Korea Southern Power (KOSPO) (2024) – Public Infrastructure

Advancing AI-Based Security Operations System

Client Overview

Established in 2001 following its spin-off from KEPCO, Korea Southern Power (KOSPO) is a leading state-owned power generation utility. Headquartered in Busan, KOSPO operates key power plants nationwide including Hadong, Shin-Incheon, and Nam-Jeju to ensure a stable national power supply.
The utility produces electricity via coal, LNG, and oil, as well as renewable energy sources such as wind and solar power, and is actively developing eco-friendly energy.

Deployed Products & Services

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

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

Background

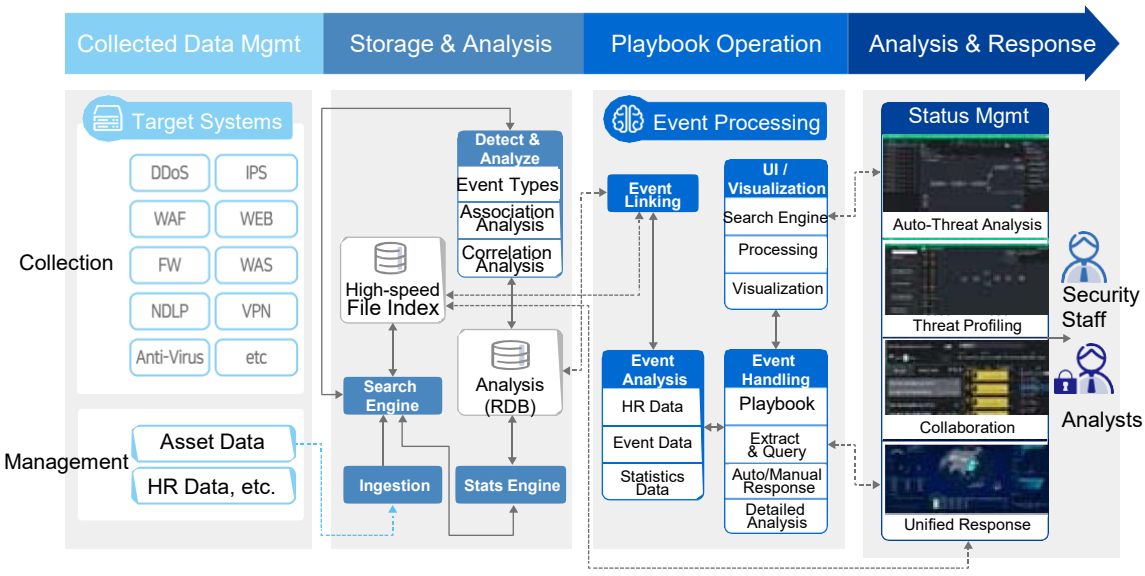
As an organization operating energy supply chains, KOSPO deployed a Unified Security Operations System to fortify the security of power plants and energy management systems against escalating cyber threats and to maintain a stable power supply. The legacy framework, centered on fragmented individual systems, faced limitations in comprehensive threat analysis and response regarding power infrastructure. This necessitated a systematic architecture capable of real-time detection and response to security events across critical facilities and IT infrastructure.

Through this initiative, KOSPO has established a foundation for sustainable power supply and secure energy operations maintaining the security of national strategic industries and enhancing responsiveness against cyber threats.

Project Period

Dec 2024 – Jan 2025

Concept map



Solution

Establishing a Unified Security Operations Framework to Protect National Energy Infrastructure

To protect energy production and supply chains as critical national industries and to enhance responsiveness against cyber threats, KOSPO deployed a Unified Security Operations System based on SIEM and SOAR.

Through this deployment, KOSPO advanced its security operations framework by utilizing SIEM for centralized management of security logs from power plants and core operating systems. This infrastructure enables real-time analysis of security events occurring across major facilities and remote power plants.

Furthermore, KOSPO maximized operational efficiency by establishing automated analysis and response processes via SOAR. To ensure immediate action against detected threats, the utility automated security policy updates and optimized security operations processes to prevent any impact on power plant operations.

Administratively, KOSPO reinforced long-term log storage and analytical capabilities, improving the precision of anomaly analysis across power plants and remote facilities. By refining audit systems for domestic and international energy security compliance, KOSPO elevated its security management capabilities as a critical national infrastructure operator.

Benefit

Protecting National Energy Infrastructure and Strengthening Cyber Response Capabilities

To ensure the stable operation of power production and supply chains as the core of national strategic industries, KOSPO deployed a Unified Security Operations System. As critical national facilities, power plants and energy management systems face high risks of physical damage and power supply disruptions in the event of cyberattacks.

Through this deployment, KOSPO established a centralized management framework for all security logs from power plants and remote facilities. By enabling real-time analysis of security events, the utility secured consistency in security operations and established an integrated response system for power grid protection.

Furthermore, KOSPO created an environment to rapidly block threats without impacting power plant operations by leveraging SOAR-based security automation. This optimization ensures swift incident response and maintains stable power supply without operational interruptions.

Through this initiative, KOSPO has enhanced the security of national energy infrastructure and established a framework for efficient, sustainable security operations amidst a rapidly evolving cyber threat landscape.

Summary

1. Establishing Unified Security Operations and Real-time Threat Response for Power Plants and Remote Facilities
2. Improving Response Speed and Power Plant Stability via SOAR-based Security Automation
3. Building Sustainable Security Operations through Enhanced Visibility of Power Grids and Major Energy Facilities