Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning

Article *in* Procedia Computer Science · January 2023

DOI: 10.1016/j.procs.2022.12.339

3 authors, including:

Aulia Arif Wardana
Telkom University
38 PUBLICATIONS **218** CITATIONS

SEE PROFILE

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 217 (2023) 1406–1415

Procedia Computer Science

www.elsevier.com/locate/procedia

4th International Conference on Industry 4.0 and Smart Manufacturing

Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning

Adabi Raihan Muhammad[1], Parman Sukarno [1], Aulia Arif Wardana[2]*

[1]*Telkom University, Bandung, Indonesia*
[2]*Wrocław University of Science and Technology, Wrocław, Poland*

Abstract

This research builds Security Information & Event Management (SIEM) based on live analysis using machine learning on Intrusion Detection System (IDS). To implement a live analysis technique on IDS using machine learning that is integrated with SIEM, we need a combined system with many processes and services. All processes and services must be orchestrated and combined into one system to make live analysis work. Selection of the right components to be combined into a system that can build live analysis techniques on IDS using machine learning that are integrated with SIEM is needed. In addition, an open-source system for easy deployment is needed in the industrial application. Therefore, this research tries to build the system using most common open-source components for cyberattack live analysis, detection, and monitoring. This research uses a combination of Elastic (ELK) Stack, Slips, and Zeek IDS to build the system. To ensure that the components selected are correct, robust, and reliable, it is necessary to measure the performance of the combined system. Measurement focuses on measuring the performance of resource consumption (CPU and RAM). The proposed system is testing using Denial of Service (DoS) test with 344.1/sec packet. The performance testing shows Elasticsearch is the most component that uses CPU and RAM consumption with 78% of CPU usage and 2300 Mb of RAM usage. The least CPU and RAM consumption is Zeek with 3.5% CPU usage and 225 Mb RAM usage. The proposed system also worked for detecting DoS attacks on the network.

* Corresponding author.
E-mail address: auliawardan@telkomuniversity.ac.id / aulia.wardana@pwr.edu.pl

1877-0509
10.1016/j.procs.2022.12.339

Keywords: cyberattack, intrusion detection, machine learning, SIEM, live analysis;

1. Introduction

SIEM is a system that can manage cyberattack logs generated by several data sources. Commonly, SIEM gets several cyberattack data sources from IDS. SIEM can also be used as live monitoring for real-time network traffic flow from several IDS [1]. The IDS acts like a sensor to capture the network traffic flow and detect anomalies on a network [2][3]. Basically, IDS is just detecting the cyberattack in the network using rule-based method and giving alarm to IT or cybersecurity team on the company. These types of IDS cannot detect the unknown threat because they rely on standard rule or signature [4]. Due to the increase of cyber-attacks with new types of attack, it is nearly impossible to always add an attack pattern/signature to a security parameter because it needs a repeating process that is not effective [5]. Therefore, an IDS with anomaly detection technique is needed. Anomaly Detection is a method using machine learning techniques that can detect if a packet in the network has suspicious behavior that is almost similar to a cyber-attack [6]. Using anomaly detection increases the effectiveness of the network in preventing attacks because of the pattern of the user so that the system learns the pattern, it classifies if there is a packet that is different from usual, and the system classifies that packet as an anomaly packet [7]. Live analysis for anomaly detection is also important to ensure the current network traffic is normal or abnormal. So, anomaly detection in each of the IDS needs to be done in live analysis mode [8].

The live analysis techniques on IDS using machine learning that are integrated with SIEM like described previously are a combined system with many processes and services. Right selection of the component and good configuration of system deployment is also needed to make robust and reliable live analysis technique on IDS using machine learning that are integrated with SIEM. It is also important to have open-source systems that are easy to deploy for industrial applications. There are some research questions to address that problem. Here is the list:

1. What is the form of architecture and open-source components that can be used to create a live analysis technique system on IDS using machine learning that are integrated with SIEM?
2. How is the performance of each component to become a combined system for live analysis technique on IDS using machine learning that are integrated with SIEM?

To answer the research question, this research tries to create a real implementation system for live analysis technique on IDS using machine learning that is integrated with SIEM to help IT security team on industry. The system builds using most common open-source components for cyberattack live analysis, detection, and monitoring. This research measures the performance of the combined system to ensure that the components selected are correct, robust, and reliable.

