KAMILIMU

TEAM HIMAYA

1. Abigael Mbugua - Project Lead and Threat Analyst
2. Peter Wambua - Penetration Tester
3. Linet Ithara - Network Security Engineer

ICT Track Mentor - John Kuria

PROBLEM BACKGROUND

Ransomware remains a major global threat and is recognized by the FBI as a top attack vector. According to the Africa Annual Cybersecurity Report – Kenya 2023, ransomware attacks are becoming increasingly sophisticated, targeting critical infrastructure, state corporations, healthcare systems, and cloud service providers. In 2022, 76% of organizations in Africa were targeted by ransomware, with 64% successfully infected, reflecting the pervasive and escalating nature of these threats.

While ransomware attacks impact various sectors, such as the 2023 Rhysida attack on the Kenya Bureau of Standards (KEBS), which exposed significant risks to institutions handling critical data, hospitals are especially vulnerable due to the sensitive patient information they manage. The private nature of healthcare data makes hospitals a high-risk target for ransomware attacks.

The Sophos 2024 report underscores the severity of the issue within the healthcare sector. It notes that 67% of healthcare organizations experienced ransomware attacks in 2024, a significant increase from 60% in 2023. Moreover, 95% of affected organizations had their backups compromised, with 66% of these attempts being successful. This high rate of backup compromise reveals severe vulnerabilities within healthcare IT infrastructure. The average recovery cost rose to $2.57 million in 2024. The tendency to pay ransoms has also increased, with 53% of healthcare organizations paying in 2024, compared to 42% in 2023.

Hempel and McIntosh, 2024 note that the consequences of healthcare ransomware attacks extend beyond financial losses. These attacks disrupt patient care by delaying access to medical records and treatments, risking patient safety. They also compromise patient confidentiality, leading to potential identity theft and fraud. These breaches damage public trust in healthcare organizations.

Specific vulnerabilities in digital systems further amplify the risk. For instance, a study conducted among staff at MediHeal group of hospitals in Nairobi found that 64% of respondents encountered cybersecurity threats through autogenerated emails, indicating significant vulnerabilities that could lead to malware introduction and compromise patient data (Raburu, 2021). Moreover, the 2023 Kenya Health Facility Census Report revealed that 31% of health facilities have a Hospital Management System; of those, 62% use an end-to-end system. While

useful, this integration creates a single point of failure, making it easier for ransomware from phishing attacks to spread across the network, leading to encrypted patient records, disrupted operations, and exposed data. These vulnerabilities highlight the need for robust cybersecurity measures to protect patient safety and privacy.

Existing solutions like Cloudflare and GreatHorn rely on static analysis methods, providing visual alerts that are reactive and limited in adaptability. While they offer some level of security, they do not effectively address the dynamic and evolving nature of ransomware threats. This study explores the research question: How might we design and implement a system that protects healthcare data more effectively against ransomware attacks, ensuring hospitals avoid reputational damage and financial losses?

To answer the research question, this project introduces an email monitoring tool implemented as an add-on that utilizes threat intelligence databases and integrated alerts to protect healthcare organizations from ransomware threats.

MARKET RESEARCH

Cloudflare and GreatHorn are advanced email security solutions that protect users from email-based threats like phishing and ransomware. One of Cloudflare's key features is email link isolation, which rewrites suspicious email links. If a user clicks on a risky link, they are given the option to open it in a secure, isolated environment. Cloudflare primarily relies on static analysis methods, scanning for known malware signatures and phishing patterns, and alerts users via static notifications through dashboards and emails. GreatHorn, on the other hand, uses sophisticated algorithms and static analysis to detect threats by evaluating hundreds of data points, such as email content, links, and attachments. It sends static alerts through smart banners and inline warnings, offering contextual information about the threat directly within the email interface.

Himaya, however, sets itself apart by offering a more dynamic and proactive approach to email security. Unlike Cloudflare and GreatHorn, which primarily rely on visual static alerts, Himaya integrates both audio and visual alerts to prevent users from clicking on malicious links. This dual-alert system ensures immediate user awareness, significantly reducing the risk of

ransomware attacks. Additionally, Himaya integrates real-time threat intelligence from multiple databases, offering timely updates on emerging threats, unlike the more static threat detection used by competitors. This real-time protection gives Himaya a competitive advantage by actively blocking threats before they infiltrate a system.

