American Journal of Technology Advancement Vol. 3, No.6 (Jun, 2026),
E-ISSN: 2997-9382
American Journal of Technology Advancement
https://semantjournals.org/index.php/AJTA

| Research Article

Check for updates

Analyze How AI Improves Incident Response Time, Alert Prioritization, and Analyst Productivity in SOC Environments

Samira Alam Chowdhury
Master of Science in Business Analytics, Trine University, USA
Email: samiraeena0000@gmail.com

Mahbub Hasan
Master of science in information studies, Trine University, USA
Email: mahbub0016@gmail.com

Mohd Jahidul Hoque
Master of Science in Business Analytics, Grand Canyon University, USA
Email: MHoque2@my.gcu.edu

Abstract
This research paper investigates ways in which Artificial Intelligence would be able to positively affect the speed of incident response, alert prioritization, and analyst productivity at Security Operations Centers by analyzing the information extracted from network traffic data. This research paper uses the quantitative experiment approach, using a public dataset with normal network traffic as well as various cyberattack classes. The study looks into aspects such as class distribution, feature behavior, and risk-based alert prioritization for insights into how Artificial Intelligence could contribute to security operations. The class distribution analysis proves that the dataset is highly unbalanced, as Recon and Scanning classes appear quite often, while other attacks are represented considerably less often. The results for feature behavior demonstrate that packet-based patterns may assist with the differentiation between normal traffic and potentially malicious one. The results of the alert prioritization prove that the highest priority alerts should focus on Recon and Scanning.

Keywords: Artificial Intelligence, Incident Response, Alert Prioritization, Analyst, Productivity, Security Operation Centers, Recon, Scanning, Classes, Dataset, Cyberattack

This is an open-access article under the CC-BY 4.0 license

1. Introduction

A. Background of Topic

Growing incidents of cyber-attack incidents on business information and the network system created an urgent situation for the enterprises to build a department responsible for handling cyber related issues. Industry builds up a departmental unit and is interpreted as Security Operation Center (SOC) due to its nature of services. SOC can be defined as a functionality or a team responsible for improving the cybersecurity posture of an organization by preventing the threats, monitoring the functionalities on the network and giving response to any threats [1]. After the innovation of

Artificial Intelligence, the task of SOC became more critical as the mechanism of cyber-attack of modern time is highly critical. Industry has evolved an efficient technique in the form of incident response and alert prioritization to prevent the negative impact of cyber-attack. Incident response refers to the procedure or technical process of an industry to respond against the cyber threats and security breach by detecting it beforehand [2]. Likewise, alert prioritization is another important process that enterprises have adopted for categorizing and prioritizing the security alerts based-on their intensity of negative impact [3]. SOC uses all these advanced technologies to make the business environment free from the threat of cyber-attack. Inclusion of Artificial Intelligence (AI) as a potential cybersecurity tool allowed the security analyst to assess the patterns of network traffic for identifying the suspicious elements. Integration of AI with the process of incident response and alert prioritizations made the system rapid and more accurate.

B. Problem Statement

The problem of cyber threat no longer restricts its periphery of negative influence till Information technology but it also brings a high expenditure and reputational damage to the organization in a market [4]. The Security Operation Center played a critical role in identifying the cyber threat and preventing it by implementing various effective methods. However, the advancement of technological mechanisms and concepts are not limited to industry but also emphasized the cyber criminals to optimize their method to make intrusion effectively. In other words, the landscape of cyber threats is extended to an extent, making the conventional techniques of SOC ineffective. The current scenario conveys the several security alerts that SOC gets from multiple monitoring tools on a regular basis. Security analysts handling the alerts with traditional methods get overwhelmed with the numerous alerts and it leads the personnel to alert fatigue [5].

Alert fatigue is not a mere inconvenience for security analysts but the overwhelmed analyst approach directly impacts the accuracy of detection, incident response time and sustainability of the team [5]. In addition, the delayed response of an analyst due to excessive alerts introduces a compliance risk in the business environment.

C. Aim of the Research

The aim of the research is to conduct a critical analysis of the SOC environment in the organizational context so that an effective resolution can be obtained for security analysts to handle the alert response in an efficient manner.

D. Objectives of the Study

The objective of the study is mentioned below:

a. To conduct an assessment to determine the method of reducing the response time with the help of AI technology.
b. To inspect the process of AI-based alert prioritizations.
c. To find out a method that can improve the productivity of a security analyst task.
d. To conduct an exploratory data on the selected dataset through various. visualization and analyze the subject critically.

E. Research Questions

The research questions for this study are depicted below:

1. How an integration of AI technology reduces the issues of incident response time in SOCs?
2. What are the ways in which AI improves the alert prioritization?
3. Does the inclusion of AI technology in the SOCs environment enhance the productivity of Security analysts?

4. What outcomes can be discovered from the chosen network traffic dataset that supports AI implementations in SOCs environment?

