

AI-Powered SOC Assistant

M. Sai Siri Shriya¹, R. Aravind Rathod², Krish Gupta³, V. Venkat Sai Krishna⁴, Vaggela Rama Chandra Murthy Raju⁵

^{1,2,3,4,5} Department of Computer Science and Engineering, Vardhaman College of Engineering, Hyderabad, India

shriyamalyala23@gmail.com¹, aravindramavath22@gmail.com², krishgupta90621@gmail.com³,
venkatsaikrishna369@gmail.com⁴, murthyraju1803@vardhaman.org⁵

*Corresponding author: Krish Gupta (krishgupta90621@gmail.com)

ABSTRACT

Cybersecurity threats are increasing rapidly as organizations rely more on digital infrastructure and online services. Security Operations Centres (SOCs) are responsible for monitoring and responding to these threats, but many still depend on manual investigation and static rule-based systems. These traditional approaches struggle to handle the large volume of alerts generated by modern networks. As a result, security analysts often face issues such as alert fatigue, delayed responses, and limited contextual information when analysing incidents, which can reduce the efficiency of security operations and increase the chances of missing critical threats. To address these challenges, this paper proposes an AI-Powered SOC Assistant that helps analysts detect and analyse potential security threats more effectively. The system combines machine learning techniques, natural language processing, and threat intelligence sources to analyse real-time security data collected from SIEM logs, OSINT sources, and external threat feeds. By correlating and analysing this information, the system can identify suspicious patterns and highlight possible attack indicators. The proposed solution also includes a risk-based alert-scoring mechanism to prioritise incidents by severity. An interactive dashboard and conversational interface allow analysts to explore alerts with natural-language queries and receive clear explanations and recommended response actions, improving investigation efficiency and overall SOC performance.

Keywords: Security Operations Center (SOC), Cyber Threat Intelligence (CTI), Machine Learning, Anomaly Detection, Isolation Forest, Generative AI, Large Language Models (LLMs), Explainable AI (XAI), SIEM, Threat Hunting, Log Analysis, Risk-Based Alert Scoring.

1. Introduction

Nowadays, cybersecurity is a fundamental requirement of modern digital infrastructure and of all organisations across industries, as reliance on digital technology continues to increase [1], [3]. Despite fast-changing technology that keeps evolving the nature of business, most organisations still operate manually and rely on rules in monitoring and responding to security incidents. The old method of security monitoring and incident response remains manual and occasionally time-consuming, and can no longer be used to manage the growing number and complexity of cyber threats. Security Operations Centres (SOCs) are also facing threats such as a high volume of alerts, inadequately skilled staff, disjointed security tools, a lack of contextual intelligence, and slow response times. The security analysts have the challenging task of investigating thousands of warning signals, many of which are not real threats, and, as a result, experience alert fatigue and reduced productivity [8]. The further complexity of modern cyber threats, including phishing, ransomware, advanced persistent threats, insider threats, and zero-day attacks, complicates their detection and mitigation. Additionally, the absence of automation and predictive intelligence leaves a gap in proactively preventing threats to the organisation, thereby making it less resilient to cyber threats. To overcome these challenges, this paper proposes the AI-Powered SOC Assistant, which will help bridge the gap between the traditional SOC process and intelligent, automated security solutions. It is scalable with an analyst-focused system that automates and uses artificial intelligence to detect threats, analyse and prioritise, and respond. The system integrates machine learning, natural language processing, and threat intelligence APIs to collect and correlate real-time information from SIEM logs, OSINT, threat feeds, and other security data, which are useful for accurate classification and decision-making [5], [10]. Moreover, it applies predictive analytics to recognise potential threats and malicious activity before they become significant security

incidents. Through its chat-based interface and interactive dashboards, SOC analysts can search security data in natural language, which is far quicker than existing mechanisms that require complex query options. Through this, the AI-Powered SOC Assistant will save time spent on responses by minimising delays, increasing the efficiency of the SOC. Finally, the proposed system is an active, intelligent, and robust security operations strategy that can help create secure digital ecosystems by efficiently utilising AI-based cybersecurity solutions.