This research has been organized into 5 sections to present the integrated SIEM and live analysis in IDS using machine learning for industrial use. The first section is Introduction. This section describes the motivation and background of the research. The second section is Literature review. This section will explain about the contribution of this research and explain the difference between this research and other research. The third section is Methods. This section explains the methodology used to create the system. The fourth is the Implementation and Evaluation. This section explores the detail of the implementation environment of the system. This section also discusses the tests scenario and result from the proposed system. The last section is the Conclusion. This section resumes and concludes all previous sections.

2. Literature Review

This section provides an overview of related papers and studies in the field of integrated SIEM and IDS on the network. This section investigates the difference between the proposed model and system in this research and another related research.

Cakmakci et al. [9] proposed SIEM to detect DDoS attacks on the network. This research uses ontologies methods to detect, recover, and respond to DDoS attacks. This research combines three security tools like firewalls, antivirus, and IDS/IPS to integrate with SIEM. This research used signature-based detection to detect DDoS attacks. This research is prepared to be implemented for IT organizations or industrial ready. Azodi et al. [10] more focus on

processing the log for integrate IDS and SIEM. This research also employs a signature-based method to analyze the traffic. Laue et al. [11] create integration of IDS and SIEM using anomaly detection method. This research stores the data into a database first then the data is analyzed. The research also used open-source tools to build the SIEM system. Anumol et al. [12] use machine learning algorithms with SIEM for attack prediction. The research uses open-source security information management (OSSIM) to perform cyber-attack analysis. The research uses Support Vector Machine (SVM) as machine learning algorithm to analyze cyber-attacks Hristov et al. [13] using enterprise SIEM for DDoS attack detection in Internet of Things (IoT) environment. The enterprise SIEM is using Splunk Enterprise and it's not free. Moukafih et al. [14] using mobile agent methods for event collection and normalization in SIEM. This research is expected to get real-time data when gathering log from multiple sources. Majeed et al. [15] build visual analysis of SIEM rules for real-time monitoring of cyberattacks in the network. This research uses rule-based detection to detect cyberattacks in the network in real-time mode. Detken et al. [16] proposed SIEM with open source software and build specifically for small-medium-enterprise (SME). The SIEM system with open-source tools is very suitable for SME. The detection method is using graph pattern method to detect cyberattack.

Based on some previous research, there is no integrated SIEM and IDS with anomaly detection method in live analysis mode. Live analysis mode in anomaly detection method means that machine learning detection and network monitoring need to perform in real-time. The SIEM also gives telegram and email alerts to the IT team when cyberattack alarm detection occurs. The system in this research is also built using opensource software and suitable for industrial applications, especially for SME because opensource software is low cost.

3. Method

This section explains about the system specification for build implemented SIEM and IDS with industrial used. This research is using opensource tools to build SIEM for live analysis-based machine learning on IDS. The opensource system is expected to help IT technicians in industry or companies to implement and use this research on their network to monitor the cyber-attack. The general of our proposed system can be seen in Fig 1.

