Botnet Detection and Incident Response in Security Operation Center (SOC): A Proposed Framework

Roslaily Muhammad, Saiful Adli Ismail, Noor Hafizah Hassan
Advanced Informatics Department-Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia

***Abstract*—In the dynamic landscape of evolving cyber threats, Security Operations Centers (SOCs) play an important role in protecting digital assets. Among these threats, botnets are particularly challenging due to their ability to take over many devices and launch coordinated attacks. Through comparative analysis, the research gaps in existing frameworks have been identified. Based on these insights, a botnet detection and incident response framework aligned with SOC practices has been proposed. This proposed framework emphasizes proactive measures by integrating threat intelligence, detection and monitoring tools to detect botnet attack and facilitate rapid response. Future research will focus on conducting evaluation and validation studies to assess the effectiveness and performance of the framework in controlled environments. This effort will contribute to develop the framework and ensuring it aligns with practical cybersecurity needs.**

Keywords—Botnet detection; threat incident response; security operation center

I. Introduction

Botnet is one of the most dangerous threats that occur in cyberattacks today which can compromise the computer systems or smartphones. Detecting it is becoming more sophisticated and challenging to detect due to the growth of Internet of Things (IoT), smart devices, cloud platforms and social media. Wainwright & Kettani [1] defined as botnets consisting of hundreds or thousands of connected devices that run bots or scripts, controlled by a single machine referred to as botmaster via Command and Control (C&C) channel. Botnets generally could propagate themselves throughout a network and infect vulnerable machines. They operate by maintaining contact with the botmaster for command and control or by using specific modules in their architecture for the same purpose [2]. A compromised host also will be infected when they open a malicious email attachment, visit an affected website, and accidentally download the bot onto their computer. Once infected, the botmaster will gain access to the victim's computer without victim acknowledgment [3]. In [4], botnet can perform DDoS attacks, spamming, malware and compromise a large computer. These activities pose a significant risk to national security, public or private organizations, and individual.

Botnets are capable of being remotely controlled by botmasters from any geographical location through Command and Control (C&C) channels. Botmasters generate revenue by renting and leasing botnets on the darknet market. Attackers frequently modify and update the structures and methodologies of botnets to evade detection [5]. This makes botnets difficult to detect. Furthermore, the complicated topological structure of botnets, particularly peer-to-peer (P2P) topology, adds to the difficulty of detection. P2P topologies are more dangerous and resilient compared to centralized topologies. The merging of malicious and legitimate traffic within P2P botnets presents one of the most significant challenges in botnet detection [6].

According to the International Data Corporation, Malaysia's cybersecurity expenditure surged to RM2.6 billion (US$627 million) in 2019 and is anticipated to exceed RM4 billion (US$1 billion) by 2024. This data is highlighted in a report from the Ministry of Communications and Digital website [7]. Companies face challenges when the time needed to detect and mitigate threats increases, along with rising costs. This indicates the inefficiencies within companies in managing incident reports related to these threats. Vielberth et al. [8] indicated that these inefficiencies are not only from within the company but also from inadequate devices, systems, applications, and networks. Additionally, there is a lack of awareness regarding which assets require protection and how to integrate tools with the existing infrastructure. Moreover, the rapid evolution of the threat landscape makes it harder for companies to keep up with new technologies.

As the threat landscape continues to evolve, organizations must deploy defensive mechanisms to safeguard their operations. In study [9], among the relevant strategies is the establishment of a Security Operations Center (SOC), which serves to monitor and protect against potential danger. Within SOC operations, threat intelligence enables the detection of botnets through analysis from diverse sources. Additionally, it facilitates the identification of patterns and behaviors based on potential indicators of their presence [10]. Furthermore, threat information can be disseminated to other organizations via threat intelligence sharing platforms and standards such as the Malware Information Sharing Platform (MISP), OpenCTI, STIX/TAXII, and OTX ([11], [12], [13].

The purpose of this study is to identify the components involved in botnet detection and incident response, with the aim of designing a comprehensive framework aligned with Security Operations Center (SOC) practices. The main contributions in this study are:

- Conducting study on botnet detection framework to discover the main components and features in framework.
- Conducting study on threat detection and incident response framework to identify the framework components, security tools and cybersecurity standard practiced by SOC.

- Provides a comprehensive analysis of framework components to identify research gaps for designing botnet detection and response framework align with the SOC practices.

This paper is organized as follows. Section II studies related work on the botnet detection framework and threat detection and incident response related to SOC. Section III discuss the methodology and framework implementation. Section IV identifies the research gaps and discussion on a proposed framework. Section V concludes the paper and discusses the potential future research.

II. Related Work

Various detection methods have been proposed by researchers in literature to detect botnets. Based on literature [14], there are three major methods of botnet detection such as host-based detection, honeynet detection and network-based detection. Recently, machine learning based detection has become the most widely used for detecting botnets methods as proven by previous literature [15], [16], [4], [5]. In addition, the number and complexity of IoT devices is also growing, it has become important to develop effective botnet detection methods.

