ICEAIST-24
International Conference on Exploring AI, IOT, Science & Technology-24
ESP Journal of Engineering Technology Advancements / ISSN: 2583-2646

Original Article

Security Information and Event Management (SIEM) Tool

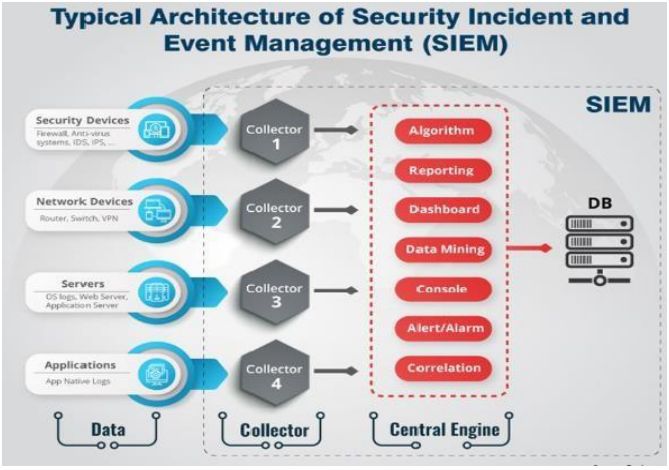
M.Bairoja[1], M. Mohamed Askhan[2], B.Bharathi Vijay[3], P. Tamilselvan[4]
[1,2,3,4]*Computer Science and Engineering, M.A.M. School of Engineering ,Tamilnadu, India.*

Abstract: *Strong and flexible cybersecurity solutions are essential in a time when cyber threats are always growing. The implementation and effectiveness of the SIEM platform – an open-source architecture for threat prevention, detection, and response – are thoroughly examined in this research. The diverse features of SIEM, such as intrusion detection, log data analysis, file integrity monitoring, vulnerability detection, configuration evaluation, incident response, regulatory compliance, cloud security, and container security, are incorporated into the suggested system architecture. Organizations may create a centralized and scalable cybersecurity strategy by combining SIEM agents with the Elastic Stack and deploying them across a variety of IT environments. Tailored threat detection and proactive incident response are made possible by customizing and optimizing SIEM rule sets. The system's resistance to new attacks is further increased via automated response systems. Constant optimization and monitoring guarantee the cybersecurity framework's dependability and effectiveness. This study offers practical insights into the implementation and efficacy of the suggested system design in reducing cyber threats and protecting organizational assets through empirical analysis and testing.*

Keywords: *Cybersecurity, Cyber threats, Incident Response, SIEM, SOC.*

INTRODUCTION

Security analysts depend on a SIEM's assistance to correlate logs and consistently spot any abnormal activity inside their system, enabling them to swiftly respond to threats or attacks. Security Event Management (SEM), which provides real-time monitoring and alerts, and Security Information Management (SIM), which collects log data and events, are combined to form a SIEM. [2] Security Information and Event Management (SIEM) systems have become an essential part of any Security Operations Center (SOC); however, classic SIEMs, which were mainly intended to be log collectors and central alert repositories that do not react to events, are being replaced. [3] Businesses developed "advanced SIEM systems that have evolved to include user and entity behavior analytics (UEBA) and security orchestration, automation, and response (SOAR)" in response to the rising number of cyberattacks." [4]



Given the complexity of most networks, security analysts would require an enormous amount of time without the aid of a SIEM to consistently spot suspicious behaviors by comparing logs between various types of devices. It is uncommon for them to recognize threats to their infrastructures and take timely action to stop any damage from occurring. Additionally, the information gathered can be used in various ways thanks to the SIEM solution. For instance, when a user's account gets locked out, the help desk staff can create a report labeled "failed authentication." The help desk would have needed to ask a system administrator to manually go through logs in order to look for failed login events if there hadn't been a SIEM. Technical issues may be resolved,

capacity can be monitored, and security can be strengthened with this kind of query-based report generation.

