International Journal on Advanced Science Engineering Information Technology

Vol.12 (2022) No. 3
ISSN: 2088-5334

Hermes Ransomware v2.1 Action Monitoring using Next Generation Security Operation Center (NGSOC) Complex Correlation Rules

Yau Ti Dun [a, b], Mohd Faizal Ab Razak [a,*], Mohamad Fadli Zolkipli [c], Tan Fui Bee [a, b], Ahmad Firdaus [a]

[a] *Faculty of Computing, Universiti Malaysia Pahang, Pahang, 26600, Malaysia*
[b] *Sysarmy Sdn Bhd, Wisma Zelan, No 12, 1, Jalan Tasik Permaisuri 2, Bandar Tun Razak, 56000, Kuala Lumpur, Malaysia*
[c] *School of Computing, UUM College Arts & Sciences, Universiti Utara Malaysia, 06010, Kedah, Malaysia*
*Corresponding author: *faizalrazak@ump.edu.my*

***Abstract*—A new malware is identified every fewer than five seconds in today's threat environment, which is changing at a rapid speed. As part of cybercrime, there is a lot of malware activity that can infect the system and make it problematic. Cybercrime is a rapidly growing field, allowing cyber thieves to engage in a wide range of damaging activities. Hacking, scams, child pornography, and identity theft are all examples of cybercrime. Cybercrime victims might be single entities or groups of persons who are being targeted for harm. Cybercrime and malware become more hazardous and damaging because of these factors. Subsequent to these factors, there is a need to construct Next Generation Security Operation Centers (NGSOCs). SOC consists of human resources, processes, and technology designed to deal with security events derived from the Security Incident Event Management (SIEM) log analysis. This research examines how Next Generation Security Operation Centers (NGSOCs) respond to malicious activity. This study develops a use case to detect the latest Hermes Ransomware v2.1 malware using complex correlation rules for the SIEM anomalies engine. This study aims to analyze and detect Hermes Ransomware v2.1. As a result, NGSOC distinguishes malware activities' initial stages by halting traffic attempts to download malware. By forwarding logs to SIEM, the use case can support Threat Analyst in finding other Indicators of Compromise (IOC) to assist organizations in developing a systematic and more preemptive approach for ransomware detection.**

***Keywords*— SIEM; NGSOC; ransomware; correlation rule; malware.**

Manuscript received 23 May 2021; revised 18 Nov. 2021; accepted 17 Jan. 2022. Date of publication 30 Jun. 2022.
IJASEIT is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.

I. INTRODUCTION

According to a 2017 Symantec corporation report, data breaches exposed more than 7.1 billion identities [1], [2]. Cyber-attacks caused unprecedented amounts of damage by using very unsophisticated tools and methods to make a big impact [3], [4]. Carefully, zero-day vulnerabilities and advanced malware are still being used, and attackers are deliberately covered up [5], [6]. The use of tools such as legal system management software and operating system features is simple: spear-phishing e-mails and "living out of the field" [3], [7].

Furthermore, a study demonstrates that the attack environment is categorized by more concentrated, clever, sophisticated, and advanced techniques such as Advanced Persistent Threats (APTs. The organizations cannot cope with the increasing volume and frequency of cyber-attacks and cannot provide control of the condition [8], [9]. In turn, user data can be encrypted using advancing coding algorithms [10] by malware like ransomware. When the malware encryption has effectively encrypted all targeted documents, the victim's computer screen will display a ransom notice telling them about the virus that cybercriminals are carrying malware. In this case, the malware author will need cryptocurrency in exchange for a decryption key that is thought to unlock data. The fearful pop-up alert warns users that the future of locked records will remain closed for good unless the user pays the required money.

Ransomware programs vary greatly from backdoors, spyware, trojan horses, malware, and worms [11]. For example, in formal paraphrasing, anti-virus software does not detect ransomware CryptoWall 4.0 compared to other malware [12]. Formal paraphrase the real reason for this is due to how this form of malware implements its agenda [13]. Infecting the device with ransomware would not corrupt or alter the data at first. It would not impact the actual data. If an adverse event occurs, most anti-virus programs are not alerted. Data malware encryption is not dangerous, and the target documents are not in danger. However, as users do not have a

key to encrypting files, they cannot access their data. This is one of the most important aspects that makes it so difficult to fight.