F. Significance of the Study

The importance of this study can be understood from the fact that it helps the SOC teams working across the different organizations to deal with numerous cyber threat alerts by integrating AI, and increases the response time. It gives an insight to the industry into the real-time solution that can be applied in a very simple way. The theories and findings of this research improve the SOCs environment in such a manner that also enhances the productivity of security analyst tasks. In other words, an analyst comes out from the alert fatigue and problem of burn out from the influence of the results applied in the business environment. Subsequently, the probability of cyber-attack failure increases with the accomplishment of this research work.

2. Literature Review

A. AI Applications in Security Operations Centers

Application of Artificial Intelligence has become an essential field or subject for researchers that reflects in the existing literature for preventing cyber threats. Islam [6] shed light on the current scenario of SOCs environment that reflects the approach of security analysts to deal with cyber threats by using the software tools and processes. Khayat et al. [7] mentioned the problem of SOCs team on relying upon a single tool or traditional mechanism, which increased its struggle to practically identify the suspicious element of cyber-attack. The research paper of Islam collected the facts entirely from the secondary resources by referring to the related work. Likewise, the research work Khayat and his peers proposed the reference architectural model by reviewing the literature only.

Both studies emphasize the increasing role of AI in Security Operations Centers, but the scope and depth of the analysis differ. Islam [6] mainly focused on explaining how AI and machine learning can support security analysts to identify malicious activities and improve efficiency of SOC operations. The study provided a high-level overview of AI enabled capabilities such as threat detection, anomaly detection, and automated response mechanisms. One of the strengths of this work is that it shows the practical use of AI in modern cybersecurity environments. The study however, was entirely based on previously published sources and did not contain any empirical validation or real-world case analysis. The results are therefore mainly theoretical and do not demonstrate how AI solutions behave in real operational SOC environments. Moreover, the research did not provide much discussion on the challenges of AI adoption such as data quality issues, model bias, and need for skilled personnel. These limitations restrict the ability of the study to provide a full understanding of the potential practical barriers organizations may face in the process of implementing AI based security solutions.

In contrast, Khayat et al. [7] conducted a systematic literature review that explored more in depth the applications of AI and machine learning in Security Operations Centers. The study drew on evidence from a large number of scholarly sources, and suggested an architectural view of how AI can be integrated into SOC processes. The approach increased the credibility of the findings, as it enabled the authors to identify recurring trends, benefits and gaps in research within the existing body of knowledge. The review highlighted the potential of AI to improve threat intelligence, automate mundane tasks and enable security analysts to make faster decisions. However, this study has a limitation as Islam [6] because it is also based on the secondary data and does not have an experimental validation. Moreover, the review emphasized more on the benefits of artificial

intelligence while giving comparatively less weight to the difficulties involved in implementation. As such, while both papers recognize the importance of AI for changing SOC processes, there is a need for empirical studies on how effective artificial intelligence-based systems have been in practice.

B. Techniques for Alert Prioritization

In recent years, alert prioritization has become a crucial field for research within Security Operation Centers as the security analysts often receive many alerts beyond their capabilities of investigating them all. Bassey et al. [8] analyzed several approaches to alert prioritization in security monitoring environments, focusing especially on severity averaging and alert entities. According to the researchers, companies receive a substantial number of security alerts daily, but not all alerts might actually be considered threats. In such a way, the phenomenon of alert fatigue occurs, thus increasing the likelihood of missing important incidents. It is vital to prioritize the alerts according to their significance. The research helped in providing insights on how prioritization techniques would enhance security monitoring processes. Unfortunately, the research emphasized theoretical aspects rather than giving evidence that these techniques were effective in practical settings.

The authors in Liu et al. [9] developed RAPID; a framework that enables real-time alert investigation to facilitate effective threat identification using contextual priority. In this work, the authors identified an existing problem in which traditional alert priority assessment tends to focus on individual alerts and do not put the situation into consideration when prioritizing. This study thus aimed at developing a tool that takes into account the context of the alert during the analysis phase. One of the advantages in this study is the practical approach that has been employed since the model has been tested using actual security data. It was shown that context-based prioritization will help to lower the time required for investigation as well as increase the accuracy of detecting potential threats. Although the study has provided many advantages, it may need considerable computing power and accurate contextual information.

In the same way, Albasheer et al. [10] conducted a survey on alert correlation in network intrusion detection systems and examined how alert correlation can be used for predicting cyber-attacks. It is important to highlight the fact that alert correlation acts as a supporting tool for alert prioritization since it helps to group relevant alerts and eliminate redundancy. A number of methodologies that enable security teams to identify patterns in attack processes were suggested. Intelligent methods used in intrusion detection systems to improve intrusion prediction accuracy were also covered by the authors. One of the strong points of the study is the thorough analysis of alert correlation methodologies. Nevertheless, it turned out that many existing methodologies fail to overcome the issue of false positives and problems with scalability. Altogether, these articles prove that alert correlation methods have a great potential in improving threat detection mechanisms, which, in turn, can lead to more efficient decision-making within Security Operation Centers despite the need for additional research on implementation issues.

