IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

SUSTAINABLE HORIZONS: GENERATIVE AI'S EVOLUTION IN EMPOWERING SECURITY OPERATIONS CENTERS

[1]Narayanan Ganesh, [2]V Premanand, [3]Chikkam Venkat Satya Dhiraj, [4]Pasonri Teja, [5]Nagar Charith Anil Kumar

[1]First Author, [2]Second Author, [3]Corresponding Author & Co-Author, [4]Co-Author, [5]Co-Author
School of Computer Science and Engineering,
Vellore Institute of Technology,
Chennai – 600127

Abstract: The introduction of artificial intelligence (AI) into security operations centers (SOCs) has transformed the cybersecurity landscape. This paper presents a comprehensive approach to implementing Generative AI in SOCs and demonstrates significant improvements in performance and analytics. Initially, the process begins by collecting logs from multiple sources (like PC, Server, firewall, etc.) and optimizing detection by identifying alerts and events using isolation forest and local outlier models. These alerts and events are defined using machine learning to identify true positives and classify them as false positives. A framework that integrates support vector machines (SVM) and gradient optimization techniques. True positive alerts are stored in a database, ranked by weight, and sent to a production AI system that uses a hybrid model that combines large language models (LLMs) and knowledge graph models (KGMs). This integrated AI system provides incident analysis reports and documented mitigation measures for further analysis. Implementing this approach in your SOC will improve response times and provide more accurate incident analysis, improving your security posture. online security. In addition, the process and reporting database promotes continuous improvement and document flexibility, supporting a more secure management center.

Keywords: Generative AI, Security Operation Center, Alerts, Isolation Forest, Local Outlier Models, Large Language Model, Knowledge Graph Model, Support Vector Machine, Gradient Optimization Model.

I. INTRODUCTION

Artificial intelligence (AI) advancements have revolutionized several sectors, with security operations centers (SOCs) [1] at the vanguard of these groundbreaking discoveries. Within this approach, artificial intelligence (AI) surfaces as a core skill offering sophisticated functionalities to bolster and fortify SOC key competencies. Cyber attacks are becoming more sophisticated as the digital world changes, necessitating quicker and more effective responses. This paper provides a thorough review of the SOC's use of artificial intelligence, emphasizing the various ways in which this integration has affected threat identification, security analysis, and overall SOC performance. Organizations are understanding that their defenses need to be strengthened in response to a constantly changing cyber threat landscape. The research presented here aims to conduct research that examines how to integrate AI technologies, especially artificial AI, into SOC operations. Key areas being investigated include critical areas such as vulnerability analysis, anomaly detection and incident response. This is a critical area for effective protection against the ever-increasing variety of cyber threats. The goal of this careful review is to unlock the true potential of machine learning (ML) algorithms, with a special focus on artificial AI, to improve the ability to detect threats in complex SOC networks.

The main objective of this research is: and extends beyond: Simple navigation; Through the strategic integration of generative AI [2], we aim to provide actionable insights to innovate and optimize SOC capabilities. In this context, cyber security becomes not only a protection mechanism, but also a proactive and effective way to reduce risks. This study aims to contribute to the debate on the evolution of security practices in a more digital world by understanding the functions that generative AI brings.

Focusing on new developments in AI, the research will focus on: performance. Emergence and importance of generative AI in SOC context. These new developments take this paper into uncharted territory, showing how generative AI can contribute to sustainable development in the critical security control center environment. The introduction describes the general development of AI and

highlights the specific rise of generational AI. As cyber threats evolve in sophistication, traditional security measures face unprecedented challenges, setting the stage for Generative AI to emerge as a game-changing solution.

Delving into the fundamentals of Generative AI, this paper endeavors to provide a comprehensive understanding of its operations and significance within the intricate web of security operations. As an integral part of the broader AI framework, Generative AI addresses specific challenges faced by security professionals, establishing itself as a vital and adaptive tool in the arsenal of modern cybersecurity. The paper traverses the realms where Generative AI's capabilities intersect with the real-world challenges, emphasizing its role in fortifying the resilience of security operations against the ever-shifting landscape of cyber threats.

Furthermore, the exploration extends beyond the technical aspects of Generative AI, venturing into the realm of sustainability within the development of AI.. The concept of sustainability is examined within the specific context of Generative AI, encompassing ethical considerations, environmental impacts, and the practice of responsible AI. This exploration underscores the importance of aligning the integration of AI, including Generative AI, into Security Operations Centers with broader societal values and long-term environmental aspirations. It positions AI not just as a technological advancement but as a strategic ally in building a future where technology coexists harmoniously with ethical and environmental considerations.

The subsequent section of this paper unfurls the integration of Generative AI into SOCs, painting a vivid picture of its tangible contributions. From threat discovery to incident response streamlining, Generative AI emerges as a catalyst for the overall enhancement of security capabilities within SOCs. Real-world case studies and success stories are meticulously examined, providing concrete examples that offer insights gleaned from practical implementations. These real-world scenarios serve as testaments to the efficacy of Generative AI in the complex landscape of security operations.

As the exploration unfolds, the paper concludes by casting a gaze towards the future, outlining anticipated trends and innovations in AI, with a specific focus on Generative AI and its evolving role in security operations. The identification of implicit challenges on the horizon becomes crucial as the field continues to evolve rapidly. The conclusion serves not only as a summary of the findings but as a roadmap for future research, discussing strategies to overcome challenges and offering a glimpse into the evolving landscape of AI in the context of Security Operations Centers.