Ransomware Hermes v2.1 may sneak into the computer in various ways. It can be in an e-mail attachment, drive-by-download websites, or bundled to freeware and shareware spread throughout the internet. Once executed, Hermes ransomware encrypts selected files on the computer using a complex algorithm. Most ransomware in recent days is using the same technique to demand payment for users to recover infected files. While encrypting important files, this ransomware may append the extension with '.HERMES'. The intruder then requests a fee to be paid in order to receive decryption instructions. Hermes virus creators seek payment in Bitcoin cash, which can be processed via their designated payment scheme. The trick is that anonymized transactions are even harder to follow electronic currencies like Bitcoin [13]. Software bugs and vulnerabilities are the most popular entry point. The virus is activated to exploit vulnerabilities and spread target compute infection when a malicious e-mail attachment is opened. Ransomware scans and encodes target files using advanced methods of encoding. The security analytical flow is used to construct a rule on malware detection based on the family ransomware. Most SIEM solutions are defined in the rules Figure 1.

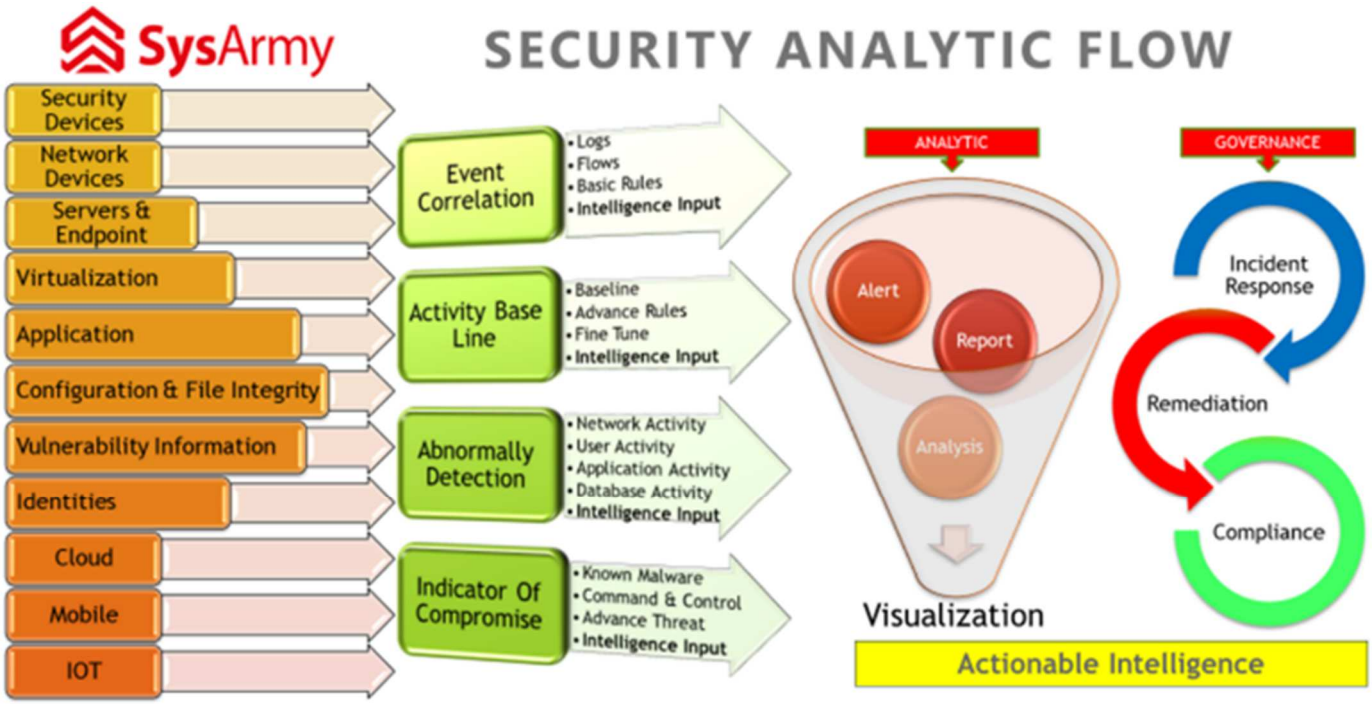

Fig. 1 NGSOC Security Analytic Flow

SIEM is a solution that provides a holistic element of the IT infrastructure's security situation. The key goals of SIEM are the detection and maintenance of almost real-time security incidents' collecting information from various network devices, including logs, events, and network flows, and comparing and analyzing data to detect incidents and abnormal operating patterns. A SIEM, when correctly implemented and configured, helps organizations discover internal/external risks [14].

