International Journal of Scientific Engineering and Science
Volume 8, Issue 3, pp. 56-61, 2024. ISSN (Online): 2456-7361

Identification of New Cyberthreats and Natural Language Processing-Based Profiling

A. Venu Gopal[1*], M. Harshitha Nagasri[2*], P. Durgesh[3*], V. Rohit Kumar[4*], S. Aravind[5*], T. Prasad[6*], P. Ajay[7*]
Department of Information Technology, Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh, India – 534202
miriyalah156@gmail.com

***Abstract*— *In the field of cybersecurity, protecting systems and data requires the ability to recognize and comprehend cyberthreats. In order to improve threat categorization, this article proposes a comprehensive system that combines the MITRE ATT&CK knowledge base with an event source. There are three primary parts to the framework: (1) the classification and identification of cyberthreats, (2) utilizing a two-layered machine learning technique for tweet classification and filtering in order to profile the objectives or goals of threats that have been detected, and (3) raising alarms in response to the threat's assessed risk. This research made a substantial contribution with the methods it created to describe the objectives or goals of identified threats. This method not only provides deeper insights into the nature of the threat but also suggests effective strategies for mitigation. Experimental evaluations of our profiling methodology yielded promising results, with an F1 score of 77%, indicating its effectiveness in accurately characterizing detected threats. By leveraging both an event source and the rich threat intelligence of MITRE ATT&CK, our framework offers a robust approach to cybersecurity threat characterization. This holistic perspective enhances threat awareness and empowers organizations to proactively defend against evolving cyber threats*.

I. INTRODUCTION

The growing dependence on the Internet in social, political, and commercial spheres has led to a higher chance of cyber attacks. To prevent these exploits, timely information about cyberattacks and vulnerabilities is crucial. Threat intelligence provides evidence-based knowledge to inform decisions on response. [2]. Cyber threat intelligence, also known as threat intelligence in the cyber security realm, offers pertinent and timely information, such as attack signatures, that can assist lower the uncertainty associated with spotting potential security flaws and assaults. Informal or official sources that formally disseminate threat information in structured data format are typically good places to find cyber threat intelligence. Well-defined data models and standard formats are followed in structured threat intelligence. As a result, security technologies can easily comprehend organized intelligence on cyberthreats to assess security threats and take the necessary action. The Common Vulnerabilities and Exposures (CVE) database and the National Vulnerability Database (NVD) are two recognized sources of cyber threat intelligence. 1.Informal sources like social media platforms, forums, dark webs, and open blogs can also provide cyber threat intelligence. Informal sources enable any individual or organization to instantly disseminate threat intelligence in unstructured data format or natural language on the Internet. Open Source Intelligence is another name for the unstructured, publicly accessible threat intelligence (OSINT) [3]. Collectively, These digital trails offer insightful information about how cyber threats are changing and can warn of an impending or ongoing attack even before malicious behavior is detected on the target machine, even before they are spoken about on social media, in dark web forums [6].Cybersecurity-associated Early warning systems for cyber security incidents, such as security vulnerability exploitation, are known as OSINT [4].Malicious actors usually need to do the following in order to carry out a cyber-attack: 1) locate vulnerabilities; 2) obtain the tools and know-how needed to take advantage of them; 3) select a target and enlist allies; 4) build or buy the infrastructure required; and 5) Prepare and execute the assault. victims as well as security analysts and system administrators are examples of other players who might talk about vulnerabilities or plan an attack response [5]. Digital traces are left behind by these actions, which are frequently carried out online via social media, professional blogs, and open and closed Web forums.