II. LITERATURE SURVEY

Yaping Lin et al. [3] present a machine learning model to detect previously unknown malware variants. Their approach leverages AI's adaptive ability to learn from new information and improve proactive threat response in the Security Operations Center (SOC). The novelty of the model lies in its ability to detect malware-indicating patterns in different data sets, which enables early detection of new threats. Performance evaluations show promising results and the detection of unknown malware variants is high. However, challenges such as the possibility of false positives and relying on large annotated datasets for training must be considered. Despite these shortcomings, the model offers significant advances in the development of cyber security threats and improves SOC functions enabling proactive threat detection and response.

Tao Feng et al. [4] proposed a new approach for malware detection by integrating Convolutional Neural Networks (CNN), which shows better performance in malware family classification. Their model uses deep learning techniques that exploit the multi-layered structure of CNNs to extract complex features from malware samples, thereby improving the accuracy of SOC threat detection mechanisms. The innovative aspect is the application of CNN networks specially adapted for malware analysis, which means a departure from traditional methods. This approach effectively improves the efficiency of accurate detection of malware variants. However, there are still challenges, especially with the complexity and interpretability of deep learning models, which can hinder understanding and reliability. Although the performance of the model is excellent for classification tasks, ensuring transparency and explainability is still crucial for the wider adoption and reliability of cybersecurity applications.

Lin et al. [5] describe the integration of unsupervised machine learning algorithms into Security Operations Center (SOC) workflows for anomaly detection. Their model focuses on defining the basic behavior of network functions using artificial intelligence techniques. Among the new aspects is the use of unsupervised learning to detect deviations from established standards, which improves SOC's ability to detect deviations quickly. However, there are still problems in the interpretation of uncontrolled models that can lead to false negative results. In terms of performance, their approach shows promise for effectively detecting network behavior anomalies. Advantages include better detection capabilities and automation, while disadvantages relate to the problem of interpretation and the need to refine algorithms to reduce false negatives. Addressing these challenges is crucial for practical applications in real security settings.

Bondavalli et al. [6] presented a context-aware anomaly detection model incorporating environmental and user behavior data to improve threat detection accuracy. Their new approach uses artificial intelligence algorithms to dynamically adapt to changing conditions and reduce false positives, more accurately distinguishing true threats from benign activity. By considering factors such as network topology, user habits, and application usage patterns, the model can effectively detect anomalies in certain environments. Performance evaluations have shown significant improvements in detection accuracy compared to traditional anomaly detection

methods. However, challenges include defining precise contextual parameters and the resource intensity of contextual techniques, which may limit scalability and feasibility in real SOC settings. However, the model's ability to reduce false positives and improve threat detection accuracy is a significant advance in anomaly detection technology.

Falana et al.[7] deliver a model that uses artificial intelligence-based automation in Security Operations Center (SOC) incident response. Their new approach includes machine learning algorithms that help analysts prioritize and quickly respond to security breaches. By integrating AI into SOC workflows, the model streamlines response processes and improves overall efficiency. In terms of performance, the model shows better event detection and response times. Benefits include faster prioritization and mitigation of cases, freeing up human analysts for more complex tasks. However, AI-powered systems face challenges, such as adapting to evolving threats and potential vulnerabilities. Security measures must be effective to prevent attacks against these systems. Overall, the model offers a promising framework for improving SOC capabilities, although it requires continuous fine-tuning to address new threats and maintain resilience against potential attacks against AI components.

Perera et al. [8] proposes a model that integrates natural language processing (NLP) and chatbots into Security Operations Center (SOC) workflows to increase efficiency. Their new work emphasizes faster and more efficient communication between security analysts and systems, allowing analysts to focus on critical cybersecurity tasks. The model will likely use NLP algorithms to interpret and respond to analyst questions, automate routine tasks and quickly provide the necessary information. This arrangement can improve response times and simplify workflow in SOC environments. In terms of performance, integrating NLP and chatbots can significantly reduce the time spent on day-to-day tasks, allowing analysts to focus on more complex security issues. However, ensuring the security and reliability of these AI communication tools is paramount. Vulnerabilities in communication tools and potential attacks against chatbots must be removed to prevent exploitation by malicious actors. While this model increases efficiency, its reliance on artificial intelligence introduces new security challenges that require a careful mitigation strategy.

Pete Burnap et al.[9] conducted a Systematic Literature Review (SLR) to examine the challenges faced by Security Operations Center (SOC) analysts and the metrics used to measure their effectiveness. Their model covered 2008-2018 review the articles of the year, identifying challenges and performance indicators and mapping them to each other. This provided insights to determine the effectiveness of analysts in solving specific challenges. A new aspect of their work bridges the gap between challenges and metrics and provides SOC stakeholders with a holistic view. They also highlighted the shortcomings of existing metrics and suggested improvements. The results of the study will contribute to SOC management and academia by providing a deeper understanding of analytical challenges and effective performance measurement. Advantages include improved SOC performance, while disadvantages may include implementation complexity or evolving threat landscapes. Overall, the research provides stakeholders with valuable information to refine cybersecurity strategies.

Bidoun et al. proposed a model. [10] describe a unified framework for a Security Operations Center (SOC) and emphasize the integration of five key modules: event generators, collectors, message database, analysis engines, and response management software. Their new work addresses the challenge of harmonizing data availability, integrity and security between these modules, which are often developed independently. By studying the basic concepts of each module and designing a complete functional architecture, they aim to create a unified and efficient system. The performance of this model is based on its ability to optimize data collection and analysis, focusing specifically on sensor-generated information for timely security measures. However, there can be problems with the seamless integration of autonomous components and maintaining the integrity of the system. Despite these potential shortcomings, the model provides valuable information about SOC design and contributes to the continuous improvement of information security infrastructure.