2. Literature Survey

The increasing sophistication, scale, and frequency of cyber-attacks have placed unprecedented pressure on modern Security Operations Centres (SOCs). Traditional SOCs rely heavily on human analysts to monitor alerts, investigate incidents, and respond to threats, which often leads to alert fatigue, delayed responses, and missed attacks. To address these challenges, recent research has increasingly focused on AI-powered, autonomous, and intelligent systems that enhance SOC efficiency, accuracy, and scalability. This literature survey reviews key studies that collectively contribute to the development of AI-powered SOC assistants, emphasising autonomous threat hunting, generative AI, agentic AI, cyber threat intelligence (CTI), structured adversary frameworks, and explainable AI-driven systems.

- Autonomous Threat Hunting: A Future Paradigm for AI-Driven Threat Intelligence (2023).** The paper presented above discusses the evolution of threat hunting from conventional, manual, and hypothesis-based methods to fully autonomous methods aided by AI [1]. In classical SOC settings, log, network traffic, and endpoint data must be analysed manually using predefined rules or indicators of compromise (IoCs). The authors propose full autonomy for threat-hunting systems that constantly monitor and analyse telemetry data using machine learning algorithms to detect abnormal and unknown attack behaviour. The paper highlights the relevance of such systems in SOCs, where there is need to make decisions in real time [1], [3]. Threat hunting systems are automated tools that can identify suspicious patterns, thereby reducing analysts' workload and dwell time. Also, AI-based threat intelligence feeds can refresh detection models on the fly to cope with new threats. Although the advantages are there, the fact that AI models are not transparent and interpretable remains a challenge that can be a limitation in adopting AI in SOCs. The paper highlights the need to create AI-based SOC assistants that enable lifelong learning and active learning [1], [11], [15].
- Generative AI Revolution in Cybersecurity: A Comprehensive Review of Threat Intelligence and Operations (2025).** This work discusses how Generative AI technologies are transforming cybersecurity practices. The study focuses on the role of Generative AI in improving threat intelligence and assisting Security Operations Centers (SOCs) in analysing and responding to security incidents more effectively. It highlights how AI models can process large volumes of security data and help analysts identify potential threats and understand complex attack patterns. The authors demonstrate the capability of large language models (LLMs) to process enormous amounts of unstructured threat intelligence data, including incident reports, malware analysis, threat blogs, and security advisories [2]. In SOC operations, GenAI can automatically summarise alerts, correlate events across multiple tools, and provide contextual explanations for identified threats. The authors clearly state that GenAI is designed to assist SOC analysts, not replace them, and act as an intelligent assistant that speeds up investigations and enhances decision-making. Moreover, GenAI can automatically generate playbooks and query security logs in natural language, requiring less expertise from junior analysts [2]. The authors also discuss the potential for adversarial attacks and the need for secure deployment. In summary, this study advocates AI-driven SOC assistants that use generative intelligence to explain alerts and respond.
- Transforming Cybersecurity with Agentic AI to Combat Emerging Cyber Threats (2025).** The authors introduce the concept of Agentic AI, which entails the application of AI as free-will agents of rationality, able to organize concerted measures [3]. In the context of Security Operations Centers (SOCs), agentic AI allows systems not only to recognize potential threats but also to take predefined or adaptive actions to counter those threats. These actions could

involve isolating infected machines or blocking IP addresses deemed malicious. The authors also emphasize the effectiveness of agentic AI while handling multi-stage or persistent cyber attacks, where rapid action is a necessity. By leveraging agentic AI with other technologies already integrated into the SOC ecosystem, such as SIEM or SOAR technologies, an organization can help achieve near real-time incident detection and response. However, the research also underscores the need to maintain a level of human-in-the-loop mechanisms to ensure accountability, control, and oversight of the actions taken by the AI system. Therefore, this research article also lends support to the idea of AI-driven SOC assistants that incorporate the ability to take actions while also providing a level of supervision by humans. This not only helps achieve rapid incident handling but also allows the organization to maintain its security policies while containing the threat.

