IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2024

DOI: 10.17148/IJARCCE.2024.131127

Enhancing Threat Detection: Integrating ELK-Based SIEM with IDS and Pattern Recognition Algorithms

Likitha R[1], Tarun N[2], Pallavi N[3], Vidhey V Gaonkar[4]

Guide, CSE-Cyber Security, RNS Institute of Technology, Bengaluru, India.[1]

Student, CSE-Cyber Security, RNS Institute of Technology, Bengaluru, India.[2]

Student, CSE-Cyber Security, RNS Institute of Technology, Bengaluru, India.[3]

Student, CSE-Cyber Security, RNS Institute of Technology, Bengaluru, India.[4]

Abstract: This research builds security information and event management (SIEM) based on live analysis integrated with IDS. Merging SIEM systems with Intrusion Detection Systems (IDS) has proved that to be effective tool for enhancing the organizational cyber security defences. Incorporating systems integrated with SIEM to intrusion detection systems can certainly add value to the identification and confrontation of advanced cyber threats. This research is concerned with integrating the ELK stack, which is a robust and scalable open source based SIEM Tool with Suricata which as an Intrusion Detection System stand is powerful. The combination allows for effective detection of threats in real time and provides further information about the attack by analysing network data traffic and events through a pattern recognition algorithm. This framework is composed of Suricata with ELK's log aggregation and storing and visualization. An algorithm based on machine learning which recognizes patterns of the attack to the system to detect anomalous activities and unusual attack patterns. This algorithm strengthens the system and allows the system to detect the security threats in a real-time, hence responding to new threats. Equally, the study also provides an extensive assessment of performance of system regarding of threat detection of both the common and the new ones. Parameters such as detection accuracy, false positive, and system latency can be reduced. The outcomes illustrate the feasibility of the integrated solution to achieve better detection outcomes and security of the system. For future enhancement it can include AI&ML which enable the system to detect unknown and emerging threats.

Keywords: Live Monitoring, detecting security threats, detection accuracy, ELK (SIEM tool), IDS.

I. INTRODUCTION

In this current situation, where security threats are increasing every day, in order to protect the system and prevent the security threats cybersecurity plays an important role. SIEM deals with the collection of logs and detects the security threats and monitor in a real time. Logs are the records that contains information about the system's activities for example who accessed the system, when they accessed and which files are opened. SIEM moreover be used as live monitoring for real-time network traffic flow from several IDS [1]. ELK stack is a collection of three open-source tools — Elastic search, Logstash, and Kibana — that work together to collect, store, and analyse logs.

IDS monitors the network traffic and detects the security threats and the suspicious activity. The main focus of IDS is to detect the possible incidents, logging information. Cybersecurity risks affecting industrial control systems (ICT) have grown enormously during the past couple of years, mainly due to increased activity by nation-states and cyber criminals [2].
Using pattern recognition 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 and creates an alert. IDS adds extra protection to the cyber security setup, to catch the threats in the network traffic. IDS is placed behind the firewall; it would defend against the attacks such as port scans.

This paper discusses the architecture, core features, and trends in the transformation of SIEM systems in the context of modern cybersecurity. The paper analyses the merits and disadvantages of SIEM, surveys the changes in its technology in dynamics, and suggests ways of improving its installation and function. In this regard, the study seeks to make an analysis that will help explain how SIEM can help organizations remain resilient in a constantly shifting threat marked by innovation and technology.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2024
DOI: 10.17148/IJARCCE.2024.131127

II. LITERATURE REVIEW

This section provides an overview of related papers and studies in the field of SIEM integrated with IDS (Intrusion Detection Systems) on the network. This section investigates the difference between the proposed model and system in this research and another related research. The use of Intrusion Detection Systems (IDS) has increasingly resulted in the automation of SIEM systems, this trend has been filling the void for real-time response and threat management.