Himaya's specialization in healthcare strengthens its competitive edge by addressing the specific security challenges faced by the 2,860 hospitals in Kenya that use HMIS. By targeting this vital sector, Himaya ensures continuous hospital operations, mitigating the risk of costly ransomware attacks. This focus not only enhances the security framework of healthcare institutions but also contributes to economic stability by preventing service disruptions and financial losses.

SOLUTION IDEA

Target User

Our primary target users for this project are Kenyan health institutions utilizing Hospital Management Systems (HMIS). These users were chosen because ransomware attacks on healthcare are becoming more common and sophisticated, as shown by reports from Sophos 2024. The critical nature of their operations, that is handling sensitive patient data, makes them especially vulnerable to these attacks, where breaches can compromise patient safety, disrupt healthcare services, and result in significant financial losses.

While other sectors like finance and government also face ransomware threats, healthcare stands out due to the highly sensitive nature of the data involved and the severe consequences of service disruptions. By focusing on healthcare, we aim to tailor our solution to address these organizations' specific challenges, so that it works better for them.

Solution Prototype

Himaya, the solution offering to enhance cybersecurity in these healthcare organizations against ransomware attacks, is a system in the form of an email monitoring tool that integrates seamlessly with email servers like the Gmail server and uses threat intelligence databases to scan and analyze emails for any ransomware signatures.

Technology Used

We chose an email monitoring tool because email remains a primary vector for ransomware attacks, especially through phishing attacks. This is justified by Raburu, 2021. By integrating real-time threat intelligence, the tool can proactively identify and mitigate threats before they infiltrate the system.

The solution consists of the following components:

- Email Server Integration: Himaya will be designed as an add-on for emails, which allows for straightforward integration into existing email systems commonly used by healthcare organizations. This ensures easy integration into existing email systems used by healthcare organizations, and minimal disruptions to daily operations while enhancing email security.
- Threat Analysis: the core functionality involves comprehensive threat analysis. The add-on will analyze incoming emails in real time, scanning for known ransomware signatures and suspicious patterns in links. Himaya will leverage threat-intelligence databases like Virus Total and MalwareBazaar. This proactive approach enables the system to detect threats before they can infiltrate the organization's infrastructure.
- Alerts: Himaya will send static alerts through smart banners and inline warnings, offering contextual information about the potential threats directly within the email interface.

Process Overview

Himaya will follow a structured and systematic process to ensure comprehensive monitoring and rapid response to potential threats. The process involves four key stages: email-server integration, add-on activation, threat analysis, and alerting. Below is a description of each stage in the process:

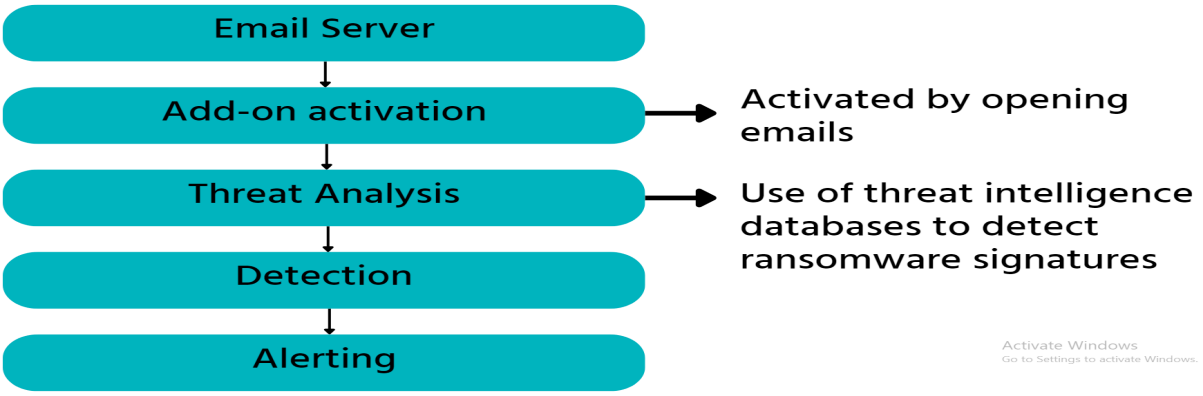


Figure 1: Diagrammatic Representation

Himaya, as stated above will be designed as an add-on for emails. Initially, it will target Gmail servers using as a Gmail add-on using Google Apps Script, which is based on JavaScript.This design allows for seamless integration with existing Gmail systems in healthcare organizations. So, it will be integrated with the existing Gmail servers in healthcare organizations.

When a user opens an unread email, the Himaya add-on activates and starts working right away, making it easy to use without interrupting email functions. Himaya will then go ahead to scan the email for any links and attachments, leveraging VirusTotal and MalwareBazaar to identify any known ransomware signatures. Once a potential threat is detected, the system generates alerts. These alerts will feature audio and visual notifications, promptly informing healthcare staff of the threat.

How our solution directly solves the problem:

Himaya tackles ransomware threats in healthcare by monitoring emails and identifying risks before they compromise sensitive patient data. This proactive approach helps prevent breaches that could disrupt patient care and lead to significant financial losses for healthcare organizations. By sending timely alerts with actionable insights, Himaya enhances patient safety and reduces the risk of medical errors or treatment delays caused by compromised data. Additionally, by preventing ransomware from infiltrating Hospital Management Systems (HMIS), the solution helps organizations avoid costly ransom payments and recovery expenses,

empowering them to maintain patient trust and deliver quality services without the threat of cyberattacks.

Assumptions Made

In developing this solution, several key assumptions will be made to guide the design and implementation:

1. That email communication will continue to be the primary attack for ransomware in Kenyan hospitals. This assumption is based on the widespread use of email for communication within hospitals and the historical data indicating that email is a common entry point for malware.
2. That hospital will be willing to invest in Cybersecurity solutions to prevent costly ransomware incidents.
3. That integration of threat intelligence databases will remain effective and up-to-date, ensuring that the solution can adapt to emerging threats.

VALUE PROPOSITION

Our seamless integration into existing email systems and real-time threat detection enables proactive risk mitigation, maintains uninterrupted healthcare services, and protects sensitive health data.

DESIGNED SOLUTION

Technologies Used

1. Google Apps Script

We chose Google Apps Script, a JavaScript-based framework specifically designed for integrating and automating tasks within Google products. This choice allows Himaya to integrate seamlessly with Gmail, the email service provider we are working on in the first phase. This enables real-time scanning and alerts without disrupting user experience.

2. VirusTotal API

The VirusTotal API was selected for its extensive database of malware signatures. It provides detailed analysis and reporting of URLs and files, helping to identify potential threats effectively. Leveraging this API enhances Himaya's ability to deliver accurate and timely threat detection.

3. MalwareBazaar API

The MalwareBazaar API grants access to a wide range of malware samples and threat intelligence data. Its incorporation broadens Himaya's understanding of ransomware variants, improving detection capabilities.

4. OTX AlienVault API

The OTX AlienVault API offers vital threat intelligence, including insights on emerging threats and vulnerabilities. Utilizing this API enables Himaya to stay updated with real-time data for proactive threat identification.

Integrating these three APIs significantly enhances Himaya's accuracy, ensuring comprehensive protection against a wide array of ransomware threats.

Screenshots of Main Modules

Module 1: Activation

This module demonstrates the activation process for Himaya. Once set up as an add-on to an email server, as shown on the right of the screencast, a user just needs to open their Gmail interface and Himaya activates automatically, to begin protection against ransomware threats.

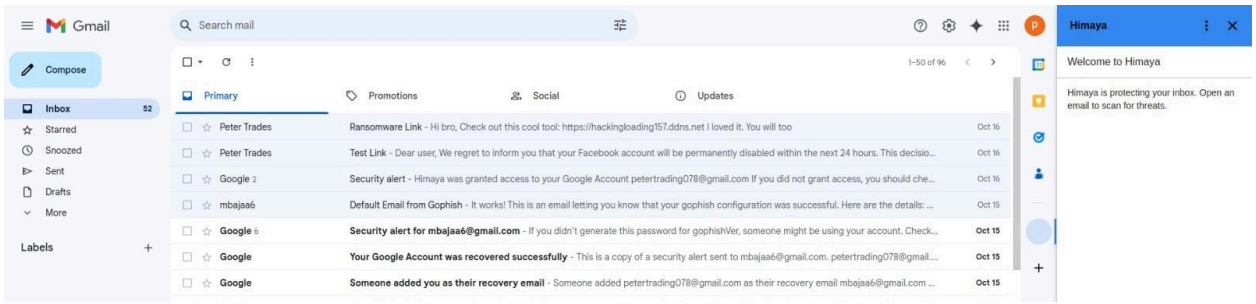


Figure 2: Himaya is activated once Gmail is opened

Module 2: Threat Analysis and Alerting

In the following screencast, Himaya scans links attached to the email for potential ransomware threats. It uses threat-intelligence databases like VirusTotal, MalwareBazaar, and OTX AlienVault API. The system analyzes the link's safety and provides users with real-time feedback.

