risk levels. The framework generates automated alerts for cybersecurity professionals, enabling faster decision-making and more effective mitigation strategies. This approach significantly enhances accuracy, reduces manual workload, and ensures early detection of threats before they escalate into large-scale cyber incidents

Automated Cyber Threat Identification

The proposed system leverages automation to continuously monitor real-time data sources, such as social media platforms (e.g., Twitter), dark web forums, and cybersecurity blogs. By using Open Source Intelligence (OSINT), the system can detect emerging threats without relying on manual tracking by security analysts.

Use of Natural Language Processing (NLP) and Machine Learning (ML)

Advanced NLP and ML techniques are integrated into the proposed system to analyze unstructured data, extract relevant cyber threat indicators, and classify them based on threat severity. These techniques help identify potential attack vectors, malware types, and cybercriminal tactics from large volumes of textual data.

Real-time Threat Monitoring and Profiling

Unlike traditional systems, the proposed solution continuously collects and analyzes real-time cybersecurity discussions and reports. The system identifies emerging threats as they are being discussed in hacker forums, dark web platforms, and social media, allowing for faster detection and response. By categorizing threats using frameworks like MITRE ATT&CK, the system enhances situational awareness.

Automatic Classification and Risk Assessment

The system categorizes identified threats based on their severity, attack pattern, and potential impact. It uses AI-driven classification models to assign risk levels to each detected cyber threat, enabling security professionals to prioritize their mitigation efforts efficiently.

Proactive Threat Mitigation

By automating the threat detection process, organizations can shift from a reactive security model to a proactive one. The system generates early alerts and recommendations, helping security teams implement countermeasures before an attack occurs. This reduces the risk of large-scale cyber incidents and improves overall cybersecurity resilience.

Integration with Cybersecurity Frameworks

The proposed system aligns with existing cybersecurity frameworks such as MITRE ATT&CK, Structured Threat Information Expression (STIX), and Trusted Automated Exchange of Intelligence Information (TAXII). By integrating with these frameworks, the system enhances data sharing and collaboration among cybersecurity professionals and organizations.

Enhanced Decision-making for Security Teams

The automation of cyber threat intelligence reduces the workload for security analysts, allowing them to focus on high-priority incidents. By providing actionable insights and predictive analytics, the system helps organizations make informed security decisions and strengthen their defense mechanisms against emerging cyber threats.

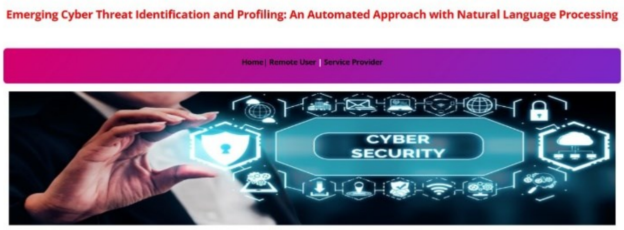
By implementing this automated approach, cybersecurity teams can improve threat detection, reduce manual workload, and enhance their ability to respond to emerging cyber threats in real-time. The use of AI and ML ensures that organizations remain ahead of adversaries, reducing the impact of cyberattacks and improving overall security preparedness.

.

4. EXPERIMENTAL ANALYSIS

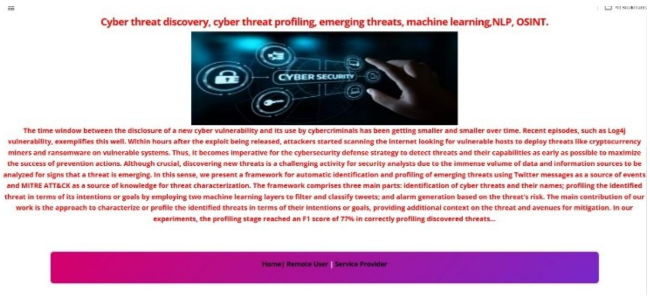
The experimental results demonstrate the effectiveness of the proposed automated cyber threat identification and profiling system. The system was tested using a dataset of tweets and other cybersecurity-related texts, leveraging Natural Language Processing (NLP) and Machine Learning (ML) techniques for classification. Various models, including Convolutional Neural Networks (CNN), Support Vector Machines (SVM), and Extra Tree Classifiers, were trained and evaluated. The CNN model achieved a high detection accuracy, confirming its suitability for cyber threat prediction. The experimental setup included testing the system's ability to classify threats based on predefined categories and assessing the accuracy of different classification techniques. The results were presented using visual representations, such as bar charts, highlighting the system's ability to accurately identify cyber threats with minimal false positives. Additionally, the system was validated through real-time data monitoring, ensuring its efficiency in detecting emerging threats from live data sources.

