International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

AI-Enabled OSSEC Framework for Power Sector

Prathamesh Pawar[1], Karan Shah[2], Harsh Patil[3], Kailas Devadkar[4], Jignesh Sisodia[5]

[1,2,3]Student, Department of Information Technology, Sardar Patel Institute of Technology
[4,5]Professor, Department of Computer Engineering, Sardar Patel Institute of Technology

Abstract
In the dynamic realm of cybersecurity, where the sophistication of threats continues to escalate, the integration of AI-driven technologies into Security Operations Centers (SOC) presents a groundbreaking paradigm shift. This paper introduces an AI-enabled OSSEC (Open Source SECurity), which amalgamates advanced linguistic capabilities with the foundational core of Security Operations Centers.
Traditional security setups often grapple with the overwhelming influx of data logs, hindering their ability to discern crucial patterns and respond effectively to potential threats. The AI-driven OSSEC addresses this challenge by harnessing natural language processing prowess to efficiently analyze and interpret diverse logs. This innovation not only streamlines the monitoring process but also empowers the system to identify nuanced anomalies that might evade conventional detection mechanisms.
Furthermore, the AI-enabled OSSEC doesn't confine itself to analysis alone; it proactively provides actionable insights and strategies for mitigating identified risks. This proactive approach ensures organizations not only detect potential threats but also respond promptly with well-informed measures. Embracing this technology fortifies cybersecurity posture, enabling Security Operations Centers to navigate the complexities of the digital landscape with unparalleled agility and precision.
This convergence of linguistic intelligence with cybersecurity operations signifies a monumental advancement in building a more resilient and responsive defense against the continuously evolving cyber threat landscape within the power sector.

Keywords: Wazuh, Security Operations Center

1. Introduction

In the ever-evolving landscape of cybersecurity, Security Operations Centers (SOCs) have emerged as critical entities in safeguarding organizations against a relentless surge of cyber threats. Over the past 15 years, the significance of SOCs has grown exponentially, particularly in the last five years, driven by the imperative need to prevent major cyber incidents. The adoption of centralized security operations has become pervasive across businesses, emphasizing the crucial role of SOCs in orchestrating effective defense strategies.
While the popularity of SOCs is undeniable, the existing academic discourse on this subject lacks a cohesive and universally accepted perspective. Previous scholarly works often provide fragmented insights into various aspects of SOCs, hindering the potential for comprehensive innovation. Recognizing

this gap, our paper undertakes a thorough literature survey to consolidate diverse viewpoints, enabling a holistic understanding of the current state-of-the-art in SOCs.

In reviewing the existing literature, we identify primary building blocks that constitute the foundation of contemporary SOCs. However, our investigation reveals a noteworthy gap in the academic research— an inclination towards examining the human and technological facets of SOCs while neglecting the pivotal connection between these elements through specific processes, particularly non-technical processes. Our research aims to address this critical oversight, recognizing the essentiality of synergizing human expertise and technological capabilities within the framework of effective processes to fully unlock the potential of SOCs.

The escalating frequency and severity of information security incidents underscore the imperative need for a robust incident management system within organizations. SOCs, with their ability to rapidly detect incidents, minimize losses, and restore infrastructure, emerge as pivotal components in addressing this pressing need. Our paper delves into the existing literature on SOCs, their missions, and key functions, proposing a classification framework and identifying key indicators for Information Security (IS) incidents in the Internet of Things Infrastructure (IoTI).

As we navigate the multifaceted landscape of cybersecurity frameworks, it is imperative to extend our focus to critical infrastructure sectors. In this context, our research also encompasses the development of a SOC framework tailored specifically for the power sector. Recognizing the unique challenges and requirements of this vital industry, we aim to establish a comprehensive framework that ensures the resilience and security of power sector networks against evolving cyber threats.