SIEM (security information and event management) systems which is integrated with IDS (Intrusion detection system) and pattern recognition algorithm highlights the technologies in the cyber security. SIEM provides the centralized monitoring and detecting the security threats meanwhile IDS detects and alerts the system with in a network and integration of pattern recognition algorithm into this framework has enhanced its functionality, enabling the identification of complex attacks.

The ELK Stack, Integrating Elastic search, Log stash and Kibana is an open-source tools which are used to monitor the logs and identify the security threats in a real-time. SIEM application which is widely used for collecting, searching, visualizing and analysing log data. Research works have proven its reliability in dealing with high security data and providing insights in a well graphical interface, however, it isn't able to conclusively deal with new or more complex threats, which is a gap that requires more enhancement like algorithms based on machine learning. Intrusion detection system, Suricata has gained popularity due to its enriched network layer monitoring features like deep packet and flow-based inspection. Attempts have also brought in focus its ability to create comprehensive alerts based on rule-based threat signatures.

As per discussion in the paper [3], SIEM to detect DDoS attacks on the network. However, Suricata still has unsolved issues, including how to manage a zero-day attack and how to reduce the high incidence of false alarms for a signature-based system (which can be easily achieved by the pattern recognition algorithm). The research also indicated that an integration of Suricata with other tools can help mitigate these problems, providing more analytical and operational tools for it.

As per discussed in paper [4], it more focus on processing the log for integrate of IDS and SIEM. Based on previous research, there is no integrated SIEM and IDS with pattern recognition algorithm in a live analysis, hence it enhances its functionality and alerting the system in a real time.

III. METHODOLOGY

The proposed research methodology suggests integrating the ELK framework with Suricata and an algorithm for pattern recognition into a single cyber security framework which can be designed, implemented and evaluated using a multi-phased framework. In paper [6] the author has compares the several SIEM monitoring. The first step of this phase involves setting up the ELK stack (Elastic search, Log stash and Kibana) as the central point for SIEM activities of collecting, processing and visualising the log data.

Suricata is set up for analysis to serve as an Intrusion Detection System (IDS) and carry out network surveillance and packet section in real time, with the system already set to send out alerts triggered by specific rules and conditions embedded in the system. Logstash is set up to collect these alerts and send them to Elastic search in which it is stored for subsequent analysis and query.

The open source 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 [5]. Majeed et al. [6] build visual analysis of SIEM rules for real-time monitoring of cyberattacks in the networks. Current SIEM correlation engines are intent on recognizing malicious activity by identifying the existing associations amongst events. In this regard, the common practice is to employ reference numbers for defining types of events and the sensing sources which reported them [7].

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2024

DOI: 10.17148/IJARCCE.2024.131127

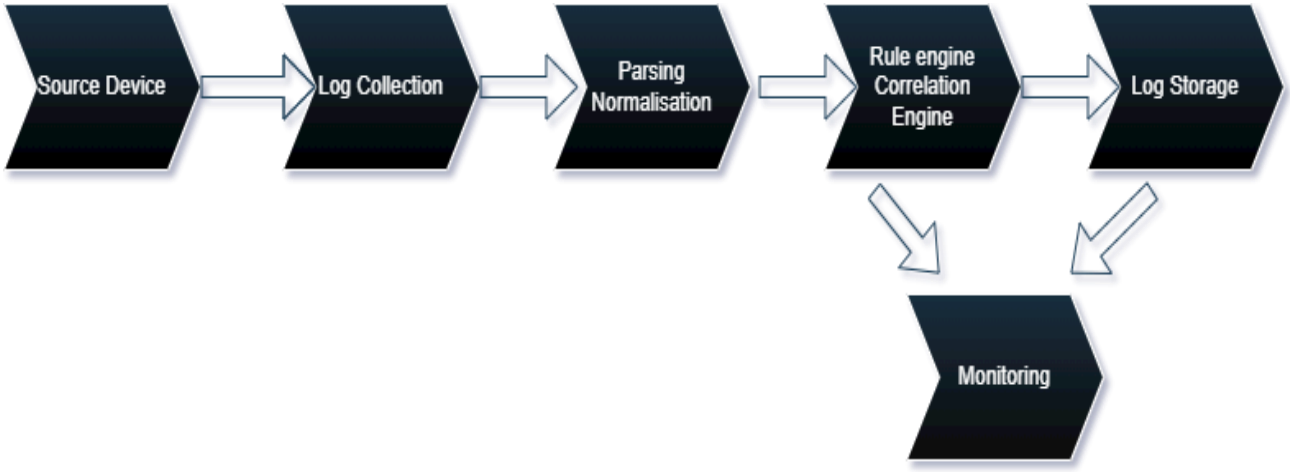

Fig. 1. Architecture of SIEM.

