Kwangju Bank (2024) – Financial Sector

EMS System Upgrade Project (Three-Phase Incident Response Implementation)

Client Overview

Kwangju Bank, established in 1968, is a South Korean regional bank and a subsidiary of JB Financial Group. Based in Gwangju Metropolitan City and Jeollanam-do, the bank contributes to revitalizing the local economy. It provides various financial products and services to individual and corporate customers and enhances customer satisfaction through its convenient digital banking services. Recently, the bank has been actively expanding into overseas markets while also focusing on social contribution activities.

Deployed Products & Services

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

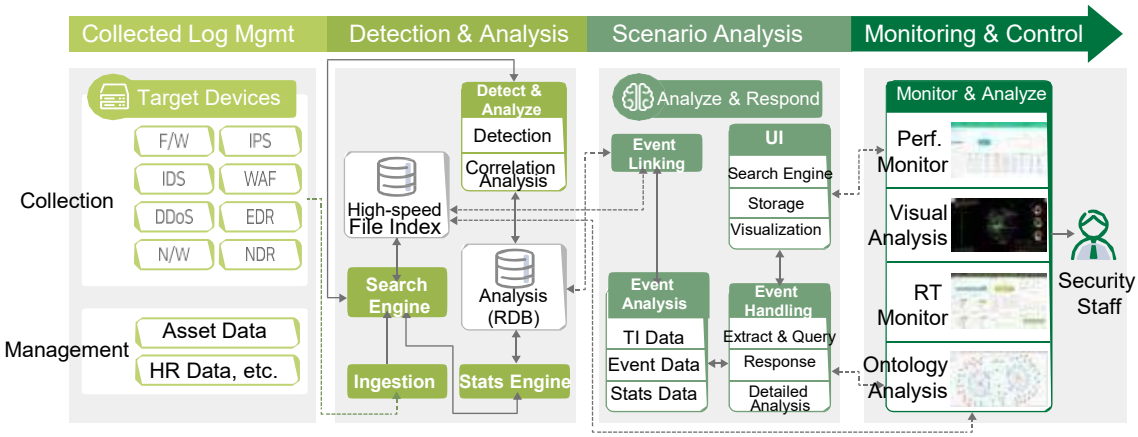
Background

As the digital financial environment evolves rapidly, Kwangju Bank established a unified security operations framework to counter increasingly sophisticated cyberattacks and ensure financial service continuity. In the financial sector, a core industry responsible for protecting customer assets and personal information, security threats can lead to direct damage and loss of trust if they escalate into financial incidents. Consequently, the bank required a system capable of comprehensively analyzing and responding to diverse security threats arising across internal systems and customer transactions.
Legacy security operations faced challenges as individual security solutions operated independently, resulting in fragmented log collection and analysis, which hindered real-time threat detection. Furthermore, the inability to effectively analyze and respond to the surge in security events posed a risk to the stability of financial services.
Accordingly, Kwangju Bank introduced a SIEM-based unified log analysis framework to centrally manage security events from its financial IT infrastructure and established an environment to reflect the latest financial security threat intelligence in real time through FCTI integration. Additionally, by strengthening endpoint and network security through EDR and NDR integration, the bank established a system for rapid threat detection and response, aiming to prevent financial security incidents and foster a reliable operating environment.

Project Period

Dec 2023 – Apr 2024

Concept map



Solution

Establishing a Unified Security Operations Framework to Strengthen Financial Security

Kwangju Bank deployed a SIEM-based unified security operations framework to enhance cyber threat response capabilities and provide more stable financial services. Through this initiative, the bank strengthened FCTI integration to collect and analyze finance-specific threat intelligence in real time, improving its responsiveness to cyberattacks.

Previously, independent operation of various security solutions hindered correlation analysis between security events, and the fragmented response frameworks limited rapid action. To address this, Kwangju Bank utilized SIEM to centralize log collection across its financial IT infrastructure and established a system to reflect the latest financial security threats in real time via FCTI integration. Furthermore, threat analysis for endpoints and networks was conducted through EDR and NDR, further strengthening financial service protection levels.

Through this deployment, Kwangju Bank strengthened its threat detection and response capabilities and secured a foundation for delivering safer financial services by establishing a tailored security framework through the integration of FCTI, EDR, and NDR.

Benefit

Enhancing Cyber Threat Response Capabilities by Establishing a Tailored Financial Security Operations Framework

As security threats in the digital financial environment continue to rise, Kwangju Bank established a unified security operations framework to enhance service stability and customer trust. The financial sector is required to maintain robust security systems to protect sensitive customer data and comply with domestic and international regulations, making sophisticated and systematic security operations essential.

Through this deployment, Kwangju Bank centralized the management of security logs across its financial IT infrastructure using SIEM and optimized the real-time reflection of finance-specific threat intelligence via FCTI integration. Additionally, endpoint and network security were reinforced through EDR and NDR integration, enabling preemptive responses by comprehensively analyzing threats within the financial system. This established an environment that provides visibility into security events and allows for faster, more precise analysis of threat types that occur frequently in the financial sector.

Through this project, Kwangju Bank secured the capability to preemptively respond to the rapidly changing financial security landscape, satisfied regulatory requirements, and established a foundation to increase the reliability and efficiency of security operations over the long term. This initiative established a framework to prevent security incidents and ensure financial service continuity.

Summary

1. Establishing a finance-tailored security operations framework through next-generation SIEM adoption to overcome the limitations of legacy ESM
2. Executing a seamless three-phase transition to overcome legacy system limitations and ensure security operations continuity
3. Expanding and enhancing analysis coverage through integration of previously unlinked devices and EDR/NDR log collection