SIEM systems use different conditions to determine if such events fit a law, and an alarm may be activated based on the danger. In general, there are three types of conditions such as event, rule, and anomaly based. When an alarm is activated, the team investigates it and escalates the incident to the appropriate team for resolution. The job of creating rules is carried out by threat analysts who are constantly looking for Indicators of Compromise (IOC) by reviewing threat intelligence feeds.

II. Materials and Method

The enormous growth in the number, level and capability of cyber-attacks to proliferate over the last three years and have infected thousands of networks global. The Center for Defense Operations is the most important and core part of these established threats (SOC). The increase in the volume and range of threats leads to an exponential increase in the number of firms building SOCs of different forms and dimensions. The 2016 Global Information Security Survey notes that SOC is available in 56% of the organizations surveyed [15]. The importance of unified, consolidated cybersecurity incident prevention, detection, and response [16] [17] will grow as more companies understand [18].

Organizations utilized SIEM to design their SOC as their security management system. This made sense because the security center required the central collection and management of logs and the simple correlation and warning of detection. However, security organizations are increasingly aware of the importance and significance of integrating persons, methods, and technology as an integral component

of SIEM. As a result, the SOC has grown to a new level of functionality, combining people, mechanisms, and technology [15], [16]. Now SOCs can manage longer and more complex initiatives, manage thousands of warnings and incidents daily, record and track violations, and transnational coordinate practices, resolving the issue of IT harmonization.

Threat analysts recognize safety hazards and establish preventative measures [19]. Figure 2 presents how to investigate anomalous behavior to identify new attack tactics and threats as they arise, leveraging knowledge obtained from tracking global events through thousands of portals, forums, RSS feeds, and commercial feeds – designing countermeasures that protect users and organizations from damage. Threat intelligence is another word for such knowledge. The threat data will then be fed into the SIEM correlation capability, scanning for established activity patterns for defense, enforcement, or other purposes.

The security intelligence capability seeks irregular activities which may not fit in any known pattern but can be malicious [8]. To allow analysts to identify and evaluate deviations (abnormal) using an automated statistical engine or a visual interpretation of statistics, the SIEM Security Intelligence feature focuses on statistical time series data analysis. Threat analysts manage security intelligence. The Threat Analyst will supervise Threat Monitoring, Threat Triage, Threat Response, Intelligence. Analytics and monitoring are Security Analyst's jobs. Threat analyst's responsibilities include, but are not limited to, Data management for threats, aiding with intelligence operations, and Collaborating with the incident management team. The correlation rule is shown in Fig 2.

