AhnLab

Case Study

Smarter Financial Security Monitoring with AhnLab SOAR

Industry

Full-Service Financial Group

Benefits

- Reduced security monitoring analysis and response time through process optimization
- Implementation of client-tailored security logic via flexible playbook design
- Visualization and systemization of the entire process from event detection to response
- Support for user-centric, intuitive workflow design
- Enhanced response capabilities based on Threat Intelligence (TI)

Solution

- AhnLab SOAR

Overview

Company K is a leading full-service financial group in Korea, offering a wide range of financial products, services, and solutions through more than 11 subsidiaries. Backed by exceptional risk management capabilities and a differentiated digital financial platform, the group is at the forefront of financial innovation.

In response to the wave of digitalization, Company K adopted AhnLab SOAR with the aim of automating security monitoring tasks while enhancing visibility and efficiency. Previously, events were manually analyzed and handled using a Security Information and Event Management (SIEM) system. With the introduction of SOAR, the group has systematically improved its security operations environment and automated processes across the board. In particular, SOAR automates first-level analysis of threat events, improving monitoring quality and enabling monitoring personnel to respond more quickly and accurately.

Following the adoption of SOAR, the security team has seen a visible improvement in operational efficiency and incident response capabilities. Seamless integration with various systems, including SIEM, firewalls, Unified Threat Management (UTM), and internal messaging platforms, has contributed to the advancement of security monitoring. Moreover, SOAR plays a key role in strengthening collaborative systems such as information sharing and joint response efforts with security personnel across subsidiaries. It is expected to become a core tool for expanding automation and efficiency in the group's overall security operations.

> By leveraging AhnLab SOAR, we were able to enhance detection event analysis by correlating TI information such as malicious IPs and hashes. We also reduced response time by approximately 10 minutes by automating repetitive tasks like attaching logs, blocking IPs, generating reports, and requesting approvals. Furthermore, the ability to flexibly design purpose-driven playbooks using various service actions and conditional branches greatly helped optimize our operations. In addition, AhnLab SOAR enabled full visualization of the entire process, from detection to response, allowing us to understand at glance the security operation flow and identify areas for improvement.
>
> *- Security Operations Manager at Company K*

Background of Solution Adoption

- Limitations of manual-centric security operations
- Personnel resource waste due to repetitive tasks
- Delays in response caused by the growing number of threat events
- Increasing need for an automation-based monitoring system

Implementation Background

Before the implementation of AhnLab SOAR, the security monitoring environment at Company K relied heavily on manual operations. Without a dedicated portal or automation system, events were detected through the SIEM platform, and monitoring personnel had to manually review logs, perform analyses, and carry out follow-up responses. This approach not only required significant time from detection to response, but also placed a continuous burden on personnel due to repetitive and routine tasks. As a result, it became increasingly difficult to maintain the quality of monitoring, and structural risks such as missed responses became more likely.

Amid these limitations, the need for a system that could ensure both continuity and efficiency in monitoring operations grew increasingly urgent. As the number of threat events surged, the manual, analysis-intensive process resulted in delayed responses and excessive alert processing burden. This made the establishment of a systematic threat management and automated response process an urgent priority.

Accordingly, Company K sought ways to reduce repetitive tasks and standardize its security operations workflow, ultimately selecting AhnLab SOAR as the solution.

AhnLab SOAR played a pivotal role in overcoming the limitations of the existing monitoring system and establishing an automation-based response framework. In particular, the automation of first-level analysis and the streamlining of repetitive tasks significantly boosted monitoring efficiency. In real-world operations, monitoring personnel experienced noticeable improvements, such as reduced response times and higher work concentration. These improvements laid a critical foundation for enabling the security operations team to concentrate on more strategic tasks.

Operational Use Case

AhnLab SOAR currently serves as the central hub of Company K's automated monitoring system by integrating with various security and operational systems. It integrates with key security infrastructure, including the internal security monitoring platform (SIEM), firewalls, the Threat Management System (TMS), and UTM, to automatically block malicious IPs upon detection. It also integrates with internal messaging and email systems, enabling fast reporting and seamless communication. This setup enables a seamless, automated security response system that covers the entire process from detection to response and reporting.

