Ministry of Health and Welfare (2024) - Public Sector

Procurement of Integrated Security Management System
(Security Monitoring Analysis and Collection System)

Client Overview

The Ministry of Health and Welfare (MOHW) is a central administrative agency of the Republic of Korea responsible for the health and welfare of its citizens. With the goal of 'realizing an inclusive welfare state where all citizens enjoy a healthy and happy life,' the Ministry establishes and implements various policies, including disease prevention and management, medical service delivery, health insurance operations, and social welfare service support. Key responsibilities include operating the health insurance system, improving the quality of medical services, managing the prevention of infectious and chronic diseases, supporting medical expenses for vulnerable groups, and providing social welfare services for the elderly, the disabled, and children. The Ministry is dedicated to continuously promoting public health and enhancing the quality of life.

Deployed Products & Services

eyeCloudXOAR v4.0 – SIEM
(Integrated Security Analysis Solution)

eyeCloudXOAR v4.0 – SOAR
(Integrated Security Response Solution)

Background

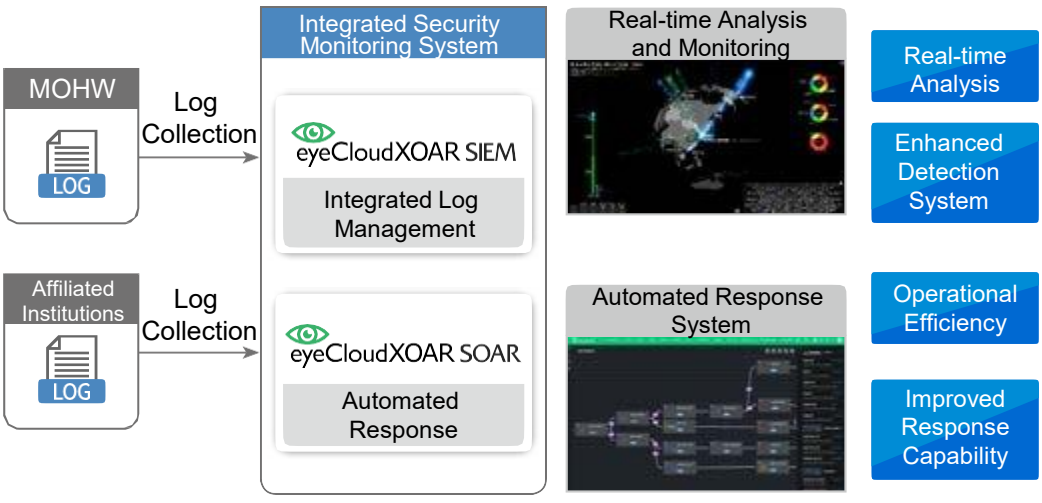
Through the Integrated Security Monitoring System Restructuring Project, the MOHW upgraded aging infrastructure and established an automated framework to enhance operational efficiency. This addressed existing limitations in protecting vast medical and administrative data while ensuring real-time detection of increasing cyber threats.

By implementing SIEM for integrated log analysis from medical and affiliated institutions and utilizing SOAR for automated response, the Ministry streamlined its security posture. The development of playbook-based processes enabled rapid response to major threats, including web hacking and malware. Consequently, the MOHW accelerated detection and response speeds, securing a systematic and automated operations environment.

Project Period

Feb 2024 – Sep 2024

Concept map



Solution

Advanced Big Data Security Monitoring & Automated Response System

The MOHW restructured its aging security monitoring system through automation to strengthen real-time threat detection and response. This project established a big data clustering-based integrated monitoring system for effective collection and analysis of massive security logs, alongside an automated response process.

To overcome previous limitations in individual log management across affiliated institutions and medical centers, the Ministry integrated and normalized data from 432 security devices. Detection capabilities were further reinforced by migrating and validating 100% of the 783 existing detection policies.

Additionally, a SOAR-based system now automates responses for 10 major threat types including web hacking and malware. API integration for firewalls enables automated blocking and remediation.

This project established an advanced security monitoring framework for protecting health and medical data, ensuring a more rapid and precise operations environment through automated threat detection and response.

Benefit

Integrated Security Monitoring & Enhanced Automated Response for Health and Medical Data Protection

The MOHW significantly bolstered its cyber threat response capabilities by restructuring its aging security monitoring infrastructure to align with the evolving digital landscape.

Key achievements include the integrated management of vast security logs from affiliated medical institutions and the 100% migration and validation of existing system detection policies. The application of a SOAR-based automated system automates the proactive detection of major security threats.

The Ministry established a SOAR-based automated response system, implementing automated processes for 10 major threat types, such as web hacking, abnormal communications, and malware. This automated framework reduced workloads for security personnel while significantly accelerating response speeds.

This integrated and automated approach has strengthened the MOHW's cybersecurity capabilities and solidified the security foundation for national health and medical data.

Summary

1. 24/7 automated threat response through 432 device integration across 92 affiliates, maximizing Cyber Security Center efficiency
2. Secure monitoring system via stable infrastructure integration and seamless migration
3. Automated security operations for enhanced medical data protection and cybersecurity capabilities