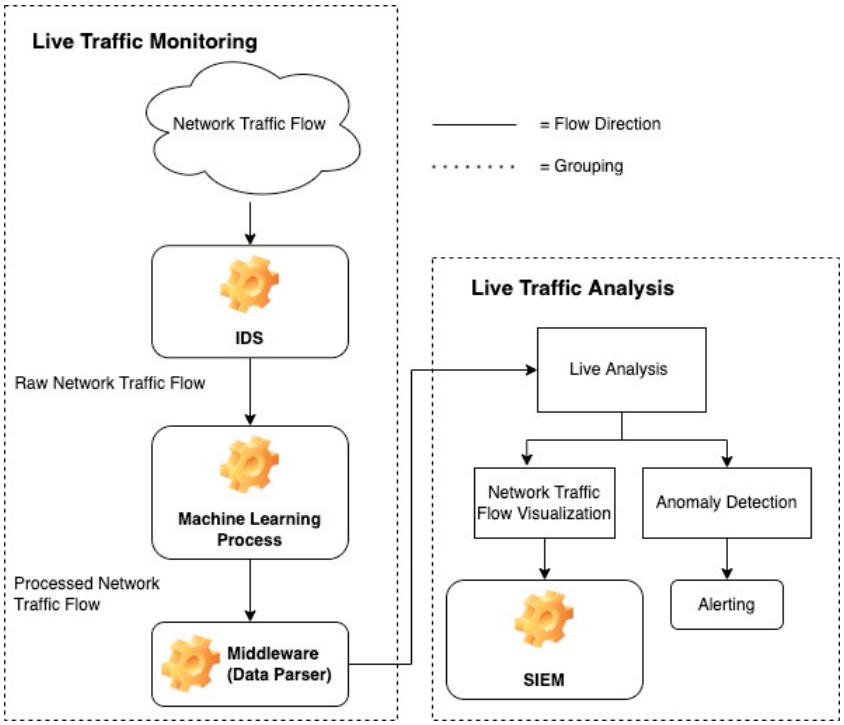


Fig 1 General system architecture.

The general proposed system is based on some research. Bertoli et al. [17] explains how important it is to use machine learning in opensource IDS because nowadays, there are so many types of cyber-attack that we are not aware of (Zero Days) and author says DoS is one of the most attacks to make network services unavailable. Research from Waleed et al. [18] study and compare several open-source IDS while using them with machine learning, and the result is that Zeek and Snort have the best accuracy with several machine learning. Granadillo et al. [19] compare several monitoring systems like ELK Stack and OSSIM. ELK Stack is the best overall monitoring system because it has many features and is easy to use for monitoring networks

Based on several previous research, this research proposes SIEM using ELK stack, IDS using Zeek IDS, and live analysis machine learning using Slips. This research uses a DoS attack as a cyberattack sample for testing the system. This study proposes an integrated IDS and SIEM system that can do live monitoring and machine learning processes at the same time. The purpose of the system is to process current network traffic immediately by machine learning to detect anomaly packets and display it in the monitoring system with a customizable dashboard. This research gives alerts to telegram and email when anomaly detection occurs. This system is useful for system admin and IT technicians to monitor their system in real-time mode.

3.1. Zeek as Intrusion Detection System

Zeek or Bro IDS is an IDS that can perform multi-layer analysis of network activities embedded with Zeek sensors. Zeek is an IDS that can be easily customized with other third-party applications so that it can make it easier to analyze a network flow traffic to look for anomalies on the network because the logs generated from IDS Zeek are divided into several types, examples of important logs such as can see on Table 1.

Table 1. Log Name and Description for data analysis.

Log Name	**Description**
conn.log	Transmission Control Protocol (TCP)/ User Datagram Protocol (UDP)/ Internet Control Message Protocol (ICMP) Connection
dhcp.log	Dynamic Host Configuration Protocol (DHCP) *leases*
dns.log	Domain Name System (DNS) Activity
http.log	Hypertext Transfer Protocol (HTTP) *request* and *replies*
ftp.log	File Transfer Protocol (FTP) Activity

Zeek generates many logs on their system, conn.log is the most important log in detecting anomalies because conn.log is the first log generated in establishing a connection, so conn.log is the foundation of other logs generated by Zeek. The conn.log keeps some logs generated from layer-3 and layer-4 on the Open Systems Interconnection (OSI) model. This conn.log is the input for machine learning tools to analyze whether there is a network traffic flow that has suspicious behavior or can be called an anomaly on a network [20].

3.2. Slips as a Machine Learning Process / Live Analysis

Slips is an Anomaly Detection tool based on Python and machine learning to detect anomalies in network traffic. Slips can perform live real-time analysis of network traffic originating from IDS Zeek, Suricata, and Packet Capture (PCAP) Files. Slips can highlight if there is a network traffic that is suspected of being an attack by using machine learning techniques to increase the accuracy of the anomaly detection results. Slips use machine learning techniques with the Support Vector Machine (SVM) algorithm in performing anomaly detection. Also, Slips uses behavioral techniques to detect packets suspected of being an attack, some of which include detecting long connections, detecting data exfiltration, detecting connections without DNS resolution, and many more. Slips has a training model built with a dataset of them [21].

The usage of Slips in our system can be seen in Fig 2. The log from IDS, namely conn.log is analyzed using Slips and is processed to JavaScript Object Notation (JSON) format for live monitoring in SIEM. The detail JSON format from the live analysis result can be seen in Table 2.