OBJECTIVE

This study's main goal is to thoroughly analyze the SIEM platform's suitability and effectiveness in tackling today's cybersecurity issues. This include assessing its efficacy in relation to regulatory compliance, cloud security, containers security, intrusion detection, configuration evaluation, file integrity monitoring, vulnerability detection, and incident response. By means of a methodical analysis of these fundamental features, our objective is to offer discernments regarding the possible advantages and constraints of using SIEM in actual cybersecurity situations.

METHODOLOGY

We use a multifaceted approach that combines theoretical research with real-world experimentation to accomplish our goals. This entails a careful analysis of the body of research on cybersecurity frameworks and techniques in addition to practical experience using the SIEM platform in virtual settings. Through the integration of theoretical understanding and empirical observations, our goal is to present a thorough evaluation of SIEM's efficacy in countering cyber threats and strengthening cybersecurity posture in general.

PROPOSED SYSTEM

The SIEM platform serves as the cornerstone of the proposed system design, which takes advantage of its extensive feature set for threat prevention, detection, and response. The system consists of multiple essential parts and configurations that work together to provide a strong cybersecurity framework that is specifically designed to meet the needs of contemporary businesses. Agents are used to monitor a variety of systems, such as cloud-based workloads, virtualized environments, on-premises servers, and containerized platforms. To guarantee thorough coverage and visibility into the complete IT infrastructure, including endpoints, servers, and network devices, agents are carefully placed. The program gathers security data, which is then collected, aggregated, and analyzed by a centralized management server. The management server is set up to effectively handle high numbers of security events and offers real-time alerting and monitoring. Policies for data storage and retention are put in place to make sure that legal obligations are met and to make forensic analysis easier. To improve data visualization and analysis capabilities, the SIEM platform is seamlessly linked with the Elastic Stack, which includes Elasticsearch, Logstash, and Kibana. In order to provide quick and effective search queries, Elasticsearch acts as the backend data store for indexing and storing security events. For data ingestion, parsing, and enrichment, Logstash is employed, guaranteeing interoperability with a range of data sources and formats. With Kibana's intuitive dashboard, reporting, and data visualization interface, security analysts can easily extract actionable insights from the security data they've gathered.

CONCLUSION

The appropriate answer to meet the demands of El Dorado County was not readily apparent. Every solution has advantages and disadvantages based on the investigation, evaluation, and testing of the various options. To compile the final report card, I integrated the Gartner use case score, critical capability ratings, and the scores based on each solution's functionality, simplicity of use, and compatibility as part of my evaluation matrix.

REFERENCES

[1] D. Fouse, "Cybercrime Is On The Rise: How Communications Can Help State And CityGovernments," Forbes, 29 June 2020. [Online]. Available: Forbes (https://www.forbes.com/sites/forbesagencycouncil/2020/06/29/cybercrime-is-on-the- risehow-communications-can-help-state-and-city-governments/?sh=7eba13d8501e).

[2] Venkata Sathya Kumar Koppisetti, 2024. "*Robotic Process Automation: Streamlining Operations in the Digital Era*" *ESP International Journal of Advancements in Computational Technology (ESP-IJACT)* Volume 2, Issue 2: 74-81.

[3] EC-Council, "WHAT IS SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM)?," 19 May 2020. [Online]. Available: EC-Council (https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/).

[4] Palo Alto Networks, "XDR: Extended Detection and Response," Palo Alto Networks,2020.

[5] Sumanth Tatineni, Anirudh Mustyala, 2024. "*Leveraging AI for Predictive Upkeep: Optimizing Operational Efficiency*" *ESP International Journal of Advancements in Computational Technology (ESP-IJACT)* Volume 2, Issue 1: 66-79.

[6] M. Rouse, "security information and event management (SIEM)," February 2020. [Online]. Available: Tech Target (searchsecurity.techtarget.com/definition/security- information-and-event-management-SIEM).