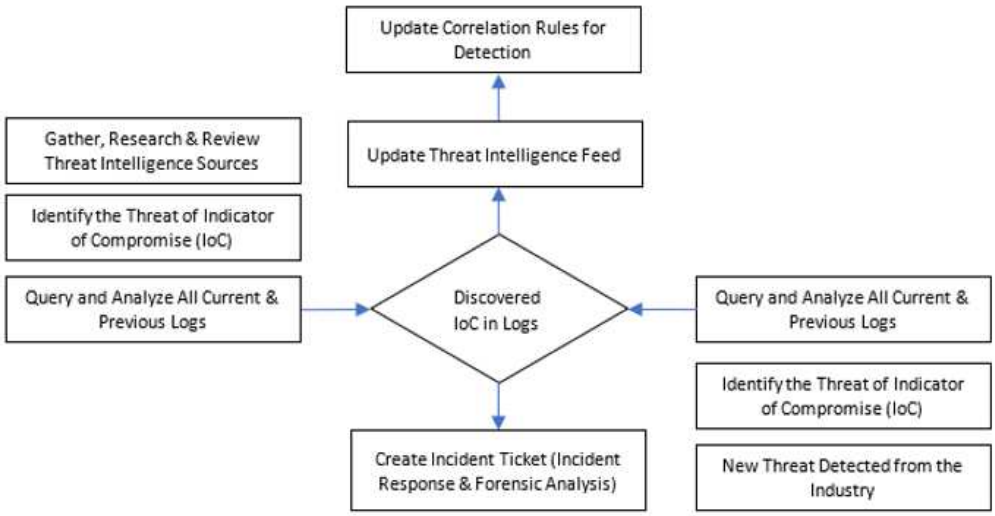

Fig. 2 Correlation Rules

The element that seeks recognizable characteristics and lines events in significant bundles is demonstrated in Figure 3 within SIEM correlation rules. Events consist of a few or more SIEM-screened logs that may or may not be malicious. A blacklist is a list of untrusted vending machines. Irregularity refers to an event that varies from the norm. Accessibility and system status are occurrences, a notice of public danger. On the other hand, information from global surveillance events is collected. A security analyst creates a safety event in the ticket system when the correlation rules are triggered.

III. Results and Discussion

Hermes ransomware, version 2.1, is the most recent version of Hermes malware, which encrypts files on a device and renders them unusable. According to the documents, the first attack occurred on February 27, 2018, at 01:54 UTC, via a compromised Korean website. Moreover, after the ransomware has been executed, the names of the infected files remain unchanged. The image below depicts a BMP file beforehand and after this ransomware encrypted it:

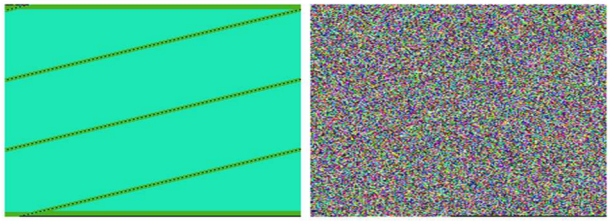

Fig. 3 Visualization of ransomware encryption

The earlier phase of the correlation rule generates a description of key compromise indicators that establish either detection rules or detection rules.

TABLE I
Summary of Hermes Ransomware v2.1

Threat Notification	**Hermes Ransomware v2.1**
Threat Type	Ransomware
Outbreak Level	Wild
Risk Level	High
Attack Vector/Method	Compromised website, Email Attachments, Executable files.
Systems Affected	Operating Systems (Windows, Mac, Linux) using Adobe Flash Player version 28.0.0.137 and earlier.

The ransomware would redeploy itself from that position after copying itself into the percent TEMP percent folder as svchosta.exe. The first sample is then discarded. Some windows, including the authorization to run a batch script with administrative privileges, can appear during execution. The batch script is in charge of deleting shadow copies and other backups.

A. Correlation Rules for Hermes Ransomware

Each SIEM, whether automated or manual, needs threat intelligence input to provide tweaked associations to minimize specific threats and risks. The advantage of manual feedback is that rules can be formulated and fine-tuned based on a specific risk scenario's risk appetite. Whether open-source or commercially licensed, more than ten popular SIEM labels are available. Each SIEM uses a different language, and correlation rules will be created in different steps between brands. However, there should be a specific technique to establish correlation rules. However, correlations are not the only technique used as the main method for interpreting the SIEM events collected. This article will concentrate on the possible similarities, what they should do, and what is inappropriate. Correlating capabilities are also spread through various modules in a single SIEM solution: some in collectors, some in intermediate aggregators, and some in core correlation engines.

Disregarding uninteresting activities is an integral stage of event processing, streamlining downstream event processing and ensuring less information overload. Filtering can be done based on event specifics, such as a dropped link from an external source via a firewall is deemed unimportant, and an IPS that blocks traffic from an external source indicates that the threat has already been neutralized. Inefficiently ransomware can be detected if the source sends particular event types. Filtering may also rely on more complex factors, including filtering following other functions. Easier filters occur at the early stage of the event life cycle and in some cases on the source device: Windows, for example, can pick which events to send to the event collector. This provides filtering distribution, maintains bandwidth in the network, and reduces the processing load on each SIEM component server.

SIEM server needs complex filtering. While many SIEMs do not define falling events, they filter by "filter in" rather than "filter out": the correlation logic selects and highlights useful events, usually through the creation of a related event in the main event monitoring channel.