To enhance botnet detection methods, collaboration with Security Operations Centers (SOCs) is crucial for strengthening the capability to monitor and respond the emerging botnet effectively. It is also responsible to monitor network activity, analyzing, investigate and response to the security threat by using a range of tools and technologies [17], [18], [8]. Incorporating advanced technologies, such as machine learning-based detection, within the SOC framework enables real-time analysis of network traffic and anomalies. Iqbal & Anwar [19] and Islam et al [20] utilized the machine learning approach that enable rapid detection and automates alert for immediate response to identify threat. The SOC is supported by the advanced technology tools such as the Security Information and Event Management (SIEM) system, intrusion detection/prevention system (IDS/IPS), advanced threat intelligence and forensic analysis tools as defense mechanism, protect organizations from the potential damage caused by threats [21], [9], [22], [23], [8].

Security Operations Centers (SOCs) also utilize the MITRE ATT&CK framework for its standardized approach to describing adversarial behaviors throughout the cyber-attack lifecycle. The MITRE ATT&CK maps adversarial behaviours into a structured matrix representation of tactics and techniques followed by procedures [24]. By incorporating botnet-related techniques into the MITRE ATT&CK matrix, organizations can map specific tactics, techniques, and procedures (TTPs) associated with botnets, enhancing their overall threat detection capabilities. MITRE ATT&CK integrates well with Threat Intelligence (TI), helping SOC analysts in correlating real-world threat intelligence with specific tactics used by attackers. This enhances their ability to detect threats. Bajpai & Enbody [25] incorporated MITRE ATT&CK mapping into their ransomware response framework to prompt technical responses, thereby enhancing their overall capabilities in dealing with ransomware.

A. Botnet Detection Framework

Many researchers have focused on finding the solutions to detect botnets by sharing their experimental experiences and suggested various solutions to mitigate this issue. Most of the solutions that authors proposed are based on machine learning approach. The purpose of the botnet detection framework is to identify botnet activity and distinguish it from legitimate network traffic.

In study [14] the authors introduced a botnet detection framework based on comparative analyses from previous research, focusing primarily on effective measures for detection. However, this framework lacks emphasis on early-stage prevention. In contrast, the collaborative framework presented by [16] provides a comprehensive approach to botnet detection, incorporating a two-phase decision-making process involving the Host Agent Detector (HAD) and Network Agent Detector (NAD). HAD captures suspicious behavior using machine learning models, extracting features from network logs. NAD was activated by HAD alerts, identifies infected machines by analyzing network flow logs. The two-phase decision-making process ensures a more accurate performance, as NAD's actions depend on HAD's alerts. Furthermore, this framework was evaluated using real-world benchmark datasets, enhancing its practical applicability. The classifier utilized in this collaborative framework aids in generating infection reports when detecting RAT-bots. However, this framework is only able to detect RAT-bots and requires time complexity to evaluate.

BotDet is a framework developed by Ghafir et al. [26] tovidentify botnet C&C traffic and consists of two main phases. Multiple modules are executed during the initial phase to find various potential botnet C&C communication methods. This framework allowing network traffic to be analyzed in real time without storing it. In addition, it uses information from the different intelligence feeds to update all blacklist. The module allows to block all alerts with same infected host and malicious item in one alert per day. This can reduce the number of email alerts received by security teams. However, external IDS alerts have been integrated to reduce the false positive rate.

In study [27], the authors utilized Correlation Attribute Eval and Principal Component filters to identify botnet features, reducing dataset dimensions and improving botnet detection efficiency. This framework consists of five components such as botnet dataset, Data pre-processing, Data normalization, machine learning and evaluation. The six classifiers (Random Forest, IBK, JRip, Multilayer Perceptron, Naive Bayes, OneR) are compared for an optimized detection model. The results highlight the significant improvement in botnet detection when combining Correlation Attribute Eval with JRip, particularly on the CICIDS2017 dataset. However, it only focuses at one dataset, might be simplifying how features are chosen, and lack of exploration of pros and cons of the chosen method.

Ismail et al. [4] proposed a Botnet Analysis and Detection System (BADS) which could detect Botnet in encrypted channel and includes the autonomous feature. The BADS framework comprises of three main components which are Network Analysis System (NAS), IDS and Alarm System

(AS). Due to conflict with some tools used to detect the botnet, this framework unable to determine the severity of botnet attack. If this method can be employed, it can assist network manager to monitor the system and provide the automation solution.

The study conducted by Ibrahim et al. [28] focuses on utilizing flow-based behavior analysis to identify newly emerging botnets, addressing the difficulties in recognizing consistent patterns within a botnet that consistently alters its signature. The framework initiates by selecting a network traffic dataset and then proceeds with the pre-processing of the chosen dataset. This study emphasizes the importance of the pre-processing phase, ensuring that the data is handled effectively to produce high performance during classification.