C. Impact of AI on Incident Response Time

As cyber threats have grown more complex, there is an increasing need for a quick and efficient incident response process. In their research work, Maddireddy and Maddireddy [11] looked into the importance of AI-driven automation in the incident response process for enhanced network security. It was highlighted that conventional incident response strategies require much manual effort on the part of human beings which slows down the detection of threats. The use of AI can enable automation of repetitive processes like threat detection and response execution.

The use of automation ensures that there is an effective reduction in time taken in response to security threats and a reduction in damage resulting from attacks. The study further emphasized the capacity of artificial intelligence systems to process huge volumes of data quickly and thus enhance decision-making process. Despite having revealed many advantages of using automation, the study was basically theoretical in nature and could provide very little information on how well AI based response systems perform in the long run.

In the same vein, Yousaf & Boomsma [12] studied the implementation of AI in SOCs with special emphasis on improving threat analysis and minimizing incident response time. It was found that AI could be useful for SOCs in increasing their productivity since it helps analyze incidents and detect threats quickly. According to the researchers, traditional methods have limitations when it comes to handling the increased number of incidents generated daily. However, through artificial intelligence methods, incidents can easily be investigated. It is also evident from the study that AI supports the efforts of security analysts by minimizing the burden of performing routine surveillance activities. Another significant aspect of the research that is worth mentioning is the connection between the use of AI systems and efficiency of their operations. The limitation of the study, on the other hand, lies in the insufficient analysis of problems related to the implementation of AI in SOCs.

Chirra [13] studied the creation of an automated AI-based incident response system aimed at accelerating the response and enhancing its quality during cyber-attack detection and handling processes. The author provided an overview of a suggested framework based on the implementation of both artificial intelligence technology and automated response processes for handling attacks. As per Chirra, the use of AI contributes towards improving the reaction speed due to faster threat detection and prompt responses. Besides, it was noted that AI solutions can further learn from past experiences and provide more efficient future responses to different cyber-attacks. However, this research did highlight some of the problems that an automated system may encounter, namely those regarding accuracy, transparency, and credibility. These papers altogether suggest that AI has had an immensely positive influence on the time taken for an incident response as a result of the automation of security measures and decision-making process. Nevertheless, more empirical work needs to be done in order to test this hypothesis.

D. AI and Analyst Productivity

E. Literature Gap

3. Methodology

A. Research Design

This paper uses a quantitative experimental method to examine the potential to boost the performance of Security Operations Center (SOC) with the help of Artificial Intelligence (AI). The research doesn't build new machine learning models; instead, it leverages an existing real-world network traffic dataset to gain insight and understand patterns. The emphasis is on exploration, visualization and pattern recognition. This approach enables us to emulate a real SOC environment and gain insights into how AI can contribute to quicker incident response, more effective prioritization of alerts and increased analyst productivity. The study uses real network flow data, including both attack and normal flows, which allows for more practical and applicable results that can be applied in a SOC's day-to-day operations. The experimental design is that of simplicity, clarity and relevance to reality, not theoretical modeling.

B. Data Source and Description

This study was based on data retrieved from Figshare repository. It is called Normal+Attacks11.csv and has network flow data including normal traffic and various attacks. Relevant attributes like flow duration, packet rates, packet lengths and inter-arrival times are part of the data. The target variable is the "label" column which shows whether the flow is Normal or an Attack (DDoS, DoS, etc.). This dataset can be used for SOC research as it is a realistic network behaviour.

C. Data Preprocessing

Data from raw data set checked for missing data set and inconsistencies. Simple cleaning procedures were carried out to prepare the data for analysis. Features were analyzed to look at their distribution and correlation with the label column. No major changes were needed as the dataset was already well-structured.

D. Software Tools Used

For this research, Tableau and Orange were selected as the main tools. Interactive visualizations and dashboards were built using Tableau to demonstrate alert patterns, class distribution, and relationships between features. Orange was used for data exploration, simple machine learning experiments and to generate some insights into the alert prioritization. Gephi was not used, because the data is tabular, and is not appropriate for network graph visualization.

E. Analysis Approach

The analysis concentrated on identifying the patterns that lie within the network traffic which are significant for SOC operations. Different patterns of attack traffic were represented in various visualizations to compare against normal traffic. Important metrics such as flow duration, packet size statistics, and inter-arrival times were carefully studied. These patterns were used to simulate an AI system that automatically prioritises high risk alerts and lowers the number of alerts that analysts would need to review manually. The aim of the overarching project was to show how AI can enable security teams to identify threats quicker, react faster, and enhance analysts' efficiency. This is a very good way to demonstrate the benefits of AI in the real world in SOCs.