II. RELATED WORK

Most firms are growing more and more concerned about cyber security, and in the previous few years, numerous research has been done in this area. The Security Operations Center (SOC) serves as these enterprises' central nervous system, providing the crucial defense against online attacks. But in order for the SOC to reliably and appropriately monitor, maintain, and safeguard a network of computes, it needs timely and pertinent threat intelligence. Because of this, security analysts gather and review a variety of information sources in an effort to become danger aware. However, if done by hand, this becomes a laborious and long task from which little knowledge can be gleaned due to the abundance of irrelevant data. Open Source Intelligence (OSINT) is a valuable tool for identifying new cyberthreats, according to research. OSINT is the gathering, examination, and application of information for intelligence purposes from publicly accessible sources [21]. Open-source blogs, deep and dark web pages, forums, and social media are a few examples of OSINT sources. These systems enable any online individual or organization to instantly broadcast information on cyber security, including incidents, fresh threats, and vulnerabilities, in plain English. We can identify Twitter as of the most illustrative social media networks among OSINT sources to gather intelligence about cyber threats [22]. System administrators, hackers, and cyber security specialists frequently discuss technical aspects of

cyberattacks and exchange experiences on Twitter [4]. Numerous research works have proposed the use of OSINT in conjunction with analytics to automatically identify online dangers from publically accessible sites like social media and forums.[23], [1], [7], [24], [25], [26], [27], [13], and [28]. The majority of recommendations, however, do not suggest recognizing and characterizing cyber dangers; Rather, they focus on finding noteworthy occurrences linked to cyberthreats or weaknesses. As per the research, [13] proposes a term-finding early cyber danger warning system that, through the mining of online discourse by cyber actors on forums, security blogs, and social media, might point to a cyberattack. The two primary parts of the system are warning generating and text mining. During the text mining phase, the input data is preprocessed to find prospective threat names. "Known" terms are discarded, and repeating "unknown" terms from various sources are chosen because they may represent the name of a newly found or emerging cyber threat. When an unknown term appears twice in a specific amount of time or meets other parameters, the second component, warning generation, is tasked with raising an alarm. The only method for identifying cyber threat names in the research approach is keyword filtering, which may lead to false positives because unknown phrases can emerge in tweets or other content that isn't always linked to cyber security. Furthermore, the identified cyber threat is not profiled in this research. A method for identifying and categorizing cyber danger [26] provides indicators in a Twitter stream. The study suggests modeling and classifying Twitter using data-driven methodology. that groups cyber security-related tweets into a predetermined list of risks and classifies tweets as either unrelated to cyber security or not. It does this by employing a Convolutional Neural Network (CNN) architecture with cascades. Using IBM's Watson Natural Language API, the pre-processing step of the proposed solution finds relevant tweets about cyber security based on Watson classification results. Furthermore, a prelabeling step is carried out during the pre-processing stage using straightforward string matching on the content of the pure tweets. Threat classifications that were considered included "vulnerability," "DDoS," "ransomware," "botnet," "data leak," "zeroday," and "general." Furthermore, the suggested approach uses CNN models that have been trained to categorize tweets as either pertinent or unrelated to cyber security. A second CNN layer receives the pertinent tweets and classifies them into one of the eight threat categories listed above. There are significant distinctions between this proposal and ours. First, the suggested course of action fails to identify the danger. Identifying the threat is a crucial first step in the creation of cyber threat intelligence since it can assist analysts in identifying and thwarting activities that use historical techniques employed by a certain threat or group. Secondly, in contrast to our methodology, which suggests a part for tweet classification by machine learning trained with the growing amount of data from MITRE ATT&CK, the proposed strategy depends on an external component to determine if a tweet is connected to cyber security or not. Third, instead of pre-filtering threats using a keyword match and a predefined a list of threat categories, we offer a way to profile the detected cyber threat to determine which step of the cyber death chain it works in. For a cyber threat analyst, this is crucial since, based on the threat profile, they may implement the required mitigation measures. A framework for autonomously extracting Twitter-based cyber threat intelligence is provided in [1].The technology uses a unique detection method to categorize the tweets according to their relevance or lack thereof to cyber threat intelligence. By learning the properties of a freshly unseen tweet from the danger descriptions found in database 5 of the Common Vulnerabilities and Exposures (CVE), the clever classifier classifies the tweet as typical or unusual with respect to cyber threat information. Typical tweets consist of deemed relevant to the cyber danger, whereas abnormal tweets are deemed unrelated to the cyber threat. The approach is assessed in the research using a data set made up of tweets from 50 well-known accounts that were closely linked to cyber security over the course of a year in 2018. In terms of categorizing cyber threat tweets, the framework performed best during the study, with an F1-score metric of 0.643. The suggested method beat a number of baselines, including binary classification methods, according to the authors. Additionally, 81 of the accurately categorized cyber threat tweets were found to be missing their CVE identifiers after analysis. Additionally, The authors 34 of the 81 tweets were discovered to were associated with a CVE identification that was among the top ten CVE descriptors of every tweet. The plan leaves out discussing how to recognize threats and what motivates them, even if it presents a method to differentiate between relevant and irrelevant tweets. When creating defense plans against new threats, those are crucial prerequisites for cyber threat intelligence. The application described in [23] uses the Twitter streaming API to gather tweets from a chosen subset of users. It then uses keyword-based filtering to eliminate tweets that have nothing to do with the infrastructure assets that are being watched. The study uses a series of two deep neural networks to categorize and extract data from tweets. The first is a binary classifier for natural language processing (NLP) that is built on a convolutional neural network (CNN) architecture [29]. It receives tweets that might be mentioning one of the infrastructure assets under observation and classifies them as irrelevant otherwise or as relevant when security-related information is included. The NER model, or named entity recognition is a neural network that uses Long-term, bidirectional memory (BiLSTM), processes relevant tweets for information extraction [30]. This network assigns one of six entities—used to find pertinent information—to each word in a tweet. Additionally, the authors decided to apply deep learning techniques due to their advantages in the discipline of machine learning [31]. As a result, they provide a neural network-based, feature-free end-to-end threat intelligence platform. From infrastructure-related tweets, the pipeline can extract valuable organizations that are suitable for issuing a security warning. It can also choose tweets that seem to include pertinent information about the security of an asset. During the assessment, a methodology was developed by which the authors evaluated multiple deep learning architecture modifications to a specified evaluation metric in order to determine which model performed the best. Additionally, the suggested models were contrasted with