B. Enriching

Source-sent events are normally restricted, and additional details must be applied to further analyses, whether automatic or manual [20]. Most enrichment data are classified as "history," which SIEM must import or learn from threat sources. A specific type of enrichment combines multiple raw log entries into one richer occurrence, each with partial information. The Collector layer will add these essential enrichment capabilities. More advanced improvements can be based on acquired data [3], [21]. This is also the stage when criteria for the correlation are developed based on malware features and how it can enter the network or connect with an external malware source IP depicted in Figure 4.

SysArmy_IOC_001.csv

```
#Malicious IP,ThreatName,Threat Category
78.130.176.223,Adwind Botnet,Botnet
78.130.176.213,Adwind Botnet,Botnet
213.208.129.198,Adwind Botnet,Botnet
79.172.242.89,Adwind Botnet,Botnet
111.118.183.211,Adwind Botnet,Botnet
212.7.218.143,Adwind Botnet,Botnet
78.130.176.192,Adwind Botnet,Botnet
78.130.176.171,Adwind Botnet,Botnet
213.208.129.219,Adwind Botnet,Botnet
216.38.7.228,Adwind Botnet,Botnet
216.38.8.187,Adwind Botnet,Botnet
184.75.210.206,Adwind Botnet,Botnet
```

Fig. 4 Malware source

Aggregation is the most basic function that focuses on "correlating" different events. It connects a variety of related events. The collection has two primary applications:

- Reduce event load by reporting much repetition, such as adding a count and time stamp to base data for the first and last incidence. This takes place at the accumulator layer.
- Recognize repeated actions, such as port scans or malware attacks.

C. Combining Rules

The master correlation rules group several events which reveal a related report. For example, if repeated download failures were followed by a good one that matched Ransomware malware hash value, it would become more important to cause rules for traffic from internal to external matching IOC ransomware [22], [23]. Sequencing is an interconnection variant that requires order among clustered events. While incident prevention is mostly connected to joints, they often filter incidents [24]. They can also, in many cases, boost or correct events by bringing together several related raw events with all relevant data. These acts are generally categorized as follows:

- Alert by the security analyst This may include an external e-mail or pop-up alert or an internal warning in the form of an incident, including in the SIEM dashboard.
- Update the case with additional details about the IOC.
- Update IOC enhancement history records, usual as html, csv, xlxs or notepad. This is also useful for managing state search tables based on incoming events like the combination of an IP address with a malicious IP list.
- Run an external action, for example, an external request or an API application. While external deed provides further rationale, the primary use of external systems, such as tickets, firewalls, intrusion detection systems, or even enhanced endpoint security is automatic remediation and integration.

D. Detection Performance

Normally, a lookup may be used to compare a field to a value chart. Though theoretically possible, no correlation engine has yet performed well in finding a partial match of multiple signatures or regular expressions within a domain [25]. One of the key correlations in the present analytic method is the minimal theoretical efficiency. Most empirical

models involve a huge amount of data that in one example, a correlation rule does not fit well. Baselining is an excellent instance: Although a rule of correlation may update a table of the baseline status, it takes time. Setting a baseline is also considerably easier if a regular query against collected events is executed. It should be observed that correlation rules can be used efficiently to calculate an event against a reference when displaying real-time results.

Correlations is the best way to analyze events as it considers each occurrence independently in memory as obtained by SIEM [26]. Correlations are used to conduct search-based research efficiently and provide more precise results in some situations. For example, for any source IP from which a firewall receives communication for a day which can easily host the resources of a SIEM server, it would have to hold an open context if a rule attempted to define a "slower" port scan in a daytime window. Table 1 shows information on vulnerability sign aspects that influence the correlation rules that can be utilized to detect ransomware infection and proliferation elements.

TABLE II
COMPROMISE INDICATOR

Domain involved in campaign	staradvertsment[.]com
	hunting.bannerexposure[.]info
	accompanied.bannerexposure[.]info
	switzerland.innovativebanner[.]info
	name.secondadvertisements[.]com
	assessed.secondadvertisements[.]com
	marketing.roadadvertisements[.]com
	bannerssale[.]com
	aquaadvertisement[.]com
	technologies.roadadvertisements[.]com
IP addresses involved in campaign	159.65.131[.]94
	159.65.131[.]94
	207.148.104[.]5
E-mail addresses involved in campaign	pretty040782@gmail[.]com
	pretty040782@keemail[.]me
File hash value involved in campaign	A5A0964B1308FDB0AEB8BD5B2A0F306C999 97C7C076D66EB3EBCDD68405B1DA2

To ensure correlation rules for effective ransomware monitoring, Hitherto, the controversy has centered on the methodological implications of correlation laws. The goal was to dispel some obscurity that traditional usage case-based correlation descriptions often motivated by marketing rather than technical considerations. Now that we have a clearer understanding of the features provided by correlation rules, we will return to use case and clarify how correlation rules contribute to the effective detection of ransomware.