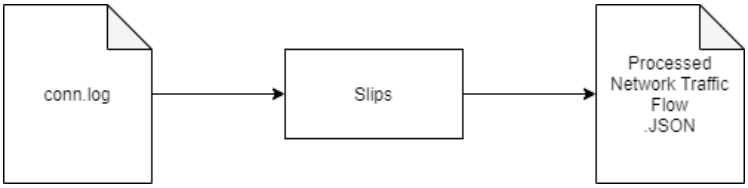


Fig 2 Slips architecture for live analysis.

Table 2. Process output from Slips in JSON format.

JSON Filed	Description
Format	Format from single value of JSON (always IDEA0)
ID	Unique character to identify single value of JSON
DetectTime	Time of attack detection
EventTime	Time of attack occur on the network
Category	Connection category
Confidence	Detection and analysis value
Note	Description of the traffic after analysis
Source	Source IP from sender or attacker
Target	Target IP from receiver or victim

3.3. ELK Stack as an SIEM / Live Monitoring

ELK Stack is a combination of three open-source components, namely Elasticsearch, Logstash, and Kibana, which are useful for Event Log Management (ELM) or can be SIEM. Logs parsed previously using the GROK programming language are directly sent through the pipeline to the ELK Stack for immediate visualization and can be directly monitored if there is a network traffic flow that has anomalies [22].

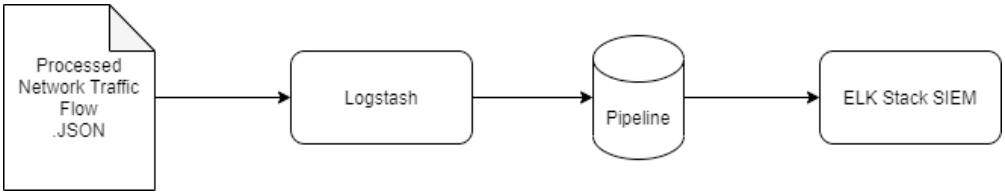


Fig 3 ELK stack architecture for SIEM live monitoring.

The usage of ELK stack as SIEM in our system can be seen in Fig 3. The JSON file that contains processed network traffic flow is processed using logstash and sent to ELK stack. The ELK stack uses this data for live monitoring. This research has also used Elastalert (one of the services from the ELK stack) to build additional features for alerting when anomaly detection is occurred.

4. Result and Discussion

This section discusses the result of implementation and evaluation of SIEM for live analysis using machine learning on IDS. The detail configuration of the system can see on this link: https://github.com/adabiraihan/IDS-based-

Machine-Learning. The system is tested in localhost environments and using Virtual Box for Linux Ubuntu, with the specification shown in Table 3.

Table 3. Hardware and Virtual Machine Specification.

Computer Hardware Specification	
CPU	Intel i7-1185G7 3.00GHz (4 Core 8 Thread)
RAM	16 GB
OS	Windows 11
Virtual Box Specification	
CPU	4 Core
RAM	8 GB
OS	Linux Ubuntu 20.04

The scenario in this system is tested by sending DoS traffic to the system with a load of 344.1/sec packet for 1 hour. The test process uses a tool called Low Orbital Ion Cannon that can DoS to specific IP in the network. This research set attack option in the tools with target on port 80, UDP traffic method, and used 10 threads. There are two components to be monitored. The two components that are monitored are ELK Stack (Elasticsearch, Logstash, and Kibana) and Zeek IDS. We cannot measure the memory usage of machine learning itself because machine learning only runs every 10 minutes.

After testing, the system works well and can detect the DoS attack. The system can make an alert after detecting the DoS attack. The attack detection alert can be seen in Fig 4. All attack detection alerts on Fig 4 are visualized by using dashboard on SIEM system. The SIEM system dashboard can be seen in Fig 5.


```
{
"Format": "IDEA0",
"ID": "e9b2aaec-f5ba-4565-861d-c236f2f0b6e6",
"DetectTime": "2022-06-12T15:31:05.681495+07:00",
"EventTime": "2022-06-12T08:35:02.046968+00:00",
"Category": ['Anomaly.Connection'],
"Confidence": 0.8,
"Note": "a connection without DNS resolution to IP: 103.132.192.30. AS: RTB HOUSE PTE. LTD.",
"Source": [{'IP4': ['192.168.0.40'], 'Type': ['Malware']}],
"Target": [{'IP4': ['103.132.192.30'], 'Type': ['Malware']}]
}
```

```
{
"Format": "IDEA0",
"ID": "b5cd7294-2fcb-4f80-805b-3849a40e8308",
"DetectTime": "2022-06-12T15:31:07.330230+07:00",
"EventTime": "2022-06-12T08:35:00.055818+00:00",
"Category": ['Intrusion.Botnet'],
"Confidence": 0.03,
"Note": "C&C channel, destination IP: 185.199.111.153 port: 443/tcp score: 0.9075",
"Source": [{'IP4': ['192.168.0.40'], 'Type': ['CC']}]
}
```

```
{
"Format": "IDEA0",
"ID": "9a69567a-1136-48bc-9ceb-9371bc481048",
"DetectTime": "2022-06-12T15:30:29.916878+07:00",
"EventTime": "2022-06-12T08:34:51.370014+00:00",
"Category": ['Recon.Scanning'],
"Confidence": 1,
"Note": "new horizontal port scan to port 443/TCP. From 192.168.0.40 to 18 unique dst IPs. Tot pkts: 529. Threat Level: medium. Confidence: 1",
"Source": [{'IP4': ['192.168.0.40'], 'Type': ['Recon']}],
"ConnCount": 529
}
```