additional renowned classifiers, as well as a thorough examination of the outcomes was given. The analysis revealed that the method could identify, on average, over 92% of the pertinent tweets and match specified entities in these tweets with cybersecurity-relevant labels, with an average F1-score exceeding 90%. They extracted tweets where the NER models could extract pertinent entities based on the best models they had found during their experiments, and they conducted a quick analysis that highlights Twitter's usefulness as a timely source of pertinent cyber threat awareness. The strategy utilized in this paper showed promise in locating risks targeted at particular asset classes. However, it becomes constrained when the goal is to recognize and describe more general emergent threats, rather than those that are specifically directed at a specific target or technology. A innovative and A innovative method that uses text information extraction and machine learning to identify cyber threat events on Twitter is presented in [19]. This approach makes use of unsupervised machine learning. After extracting the terms from tweets that are classified as keywords, named entities, or both, the discovered events are rated according to an importance score. By contrasting the detection error rate and efficiency with a ground truth provided by a human annotator, the proposal is evaluated. The concept shown potential in detecting cyber threat occurrences by the clustering of tweets having a false positive rate of 16.67% and a true positive rate of 75% that contain comparable terms. Additionally, a heuristic for rating the significance of events based on the influence of a Twitter profile's follower count is proposed in the paper. Similar criteria, as outlined in III-A12, are used in our technique to determine the alert's importance level depending on various attributes of the detected cyber threat, such as the quantity of followers a certain Twitter profile has. The offered strategy ignores the identification of risks and the reasons behind them. The work proposed in [9] demonstrates a Multi-Task Learning (MTL) technique that combines Integrating two models into a comprehensive pipeline for cybersecurity-oriented Natural Language Understanding (NLU). Using MTL, a technique to inductive transfer learning, a model is trained on several tasks so that the knowledge from one task may be applied to improve performance on subsequent tasks [32], [33]. The authors state that new research in NLP has demonstrated that MTL frequently enhances the functionality of cutting-edge models [34]. MTL techniques have demonstrated that learning several related tasks enhances the model's generalization capacity and significantly lowers the likelihood of overfitting, in addition to improving outcomes on assignments with a shared domain [35]. Twitter is utilized as the OSINT data stream source in the planned Pipeline for MTL cyber threat intelligence.