2. Architecture

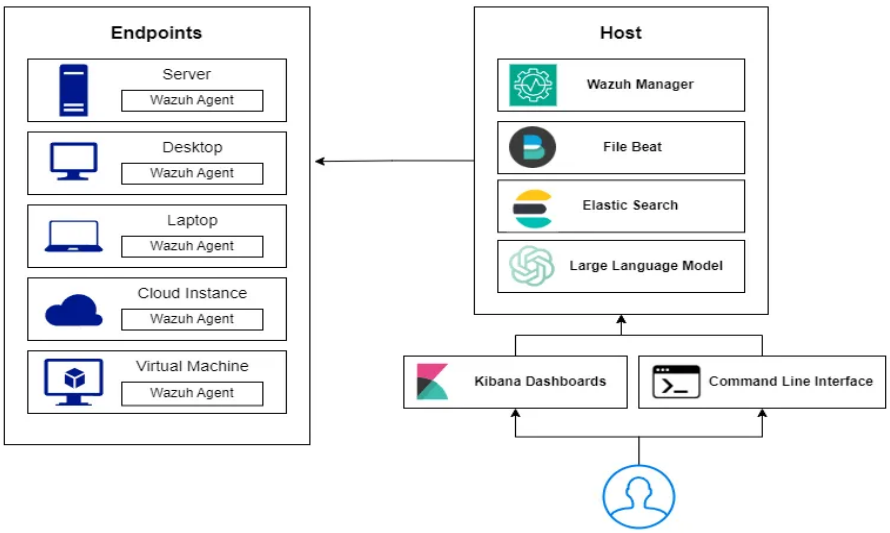

Figure 1 : Architecture

1. Wazuh Integration:

The integration of Wazuh into the Power Sector's infrastructure security landscape is a foundational pillar in fortifying defenses against cyber threats. Wazuh's deployment initiates with the strategic placement of Wazuh agents across critical nodes within the network architecture. These agents serve as vigilant sentinels, meticulously collecting and forwarding logs originating from diverse applications, systems, and devices distributed throughout the infrastructure.

A. Agent Deployment and Log Collection:

Wazuh agents are strategically deployed across critical nodes within the Power Sector's infrastructure, ensuring comprehensive coverage. These agents are configured to monitor and collect logs in real-time, capturing crucial data pertaining to system activities, network traffic, and application behaviors. Through robust log aggregation mechanisms, Wazuh agents efficiently transmit the collected logs to the centralized Wazuh manager for further processing and analysis.

B. Centralized Log Management with Wazuh Manager:

At the heart of the Wazuh framework lies the Wazuh manager, a centralized component orchestrating log management, intrusion detection, and security information and event management (SIEM) functions. The Wazuh manager serves as the nerve center of the security infrastructure, providing security analysts with a holistic view of the threat landscape within the Power Sector. By aggregating and correlating logs from distributed agents, the Wazuh manager enables proactive threat detection, incident response, and forensic analysis, thereby safeguarding critical assets and infrastructure components.

C. Real-time Threat Monitoring and Response:

Leveraging advanced correlation and detection capabilities, the Wazuh manager empowers security analysts to monitor network activities in real-time and respond swiftly to emerging threats. By employing predefined rules, anomaly detection mechanisms, and threat intelligence feeds, Wazuh facilitates the identification of suspicious behaviors, malicious activities, and security incidents across the Power Sector's infrastructure. Through automated alerts, notifications, and remediation workflows, security teams can mitigate risks effectively, ensuring the continuous operation and resilience of essential services.

D. Scalability and Customization:

Wazuh's modular architecture and extensible framework enable seamless scalability and customization to accommodate the dynamic requirements of the Power Sector's infrastructure. Whether scaling across distributed environments, integrating with third-party security solutions, or tailoring detection rules to specific use cases, Wazuh provides the flexibility and agility necessary to adapt to evolving cyber threats and regulatory mandates.

2. AI Integration:

The integration of artificial intelligence (AI) capabilities into the Wazuh framework marks a significant advancement in bolstering the security posture of the Power Sector's infrastructure. Through the Python CLI program, Wazuh seamlessly interfaces with advanced natural language processing (NLP) models, facilitating enhanced log analysis, threat detection, and response strategies.