- **HuntGPT: Combining Machine Learning-Based Anomaly Detection, Large Language Models, and Explainable AI (2023).** HuntGPT is a new paradigm of combining machine learning-based anomaly detection, large language models (LLMs), and explainable AI (XAI) to assist SOC analysts [6]. The suggested framework will start with the anomaly detection relying on ML and subsequently proceed with the application of the LLMs to produce an explanatory version of identified threats that could be understood by humans. This is a work of significant value to the implementation of SOC AI-based solutions: the lack of interpretability [6], [8]. The analysis proves that the analysis of the information by analysts becomes more trustful, and the effectiveness of the investigation is enhanced with the help of explicatory, conversational AI products.

3. Proposed Approach

3.1 Overview of the System

Recent developments in artificial intelligence have driven a paradigm shift in the cybersecurity domain, particularly within Security Operation Centres (SOCs). Conventional threat detection and response mechanisms, which are highly dependent on manual analysis and rule-based systems, are increasingly under strain as the number of sophisticated cyber threats rises. AI-based SOC assistants, which utilise autonomous threat hunting, generative intelligence, agentic AI, and explainable AI, provide a potential solution to this problem by automating threat detection, analysis, and response, and improving analyst productivity and decision-making. These assistants are capable of handling massive amounts of structured and unstructured data, providing human-readable explanations, and delivering coordinated responses in near real time. However, challenges such as model interpretability, secure deployment, and the need for human oversight are still important considerations. In summary, the literature clearly indicates a trend of incorporating AI as an interactive, explainable, and proactive co-analyst to enhance SOC capabilities and improve organisational cyber resilience [1]-[6], [14].

3.2 System Description

- The SOC Assistant uses AI to continuously collect and analyse security data from different sources, such as network logs, system events, threat intelligence feeds, and security tools such as SIEM and IDS/IPS systems. With the help of machine learning algorithms and pattern recognition techniques, the system is able to analyze the security information and detect potential threats, suspicious behavior, and even zero-day attacks in real time. This improves the efficiency of threat detection by providing better visibility into security threats and reducing false positives reported by other security systems using rule-based approaches. This allows security analysts to better understand the situation and detect threats more effectively and efficiently.
- Additionally, the system can assist in automating response activities to security incidents by correlating response actions with security alert information. This is done by categorizing the detected security incidents into different severity levels. This allows security analysts to prioritize their activities based on the severity level of the threats detected by the system. With the help of AI-based decision support tools, the SOC Assistant can provide security analysts

with useful information on security threats, including attack timelines and other details that may help reduce the time required to investigate them. In addition, the system can integrate with SOAR tools to automate response actions such as blocking IP addresses and sending alerts to security analysts.

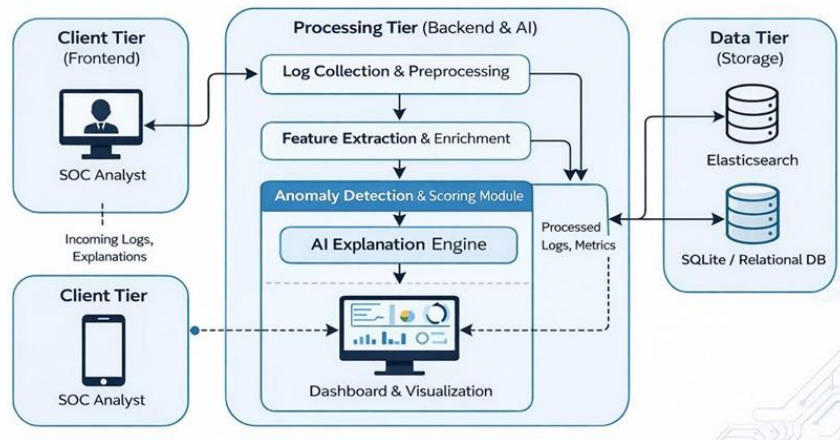


Fig. 1: System Design

- The proposed solution, as shown in Figure 1, is built with a modular and extensible architecture that can easily integrate with existing security infrastructure while improving and adding more features in the future. It adheres to best security practices, including role-based access control, secure data handling, and system monitoring, to protect critical security-related information [1], [8]. It includes an interactive, user-friendly dashboard that allows security analysts in the SOC to easily monitor security-related information and system activities, and generate detailed reports in real time. By presenting security-related information in an easily understandable way, the proposed system can help security analysts better understand security situations and threats. In addition, the proposed system can learn from security-related information and feedback from security analysts, enabling it to adapt to new security threats and gradually improve its accuracy in detecting them. It can analyze security information in real time from different sources to provide a better understanding of the security situation in the entire organization [3], [10]. With the help of automated, AI-driven analysis, and human expertise, the proposed SOC Assistant can help security analysts make better decisions more efficiently to prevent complex security threats.