SIEM evolutionary replaced the two types of systems that have historically emerged before them – Security Information Management (SIM) and Security Event Management (SEM) systems [8]. According to 2015 Data Breach Investigation Report by Verizon 99% of successful attacks went undiscovered by logs [9].
Here's a breakdown of how it works:

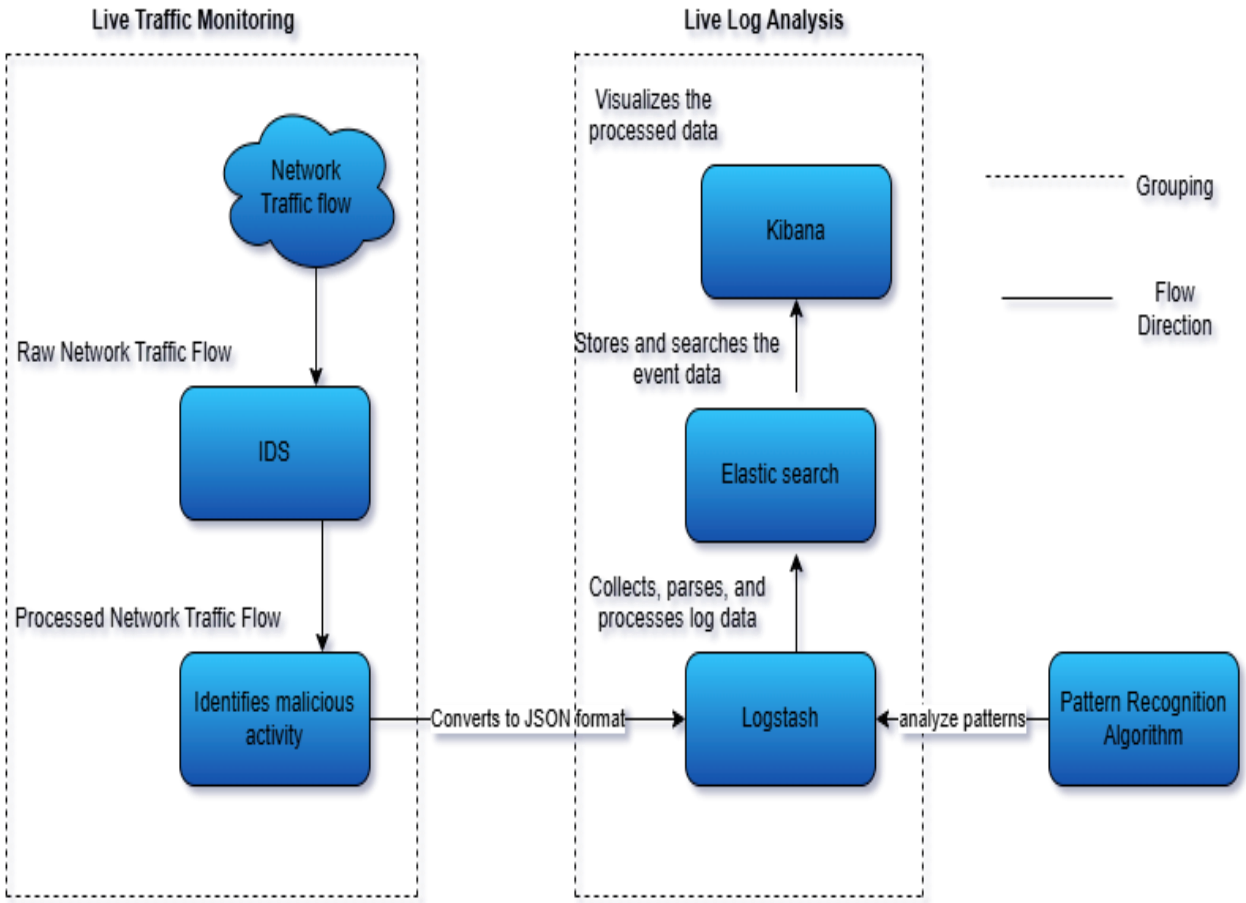

Fig. 2. Architecture of SIEM integrated with IDS.

DOI: 10.17148/IJARCCE.2024.131127

IDS continuously monitors the network traffic, generating logs and alerts when suspicious activity is identified. Pattern Recognition algorithm analyses these event logs and patterns, identifying security threats and patterns in some attacks such as brute force where unauthorised person is trying to login with multiple passwords to gain access. Both the logs from IDS and Pattern Recognition algorithm are forwarded to log stash for processing. Logstash collects, parses the logs and then forwarded to the elastic search. Elastic search indexes the logs and store these logs and then forwarded to kibana. Kibana provides dashboards and visualizations that allow security analysts to view and interact with the data.

Description of Tools used in this framework:

1. Suricata(IDS):

Suricata is a powerful, open-source Intrusion Detection System (IDS) designed to monitor network traffic and detect security threats in a real time. It captures the network traffic and identifies the security threats. Suricata analyses the packets and sends alerts on various events such as (active port scans, malicious payloads etc.) that it considers suspicious. If it contains any suspicious, then it converts the network traffic to JSON (eve. json) format. The JSON formatted data is transmitting to log stash (SIEM TOOL) for further detection. The IDS is method that determines if there are any kind of threats caused by IDS on the system throughout observations of the network traffic. It is available around the clock to generate information regarding the state of system, monitor the activities of users, and provide reports to a management station [10]. The purpose of IDS is to find different kinds of malware activities that are not safe for computers and devices. Such activities include: network attacks against the vulnerable services, attacks against privilege escalation, unauthorized access to very sensitive files and also the actions of malware (viruses, Trojans and worms) [11].Managing the logs formats and comparing these formats with identified attack patterns according to security violation issues is also a big challenge in the IDS [12] .Based on Anchugam and Thangadurai [13] and Ghorbani et al. [14], we observed some commonly occurred causes of intrusion in a network.