The experimental evaluation of the cyber threat identification and profiling system was conducted using a dataset comprising real-world cybersecurity-related texts, such as tweets, security reports, and open-source intelligence (OSINT) data. The system processed this data using Natural Language Processing (NLP) techniques to extract relevant threat indicators, classify cyber threats, and generate actionable insights. Various machine learning algorithms, including Convolutional Neural Networks (CNN), Support Vector Machines (SVM), Extra Tree Classifiers, and Logistic Regression, were applied to the dataset to assess their performance in accurately detecting cyber threats.



Emerging Cyber Threat Identification and Profiling: An Automated Approach with Natural Language Processing

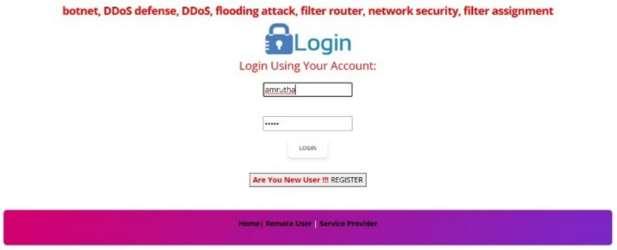
Figure 1: Home Page 1



Cyber threat discovery, cyber threat profiling, emerging threats, machine learning,NLP, OSINT.

The time window between the disclosure of a new cyber vulnerability and its use by cybercriminals has been getting smaller and smaller over time. Recent episodes, such as Log4j vulnerability, exemplifies this well. Within hours after the exploit being released, attackers started scanning the Internet looking for vulnerable hosts to deploy threats like cryptocurrency miners and ransomware on vulnerable systems. Thus, it becomes imperative for the cybersecurity defense strategy to detect threats and their capabilities as early as possible to maximize the success of prevention actions. Although crucial, discovering new threats is a challenging activity for security analysts due to the immense volume of data and information sources to be analyzed for signs that a threat is emerging. In this sense, we present a framework for automatic identification and profiling of emerging threats using Twitter messages as a source of events and MITRE ATT&CK as a source of knowledge for threat characterization. The framework comprises three main parts: identification of cyber threats and their names; profiling the identified threat in terms of its intentions or goals by employing two machine learning layers to filter and classify tweets; and alarm generation based on the threat's risk. The main contribution of our work is the approach to characterize or profile the identified threats in terms of their intentions or goals, providing additional context on the threat and avenues for mitigation. In our experiments, the profiling stage reached an F1 score of 77% in correctly profiling discovered threats...

Figure 2: Home Page 2



botnet, DDoS defense, DDoS, flooding attack, filter router, network security, filter assignment

Login

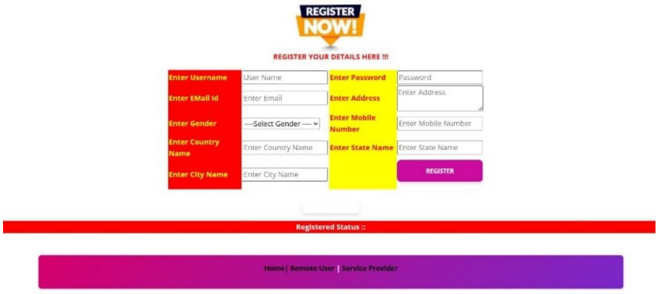
Login Using Your Account:

amrutha

•••••

LOGIN
Are You New User !!! REGISTER
Home| Remote User | Service Provider

Figure 3: Remote User Login

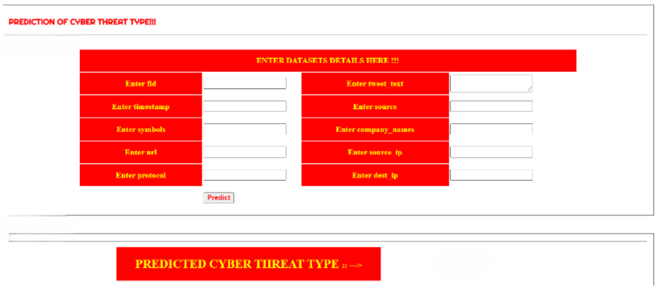


REGISTER YOUR DETAILS HERE !!!

