10/17/2023

Individual Assignment

MBAN 6200A

Nandhu Krishnan Muralidharan Nair
220052718

Sick Kids Hospital, a leading healthcare institution, recently faced a severe security breach that disrupted its operations, resulting in delayed lab and imaging results, phone line outages, and the shutdown of the staff payroll system. The organization is now in dire need of a robust cybersecurity solution to prevent and respond to future cyberattacks effectively.

Introduction

Sick Kids Hospital, located in Toronto, is renowned for its world-class healthcare services and innovative medical research. However, it has recently been targeted by a ransomware cyberattack, leading to severe operational disruptions. The attackers compromised the hospital's infrastructure, causing delayed access to critical lab and imaging results, phone communication breakdowns, and the unavailability of the staff payroll system. This incident has underscored the critical need for a comprehensive cybersecurity solution to protect the organization's sensitive data and ensure uninterrupted healthcare services.

Description of AI Use Case

To address the security challenges faced by Sick Kids Hospital, we propose the implementation of the CrowdStrike security tool, which leverages the power of the CrowdStrike® Security Cloud and AI. This platform offers real-time indicators of attack, threat intelligence, knowledge of evolving adversary tradecraft, and enriched telemetry from across the enterprise. The key AI use case involves:

- **Real-time Threat Detection**: CrowdStrike's AI algorithms continuously monitor the hospital's network and systems, detecting anomalies and potential threats in real-time. It leverages threat intelligence and machine learning to identify even the most sophisticated attacks.
- **Automated Protection and Remediation**: In the event of a security breach, the AI-driven system can autonomously respond to mitigate the threat, isolating compromised systems and preventing lateral movement of attackers.
- **Elite Threat Hunting**: CrowdStrike's expert threat hunters, supported by AI, proactively search for signs of malicious activity, ensuring that no threat goes undetected.
- **Prioritized Observability of Vulnerabilities**: The system provides detailed visibility into the hospital's infrastructure vulnerabilities, helping the IT team prioritise and remediate them efficiently.

Business Case and Implementation Plan

Business Case:

The implementation of the CrowdStrike security tool is not just a security measure; it's an investment in the continuity of care and the protection of sensitive patient data. The potential benefits of this solution include:

- Enhanced security and reduced vulnerability to cyberattacks.
- Minimized operational disruptions and downtime.
- Protection of patient and staff data.
- Ensured compliance with data protection regulations.
- Increased confidence from patients and partners in the hospital's ability to secure data.

Implementation Plan:

i. **Assessment**: Conduct a comprehensive assessment of the hospital's existing security infrastructure and vulnerabilities.
ii. **CrowdStrike Deployment**: Install and configure the CrowdStrike security tool across the hospital's network.
iii. **Integration**: Ensure seamless integration with existing security measures and protocols.
iv. **Training**: Train the hospital's IT and security teams on using the CrowdStrike platform effectively.
v. **Testing**: Conduct extensive testing and validation to ensure the system functions correctly.
vi. **Monitoring and Maintenance**: Continuously monitor the system and perform regular updates and maintenance.
vii. **Response Plan**: Develop and document a detailed incident response plan to address any future cyber incidents effectively.

Risks and Issues Discussion

While the implementation of the CrowdStrike security tool is a proactive step towards mitigating cyber threats, it's essential to acknowledge potential risks and issues:

- Initial Costs: The implementation will involve initial costs for software, hardware, and training.
- Integration Challenges: Integrating the new system with existing infrastructure may pose challenges.
- False Positives/Negatives: AI-driven systems may generate false positives or miss certain threats.
- Training Requirements: Adequate training is necessary to ensure the AI tool is used effectively.
-

Measuring Outcomes

To determine the value of the AI solution, we will measure the following key performance indicators:

- **Reduction in Security Incidents**: Tracking the number of security incidents and breaches before and after implementation.
- **Downtime Reduction**: Measuring the time required to recover from a cyber incident post-implementation.
- **Compliance Improvements**: Ensuring adherence to relevant data protection regulations.
- **Patient and Staff Satisfaction**: Gauging the satisfaction of patients and staff with the hospital's data security measures.

In conclusion, the implementation of the CrowdStrike security tool is a proactive and critical step in safeguarding Sick Kids Hospital's operations, data, and reputation. By leveraging the power of AI, the hospital can not only prevent future attacks but also ensure uninterrupted healthcare services and maintain patient trust.

Reference

https://toronto.ctvnews.ca/ransomware-group-lockbit-apologizes-saying-partner-was-behind-sickkids-attack-1.6214906

https://www.crowdstrike.com/falcon-platform/