Executive Summary Highlights

Prepared by: Isabelle Jaber

Date: September 18th, 2024

RISK ASSESSMENT EXECUTIVE SUMMARY

This report provides an overview of key AI-related security risks identified for VISION's operations, focusing on applications and assets such as the Data Integration Platform, Cloud Storage, Data Annotation Application, Customer Relationship Management (CRM) System, and Pre-Trained AI Model Library. Given VISION's involvement in sensitive healthcare data processing and AI development, robust security measures are essential to safeguard data, maintain client trust, and ensure regulatory compliance. The risks identified include Data Breaches, Unauthorized Access, Adversarial Attacks, and Model Poisoning. Recommendations are provided to mitigate these risks and enhance VISION's overall security posture.

THREAT MODEL EXECUTIVE SUMMARY

This report presents a detailed threat modeling analysis for VISION's healthcare imaging AI solution. The analysis focuses on AI-specific threats within the context of handling sensitive medical data. Key findings identify potential risks associated with AI model integrity, training data security, and compliance with data privacy regulations. The report uses the STRIDE framework to categorize and assess threats and provides compensating controls and recommendations to address these issues. Implementing these measures will enhance the security of the AI systems and protect patient data from various threats

NETWORK & DATA SECURITY EXECUTIVE SUMMARY

This report presents an analysis of network and data security for VISION, a technology company specializing in computer vision. The report details the current network and data architecture, identifies specific security concerns, and offers strategic solutions to mitigate risks, especially those related to AI technologies. It emphasizes safeguarding sensitive data, particularly in the context of a new healthcare client that requires secure and efficient processing of medical imaging data.

THIRD-PARTY RISK EXECUTIVE SUMMARY

This report provides a comprehensive third-party risk analysis for VISION, focusing on the security implications of incorporating AI technologies in collaboration with external vendors. VISION, specializing in computer vision, relies on various third-party vendors for its operational needs, including data management, cloud services, and cybersecurity. Given the sensitive nature of the data involved, particularly with the recent engagement with a large healthcare provider, it

is crucial to assess the risks associated with these third-party relationships and ensure effective management strategies are in place. This analysis aims to identify potential risks, outline responsibilities within cloud service models, and recommend strategies for mitigating third-party risks, especially in the context of AI security.

INCIDENT RESPONSE PLAN EXECUTIVE SUMMARY

This Incident Response Plan focuses on VISION's Artificial Intelligence (AI) infrastructure, which powers critical computer vision models for healthcare diagnostics. As machine learning systems are vulnerable to a variety of specific threats, such as model poisoning, adversarial attacks, and data manipulation, this Incident Response Plan is designed to respond to incidents targeting VISION's AI models, data pipelines, and underlying infrastructure. The plan ensures that VISION can quickly mitigate security threats to its Machine Learning (ML) services and maintain reliable service delivery for clients.

BUSINESS CONTINUITY PLAN EXECUTIVE SUMMARY

This Business Continuity Plan (BCP) outlines strategies to ensure VISION maintains uninterrupted operations despite potential disruptions. Given the sensitive nature of healthcare data processed by VISION, the BCP focuses on safeguarding machine learning environments against risks such as system failures, cyberattacks, and regulatory breaches. This plan positions VISION to effectively respond to disruptions, ensuring the continuity of high-quality services and compliance with regulatory obligations. Regular updates and proactive testing will be crucial for sustaining operational integrity in the face of emerging challenges.