[7] Sridhar Selvaraj, 2024. "*Futuristic SAP Fiori Dominance*" *ESP International Journal of Advancements in Computational Technology (ESP-IJACT)* Volume 2, Issue 1: 32-37. | Google Scholar

[8] LogRhythm, "Security Information and Event," 2021. [Online]. Available: LogRhythm (https://logrhythm.com/solutions/security/siem/).

[9] Chanthati, Sasibhushan Rao. (2021). How the Power of Machine – Machine Learning, Data Science and NLP Can Be Used to Prevent Spoofing and Reduce Financial Risks. 10.13140/RG.2.2.18761.76640.

[10] Gartner, "Gartner Magic Quadrant," [Online]. Available: Gartner (https://www.gartner.com/en/research/magic quadrant).

[11] Muthukumaran Vaithianathan, Mahesh Patil, Shunyee Frank Ng, 2024. "*Comparative Study of FPGA and GPU for High-Performance Computing and AI*" *ESP International Journal of Advancements in Computational Technology (ESP-IJACT)* Volume 2, Issue 2: 114-124.

[12] Solutions Review, "SIEM Vendor Map," Solutions Review, Woburn, 2021.

[13] ArcSight, "ArcSight's Latest and Greatest," 2020. [Online]. Available: ArcSight (https://www.microfocus.com/media/article/arcsights-latest-and-greatest-article.pdf).

[14] IBM, "IBM QRadar SIEM," IBM, Somers, 2019.

[15] Kushal Walia, "Exploring the Challenges of Serverless Computing in Training Large Language Models," International Journal of Computer Trends and Technology, vol. 72, no. 4, pp. 71-76, 2024. Crossref, https://doi.org/10.14445/22312803/IJCTT-V72I4P109

[16] LogRhythm, "Be Security First," 2021.

[17] Gartner, "Critical Capabilities for Security Information and Event Management," 2020.

[18] Gartner, "Magic Quadrant for Security Information and Event Management," 2020.

[19] LogRhythm, "LogRhythm NextGen SIEM Platform," 2021. [Online]. Available: LogRhythm (https://logrhythm.com/products/nextgen-siem-platform/).

[20] Naresh Kumar Miryala, Divit Gupta, "Big Data Analytics in Cloud – Comparative Study," *International Journal of Computer Trends and Technology*, vol. 71, no. 12, pp. 30-34, 2023. Crossref, https://doi.org/10.14445/22312803/IJCTT-V71I12P107

[21] Splunk, "Splunk Fundamentals 1," [Online]. Available: Splunk (https://www.splunk.com/en_us/training/free-courses/splunk-fundamentals-1.html).

[22] Palo Alto Networks, "Cortex XDR 2.0 Demo," Palo Alto Networks, 13 January 2020. [Online]. Available: Palo Alto Networks (https://www.paloaltonetworks.com/resources/demos/cortex-xdr-2-0-demo).

[23] Elastic Co, "Elastic," [Online]. Available: demo.elastic.co.

[24] Naga Ramesh Palakurti, 2023. "*Evolving Drug Discovery: Artificial Intelligence and Machine Learning's Impact in Pharmaceutical Research*" *ESP Journal of Engineering & Technology Advancements* 3(3): 136-147. [Link]

[25] Naga Ramesh Palakurti, 2022. "*AI Applications in Food Safety and Quality Control*" ESP Journal of Engineering & Technology Advancements 2(3): 48-61. [Link]

[26] Chanthati, S. R. (2024). An automated process in building organic branding opportunity, budget Intensity, recommendation in seasons with Google trends data. Sasibhushan Rao Chanthati. https://doi.org/10.30574/wjaets.2024.12.2.0326

[27] Kumar Shukla, Nimeshkumar Patel, Hirenkumar Mistry, 2024." *Securing The Cloud: Strategies and Innovations In Network Security For Modern Computing Environments"* Volume 11, Issue 04 pp. 1786-1796. [Link]

[28] Muthukumaran Vaithianathan, Mahesh Patil, Shunyee Frank Ng, Shiv Udkar, 2024. "*Verification of Low-Power Semiconductor Designs Using UVM*", *ESP Journal of Engineering & Technology Advancements* 4(3): 28-44.