F. Ethical Considerations

The data set is publicly available on Figshare repository and was ethically acquired for academic research only. Does not provide any personal, private or sensitive information about a person. All records are anonymous and contain no information about the users. The responsible application of Artificial Intelligence (AI) for security operations is strongly encouraged by this research. The study highlights the importance of using AI as a tool to assist human analysts, not replace them. All findings and recommendations are intended to enhance cyber security practices and be transparent, equitable and accountable. The research respects ethical standards in that it uses open data, doesn't engage in bias amplification and is geared towards the practical benefits of SOC teams. The final goal is to foster safe surroundings with the aid of moral and accountable AI use.

4. Conceptual Framework

The notion of Artificial Intelligence (AI) application in the enhancement of Security Operations Centers (SOCs) is used in the conceptual framework of this study. The framework aims at showing the capabilities of AI applications in terms of reducing response times, alert prioritization, and increasing the efficiency of the analysts in analyzing network traffic flows.

The key element of the proposed structure is an analysis model based on artificial intelligence technology using network flow data. This stage emphasizes the detection of attacks, evaluation of

risks, and quick decision making. The predictive efficiency of the presented framework can be evaluated by measuring patterns discovery, classes separation, and alert reduction. Nevertheless, the predictive capabilities themselves cannot be considered enough for effective operation in SOC.

First is the AI Predictive Layer, which evaluates certain flow characteristics such as flow duration, packet rate, and inter-arrival time in order to identify both benign and malicious flows. Next comes the Alert Prioritization Layer, where the system assigns risk scores for alerts depending on their level of seriousness. Finally, is the Decision Support and Productivity Layer, whose main function is to lessen the burden of the analyst, speed up response, and boost SOC effectiveness.

