Secure the Future Competition Report: Health Sector

Ethan Neves

California State University, East Bay

Palo Alto Networks Cybersecurity Academy

December 23, 2023

Table of Contents

Executive Summary

The healthcare sector is one of the most common points of interest when considering attacks from malicious actors. The first section in my report addresses the current and potential future state of artificial intelligence within the sector. Considering patient diagnostics and future threat detection techniques. The second section addresses where healthcare security personnel can gather intelligence on threat actors and common attack tools and techniques. Providing recommendations on valuable threat intelligence sources. The third section provides steps to mitigate vulnerabilities and compromised data with an example of an enterprise solution, while providing policy statements in accordance. The final section examines potential solutions for IoT device monitoring while addressing an independent solution versus an enterprise one. The current and future state of the sector is acknowledged and analyzed in each section of the report in an attempt to provide guidance to secure the future of the healthcare sector. The conclusion of the report summarizes discoveries and outcomes made within each section of the report with overall recommendations to secure the future.

Section 1 – Adversarial Behavior, Artificial Intelligence and Machine Learning

The healthcare industry has faced an increasing and alarming amount of adversarial behavior and cyberattacks, with threat actors like cybercriminals, hacktivists, nation-state actors, and insiders targeting organizations for financial gain, extortion, and espionage. All using tactics ranging from social engineering, phishing, DDoS attacks, and ransomware to exploit the vulnerabilities of the healthcare industry. Notable ransomware groups like Lockbit 3.0, CI0p, Royal, and BianLian have explicitly targeted healthcare organizations, resulting in data breaches of millions of patient's sensitive data and information (CISA, 2023). According to *Unit 42 IoT*

Threat Report (2020), "83% of medical imaging devices are running on unsupported operating systems," which poses serious vulnerabilities. As healthcare networks start to integrate more IoT supported devices, future risks are posed, introducing potential zero-day vulnerabilities, and data breaches. The rapid expansion of remote patient monitoring devices during the Covid-19 pandemic has created further vulnerabilities and attack surfaces in this sector. Remote consultations and monitoring are very susceptible to cyber threats, which can compromise patient data, and possibly lead to a misdiagnosis (He et al., 2020).

In the healthcare industry artificial intelligence is commonly used to help produce more accurate diagnoses and enable more personalized treatments (Barth, 2023). In the future we can expect to see an influx of virtual nursing assistants powered by AI, and less invasive surgeries with the help of AI-enabled robots (IBM Education, 2023). To respond to common adversarial behaviors in the health industry like ransomware and social engineering, it is important to implement both a preventative and reactive approach. Using AI-driven threat detection, with solutions ranging from, "machine learning-based anomaly detection to AI-powered threat intelligence platforms" (Vegesna, 2023). Another solution would be to utilize adaptive AI, "capable of identifying subtle patterns and behaviours indicative of AI-generated threats" to help counter social engineering attacks powered by AI (Falade, 2023).

Section 2 - Threat Intelligence, Intelligence Sharing, and Adversary Playbooks

A valuable threat intelligence source I recommend is The Health Information Sharing and Analysis Center (H-ISAC). The H-ISAC is a trusted community of infrastructure owners that focuses on, "sharing timely, actionable and relevant information with each other including intelligence on threats, incidents and vulnerabilities" (Health-ISAC, 2023). Another potential

valuable addition for the future security posture of the health sector is FBI InfraGard, as they have a specialized threat feed for the health sector. InfraGard focuses on threat detection and mitigation, while combining the insights of government agencies and private sector professionals. Additionally, they are, "one of the only threat intelligence solutions that focuses on threat detection and mitigation for U.S. critical infrastructure (Hitler, 2023).

When sharing intelligence, it is important to understand the expectations and procedures for reporting for each source and sector. The Healthcare & Public Health Sector Coordinating Councils (HSCC) define a set of health industry cybersecurity information sharing best practices. Outlining benefits and value of information sharing, what how and with whom to share information, and even several case studies and examples. Following general parameters to share indicators of compromise (IoCs), tactics, techniques, and procedure (TTPs), while also prioritizing sharing emerging threats, vulnerabilities, and incidents impacting patient data or infrastructure (Healthcare and Public Health Sector, 2020). Adversary playbooks in the health sector must be updated with AI tools, define compatible systems, address IoT and remote patient monitoring. While also containing information on main threat actors and attacks in healthcare like ransomware, data breaches, and nation-state actors (Harris, 2023). With the large amount of PII (personal identifiable information) involved in healthcare records it can be a challenge to stay in terms with the Health Insurance Portability and Accountability Act (HIPPA). As HIPPA places additional responsibility on healthcare organizations to protect individuals' electronic personal health information that they receive, use, or maintain (Palo Alto Networks, 2023a). All playbook partners, and alliances like H-ISAC, NH-ISAC, AHA, and HIMSS must be sure they are sharing intelligence in accordance with HIPPA.