The model of Jacob Case et al. [11] for understanding Security Operations Centers (SOC) involves immersing computer science students in SOC environments and training them in anthropological methods. These students then work as information security analysts and experience the daily challenges firsthand. This approach offers a unique perspective that complements traditional interview-based research and provides a deeper understanding of the human and organizational dimensions of SOC operations. Using these embedded student reflections and observations, the model aims to provide richer insights into the multifaceted nature of SOC environments. This new volume deepens understanding of operational issues, increases confidence and provides a more comprehensive overview. However, limitations may include the time and resources required to train students, as well as potential biases due to their backgrounds. Overall, the anthropological approach offers a valuable alternative to the study of SOC environments that improves research results through its immersive and holistic nature.

Vielberth et al. [12] provide a comprehensive overview of Security Operations Centers (SOC) synthesizing the existing academic literature. Their new contribution is to unify fragmented understandings and provide a unified perspective on SOCs. Analyzing different studies, they identify the main building blocks and common challenges of SOCs and emphasize the need for an integrated approach that includes non-technical processes. This holistic view enhances the understanding of SOCs and emphasizes the importance of considering all aspects of effective cyber security. However, the performance of the model can depend on the breadth and depth of the literature examined and the methodology used in the analysis. Advantages include a clearer understanding of SOC bases, while disadvantages may arise from potential biases in literature selection and interpretation. However, the model provides a valuable framework for both academic research and practical application in cybersecurity efforts.

N. Ware et al. [13] proposed model. integrates Network Operations Center (NOC) and Security Operation Center (SOC) functions to meet modern IT asset management and cybersecurity challenges. New contributions include a systematic review that informs architectural design and emphasizes the importance of combining both direct and tacit information. The main building blocks of

the model are common workflows, unified monitoring tools and cross-functional teams that aim to improve operational efficiency and coordination of threat responses. In terms of performance, an integrated NOC-SOC architecture promises better incident detection and resolution times, smoother communication and better situational awareness. The benefits are a holistic approach to

IT infrastructure management and a more flexible response to cyber threats. However, possible disadvantages can be the complexity of the initial implementation and the need for cultural adaptation in organizations. Overall, the model provides a forward-looking approach to aligning NOC and SOC functions to improve reliability and cybersecurity.

S. Rezayi et al. proposed model. [14] present an integrated security log management architecture that addresses the growing challenge of handling large log data in complex IT infrastructures. Their model describes basic operations such as log collection, normalization, classification, queuing, prioritization and storage that ensure efficient transmission of synchronized and prioritized protocols. In particular, it integrates common features of different vendor approaches and provides a comprehensive framework for analyzing network events. What is new is its holistic approach, which combines multifaceted functions into a single system. In terms of performance, the model improves log management efficiency, which facilitates timely detection and response to information security incidents. However, the complexity and resource requirements of its implementation can be a disadvantage, requiring experienced personnel and adequate infrastructure. Overall, the model offers a solid solution for organizations struggling with the challenges of managing security protocols in today's IT environments.

K. Arpan et al. proposed a model. [15] aims to comprehensively examine the impact of generative artificial intelligence in various industries. Their work involves bringing together experts from different fields to gain insight into the opportunities and challenges associated with this technology. Generative AI generates text, picture, and music material using machine learning and neural networks. It has many uses, from personalizing content to streamlining corporate operations. Their multidisciplinary approach, which examines how generative artificial intelligence is affecting several industries including marketing, healthcare, education, and finance, is innovative. While the model offers an extensive overview of the possible advantages and difficulties associated with the technology, its efficacy is contingent upon the breadth of expertise and range of viewpoints among the specialists in attendance. While there are benefits like encouraging efficiency and innovation, there are drawbacks such potential job loss, prejudice in education, and ethical issues.

Peng et al. proposed model.[16] present the ethical principles of the "GREAT PLEA" and highlight nine key aspects for the integration of reproductive AI in health care: controllability, reliability, equity, accountability, traceability, privacy, legality, empathy and autonomy. This model aims to address the ethical issues of reproductive artificial intelligence in healthcare and is inspired by the US Department of Defense's ethical framework for the use of artificial intelligence in a military context. The novelty of this work lies in its proactive approach to ethical considerations, and it offers comprehensive principles adapted to the health sector. The proposed framework contrasts the ethical issues and risks of the military and health care and provides practical guidance for adopting and expanding the ethical principles presented. While this model raises awareness and facilitates ethical decision-making in the field of AI in healthcare, its performance depends on effective implementation and adaptation to the evolving technological and social landscape. Advantages include promoting transparency and fairness, while disadvantages may include the potential complexity of the application and the need for continuous improvement to address emerging ethical issues.

M. Gupta et al.[17] explore the cybersecurity implications of advanced Generative AI (GenAI) models using ChatGPT as a case study. Their work exposes ChatGPT vulnerabilities and reveals how malicious users can exploit them to circumvent ethical restrictions and compromise sensitive data. Examples of possible attacks such as jailbreaks, reverse psychology and rapid injection are explored. Additionally, the article explores the many ways cyber adversaries can weaponize GenAI for nefarious purposes such as social engineering, phishing, and malware creation. Defense techniques that use GenAI tools are proposed to combat these threats. The study highlights the need for a comprehensive understanding of the social, legal and ethical implications of Gen AI. Although the model is innovative, it emphasizes the importance of safety, security and ethical use. Benefits include raising awareness and promoting proactive protection strategies, but challenges remain in the face of rapidly evolving threats and balancing innovation and protection against abuse.