E. Empowering Advanced Log Analysis:

The synergy between Wazuh's log management capabilities and AI-driven NLP models revolutionizes the process of log analysis within the Power Sector's infrastructure. By leveraging Wazuh APIs, the Python CLI program extracts raw log data from diverse sources across the network, encompassing critical nodes and endpoints. Subsequently, this data is ingested into ChatGPT/Gemini-like models, which excel in contextual understanding and pattern recognition. Through sophisticated analysis techniques, these models dissect log entries, discerning subtle indicators of security incidents, abnormal behaviors, and potential vulnerabilities. This enables security analysts to uncover latent threats, prioritize response efforts, and fortify the resilience of the infrastructure against cyber attacks.

F. Contextual Understanding and Pattern Recognition:

The AI-driven NLP models deployed through the CLI program possess the capacity to grasp contextual nuances embedded within log entries, thereby enhancing the depth and accuracy of security analysis. By

discerning semantic relationships and syntactical patterns, these models decipher complex narratives within log data, enabling the identification of anomalous activities and emerging threat vectors. Through continuous learning and adaptation, the models evolve to recognize evolving attack methodologies and adversarial tactics, empowering security teams with proactive insights and preemptive countermeasures

G. Human-Centric Interface and Decision Support:

The bidirectional communication facilitated by the CLI program between security analysts and AI models transcends traditional log analysis paradigms, offering a natural language interface for interacting with security data. This intuitive interface empowers analysts to pose inquiries, solicit insights, and issue commands in plain language, streamlining the investigative process and facilitating informed decision-making. By bridging the gap between technical log data and human cognition, the AI-enhanced CLI program fosters collaboration, creativity, and agility within the security operations workflow, empowering analysts to devise effective mitigation strategies and respond decisively to security incidents.

3. CLI Program:

The Python CLI program is designed to provide a user-friendly and intuitive interface for security analysts and administrators operating within the Power Sector. It encapsulates several key features that enhance the usability and efficiency of the security framework:

a. **Log Analysis*:*** The CLI program allows users to perform in-depth log analysis, utilizing the capabilities of the integrated Wazuh framework. It assists in identifying potential security threats, abnormal patterns, and anomalous activities within the log data.

b. **Contextual Information Retrieval:** By integrating with ChatGPT/Gemini-like models, the CLI program enhances the contextual understanding of log entries. Analysts can query the system for additional information related to specific logs, gaining insights that go beyond traditional log analysis.

c. **Responsive Querying:** The natural language processing capabilities embedded in the AI models enable security analysts to interact with the system using plain language queries. This responsive querying facilitates real-time investigation and decision-making, allowing for swift and informed responses to security incidents.

4. Wazuh APIs:

The CLI program interfaces with Wazuh's APIs to retrieve recent logs, perform log analysis, and interact with the Wazuh manager. The integration ensures that the AI-enhanced features seamlessly complement the existing functionalities of Wazuh. The CLI program acts as an intelligent layer, enriching the traditional log analysis capabilities with advanced AI-driven insights.

The bidirectional communication between the CLI program, AI models, and Wazuh creates a symbiotic relationship where each component enhances the capabilities of the others. The result is a cohesive and intelligent security framework tailored to the specific needs of the Power Sector.