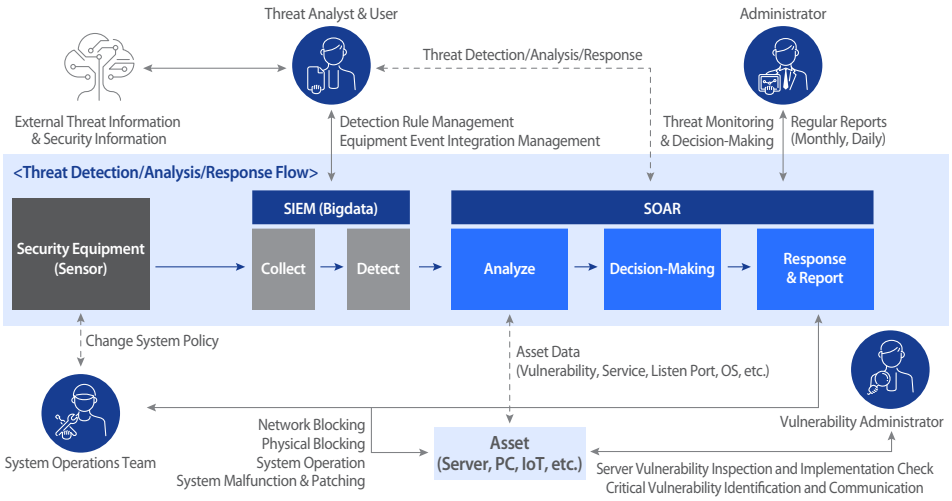

Figure 1. AhnLab SOAR's Response Process

Operational Use Case

- Implementation of automated security monitoring through integration with various systems
- Automated threat response using over 80 playbooks
- Enhanced proactive intelligence analysis capabilities
- Improved monitoring efficiency built on a stable operational foundation

In the current operational environment, over 80 playbooks are actively running, automating the handling of repetitive events and responses to a wide range of threat scenarios. While no security incidents involving specific threats such as ransomware or phishing have occurred so far, the correlation of TI data and detection events through SOAR has enabled advanced, proactive analysis using threat intelligence such as malicious IPs and hashes. As a result, detection accuracy has improved, and the monitoring team's ability to respond preemptively has also been strengthened.

From an operational standpoint, AhnLab SOAR is regarded as a stable system, and the user experience has also been satisfactory. Previously, the "Jupyter" feature was used to pre-test script nodes, and its removal following a version upgrade is a noted drawback. Nevertheless, the platform's powerful automation capabilities and flexible integration architecture continue to provide practical benefits to monitoring operations. With ongoing improvements and future expansion, even greater operational optimization is expected.

Implementation Benefits

Following the introduction of AhnLab SOAR, Company K was able to systematically advance its end-to-end monitoring process from detection to response. When an event occurs, SOAR automatically outputs all relevant information needed for analysis, including case history, attacker logs, and asset data. This allows monitoring personnel to quickly analyze the situation and efficiently carry out follow-up actions such as IP blocking and sending approval requests. As a result, the time required for event analysis and response has been reduced by approximately 10 minutes.

As the use of AhnLab SOAR gradually expanded, significant improvements were seen in monitoring operations. In particular, the automation of previously repetitive and time-consuming tasks led to a substantial reduction in the workload of the monitoring team. Additionally, the speed and accuracy of incident response have significantly improved, enabling more effective security operations.

Above all, the most satisfactory feature has been the playbook. With its support for a wide range of service actions, user-defined tasks, and conditional branches, the playbook functionality allows the security team to flexibly design response logic tailored to specific threats. Furthermore, by automating the task of disseminating external trends to security personnel of affiliates through AhnLab SOAR, satisfaction with the use of SOAR has increased across various departments. Some affiliates have even begun discussing their own use cases for SOAR, demonstrating a positive and growing interest in the platform.