3.3 System Architecture

The AI-powered SOC Assistant is designed using a multi-tier architecture to ensure high scalability, flexibility, and operational efficiency. The client tier provides SOC analysts with a web-based dashboard, allowing them to monitor alerts, review AI-generated insights, and interact with the system through natural language or traditional interfaces [6], [13]. An API Gateway manages secure and reliable communication between the frontend and backend, enforcing authentication and data integrity. The middle tier is responsible for processing security logs using advanced machine learning models for anomaly detection, storing events in Elasticsearch, and generating detailed, human-readable explanations through AI models. It also maintains structured and historical data in SQLite for in-depth analysis, reporting, and trend monitoring.

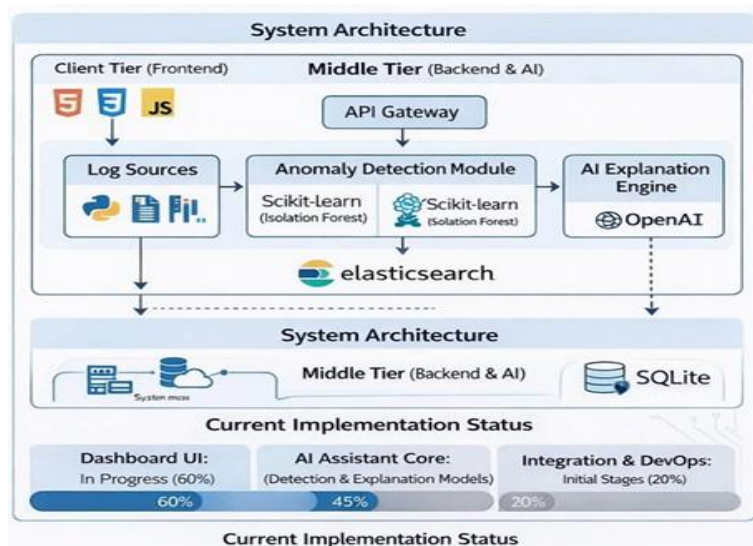


Fig. 2: System Architecture

Figure 2 demonstrates that a layered architecture ensures efficient processing of large-scale security data, supports real-time alert correlation, enables seamless integration with existing SOC tools, and allows future expansion to incorporate additional AI capabilities [3], [11].

3.4 Methodology

Step 1 - Dashboard Access: SOC analysts interact with the system via a web-based dashboard that allows them to view security alerts, monitor system activity, and view the status of the entire platform, as shown in Figure 3.

Step 2 - API Gateway Processing: User requests made through the dashboard are routed via an API Gateway to backend systems.

Step 3 - Log Collection: The security information and event management system collects security logs from various sources, including system, application, and network logs, as well as external threat information.

Step 4 - Data Preparation: Collected log data is cleaned and structured to make it more suitable for machine learning models.

Step 5 - Anomaly Detection: Machine learning models like Isolation Forest analyze the processed log data to identify any unusual activity or potential security threats.

Step 6 - Event Storage and Indexing: Detected events and anomalies are indexed and stored in Elasticsearch, allowing for quick search and analysis of historical logs.

Step 7 - AI-Based Explanation: An explanation module uses AI to provide the analyst with a description of the detected anomalies.

Step 8 - Backend Data Storage: Detected alerts, explanations, and other data are stored securely in a SQLite database for future reference and reporting.

Step 9 - Visualization and Reporting: The dashboard provides the analyst with the ability to visualize the alerts, insights, and other system metrics.

Step 10 - Continuous Improvement: The system improves over time by learning from past incidents, analyst feedback, and emerging threat patterns.