Fig 4 Attack detection result sample.

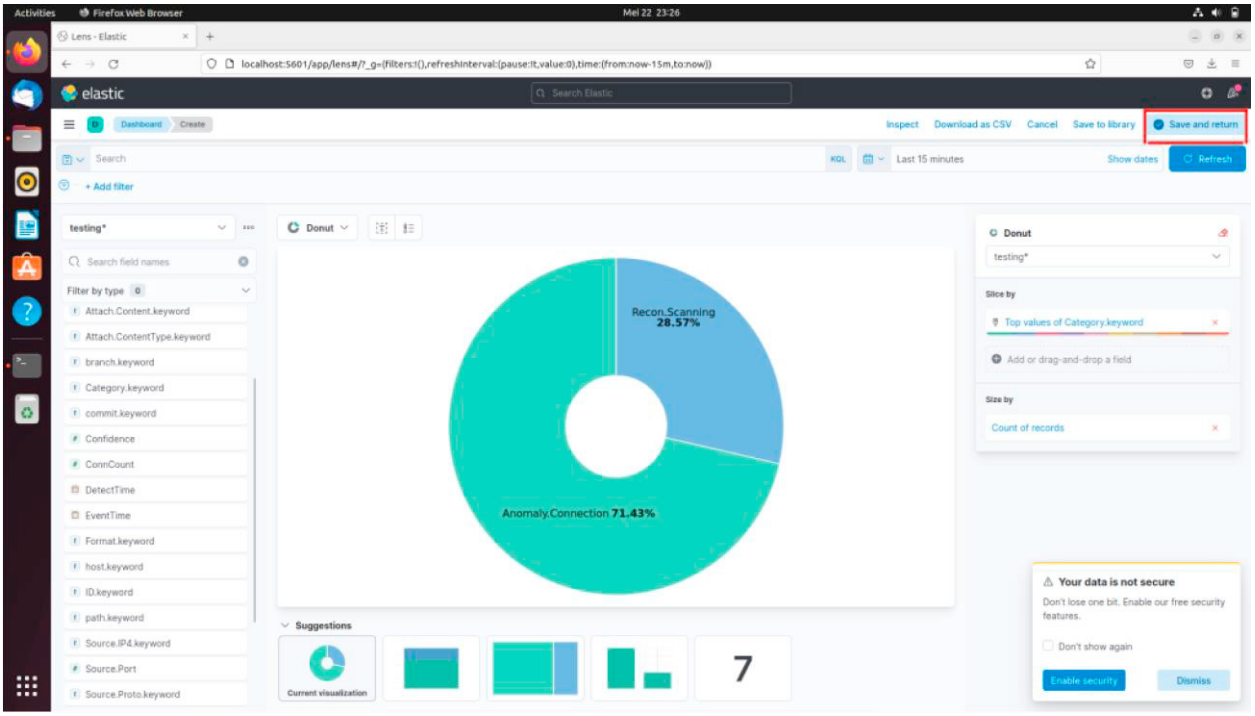
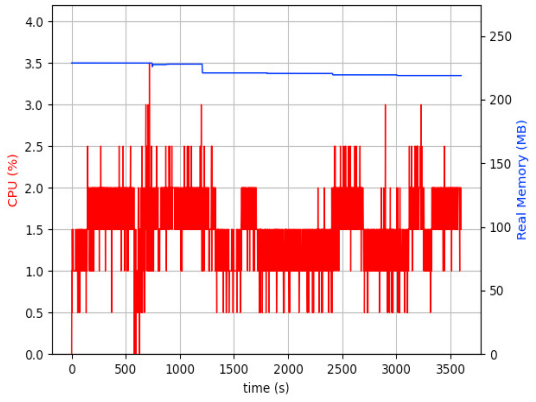
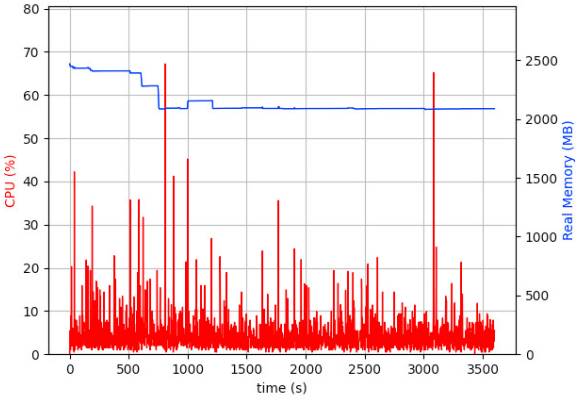