Implementation Benefits

- Reduced average analysis and response time by 10 minutes
- Reduced work burden for monitoring personnel through automation of repetitive tasks
- Flexible response logic design using playbooks
- Improved speed and accuracy in handling security events
- Strengthened collaboration through automated information sharing among affiliates

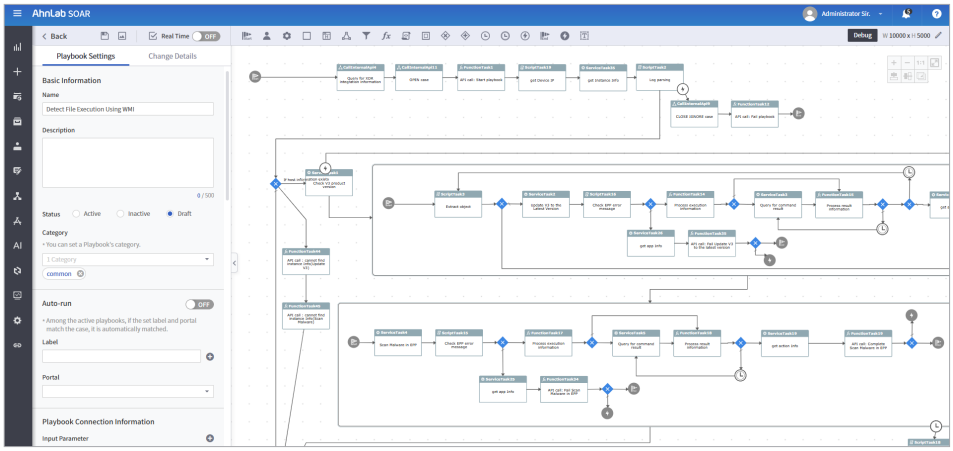

Figure 2. Built-In Playbook Provided by AhnLab SOAR

Future Plans

Company K aims to build an automated analysis process for security events by combining AI and machine learning (ML) with SOAR. Their goal goes beyond simply reducing repetitive tasks as they aim to integrate AI/ML-based analytical data with SOAR's response logic to minimize human intervention and establish a more precise and efficient response system.

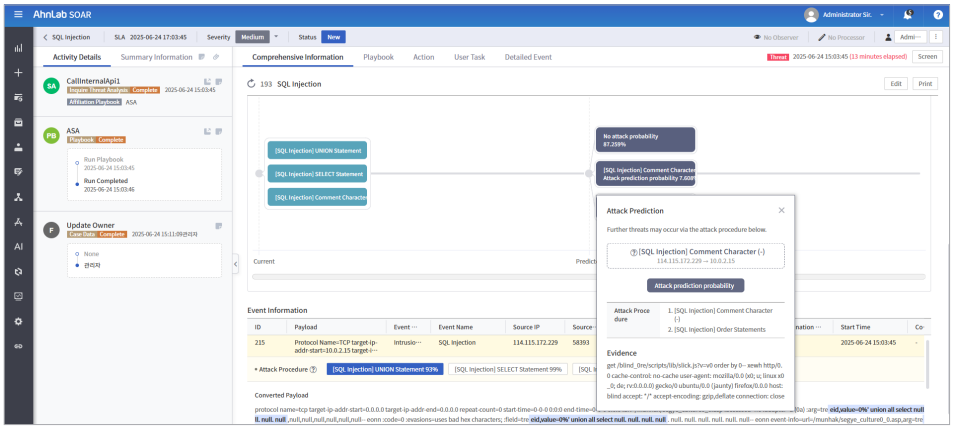

Figure 3. Proactive Response to Additional Attacks through AI-Based Correlation Analysis

In addition, the scope of AhnLab SOAR's application is expanding beyond security monitoring. Along with the advancement of overall monitoring operations—such as expanding IP blocking, collecting TI data, and integrating with firewall block management systems—there are plans to achieve automation of tasks beyond security operations as well. Ultimately, the goal is to achieve automation-driven efficiency across the entire IT operation of the organization.

Improvements are also expected in dashboard customization. If the provided widgets can be adjusted more flexibly and integrated with playbooks to enable task-specific visualizations, it will offer a foundation for easily grasping the flow of security events and responding swiftly. In this regard, AhnLab SOAR's intuitive workflows and scalable design are key strengths, making it a valuable solution for organizations seeking to automate and systematize not only threat response but also broader security operations.

AhnLab

AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea
www.ahnlab.com/en | global.sales@ahnlab.com