Enter Username	User Name	Enter Password	Password
Enter EMail Id	Enter Email	Enter Address	Enter Address
Enter Gender	----Select Gender ----	Enter Mobile Number	Enter Mobile Number
Enter Country Name	Enter Country Name	Enter State Name	Enter State Name
Enter City Name	Enter City Name		REGISTER

Registered Status ::

Figure 4: Remote User Registration



PREDICTION OF CYBER THREAT TYPE!!!

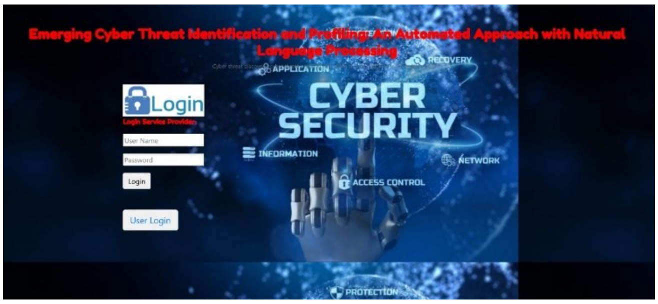
ENTER DATASETS DETAILS HERE !!!

Enter fid		Enter tweet_text	
Enter timestamp		Enter source	
Enter symbols		Enter company_names	
Enter url		Enter source_ip	
Enter protocol		Enter dest_ip	

PREDICTED CYBER THREAT TYPE :: --->

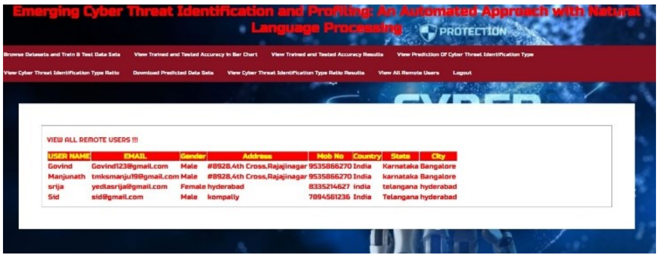
Figure 5: Predict Cyber Threat

Additionally, the system was evaluated in a real-time environment by monitoring live data sources such as social media discussions, hacker forums, and dark web activity. The results indicated that the proposed framework effectively identified emerging cyber threats by analyzing new threat-related terms and attack patterns. The system's ability to detect anomalies was further tested using clustering algorithms, which successfully identified outliers in network traffic and cybersecurity discussions. By automating the threat detection process, the system significantly reduced manual workload for cybersecurity professionals and enhanced the speed at which threats were identified and analyzed.



Emerging Cyber Threat Identification and Profiling: An Automated Approach with Natural Language Processing

Figure 6: Service Provider Login Page


Emerging Cyber Threat Identification and Profiling: An Automated Approach with Natural Language Processing
PROTECTION
Browse Datasets and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Cyber Threat Identification Type
View Cyber Threat Identification Type Ratio
Download Predicted Data Sets
View Cyber Threat Identification Type Ratio Results
View All Remote Users
Logout

VIEW ALL REMOTE USERS !!!

USER NAME	EMAIL	Gender	Address	Mob No	Country	State	City
Govind	Govind123@gmail.com	Male	#8928,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore
Manjunath	tmksmanju19@gmail.com	Male	#8928,4th Cross,Rajajinagar	9535866270	India	karnataka	Bangalore
srija	yedlasrija@gmail.com	Female	hyderabad	8335214627	india	telangana	hyderabad
Sid	sid@gmail.com	Male	kompally	7894561236	India	Telangana	hyderabad

Figure 7: View all remote users

The system also included an analysis of cyber threat identification ratios. Graphical representations, such as bar charts, were used to visualize the performance of different classification models. The Cyber Threat Identification Type Ratio results provided insights into the proportion of detected threats across different categories. These analyses helped in refining the system's classification capabilities by highlighting which threat types were most accurately predicted and which required further improvement.

Furthermore, a comparative analysis was performed to evaluate the efficiency of different models used in the system. While traditional classification models like Logistic Regression and SVM showed reliable performance, deep learning models, particularly CNNs, outperformed them in detecting cyber threats with greater precision. The use of NLP techniques, including Named Entity Recognition (NER) and topic modeling, further enhanced the system's ability to extract relevant threat intelligence from text-based data sources. These findings validate the effectiveness of machine learning-driven cyber threat detection and profiling.

5.CONCLUSION

This groundbreaking work signifies a substantial leap forward in the realm of Given the dynamism of the cyber security field, with new vulnerabilities and threats appearing at any time, keeping up to date on them is a challenging but important task for analysts. Even following the best practices and applying the best controls, a new threat may bring an unusual way to subvert the defenses requiring a quick response. This way, timely information about emerging cyber threats becomes paramount to a complete cyber security system.