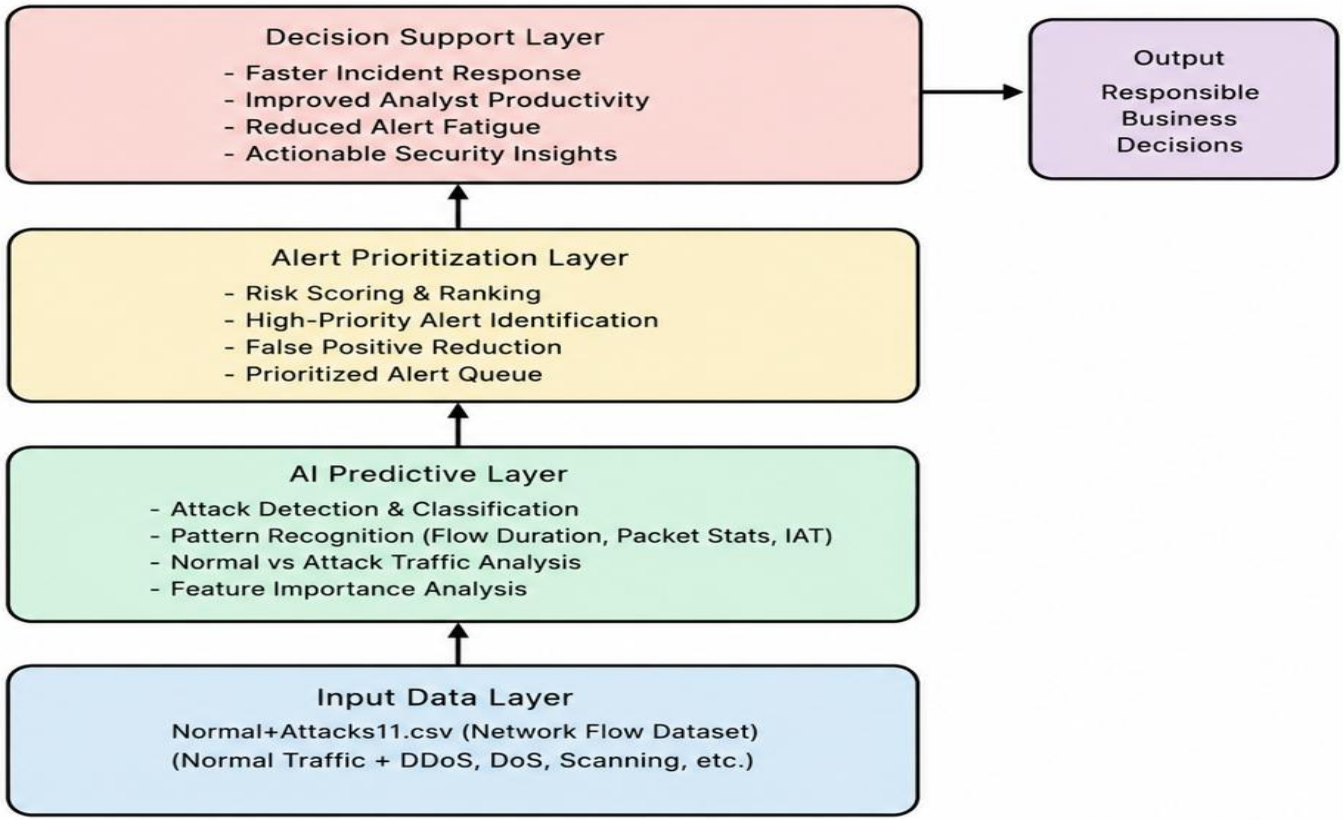


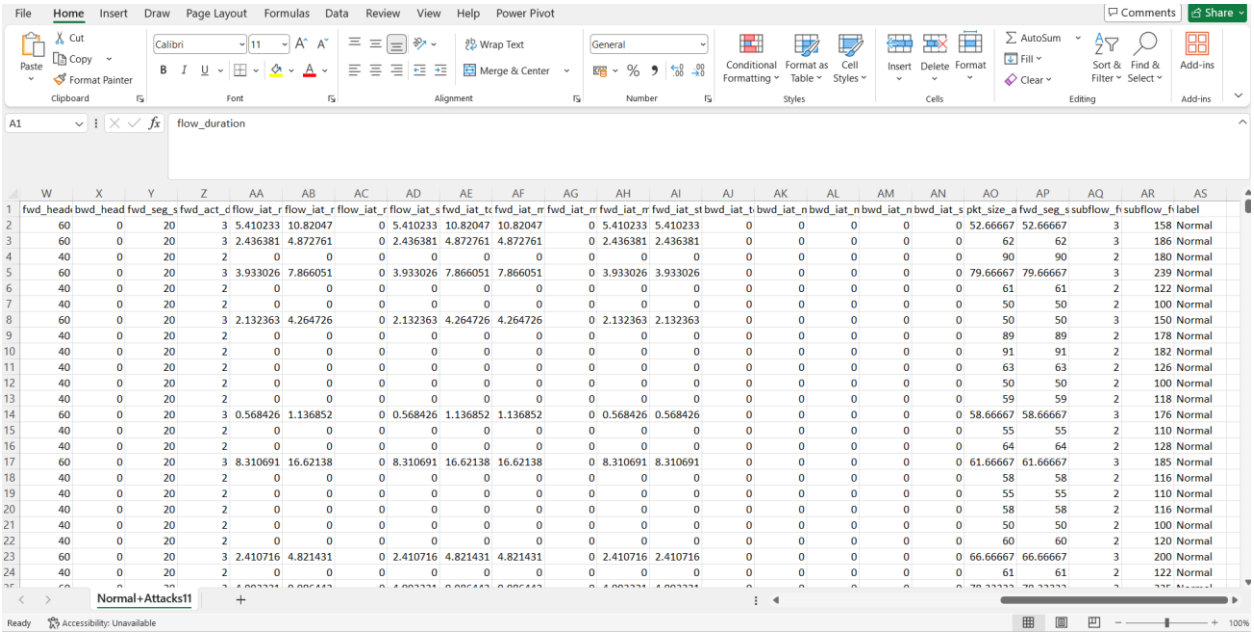
Figure 1. Conceptual Framework for SOC Operations
(Source: Created by learner)

This figure depicts a stratified and controlled implementation process of utilizing Artificial Intelligence within SOC operations. The starting point of the implementation is the Input Data layer, which contains flow logs from the dataset named “Normal+Attacks11.csv”. This data acts as the primary source for analysis purposes. The next layer that follows is the AI Predictive Layer, which is used for detecting and classifying normal and attack flows based on their features. Above this, there is the Alert Prioritization layer, where alert prioritization increases efficiency and makes the process more transparent. Finally, the top layer is called the Decision Support Layer, where results are presented in terms of practical benefits like faster response to incidents, alert fatigue reduction, and increased productivity of the analysts.

5. Dataset Overview

The dataset used in the current study is called "Normal+Attacks11.csv" [14]. It comes from the Figshare repository and has been downloaded by the authors of the paper. In total, there are 149,434 network flow records that contain 45 feature columns that characterize real-world network

traffic behavior [14]. These records contain examples of normal network traffic behavior and different kinds of cyber-attacks like DDoS, DoS, Scanning, Bruteforce, and Reconnaissance [15]. Some of the most interesting features of this dataset include flow duration, bytes per second, packets per second, forward/backward packet statistics, packet length, and IAT features. The label column represents the target variable, which includes only two labels: "Normal" or one of the attack types mentioned above. This dataset can be considered very useful for conducting SOC research since its data can be easily used as an example of network traffic security professionals analyzing on a daily basis.



(*Source Link: https://figshare.com/articles/dataset/UAV-GCS_Intrusion_Detection_Dataset_UAV-GCS-IDS_/29608541?file=56418635*)

6. Results

A. Class Distribution Analysis



Figure 2. Visualization of Various Cyber Attacks Classified
(Source: Created by learner)

It is evident from Figure 2 that there is an extreme skewness in terms of class distribution in the cyberattack data set. Recon and Scanning are the classes with the highest number of occurrences, having 50,155 entries each. However, DoS, DDoS, and Normal have moderately high numbers of occurrences. Conversely, BruteForce, MITM, Reply, Fake Landing, and particularly Evil have significantly lower numbers of occurrences.