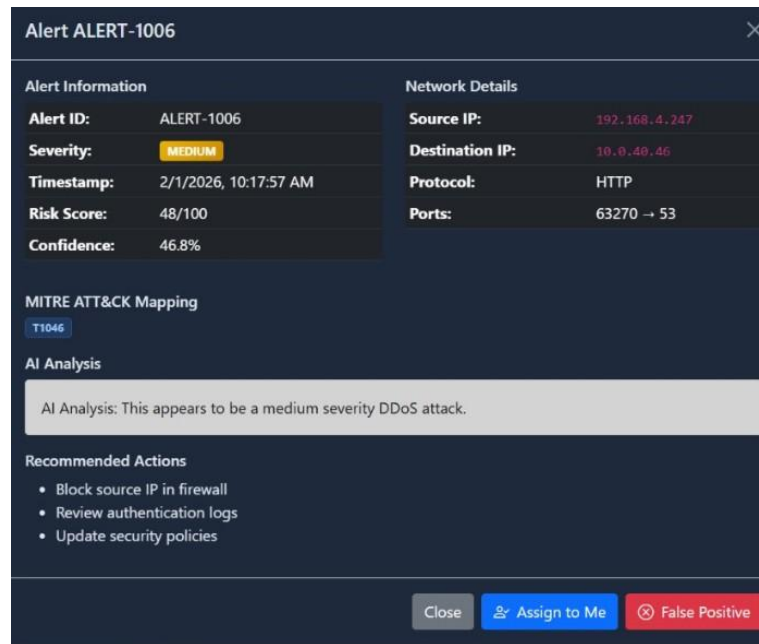


Fig. 3: Threat Analysis

4. Results and Discussion

This project aims at developing an AI-driven Security Operations Center (SOC) Assistant that is intended to enhance the speed, accuracy, and efficiency of cyber threat detection and analysis [13]. The topic of this project has been derived from the rising tide of security alerts and their complexity, as well as the limitations of traditional rule-based security monitoring systems. A comprehensive literature review examined existing SOC solutions, SIEM and SOAR systems, and prior research on ML-based anomaly detection, AI explainability, and agent- or generative-model approaches for cybersecurity applications, emphasising the need for intelligent and automated decision support [1], [2], [14]. Based on the findings from the literature study, we have designed a multi-tiered system. This system integrates log collection, preprocessing, feature extraction, machine-learning-based anomaly detection, AI-driven explanation generation, and efficient data storage. The system is designed to handle both real-time and historical security logs, detect anomalies, generate human-understandable explanations, and display results on an interactive dashboard to support security analysts' decision-making. The findings of this project indicate improved threat detection accuracy, reduced false positives, faster incident response, and increased productivity for security analysts due to enhanced visualisations and AI-driven explanations. Throughout this project, the team gained hands-on experience in cybersecurity operations, machine learning, resilient system architecture design, and AI integration into real-world SOC operations.

Table 1: Comparative Analysis of AI-Based SOC Systems

Ref.	Approach	Technology Used	Deployment Context	Limitations	Proposed System Advantage
[1]	Autonomous Threat Hunting	Machine Learning-based anomaly detection	Enterprise SOC environments	Limited interpretability and human interaction	Adds explainable AI and interactive chat-based analysis
[2]	Generative AI in Cybersecurity Operations	Large Language Models (LLMs)	Alert summarisation and intelligence analysis	Risk of hallucination and secure deployment challenges	Combines LLM explanations with structured SIEM correlation
[3]	Agentic AI for Incident Response	Autonomous AI agents with SOAR integration	Real-time coordinated response systems	Requires strict human oversight and governance	Supports human-in-the-loop control with explainable automation
[4]	Cyber Threat Intelligence	Threat feeds + MITRE ATT&CK mapping	Intelligence-driven SOC workflows	Static rule dependency	Dynamic risk scoring and predictive analytics integration

Ref.	Approach	Technology Used	Deployment Context	Limitations	Proposed System Advantage
	Frameworks (CTI)				
[5]	HuntGPT Framework	ML anomaly detection + LLM + Explainable AI	Conversational SOC assistant	Research-stage implementation	Fully integrated multi-tier architecture with dashboard and backend storage
[6]	AI-Based SOC Automation Systems	ML + Blockchain + Automation tools	SOC optimisation environments	High integration complexity	Modular and scalable API-driven architecture
[7]	Cognitive SOC Systems	AI-based correlation and behavioural analytics	Enterprise security monitoring	High computational requirements	Efficient log indexing using Elasticsearch with lightweight ML models
Proposed	AI-Powered SOC Assistant	Isolation Forest + LLM-based explanation engine + SIEM + API Gateway + Elasticsearch + SQLite	Real-time interactive enterprise SOC with dashboard	Dependent on log quality and model tuning	End-to-end automated detection, explainable insights, risk scoring, predictive analytics, chat-based interface, and scalable architecture

The dashboards, as shown in Figure 4, provide real-time and historical security insights, including alert severity distribution, risk scores, attack types, MITRE ATT&CK technique mapping, threat timelines, and response metrics, in an intuitive visual format.