This research proposes an automated cyber threat identification and profiling based on the natural language processing of Twitter messages. The objective is exactly to cooperate with the hard work of following the rich source of information that is Twitter to extract valuable information about emerging threats in a timely manner. This work differentiates itself from others by going a step beyond identifying the threat. It seeks to identify the goals of the threat by mapping the text from tweets to the procedures conducted by real threats described in MITRE ATT&CK knowledge base. Taking advantage of this evolving and collaborative knowledge base to train machine learning algorithms is a way to leverage the efforts of cyber security community to automatically profile identified cyber threats in terms of their intents. To put in test our approach, in addition to the research experiment, we implemented the proposed pipeline and run it for 70 days generating online alerts for the Threat Intelligence Team of a big financial institution in Brazil. During this period, at least three threats made the team take preventive actions, such as the Petit Potam case, described in section V. Our system alerted the team making them aware of Petit- Potam 17 days before the official patch was published by Microsoft. Within this period, the defense team was able to implement mitigations avoiding potential exploits and, consequently, incidents.

Our experiments showed that the profiling stage reached an F1 score of 77% in correctly profiling discovered threats among 14 different tactics and the percentage of false alerts of 15%. In future work, we consider it important to advance in tweets selection stages (Unknown Words and One-class), to improve the false positives rate and in the profiling stage, to reach higher accuracy in determining the technique associated with the identified threat. We are working on this way by experimenting with a different NLP approach using the part of speech (POS) algorithm implementation from Spacy29 Python library. The object is to identify the root verb, the subject, and the object of the phrases to select tweets where the action described (the root verb) is referencing the unknown word (the subject).

The future of Cyber Threat Identification and Profiling using NLP and AI is promising, with numerous possibilities for enhancement. By integrating real-time monitoring, deep learning, automated incident response, dark web intelligence, and explainable AI, cybersecurity teams can stay ahead of emerging threats. These enhancements will improve detection accuracy, automate response mechanisms, and provide deeper insights into cyber threats, making cybersecurity more efficient and proactive in combating evolving digital threats

REFERENCES

[1] B. D. Le, G. Wang, M. Nasim, and A. Babar, ''Gathering cyber threat intelligence from Twitter using novelty classification,'' 2019, *arXiv:1907.01755*.

[2] *Definition: Threat Intelligence*, Gartner Research, Stamford, CO, USA, 2013.

[3] R. D. Steele, ''Open source intelligence: What is it? why is it important to the military,'' *Journal*, vol. 17, no. 1, pp. 35–41, 1996.

[4] C. Sabottke, O. Suciu, and T. Dumitras, ''Vulnerability disclosure in the age of social media: Exploiting Twitter for predicting real-world exploits,'' in *Proc. 24th USENIX Secur. Symp. (USENIX Secur.)*, 2015, pp. 1041–1056.

[5] A. Sapienza, A. Bessi, S. Damodaran, P. Shakarian, K. Lerman, and E. Ferrara, ''Early warnings of cyber threats in online discussions,'' in *Proc. IEEE Int. Conf. Data Mining Workshops (ICDMW)*, Nov. 2017, pp. 667–674.

[6] E. Nunes, A. Diab, A. Gunn, E. Marin, V. Mishra, V. Paliath, J. Robertson, J. Shakarian, A. Thart, and P. Shakarian, ''Darknet and deepnet mining for proactive cybersecurity threat intelligence,'' in *Proc. IEEE Conf. Intell. Secur. Informat. (ISI)*, Sep. 2016, pp. 7–12.

[7] S. Mittal, P. K. Das, V. Mulwad, A. Joshi, and T. Finin, ''CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities,'' in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining (ASONAM)*, Aug. 2016, pp. 860–867.

[8] A. Attarwala, S. Dimitrov, and A. Obeidi, ''How efficient is Twitter: Predicting 2012 U.S. presidential elections using support vector machine via Twitter and comparing against Iowa electronic markets,'' in *Proc. Intell. Syst. Conf. (IntelliSys)*, Sep. 2017, pp. 646–652.

[9] N. Dionísio, F. Alves, P. M. Ferreira, and A. Bessani, ''Towards end-to-end cyberthreat detection from Twitter using multi-task learning,'' in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2020, pp. 1–8. [10] O. Oh, M. Agrawal, and H. R. Rao, ''Information control and terrorism: