Security Operations and Automation Platform Architecture for Healthcare

Yusuf A.S
New York Institute of Technology
College of Engineering and Computer Science
Brooklyn, USA

Fatoye O.E
Leadcity University
Computer and Information Science
Ibadan, Nigeria

Ayinde A.Q
Northcentral University
School of Technology
Arizona, USA

Omotunde O.I
Ladoke Akintola University of Technology
Department of Agronomy
Ogbomosho, Nigeria

***Abstract*— Some hospitals have a centralized security operation team that monitors, tracks, and analyzes event data to detect threats and prevent attack actors from taking advantage of any vulnerabilities within their network infrastructure. Hospitals must adopt a high-level multi-functional SOAPA system architecture to conduct incidents investigation by tracking the sources of the incidents. It is important to conduct a risk assessment plan by analyzing the event data stored in the hospital repositories, either on-premises or cloud.**

The security operating center (SOC) will leverage the visual analytic feature of the SOC dashboard to monitor threat patterns using the analyzed event data from all the data sources to track changes in the infrastructural activities. The SOC team will monitor and evaluate the growth in the network traffic-based bandwidth usage for all inventoried assets and data flow activities across the network. Also, an appropriate data management system must be adopted to prevent data loss when data is migrated into a machine learning platform that can detect and prevent cyber-attacks in real time.

Keywords—Cyber attacks; cybersecurity; architecture; incident; machine learning.

I. INTRODUCTION

A high-level multi-functional security and automation platform architecture (SOAPA) design can be adopted by the hospital to ensure that a robust cybersecurity solution is deployed across their network to prevent, detect and alert the security stakeholders within the hospital network should any incident occurs when monitoring the data flow and during the event data analysis using the architectural framework of the SOAPA. The architecture is divided into three main blocks, namely, the data services functions, the security operations functions, and the user interfaces section, as shown in figure 1. A centralized database management system is developed as the data house of the SOAPA system, and the data are pulled from various data repositories (on-premises and cloud). These data come from data generated within the hospital network internally and from the external devices light internet of things (IoT), internet of medical thing (IoMT), and bring your own device (BYOD) that are either accessing the hospital assets or populating hospital databases based on the operations virtualization and digitalization of business operations.

II. THE SYSTEM ARCHITECTURE

A high-level multi-functional Security Operations and Automation Platform Architecture (SOAPA) will be designed for hospital operations. This architecture is divided into three blocks: data services, security operations, and User Interface Management Station. These three blocks can be connected to design a robust system that can ensure the processing and resolution of incidents using the event data from the organization repositories.

At the data services function, the function is layered to work based on a handshake concept to ensure that event data are analyzed and broken down into a digestible insight before they are passed to the security operations functions. The topmost layer of the data services functions is the data storage platform. The data storage platform used by most hospitals is the on-premises, cloud, and data from applications running on the hospital network infrastructure. These data include database logs, application logs, and Internet of Medical Things log data. The data storage platform identified the historical data from all the data repositories within and outside the hospital network. This historical data is stored in a separate location, and the data migration activities from the data repositories to the historical data mart are monitored by a data loss prevention service known as DLP to ensure the quality of the stored data is maintained. A security log configuration is enabled to ensure that the data is secured before it is moved into a centralized database management system (DBMS) that the security operation center has adopted as the main data repository that will be used in analyzing all events data in the organization. As an iterative process, the DLP must monitor the DBMS to ensure that no data is lost during the data migration process from the historical data mart to the DBMS. The response from the security logs that act as the security agent for the data services functions is configured to send real-time alerts and notifications to the SOC team should an error during the migration or incident are detected. Before the data is moved to the DBMS, the data is scanned for vulnerabilities using probes, network analyzers, and industry-approved scanners. Alerts and notifications are sent to the centralized dashboard at the SOC so that the security team can rectify the issue to ensure that only quality data can be migrated to the security operations functions. The topmost layer of the security operations functions captures some security operation techniques or functions that the hospital can adopt. In this paper, the Security and Incident Event Management (SIEM) system and the Security Orchestration, Automation, and Response (SOAR) are the functions that will be considered and recommended for a hospital to ensure that the SOAPA system responds efficiently and effectively to tasks and focus on detecting incident from the event data housed in the centralized DBMS (Oltsik, 2019). The Security and Incident Event Management (SIEM) system and the Security Orchestration, Automation, and Response (SOAR) are configured to reduce the mean time to respond (MTTR), mean time to detect (MTTD), and ultimately the time to investigate (TTI) which is the driven force for the incident response investigations based on the data from the centralized DBMS.