Fig 5 SIEM Dashboard.

The performance testing of 4 components (Elasticsearch, Logstash, Kibana, and Zeek) from the system can be seen in Fig 6 and Fig 7. The red graph is represented CPU usage in percent (%) and the blue graph is represented RAM usage in Megabyte (MB).

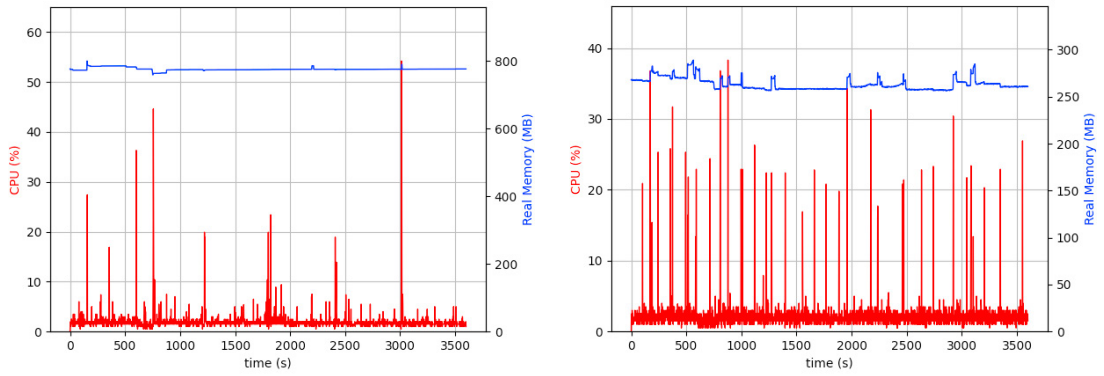


a) Zeek performance



b) Elasticsearch performance

Fig 6 Zeek and ELK performance.



a) Logstash performance b) Kibana performance

Fig 7 Logstash and Kibana performance.

Fig 6 on point A shows that Zeek as an IDS only used a little CPU and RAM. It is because Zeek only acts as a sniffing tool or network monitoring. Zeek only gathers log data from the network and divides it into several types of logs. For 1-hour Zeek max usage is 3.5 % CPU usage and 225 Mb of RAM usage. The highest CPU usage may be due to a big load of network traffic during that time, after that the graph is stable at around 2.5% - 0.5% CPU usage and RAM are stable at around 210 – 220 Mb of RAM usage. Zeek seems to have a solid red color in Fig 6 on point A, which means that Zeek always receives a non-stop packet from a DoS attack.

Elasticsearch is one of 3 products in ELK Stack, consisting of Elasticsearch, Logstash, and Kibana. Elasticsearch has a function as a search and analytics engine built on Apache Lucene or, in simple terms, the Elasticsearch function as a database that stores a log generated from Zeek and Machine Learning process that was ingested using Logstash and is displayed in Kibana Dashboard.