3. Implementation

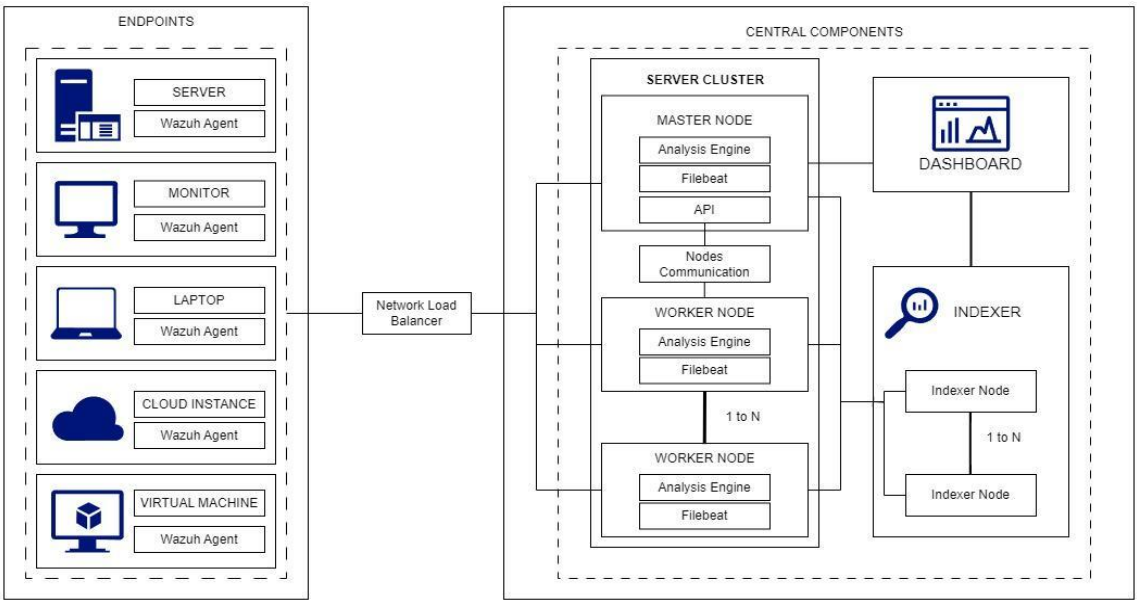

Figure 2 : Implementation

1. **Deployment of Wazuh Agents*:*** The first phase of the implementation process entails the deployment of Wazuh agents across critical nodes within the Power Sector's infrastructure. Leveraging Wazuh's agent-based architecture, agents are strategically installed on endpoints, servers, and network devices to collect and forward logs generated by various applications and systems. Through centralized configuration management and deployment tools, Wazuh agents are deployed seamlessly, ensuring comprehensive coverage and visibility across the infrastructure.
2. **Development of Python CLI Program:** The development of the Python CLI program serves as the conduit for integrating Wazuh's log data with advanced AI capabilities, including GPT-4-All. Built upon Python's robust libraries and frameworks, the CLI program interfaces with Wazuh's APIs to extract relevant log data and facilitate communication with AI-driven NLP models. Leveraging modular design principles and best practices in software engineering, the CLI program offers a user-friendly interface for security analysts and administrators, enabling seamless interaction with security data and AI-driven insights.

   Furthermore, the CLI program integrates GPT-4-All, a state-of-the-art natural language processing (NLP) model, to enhance its capabilities in understanding and generating human-readable responses. Through bidirectional communication with GPT-4-All, security analysts can pose queries, solicit insights, and issue commands in natural language, thereby streamlining the investigative process and facilitating informed decision-making.

   This integration empowers security analysts with a comprehensive toolkit for log analysis, anomaly detection, and real-time response, combining the strengths of Wazuh's log management with the advanced linguistic understanding provided by GPT-4-All. As a result, the Python CLI program serves as a versatile platform for leveraging AI-driven insights to fortify the security posture of the Power Sector's infrastructure against emerging cyber threats and vulnerabilities.
3. **Integration of AI-driven NLP Models:** The integration of AI-driven natural language processing (NLP) models represents a pivotal step in augmenting Wazuh's capabilities with advanced contextual understanding and decision support. Leveraging advanced language models (LLMs), log data

extracted by the CLI program is fed into NLP models for advanced analysis. Through sophisticated pattern recognition algorithms and attention mechanisms, these LLMs decipher complex narratives within log entries, enabling a deeper understanding of the context surrounding security events.

