Korea Internet & Security Agency (KISA) (2024) - Public Sector

2024 Collaboration-Based Integrated Security Model Development Pilot Project

Client Overview

The Korea Internet & Security Agency (KISA) is a quasi-governmental institution (commissioned-service type) under the Ministry of Science and ICT, responsible for internet promotion, information security, and international cooperation. As a specialized agency for information security, KISA focuses on expanding cyber safety nets, fostering the data economy, and spearheading innovative services based on emerging technologies such as blockchain and 5G. The agency also concentrates on nurturing ICT and information security industries and talent.

Deployed Products & Services

- **eyeCloudXOAR v4.0 – SIEM** (Integrated Security Analysis Solution)
- **eyeCloudXOAR v4.0 – SOAR** (Integrated Security Response Solution)
- **OPEN XDR** (Open Extended Detection Response Integrated Security Platform)

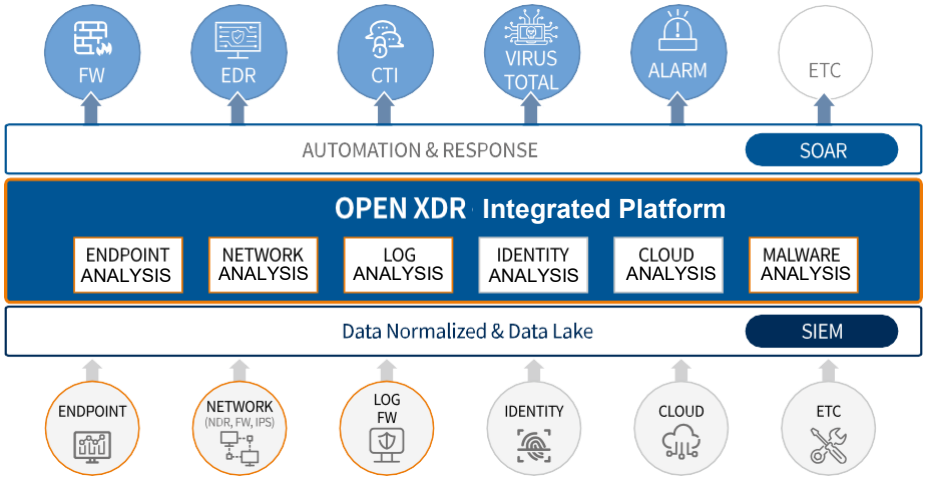
Background

KISA launched this pilot project to resolve operational inefficiencies by integrating fragmented security solutions into a unified threat detection and response system. Previously, independent operations of individual systems hindered the correlated analysis of security data across SIEM, EDR, and NDR, leading to inconsistent threat detection. This has weakened the domestic security market's competitiveness, raising concerns about potential exclusion from the global market. To resolve these issues, KISA initiated the OPEN XDR project as part of the 2024 Collaboration-Based Integrated Security Model Development Pilot Project.
This project aims to bolster cyber threat response and market competitiveness by building an open security platform. Key focus areas include integrating diverse security solutions, promoting threat intelligence sharing and cooperation, and advancing the technical capabilities of the domestic security industry. Through the OPEN XDR project, Seculayer expects to lead innovation in the domestic security market and contribute to a secure digital environment.

Project Period

May 2024 – Nov 2024

Concept map



Solution

Strengthening Threat Response and Operational Efficiency via a Collaboration-Based Integrated Security Platform

KISA established an open architecture (OPEN XDR) integrated security model to enhance connectivity and data integration across diverse security solutions. This model maximizes operational efficiency by improving security event analysis accuracy and establishing a rapid response framework.
Previously, independent operations of individual solutions led to inconsistent threat detection and limited correlated analysis. This project unified SIEM, EDR, and NDR to enable centralized threat detection and enhanced security event connectivity through real-time correlated analysis.
With API-based standard integration, KISA ensured compatibility among various solutions and built a collaboration-based threat intelligence sharing system. This resulted in a scalable security model applicable across diverse sectors, including public and financial institutions.
Through this initiative, KISA optimized cross-solution integration and established an environment to maximize monitoring efficiency via real-time threat detection and automated response.

Benefit

Open XDR-Based System for Real-Time Threat Response and Security Operations Optimization

KISA enhanced real-time threat detection and response by shifting from siloed operations to an Open XDR-based integrated security model.
By integrating SIEM, EDR, and NDR, KISA established a framework to identify latent threats that were previously difficult to detect using independent solutions. Furthermore, applying SOAR-based automated response reduced the time from detection to remediation of security events while minimizing operational overhead.
API-based standard integration ensured compatibility across security solutions and established a collaborative threat intelligence sharing system. This scalability enabled a versatile security model applicable to diverse sectors, including public and financial institutions.
Through this initiative, KISA optimized cross-solution integration and established an environment to maximize monitoring efficiency via real-time threat detection and automated response.

Summary

1. OPEN XDR Integrated Platform for Unified Security Management and Threat Response
2. API-based integration for enhanced scalability and threat intelligence sharing
3. OPEN XDR deployment for reduced detection/response time, lower operational costs, and optimized integration