AES is an algorithm that uses a random key to encrypt files. Ransomware uses two RSA key pairs: an attackers' hard-coded public key [12]. Then the survivor's vital pair. It's generated at the attack started. This key pair's private key is encrypted with the public key of the attackers and saved NOT REMOVE in the UNIQUE ID format. When the victim delivers this file, attackers can save the victim's private key using their own private key. The victim's public key is plain text in PUBLIC. The use of encrypting randomly generated AES keys per file is shown in Figure 4, which provides an example of the affected file.

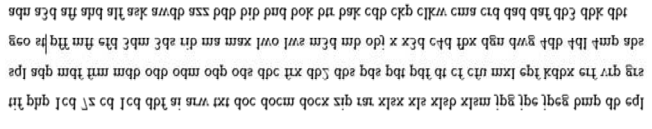

Fig. 5 Infected by Ransomware

IV. CONCLUSION

Online sources, including Global Threat Notification, news feeds, market papers, and social media, can find several compromise indicators (IOCs). These use cases may be useful for formulating correlation rules and helping Threat Analyst consider how to construct further. Most use cases are company-specific and require some tinkering to satisfy environmental needs. The good news is that nothing breaks when building these rules. Each rule would result in a better-monitored environment, reducing the time needed to detect a cyber-attack.

Ransomware has lately become a profitable hacker business and has evolved into a new form of malware. In developing a more proactive approach to detecting and recovering from cyberattacks, companies need new launching ransomware attacks. The results from this study will support organizations that use advanced correlation laws to create a systemic structure for detecting Ransomware.

ACKNOWLEDGMENT

This work was supported in part by the SysArmy Sdn Bhd and Faculty of Computing, UMP (Project ID: UIC190807)

REFERENCES

[1] GData blog, "Malware trends 2017," 2018.

[2] Gartner, "Rethink Your Security & Risk Strategy with 2021 Cybersecurity Frameworks and Best Practices," 2021.

[3] S. Abijah Roseline and S. Geetha, "A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks," *Comput. Electr. Eng.*, vol. 92, no. May, p. 107143, 2021, doi: 10.1016/j.compeleceng.2021.107143.

[4] S. R. T. Mat, M. F. Ab Razak, M. N. M. Kahar, J. M. Arif, S. Mohamad, and A. Firdaus, "Towards a systematic description of the field using bibliometric analysis: malware evolution," *Scientometrics*, vol. 126, no. 3, pp. 2013–2055, 2021, doi: 10.1007/s11192-020-03834-6.

[5] H. Hanif, M. H. N. Md Nasir, M. F. Ab Razak, A. Firdaus, and N. B. Anuar, "The rise of software vulnerability: Taxonomy of software vulnerabilities detection and machine learning approaches," *J. Netw. Comput. Appl.*, vol. 179, no. February, p. 103009, 2021, doi: 10.1016/j.jnca.2021.103009.

[6] 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," *Int. J. Nonlinear Anal. Appl.*, vol. 12, no. 2, pp. 869–895, 2021, doi: 10.22075/ijnaa.2021.5145.

[7] S. R. T. Mat, M. F. A. Razak, M. N. M. Kahar, J. M. Arif, and A. Firdaus, "A Bayesian probability model for Android malware detection Sharfah," *ICT Express*, pp. 1–12, 2021, doi: 10.1016/j.icte.2021.09.003.

[8] S. R. T. Mat, M. F. A. Razak, M. N. M. Kahar, J. M. Arif, S. Mohamad, and A. Firdaus, "Towards a systematic description of the field using bibliometric analysis: malware evolution," *J. Sci.*, pp. 1–38, 2021.

[9] M. F. J. Klaib, M. R. A. Sara, and M. Hasan, "D-GREEDY: Greedy shortest superstring with delayed random choice," *Int. J. Softw. Eng. Comput. Syst.*, vol. 6, no. 1, pp. 8–17, 2020.