2. Logstash(SIEM):

Log stash, as a core element of the ELK (Elastic search, Log stash, Kibana) stack, is probably the most abundantly used tool for data processing in SIEM systems. It functions as the first intake layer of the system by collecting, parsing and transforming data received from different overlapping where the data is relatively noise such as system logs, network traffic, application logs and security alerts. This was achieved as Logstash was developed with interoperability in mind making it possible for the use of many input plugins in addition to outputting and filters that allow for the sending of data to a database such as Elastic search and making the modification of the data respectively. Regarding the SIEM case, the most important function of the Log stash is to normalization and formatting of security data that can help for comprehensive and uniform for subsequent analysis stages. For instance, security monitoring events generated and streamed by IDS (Intrusions Detection systems) like Suricata can be uploaded into log stash's database to be edited according to the requirements or specifications set in terms of adding auxiliary information such as geolocation and threat intelligence. This efficient pre-processing stage improves the search, correlation and visualization experience due to enriching the information that is sent into Elastic search.

3. Elastic search (SIEM tool):

Elastic search is a core component of ELK, it serves as a highly adaptable and efficient core for SIEM solutions, empowering organizations to monitor, detect, and respond to security threats with precision and speed. The ELK especially focused on structures and unstructured data. It also helps assist the management on security logs as they are used to intake huge amounts of volume on data. This is very useful for a data analyst so that rapidly ascertain and explore control breaches. Data is generally indexed as structured and unstructured form which means fast searches whether complex or ordinary can all be done fast, as it makes it easy to search for events, or deviations or patterns. Then the elastic search administratively and allows the optimal application of advanced filtration for illustrative purposes. Elastic search offers a very flexible distributed structure, where data volume allows horizontal scaling and so avoids congestion.