Peertrap is a botnet detection framework developed by Xing et al. [6] based on Self- avoiding random walks (SAW) algorithm to detect the unstructured P2P botnet under C&C channel encryption. The dataset was used for an evaluation experiment, and the experimental results were compared to those of the current method on an unstructured data set. This framework has achieved high accuracy detection of P2P bots with existence of legitimate P2P traffic. Nevertheless, this framework only focuses on P2P botnet detection process without provides response should be taken by security team. The report will be generated once the P2P botnet has been detected.

Table I provides a comprehensive overview of various studies conducted on the detection methods and framework components employed in botnet detection.

B. *Threat Detection and Incident Response Framework related to SOC*

Threat detection and Incident response framework refers to a structured approach used by security operations teams to detect and respond to security incidents within an organization's information systems. A Security Operations Center (SOC) is a centralized unit that monitors and manages security-related issues on an ongoing basis. The framework provides guidelines and processes for identifying, analysing, responding, and mitigating security incidents. To achieve the SOC goal of providing and responding to incident threat, the framework such as Incident Response Lifecycle, ISO/IEC 27035:2016 and NIST Computer Security Incident Handling Guide have been used as guides to respond the incident threat [23]. SOC incident management is the process of identifying, detecting, analyzing, and responding to the information security in a systematic way.

Ti Dun et al. [31] investigated how Next Generation Security Operation Centers (NGSOCs) respond to malicious activities in their research. A specific use case was developed to detect the Hermes Ransomware v2.1 malware, utilizing complex correlation rules within the SIEM anomalies engine. This study aimed to analyze and identify the presence of Hermes Ransomware v2.1. However, this framework has a limitation because many of these use cases are created for specific companies, which may pose challenges when trying to apply them to different environments with varying needs.

In research [20], a novel Artificial Intelligence (AI)-based framework called SmartValidator was developed to automate the validation of alerts using Cyber Threat Information (CTI) in Security Operation Centres (SOCs). This framework was developed to overcome the manual updating process that caused delays in responding to attacks. SmartValidator, leveraging Machine Learning (ML) techniques, consists of three layers for data collection, model building, and alert validation.

Wang et al. [32] introduced a comprehensive Security Operation Center (SOC) to address and mitigate the identified issues. This framework focuses on establishing essential components within the SOC to enhance defense against specific types of attacks, acquire high-quality threat intelligence, and achieve faster automated response capabilities. In this framework, a multi-perspective behavior analysis component is implemented to analyze various types of attacks. Furthermore, additional components were developed to construct an integrated SOC platform, including those for data collection and big data storage.

A framework [25] has been developed for combating ransomware attacks that provides a detailed approach that balances between adaptability and practicality, making it useful for both technical team and stakeholders. The framework components were adapted from general IR procedure. However, technical response actions in the framework were derived using MITRE ATT&CK mappings and the identification of process-related actions depended solely on the authors' industry experiences.

Lai et al. [33] introduced a framework for the Security Operations Center (SOC) known as RansomSOC, designed to enhance detection and response capabilities against ransomware attacks. It incorporates a unique real-time emergency local data backup scheme that exploits ransomware design flaws, ensuring immediate backup of critical files even post-attack initiation to minimize the impact on encrypted files. Additionally, RansomSOC employs easily detectable ransomware honey files, created based on entropy value changes, facilitating rapid detection of ransomware attacks. The framework primarily consists of eight components: Ransomware Sandbox, Logs Analyzer, Logs Collector, File Content Entropy and Extension Comparison, File Protector Definition Generator, Administrator Notification Center, Data Backup Orchestra Center, and Defense Command Orchestra Center. However, this framework requires a broader investigation into various ransomware families and practical integration scenarios of RansomSOC with a typical SOC.

Table II summarizes various studies focusing on different types of cyber threats and the corresponding frameworks, components, cybersecurity tools, and standards or frameworks utilized.