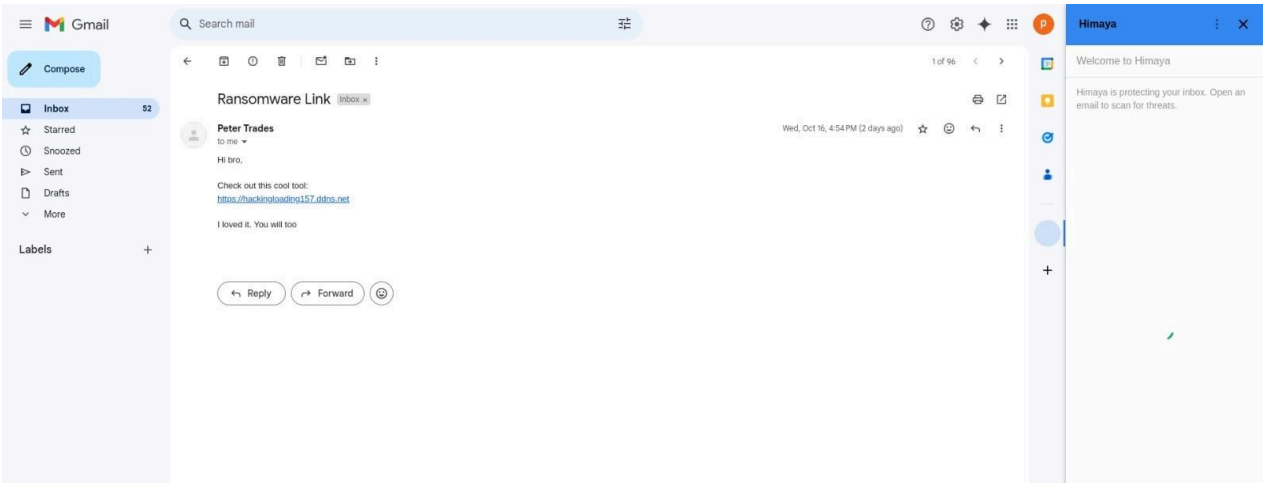


Figure 3: Himaya scanning for Ransomware Signatures that may be attached to the link

Once ransomware is detected within the system, users receive an alert. The notification includes both a message and an audio pop-up that ensures users are aware of the risk.

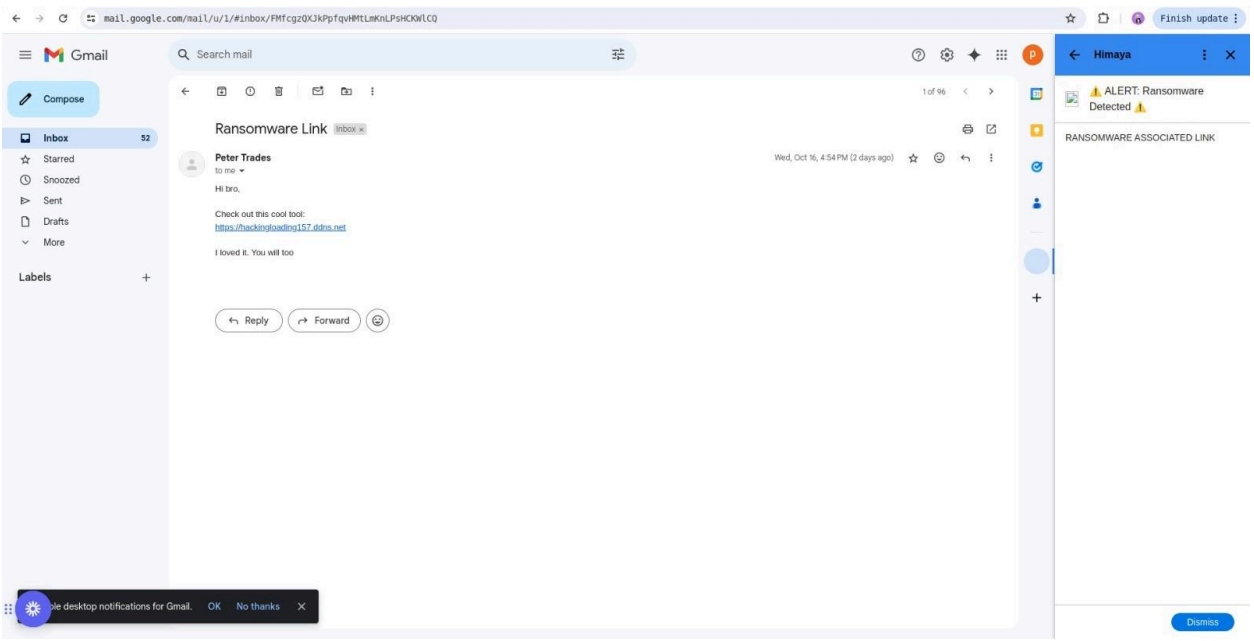


Figure 4: Himaya alerting the user that Ransomware has been detected

Himaya also offers scanning capabilities for documents attached to emails. Figure 4 showcases how the application checks documents for ransomware threats and alerts the user.

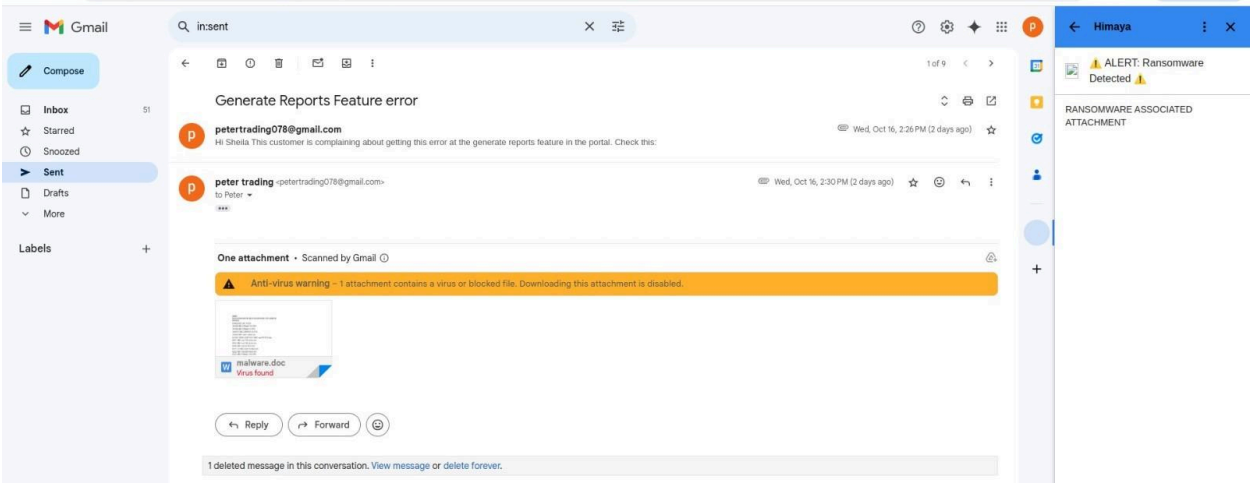


Figure 5: Himaya alerting the user that there is Ransomware attached to the document

Finally, if the attachments to an email are deemed safe as shown in Figure 6 below, Himaya flags them accordingly.

