Palo Alto - Secure the Future

Angela Milova

Brigham Young University

Table of Contents

Executive Summary ……3

Section 1 ……4

Adversarial Behavior ……4

Artificial Intelligence & Machine Learning ……..4

Section 2 ……5

Threat Intelligence & Intelligence Sharing ……5

Adversary Playbooks ……5

Section 3 ……6

Data Island Management ……...6

Enterprise Cloud-based Security ……...6

Section 4 ……....7

DevSecOps & Enterprise Security ……7

Conclusion ……8

References ……9

Executive Summary

In the face of rising adversarial behavior, particularly highlighted by high-stakes ransomware attacks like the Hive Attack demanding $240 million, the healthcare sector is confronted with a dynamic threat landscape encompassing Zero-day exploits and AI integration concerns. AI and ML play a great role in diagnostics threats, with recommended resources like the MITRE ATT&CK Framework and Abuse.ch providing comprehensive guides and real-time threat feeds.

To address the evolving threat landscape, a specific Adversary Playbook for healthcare seeks to establish a robust framework, acknowledging the challenges posed by the ever-changing nature of cyber threats. Identifiable data islands, such as Patient Health Records and IoT devices, necessitate the implementation of robust management policies to ensure secure usage and unify data sources. For cloud-based security, PRISMA by Palo Alto emerges as a comprehensive solution offering versatile authentication, SSL/TLS protocols, and compliance with standards like HIPAA and GDPR. Its monitoring capabilities further facilitate prompt threat detection. Implementing a DevSecOps model involves adopting a zero-trust approach, and the integration of Cortex XSOAR to enhance SOAR capabilities becomes a logical progression in this security strategy. In the feasibility study, exploring the pros and cons of independent security product implementations versus enterprise solutions adoption can show more about the security solutions related to the healthcare sector.

Furthermore, evaluating SASE models, including ZTNA, directly addresses the unique security challenges within the healthcare sector. This emphasis on solutions connects back to the earlier discussions on the specific threats and management policies required for data islands and cloud-based security.

Section 1

Adversarial Behavior

The health sector faces a significant surge in adversarial behavior, notably due to its critical need for uninterrupted service delivery, making it an attractive target for threat actors. Ransomware-induced lockdowns pose catastrophic consequences, exemplified by the Hive Attack's $240 million ransom demand in November 2021 (Health and Human Services, 2022). Threat actors, including cybercriminals and nation-states like China, Russia, and North Korea, exploit vulnerabilities in various ways, employing methods like social engineering, phishing, and DDoS attacks (Baisley, Cherrat, 2023). The 2022 Ponemon Institute Inside Report reveals a nearly 50% rise in insider threats, emphasizing the need to address both insider and external threats (Health Industry, n.d). The evolving threat landscape introduces vulnerabilities, such as Zero-day exploits, Supply Chain Risks, and challenges associated with AI and machine learning integration (Xhofleer, 2023). Fast responses from IT professionals are crucial, as evidenced by Unit 42's Palo Alto Attack Surface Threat report (Unit 42, n.d).

Artificial Intelligence (AI) and Machine Learning (ML)

In the health sector, AI is employed for various applications, including diagnostics, personalized medication, and administrative tasks. Meanwhile, ML integration in healthcare aids in analyzing large amounts of data to predict disease prevention and assists healthcare providers in tailoring personalized treatments based on patients' needs (Alowais, Alghamdi, Alsuhebany, et al., 2023). The future of AI and ML in the health sector extends beyond enhancing patients' experiences; it can also significantly improve cybersecurity measures. Regarding adversarial behaviors, AI can play a crucial role in identifying patterns in network traffic or user behavior. It identifies and maps techniques used by healthcare threat actors (Bouchama, Kamal, 2021).