TABLE I. SUMMARY STUDIES OF BOTNET DETECTION FRAMEWORKS

Author	Detection methods	Framework Components	Features
[6]	Machine Learning	• data pre-processing • features extraction • shared neighbour graph construction. • community detection • Classification	• real network traffic, P2P botnet traffic, P2P • legitimate application • P2P Feature Extraction • Community Detection using Self- avoiding random walks (SAW) algorithm. • Filter out the botnet community
[4]	Signature based	• Network Analysis System (NAS) - data collection and conversion - Feature Extraction and selection -Botnet Prediction and Classification • IDS - Intrusion Detection System • Alarm system (AS)	• Data set of encrypted, Botnet traffic, public data set • Tranalyzer is used to extract the Botnet features. • IDS -Snort based detection mechanism. • Notify the severity of attacks, suggest the protection strategy and generate report.
[16]	Host and network based	• Host agent detector (HAD) process- monitoring module Java RAT Tracking module. • Network agent detector (NAD) • Feature extraction • Classifier • Alarm report	• RAT infections collected from file system, network trace. • The Host Agent Detector (HAD) capturing any suspicious behaviour. • anomaly detection • Network Agent Detector (NAD) – block any infected machines by analysing their network's flow logs.
[26]	Machine Learning	• Network traffic. • Malicious IP address detection (MIPD) • Malicious SSL certificate detection (MSSLD) • Domain Flux detection (DFD) • ToR connection detection (TORCD) • Automatic updates - Intelligence feeds • botnet correlation framework (CF)	• Intelligence feed • malicious IP address, Tor connection SSL certificate (encrypted) • network traffic to search for a match in the source and destination IP addresses for each connection with the IP blacklist. • The detection is based on a blacklist of malicious IPs of C&C servers, Correlation framework. • Alert notification sends via email
[15]	Machine Learning	• Behavior extractor • Behavior identifier • Feedback provider	• network traffic from IRC, P2P and HTTP botnets. • Behavior Extractor collects network traffic from hosts and builds a representation of host behavior • Support Vector Machine (SVM) classifier. • Normal and cooling state is for legitimate host. • Alert state if net admin confirms the host is malicious.
[29]	Host based detection	• Network traffic. • Management P2P Traffic Detection • Sequence database generation. • Event Mining • Event sequence generation • Frequent behavior mining • Bot Flows	• botnet traffic (ISOC dataset) malicious network traffic (P2P application) • patterns (frequent behaviour) • Machine Learning algorithms two-phase Sequential Pattern Mining (SPM) approach.
[30]	Network based detection	• Pre-processing • Traffic Clustering • Rules detection • Behavior Detection Model	• Public dataset, Botnet dataset - C&C flow • DNS and HTTP filter, SSL certificate filter (encrypted) historical flow (label as C&C, non-C&C) • Behaviour model building • Rules detection (RD) & behaviour detection
[27]	Machine Learning	• Botnet dataset • Data prepressing • Data Normalization • Machine Learning • Evaluation	• CICIDS2017 • Feature selection, Classification performance metrics
[28]	Machine Learning	• Input • Pre-processing Data • Classification • Evaluation	• Data sources and data distribution • Labelling and cleaning, Dividing Dataset, Feature selection, • Aggregation and Data Quality Process • Build model. • Performance parameter

TABLE II. SUMMARY OF THREAT DETECTION AND INCIDENT RSSPONSE FRAMEWORK RELATED TO SOC

Author	Type of threat	Framework Components	Cybersecurity tool	Cybersecurity standard & framework
[34]	Cyber threat	• Data source layer • System management • Services management layer	Network Management System (NMS)	Not mentioned

[20]	Cyber threat	• Threat collection data layer • Threat data prediction model building layer. • Threat data validation layer	OSINT, MISP	Not mentioned
[31]	Ransomware	• Correlation rules for Hermes Ransomware • Enriching • Combining rules • Detection performance	SIEM	Not mentioned
[32]	Cyber threat	• Data Collection • Data Pre-processing • Big Data Storage • Multi perspective Behavior Analysis • Threat Intelligence • Application services	ElasticSearch	Not mentioned
[25]	Ransomware	• Preparation • Identification • Containment • Eradication • Recovery • Post-incident	EDR	NIST, MITRE ATT&CK
[35]	Cyber threat	• Data sources and threat intelligence • Data pipelines • Storage and visualization • Alerting	MISP, ZEEK, ELASTIC Search, KIBANA, ElastAlert, PocketSOC	Not mentioned
[33]	Ransonware (Black Matter, Conti, Dark Side, and Revil)	Ransomware Sandbox, Logs Analyzer, Logs Collector, File Content Entropy and Extension Comparison, File Protector Definition Generator, Administrator Notification Center, Data Backup Orchestra Center, and Defense Command Orchestra Center	Not mentioned	Not mentioned

III. Methodology

This research began with Phase 1 which involved a comprehensive review of existing literature conducted across various academic databases, including Scopus, IEEE, ScienceDirect, and Google Scholar. Keywords and phrases related to the research question were used to construct an effective search strategy. The search terms included "botnet" OR "threat" AND "detection framework" AND "incident response framework" AND "security operation center". Boolean operators have been used to refine and broaden the search needed. In this paper, the researcher utilizes a literature review to identify existing frameworks related to botnet and SOC, analyze them, and extract the information presented in Table I and Table II. The findings of the review are presented in Table III, which outlines the research gaps necessary for designing a proposed framework.

Based on the research gaps gained from the literature review, an initial framework was developed. This framework was designed to address the specific components of detecting and responding to botnet activities within a SOC environment. The phase 2 will involve conducting experiments to refine and improve the initial framework. This phase may include testing detection and response strategies, evaluating the effectiveness of various tools and technologies, and simulating botnet attacks in a controlled environment.

Once the framework is refined through the experimental phase, expert interviews will be conducted. In Phase 3 which validates the framework, experts in the field of cybersecurity and SOC management will be selected based on their knowledge and experience with botnet detection and incident response. The open-ended questions will be used to validate the framework through these interviews. Expert feedback on the framework will help validate its relevance, practicality, and effectiveness in real-world SOC environments. This validation process will help ensure that the framework is aligned with industry best practices for botnet detection and incident response in SOC. A comprehensive framework and a well-validated approach to botnet detection and incident response in SOCs will be developed in Phase 4. This framework will also incorporate threat intelligence and best practices in the field. The overall research methodology is presented in Fig. 1.