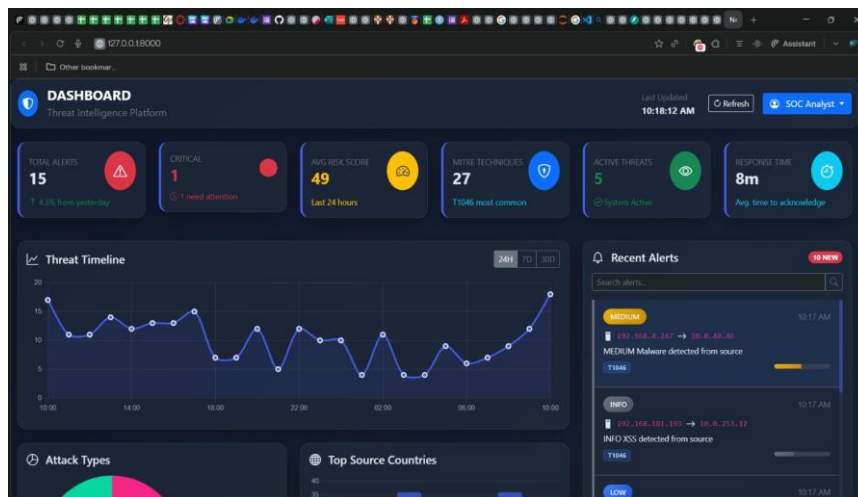


Fig. 4: Dashboard Overview

In this case, the SOC Assistant, through its artificial intelligence technology, flags the Alert ALERT-1006 as a medium-priority event, with a calculated risk score of 48/100 and a confidence level of 46.8%. According to the system's analysis, this activity exhibits characteristics similar to a potential DDoS attack; however, according to the MITRE ATT&CK framework (T1046), it represents a network service scanning activity. Based on this activity's analysis, the source IP address 192.168.4.247 attempted to communicate with the destination IP address 10.0.40.46 via HTTP. An unusual activity is detected in this case because it attempts to access a destination on Port 53, which is commonly associated with DNS. To avoid this potential risk, it is recommended that this source IP address be blocked using firewall rules, authentication logs checked to detect potential unauthorized access, and security policies updated to avoid similar activity in the future [1]-[6], [10]-[15].

5. Conclusion

The AI-Powered SOC Assistant represents an important advancement in modern cybersecurity operations by demonstrating how artificial intelligence and machine learning can improve traditional Security Operations Centre (SOC) processes. Conventional rule-based detection systems often generate numerous alerts and false positives, which can overwhelm analysts and hinder quick responses to real

security incidents. In contrast, the proposed SOC Assistant introduces a more intelligent approach that combines real-time data processing, automated anomaly detection, and natural language interaction. Through its modular design and AI-driven analysis, the system simplifies security monitoring and helps analysts detect and investigate threats more efficiently. One of the most important benefits of the system is its ability to reduce alert fatigue through informed classification and risk-based prioritisation. Alerts are enhanced with third-party threat intelligence and compared against the MITRE ATT&CK framework, which provides organised information on adversaries' tactics. Explanations written using the conversational interface can empower human analysts to make decisions without having to sift through complex queries.

The dashboard, with its graphical elements and chat-based assistant, is flexible enough to accommodate a wide range of organisational needs and the competency levels of analysts. The AI-Powered SOC Assistant would be able to detect zero-day attacks and subtle behavioural anomalies that can evade traditional signature-based methods by relying on machine learning models such as Isolation Forest. Repetitive procedures, such as alert triage, evidence enrichment, etc., can be automated to enable analysts to concentrate on high-level strategic defence organisational and investigative work. Overall, this project demonstrates a scalable, intelligent platform that supports SOC analysts and improves an organisation's security posture. It signifies a move towards a proactive security posture, in which the capabilities of human and machine intelligence are leveraged to protect digital assets in the complex, evolving threat landscape.

