Phoenix: International Multidisciplinary Research Journal
Vol 1, No. 3, July-Sep, 2021
ISSN: 2583-6897

AI-ASSISTED SECURITY ORCHESTRATION IN HEALTHCARE INCIDENT RESPONSE

Gaurang Deshpande
Software Developer
IBM, USA
Email: gaurangdeshpande89@gmail.com

Deepak Singh
Advisory Solution Architect
Gainwell Technologies, USA
Email: deepaksingh1981@gmail.com

Abstract- This paper discusses how Security Orchestration, Automation, and Response (SOAR) systems with the help of Artificial Intelligence (AI) can be used to improve incident response in healthcare settings. With growing cases of advanced cyberattacks on patient health records and the internet of medical devices, manual response systems are failing to address the challenge among healthcare facilities. Integration of SOAR and AI technologies, including machine learning and natural language processing, can help automate the threat detection process, simplify the response process, and eliminate analyst burnout.

This study reviews several studies to measure the AI-SOAR models, point out effective case studies, and determine the practical advantages of healthcare cybersecurity. Moreover, it specifies the main challenges, i.e. adversarial attacks, integration issues, and ethical issues, and offers such effective solutions as adversarial training, standard APIs, and human-in-the-loop systems. The results imply that, although AI-SOAR systems have a considerable positive impact on the resilience of healthcare cybersecurity, interoperability, explainability, and strong governance should be regarded as key requirements for successful implementation.

Keywords: AI-SOAR, Security Orchestration, Automation, electronic health records (EHRs), patient safety, malware, ransomware, targeted phishing attacks, security information and event management system (SIEM),

I. INTRODUCTION

A. Background of the study

Healthcare systems are becoming more and more dependent on connected devices and equipment, electronic health records (EHRs), and telehealth infrastructure, which leads to high levels of data traffic but also to an excessive increase in the hospital attack surface. Patient safety and their privacy are threatened by malware, ransomware and targeted phishing attacks [9]. Such threats need to be detected and responded to quickly, but the majority of incident response (IR) procedures are manual, time-consuming and subject to human error.

B. Overview

Security Orchestration, Automation, and Response (SOAR) systems work together to provide security information and event management system (SIEM) functionality, together with automated workflows and response playbooks [3]. With the addition of AI-- especially machine learning and natural language processing these platforms can process large quantities of security telemetry, help prioritise alerts, and automatically execute containment responses like isolating an infected system, or blocking a suspicious infrastructure.

C. Aim and Objectives

The objectives of this study include: 1) To research how AI technologies like machine learning, natural language processing can be used in automating incident response processes in health care. 2) To investigate the relationship between AI-based orchestration platforms and current health care security frameworks. 3) To determine the pragmatic advantages of implementing AI-enabled SOAR in healthcare upon the overview of the available frameworks, applications, and case studies. 4) To evaluate how difficult it is to implement an AI-assisted SOAR system in healthcare and its actionable solution

D. Problem Statement

Delays, classification of misplaced threats, and alert fatigue are among the problems of healthcare incident response that are common. With AI-assisted SOAR, there is a more rapid and scalable response, but there are novel threats: the vulnerability to adversarial attacks, data bias, and difficulties of integrating it into the existing workflow and operator resistance [10].

E. Scope and Significance

This study undertakes a literature review in order to appraise the use of AI-SOAR frameworks as well as ML-based threat detection tools and their relevance in the medical field. The study provides guidance to the healthy and safe uptake of AI-driven orchestration in clinical settings by means of identifying implementation barriers and providing viable solutions.

II. LITERATURE REVIEW

A. AI-based Security Orchestration Framework in Healthcare System

The use of artificial intelligence (AI) in healthcare security systems has, to a large extent, been stimulated by the growing dependence on Internet of Medical Things (IoMT) and cloud-based health services. HealthGuard, one of the most cited frameworks, is also developed based on the supervised machine learning algorithms (Artificial Neural Networks (ANN), Decision Trees (DT), k-Nearest Neighbours (k-NN), and Random Forest (RF)) to identify the anomalies of medical device behaviour ***[Refer to Figure 1]***. It tested IoMT devices of eight categories in three different case scenarios and produced a near 91% accuracy rate and F1-score [1]. This shows how effectively AI can be applied in detecting abnormal behaviours in real-time healthcare settings to minimise reliance on traditional rule-based intrusion detection systems. The popularity of HealthGuard demonstrates that machine learning models can effectively identify new threats in dynamic medical ecosystems without necessarily demanding manual updates to the rule set all the time.

Another system is analysed wherein the real-time threat intelligence with assisted cloud EHR systems was adopted [6]. Their model with AI support created deep packet inspection, along with behavioural correlation, so that possible breaches could be marked. The fact that these models can learn the serial patterns of the network and hone in on it in the future is a viable area of developing ideas to decrease the alert burnout and human error in the Security Operations Centres (SOC) of hospitals.

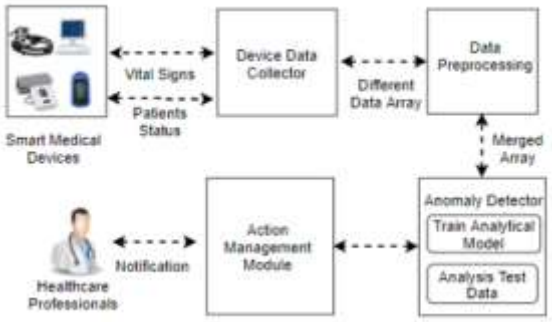

Figure 1: HeathGuard Framework

(Source: [1])

B. Intelligent Agent Architectures for EHR Access Control

Other than the use of AI in anomaly detection, there has been access control using AI in the electronic health habitat. A solution was proposed to access control of sensitive patient records, which is based on the Intelligent Use of Based Access Control (IBAC) framework [2]. Such agents dynamically evaluate the user's role and access patterns and take into consideration contextual factors (e.g. location, time and device security) before access is granted or denied.

The advantage of such a method is its real-time flexibility, scalable decision making, and ability to work on a large scale in health organisations. Nevertheless, it is only effective when integrated without a fracture in hospital departments and systems. Despite the encouraging demonstrations in the study, deployment in the real world still has a long way to go to scale because of interoperability and harmonisation of policies.

C. AI-Supported SOAR Automation for Incident Response

According to the multivocal literature review, the use of AI and automation in SOAR platforms is increasing [3]. The most important automation consisted of alert triage, incident prioritisation, as well as response action executions. Machine learning puts a collection of security events into groups and ranks the events to alert based on the severity level, historical trends and known threat intelligence [3]. Examples of such platforms include IBM Resilient and Palo Alto Cortex XSOAR. This lessens the burden of the analysts to a considerable extent, accelerates the process of containment and improves the accuracy of the decisions made.

An interesting case is the SOAR ML model MADE (Machine learning for Automated Detection and Escalation) demonstrated a precision of 97% to classify high-severity events in enterprise settings [5]. The research revealed that the integration of AI-enabled playbooks enabled the

incident response action orchestration to occur faster, including quarantining devices and separating malicious network traffic, especially in an IT environment like hospitals.

D. Challenges and Solutions in AI-SOAR Implementation

Adversarial attacks can be applied to AI systems, especially machine learning based systems. Examples of such techniques include Fast Gradient Sign Method (FGSM) and Carlini & Wagner (C&W), whose inputs can be manipulated to evade anomaly detectors. It is suggested that adversarial training and sturdy testing regimes are used to maintain the robustness of AI models to such manipulations [1].

The healthcare IT systems tend to encompass numerous software, legacy infrastructure and third-party vendors. The implementation of AI-SOAR tools in current EHRs and security information and event management (SIEM) systems needs to be embedded with standard APIs, data schema, and taxonomies [3]. The possible remedy is the implementation of the taxonomy-driven orchestration frame that will allow mapping of various inputs and outputs of various tools to achieve unified visibility and control.

Decisions made by AI, which are applied to patient information or controls accessing information, must be transparent and explainable. Ethical dangers of opaque AI systems in the health sector and suggested establishing special expert committees that would oversee the algorithmic decisions made and guarantee the compliance of the algorithms with patient rights [4].

III. METHODOLOGY

A. Research Design

This paper uses an explanatory design research to understand the benefits of AI on security orchestration with healthcare incidents responders. The design aims at conceptualising the cause-effect relationships, including the effects of AI on the speed of detection, efficiency of automation, and cyber resilience in general [12]. It integrates the qualitative methods and quantitative methods to ensure the complete picture of present implementations, operational issues as well as performance results. The framework allows incorporating theoretical knowledge into empirical evidence to describe how and why AI-assisted SOAR systems in healthcare can be effective.

B. Data Collection

Both qualitative and quantitative pieces of information used for this study using secondary data collection methods. The peer-reviewed journals, case studies and the cybersecurity white papers with qualitative data were sought on the implementation strategies and ethical issues. The graphs, charts and statistical data of breaches were taken on the basis of the trusted organizations. Such data included the most important indicators, such as incident response time and the accuracy of AI detection. The combination of these sources of information allows carrying out a comprehensive examination of AI-enhanced security orchestration in the healthcare setting.

C. Case Studies and Examples

Case study 1: Milton Keynes University Hospital's Darktrace Issue

Milton Keynes University Hospital responded to the rising number of ransomware infections of UK hospitals in 2017 by deploying Darktrace self-learning AI and an autonomous response system, which is essentially an AI-added SOAR [7]. The system was always analysing the

behaviour of the networks and responding to aberrations without conditions set over it. This unsupervised, real-time AI allowed the hospital to eliminate threats in seconds and stay in service. The initiative became one of the first massive practices of AI orchestration in cybersecurity infrastructures at the NHS.

Case Study 2: Vectra AI in the Bolton NHS Foundation Trust (2018)

Bolton NHS Foundation Trust in 2018 implemented the Cognito platform by Vectra AI to enhance its threat detection and response capacity in its medical IT structure [8]. Cognito system offered behavioural analytics driven by AI, which monitored on-premise and cloud activities in real-time, looking for abnormal activities, which included lateral traffic, privilege escalations, and insider threats. This orchestration platform helped to decrease false positives by eliminating irrelevant events and prioritising the threats according to urgency. Bolton NHS has included the Cognito platform in its security operations by automating alert triage and enabling quicker resolution of incidents with its existing IT environment.

D. Evaluation Metrix

Technical and operational measures are combined to assess AI-assisted SOAR systems' use in health care. Important measures are detection accuracy, false positive rate (FPR), the mean time to detection (MTTD) and containment (MTTC) that affect the responsiveness of the system [11]. Decreases in alert volumes are measures of the effectiveness of the triaging of low-level incidents, whereas integration success exposes compatibility with EHRs and other infrastructures. Ethical Compliance, AI Explainability guarantee is provided by a Human level of control. These measures allow one to compare various platforms to demonstrate how they can improve the process of responding to incidents and mitigate manual labour in healthcare cybersecurity settings.

IV. RESULTS

A. Data Presentation

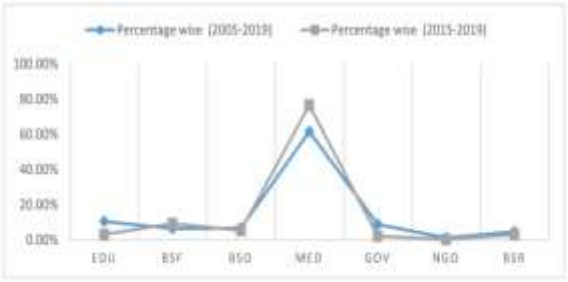

Figure 2: Representation of Data Breach Incident in some sectors, including Healthcare
(Source: [9])

Figure 2 highlights the data breach issues that happened been 2005 to 2019 and between 2015 to 2019. In this graph, the percentages of data breach issues between 2005-2019 are highlighted in the blue line, and the percentage of data breach issues between 2015-2019 is highlighted in the black line [9]. It is observed that within the healthcare industry, the data breach issues increased between 2015-2019 in comparison to the 2005-2019 period. Between 2015 - 2019 total of 80% of data breach cases were identified in the healthcare sector [9].

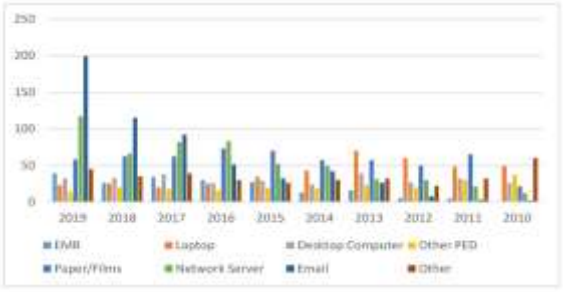

Figure 3: Number of breached incidents every year carried out on each location
(Source: [9])

In Figure 3, eight locations were breached and these are namely Electronic Medical Records (EMR), Laptop, Desktop computers, Other Portable electronic devices, Paper documents, Network Server, Email, and Other [9]. Electronic Medical Records (EMR) experienced the fewest cases of intrusion with pegged at 195; this amounts to a mere 5.99% of the total of 3253 cases it implemented during the said span of time. Other Portable Electronic Devices (PED) take the second position behind the EMR, reaching 6.64% of the total [9].

B. Findings

A graphical interpretation is given in Figure 2, the figure shows that there is a decline in the slope of the graph in each sector in the second case (2015-2019) as compared to the first case (2011-2015), except in the MED sector and then the BSF sector. According to the graph, attackers rely on the healthcare industry as the most appropriate target due to the commercial value of the EHRs. Figure 3 underlines the fact that malicious encroachments to sensitive healthcare information are carried out by cyber criminals who apply various methods to exploit EHRs: malware, ransomware, or phishing attacks. Hackers have become vulnerable to attack over email and Network servers. A comparative presentation of these places is done based on such things as the number of incidents breached daily that have been performed on these places annually, as presented in Figure 3.

C. Case Study Outcomes

Case Study	Strategy	Impact	Outcomes
Case study 1: Milton Keynes University Hospital ’s Darktrace Issue	Installed Darktrace as its self-learning AI that is enabled by an autonomous	Helped the hospital identify and eliminate ransomware attacks	Properly keeping the hospital in case of cyberattacks, was one of the first

	response system where AI (AI-enhanced SOAR) monitors and responds to threats in real-time and without preconfigured rules [7].	in a few seconds, which keeps any service disruption at a minimum in a time when the UK healthcare sphere experiences a surge in cyberattacks [7].	NHS institutions to introduce massively scaled AI orchestration in cybersecurity, and established a benchmark in AI-empowered offence.
Case Study 2: Vectra AI in the Bolton NHS Foundation Trust (2018)	Installed the Cognito platform developed by Vectra AI, and the AI-powered approach that helps to track both cloud and on-premise systems	Minimised false positive warnings by elimination of irrelevant events, enhancing on speed and accuracy of distinguishing threats and	Increased operational effectiveness of cybersecurity management, allowing fast incident resolution and more tightly integrating AI

	in real-time and automatically prioritise reports and alerts based on their severity [8].	responding to them in the already installed IT framework.	orchestration into legacy systems in healthcare [8].

Table 1: Case Study Outcomes

(Source: Self-developed)

The two NHS case studies point to the strong positive impact of AI-assisted security orchestration on cybersecurity in the health industry. The application of Darktrace in the Milton Keynes Hospital showed the capability of unsupervised AI to handle threats to critical infrastructure itself. In the meantime, Bolton NHS demonstrated the effectiveness of AI-powered analytics and prioritisation that help in mitigating alert fatigue and streamlining the response.

D. Comparative Analysis

Sources	**Focus**	**Findings**	**Gaps**
[1]	Security model of smart healthcare systems in machine learning [1].	The proposed HealthGuard framework identifies anomalies and increases healthcare IoT security [1].	Little practical implementation and testing in various medical settings.

[2]	Smart e-Healthcare security of multi-agents.	Multi-agent systems enhance flexibility in the response and detection of threats in real-time [2].	There is a lack of details on integration with the current healthcare IT infrastructure and scalability assessment [2].
[3]	Review of all available security orchestration techniques [3].	Emphasised the advantages of automation and orchestration and described the issues with standardisation.	Basic empirical research confirms the framework of orchestration in a healthcare setting [3].
[4]	Umbracle and difficulties in the implementation of medical	Found some of the main issues concerning trust, explainability,	The necessity of the frameworks targeted towards AI

	AI [4].	and ethics when it came to adopting medical AI [4].	malfunctions and the increased stakeholder trust.
[5]	MADE an automated system to detect and escalate the threat [5].	Illustrated successful machine learning-based automated threat transfer and escalation.	More technically oriented in detection; less related to the problem, challenges and stakeholders in healthcare [5].