Section 2

Threat Intelligence and Intelligence Sharing

Two highly recommended resources for Threat Intelligence are the MITRE ATT&CK Framework and Abuse.ch. The MITRE ATT&CK Framework provides a comprehensive guide to understanding threat actors' Tactics, Techniques, and Procedures (TTPs), fostering collaboration in the cybersecurity community and enhancing incident response capabilities (Xiong, Legrand, Åberg, et al., 2022). On the other hand, Abuse.ch focuses on real-time threat feeds related to malware, phishing, and botnets. Platforms like Malware Bazaar and Threat Fox offer actionable insights, enabling organizations to test the impact of malware, monitor systems for specific threats, and identify indicators of compromise (IOCs) (Abuse.ch, n.d). Furthermore, information sharing is crucial for the Health Sector to be more protected. Expectations for sharing intelligence involve a collaborative and transparent approach. The parameters for sharing data with the intelligence community will revolve around relevance, accuracy, and legality. When sharing threat intelligence-related data, such as specific threats, vulnerabilities, and incidents, it must be ensured that any personally identifiable information (PII) and sensitive data are not shared (Federal Government, n.d).

Adversary Playbooks

In defining the Sector Playbook, the primary goals and objectives are to establish a comprehensive framework for understanding, mitigating, and responding to cyber threats specific to the health industry. Objectives involve identifying vulnerabilities unique to our industry, formulating proactive defense strategies, and enhancing incident response capabilities (Roberts, Brown, 2017). Challenges may arise due to the dynamic nature of cyber threats, demanding continual adaptation.

Section 3

Data Island Management

In the healthcare sector, identifiable data islands encompass Patient Health Records (PHRs), IoT medical equipment, and Research and Clinical Trial Data. A comprehensive Endpoint Mobile and IoT Device Management policy must be enforced to address security vulnerabilities associated with these islands. This policy prioritizes device security within the healthcare sector and includes staff training to ensure secure device usage (Praveen, 2023). Additionally, the implementation of a Data Integration Policy is crucial, given the sector's handling of sensitive patient data and clinical trial information from various healthcare domains (Zarour, Alenezi, Ansari, et al., 2021).

Enterprise Cloud-Based Security

PRISMA by Palo Alto offers a robust solution for enhancing the security of IoT and mobile devices within the Enterprise cloud-based security management system. It has versatile authentication support, including methods like SAML, TACACS+, RADIUS, and MFA (Strata Cloud Manager, n.d). Employing SSL/TLS protocols for data in transit and encryption for data at rest, PRISMA strengthens data protection (Strata Cloud Manager, n.d). The system incorporates data governance features for policy-driven data retention and deletion, ensuring compliance (Palo Alto Networks, n.d). PRISMA's monitoring and analytics capabilities provide visibility into device activities, facilitating prompt threat detection and response (Palo Alto Networks, n.d). Auditing features track user interactions, supporting real-time notifications for security incidents (Palo Alto Networks, n.d). Additionally, PRISMA aligns with industry compliance standards such as HIPAA and GDPR, providing a robust framework for meeting regulatory requirements (Palo Alto Networks, n.d).

Section 4

DevSecOps Policies and Procedures & Enterprise Security

Embracing a DevSecOps model for our healthcare application involves implementing a robust zero-trust model for secure authentication, ensuring thorough verification of every user and device regardless of location. Leveraging multi-factor authentication (MFA), device posture checks, and continuous monitoring, our application establishes a resilient security posture (Zscaler, n.d). To enhance our Security Orchestration, Automation, and Response (SOAR) capabilities, the integration of Cortex XSOAR can be a great solution as Cortex XSOAR can monitor the application and devices, automate security alert analysis, and orchestrate responses (Palo Alto, 2020). In securing the future of the healthcare sector, the application of networking infrastructure by adopting a cloud-first and unified Secure Access Service Edge (SASE) architecture can be a good solution (Islam, Colomo-Palacios, Chockalingam, 2021). Leveraging cloud-based security services, this approach provides scalable and integrated solutions that enhance data protection, streamline connectivity, and ensure adaptability to evolving threats.

For the feasibility study of our end-to-end solution, the choice between independent security product implementations and enterprise solutions adoption presents distinct advantages and drawbacks. Independent implementations offer customization but may lead to integration challenges, while enterprise solutions provide cohesion but may limit customization (Lwakatare, 2017). In evaluating SASE models for our healthcare applications or devices, considerations include the specific needs of our sector. A SASE model, such as Zero Trust Network Access (ZTNA), offers promising frameworks focusing on user identity and zero-trust principles, respectively (Sarkar, Choudhary, Shandilya, 2022). The choice will depend on our healthcare sector's unique requirements and risk mitigation strategies.