[10] W. Z. A. Zakaria, M. F. Abdollah, O. Mohd, and A. F. M. Ariffin, "The rise of ransomware," *ACM Int. Conf. Proceeding Ser.*, no. May, pp. 66–70, 2017, doi: 10.1145/3178212.3178224.

[11] R. Jusoh, A. Firdaus, S. Anwar, M. Z. Osman, M. F. Darmawan, and M. F. Ab Razak, "Malware detection using static analysis in Android: a review of FeCO (features, classification, and obfuscation)," *PeerJ Comput. Sci.*, vol. 7, no. e522, pp. 1–54, 2021, doi: 10.7717/peerj-cs.522.

[12] A. Alabdulatif, H. Kumarage, I. Khalil, and X. Yi, "Privacy-preserving anomaly detection in cloud with lightweight homomorphic encryption," *J. Comput. Syst. Sci.*, vol. 90, no. May, pp. 28–45, 2017, doi: 10.1016/j.jcss.2017.03.001.

[13] T. Dargahi, A. Dehghantanha, P. N. Bahrami, M. Conti, G. Bianchi, and L. Benedetto, "A Cyber-Kill-Chain based taxonomy of crypto-ransomware features," *J. Comput. Virol. Hacking Tech.*, vol. 15, no. 4, pp. 277–305, 2019, doi: 10.1007/s11416-019-00338-7.

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

[15] P. Danquah, "Security Operations Center: A Framework for Automated Triage, Containment and Escalation," *J. Inf. Secur.*, vol. 11, no. 04, pp. 225–240, 2020, doi: 10.4236/jis.2020.114015.

[16] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, "Towards a Framework for Measuring the Performance of a Security Operations Center Analyst," *Int. Conf. Cyber Secur. Prot. Digit. Serv. Cyber Secur. 2020*, 2020, doi: 10.1109/CyberSecurity49315.2020.9138872.

[17] O. V. Lee *et al.*, "A malicious URLs detection system using optimization and machine learning classifiers," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 17, no. 3, pp. 1210–1214, 2020, doi: 10.11591/ijeecs.v17.i3.pp1210-1214.

[18] W. P. Aung, H. H. Lwin, and K. K. Lin, "Developing and Analysis of Cyber Security Models for Security Operation Center in Myanmar," *2020 IEEE Conf. Comput. Appl. ICCA 2020*, pp. 1–6, 2020, doi: 10.1109/ICCA49400.2020.9022821.

[19] N. N. M. Nasri, M. F. A. Razak, R. D. R. Saedudin, S. Mohamad-Asmara, and A. Firdaus, "Android malware detection system using machine learning," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 1 Special Issue 5, pp. 327–333, 2020, doi: 10.30534/ijatcse/2020/4691.52020.

[20] B. Bouyeddou, F. Harrou, B. Kadri, and Y. Sun, "Detecting network cyber-attacks using an integrated statistical approach," *Cluster Comput.*, vol. 24, no. 2, pp. 1435–1453, 2021, doi: 10.1007/s10586-020-03203-1.

[21] N. Miloslavskaya and S. Furnell, "Network Security Intelligence Centres for Information Security Incident Management," *Adv. Intell. Syst. Comput.*, vol. 1310, no. May, pp. 270–282, 2021, doi: 10.1007/978-3-030-65596-9_34.

[22] R. Malkawe, M. Qasaimeh, F. Ghanim, and M. Ababneh, "Toward an early assessment for ransomware attack vulnerabilities," *ACM Int. Conf. Proceeding Ser.*, no. May, p. 3368734, 2019, doi: 10.1145/3368691.3368734.

[23] Infoblox, "Hermes Ransomware Cyber Report," *Pp 1-3*, no. February 2017, pp. 2017–2019, 2017.

[24] J. ho Hwang, J. Kwak, and T. jin Lee, "Fast k-NN based Malware Analysis in a Massive Malware Environment," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 12, pp. 6145–6158, 2019, doi: 10.3837/tiis.2019.12.019.

[25] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," *IEEE Access*, no. May, p. 3045514, 2020, doi: 10.1109/ACCESS.2020.3045514.

[26] M. H. Khyavi, "ISMS role in the improvement of digital forensics related process in SOC's," *Cryptogr. Secur.*, 2020.