[29] Doctor, A., B. Vondenbusch, and J. Kozak. "Bone segmentation applying rigid bone position and triple shadow check method based on RF data." Acta of Bioengineering and Biomechanics, 13.2 (2011): 3-11.

[30] Jaseem Pookandy, Enhancing Customer Relationship Management with Salesforce: A Comprehensive Review, International Journal of Computer Engineering and Technology (IJCET), 15(4), 2024, pp. 64-84

[31] Muthukumaran Vaithianathan, Mahesh Patil, Shunyee Frank Ng, Shiv Udkar, 2024. "*Energy-Efficient FPGA Design for Wearable and Implantable Devices*" *ESP International Journal of Advancements in Science & Technology (ESP-IJAST)* Volume 2, Issue 2: 37-51.

[32] Julian, Anitha , Mary, Gerardine Immaculate , Selvi, S. , Rele, Mayur & Vaithianathan, Muthukumaran (2024) Blockchain based solutions for privacy-preserving authentication and authorization in networks, *Journal of Discrete Mathematical Sciences and Cryptography*, 27:2-B, 797–808, DOI: 10.47974/JDMSC-1956

[33] Muthukumaran Vaithianathan, 2024. "Digital Signal Processing for Noise Suppression in Voice Signals", IJCSPUB - INTERNATIONAL JOURNAL OF CURRENT SCIENCE (www.IJCSPUB.org), ISSN: 2250-1770, Vol.14, Issue 2, page no.72-80, April-2024, Available: https://rjpn.org/IJCSPUB/papers/IJCSP24B1010.pdf

[34] Muthukumaran Vaithianathan, "Real-Time Object Detection and Recognition in FPGA-Based Autonomous Driving Systems," *International Journal of Computer Trends and Technology*, vol. 72, no. 4, pp. 145-152, 2024. Crossref, https://doi.org/10.14445/22312803/IJCTT-V72I4P119

[35] Muthukumaran Vaithianathan, Mahesh Patil, Shunyee Frank Ng, Shiv Udkar, 2023. "*Comparative Study of FPGA and GPU for High-Performance Computing and AI*" *ESP International Journal of Advancements in Computational Technology (ESP-IJACT)* Volume 1, Issue 1: 37-46. [PDF]

[36] Muthukumaran Vaithianathan, Mahesh Patil, Shunyee Frank Ng, Shiv Udkar, 2024. "*Low-Power FPGA Design Techniques for Next-Generation Mobile Devices*" *ESP International Journal of Advancements in Computational Technology (ESP-IJACT)* Volume 2, Issue 2: 82-93. [PDF]