The bidirectional communication between the CLI program and LLMs empowers security analysts with a natural language interface for interacting with security data, facilitating real-time investigation and decision-making. By leveraging LLMs to interpret log entries and identify patterns indicative of security incidents, analysts can uncover latent threats and prioritize response efforts effectively. This integration enables security teams to gain actionable insights from log data, enhancing the overall security posture of the Power Sector's infrastructure

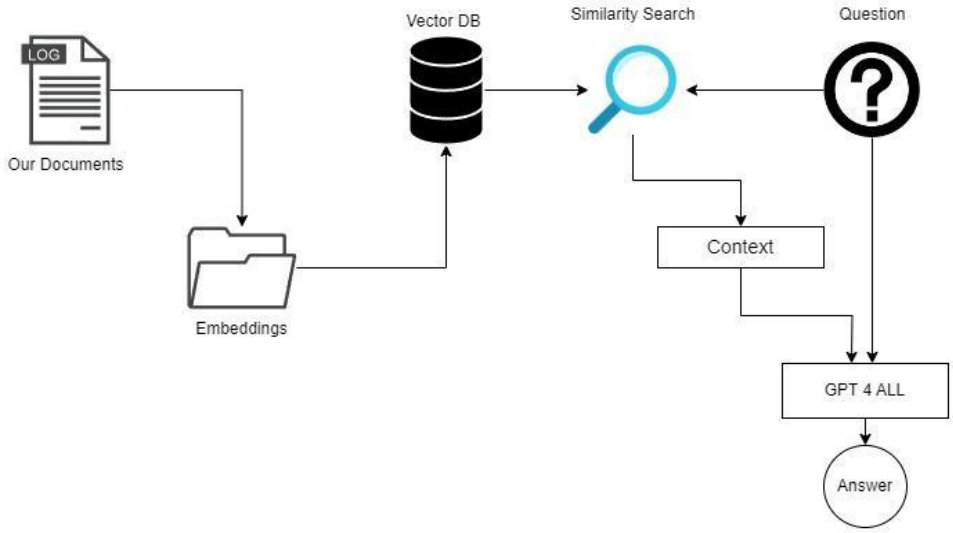

Figure 3 : Flow

.

4. Results

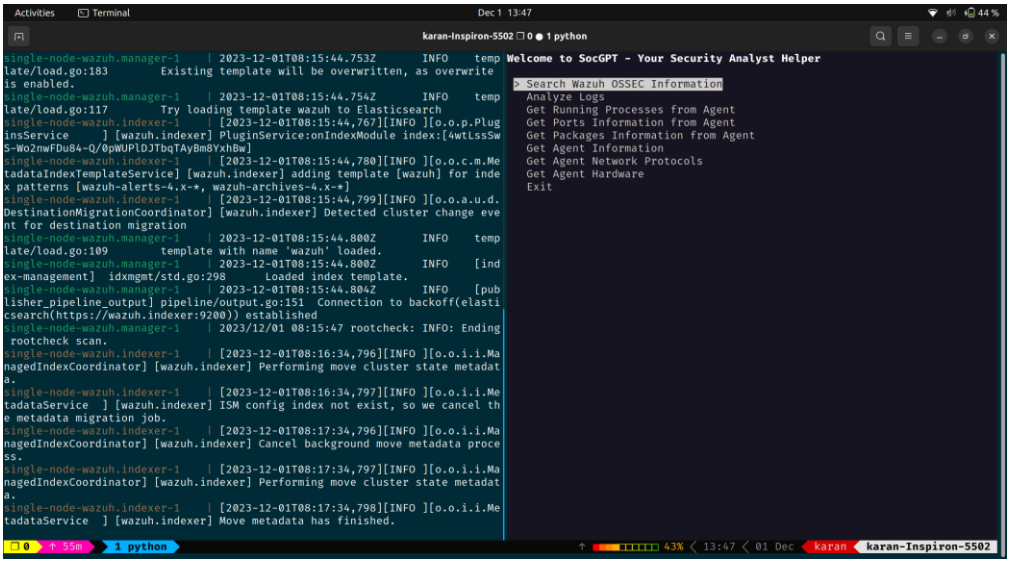

Figure 4 : Console and CLI

The integration of advanced AI capabilities within the Power Sector's infrastructure security framework has yielded significant improvements in log analysis, threat detection, and response orchestration. Key findings include:

1. **Enhanced Log Analysis:** AI-driven natural language processing (NLP) models have enabled deeper contextual understanding of log entries, facilitating more informed decision-making by security analysts.
2. **Proactive Threat Detection*:*** The framework's proactive anomaly detection capabilities have enabled the identification of emerging threats and vulnerabilities, minimizing potential risks to critical assets.
3. **Real-time Decision Support*:*** Bidirectional communication between the AI-enhanced framework and security analysts has facilitated real-time decision support, empowering analysts to orchestrate response actions effectively.
4. **Continuous Improvement:** Iterative refinement processes have ensured the framework's adaptability to evolving threat landscapes and organizational requirements, enhancing its effectiveness over time.

In summary, the integration of advanced AI capabilities has significantly strengthened the security posture of the Power Sector's infrastructure, enabling proactive threat mitigation and agile response strategies.

5. Analysis

The analysis of the integrated framework for enhancing the security posture of the Power Sector's infrastructure reveals key insights into its effectiveness, scalability, and potential impact on cybersecurity operations. This section presents a critical examination of the framework's performance, highlighting its strengths, limitations, and areas for further improvement.

Effectiveness of AI-driven Log Analysis

The AI-driven log analysis capabilities have proven to be highly effective in uncovering subtle indicators of security incidents and anomalous activities within the Power Sector's infrastructure. By leveraging advanced natural language processing (NLP) models, the framework excels in contextual understanding, pattern recognition, and anomaly detection, enabling security analysts to gain deeper insights into the underlying causes and implications of security events. The proactive nature of the framework's anomaly detection capabilities has enabled security teams to identify and mitigate threats in real-time, thereby reducing the risk of potential breaches and minimizing the impact on critical assets and infrastructure components.

Scalability and Adaptability

One of the key strengths of the integrated framework lies in its scalability and adaptability to evolving threat landscapes and organizational requirements. The modular design of the framework allows for seamless integration with existing security infrastructure and tools, facilitating deployment across diverse environments within the Power Sector. Moreover, the iterative refinement processes and continuous learning mechanisms inherent in the framework enable it to adapt to emerging threats, refine detection capabilities, and prioritize response efforts effectively. This scalability and adaptability ensure that the framework remains resilient and effective in safeguarding critical assets against evolving cyber threats and vulnerabilities.

Human-Centric Interface and Usability

The human-centric interface of the framework, facilitated by natural language interfaces and interactive dashboards, enhances usability and accessibility for security analysts and administrators. The integration of AI-driven insights with existing security workflows streamlines incident response processes, enabling swift and decisive action in the face of security incidents. However, there may be challenges associated with the interpretation and validation of AI-generated insights, particularly in complex or ambiguous scenarios. Addressing these challenges through user training, documentation, and collaborative decision-

making processes can enhance the usability and effectiveness of the framework in real-world security operations.

Limitations and Future Directions

Despite its effectiveness, the integrated framework may face certain limitations, including the need for continuous monitoring and refinement to mitigate false positives and ensure the accuracy of AI-driven insights. Furthermore, the integration of AI capabilities may introduce additional complexity and resource requirements, necessitating careful consideration of computational resources and operational constraints. Future research directions may include the exploration of advanced AI techniques, such as reinforcement learning and adversarial training, to enhance the robustness and resilience of the framework against sophisticated cyber threats.

6. Conclusion

In conclusion, the integration of advanced artificial intelligence (AI) capabilities within the Power Sector's infrastructure security framework represents a significant advancement in fortifying the resilience and effectiveness of cybersecurity operations. Through the deployment of a comprehensive framework encompassing Wazuh's log management capabilities, Python CLI program, and AI-driven natural language processing (NLP) models, security analysts and administrators have gained unprecedented insights, agility, and decision support in safeguarding critical assets against emerging cyber threats and vulnerabilities.

The research findings demonstrate the effectiveness of AI-driven log analysis in uncovering subtle indicators of security incidents, proactively detecting anomalies, and facilitating real-time response orchestration. By leveraging advanced NLP models, the framework excels in contextual understanding, pattern recognition, and human-centric interaction, empowering security teams to make informed decisions and prioritize response efforts effectively.