Section 3 - Data Islands and Enterprise Cloud Services

A number of attack surfaces and data islands exist within the healthcare sector, expanding vulnerabilities and exploits that can be taken advantage of. Some potential data islands include, Device Data (X-Ray, MRI, CT, etc…), Billing Records and Systems, Electronic Healthcare Records (ERH), Inventory Systems (Medications and Drugs), and even Scheduling Systems as they can contain PII and are often overlooked for security (Affita et al., 2023). To secure the future we must strengthen security measures for mobile, IoT and endpoint devices to stop data breaches and unauthorized access. All devices should have and follow a set of best practices including MFA, robust encryption (elliptic curve, RSA or similar), regular OS and security updates/patches, and methods of anonymizing and/or cleansing data. For databases and records, database redundancy should be included with secure and robust authentication and access control systems, with minimum encryption requirements and standards for data storage (Herman, 2023).

An enterprise cloud-based security management system that I would implement to help reduce security vulnerabilities and data exposure for IoT and mobile devices is AWS IoT Device Management in conjunction with AWS IoT Device Defender. The system should address authentication through digital signatures and certificates and address data encryption through updated and secure methods like TLS (Amazon Web Services, 2023a). It should also address data cleansing to remove data that doesn't need to be stored in a system but gives potential risks, like PII. AWS' approach to device monitoring is done using, "machine learning…to monitor traffic from a malicious IP or a spike in connection attempts" (Amazon Web Services, 2023b). Additionally, the system will get security alerts if an audit fails or anomalies are detected, to

ensure quick action is taken. It's important that this system also addresses healthcare industry standards like HIPPA in an effort to protect individuals' information in accordance.

Section 4 – DevSecOps, SRE, SOAR, ZTNA and SASE

In securing the future of healthcare a SOAR solution like ServiceNow Security Incident Response (SIR) will help to effectively monitor applications and devices. It can also assist in automating security alerts. As the nature of healthcare operations is varied, and SIR provides both integration and configurability, it makes it a good choice as it extends beyond just incident response (Zawalnyski, 2022). To secure networking infrastructure with authentication based on zero trust, the utilization of a cloud-first and unified SASE architecture will be the most robust. The migration of applications and sensitive healthcare data into secure cloud environments would assist with security and scaling of organizations. 'Prisma SASE' by Palo Alto Networks, powered by AI and built for Zero Trust helps in protecting, "against the latest AI-driven threats and fuel(s) innovation and productivity everywhere" (Palo Alto Networks, 2023b). According to the research (Mehrtak et al., 2021), by centralizing sensitive data and apps in cloud environments, healthcare companies will be able to both increase their cybersecurity defenses as well as streamline operations without having to worry about cyber threats. The incorporation of AI and a Zero Trust model in solutions reflects a forward-thinking approach, safeguarding healthcare ecosystems against emerging threats while fostering innovation.

Conducing a feasibility study for my solution, choosing an independent security product implementation gives the advantage of more tailored solutions to security needs of the healthcare sector, as seen with AWS' IoT Device Management. However, this approach could also lead to integration challenges and higher costs as the number of IoT devices in healthcare continues to

grow (Zawalnyski, 2022). Conversely, adopting a unified SASE model like Prisma SASE from Palo Alto Networks gives a more comprehensive solution for networking infrastructure while addressing zero trust network access. While also simplifying management and allowing scalability (Palo Alto Networks, 2023b). However, this also requires an alignment with healthcare organizational workflows and integration processes.

Conclusion

When examining adversarial behavior within the healthcare industry, I found the need for a more robust security solution. Common ransomware and social engineering attacks in conjunction with vulnerabilities in healthcare devices make aware the sector's susceptibility to attack. Current and future AI and ML will not only help in assisting patient diagnoses, but also in advanced threat detection. Intelligence sharing also proves a necessary development with intelligence sources like H-ISAC and FBI InfraGard providing valuable information on current threats. The HSCC both outlines and explains the importance of implementing best practices to secure data. Common data islands in healthcare pose vulnerabilities, showing the importance of IoT, mobile, and endpoint security. I recommend an enterprise cloud-based solution like AWS IoT Device Management, that contains robust authentication, encryption, monitoring, and data cleansing. Finally, adopting a unified SASE model like Prisma SASE will help to secure networking infrastructure while utilizing zero trust authentication. To secure the future of healthcare, an approach involving Artificial Intelligence, collaborative intelligence sharing, and robust security systems is necessary, ensuring both a proactive and reactive approach providing resilience against new emerging threats while allowing efficiency, innovation, and scalability.