Conclusion

Securing the future of the healthcare sector demands a comprehensive strategy. To begin, continued integration of AI and ML applications in diagnostics and personalized treatments is recommended, emphasizing the incorporation of cybersecurity measures within these technologies. Strengthening Threat Intelligence remains important, and collaborative platforms like the MITRE ATT&CK Framework and Abuse.ch should be actively leveraged, with a special focus on transparent and relevant information sharing.

The development and ongoing adaptation of an Adversary Playbook specific to healthcare are crucial for the industry's resilience against evolving cyber threats. Implementing robust management policies for data islands, including Endpoint Mobile and IoT Device Management, alongside Data Integration Policies, becomes imperative to ensure secure data usage and unify fragmented sources.

The utilization of PRISMA by Palo Alto can help the healthcare system implement better cloud-based security. Organizations should prioritize continuous monitoring and prompt threat detection capabilities offered by PRISMA. Furthermore, adopting a DevSecOps model, incorporating a zero-trust approach and the integration of Cortex XSOAR, should become standard practice to enhance security orchestration, automation, and response.

In the feasibility study, organizations are advised to carefully weigh the pros and cons of independent security product implementations versus enterprise solutions adoption, prioritizing a balanced approach aligned with their specific needs. Additionally, adopting SASE models, particularly Zero Trust Network Access, should be tailored to address healthcare's unique security challenges. The future of healthcare cybersecurity lies in a proactive, collaborative, and adaptable strategy integrating advanced technologies.

References

Abuse.ch. BFH. (n.d.). https://www.bfh.ch/en/research/reference-projects/abuse-ch/

Alowais, S. A., Alghamdi, S. S., Alsuhebany, N., Alqahtani, T., Alshaya, A. I., Almohareb, S. N., & Albekairy, A. M. (2023). Revolutionizing healthcare: the role of artificial intelligence in clinical practice. *BMC Medical Education*

Baisley, T., & Cherrat, Y. (2023). Cyber Threats and Engagements in 2022.

Bouchama, F., & Kamal, M. (2021). Enhancing Cyber Threat Detection through Machine Learning-Based Behavioral Modeling of Network Traffic Patterns. *International Journal of Business Intelligence and Big Data Analytics*

Federal Government Cybersecurity Incident & Vulnerability Response Playbooks - CISA. (n.d)

Health and Human Services. (2022). FACT SHEET: Ransomware and HIPAA.

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (n.d.).

Islam, M. N., Colomo-Palacios, R., & Chockalingam, S. (2021, September). Secure access service edge: A multivocal literature review. In *2021 21st International Conference on Computational Science and Its Applications (ICCSA)* (pp. 188-194). IEEE.

Jabarulla, M. Y., & Lee, H.-N. (2021, August 8). *A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications*.

Lwakatare, L. E. (2017). DevOps adoption and implementation in software development practice: concept, practices, benefits and challenges.

Palo Alto Networks - *Cloud Visibility, Cloud Compliance & Cloud Governance*. (n.d.).

Palo Alto Networks, Inc. (2020, February 24). *Palo Alto Networks introduces cortex XSOAR,*

redefines security orchestration and automation with integrated threat Intel Management. PR Newswire: press release distribution, targeting, monitoring and marketing.

Praveen. (2023, November 20). *IOT security: Safeguarding Critical Networks against Digital assaults*. Cybersecurity Exchange.

Roberts, S. J., & Brown, R. (2017). *Intelligence-driven incident response: Outwitting the adversary*. " O'Reilly Media, Inc.".

Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of zero trust networks in cloud computing: A comparative review. *Sustainability*, *14*(18), 11213.

Strata Cloud manager. Manage: Authentication. (n.d.).

Unit 42 attack surface threat report - start.paloaltonetworks.com. (n.d.-b).

Xhofleer, T. (2023, October 2). *Ai helps hackers steal data. Healthcare Providers Must Get Ready now*. ICT&health.

Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*

Zarour M, Alenezi M, Ansari MTJ, Pandey AK, Ahmad M, Agrawal A, Kumar R, Khan RA. Ensuring data integrity of healthcare information in the era of digital health. Healthc Technol Lett. 2021 Apr 16;8(3):66-77. doi: 10.1049/htl2.12008. PMID: 34035927; PMCID: PMC8136763.

Zscaler - *What is Zero trust security, Principles & Benefits*. (n.d.).