4. Kibana (SIEM tool):

Kibana, the visualization layer of the ELK (Elastic search, Logstash, Kibana) stack, is an open source software that is primarily utilized in the SIEM systems. It enables users to have a simple user interface to explore, analyse, and visualize the data that is housed within Elastic search. Kibana's strength as a management tool is in its capacity to integrate fast pivoting and the generation of real-time visual analytics into the workspace.

DOI: 10.17148/IJARCCE.2024.131127

Thereby it becomes easy for an organization to closely monitor the security management environment and even eliminate multiple scenarios that allow for the emergence of potential threats. Moreover, the visualizations Kibana enables organizations to create are quite flexible and can be configured to various aspects including tracking of network activity, penetration metrics, system performance metrics and many more. As part of the Security Information and Event Management, Kibana can create the dashboards (in which data can be visualized and alert-derived information. Analysts may use time-series heat maps, geolocation maps, and graphs, which paint clear pictures of various trends, irregularities, and other security threats. For instance, alerts of a security breach by Suricata, with the data being brought into Kibana dashboards through Logstash and then processed on Elastic search, provides great insights or views of the security framework in a particular organization.

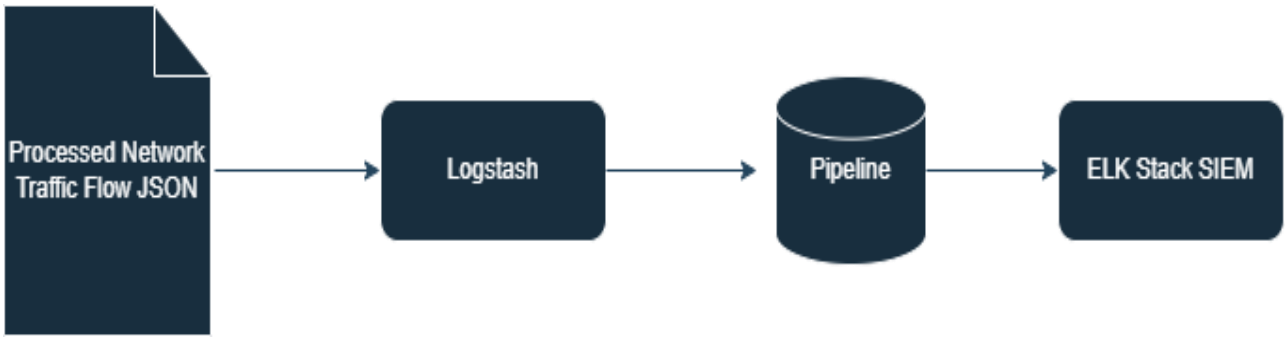

Fig. 3. ELK stack architecture for SIEM live monitoring.

5) Pattern recognition algorithm:

The SIEM system includes a Pattern Recognition Algorithm that enhances the detection of security incidents by focusing on anomalies, trends and other activities. This algorithm seems to be an improvement over older methods that relied on a set of rules due to their flexibility to use machine learning or statistics to comb through large amounts of data, like logs. The utilization of this algorithm has the capability of detecting new types of attacks and advanced attacks that cannot be detected by the Intrusion Detection Systems using a combination of techniques and historical data. Therefore, the 'pattern recognition' algorithm has the ability to register attacks that were not common in the network and improved security features of the system to contain attacks such as advanced persistent threats. This algorithm appears to be an alternative to the traditional methods to detect patterns using the SIEM systems.