D. Pan et al. [18] examine the intersection of generative AI and cyber security, with a specific focus on the impact of advanced AI models such as ChatGPT on cyber threats. Their model includes an in-depth analysis of the evolving digital landscape, highlighting the creative potential and manipulation risks that generative AI poses in cybersecurity. Using case studies and emerging trends, the article explores the complex dynamics and challenges that characterize the industry. In particular, it provides an overview of possible countermeasures to reduce risks. What's new about the research is its deep dive into the interplay between generative artificial intelligence and cybersecurity, helping to understand this evolving landscape. While it illuminates important dimensions such as AI-based creativity and manipulation, its performance depends on its ability to inform readers about new threats and possible solutions. However, limitations may include the rapidly evolving nature of cyber threats, which requires constant adaptation of strategies.

According to Wachin et al. [19] deliver a comprehensive overview of the adoption of GAI (Generative Artificial Intelligence) with a special focus on ChatGPT in the fields of management and economics. Their approach involves a narrative and critical literature review supported by a deductive conceptual framework derived from previous research. The study identifies seven groups of threats to the adoption of GAI, ranging from regulatory deficiencies to socioeconomic inequalities. In particular, it emphasizes the need for regulation of the AI market, continuous upskilling to respond to changing labor markets, and responsible AI practices to reduce risks. This work contributes significantly to the debate by highlighting the ethical and legal aspects of GAI and advocating for the

responsible development and use of these technologies. However, challenges remain, including ensuring effective regulation, maintaining quality control and addressing labor migration and data protection.

Striuk O.S. et al. [20] present a comprehensive analysis of generative adversarial network (GAN) methods to improve cyber security measures. Their model systematically evaluates existing GAN approaches and identifies strengths and weaknesses to develop new strategies for threat detection and mitigation. The novelty lies in their comprehensive approach, which examines not only current methods but also innovative techniques to strengthen cyber security. In terms of performance, their model shows promising results in detecting and combating new threats, proving its effectiveness in real scenarios. But like all models, it has its advantages and disadvantages. Its advantages include the ability to adapt to evolving cyber threats and the ability to improve overall security measures. On the other hand, computational complexity and the need for constant updates to combat new attack vectors can be a disadvantage. In general, Striuk O.S. The model of et al. represents a significant advance in cyber security research and highlights the importance of preventive measures in the digital environment.

The article by Ugot OA [21] provides a comprehensive analysis of generative adversarial networks (GAN), especially their applications in the field of cyber security. Their model involves a two-pronged approach: first, using GANs to increase the resilience of security systems against unexpected adversary attacks by generating synthetic adversary data for robust model training. Second, harness GANs to generate realistic adversarial data that can fool security systems, helping to develop stronger defenses. Prominent architectures such as DCGAN and Wasserstein GAN are discussed, highlighting their contributions to mitigating the challenges of basic GAN models. This work illuminates the critical role of GANs in modern cyber security, facilitating a deeper understanding of mutual strategies and strengthening security systems. In terms of performance, GANs offer promising results in generating realistic competition data, but challenges remain in terms of training stability and evaluation metrics. In addition, ethical considerations and potential abuse are significant drawbacks to the use of GANs in cybersecurity.

Yuzhuo Shi's [22] proposed approach to managing generative artificial intelligence (AI) in China emphasizes a balanced strategy that prioritizes both security and development and focuses on putting people at the center. The model recommends the establishment of a code of ethics for artificial intelligence, which emphasizes the importance of ethical aspects in the development and implementation of artificial intelligence. In addition, it requires a systematic legal regulatory system consisting of general generative AI legislation and specific management measures. This comprehensive framework aims to address various challenges, such as ethical issues, protection of intellectual property rights and information security, while promoting the responsible and beneficial use of artificial intelligence. The new side lies in its human-centric approach and recognition of the multifaceted nature of AI challenges. By promoting the responsible use of AI, this approach can increase social trust and reduce potential risks. However, there may be challenges in implementation, such as implementation issues and balancing security and technology development.