The proposed AI-Powered SOC Assistant demonstrates the capabilities of artificial intelligence and machine learning to improve conventional Security Operations Centre (SOC) operations. Conventional systems rely on rule-based approaches to detect security incidents, which often result in false positives and provide limited context for the security analyst, thereby making the overall process more complicated. However, the proposed system demonstrates a more efficient approach to security operations, integrating real-time data analysis and automated anomaly detection with a natural language interface.

Another key feature of the proposed system is the incorporation of explainable artificial intelligence, whereby the overall transparency of the machine learning model and the decision-making process is improved by incorporating contextual information, such as risk scores and MITRE ATT&CK, for each security incident. One of the platform's major characteristics is the dual-dashboard feature, which can boost analyst productivity and improve situational awareness within the SOC environment. The visual dashboard offers a complete view of activity across the systems, including real-time alerts, system health, and security information. It offers information through effective visuals like threat heatmaps, timelines of events, and risk prioritization charts. Analysts can filter information, view individual incidents in detail, and correlate data from multiple sources to create detailed reports for managerial needs or compliance requirements. Moreover, the platform offers a chat-based interface through which the analysts can interact with the system. This interface offers AI-based explanations to the analysts. The interface provides analysts with a step-by-step explanation as they investigate alerts. This interface helps the analysts to effectively explore the alerts, analyze the possible attack scenarios, and understand the response actions. Overall, the visual dashboard and chat-based interfaces provide a streamlined approach for analysts. This approach helps analysts work effectively with automated intelligence. This approach can reduce analysts' response time. This approach can be particularly effective for both junior and senior analysts. By applying the Isolation Forest algorithm, the system can identify previously unseen attack patterns. This approach can be particularly effective, as signature-based security tools may not be able to identify unknown attack patterns.

6. Future Scope

The future of the AI-powered SOC Assistant lies in making it not just an assistant but a predictive security system, making it autonomous.

- SOAR Integration and Autonomous Incident Response:** The second area to look into for future development lies in the move to active threat remediation, as opposed to detection. It would be able to execute complex playbooks on its own, with better integration with Security

Orchestration, Automation, and Response (SOAR). This would allow the system to do real-time containment, e.g. isolating an infected host on the network, resetting compromised credentials, or updating firewall rules in milliseconds. Such a development would change the SOC analyst not only into a manual reactor but also into a strategic manager of an automated, self-recovery of the security structure.

- **Federated Learning and Global Threat Intelligence:** To be ahead of advanced international adversaries, the platform might apply Federated Learning architectures. This would enable AI models to be trained on a variety of data across different organisations simultaneously, without the sensitive data leaving its natural habitat. The assistant could then produce a shared set of collective immune-system code using only the model's learned weights, and before they are even targeted in one sector, they can be identified by all the other connected organisations in total silence, before they are even aware that they are targeted.
- **Zero-Trust Architecture and Continuous Adaptive Risk Assessment:** The SOC Assistant based on AI will be able to become the core intelligence point of the Zero-Trust security system. Rather than relying on fixed authentication techniques, the system might constantly assess user behaviour, device posture, network behaviour, and context-related risk indicators. The assistant would automatically impose micro-segmentation, adaptive access control and least-privilege policies by dynamically recalculating trust scores in real time. This would go a long way toward limiting the flow of information laterally within networks and keeping trust on the table at all times.
- **Adversarial Robustness and Self-Healing Models:** Since cyber attackers are increasingly trying to attack AI systems via adversarial inputs, prompt injection, and data poisoning attacks, future development should focus on model robustness. The SOC Assistant may incorporate adversarial training and model integrity checks on anomalies to identify any attempts at manipulation. Also, self-healing features can enable the system to automatically isolate the compromised models, restore the system to secure checkpoints, and re-train on verified databases. This resilience would ensure continuity of operations even when the AI infrastructure has been targeted.
- **Cybersecurity Digital Twin and Predictive Attack Simulation:** The other direction with promise is the development of a digital twin of the enterprise infrastructure in the field of cybersecurity. This virtual version of the network backdrop can simulate attack conditions, red team activities, and threat distribution paths in a controlled environment. Using predictive analytics and reinforcement learning algorithms, the assistant would be able to identify potential vulnerabilities before exploitation occurs. This would transform the SOC from a reactive attack defence division to a predictive-based security intelligence center.