B. Feature Behavior Analysis

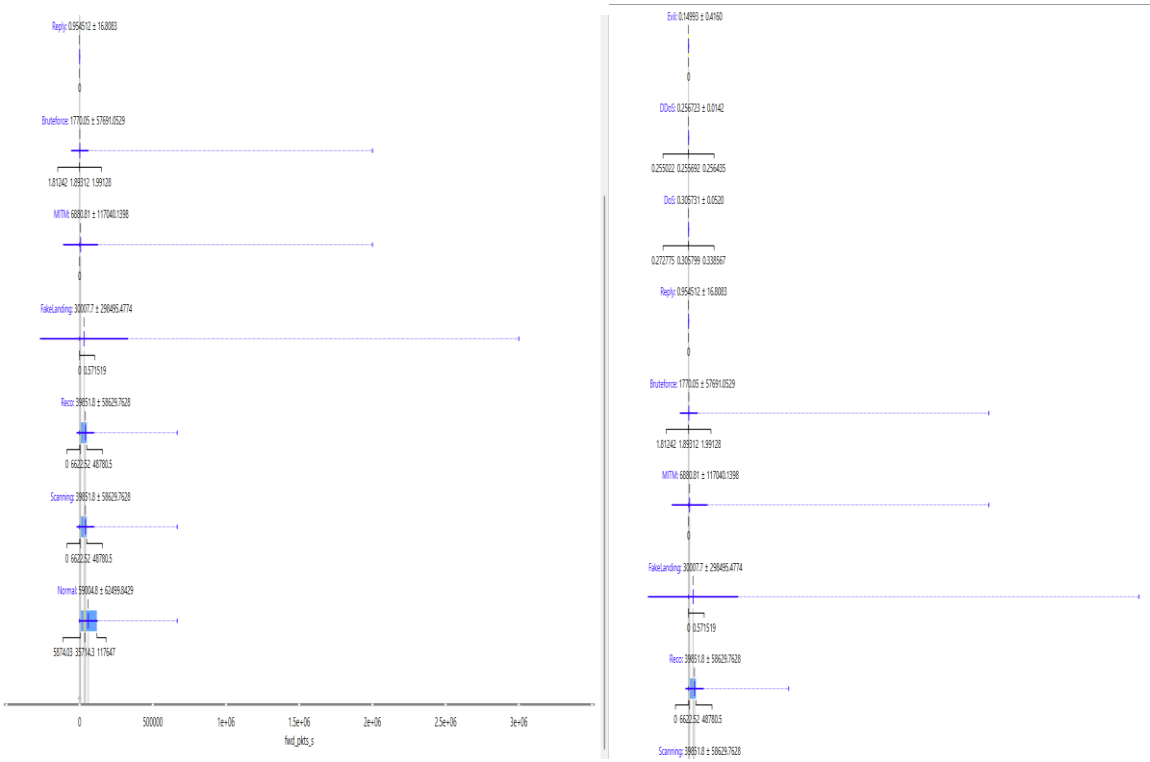


Figure 3. Network Traffic Feature Behavior Analysis
(Source: Created by learner)

From the box plot analysis of the feature fwd_pkts_s, it is clear that there is a lot of difference between the normal traffic and the attack types when it comes to the transmission rate of packets. The normal traffic category shows higher packet transmission rates as compared to some of the attack categories, but the Fake Landing, MITM, and Bruteforce attacks have high mean values and ranges, meaning that there is abnormal packet transmission. The Fake Landing attack type shows high variability, indicating inconsistency in the packet transmission process.