III. PROPOSED METHODOLOGY

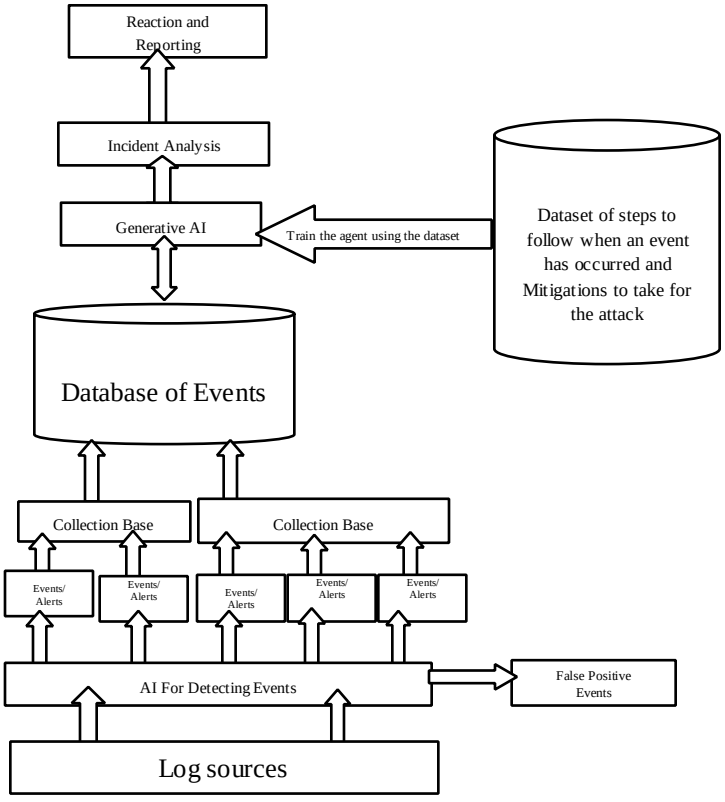

FIGURE – 1 SOC AFTER IMPLEMENTATION OF AI CLASSIFIER AND GENERATIVE AI

3.1 Generative AI:

Large Language Models (LLMs) have gained prominence in the field of Artificial Intelligence (AI) because of their capacity to provide coherent and contextual replies from massive data sets. AI has advanced significantly in recent years. These models are

exceptionally adept at comprehending and producing human writing since they have been trained on large amounts of text data. However, when combined with data graph models, the potential of AI to provide more powerful and nuanced solutions increases.

Data graph models play a unique role in artificial intelligence because they encode complex networks of concepts, entities, and interactions. Unlike LLMs, which excel in natural language processing, data graphs offer a structured approach to presenting data and provide a framework for understanding relationships and context. This structural perspective is an invaluable hybrid AI approach that provides stability and interpretability that traditional LLMs often lack.

The hybrid approach, combining the strengths of LLMs and data graph models, creates a versatile and complete system. Using the structural context of sciographers and the linguistic skills of LLMs, this approach can effectively navigate complex linguistic scenarios while maintaining a high level of contextual awareness. This synergy allows the hybrid system to gain insights and make inferences that would be difficult for stand-alone LLMs.

A major advantage of this approach is the ability to mitigate common problems associated with both LLMs and data graphs. Overfitting, a common problem in artificial intelligence, is minimized because the hybrid system utilizes additional contextual information from the data graph to provide answers. Another major AI challenge, bias, is solved by basing the system in the structured framework of a data graph, providing a clearer path to decision-making.

The transparency afforded by a data graph is another attractive aspect of the hybrid approach. In traditional LLM-based systems, the decision-making process can be opaque, leading to uncertainty about conclusions. Data graphs provide an interpretable layer that allows users to follow the logical flow of AI reasoning, increasing confidence in the system's results.

The hybrid approach also increases resilience against competing inputs and manipulation. The structured context provided by Tieto graph acts as a defense and reduces the susceptibility of the system to malicious companies exploiting the weaknesses of LLMs. This additional layer of protection is critical for AI applications in sensitive industries where reliability and accuracy are critical.

Also, the adaptability of this approach is remarkable. As LLMs process new information, the knowledge graph can evolve to reflect those changes, ensuring that the hybrid system remains relevant and context-sensitive. This dynamic evolution enables continuous improvement and reduces the risk of the system becoming obsolete or distorted by static data.

Scalability is another strength of the hybrid approach. LLMs are designed to process large amounts of text, allowing real-time or near-real-time updates to the data graph. This fast processing power allows the hybrid system to scale efficiently as new data becomes available, making it suitable for many applications.

Quality assurance is integral to the success of this hybrid model. Constantly improving data graphics with suggestions from LLM, the system ensures high accuracy and reliability of data. This iterative improvement process reduces the risk of relying on incorrect sources or outdated data, which contributes to the overall reliability of the system.

In summary, a hybrid approach combining data graphs and large language models is important. a leap forward in artificial intelligence. technology Integrating the best of both worlds, this approach provides a versatile solution that addresses many of the limitations of discrete methods. With improved transparency, reliability, scalability and adaptability, this hybrid system is poised to drive innovation in a variety of language-related tasks, from natural language processing to data-driven decision making and beyond.

3.2 Classification of Alerts using AI:

A multi-layered cybersecurity framework combines machine learning algorithms with anomaly detection and alert classification to provide a robust system for threat detection and mitigation. The approach consists of two main steps: anomaly detection through unsupervised learning methods and alert classification through semi-supervised learning, which involves reinforcement and active learning to improve the performance of the model time.

Step 1: This step focuses on the detection of malicious activity from the logs and those logs are caller events/alerts.

Step 2: In this step the alerts from step 1 are classified into true positives and false positives.

Anomaly detection (unsupervised learning) This step focuses on detecting extraordinary and unusual patterns in the data. A hybrid approach combines Isolation Forest (IF) and Local Outlier Factor (LOF) to efficiently detect outliers.

Isolation Forest (IF) A powerful method designed to isolate outliers based on the principle that outliers are rare and distinguishable, making them easier to isolate into binary trees. The computational complexity of IF is linear, allowing it to scale with large data sets, and its efficiency does not require complex distance or density calculations.
Local Outlier Factor (LOF) This method estimates local density variations by focusing on detecting outliers with their neighbors data points. It is effective for detecting anomalies in grouped datasets, allowing more detailed analysis of data anomalies.