Table 2: Comparative Analysis

(Source: Self-developed)

A critical analysis of the literature and highlighting the findings and gaps helps to understand the depth of AI-assisted security orchestration in healthcare incident response.

V. DISCUSSION

A. Interpretation of results

The results reveal how AI-assisted procedures in security orchestration are ensuring improved responses to unanticipated incidents. The AI-assisted real-time threat intelligence in the context of cloud EHRs has been able to support deep packet inspection [6]. Thus, there is proactive identification of possible breaches, reducing the possibility of any incidents. The AI plays a key role in identifying any potent anomaly detection within the system, especially in the case of access patterns [2]. The SOAR-empowered AI is being impactful in identifying high-precision events by 97%, demonstrating the capacity for improved orchestration [3].

However, there are potent challenges associated with the integration of AI, especially in healthcare systems. The ethical guidelines will require certain quality standards for the effective protection of confidential data being used by AI [13]. The poorly trained AI models can fail to identify any sort of sudden events within the system. The bias in AI models coming from diverse sources can fail to identify security events [14]. Thus, to derive effective results, proper guidelines and data for model training are required.

B. Practical Implications

There are practical implications of the research, improving the response to unanticipated incidents within healthcare. The study establishes that the SOAR-empowered AI successfully discerns any security threats encountered [3]. The use of AI in healthcare organisation security can successfully mitigate the threats posed to the system. The AI-powered security orchestration can aid companies in the pre-identification of threats and take measures to tackle them. Robust frameworks for data security in healthcare can be developed through the knowledge attained.

C. Challenges and Limitations

The AI, despite its potent advantages, is facing the limitations of ethical impacts and poorly trained models. AI, with its integration in healthcare, is subject to ethical implications. The confidential data needs to be accessed in order to detect threats. Further, poorly trained models can result in amplification of bias [14]. Under such circumstances, it can be difficult to identify new threat incidents or access patterns that are deviating from previous attacks made on the system.

D. Recommendations

Healthcare organisations looking to integrate AI into their EHR systems should develop trained models free from bias. There should be transparency with patients regarding the data being stored in the system to facilitate their care. The AI integrated with healthcare systems will require proper training of employees. The employees should be trained to analyse the severity of the alerts identified by AI and make appropriate decisions for the system. Healthcare organisations should train AI models with the latest security incident data to gain accurate insights into any kind of anomalies in the system.

VI. CONCLUSION AND FUTURE WORK

The study establishes that AI orchestration is highly impactful in reducing threats posed to healthcare systems. The AI can rank the severity of the alerts and identify the incidents. However, there are potent challenges regarding the ethical concerns and the bias present in training models. Drawing on the same, future work should focus on how the AI can be better trained to address the security incidents faced in healthcare organisations. The knowledge will benefit in developing robust systems free from bias.

VII. REFERENCE LIST

[1] Iqtidar Newaz, A.K.M., Sikder, A.K., Ashiqur Rahman, M. and Selcuk Uluagac, A., 2019. HealthGuard: A Machine Learning-Based Security Framework for Smart Healthcare Systems. *arXiv e-prints*, pp.arXiv-1909.

[2] Khan, F. and Reyad, O., 2020. Application of intelligent multi-agent-based systems for E-healthcare security. *arXiv preprint arXiv:2004.01256*.