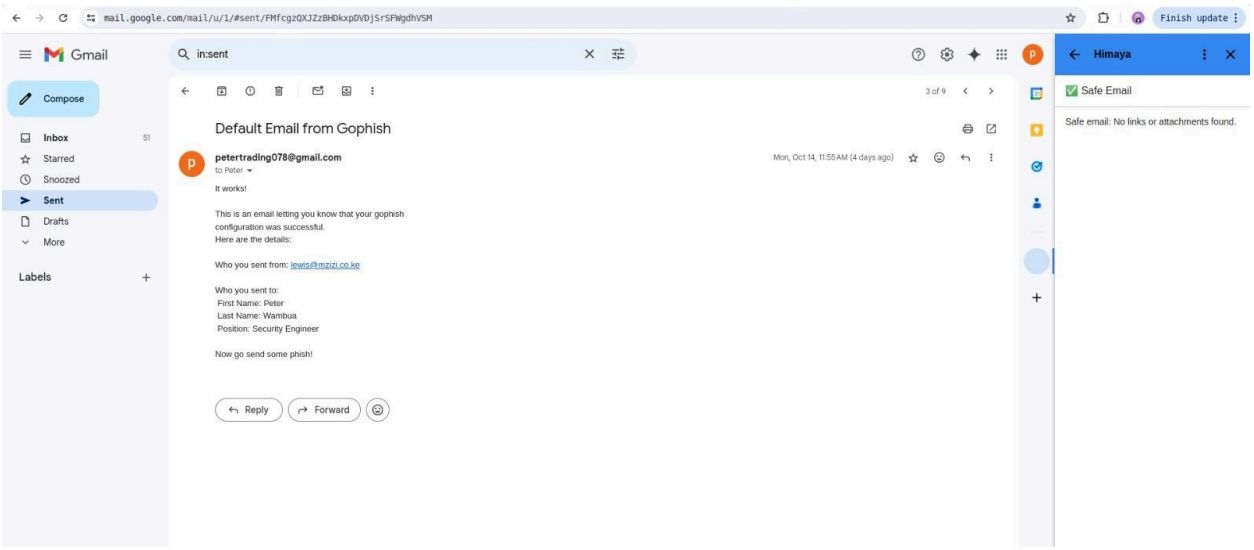


Figure 6: A safe email as detected by Himaya

Link to the solution

https://github.com/Wambuapeter/Himaya

Himaya

BUSINESS MODEL

Himaya's business model generates revenue through a freemium-to-premium structure. The freemium tier offers basic ransomware detection and limited email scans at no cost, making it accessible for smaller clinics and healthcare facilities. This free version helps attract users, allowing them to experience the essential protection offered by Himaya while building trust and credibility within the healthcare industry. The premium subscription model is designed to scale with the needs of larger hospitals. It offers advanced features like unlimited email scans, with subscription pricing based on the size of the hospital and the volume of email activity. This ensures affordability for smaller institutions and flexibility for larger organizations that require more comprehensive protection.

To ensure financial sustainability, we plan to partner with HMIS providers, integrating our email security solution into their software packages. This strategy leverages the growth of tech in healthcare and provides direct access to a larger market, generating shared revenue streams. Beyond partnerships, Himaya will drive expansion through targeted marketing efforts, such as SEO and email marketing, ensuring we continue to attract and engage clients independently.

RESPONSIBLE COMPUTING

Himaya is designed to uphold key principles of responsible computing by addressing privacy, accountability, inclusivity, and accessibility to ensure that all healthcare facilities using Hospital Management Information Systems (HMIS) in Kenya are protected from ransomware attacks.

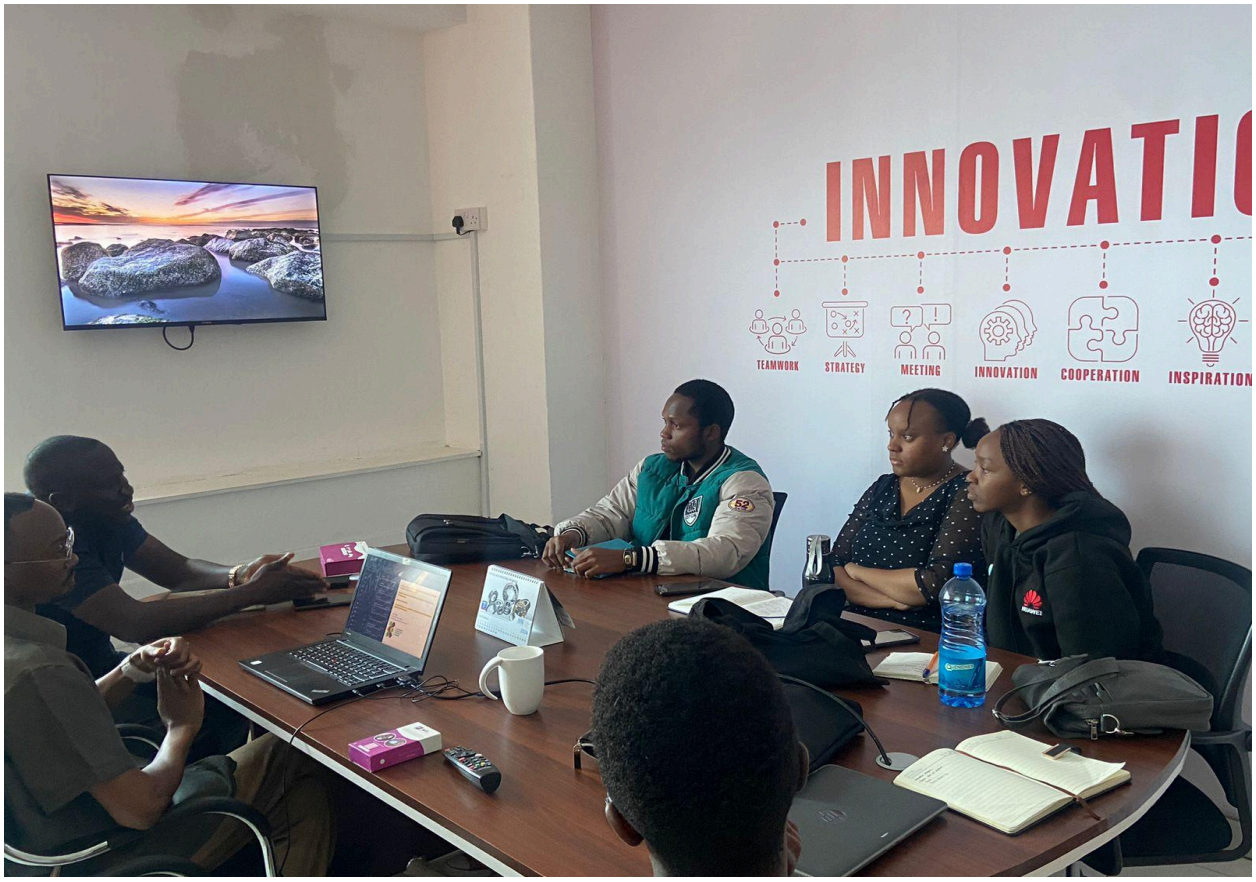
1. **Privacy**: Himaya prioritizes data security and privacy in three critical ways. First, it employs strong authentication mechanisms to ensure that no unauthorized users can access the tool, safeguarding sensitive information. Second, Himaya uses HTTPS, a secure protocol, to protect communication between users and the system. Finally, the tool adopts a data minimization approach, meaning it only scans emails for ransomware in real-time and does not store any information after the process is complete, ensuring that data is not retained beyond its intended purpose.
2. **Accountability**: Himaya operates transparently by informing users during installation that it will have access to their emails. Moreover, we prioritize obtaining informed

