NH Information System (2023) – Financial Sector

Nonghyup Information Systems Unified Security Operations Enhancement Project

Client Overview

Nonghyup Information Systems, a subsidiary of the National Agricultural Cooperative Federation (NACF), provides system development and maintenance for the NACF, regional cooperatives, affiliates, and agricultural and fishery organizations, as well as financial institutions. As a competitive IT specialist, it effectively supports group-wide informatization and leads projects for the digitalization of the agricultural sector and rural communities.

Deployed Products & Services

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

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

Background

Operating IT infrastructure across the financial, distribution, and economic sectors, Nonghyup Information Systems required a more precise security operations framework, as security threats directly impact financial service stability and customer trust. Legacy systems focused on independent threat analysis and response, but the lack of real-time detection and correlation analysis caused delayed responses to complex security threats.

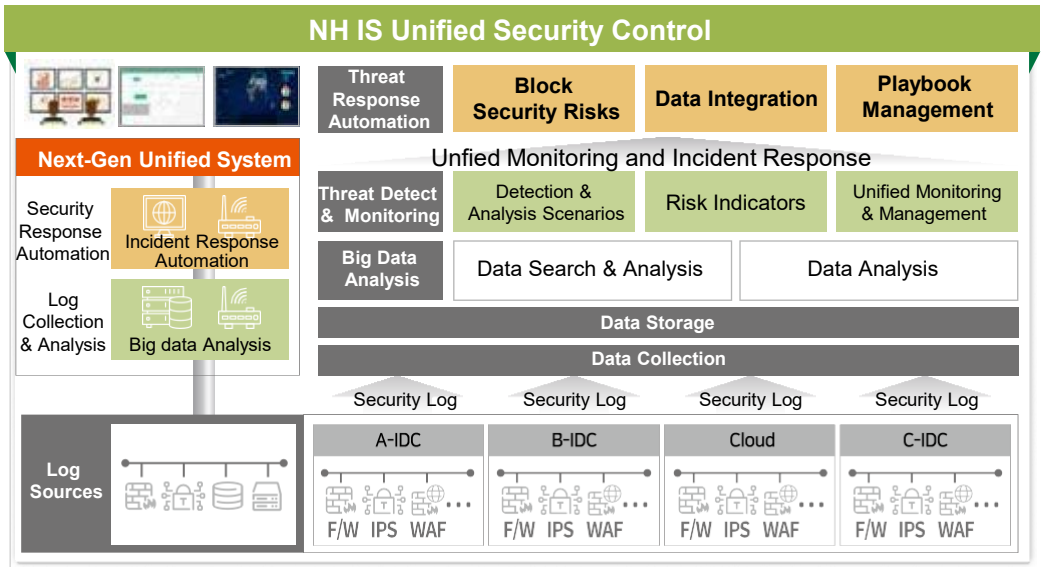
The Nonghyup IDC plays a critical role in providing IT services to NACF affiliates and external clients. As vulnerabilities in legacy systems risked degrading customer satisfaction through data breaches or system failures, Nonghyup Information Systems utilized SIEM for integrated analysis of system-wide security logs to detect threats preemptively and deployed SOAR to establish an automated response framework for security events occurring within financial transactions and internal operations.

With this, the company protected transaction data and transformed security event response from simple alerting into a cohesive system of analysis and action, strengthening the continuity and reliability of financial services.

Project Period

Dec 2022 – Jun 2023

Concept map



Solution

Establishing a Big Data-based Unified Security Operations Framework for Next-Generation Threat Response

Nonghyup Information Systems deployed a next-generation unified security operations system to strengthen response capabilities against hacking and infringement incidents while modernizing its security infrastructure. The company established a real-time log collection and analysis framework leveraging big data analytics and introduced an automated threat detection and response system.

Previously, analyzing massive volumes of security events individually and the lack of real-time detection frameworks limited threat response speeds. To address this, a big data-based architecture was introduced to process an average of over 80GB of logs daily in real time, significantly enhancing detection performance.

An automated response framework using SOAR enabled immediate action upon threat detection, with playbook-based processes optimizing security policy updates and blocking procedures.

The system was tailored to Nonghyup's financial IT environment to differentiate and analyze security events across internal and external transaction networks. Utilizing specialized Threat Intelligence (TI) data further increased threat response effectiveness and optimized security policies suited to the financial sector.

Benefit

Maximizing Stability and Operational Efficiency in Financial IT Environments

Nonghyup Information Systems upgraded its unified security operations system to preemptively respond to diverse security threats in the rapidly evolving financial IT landscape, automating the entire process of security event detection, analysis, and response to drastically improve real-time operational efficiency and response speeds.

By automating previously manual workflows, the system enables immediate action against real-time threats. SOAR-based automation for updating firewall policies and responding to threats within financial transaction networks has significantly strengthened customer data and financial service protection. A framework differentiating internal and external network security events has further refined security operations and enhanced external intrusion detection capabilities.

Refined log storage and audit frameworks for financial regulatory compliance have increased the efficiency of security audits and incident analysis, while improved accuracy and response speeds have bolstered financial service stability.

Through this upgrade, Nonghyup Information Systems has established a more secure and efficient financial IT environment, enabling the delivery of trusted financial services to its customers.

Summary

1. Advancing collaborative response processes, including real-time automated response, threat hunting, identification, and registration, via incident response automation within the next-generation unified security operations system
2. Strengthening incident response frameworks for IDC and NACF affiliate IT asset infrastructure
3. Securing the reliability of security operations by refining log management and audit frameworks for financial regulatory compliance