Through the Twitter API, the suggested application collects tweets from an already-made list of accounts that have been chosen in accordance with their inclination to post news about security issues pertaining to a specific IT system. Before being input to the Deep Neural Networks (DNN) stage, after being filtered for the first time on the basis of tweets mentioning IT infrastructure assets, the data is normalized. Two output modules are separated from an MTL DNN model for text processing: a Named Entity Recognizer (NER) and a binary classifier. Both share representation layers at the character and word levels, which can be either a form of Similar to a Long short-term memory (LSTM) [36] or convolutional neural network (CNN) [29] are examples of recurrent neural networks (RNN). The output modules work together to provide a succinct artifact that reports a security event—like a security update or vulnerability disclosure—in order to raise an alert. Previous research [23] achieved similar results for binary classification and named entity identification tasks, but required more complicated techniques for online changes of the model's parameters and dataset, as well as an information pipeline. This is where the suggested method of Multi-Task Learning (MTL) comes in.But like the earlier study, it becomes constrained when the goal is to recognize and describe more general emerging threats rather than those that are specifically directed at a specific target or technology flaws. In [5], a method for automatically creating alerts about impending or ongoing cyberthreats is presented. The study outlines a basic system that generates notifications that act as early warning signs of possible security breaches employing Twitter and the Dark Web Forum as online social media sensors. The system scans the social media feeds of a number of well-known security researchers, analysts, and whitehat hackers for content(tweets) regarding vulnerabilities, exploits, and other pertinent cybersecurity subjects. Following that, it employs text mining methods to weed out superfluous terms and pinpoint important ones. The system then verifies whether any of the terms found have ever been utilized in the filtering step forums pertaining to darkweb hacking. Finally, it provides information on the number of mentions and post content. Such information might be incredibly useful, as mentions identified by the algorithm could lead to discussions about novel vulnerabilities along with source codes intended to exploit them, and they could also point to links to credentials that have been stolen. The system is based on a database of posts from about 200 forums and markets for darkweb and deepweb hacking that is updated every day [7], [6], and [37]. Ultimately, the system produces alerts for the recently identified terms as well as information about how frequently they appear on social media and the dark web, what may be mentioned about them there, as well as a list of terms that offer semantic context to help with situational awareness and warning interpretation. More warnings can be generated during the same time period according on the algorithm's design. This decision was made out of a desire to watch the attention that the potential cyberthreat is receiving, namely the development of darkweb activity surrounding the phrases that have been found. This paper proposes a method that correlates phrases that show up in tweets and subsequently entries on forums for darkweb hacking to identify current cyber dangers. Even though we receive tweets from well-known accounts, there are frequently messages that contain cybersecurity-related terms along with unidentified terms that aren't necessarily discussing threats. As was really the case, the false positive rate may rise in the lack of a filter which enhances the chance that the tweets correspond to the description of a threat's behavior. Furthermore, the suggested alert system aims to convey the threat's intent by presenting the phrases that appeared beside the unknown keyword (threat) in order to contextualize the

International Journal of Scientific Engineering and Science
Volume 8, Issue 3, pp. 56-61, 2024. ISSN (Online): 2456-7361

discovered threat. The necessity and significance of early cyber threat identification have been shown by recent study. In order to enhance the efficacy of attack detection, writers have submitted studies utilizing a wide range of Deep learning, machine learning, and natural language processing on datasets that mostly originate from open sources (OSINT), including Twitter, blogs, the dark web, and the deep web. However, our study is different from earlier work in that We are able to combine two fresh attributes, in addition to encouraging the discovery of potential attacks: 1) Explain how the attack was profiled utilizing the MITRE architecture, and 2) Give the findings of the risk-based profile and identification.