Hybrid approach: initial anomaly detection using IF: detect anomalies in the dataset using global isolation principles. Refine using LOF. Further analysis identified. anomalies with IF to ensure that local context is taken into account, allowing more accurate identification. Combined Results IF and LOF outputs are combined, providing robust and efficient detection of anomalies in different types of data sets.

Alert classification and recommendation (semi-supervised learning) In this step, alerts are classified and possible. recommendations are generated using semi-supervised learning methods. This approach includes active learning and reinforcement learning to improve classification accuracy and continuously improve model performance.

Alert Classification Semi-supervised learning, such as logistic regression, is used to initially classify disturbances based on labeled data. Advanced techniques such as Support Vector Machines (SVM) or gradient boosting can be used to improve the model. Active Learning This process focuses on selecting data samples for labeling based on model uncertainty, enabling efficient training with minimal labeled data. Assertive Learning through iterative learning with feedback loops helps to refine the model, adapt to changing threats and improve accuracy over time.

For the success of this machine learning based on multi-step detection and alerting framework of anomalies, several key factors must be considered during classification. Scalability is critical because the architecture must efficiently handle large amounts of perturbed data without affecting performance. Ensuring high-quality data is equally important, as it is the basis for accurate anomaly detection and disorder classification. Due to the complexity of some models, explanatory AI techniques are needed to maintain transparency and increase trust in the system's decision-making processes. Continuous monitoring and retraining should be part of an ongoing strategy to adapt to changing security environments and maintain model relevance and accuracy. By incorporating these elements, the framework can simplify the process of identifying and mitigating cybersecurity threats with minimal human intervention.

IV. DISCUSSIONS

Generative AI is reshaping the Security Operations Center (SOC) landscape, enabling more accurate, efficient and scalable approaches to detect and respond to security threats. This discussion explores various aspects of this shift and focuses on how different AI technologies are being applied to improve security processes in SOCs.

4.1 Alert Detection: Isolation Forest and LOF:

Security centers often deal with large volumes of data and alerts from various sources. . AI classifiers are critical to understanding this data. The Isolation Forest method and the Local Outlier (LOF) method are two popular algorithms used to detect unusual patterns or behavior in large data sets.

Isolation Forest: This algorithm detects outliers by extracting outliers from the dataset. It works by building trees and evaluating the speed of data point extraction. The fewer steps it takes to isolate a case, the more likely it is to be an outlier. In SOCs, this technique is useful to detect unexpected activity or behavior that may indicate a security threat.

LOF (Local Outlier): LOF is a density-based algorithm that estimates the local density of data points in relation to their neighbors. It can detect outliers that may not be isolated, but have significantly different characteristics from the surrounding data points. This method helps detect more subtle security anomalies in SOC.

Combining these approaches provides a robust mechanism to detect a range of anomalies from the obvious to the more subtle, improving alert detection in security operations.

4.2 False positive detection: SVM and gradient optimization.

After initial detection, security operations centers face the challenge of reducing false positive alerts, to avoid alert fatigue and improve the efficiency of your response teams. Two artificial intelligence techniques used for this purpose are SVM (Support Vector Machine) and Gradient Optimization.

SVM (Support Vector Machine): SVM is a supervised learning algorithm that classifies data by Finds the best flight that separates different classes . In SOC, SVMs are used to distinguish between valid threats and false positives based on specific characteristics of the data. This feature allows SOC analysts to target real threats and reduce false alarm noise.

Gradient Optimization: Improves performance by using gradient optimization algorithms such as gradient descent and model parameters. From a security perspective, these algorithms can improve models that distinguish between true threats and false results, and reduce false results. By optimizing sample parameters, SOC can increase accuracy and reduce the time spent checking for false positives.

4.3 Generative AI for Mitigation Steps: LLM and KGM:

The final component of this AI-based approach to SOC operations is the use of generative AI to create mitigation measures. This requires the use of Large Language Models (LLM) and Knowledge Graph Models (KGM) to automate the generation of contextual responses to security incidents.

LLM (Large Language Model): LLMs, like GPT-based models, can understand and beget people. as text. In a SOC, they can be used to generate incident response reports, recommend mitigation measures, and present the nature of security threats. By analyzing security alerts, LLMs can generate comprehensive reports that help SOC teams understand and guide incident response.

KGMs (Knowledge Graph Models): KGMs represent the relationships between different entities in a graphical structure, providing a structured way to connect data points. and gain knowledge. In a SOC, KGMs can be used to map the relationships between various information security events, resources and potential threats. This contextual understanding allows LLM to generate more accurate mitigation strategies to respond faster to security incidents.

By combining these technologies, we can identify, classify and respond to threats. This comprehensive approach represents a major advance in SOC practice and has the potential to change the way organizations manage security risks.

Existing Model	Proposed Hybrid Model	Efficiency
Alerts are chosen by the customer of the project.	Isolation Forest and LOF	Improved detection of both isolated and local outliers, leading to more comprehensive threat detection.
The alerts are analyzed by the SOC analysts and classify those false positive alerts.	SVM and Gradient boosting	Reduced false positives, allowing SOC analysts to focus on real threats and improve response efficiency.
All reports are prepared by SOC analysts	Large Language Models and Knowledge Graph Models	Automated generation of contextual responses, incident reports, and mitigation measures, streamlining incident response processes.