C. Alert Prioritization Simulation

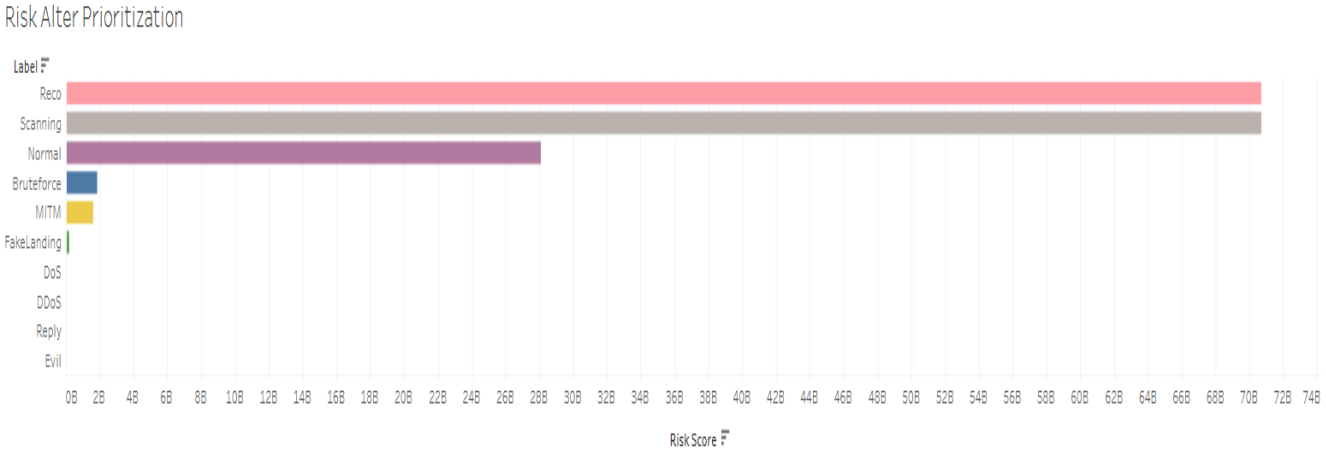


Figure 4. Risk Alert Prioritization Visualization
(Source: Created by learner)

The risk-based alert priority approach is illustrated by Figure 4. From the figure, it can be observed that Recon scores higher than Scanning. These two operations are supposed to attract the quickest analysis due to the high-risk exposure levels associated with them. Normal traffic scores

considerably lower, but the activities of BruteForce, MITM, and FakeLanding have even lesser impact on the alert weights. The activities of DoS, DDoS, Reply, and Evil yield close to negligible scores.

7. Discussion

The findings indicate that the dataset comprises an imbalanced distribution of cyberattack classes. This imbalance might lead to biased results and conclusions. More specifically, Recon and Scanning generate the highest number of instances, whereas DoS, DDoS, and Normal traffic generate an average number of instances; BruteForce, MITM, Reply, FakeLanding, and Evil generate very few instances. The imbalance may influence the learning ability of a detection model: for example, a model may be able to learn to distinguish the majority classes better while being unable to learn the minority classes as well. Consequently, the minority-class instances are more likely to be misclassified as the majority class. Considering that rare but dangerous cyberattacks should also be recognized with high precision, the classification performance may not be satisfying.

The behavior feature analysis describes how certain classes of traffic behave with respect to the fwd_pkts_s feature. Normal traffic exhibits stable and low packet transmission, whereas some of the attack classes have higher variation and a wider spread. In particular, FakeLanding, MITM, and Bruteforce values are less concentrated than normal values; in addition, FakeLanding has the highest spread of all the classes which could indicate erratic packet movement during suspicious communication. These observations are helpful because they provide some insight that this feature could potentially separate normal from abnormal behavior. When feature values for an attack group are significantly different from those of normal traffic, they can be better used for classification, thus enhancing the overall value of the feature in the detection process.

The alert prioritization study puts our findings into practice. By far, the maximum risk score is obtained by Recon and Scanning; this suggests that those two types of activities should be attended to first. Normal traffic has a significantly lower score, while BruteForce, MITM, and FakeLanding are only of limited alerting importance. The other DDoS, Reply and Evil classes contribute almost nothing to the alert weight. This table is developed to best direct the security analyst's attention to the most suspicious activities and avoid unnecessary alerts in the normal and low-priority attack classes during routine monitoring

In general, the results all give positive expectations for the use of the ISCX dataset. We can say its application for anomaly detection appears effective, but the dense areas need to be tackled to be sure the model does not over-fit on less relevant details. Appropriate feature selection is key to achieve this, and the alert analyses provide guidance on which characteristics give the most faithful results. They also indicate that low ranking thresholds can be used within the implementation as long as the pattern vectors distinguishing classes without alert peaks are kept. This is an added benefit as it makes generating prioritized alarm lists computationally cheaper and encourages more information sharing on the indicators associated with particular attacks.

8. Future Work

Future work needs to concentrate on enhancing the dataset and increasing the dependability of the analytical process for not overlooking rare attack classes in the detection phase. Our results reveal strong class imbalance in which Recon, and Scanning are observed much more frequently than Evil, FakeLanding, MITM, Reply, and BruteForce. Thus, resampling methods, class weighting, and data augmentation should be incorporated in future work to enhance fairness for each class.

Furthermore, authors suggest the inclusion of more network traffic features as more of these closely related to the abnormal behavior may increase the classification quality such as flow duration, statistics of packet size, and inter arrival time. Finally, future research needs to compare various machine learning models and present the contribution of each feature for the estimated results to be easily interpretable by an analyst in a real security environment.

