International Research Journal of Innovations in Engineering and Technology(IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 299-306, November-2023

https://doi.org/10.47001/IRJIET/2023.711041

Security Operation Center for Healthcare Sector

[1]Abeysinghe A.M.S.B., [2]De Zoysa M.T.R., [3]Samuditha K.M.Y., [4]Dissanayake D.J.D.H.T., [5]Kanishka Yapa [6]Uditha Dharmkeerthi

[1,2,3,4,5,6]Faculty of Computing, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka

Authors E-mail: [1]it20146542@my.sliit.lk, [2]it20200138@my.sliit.lk, [3]it20204266@my.sliit.lk, [4]it20255138@my.sliit.lk, [5]kanishka.y@sliit.lk, [6]uditha.d@sliit.lk

***Abstract* - The rapid rise of cybersecurity threats has led to the development of advanced security operations centers (SOCs) that can identify and respond to cyber-attacks in real-time. This research aims to design and implement a next-generation automated SOC using an automated ELK stack, threat hunting, intelligence, MITRE attack framework, and HIPAA compliance. The system will be evaluated using real-world scenarios to assess its effectiveness in enhancing SOC operations and threat identification. The study predicts that the next-generation automated SOC with an ELK stack will significantly improve cybersecurity operations by providing real-time network activity visibility, identifying, and analyzing threats, and automating response activities. The findings will emphasize the importance of incorporating new technologies into SOC operations and the need for continuous monitoring and enhancement. The study recommends further research into the integration of the ELK stack into automated SOC operations for better threat identification and response.**

Keywords: ELK, SOC, Kibana, Logstash, Automated MITRE Attack, Automated Threat Hunting, Automated Threat Intelligence, HIPAA Compliance, RBAC (Role Based Access Control), Machine Learning.

I. INTRODUCTION

Cybercriminals often focus their attention on healthcare providers and related institutions. The continuum of care results in a landscape that is convoluted and diverse in terms of the individuals, devices, apps, and procedures that comprise it. This landscape provides potential entry points for attackers into the network. A further tactic that attackers might use to carry out ransomware attacks is to threaten the interruption of essential life-saving utilities. The culmination of all these actions produces data that may be put to use to trace down attackers and stop them in their path. Indicators of data breach may be found across all sectors, but healthcare organizations want high-quality data that is tailored to their operating conditions in order to cut down on the amount of time it takes to discover and react to threats. Due to the sensitive nature of patient data, the healthcare business is a top target for the perpetration of cyberattacks. It is possible for patients, healthcare professionals, and healthcare organizations to face serious repercussions as a result of the theft, loss, or improper use of sensitive information. As a result, it is essential to have an efficient cybersecurity plan in order to safeguard patient data and stay in compliance with HIPAA regulations. An automated SOC can identify and react to potential dangers in real time, making it possible to take a complete and preventative approach to information security. The manual SOC technique that has been used in the past is no longer adequate due to the growing number of cyber threats and their increased complexity. An automated Security Operations Center (SOC) can analyze vast amounts of data, identify trends, and detect dangers that human analysts may overlook. This advantage over traditional SOCs allows for automation of mundane tasks like patch management, vulnerability scanning, and incident response, freeing security analysts to focus on more important responsibilities.

This leads to enhanced efficiency and efficacy in threat detection and response, reducing the risk of cyberattacks and data breaches. An automated SOC plays a crucial role in protecting patient data and maintaining HIPAA compliance. It enables real-time detection and response to cyber threats, minimizing the risk of data breaches and cyber assaults. Additionally, an automated SOC can help healthcare companies lower the cost of cybersecurity operations by automating mundane operations and combining threat intelligence, vulnerability management, and compliance management. This integration helps identify potential security concerns before they become a threat, minimizing the probability of data breaches and cyber assaults. The healthcare sector is increasingly targeted by sophisticated and persistent cyber-attacks, making the need for an automated SOC even more crucial. Advanced capabilities of automated SOC solutions, such as machine learning and artificial intelligence, can help organizations identify and respond proactively to complex threats. Overall, healthcare institutions must have an automated SOC to safeguard patient information and maintain HIPAA compliance. The healthcare industry requires an automated Security Operations Center (SOC) to identify vulnerabilities and weaknesses in defense mechanisms. The MITRE Attack framework enables SOC to conduct simulations of real-world attack scenarios, maintaining a