III. PROPOSED METHOD

This work's primary goal is to suggest a method for automatically recognizing and characterizing new cyberthreats using Open Source Intelligence, or OSINT, is used to provide cyber security engineers with timely notifications. We provide a solution whose major phases are outlined below in order to accomplish this aim.

1) Constantly keeping an eye on and gathering tweets from well-known individuals and organizations to search for obscure phrases associated with harmful activities and cyberthreats;
2) Identifying phrases most likely names of threats and removing the least likely ones utilizing natural language processing (NLP) and machine learning;
3) Making use of the examples supplied by MITRE ATT&CK methodologies to determine the most likely strategy used by the detected threat;4) producing timely notifications for emerging or new dangers, describing them or their intentions and assigning a risk level depending on how quickly the threat has changed since it was first discovered. Malicious actors usually need to do the following in order to carry out a cyberattack: The steps involved in successfully exploiting vulnerabilities are as follows: 1) identify the weaknesses; 2) gather the appropriate tools and expertise; 3) select a goal and enlist helpers;4) construct or acquire the necessary infrastructure; and 5) plan and carry out the attack. victims as well as security analysts and system administrators are examples of other players who might talk about vulnerabilities or plan an attack response.

System Architecture

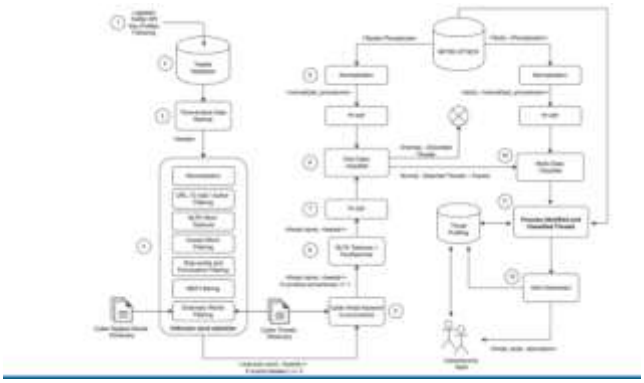

Fig 1: Proposed Work Flow

IV. METHODOLOGY

The Natural language processing (NLP) approaches serve as the foundation for automated evolving cyber threat detection and profiling methodologies. It includes several important stages, including feature extraction, data pre-processing, and collection, NLP application, machine learning model utilization, and threat profiling and risk assessments

1. Data Collection and Pre-processing

Data Sourcing: Cyber threat data is systematically gathered from diverse channels including security bulletins, online forums, social media platforms, and specialized threat intelligence feeds.

Preprocessing Procedures: The collected data is carefully preprocessed to remove noise and extraneous information and guarantee consistency in text formatting. This includes things like removing special characters, HTML tags, and text encoding normalization.

Tokenization: Following preprocessing, the text data is tokenized into constituent words and sentences, facilitating subsequent analysis.

2. Feature Extraction

TF-IDF Representation: The methodology extracts relevant features from the pre-processed text corpus applying the method known as TF-IDF (Term Frequency-Inverse Document Frequency). Using this method, terms are given weights according to how often they occur in a document in relation to the total dataset. The following is the mathematical calculation for TF-IDF:

$$\mathrm{TF}(w,D) = \frac{f(w,D)}{\text{Total words in } D}$$

$$\mathrm{IDF}(w,D) = \log\left(\frac{N}{\text{Number of documents containing word } w}\right)$$

$$\mathrm{TF-IDF}(w,D) = \mathrm{TF}(w,D) \times \mathrm{IDF}(w,D)$$

3. NLP Techniques

Named Entity Recognition (NER): NER is used to locate and classify identified entities within the written work corpus, including places, businesses, and people.