Testing the system in an actual Security Operations Center could reveal more than simulations alone. Though results suggest Artificial Intelligence speeds up responses, real proof needs field tests measuring detection accuracy and false alarms. Alert sorting might shift if threats evolve - this behavior deserves closer looks later on. Workload changes for analysts matter just as much as how fast decisions are made. Trust grows when systems show their reasoning clearly, avoid skewed judgments, and keep humans in charge. Seeing how bias appears - or gets blocked - could shape future updates. Confidence in daily operations depends on evidence from messy, live environments, not clean lab runs. Later efforts might track how well machines adapt when attack patterns drift over weeks. Performance isn't only about speed - it includes who carries the load and why choices get made. Long-term usefulness comes from blending machine help with human judgment, not replacing it.

9. Conclusion

The analysis indicates that the use of AI allows Security Operations Centers to become faster in responding to possible dangers and provides better sorting of alarms, but additionally, it increases the productivity of analysts. There is one important fact worth noting – some types of attacks, such as Recon and Scanning, occur frequently enough to create difficulties in balancing the detection process. As can be seen from this report, there are specific characteristics of the network flow, specifically forward packets per second, which work as a marker that distinguishes typical activity from suspicious actions. It seems that focusing on possible risks from the very beginning becomes especially important, as the Recon and Scanning attacks imply higher risks than most of the other ones. It can be considered that machines will take care of everyday tasks while leaving the most urgent ones for humans. This solution may not suit all tools; however, it integrates well into existing processes.

References

[1] Microsoft, "What is a security operations center (SOC)?," Microsoft Security, [Online]. Available: https://microsoft.com/en-in/security/business/security-101/what-is-a-security-operations-center-soc. [Accessed: May 28, 2026]

[2] M. Kosinski and J. Holdsworth, "What is incident response?," *IBM Think*, IBM, 2026. [Online]. Available: https://www.ibm.com/think/topics/incident-response [Accessed: May 29, 2026].

[3] X. Wang, X. Yang, X. Liang, X. Zhang, W. Zhang, and X. Gong, "Combating alert fatigue with AlertPro: Context-aware alert prioritization using reinforcement learning for multi-step attack detection," *Computers & Security*, vol. 137, p. 103583, 2024. .

[4] L. Ahluwalia, "Why Traditional SOCs Aren't Enough," CyberDefense Magazine, Apr. 15, 2026. [Online]. Available: https://cyberdefensemagazine.com/why-traditional-socs-arent-enough/. [Accessed: 29-May-2026].

[5] Rapid7, "What Is Alert Fatigue in Cybersecurity?," Rapid7 Fundamentals, 2025. [Online]. Available: https://www.rapid7.com/fundamentals/alert-fatigue-cybersecurity/. [Accessed: May 29, 2026].

[6] M. A. Islam, "Application of artificial intelligence and machine learning in security operations center," Ph.D. dissertation, Middle Georgia State Univ., 2023.

[7] M. Khayat, E. Barka, M. A. Serhani, F. Sallabi, K. Shuaib, and H. M. Khater, "Empowering security operation center with artificial intelligence and machine learning—A systematic literature review," *IEEE Access*, vol. 13, pp. 19162-19197, 2025.

[8] C. Bassey, S. Idowu, and C. Ojo, "Alert prioritization techniques in security monitoring: A focus on severity averaging and alert entities," *Saudi Journal of Engineering and Technology*, vol. 9, no. 7, pp. 334–339, 2024.

[9] Y. Liu, X. Shu, Y. Sun, J. Jang, and P. Mittal, "RAPID: Real time alert investigation with context aware prioritization for efficient threat discovery," in *Proceedings of the 38th Annual Computer Security Applications Conference (ACSAC)*, Austin, TX, USA, 2022, pp. 827–840.

[10] H. Albasheer, M. S. Md Siraj, A. Mubarakali, O. E. Tayfour, S. Salih, M. Hamdan, *et al*., "Cyber attack prediction based on network intrusion detection systems for alert correlation techniques: A survey," *Sensors*, vol. 22, no. 4, Art. no. 1494, 2022.

[11] B. R. Maddireddy and B. R. Maddireddy, "Enhancing network security through AI powered automated incident response systems," *International Journal of Advanced Engineering Technologies and Innovations*, vol. 1, no. 2, pp. 282–304, 2023.

[12] Z. Yousaf and D. Boomsma, *AI Driven SOC Operations: Improving Incident Response Time and Threat Analysis*, 2024.

[13] D. R. Chirra, "Towards an AI driven automated cybersecurity incident response system," *International Journal of Advanced Engineering Technologies and Innovations*, vol. 1, no. 1, pp. 429–451, 2023.

[14] H. J. Hadi, *UAV GCS Intrusion Detection Dataset (UAV GCS IDS)*, Figshare, Jul. 21, 2025. [Online]. Available: https://doi.org/10.6084/m9.figshare.29608541. [Accessed: May 30, 2026].

[15] J. Magalhães, R. Cruz, T. Cruz, P. Simões, and E. Monteiro, “GeNIS: A modular dataset for network intrusion detection and classification,” *Data in Brief*, vol. 58, Art. no. 111487, 2025.