The SOAPA architectural system designed for a hospital is composed of an integration layer, security operation platform, and analytic layer that will allow the system to work efficiently and effectively so that the SOC team can monitor the collaborations between the security operations team and security stakeholders with the integration of technologies and processes that can be adopted to enhance data security and protection within the hospital network [2].

The SOAPA used a distributed data service layer as a key component of the SOAPA with integrated security operations, automation, and orchestrations to evaluate, mitigate and prevent risks to improve the performance of the SOAPA system and the efficiency of the SOC team in response to incidents [3]. The SOAPA is a bottom-up architecture that gives the SOC team the flexibility to collect, process, and allocates the data from the DBMS to the right tools at the right time. The cybersecurity analytics functions are enabled in the analytics layer to analyze the event data, manage it and report the analyzed data to the host of technologies integrated into the SOAPA system design. The SOAPA allows the statistical models from SOAR to be used in analyzing indicators that can serve as a key performance index for the SOC team in analyzing data. The SOAR can be used to provide an insight from the dataset in DBMS and can be used to improve threat detection, prevention, and response [4]. The SOAR solution adopted by the SOC team forms that of the security operations within the SAOPA. The security platform layer monitors the security operations to conduct investigations and orchestrate disparate tools to create a workflow that is usable by the system to analyze data from the DBMS. This process can be automated to remediate the triggered actions as a result of the threats or incidents that were detected by the SOAPA system. The SOC team should leverage the capabilities of SOAR and SIEM in analyzing historical log data that are extracted from the application, system, and database log data.

While SIEM has a robust security solution that can prevent and detect cyber security attacks, it is important that hybridizing SIEM with the SOAR solution will improve the performance of the SOAPA system when the system is fully optimized. The SOAPA is an automated solution that is potent in data gathering, data investigation, preventing cyber threats, detecting attacks, provide adequate data management systems, among others [5]. The SOAPA enables the integration of advanced analytics with security operations management to improve the organization's security plan from the data service function layer to the threat detection using the incident response from the analyzed event data. The SOAPA analytics has an in-built engine that can be adopted to identify the problems defined or pre-defined by the SOC team. The automation and orchestration layer of the SOAPA can be used to develop an automated tool that can be used to monitor important security activities such as indicator enrichment, alert and notification triage, threat intelligence collection, incident response, and reporting via the SOC centralized dashboard [6]. The user interface is the centralized location where the SOC team will monitor and receive alerts and notifications for any incident detected by the SOAPA system. Also, the centralized dashboard deployed at the SOC will be configured to track indicators that will be intuitive by the soc team in analyzing the network security of the hospital in real time. This dashboard can also be used in sending visual analytic reports (incident reports to the security stakeholders and the leadership of the hospital) and will be an appropriate tool in incident case management.