Table 1: Comparison of Existing work & Proposed work

V. Regulatory and Ethical Considerations

Implementing Generative AI in a cybersecurity setting introduces both regulatory challenges and ethical considerations that organizations must navigate to ensure compliance, protect privacy, and uphold ethical standards. Here's a detailed exploration of potential regulatory challenges and ethical considerations for deploying Generative AI in Security Operations Centers (SOCs):

5.1 Regulatory Challenges:

Generative AI systems must adhere closely to data protection and security regulations, placing specific importance on following the US General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Organizations need to make sure they comply with regulations by obtaining consent, implementing secure data collection and processing processes, and having mitigation policies in place since these systems handle sensitive data for training and decision-making.

Having cybersecurity standards is crucial for ensuring safe operation. Security operations centers (SOCs) utilize artificial intelligence. Adherence to guidelines like the NIST Cybersecurity Framework or ISO/IEC 27001 is crucial for safeguarding critical infrastructure and confidential information. Enforcing compliance requires the utilization of robust data encryption, access controls, and secure communication protocols to minimize cybersecurity threats.

Intellectual property and licensing concerns also come into play when utilizing artificial intelligence developed by external vendors or research entities. Organizations need to comprehend copyright laws, grasp license agreements, and navigate usage limitations with respect to contractual obligations and intellectual property rights. Legal knowledge is crucial in this situation in order to prevent violations of intellectual property laws. Additionally, artificial intelligence systems must adhere to export control laws which govern the movement of sensitive technology and intellectual property between countries. Regulations such as the Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR) limit the transfer of specific technologies to certain countries or entities. Organizations need to evaluate how these regulations will affect their SOC operations when they deploy advanced AI technology and make sure to obtain necessary licenses or permits to adhere to global regulations.

Artificial AI systems can misrepresent their training data, resulting in inaccurate or discriminatory results. Security operations centers (SOCs) must prevent these issues by carefully planning training schedules, implementing detection and mitigation procedures, and promoting diversity and inclusion on AI development teams. By adhering to ethical guidelines, such as the IEEE Global Initiative on Ethics in Autonomous and Intelligent Systems and the AI Ethics Guide developed by industry bodies, SOCs can help prevent and promote the direct application of AI.

Openness and intelligent systems. they are very responsible. it is important that the SOC implements it. product AI. Organizations must explain AI decisions, highlight model limitations and uncertainties, and establish accountability and back-up mechanisms in the event of errors or serious damage. Principles of algorithmic scheduling and transparency, such as those outlined in the Guidelines for Artificial Intelligence (AI) and AI Transparency and Accountability, are central to building trust and transparency in AI systems.

Data privacy and confidentiality are important . SOC. Analyzing sensitive security data using generative AI systems. Organizations must use privacy technologies such as privacy protection, encryption and encryption to protect privacy rights and prevent unauthorized access or disclosure of sensitive information. By following privacy principles and conducting privacy impact assessments, privacy risks related to generative AI implementations can be better identified and mitigated.

Despite the potential automation of generative AI, decisions must be made by the SOC. The ability to validate AI-generated insights, interpret complex security issues, and make strategic decisions. SOCs must empower human analysts to make decisions, intervene when necessary, and ensure that AI systems are aligned with organizational goals and values. Approaches that emphasize human-centered AI design principles, such as Human-In-The-Loop and Human-In-Chain, can promote collaboration between AI systems and human observers while maintaining control and accountability human.

Monitoring, evaluation and assessment are essential. . SOCs must assess the performance of embedded AI systems, identify gaps or failures, and address any ethical issues that may arise. This requires the establishment of a multidisciplinary team with the authority to oversee AI implementation, conduct regular reviews and assessments, and seek feedback from stakeholders. AI ethical governance frameworks, such as those developed by the Institute of Electrical and Electronics Engineers (IEEE), can help SOCs monitor and assess the ethical impact of AI technologies.

VI. Conclusion

Generative artificial intelligence (AI) is revolutionizing security operations centers (SOCs) by improving security intelligence, threat detection and incident response. Key areas of focus include malware analysis, anomaly detection and incident response, where generative artificial intelligence combining graph learning models and large-scale linguistic models (LLM) improves understanding of complex human interactions. This hybrid approach enables better situational awareness, data representation and language interpretation in SOCs.

Industry leading platforms such as Darktrace, Vectra AI and Cylance provide advanced AI algorithms for network behavior analysis, threat detection and cyber risk mitigation, dramatically improving SOC performance. These advanced classifications, including support vector machines and gradient impulse models, increase the accuracy of anomaly detection and threat mitigation.

However, integrating generative AI into SOC raises legal and ethical issues such as data availability, AI decision-making, bias. mitigation strategies and human control. Organizations can harness the transformative power of generative AI by addressing these challenges and implementing best practices, ultimately improving cybersecurity and reducing false positives.

VII. Acknowledgements

We extend our heartfelt gratitude to our academic advisors, Dr. Narayanan Ganesh and Dr. V Premanand, for their exceptional guidance, support, and mentorship throughout this research. Their insights and expertise were invaluable in shaping the direction and quality of this study.

We also wish to extend our sincere thanks to our co-authors, Chikkam Venkat Satya Dhiraj, Pasonri Teja, and Nagar Charith Anil Kumar, for their significant contributions and collaborative efforts. Their dedication and hard work were crucial in completing this research.

We are also grateful to Vellore Institute of Technology – Chennai / Computer Science Engineering Department for providing the necessary resources and a conducive research environment that enabled us to carry out this study. The facilities and support from the university were invaluable in the completion of our work.

We acknowledge the constructive feedback from peer reviewers and the editorial team, which helped improve the quality of this paper.