Moreover, the scalability, adaptability, and usability of the integrated framework position it as a promising solution for addressing the evolving cybersecurity challenges faced by the Power Sector. Through iterative refinement processes and continuous learning mechanisms, the framework evolves to reflect changes in the threat landscape, organizational requirements, and technological advancements, ensuring its relevance and effectiveness over time.

While certain limitations and challenges exist, including the need for ongoing monitoring, validation, and refinement of AI-driven insights, the overall impact of the integrated framework on enhancing the security posture of the Power Sector's infrastructure is undeniable. By harnessing the power of AI-driven log analysis, proactive threat detection, and human-centric decision support, the framework empowers security analysts with the tools and capabilities necessary to mitigate risks, respond decisively to security incidents, and uphold the integrity of critical assets and infrastructure components.

In summary, the research underscores the transformative potential of integrating advanced AI capabilities within cybersecurity frameworks, paving the way for more resilient, adaptive, and effective security operations within the Power Sector and beyond. As cyber threats continue to evolve in complexity and sophistication, the integration of AI-driven insights and technologies will play a pivotal role in shaping the future of cybersecurity, safeguarding critical assets, and preserving the integrity of digital ecosystems.

7. Acknowledgement

We are highly grateful to our Project Guides Dr. Kailas Devadkar and Prof. Jignesh Sisodiya, Department

of Information Technology, Sardar Patel Institute of Technology (SPIT) for constant encouragement, effort and guidance. He has always been involved in discussing our topic at each phase to make sure that our approach was designed and carried out in an appropriate manner and that our conclusions were appropriate, given our results.

8. References

1. M. Vielberth, F. Böhm, I. Fichtinger and G. Pernul, “Security Operations Center: A Systematic Study and Open Challenges,” in IEEE Access, vol. 8, pp. 227756-227779, 2020, doi: 10.1109/ACCESS.2020.3045514.
2. I. Choi, J. Lee, T. Kwon, K. Kim, Y. Choi and J.Song, ”An Easy-to-use Framework to Build and Operate AI-based Intrusion Detection for In-situ Monitoring,” 2021 16th Asia Joint Conference on Information Security (AsiaJCIS), Seoul, Korea, Republic of, 2021, pp. 1-8, doi: 10.1109/AsiaJCIS53848.2021.00011.
3. S. Oesch et al., “An Assessment of the Usability of Machine Learning Based Tools for the Security Operations Center,” 2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), Rhodes, Greece, 2020, pp. 634-641, doi:10.1109/iThings-GreenComCPSCom-SmartData-Cybermatics50389.2020.00111.
4. V. S. Rajkumar, A. Stefanov, S. Musunuri and J. de Wit, “EXPLOITING RIPPLE20 TO COMPROMISE POWER GRID CYBER SECURITY AND IMPACT SYSTEM OPERATIONS,” CIRED 2021 - The 26th International Conference and Exhibition on Electricity Distribution, Online Conference, 2021, pp. 3092-3096, doi: 10.1049/icp.2021.2146.
5. S. Yuan and C. Zou, "The security operations center based on correlation analysis," 2011 IEEE 3rd International Conference on Communication Software and Networks, Xi'an, China, 2011, pp. 334-337, doi: 10.1109/ICCSN.2011.6013727.
6. M. Mutemwa, J. Mtsweni and L. Zimba, "Integrating a Security Operations Centre with an Organization’s Existing Procedures, Policies and Information Technology Systems," 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), Mon Tresor, Mauritius, 2018, pp. 1-6, doi: 10.1109/ICONIC.2018.8601251.
7. D. Weissman and A. Jayasumana, "Integrating IoT Monitoring for Security Operation Center," 2020 Global Internet of Things Summit (GIoTS), Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/GIOTS49054.2020.9119680.
8. S. Kowtha, L. A. Nolan and R. A. Daley, "Cyber security operations center characterization model and analysis," 2012 IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 2012, pp. 470-475, doi: 10.1109/THS.2012.6459894.