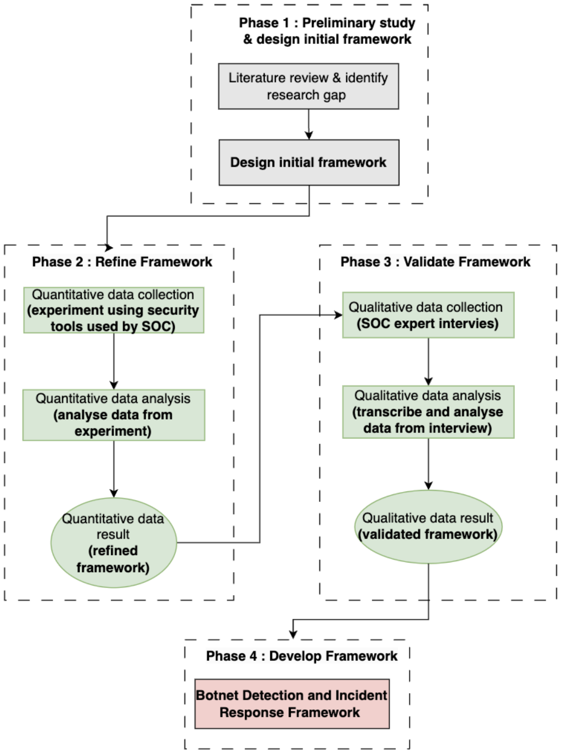
Phase 1 : Preliminary study & design initial framework
Literature review & identify research gap
Design initial framework
Phase 2 : Refine Framework
Quantitative data collection (experiment using security tools used by SOC)
Quantitative data analysis (analyse data from experiment)
Quantitative data result (refined framework)
Phase 3 : Validate Framework
Qualitative data collection (SOC expert intervies)
Qualitative data analysis (transcribe and analyse data from interview)
Qualitative data result (validated framework)
Phase 4 : Develop Framework
Botnet Detection and Incident Response Framework

Fig. 1. Research methodology.

IV. Results and Discussion

This research has identified nine relevant papers on botnet detection frameworks and seven related papers focusing on threat detection and response frameworks associated with Security Operations Centers (SOCs). This paper should focus on the development of a framework for detecting botnets that aligns with Security Operations Center (SOC) practices. Table III provides a comparison of the framework components derived from Table I and Table II, facilitating the development of frameworks for botnet detection and incident response.

This section provides several observations on how botnet detection frameworks can be aligned with Security Operations Center (SOC) practices by identifying gaps in the existing literature. There are several research gaps in the current literature dealing with botnet detection that can be identified from the current review. These gaps can be summarized as follows:

- There is a lack of botnet-focused frameworks. While various frameworks have been developed and studied, none seem to focus on the detection of botnet activity. This gap in the literature suggests future research to design and implement a botnet detection framework aligned with SOC practices.
- There is limited on alert notification and response mechanisms, it facilitates quick actions upon the identification of botnet activities, contributing to accurate detection and immediate response efforts.
- The limited utilization of security tools in botnet detection.
- Lack of integration of threat intelligence within the botnet framework.
- Limited on the adoption and adherence to comprehensive cybersecurity standards and frameworks.
- Lack of dynamic detection mechanisms capable of automatically updating to align with the latest TTPs of evolving botnets.

Addressing these gaps can lead to the development of more effective botnet detection and incident response frameworks aligned with the SOC practices.

A. *Proposed Framework*

The development of the proposed framework is guided by the gaps in existing frameworks. The proposed framework is a comprehensive of botnet detection and incident response framework aligned with the SOC practices is illustrated in Fig. 2. The proposed framework is designed to assist organizations in efficiently detecting and response to botnet related incidents. It emphasizes proactive measures by integrating with the threat intelligence, detection techniques and monitoring tools that enable botnet attack can detect, generate accurate analysis and rapid response and continuously updating the new botnet threat. This framework contributes to reducing impact of threat especially botnet-related and ability to adapt the evolving threat landscape.

TABLE III. Comparative Analysis of Botnet Detection and Incident Response Framework Components

		Framework Components							
	Author	Data Collection & data source	Data pre-processing	Features behaviour extraction & selection	Detection	Alert notification & response	Cybersecurity tool	Threat intelligence	Cybersecurity Standard & Framework
Botnet detection framework	[6]	√	√	√	√				
	[4]	√		√	√	√	√		
	[15]	√		√	√	√			
	[25]		√	√	√	√		√	
	[14]	√		√	√	√			
	[28]	√		√	√	√			
	[29]	√	√	√	√	√			
	[26]	√	√	√	√				
	[27]	√	√	√	√				
Detection & response framework	[33]	√			√		√		
	[19]	√	√	√	√	√	√	√	
	[30]	√		√	√		√		
	[31]	√	√	√	√	√	√	√	
	[24]	√			√	√	√	√	√
	[34]	√					√	√	
	[32]	√		√	√	√			