[3] Islam, C., Babar, M.A. and Nepal, S. (2019). *A Multi-Vocal Review of Security Orchestration. ACM Computing Surveys, 52(2), pp.1–45.* Available at: https://dl.acm.org/citation.cfm?id=3305268 [Accessed on: 10th November 2020]
[4] Quinn, T.P., Senadeera, M., Jacobs, S., Coghlan, S. and Le, V. (2020). *Trust and medical AI: the challenges we face and the expertise needed to overcome them. Journal of the American Medical Informatics Association, 28(4), pp.890–894.* Available at: https://arxiv.org/pdf/2008.07734.pdf#:~:text=Failures%20in%20medical%20AI%20could. [Accessed on: 18th December 2020]
[5] Oprea, A., Li, Z., Norris, R. and Bowers, K. (2018). *MADE. Proceedings of the 34th Annual Computer Security Applications Conference.* Available at: https://www.ccs.neu.edu/home/alina/papers/MADE.pdf. [Accessed on: 17th December 2020]
[6] Elhoseny, M., Salama, A.S., Abdelaziz, A. and Riad, A.M. (2017). *Intelligent systems based on loud computing for healthcare services: a survey. International Journal of Computational Intelligence Studies, 6(2/3), p.157.* Available at: https://www.researchgate.net/publication/322278198_Intelligent_systems_based_on_loud_computing_for_healthcare_services_a_survey [Accessed on: 16th December 2020].
[7] cambridgenetwork.co.uk (2018). *Darktrace AI defends millions of NHS patients' data in the UK | Cambridge Network.* Cambridgenetwork.co.uk. Available at: https://www.cambridgenetwork.co.uk/news/darktrace-ai-defends-millions-nhs-patients-data-uk [Accessed on: 20th December 2020].
[8] buildingbetterhealthcare.com (2018). *Bolton NHS Foundation Trust selects Vectra to automate threat detection.* Buildingbetterhealthcare.com. Available at: https://buildingbetterhealthcare.com/bolton-nhs-foundation-trust-selects-vectra-to-automate-threat-detection-148508 [Accessed on: 21st December 2020].
[9] Spence, N., Niharika Bhardwaj, M.B.B.S. and Paul III, D.P., 2018. Ransomware in healthcare facilities: A harbinger of the future?. *Perspectives in Health Information Management*, pp.1-22.
[10] Dalal, A., 2018. Cybersecurity And Artificial Intelligence: How AI Is Being Used in Cybersecurity To Improve Detection And Response To Cyber Threats. *Turkish Journal of Computer and Mathemafics Educafion Vol*, *9*(3), pp.1704-1709.
[11] Gunduz, H. and Jayaweera, D., 2020. Modern power system reliability assessment with cyber-intrusion on heat pump systems. *IET Smart Grid*, *3*(5), pp.561-571.
[12] Maforah, N. and Leburu-Masigo, G. (2018). APPLICATION OF THE MIXED METHODS RESEARCH USING SEQUENTIAL EXPLANATORY DESIGN. *ICERI2018 Proceedings*. Available at: https://www.researchgate.net/publication/329228095_APPLICATION_OF_THE_MIXED_METHODS_RESEARCH_USING_SEQUENTIAL_EXPLANATORY_DESIGN. [Accessed on: 19th December 2020]
[13] Helbing, D. (2018). Societal, economic, ethical and legal challenges of the digital revolution: from big data to deep learning, artificial intelligence, and manipulative technologies. In *Towards*

digital enlightenment: Essays on the dark and light sides of the digital revolution (pp. 47-72). Cham: Springer International Publishing.
[14] Roselli, D., Matthews, J. and Talagala, N., 2019, May. Managing bias in AI. In *Companion proceedings of the 2019 world wide web conference* (pp. 539-544).
[15] Chintale, P. (2020). Designing a secure self-onboarding system for internet customers using Google cloud SaaS framework. IJAR, 6(5), 482-487.
[16] Konda, R. ZERO TRUST ARCHITECTURE FOR REMOTE INTEGRATION: SECURING APIS WITH MULESOFT FOR MOBILE BANKING APIS THROUGH API POLICY GATEWAYS.
[17] Goli, S. R. (2021). SRE in Fintech: Ensuring High Availability and Compliance In Cloud-Based Financial Services. Available at SSRN 5741643.
[18] Goli, A. K. R. (2021). CLOUD-FIRST STRATEGIES: A COMPARATIVE STUDY OF BUSINESS OUTCOMES IN MULTI-CLOUD VS. HYBRID ENVIRONMENTS. Journal of Critical reviews, 8(1).