Case Study

AhnLab

# Enhancing Security Operations Through Automated Threat Analysis and Response

**Industry**
Information & Communications Technology (ICT)

**Company Size**
Large Enterprise

**Solutions**
AhnLab MDS + API Automation

Company M operates a Security Operations Center responsible for cyber threat response, data protection, and security solution management. To address emerging malware variants and ransomware threats, the company leveraged the AhnLab Threat Intelligence Reporting Center alongside multiple security solutions for threat analysis and response. As threats grew more sophisticated and security resources remained limited, manual analysis workflows began to slow response times and reduce operational efficiency. By adopting AhnLab MDS and an API-based automation framework, Company M enhanced its analysis process, achieving faster threat response, improved analysis accuracy, and maximized operational efficiency.

## Expanding Response Coverage with Integrated Analysis

Company M operates a threat analysis process integrated with the AhnLab Threat Intelligence Reporting Center. By verifying whether emerging malware variants and suspected ransomware files missed by existing security solutions are actual threats or false positives, the company minimizes detection gaps and improves analysis precision. This approach enables Company M to analyze diverse threat data based on consistent criteria and strengthen its response capabilities against emerging and variant threats.

## Less Manual Work, Faster Response Through Automation

Previously, Company M relied on a web-based method to automatically retrieve analysis results from the AhnLab Threat Intelligence Reporting Center for verification. However, the process often captured irrelevant data and required additional processing, limiting operational efficiency.

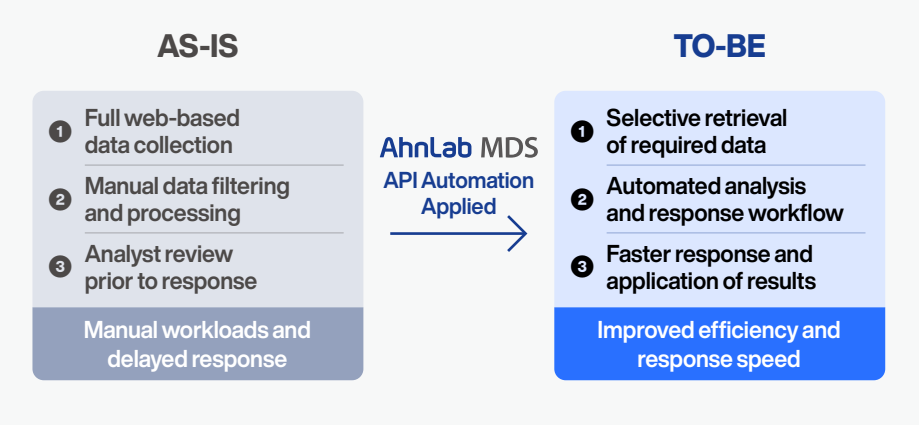
Some samples still required manual analyst review, creating repetitive workloads and delaying response. By gradually introducing automation through an AhnLab MDS-integrated analysis framework, Company M reduced repetitive verification tasks, enabled faster application of analysis results to security operations, and improved overall response speed.

### Results

Expanded threat detection coverage and reduced detection gaps

Established an API-based automation framework

Improved analysis efficiency and accelerated response




**"API-based integration helped us automate the end-to-end analysis workflow, reducing repetitive verification tasks and improving security operations efficiency."**

- Security Operations Manager, Company M

## Ensuring Data Accuracy and Operational Stability Through API-based Automation

Company M's previous web-based data collection method required retrieving the entire webpage before extracting the required information. This increased processing time, generated unnecessary traffic, and made it difficult to maintain data accuracy and integrity.

To address these challenges, Company M worked with AhnLab's Customer Success Manager to define its operational requirements and build an automation framework optimized for its security monitoring environment using AhnLab's common API.

Through API-based integration between its security monitoring system and the AhnLab Threat Intelligence Reporting Center, Company M enabled selective data retrieval and direct server-to-server communication without webpage loading.

As a result, Company M improved data accuracy and processing efficiency while establishing a more stable, automation-driven security operations environment.

**"By working closely with AhnLab CSM, we were able to continuously improve our API integration and security monitoring system, establishing a more stable security operations environment."**

- Security Monitoring Team Representative, Company M

AhnLab MDS is a sandbox-based intelligent threat response solution that detects, analyzes, and responds to threats across network, email, and endpoint environments. It combines static analysis, dynamic sandbox analysis, memory analysis, and exploit detection to identify known malware, emerging variants, advanced threats, and APT attacks with high accuracy. Its email threat response and CDR-based document sanitization capabilities help organizations strengthen proactive defense, ensure business continuity, and improve operational efficiency.