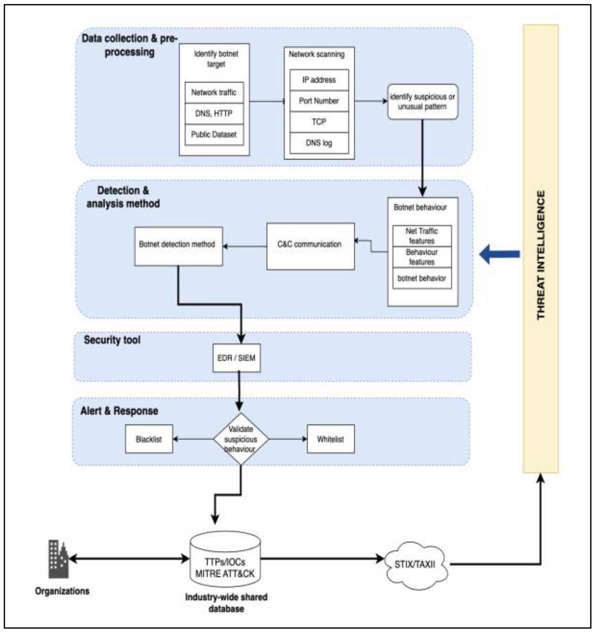

Fig. 2. A proposed framework.

The details of the proposed components in a proposed framework are explain below:

1) *Data collection and pre-processing:* Data collection components are required to understand normal and malicious activities in the network. This involves gathering data from various sources such as network devices, endpoints and logs. It also encompasses identifying potential targets, conducting network scans, and identify suspicious and unusual patterns of botnet.

2) *Detection and Analysis method:* The detection and analysis methods component is essential to recognize and analyze the potential botnet activities. It refers to the detection methods used to detect botnet activities within network or system.

3) *Security tool:* Security tool play an important role in enhancing the capabilities of a framework, offering a variety of functions for an effective defence against botnet activities. Additionally, security tools often support automated response mechanisms that enable immediate actions such as isolating infected devices or blocking malicious traffic upon botnet detection.

4) *Alert & Response:* It will generate alert based on detected botnets and taking action to mitigate and eliminate the botnet. When an alert is generated, threat intelligence data can be used to enhance the alert with additional context, such as known indicators of compromise (IOCs), threat actor profiles, historical attack patterns, and relevant mitigation strategies. This additional information provides security analysts with a deeper understanding of the potential threat, enabling more informed decision-making during the response process.

5) *Threat Intelligence:* It provides up-to-date information on emerging botnet threats that allows the framework to keep updated on evolving tactics employed by malicious actors. By contextualizing indicators of compromise (IoCs), threat intelligence assists the framework in distinguishing between normal and suspicious network activities, enhancing its accuracy in detection.

6) *Cybersecurity Standard and Framework adoption:* The integration of cybersecurity standards and frameworks into a botnet detection creates best practices, guiding the design and deployment of the botnet detection framework based on industry-recognized principles. Basically, the integration of cybersecurity standards and frameworks enhances the overall resilience and effectiveness of a botnet detection framework in safeguarding organizations against evolving cyber threats.

B. Proposed Experimental Approach

The testbed setup involved a virtualized environment created using a virtualization tool such as VirtualBox. The virtual machines will run the operating systems, with Windows 10 as the vulnerable machine and Kali Linux as the botnet attack machine. The virtual servers also will create to run various services that install Ubuntu operating system. Wazuh, TheHive, and Cortex will be installed on separate VMs within the network. Wazuh is an open-source tool that will be used to monitor unusual network traffic, system logs, file changes associated with botnet activity, and other indicators of compromise (IOCs). TheHive and Cortex will be used for incident response and threat intelligence management. Data will be collected on Wazuh alerts, TheHive cases, and Cortex analysis results, then will be analyzed to evaluate the effectiveness of the detection and response. Metrics such as detection rate, false positive rate, and response time will be used for measurement. The purpose of the testbed is to evaluate the botnet detection and response strategies in a controlled environment. Fig. 3 illustrates the proposed botnet detection and incident response testbed.

