Korea Exchange (KRX)
(2023) – Financial Sector
Unified Security Management System Reconstruction for Enhanced Intelligent Cyber Attack Response

Client Overview

The Korea Exchange (KRX) is an institution established to ensure fair price formation, seamless trading of securities and derivatives, and efficient market management. By reconstructing its unified security management system across geographically separated locations, including the Busan headquarters and Seoul office, as well as environmentally separated networks such as the internet and internal business networks, the KRX has strengthened its response capabilities against new and evolving intelligent cyberattacks driven by digital transformation.

Deployed Products & Services

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

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

Background

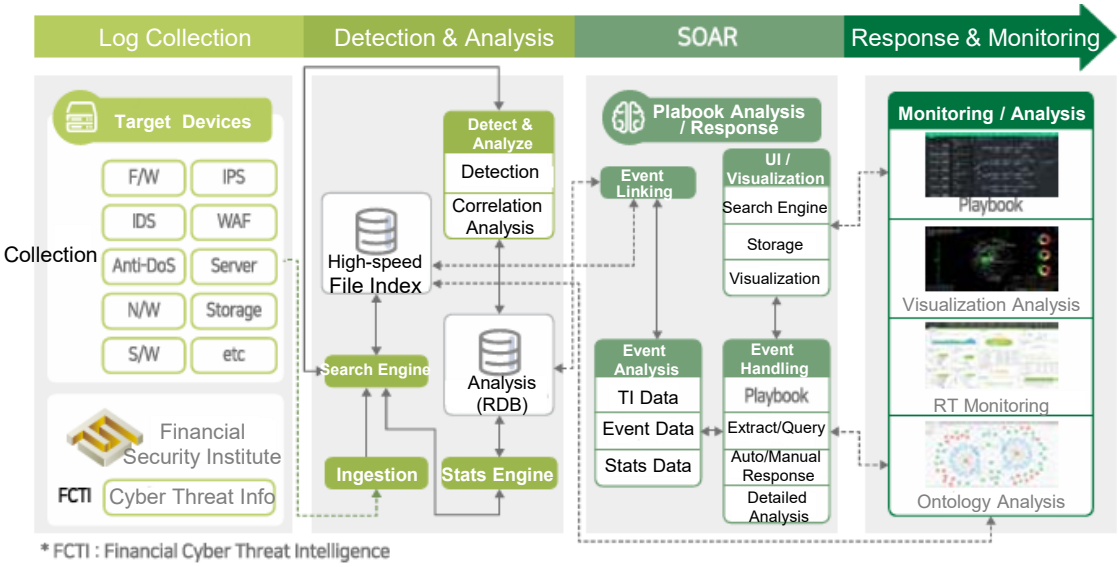
As the frequency and sophistication of cyberattacks continue to rise rapidly, legacy security operations systems, which are limited to single-event processing on single servers, have become inadequate for analyzing and responding to new cyber threats. Accurately analyzing surging cyberattacks with limited personnel required expanding the scope and targets of log collection, while rapidly responding to vast amounts of data necessitated a distributed processing-based data collection and analysis platform.

To reconstruct its system with a proven solution, KRX selected Seculayer's eyeCloudXOAR SIEM and SOAR products. Validated for their proprietary distributed data processing technology, accurate and consistent hybrid analysis, and flexible complex scenario analysis, these solutions were chosen for their track record managing Korea's largest daily data processing site (40TB/day) and extensive deployment experience in the field.

Project Period

Apr 2023 – Aug 2023

Concept map



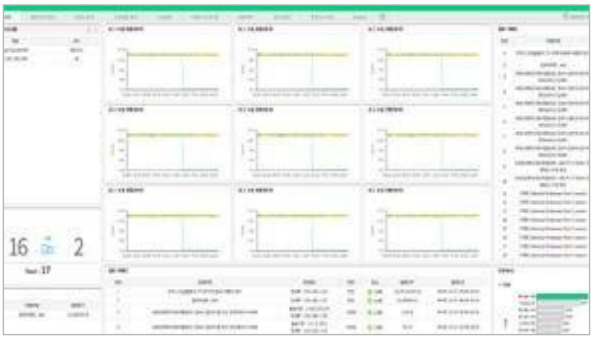
Solution

For security operations, KRX integrated approximately 300 security devices and information systems to collect around 300GB of data daily, establishing a SOAR-based operational response framework utilizing playbooks specialized for KRX business processes and FCTI threat intelligence from the Financial Security Institute.

Various dashboards for monitoring critical information are currently in operation, with customized dashboards tailored to individual job functions used for daily tasks.

Integrated Dashboard

Performance Monitoring Dashboard



Benefit

By extracting the routines and characteristics of known security threats and registering them as events, threats can be identified immediately upon occurrence. Automation further enables identification of a wider variety of new threats and expands the scope of breach analysis and response, allowing for rapid detection and mitigation of emerging threat patterns.

Through FCTI integration, KRX is building a more robust security network by continuously sharing new threats across various institutions. Security management processing time has been reduced to one-sixth of its previous duration, enabling significantly faster responses to new threats.

Summary

1. Establishing 4th-generation SIEM and SOAR to overcome the collection scope and performance limitations of 3rd-generation ESM
2. Preemptive response to financial security threats through FCTI threat intelligence-based correlation analysis
3. Establishing failure and performance monitoring systems alongside security operations