Acknowledgements

The authors would like to thank the Department of Computer Science and Engineering, Vardhaman College of Engineering, Hyderabad, India, for the support and resources provided throughout this research.

Funding Source

No funding was received for this study.

Conflict of Interest

The authors declare no conflict of interest.

References

- [1] S. R. Sindiramutty, "Autonomous Threat Hunting: A Future Paradigm for AI-Driven Threat Intelligence," arXiv preprint arXiv:2305.01234, 2023.

- [2] M. Uddin, M. S. Irshad, I. Ali, F. Alanazi, F. Ahmed, M. Maaz, S. Hussain, and S. S. Ullah, "Generative AI Revolution in Cybersecurity: A Comprehensive Review of Threat Intelligence and Operations," *Artificial Intelligence Review*, vol. 68, no. 1, pp. 45-62, 2025.
- [3] N. Kshetri, "Transforming Cybersecurity with Agentic AI to Combat Emerging Cyber Threats," *Telecommunications Policy*, vol. 49, no. 4, 2025.
- [4] S. A. Suayyid, M. S. Al-Ghamdi, H. A. Almuhausen, and A. M. Almuhaideb, "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience," *Sensors*, vol. 23, no. 8, pp. 3812-3830, 2023.
- [5] J. Chukwu, "Leveraging the MITRE ATT&CK Framework to Enhance Organizations Cyberthreat Detection Procedures," Carleton University, 2023.
- [6] T. Ali and P. Kostakos, "HuntGPT: Integrating Machine Learning-Based Anomaly Detection and Explainable AI with Large Language Models," *arXiv preprint arXiv:2309.12345*, 2023.
- [7] M. W. Shaukat, R. Amin, M. M. A. Muslam, A. H. Alshehri, and J. Xie, "A Hybrid Approach for Alluring Ads Phishing Attack Detection Using Machine Learning," *Sensors*, vol. 23, no. 12, 2023.
- [8] U. A. Usmani, A. Happonen, and J. Watada, "Human-Centered Artificial Intelligence: Designing for User Empowerment and Ethical Considerations," *IEEE*, 2023.
- [9] A. H. El-Kady, S. Halim, and M. M. El-Halwagi, "Analysis of Safety and Security Challenges and Opportunities Related to Cyber-Physical Systems," *Process Safety and Environmental Protection*, 2023.
- [10] A. Sharma and R. Spunda, "SOC Optimization Through AI-Powered Automation and Blockchain Integration," *ResearchGate*, 2025.
- [11] F. Binbeshr, M. Imam, M. Ghaleb, M. Hamdan, M. A. Rahim, and M. Hammoudeh, "The Rise of Cognitive SOCs: A Systematic Literature Review on AI Approaches," *IEEE Open Journal of the Computer Society*, 2025.
- [12] A. Mohammed, "Artificial Intelligence-Powered Cyber Attacks: Adversarial Machine Learning," *Authorea Preprints*, 2025.
- [13] S. Mukherjee, K. Thapliyal, U. Paul, R. S. Bhandari, A. Sinha, and Y. Sinha, "AI-Powered Threat Intelligence: Enhancing Real-Time Cyber Threat Detection and Response," *IEEE*, 2025.
- [14] A. Spyros, I. Koritsas, A. Papoutsis, P. Panagiotou, D. Chatzakou, D. Kavallieros, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, "AI-Based Holistic Framework for Cyber Threat Intelligence Management," *IEEE Access*, vol. 13, pp. 1245-1260, 2025.
- [15] A. I. Abdulrahman, M. Imam, U. C. Ogor, G. T. Ayodele, C. A. Anadozie, and J. Alebiosu, "AI-Driven Threat Intelligence and Automated Incident Response: Enhancing Cyber Resilience through Predictive Analytics," *Research Journal in Civil, Industrial and Mechanical Engineering*, 2025.