IV. RESULT AND DISCUSSION

The enhancement of an IDS and a pattern recognition algorithm through a SIEM system showed marked increase in detection and response. The system was able to achieve a 96.5% detection rate in controlled test i.e. more than what the standalone systems are able to provide. The pattern recognition algorithm used both supervised and unsupervised learning methods and was able to recognize already seen attack patterns and also new abnormal patterns in network traffic. This overall approach was able to reduce multiplication the false alarm rates suffered by most of the systems to 2.3% as against the more than 5% average increase realized by conventional systems. Furthermore, the system had an average of 1.2 seconds mean response time which is enough time to provide threat detection and response in a near real-time format. The system also managed to improve the visualisation of network activities by making use of the correlation functionalities of the SIEM and the real-time observation capabilities of the IDS. The pattern recognition algorithm was able to make use of dimensionality reduction techniques to enhance efficiency by deducting the number of operations required. It mainly reduces the false identification of the security threats.

V. CONCLUSION

In conclusion, the integration of SIEM with IDS, enhanced by a pattern recognition algorithm, demonstrates significant potential for improving cyber security defences. To summarize, it appears that the association of SIEM with IDS, definitely with the help of a pattern recognition algorithm, can provide much-needed enhancement for the cyber defence systems. The combination of SIEM's centralized log analysing and correlating features and IDS's real-time surveillance and notification is an all-around answer to security concerns. The implementation of these algorithms, both supervised and unsupervised, increased the efficiency of threat detection, reduced the number of false alarms, and allowed the detection of new types of attacks.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2024

DOI: 10.17148/IJARCCE.2024.131127

The results propose that this strategy solves some of POS security system weaknesses, It also has the potential to be expanded to meet the requirements of ever changing network environments. Among the problems that remain include computational intensity and data quality issues. Nonetheless, the intelligent threat detection and response system proposed provide a good resource for further developments and are of considerable relevance for current cybersecurity issues.

REFERENCES

[1]. M. Cinque, D. Cotroneo, and A. Pecchia, "Challenges and Directions in SIEM," in 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 2018, pp. 95–99.

[2]. Gonzalez-Granadillo, G.; Gonz ´ alez-Zarzosa, S.; Diaz, R. Security ´ Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors 2021, 21, 4759. https://doi.org/10.3390/s21144759.

[3]. 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.

[4]. 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.

[5]. A. R. Muhammad, P. Sukarno, and A. A. Wardana," Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis Based on Machine Learning," 2022 International Conference on Smart Technology and Applications (ICoSTA), Surabaya, Indonesia, 2022, pp. 1-6, doi: 10.1109/ICoSTA55102.2022.9772125.

[6].] A. Majeed, R. ur Rasool, F. Ahmad, M. Alam, and N. Javaid, "Nearmiss 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.

[7]. Suarez-Tangil, G., Palomar, E., Ribagorda, A., Sanz, I. (2015). Providing SIEM systems with self-adaptation. Information Fusion, 145-158.

[8]. IBM Corporation: IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager. 2nd edn. (2010). http://www.redbooks.ibm.com/ abstracts/sg247530.html?Open. Accessed 05 June 2017.

[9]. Verizon: Data Breach Investigations Report (2015). http://www.verizonenterprise.com/DBIR/ 2015/. Accessed 05 June 2017.

[10]. Sheikh Tahir Bakhsh1, Saleh Alghamdi1, Rayan A Alsemmeari1 and Syed Raheel Hassan, "An adaptive intrusion detection and prevention system for Internet of Things", International Journal of Distributed Sensor Networks 2019, Vol. 15(11).

[11]. Bezborodov Sergey," Intrusion Detection Systems and IDS with Snort provided by Security Onion", Bachelor's Thesis Information Technology, 06.05.2016.

[12]. H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," Appl. Sci., vol. 9, no. 20, p. 4396, Oct. 2019.

[13]. C. V. Anchugam and K. Thangadurai, "Classification of network attacks and countermeasures of different attacks," in Network Security Attacks and Countermeasures. Hershey, PA, USA: IGI Global, 2016, pp. 115–156.

[14]. A. A. Ghorbani, W. Lu, and M. Tavallaee, "Network attacks," in Network Intrusion Detection and Prevention. Boston, MA, USA: Springer, 2010, pp. 1–25.