[37] Dhamotharan Seenivasan, Muthukumaran Vaithianathan, 2023. "*Real-Time Adaptation: Change Data Capture in Modern Computer Architecture*" ESP International Journal of Advancements in Computational Technology (ESP-IJACT) Volume 1, Issue 2: 49-61. [PDF]
[38] Muthukumaran Vaithianathan, Mahesh Patil, Shunyee Frank Ng, Shiv Udkar, 2024. "*Integrating AI and Machine Learning with UVM in Semiconductor Design*" ESP International Journal of Advancements in Computational Technology (ESP-IJACT) Volume 2, Issue 3: 37-51. [PDF]
[39] Chanthati, Sasibhushan Rao. (2021*). A segmented approach to encouragement of entrepreneurship using data science.* World Journal of Advanced Engineering Technology and Sciences. https://doi.org/10.30574/wjaets.2024.12.2.0330, [link]
[40] Patel, N. (2024, March). SECURE ACCESS SERVICE EDGE(SASE): "EVALUATING THE IMPACT OF CONVEREGED NETWORK SECURITYARCHITECTURES IN CLOUD COMPUTING." Journal of Emerging Technologies and Innovative Research. https://www.jetir.org/papers/JETIR2403481.pdf
[41] Vishwanath Gojanur , Aparna Bhat, "Wireless Personal Health Monitoring System", IJETCAS:International Journal of Emerging Technologies in Computational and Applied Sciences,eISSN: 2279-0055,pISSN: 2279-0047, 2014. [Link]
[42] Mistry, H., Shukla, K., & Patel, N. (2024). Transforming Incident Responses, Automating Security Measures, and Revolutionizing Defence Strategies throughAI-Powered Cybersecurity. Journal of Emerging Technologies and Innovative Research, 11(3), 25. https://www.jetir.org/
[43] Aparna Bhat, "Comparison of Clustering Algorithms and Clustering Protocols in Heterogeneous Wireless Sensor Networks: A Survey," 2014 INTERNATIONAL JOURNAL OF SCIENTIFIC PROGRESS AND RESEARCH (IJSPR)-ISSN : 2349-4689 Volume 04- NO.1, 2014. [Link]
[44] Shashikant Tank Kumar Mahendrabhai Shukla, Nimeshkumar Patel, Veeral Patel, 2024." AI BASED CYBER SECURITY DATA ANALYTIC DEVICE", 414425-001, [Link]
[45] Aparna Bhat, Rajeshwari Hegde, "Comprehensive Study of Renewable Energy Resources and Present Scenario in India," 2015 IEEE International Conference on Engineering and Technology (ICETECH), Coimbatore, TN, India, 2015. [Link]
[46] Sarangkumar Radadia Kumar Mahendrabhai Shukla ,Nimeshkumar Patel ,Hirenkumar Mistry,Keyur Dodiya 2024." CYBER SECURITY DETECTING AND ALERTING DEVICE", 412409-001, [Link]
[47] Aparna K Bhat, Rajeshwari Hegde, 2014. "Comprehensive Analysis Of Acoustic Echo Cancellation Algorithms On DSP Processor", International Journal of Advance Computational Engineering and Networking (IJACEN), volume 2, Issue 9, pp.6-11. [Link]
[48] Nimeshkumar Patel, 2022." QUANTUM CRYPTOGRAPHY IN HEALTHCARE INFORMATION SYSTEMS: ENHANCING SECURITY IN MEDICAL DATA STORAGE AND COMMUNICATION", Journal of Emerging Technologies and Innovative Research, volume 9, issue 8, pp.g193-g202. [Link]
[49] Bhat, A., & Gojanur, V. (2015). Evolution Of 4g: A Study. International Journal of Innovative Research in ComputerScience & Engineering (IJIRCSE). Booth, K. (2020, December 4). How 5G is breaking new ground in the construction industry. BDC Magazine.https://bdcmagazine.com/2020/12/how-5g-is-breaking-new-ground-in-the-constructionindustry/. [Link]
[50] Nimeshkumar Patel, 2021." SUSTAINABLE SMART CITIES: LEVERAGING IOT AND DATA ANALYTICS FOR ENERGY EFFICIENCY AND URBAN DEVELOPMENT", Journal of Emerging Technologies and Innovative Research, volume 8, Issue 3, pp.313-319. [Link]
[51] Bhat, A., Gojanur, V., & Hegde, R. (2014). 5G evolution and need: A study. In International conference on electrical, electronics, signals, communication and optimization (EESCO)—2015.[Link]
[52] A. Bhat, V. Gojanur, and R. Hegde. 2015. 4G protocol and architecture for BYOD over Cloud Computing. In Communications and Signal Processing (ICCSP), 2015 International Conference on. 0308-0313. Google Scholar. [Link]