References

Affia, A. O., Finch, H., Jung, W., Samori, I. A., Potter, L., & Palmer, X.-L. (2023). IoT Health Devices: Exploring Security Risks in the Connected Landscape. *IoT*, *4*(2), 150–182. https://doi.org/10.3390/iot4020009D

Amazon Web Services. (2023a). *AWS IoT Device Management Features - AWS*. Amazon Web Services, Inc. https://aws.amazon.com/iot-device-management/features/#:~:text=These%20secure%20device%20connections%20are

Amazon Web Services. (2023b). *Securing IoT Devices - AWS IoT Device Defender - AWS*. Amazon Web Services, Inc. https://aws.amazon.com/iot-device-defender/?nc=sn&loc=2&dn=5

Barth, S. (2023). *Artificial Intelligence (AI) in Healthcare & Hospitals*. ForeSee Medical. https://www.foreseemed.com/artificial-intelligence-in-healthcare

CISA. (2023, May 16). *#StopRansomware: BianLian Ransomware Group | CISA*. Www.cisa.gov. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a

Falade, P. (2023). Decoding the Threat Landscape : ChatGPT, FraudGPT, and WormGPT in Social Engineering Attacks. *J. Sci. Res. Comput. Sci. Eng. Inf. Technol*, *9*(5), 185–198. https://doi.org/10.32628/CSEIT2390533

Harris, E. (2023, May 28). *How Healthcare Leaders Can Prepare: Crisis Playbook Development and Best Practices*. Revive. https://www.reviveagency.com/blog/how-healthcare-leaders-can-prepare-crisis-playbook-development-and-best-practices/

He, Y., Aliyu, A., Evans, M., & Luo, C. (2020). Healthcare Cyber Security Challenges and Solutions Under the Climate of COVID19: A Scoping Review (Preprint). *Journal of Medical Internet Research*, *23*(4). ncbi. https://doi.org/10.2196/21747

Health-ISAC. (2023). Health-ISAC - Health Information Sharing and Analysis Center. https://www.h-isac.org

Healthcare and Public Health Sector. (2020, March). *Health industry cybersecurity information sharing best practices*. Healthsectorcouncil.org; Healthcare and Public Health Sector Coordinating Councils. https://www.aha.org/system/files/media/file/2020/03/health-industry-cybersecurity-information-sharing-best-practices-march-2020.pdf

Herman, E. (2023, December). *A Critical Overview of Industrial Internet of Things Security*. ResearchGate. https://www.researchgate.net/publication/373388715_A_Critical_Overview_of_Industrial_Internet_of_Things_Security_and_Privacy_Issues_Using_a_Layer-Based_Hacking_Scenario

Hiter, S. (2023, August 10). *6 Best Threat Intelligence Feeds to Use in 2023*. ESecurity Planet. https://www.esecurityplanet.com/products/threat-intelligence-feeds/

IBM Education. (2023, July 11). *The benefits of AI in healthcare*. IBM Blog. https://www.ibm.com/blog/the-benefits-of-ai-in-healthcare/

Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P., Soleymanzadeh, M., Vahedi, F., Mehraeen, E., & Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing. *Journal of Medicine and Life*, *14*(4), 448–461. https://doi.org/10.25122/jml-2021-0100

Palo Alto Networks. (2023a). *Healthcare Cybersecurity*. Palo Alto Networks. https://www.paloaltonetworks.com/industry/unit42-healthcare

Palo Alto Networks. (2023b). *Prisma SASE*. Palo Alto Networks. https://www.paloaltonetworks.com/sase

Unit 42 IoT Threat Report. (2020, March 10). Unit42. https://unit42.paloaltonetworks.com/iot-threat-report-2020/

Vegesna, D. V. V. (2023). Enhancing Cyber Resilience by Integrating AI-Driven Threat Detection and Mitigation Strategies. *Transactions on Latest Trends in Artificial Intelligence*, *4*(4). https://ijsdcs.com/index.php/TLAI/article/view/396/140

Zawalnyski, A. (2022, April 26). *The Top 10 SOAR Solutions*. Expert Insights. https://expertinsights.com/insights/the-top-soar-solutions/