Part-of-Speech (POS) Tagging: POS tagging assigns grammatical categories to words, aiding in syntactic analysis and interpretation.

Word Embeddings: NLP models like Word2Vec or GloVe are leveraged to generate semantic representations of words, capturing contextual similarities and relationships.

Topic Modeling: Textual data is subjected to techniques like Latent Dirichlet Allocation (LDA) to identify patterns and subjects that are emerging and relevant to cyber threats.

4. Machine Learning Models

Supervised Learning: Using extracted characteristics, Support vector machines and random forests (RF) (SVM)
are two examples of machine learning models that are trained on labeled data to categorize text articles into predetermined threat categories.

International Journal of Scientific Engineering and Science
Volume 8, Issue 3, pp. 56-61, 2024. ISSN (Online): 2456-7361

Unsupervised Learning: Unsupervised techniques, including clustering algorithms, are employed to discern patterns and anomalies in the text corpus without reliance on labeled data.
Deep Learning: Recurrent neural networks (RNNs) and transformers are examples of deep learning architectures that are integrated for more complex textual data analysis, particularly in tasks like sentiment analysis and sequence labeling.

5. Threat Profiling and Risk Assessment

Threat Profiling: Identified cyber threats are systematically profiled based on their attributes, severity, and potential impact. This involves categorization into distinct threat types and summarization of key characteristics.
Risk Assessment: The methodology entails assessing the risk associated with each identified threat through risk scoring mechanisms and leveraging threat intelligence feeds to estimate likelihood and potential impact on organizational assets and operations.
Reporting and Visualization: Comprehensive reports and visualizations are generated to effectively communicate identified threats and their profiles to stakeholders, thereby facilitating informed decision-making and prioritization of mitigation strategies.

TABLE 1: Performance Comparison of ML Approach

ALGORITHM	PRECISION	RECALL	F1 - SCORE	ACCURACY
Decision Tree	80	89	84	76
Logistic Regression	80	92	86	78
SVM	81	87	84	77
Random Forest	78	97	87	79
Gradient Boosting	77	90	83	74

V. RESULTS

Output Screens

Fig. 1. Accuracy for the ml algorithms

In above screen shows the different machine learning algorithms accuracy.

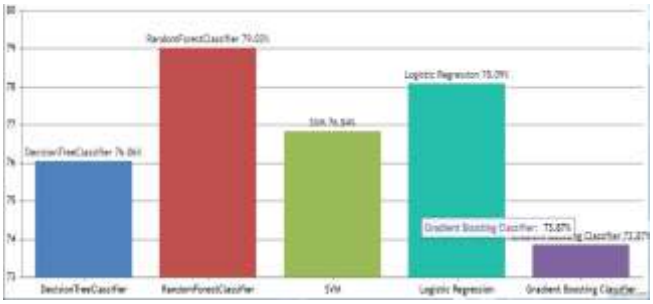

Fig. 2. Accuracy in Bar Charts

In above screen shows algorithms accuracy in bar charts.

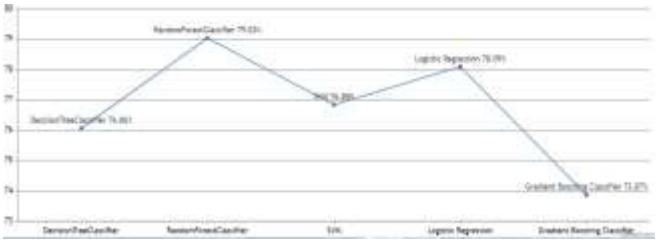

Fig. 3. Accuracy in Line Chart

In above screen shows the accuracy in line chart.