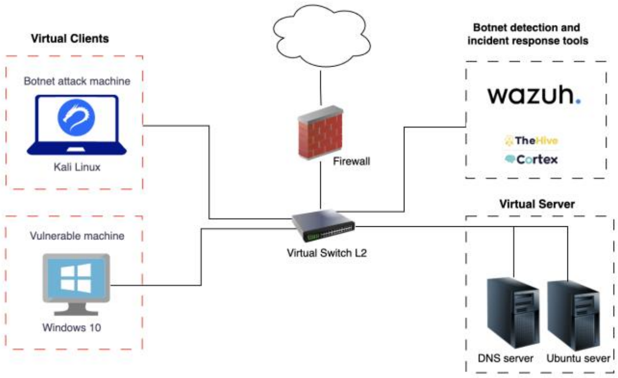

Fig. 3. A proposed testbed

V. Conclusion and Future Work

In conclusion, this study has conducted a comprehensive literature review on detection and incident response frameworks in Security Operations Centers (SOCs). By analyzing the main components, security tools, and cybersecurity standards used in these frameworks, this research has identified several research gaps that can be used to develop more effective and comprehensive botnet detection frameworks. Future work will focus on conducting evaluation and validation studies to assess the effectiveness and performance of the framework by implementing the experiment approach in controlled environment. Additionally, gathering feedback from cybersecurity experts to validate this framework and identify areas for improvement. Overall, this research contributes to the existing body of knowledge in cybersecurity by providing insights into the development and implementation of botnet detection and incident response frameworks in SOCs.

ACKNOWLEDGMENT

This work was supported/funded by the Ministry of Higher Education under Fundamental Research Grant Scheme (FRGS/1/2021/ICT07/UTM/02/2).

REFERENCES

[1] P. Wainwright and H. Kettani, “An analysis of botnet models,” ACM International Conference Proceeding Series, pp. 116–121, 2019, doi: 10.1145/3314545.3314562.

[2] E. C. Ogu, O. A. Ojesanmi, O. Awodele, and S. Kuyoro, “A botnets circumspection: The current threat landscape, and what we know so far,” Information (Switzerland), vol. 10, no. 11, 2019, doi: 10.3390/info10110337.

[3] N. Goodman, “A Survey of Advances in Botnet Technologies,” Feb. 2017, [Online]. Available: http://arxiv.org/abs/1702.01132.

[4] Z. Ismail, A. Jantan, and M. N. Yusoff, “A framework for detecting botnet command and control communication over an encrypted channel,” International Journal of Advanced Computer Science and Applications, vol. 11, no. 1, pp. 319–326, 2020, doi: 10.14569/ijacsa.2020.0110140.

[5] A. S. Mashaleh, N. F. Binti Ibrahim, M. Alauthman, and A. Almomani, “A Proposed Framework for Early Detection IoT Botnet,” Institute of Electrical and Electronics Engineers (IEEE), Jan. 2023, pp. 1–7. doi: 10.1109/acit57182.2022.9994166.

[6] Y. Xing, H. Shu, F. Kang, and H. Zhao, “Peertrap: An Unstructured P2P Botnet Detection Framework Based on SAW Community Discovery,” Wirel Commun Mob Comput, vol. 2022, 2022, doi: 10.1155/2022/9900396.

[7] “Protecting SME From Cyber Attacks.” Accessed: Apr. 11, 2023. [Online]. Available: https://www.kkd.gov.my/en/pengumuman-kkmm/233-kpkk-news/19611-protecting-sme-from-cyber-attacks.

[8] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, “Security Operations Center: A Systematic Study and Open Challenges,” IEEE Access, 2020, doi: 10.1109/ACCESS.2020.3045514.

[9] M. Majid and K. Ariffi, “Success Factors for Cyber Security Operation Center (SOC) Establishment,” European Alliance for Innovation n.o., Oct. 2019. doi: 10.4108/eai.18-7-2019.2287841.

[10] A. Caglayan, M. Toothaker, D. Drapeau, D. Burke, and G. Eaton, “Behavioral analysis of botnets for threat intelligence,” Information Systems and e-Business Management, vol. 10, no. 4, pp. 491–519, 2012, doi: 10.1007/s10257-011-0171-7.

[11] M. S. Abu, S. R. Selamat, A. Ariffin, and R. Yusof, “Cyber threat intelligence – Issue and challenges,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 10, no. 1, pp. 371–379, Apr. 2018, doi: 10.11591/ijeecs.v10.i1.pp371-379.

[12] O. C. Briliyant, N. P. Tirsa, and M. A. Hasditama, “Towards an Automated Dissemination Process of Cyber Threat Intelligence Data using STIX,” in Proceedings - IWBIS 2021: 6th International Workshop on Big Data and Information Security, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 109–114. doi: 10.1109/IWBIS53353.2021.9631850.

[13] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, “Cyber threat intelligence sharing: Survey and research directions,” Comput Secur, vol. 87, Nov. 2019, doi: 10.1016/j.cose.2019.101589.

[14] H. Singh and A. Bijalwan, “A Framework on botnet detection and forensics,” Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering, vol. 10, no. June, pp. 93–101, 2017, doi: 10.15439/2017r28.

[15] J. Álvarez Cid-Fuentes, C. Szabo, and K. Falkner, “An adaptive framework for the detection of novel botnets,” Comput Secur, vol. 79, pp. 148–161, Nov. 2018, doi: 10.1016/j.cose.2018.07.019.

[16] S. S. Awad, “Collaborative Framework for Early Detection of RAT-Bots Attacks,” 2019.