Fig 6 on point B shows that after running DoS attack for 1-hour, Elasticsearch max CPU usage is 78%, and RAM usage is 2300 Mb. There are so many spikes during this test because Elasticsearch always receives logs from the Zeek and Machine Learning processes. Elasticsearch always processes logs received from Zeek and Machine Learning processes to display in Kibana Dashboard. Elasticsearch consumes the most system CPU and RAM because Elasticsearch is the central log that stores all the log generated by a user in the network.

Logstash is a parsing tool that has a role as a parsing tool, from Zeek and Machine Learning process. For parsing to Logstash, Zeek already has modules that can be integrated with Logstash. However, for the machine learning process it needs a Grok Filter to parse the result of the machine learning process.

Fig 7 on point A shows that after Logstash ran for 1-hour to parse log that generated by Zeek and Machine Learning process, Logstash reached max 54% of CPU usage and 800 Mb of RAM usage. As mentioned previously, this system runs a machine learning process every 10 minutes, Logstash always experiencing spikes every 10 minutes because of machine learning processes that need to be parsed to Elasticsearch.

Kibana is a dashboard monitoring tool to visualize data stored in Elasticsearch. Kibana can visualize many types of tables or graphs, with so many features, such as using a filter that data should visualize, using a formula to display some data, and many more.

Fig 7 on point A shows that Kibana spikes when the user presses the refresh button in the Kibana Dashboard. It causes the system to consume more CPU and RAM because Kibana retrieves the data from Elasticsearch to be displayed. Kibana peak system usage is 47% CPU usage and 280 Mb RAM usage.

5. Conclusion and Future Work

IDS and SIEM undoubtedly are very important to install in every network to monitor the network's traffic to mitigate cyber-attack from occurring, especially by using machine learning to process the log monitored by IDS. Hence, it can classify benign or malicious traffic. The proposed system in this paper tries to mitigate the attack by

combining 3 components: IDS, Machine Learning, and SIEM built from an open-source project. Everyone can use this system to mitigate cyber-attacks. The performance testing shows Elasticsearch is the most component that uses CPU and RAM consumption (78% of CPU usage and 2300 Mb of RAM usage) and the least CPU and RAM consumption is Zeek (3.5% CPU usage and 225 Mb RAM usage). Please note that SIEM system (Elasticsearch) needs a high specification because of the process monitoring in real-time, so it needs a medium to high specification to prevent it from crashing. The proposed system works well to detect DoS attacks in real-time condition on the network.

Future work for this proposed system needs to try on the large scale of network with multiple IDS. Large networks and multiple IDS make the performance measurement more detailed than this research. The optimization configuration can also be implemented in the future work to reduce the usage of medium to high specification resources for virtual machines

References

[1] M. Cinque, D. Cotroneo, and A. Pecchia, "Challenges and Directions in Security Information and Event Management (SIEM)," in *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, 2018, pp. 95–99, doi: 10.1109/ISSREW.2018.00-24.

[2] A. Yulianto, P. Sukarno, and N. A. Suwastika, "Improving AdaBoost-based Intrusion Detection System (IDS) Performance on CIC IDS 2017 Dataset," *J. Phys. Conf. Ser.*, vol. 1192, p. 12018, Mar. 2019, doi: 10.1088/1742-6596/1192/1/012018.

[3] B. A. A. Al'Aziz, P. Sukarno, and A. A. Wardana, "Blacklisted IP distribution system to handle DDoS attacks on IPS Snort based on Blockchain," *Proceeding - 6th Inf. Technol. Int. Semin. ITIS 2020*, pp. 41–45, 2020, doi: 10.1109/ITIS50118.2020.9320996.

[4] H. Holm, "Signature Based Intrusion Detection for Zero-Day Attacks: (Not) A Closed Chapter?," in *2014 47th Hawaii International Conference on System Sciences*, 2014, pp. 4895–4904, doi: 10.1109/HICSS.2014.600.

[5] N. Hubballi and V. Suryanarayanan, "False alarm minimization techniques in signature-based intrusion detection systems: A survey," *Comput. Commun.*, vol. 49, pp. 1–17, 2014, doi: https://doi.org/10.1016/j.comcom.2014.04.012.

[6] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.*, vol. 28, no. 1, pp. 18–28, 2009, doi: https://doi.org/10.1016/j.cose.2008.08.003.

[7] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *J. Comput. Sci.*, vol. 25, pp. 152–160, 2018, doi: https://doi.org/10.1016/j.jocs.2017.03.006.