consent from users before scanning their emails, ensuring they understand the tool's purpose and how to respond to potential threats. Additionally, Himaya integrates with multiple threat intelligence databases, including Malware Bazaar, VirusTotal, and OTX, to validate the accuracy of detected ransomware signatures. This ensures that only legitimate threats are flagged, minimizing false positives and confirming that alerts originate from credible sources rather than unverified or speculative data.

3. **Inclusivity**: Himaya is designed to include all healthcare institutions in Kenya that use HMIS, including private hospitals, clinics, and public hospitals. By ensuring comprehensive protection for all types of healthcare facilities, Himaya aims to facilitate undeterred access to healthcare services, regardless of the size or type of institution.
4. **Accessibility**: Himaya ensures accessibility for healthcare facilities of all scales by offering flexible pricing models that cater to their financial capacities. Smaller hospitals or clinics can use the tool for free on a limited number of machines, while larger facilities can opt for premium plans based on the number of machines they need to protect. Additionally, Himaya is user-friendly, featuring both visual and audio notifications that are easy to recognize, making ransomware alerts noticeable to everyone. The tool does not require any technical background to use, with just minimal training provided upon installation. This ensures that every user, regardless of technical expertise, can comfortably operate the system, further enhancing accessibility.
5. **Biasness:** Himaya addresses bias through two key strategies. First, it utilizes threat intelligence from multiple sources, including VirusTotal, OTX, and Malware Bazaar. While each database is reliable on its own, relying on just one could introduce bias by potentially missing specific ransomware threats. To mitigate this, Himaya combines these sources to create a more balanced and comprehensive detection system. Second, to tackle the bias of alert fatigue, our system generates audio and visual alerts only when a confirmed ransomware threat is detected. This targeted approach minimizes unnecessary notifications, ensuring that users remain responsive and engaged while reducing the risk of desensitization from frequent false alarms. This careful balance allows users to stay vigilant without experiencing excessive disruptions.

TRACTION

We have engaged in discussions with Xantonn Group, an HMIS provider serving approximately 50-100 hospitals in Kenya, to understand their system's functionality and explore how our tool, Himaya, can integrate as an added software solution to enhance HMIS security.