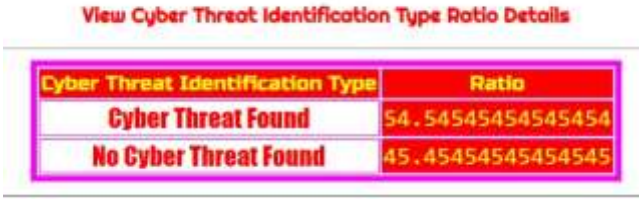

Fig4 Cyber Threat Detection Ratio

In above screen shows the detection ratio of the cyber threats.

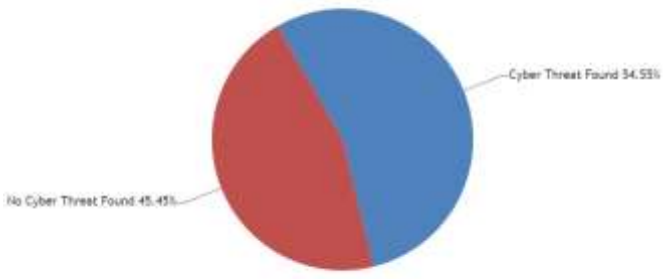

Fig. 5. Cyber Threat Detection Ratio Pie Chart

In above screen shows the detection ratio pie chart

VI. CONCLUSION

Keeping abreast of emerging vulnerabilities and threats is a difficult but crucial duty for analysts, given the dynamic nature of the cyber security industry. Even with the strongest standards and controls in place, a novel threat can emerge and find a novel way around the defenses, necessitating an immediate reaction. In this sense, up-to-date knowledge of newly developing cyberthreats becomes critical to a functioning cyber security

system. This study suggests using Twitter tweets are subjected to natural language processing in order to automate the detection and profiling of cyber risks. The goal is to precisely collaborate with the diligent effort of monitoring Twitter, a wealth of information, in order to promptly extract important information about new dangers. This work sets itself apart from others by not stopping at just pointing out the danger. By comparing the language from tweets to the actions taken by actual threats as detailed in the MITRE ATT&CK data repository, it attempts to determine the threat's objectives. By using this dynamic and cooperative a database of knowledge to instruct machine learning algorithms, the cyber security community's efforts can be harnessed to create a profile automatically detected cyber threats according to their intentions. Along with carrying out the study experiment, we put our strategy to the test by implementing the suggested pipeline and running it for 70 days, creating online warnings for a large company's Threat Intelligence Team Brazilian banking institution. At least three threats during this time prompted the team to take precautionary measures; one such instance is the Petit Potam case, which is covered in section V. Petit-Potam was brought to the team's attention by our system 17 days prior to Microsoft's official patch release. The defensive team was able to put mitigations in place during this time frame, preventing potential exploits and events as a result. Our tests revealed demonstrated the profiling stage correctly identified dangers among 14 different techniques, achieving an F1 score of 77%, with a 15% false alert rate. Future research should concentrate on enhancing the false positives rate in the tweet selection phases (Words Unknown and Single-class) and increasing the accuracy of the technique connected to the recognized threat in the profiling stage. We are attempting to address this by utilizing the implementation of the Part of Speech (POS) algorithm from the Spacy29 Python library in an experiment with an alternative NLP methodology. Finding subject, object, and root verb of the sentences is the goal in order to choose tweets where the action (the root verb) refers to the topic, or the unidentified word.

