Korea East-West Power (EWP) (2023) – Public Infrastructure

Advancing AI-Based Security Operations System

Client Overview

Korea East-West Power (EWP) is a power generation utility spun off from KEPCO in 2001 following the government's power industry restructuring policy. With Dangjin Thermal Power as its core facility, EWP operates six power plants nationwide, including Ulsan, Honam, Donghae, and Ilsan Cogeneration.

Deployed Products & Services

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

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

Background

In 2016, aging infrastructure, specifically eyeCloudSIM v2.5 (Unified Log Management) and BlueBird (Incident Response), imposed constraints on data processing and analysis.

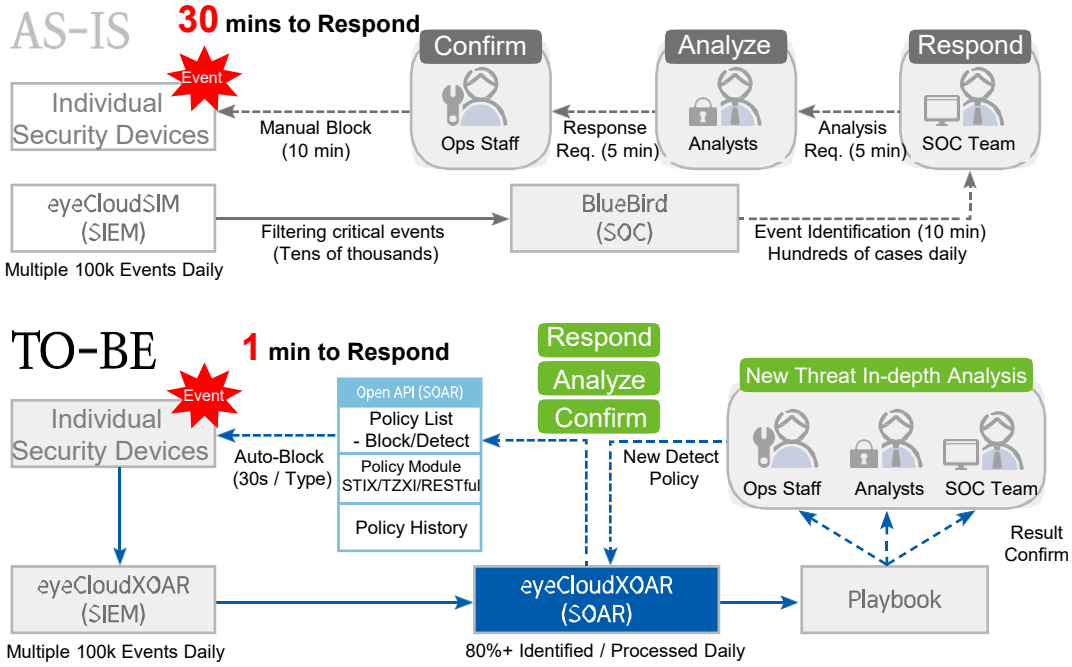
Consequently, EWP established plans to expand its system capacity to handle increasing log volumes and to deploy an automated ticketing system.

Considering integration with legacy products and the need for a seamless, non-disruptive migration of security operations, EWP selected and deployed Seculayer's eyeCloudXOAR v4.0.

Project Period

Jul 2023 – Dec 2023

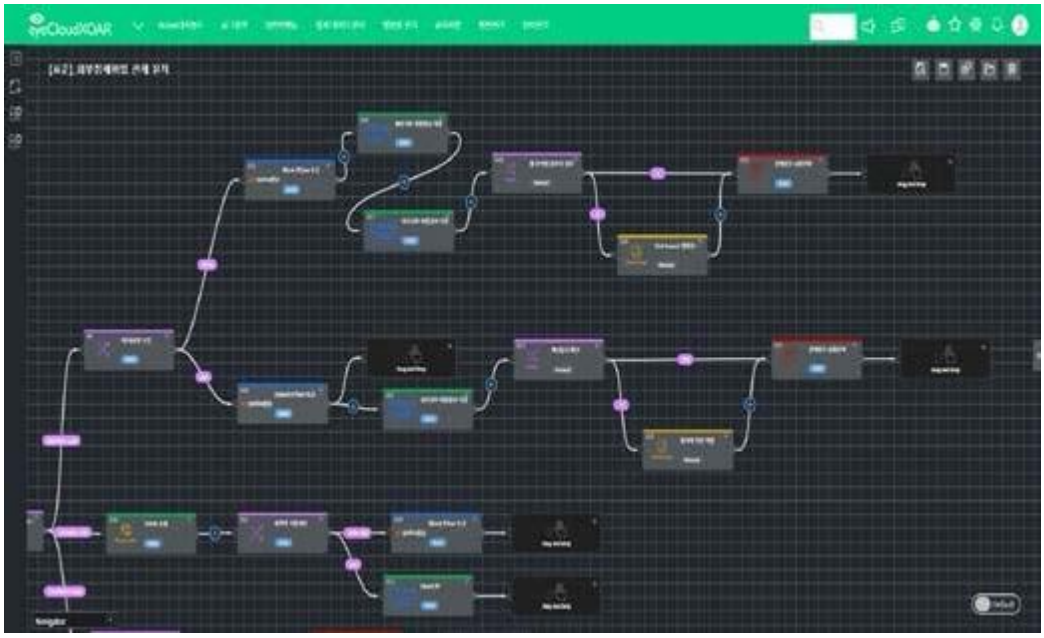
Concept map



Solution

By migrating legacy eyeCloudSIM and integrating new equipment, EWP connected approximately 100 units of security devices and servers and established a system capable of collecting and analyzing 100GB of data, or roughly 300 million logs, daily.

Through the implementation of automated playbooks, the system performs automated responses to an average of 50 security threats per day.



Benefit

By transitioning from manual workflows in the legacy Security Operations Center (SOC) to playbook-driven automation, EWP has automated its threat response operations.

This initiative ensures that all security personnel follow the same optimized response processes, resulting in the upward standardization of response quality independent of individual operator skill levels.

Notably, integration with Palo Alto Networks firewalls for automated blocking has drastically reduced security response times from 30 minutes to under 1 minute.

Furthermore, case-specific response statuses are now visualized for real-time monitoring and systematic management.

Summary

1. Upgrading from eyeCloudSIM v2.5 to eyeCloudXOAR v4.0
2. Applying Standardized and Automated Playbooks to Legacy Manual SOC
3. Reducing Response Time via Palo Alto Firewall Blocking
(30 mins → <1 min)