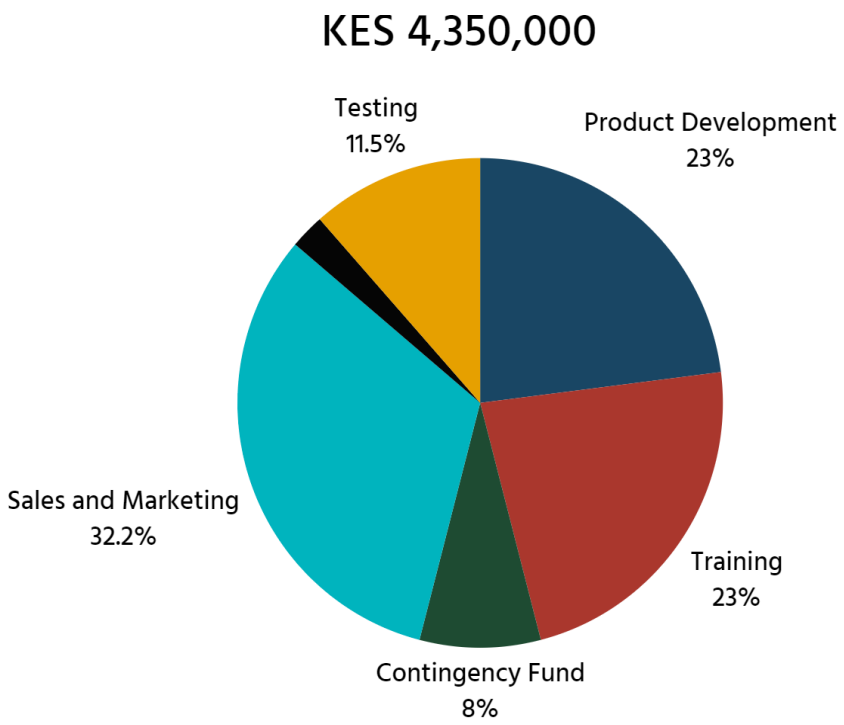
Meeting with Xantonn Group, HMIS Providers

FUNDING/SUPPORT NEED

To bring Himaya to these healthcare organizations, we require funding. Himaya is entering the pilot phase to develop, test, and launch its cybersecurity solution. The pilot will cover the next 12 months, followed by a growth phase extending to three years. The following breakdown covers the anticipated expenses and funding requirements.

Pilot Plan Funding

Category	**Description**	**Estimated Cost in Kenya Shillings**
Product Development	Cloud Infrastructure, Ransomware detection, and email scanning	1,000,000
Training and support	Training hospital IT staff and providing technical support	1,000,000
Sales and Marketing	Brand building, visibility, and customer acquisition through Search Engine Optimization (SEO), Sales Team, and Email marketing campaigns	1,400,000
Legal and Compliance	License registration, Certificate of incorporation, and CAK licensing	100,00
Pilot Testing	Partnering with at least one clinic to test the platform	1,000,000
Contingency Fund	Unforeseen expenses	350,000



Post-Pilot Funding (Years 2-3)

Following the pilot stage, Himaya will focus on scaling operations and refining the platform while expanding its customer base. The projected cost for this post-pilot phase is ksh 8,200,000. This includes ksh 2,000,000 for product enhancement to cater to other email service platforms, cloud infrastructure expansion, and integration of advanced features such as a guide on actions to take once an alert is sent. Additionally, ksh 3,000,000 will be allocated for sales and marketing efforts to penetrate new regions and hire a dedicated sales team. Compliance and certification costs are estimated at ksh 200,000. Finally, collaboration with HMIS providers is projected to cost ksh 3,000,000.

In total, the funding requirement for both the pilot and post-pilot phases amounts to ksh 13,050,000. This funding will ensure Himaya's successful development, compliance, marketing, and operational growth in the competitive cybersecurity landscape, ultimately safeguarding healthcare data.

TEAM

Abigael Mbugua- Project Lead and Threat Analyst

Abigael's role as both the project lead and the threat analyst includes overseeing the development and implementation of Himaya, ensuring that the project stays on track and meets its cybersecurity goals. As a threat analyst, she manages the integration of threat intelligence databases and analyzes ransomware signatures and suspicious email patterns. Her leadership ensures team coordination, while her analytical expertise ensures that Himaya stays updated with the latest ransomware trends and threats.

Peter Wambua- Penetration Tester

Peter’s role as a penetration tester in Himaya involves identifying security vulnerabilities in the email monitoring tool by simulating phishing attacks and testing for weaknesses in its integration with email servers. He ensures Himaya’s ability to detect and block ransomware attempting to bypass its defenses and provides recommendations for enhancing its security.

Linet Ithara- Network Security Engineer

Linet, as a network engineer for Himaya, ensures secure integration of the email monitoring tool with healthcare email servers like Gmail. She configures the system for seamless communication with external threat intelligence databases, secures network traffic, and maintains the network's integrity. She also handles the project documentation.