[17] Y. T. Dun, M. F. A. Razak, M. F. Zolkipli, T. F. Bee, and A. Firdaus, “Grasp on next generation security operation centre (NGSOC): Comparative study,” International Journal of Nonlinear Analysis and Applications, vol. 12, no. 2, pp. 869–895, Jun. 2021, doi: 10.22075/ijnaa.2021.5145.

[18] H. J. Ofte and S. Katsikas, “Understanding situation awareness in SOCs, a systematic literature review,” Comput Secur, vol. 126, Mar. 2023, doi: 10.1016/j.cose.2022.103069.

[19] Z. Iqbal and Z. Anwar, “SCERM—A novel framework for automated management of cyber threat response activities,” Future Generation Computer Systems, vol. 108, pp. 687–708, Jul. 2020, doi: 10.1016/j.future.2020.03.030.

[20] C. Islam, M. A. Babar, R. Croft, and H. Janicke, “SmartValidator: A framework for automatic identification and classification of cyber threat data,” Journal of Network and Computer Applications, vol. 202, Jun. 2022, doi: 10.1016/j.jnca.2022.103370.

[21] L. Axon, J. Happa, A. J. Van Rensburg, M. Goldsmith, and S. Creese, “Sonification to Support the Monitoring Tasks of Security Operations Centres,” IEEE Trans Dependable Secure Comput, vol. 18, no. 3, pp. 1227–1244, May 2021, doi: 10.1109/TDSC.2019.2931557.

[22] M. Saraiva and N. Coelho, “CyberSoc Implementation Plan,” in 10th International Symposium on Digital Forensics and Security, ISDFS 2022, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ISDFS55398.2022.9800819.

[23] D. Shahjee and N. Ware, “Integrated Network and Security Operation Center: A Systematic Analysis,” IEEE Access, vol. 10, pp. 27881–27898, 2022, doi: 10.1109/ACCESS.2022.3157738.

[24] P. Rajesh, M. Alam, M. Tahernezhadi, A. Monika, and G. Chanakya, “Analysis Of Cyber Threat Detection And Emulation Using MITRE Attack Framework,” 2022 International Conference on Intelligent Data Science Technologies and Applications, IDSTA 2022, pp. 4–12, 2022, doi: 10.1109/IDSTA55301.2022.9923170.

[25] P. Bajpai and R. Enbody, “Know Thy Ransomware Response: A Detailed Framework for Devising Effective Ransomware Response Strategies,” Digital Threats: Research and Practice, Jun. 2023, doi: 10.1145/3606022.

[26] I. Ghafir et al., “BotDet: A System for Real Time Botnet Command and Control Traffic Detection,” IEEE Access, vol. 6, pp. 38947–38958, 2018, doi: 10.1109/ACCESS.2018.2846740.

[27] A. F. Jabbar and I. J. Mohammed, “Development of an Optimized Botnet Detection Framework based on Filters of Features and Machine Learning Classifiers using CICIDS2017 Dataset,” in IOP Conference Series: Materials Science and Engineering, IOP Publishing Ltd, Nov. 2020. doi: 10.1088/1757-899X/928/3/032027.

[28] W. N. H. Ibrahim, M. S. Anuar, A. Selamat, and O. Krejcar, “BOTNET DETECTION USING INDEPENDENT COMPONENT ANALYSIS,” IIUM Engineering Journal, vol. 23, no. 1, pp. 95–115, 2022, doi: 10.31436/IIUMEJ.V23I1.1789.

[29] F. F. Daneshgar and M. Abbaspour, “A two-phase sequential pattern mining framework to detect stealthy P2P botnets,” Journal of Information Security and Applications, vol. 55, Dec. 2020, doi: 10.1016/j.jisa.2020.102645.

[30] J Jiang, Q Yin, Z Shi, M Li, and B Lv, A New C&C Channel Detection Framework Using Heuristic Rule and Transfer Learning. 2019.

[31] Y. Ti Dun, M. Faizal, A. Razak, M. F. Zolkipli, T. F. Bee, and A. Firdaus, “Hermes Ransomware v2.1 Action Monitoring using Next Generation Security Operation Center (NGSOC) Complex Correlation Rules,” vol. 12, no. 3, 2022.

[32] J. Wang et al., “A comprehensive security operation center based on big data analytics and threat intelligence PoS(ISGC2021)028,” 2021. [Online]. Available: https://pos.sissa.it/.

[33] A. C. T. Lai et al., “RansomSOC: A More Effective Security Operations Center to Detect and Respond to Ransomware Attacks,” Journal of Internet Services and Information Security, vol. 12, no. 3, pp. 63–75, Aug. 2022, doi: 10.22667/JISIS.2022.08.31.063.

[34] D. Shahjee and N. Ware, “Designing a Framework of an Integrated Network and Security Operation Center: A Convergence Approach,” in 2022 IEEE 7th International conference for Convergence in Technology, I2CT 2022, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/I2CT54291.2022.9825084.

[35] D. Crooks, L. Vâlsan CERN, and A. Sinica, “Building a minimum viable Security Operations Centre for the modern grid environment,” 2019. [Online]. Available: https://pos.sissa.it/