[8] C. M. Ahmed, M. R. Gauthama Raman, and A. P. Mathur, "Challenges in Machine Learning based approaches for Real-Time Anomaly Detection in Industrial Control Systems," *CPSS 2020 - Proc. 6th ACM Cyber-Physical Syst. Secur. Work. Co-located with AsiaCCS 2020*, pp. 23–29, 2020, doi: 10.1145/3384941.3409588.

[9] S. D. Cakmakci, H. Hutschenreuter, C. Maeder, and T. Kemmerich, "A Framework for Intelligent DDoS Attack Detection and Response using SIEM and Ontology," *2021 IEEE Int. Conf. Commun. Work. ICC Work. 2021 - Proc.*, pp. 7–12, 2021, doi: 10.1109/ICCWorkshops50388.2021.9473869.

[10] A. Azodi, D. Jaeger, F. Cheng, and C. Meinel, "A new approach to building a multi-tier direct access knowledgebase for IDS/SIEM systems," *Proc. - 2013 IEEE 11th Int. Conf. Dependable, Auton. Secur. Comput. DASC 2013*, pp. 118–123, 2013, doi: 10.1109/DASC.2013.48.

[11] T. Laue, C. Kleiner, K. O. Detken, and T. Klecker, "A SIEM Architecture for Multidimensional Anomaly Detection," *Proc. 11th IEEE Int. Conf. Intell. Data Acquis. Adv. Comput. Syst. Technol. Appl. IDAACS 2021*, vol. 1, pp. 136–142, 2021, doi: 10.1109/IDAACS53288.2021.9660903.

[12] E. T. Anumol, "Use of Machine Learning Algorithms with SIEM for Attack Prediction," in *Intelligent Computing, Communication and Devices*, 2015, pp. 231–235.

[13] M. Hristov, M. Nenova, G. Iliev, and D. Avresky, "Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT," *2021 IEEE 20th Int. Symp. Netw. Comput. Appl. NCA 2021*, pp. 9–13, 2021, doi: 10.1109/NCA53618.2021.9685977.

[14] N. Moukafih, G. Orhanou, and S. Elhajji, "Mobile agent-based SIEM for event collection and normalization externalization," *Inf. Comput. Secur.*, vol. 28, no. 1, pp. 15–34, 2020, doi: 10.1108/ICS-01-2019-0008.

[15] A. Majeed, R. ur Rasool, F. Ahmad, M. Alam, and N. Javaid, "Near-miss situation based visual analysis of SIEM rules for real time network security monitoring," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 4, pp. 1509–1526, 2019, doi: 10.1007/s12652-018-0936-7.

[16] K. O. Detken, T. Rix, C. Kleiner, B. Hellmann, and L. Renners, "SIEM approach for a higher level of IT security in enterprise networks," *Proc. 2015 IEEE 8th Int. Conf. Intell. Data Acquis. Adv. Comput. Syst. Technol. Appl. IDAACS 2015*, vol. 1, no. September, pp. 322–327, 2015, doi: 10.1109/IDAACS.2015.7340752.

[17] G. De Carvalho Bertoli *et al.*, "An End-to-End Framework for Machine Learning-Based Network Intrusion Detection System," *IEEE Access*, vol. 9, pp. 106790–106805, 2021, doi: 10.1109/ACCESS.2021.3101188.

[18] A. Waleed, A. F. Jamali, and A. Masood, "Which open-source IDS? Snort, Suricata or Zeek," *Comput. Networks*, vol. 213, no. March, p. 109116, 2022, doi: 10.1016/j.comnet.2022.109116.

[19] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," *Sensors*, vol. 21, no. 14, 2021, doi: 10.3390/s21144759.

[20] A. Tiwari, S. Saraswat, U. Dixit, and S. Pandey, "Refinements In Zeek Intrusion Detection System," in *2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2022, vol. 1, pp. 974–979, doi: 10.1109/ICACCS54159.2022.9785047.

[21] P. Venosa, S. Garcia, and F. J. Diaz, "A Better Infected Hosts Detection Combining Ensemble Learning and Threat Intelligence," in *Computer Science -- CACIC 2019*, 2020, pp. 354–365.

[22] S. J. Son and Y. Kwon, "Performance of ELK stack and commercial system in security log analysis," in *2017 IEEE 13th Malaysia International Conference on Communications (MICC)*, 2017, pp. 187–190, doi: 10.1109/MICC.2017.8311756.