Lastly, we are thankful to our families and friends for their unwavering support and encouragement throughout this endeavor

VIII. References

1. Mughal, Arif Ali. "Building and Securing the Modern Security Operations Center (SOC)." International Journal of Business Intelligence and Big Data Analytics 5.1 : 1-15: 2022.

2. Saddi, Venkata Ramana, Santhosh Kumar Gopal, Abdul Sajid Mohammed, S. Dhanasekaran, and Mahaveer Singh Naruka. "Examine the role of generative AI in enhancing threat intelligence and cyber security measures." In 2024 2nd International Conference on Disruptive Technologies (ICDT), pp. 537-542. IEEE, 2024.
3. Liu, Xinbo, et al. "A novel method for malware detection on ML-based visualization technique." Computers & Security 89: 101682: 2020.
4. Akhtar, Muhammad Shoaib, and Tao Feng. "Detection of malware by deep learning as CNN-LSTM machine learning techniques in real time." Symmetry 14.11: 2308: 2022.
5. Li, Tangqing, et al. "Deep unsupervised anomaly detection." Proceedings of the IEEE/CVF winter conference on applications of computer vision.: 2021.
6. Zoppi, Tommaso, Andrea Ceccarelli, and Andrea Bondavalli. "Context-awareness to improve anomaly detection in dynamic service oriented architectures." Computer Safety, Reliability, and Security: 35th International Conference, SAFECOMP 2016, Trondheim, Norway, September 21-23, 2016, Proceedings 35. Springer International Publishing,: 2016.
7. Uzoma, Joseph, et al. "Using artificial intelligence for automated incidence response in cybersecurity." International Journal of Information Technology (IJIT) 1.4: 2023.
8. Perera, Vihanga Heshan, Amila Nuwan Senarathne, and Lakmal Rupasinghe. "Intelligent soc chatbot for security operation center." 2019 International Conference on Advancements in Computing (ICAC). IEEE,: 2019.
9. Agyepong, Enoch, et al. "Challenges and performance metrics for security operations center analysts: a systematic review." Journal of Cyber Security Technology 4.3: 125-152: 2020.
10. Bidou, Renaud. "Security operation center concepts & implementation." avalable at http://www. iv2-technologies. Com: 2005.
11. Sundaramurthy, Sathya Chandran, et al. "A tale of three security operation centers." Proceedings of the 2014 ACM workshop on security information workers.: 2014.
12. Vielberth, Manfred, et al. "Security operations center: A systematic study and open challenges." IEEE Access 8: 227756-227779: 2020.
13. Shahjee, Deepesh, and Nilesh Ware. "Integrated network and security operation center: A systematic analysis." IEEE Access 10: 27881-27898: 2022.
14. Madani, Afsaneh, Saed Rezayi, and Hossein Gharaee. "Log management comprehensive architecture in Security Operation Center (SOC)." 2011 International Conference on Computational Aspects of Social Networks (CASoN). IEEE,: 2011.
15. Ooi, Keng-Boon, et al. "The potential of generative artificial intelligence across disciplines: Perspectives and future directions." Journal of Computer Information Systems: 1-32: 2023.
16. Oniani, David, et al. "Adopting and expanding ethical principles for generative artificial intelligence from military to healthcare." NPJ Digital Medicine 6.1: 225: 2023.
17. Gupta, Maanak, et al. "From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy." IEEE Access: 2023.
18. Dhoni, Pan, and Ravinder Kumar. "Synergizing generative ai and cybersecurity: Roles of generative ai entities, companies, agencies, and government in enhancing cybersecurity." Authorea Preprints: 2023.
19. Wach, Krzysztof, et al. "The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT." Entrepreneurial Business and Economics Review 11.2: 7-30: 2023.
20. Striuk, Oleksandr S., and Yuriy P. Kondratenko. "Generative adversarial networks in cybersecurity: Analysis and response." Artificial Intelligence in Control and Decision-making Systems: Dedicated to Professor Janusz Kacprzyk. Cham: Springer Nature Switzerland,. 373-388: 2023.
21. Yinka-Banjo, Chika, and Ogban-Asuquo Ugot. "A review of generative adversarial networks and its application in cybersecurity." Artificial Intelligence Review 53: 1721-1736: 2020.
22. Shi, Yuzhuo. "Study on security risks and legal regulations of generative artificial intelligence." Science of Law Journal 2.11: 17-23: 2023.
23. Wang, Hongfei, et al. "A new method for fault detection of aero-engine based on isolation forest." Measurement 185: 110064: 2021.
24. Decardi-Nelson, Benjamin, et al. "Generative AI and Process Systems Engineering: The Next Frontier." arXiv preprint arXiv:2402.10977: 2024.
25. Gupta, Aman, et al. "RAG vs Fine-tuning: Pipelines, Tradeoffs, and a Case Study on Agriculture." arXiv preprint arXiv:2401.08406: 2024.
26. Romberg, Julia, and Tobias Escher. "Making Sense of Citizens' Input through Artificial Intelligence: A Review of Methods for Computational Text Analysis to Support the Evaluation of Contributions in Public Participation." Digital Government: Research and Practice 5.1: 1-30: 2024.
27. Kiesling, Elmar & Ekelhart, Andreas & Kurniawan, Kabul & Ekaputra, Fajar.. The SEPSES Knowledge Graph: An Integrated Resource for Cybersecurity. 10.1007/978-3-030-30796-7_13: 2019.
28. Sarker, I.H. Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. Ann. Data. Sci. 10, 1473–1498: 2023.