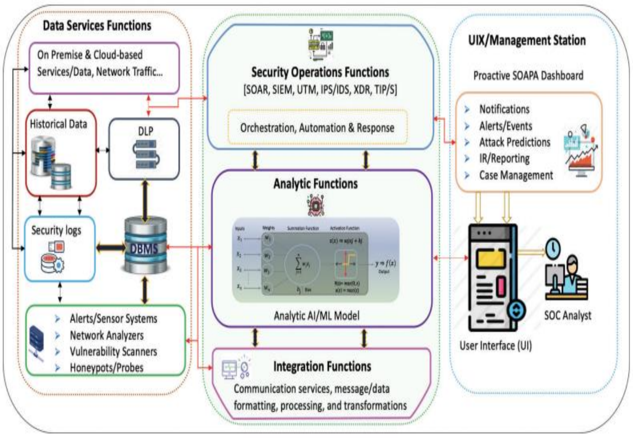

Figure 1: Multi- Functional SOAPA System

III. INTEGRATION OF MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE IN SOAPA SYSTEM

Due to the exponential growth in health data, Big Data Cybersecurity Analytics can be leveraged by using this data in training the machine learning algorithms to detect patterns in threat when analyzing event data from the DBMS discussed in the paragraphs above. Numerous SOAR solutions can be integrated into the SOAR solutions to ensure the effective and high performance of the SOAPA system design for the hospital. Before hospital can choose the vendor to provide the SOAR solution, it is essential to review the level of orchestration by considering the framework that supports the orchestration capability identified by the SOC team. In this paper, three (FireEye, IBM Resilient, and Rapid7) different SOAR solutions from different vendors were considered, and the application to the architectural design and integration to the SOAPA system will be discussed. FireEye implemented a machine learning-driven PowerShell detection engine that detects and prevents PowerShell attacks and detects malware and penetration test activities [1]. The IBM Resilient captured prioritization, incident categorization, and event data analysis. The machine learning model selected by the SOC team is used in training the algorithms selected by the SOC team in analyzing the historical data in predict time to resolve new incidents and detect familiar incidents that have been rectified in the past[10] This solution can be used in clustering and classifying threat patterns based on the incident attributes, as the SOAPA system is detecting more attacks. The solution can also be used with artificial intelligence to support intelligence functions such as incident triage [7]. The third solution that was investigated is the Rapid7 SOAR solution known as Insight Connect, and its corresponding SIEM solution is known as InsightIDR [8]. The SOC team applies the InsigntConnect SOAR to optimize operations using a library of more than 200 plug-ins and a visual analytic workflow builder. This solution provides correlation and threat detection rules, threat actor behavior analytics, compliance dashboard, log management, and machine learning that can be integrated into the SOAPA workflow. This solution combines human input and machine learning to detect and prevent attacks in real-time, and context will be generated as feedback to the SOC team about the user and adversary for immediate response incident response. This solution used machine learning and advanced analytics to analyze event data that can be automated to rapidly detect threats coming from virtualized or cloud environments [9].

IV. CONCLUSION

The SOAPA system design is divided into three main blocks (data services functions, security operations functions, and user interface Station). The data services functions are responsible for data generation, data aggregation, data protection, and data storage capabilities [11], [12], SOAPA carries out the orchestration, automation, and response task and focuses on incident response operations to detect, classify, and address threats detected by SOAPA systems to create actionable alerts or intelligence. The data services functions are responsible for pulling data from all the data sources to the organization-monitored DBMS that is monitored using the DLP and security logs in generating both false and real alerts so that the SOC team can be swift in responding to data migration from the source platform to the DBMS that will be used in analyzing the organization incidents or threats. The Security Operation Function is based on the orchestration, automation, and response to incidents. The SOAR and SIEM platforms were integrated into the SOAPA solution to conduct some analytic functions using machine learning and artificial intelligence features to train the SOAPA in detecting and preventing cyber threats in real time. Three solutions of the SOAR were evaluated based on their performance and capabilities, which can analyze the CHN data in their repositories to improve their network security and quality of service to their numerous customers. The alerts and notifications will be monitored by the SOC team using the centralized dashboard deployed in their location to track, monitor, detect, prevent and analyze the network security using the network vulnerability scanner and some other appropriate tools.

REFERENCE

[1] FireEye, (2020). “Security orchestrator: simplify threat response through integration and automation,” 2020. [Online]. Available: https://www.fireeye.com/solutions/security-orchestrator.html.

[2] Kinyua, J., & Lawrence, A. (2021). “AI/ML in Security Orchestration, Automation and Response: Future Research Directions.” *Intelligent Automation & Soft Computing 28*(2): 527–45.

[3] Laliberte, B. (2019) “The importance of a common distributed data services layer,” 2019. [Online]. Available: https:// www.esg-global.com/research/esg-brief-the-importance-of-a-common-distributed-data-services-layer

[4] Oltsik, J. (2020). “SOAPA: Unifying SIEM and SOAR with IBM security QRadar and IBM security resilient,” 2020. [Online]. Available: https://www.ibm.com/security/digital-assets/resilient/unifying-siem-and-soar-with-soapa/.

[5] Oltsik, J. (2019). “Devo: A modern security operations and analytics platform,” 2019. [Online]. Available: https://www. devo.com/soapa/.

[6] Oltsik, J. (2019). “SOAPA vs. SOAR: How these security terms differ,” 2019. [Online]. Available: https://www.csoonline.com.

[7] Palo Alto Networks, (2019). “Completes acquisition of Demisto, Palo Alto Networks,” 2019. [Online]. Available: https:// www.paloaltonetworks.com.

[8] Rapid 7, (2020). “Catching modern threats: InsightIDR detection methodologies,” 2020. [Online]. Available: https:// www.rapid7.com/resources

[9] ServiceNow, (2018). “ServiceNow security operations,” 2018. [Online].Available:https://www.servicenow.com/ products/predictive-intelligence.html.

[10] Nwagwu U , Ayinde A.Q , Olasoji, Y.(2021). Application of Instance Learning Algorithms to Analyze Logistics Data, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 10, Issue 07 (July 2021),

[11] Nwagwu, U. (2020). *A SWOT analysis on the use of blockchain in supply chains* (Doctoral dissertation, Wichita State University).

[12] Nwagwu U, Ayinde A.Q, Isolagbenla K.O, Yusuf A.S (2021) Pattern Mining of Hospitalization Data of Covid-19 Patients with Underlying Conditions, International Journal of Engineering Research and Technology (IJERT), Volume 11.