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: Tracking the Mumbai terrorist attack through Twitter,’’ Inf. Syst. Frontiers, vol. 13, no. 1, pp. 33–43, Mar. 2011.
[11] T. Sakaki, M. Okazaki, and Y. Matsuo, ‘‘Earthquake shakes Twitter users: Real-time event detection by social sensors,’’ in Proc. 19th Int. Conf.World Wide Web, Apr. 2010, pp. 851–860.
[12] B. De Longueville, R. S. Smith, and G. Luraschi, ‘‘‘OMG, from here, I can see the flames!’: A use case of mining location based social networks to acquire spatio-temporal data on forest fires,’’ in Proc. Int. Workshop Location Based Social Netw., Nov. 2009, pp. 73–80.
[13] A. Sapienza, S. K. Ernala, A. Bessi, K. Lerman, and E. Ferrara, ‘‘DISCOVER: Mining online chatter for emerging cyber threats,’’ in Proc. Companion Web Conf. Web Conf. (WWW), 2018, pp. 983–990.
[14] R. P. Khandpur, T. Ji, S. Jan, G. Wang, C.-T. Lu, and N. Ramakrishnan, ‘‘Crowdsourcing cybersecurity: Cyber attack detection using social media,’’ in Proc. ACM Conf. Inf. Knowl. Manage., Nov. 2017, pp. 1049–1057.
[15] Q. Le Sceller, E. B. Karbab, M. Debbabi, and F. Iqbal, ‘‘SONAR: Automatic detection of cyber security events over the Twitter stream,’’ in Proc. 12th Int. Conf. Availability, Rel. Secur., Aug. 2017, pp. 1–11.
[16] K.-C. Lee, C.-H. Hsieh, L.-J.Wei, C.-H. Mao, J.-H. Dai, and Y.-T. Kuang, ‘‘Sec-buzzer: Cyber security emerging topic mining with open threat intelligence retrieval and timeline event annotation,’’ Soft Comput., vol. 21, no. 11, pp. 2883–2896, Jun. 2017.
[17] A. Ritter, E. Wright, W. Casey, and T. Mitchell, ‘‘Weakly supervised extraction of computer security events from Twitter,’’ in Proc. 24th Int. Conf. World Wide Web, May 2015, pp. 896–905.
[18] A. Queiroz, B. Keegan, and F. Mtenzi, ‘‘Predicting software vulnerability using security discussion in social media,’’ in Proc. Eur. Conf. Cyber Warfare Secur., 2017, pp. 628–634.
[19] A. Bose, V. Behzadan, C. Aguirre, and W. H. Hsu, ‘‘A novel approach for detection and ranking of trendy and emerging cyber threat events in Twitter streams,’’ in Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining (ASONAM), Aug. 2019, pp. 871–878.
[20] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, ‘‘Mitre ATT&CK: Design and philosophy,’’ MITRE Corp., McLean, VA, USA, Tech. Rep. 19-01075-28, 2018.
[21] B.-J. Koops, J.-H. Hoepman, and R. Leenes, ‘‘Open-source intelligence and privacy by design,’’ Comput. Law Secur. Rev., vol. 29, no. 6, pp. 676–688, Dec. 2013.
[22] R. Campiolo, L. A. F. Santos, D. M. Batista, and M. A. Gerosa, ‘‘Evaluating the utilization of Twitter messages as a source of security alerts,’’ in Proc. 28th Annu. ACM Symp. Appl. Comput., Mar. 2013, pp. 942–943.
[23] N. Dionísio, F. Alves, P. M. Ferreira, and A. Bessani, ‘‘Cyberthreat detection from Twitter using deep neural networks,’’ in Proc. Int. Joint Conf. Neural Netw. (IJCNN), Jul. 2019, pp. 1–8.
[24] A. Niakanlahiji, J.Wei, and B. Chu, ‘‘A natural language processing based trend analysis of advanced persistent threat techniques,’’ in Proc. IEEE Int. Conf. Big Data (Big Data), Dec. 2018, pp. 2995–3000.
[25] G. Ayoade, S. Chandra, L. Khan, K. Hamlen, and B. Thuraisingham, ‘‘Automated threat report classification over multi-source data,’’ in Proc. IEEE 4th Int. Conf. Collaboration Internet Comput. (CIC), Oct. 2018, pp. 236–245.