Headline

AI-based managed security service advancement strategy and development direction

Team Leader, Secudium DevOps Team, Kim Jong-hyun

■ Outline

According to the Korea Internet & Security Agency (KISA), the number of infringement incident reports in the first half of last year was 664, up by 40% compared to the same period last year. As the 'Attack Surface' expands due to the acceleration of digital transformation, including increased use of IoT and connected devices, introduction of cloud, and hybrid work models, new vulnerabilities are increasing.

Managed Security Service(MSS) service supports threat monitoring 24 hours a day, 365 days a year. As it requires accurate judgment and quick response to numerous security threats that come our way in real time, it is considered a particularly difficult and arduous task among various cyber security areas. Above all, hackers are attempting attacks in various ways targeting IT assets in unspecified countries, and hacking technology is also becoming more intelligent day by day. So we must say on our toes day and night.

■ Difficulty of existing managed security service

There is a fundamental difficulty in the nature of control, i.e., monitoring threats 24 hours a day, 365 days a year. Through this report, we will look at three major difficulties.

Question 1. Are you analyzing all collected/log events?

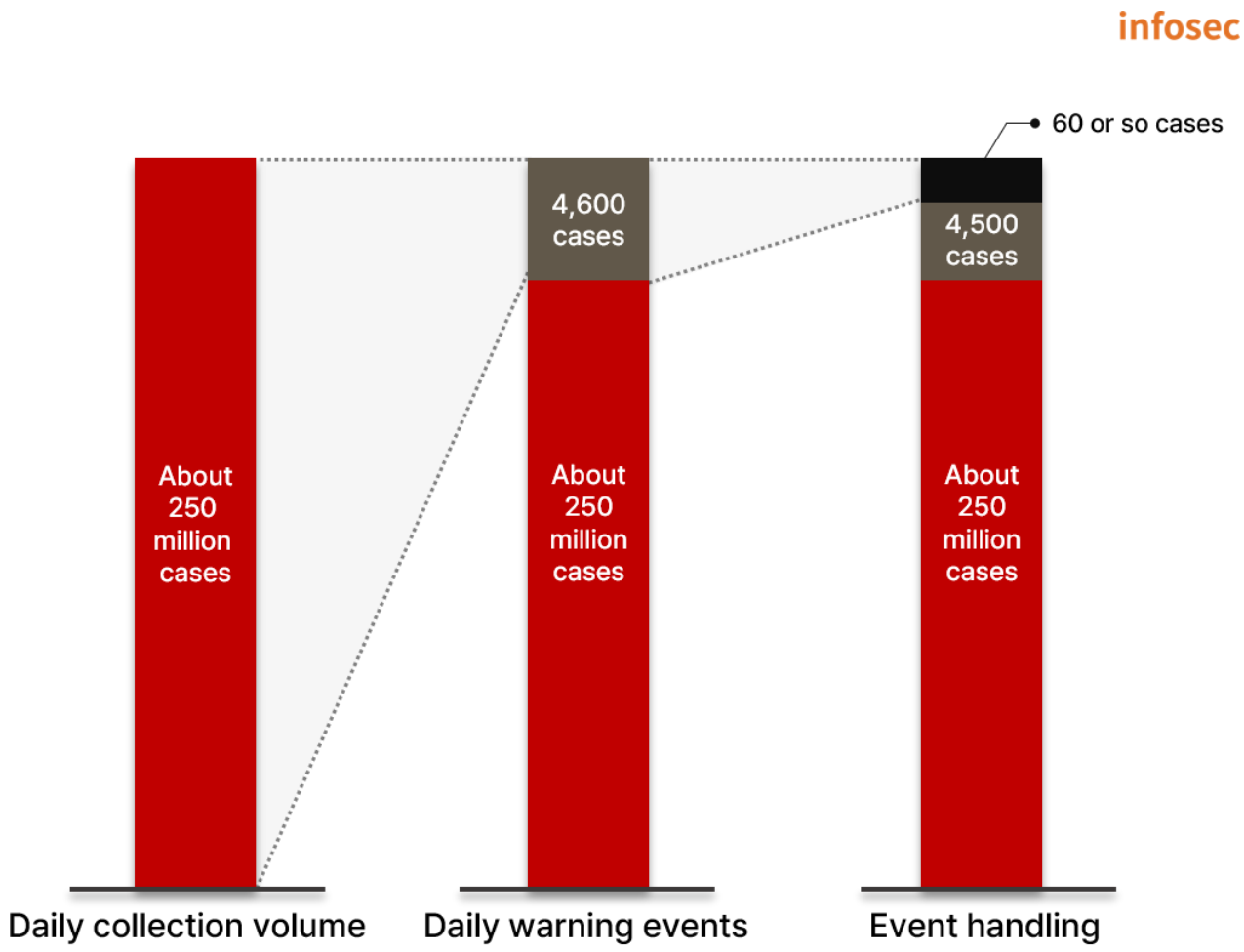


Figure 1. Current status of threat events

The figure above is a graph showing the current status of threat events collected and handled by Company A's control center. Approximately 250 million cases are collected daily and 4,600 warnings are generated by the control platform, of which approximately 60 threats are analyzed/responded to according to priority. You may wonder whether the 4,500 or so unanalyzed warnings are truly safe, and whether there are no security threats in the approximately 250 million logs that did not generate warnings.

Question 2. Is the consistency of infringement threat detection/analysis maintained?

Managed security service check raw data from collected logs to determine threats or use Reputation DB or Threat Intelligence such as VirusTotal.

Figure 2. Data used when determining threats

1) What if the raw data is obfuscated and cannot be immediately confirmed, or even if decrypted, it is difficult to judge depending on the difficulty of the technology? 2) If 89 of VirusTotal's 91 analysis engines are normal and only 2 engines are detected as suspicious, should this be considered a threat? Should it be considered normal? 3) Threat Intelligence confirmed it as a C&C IP, but what if the last activity date was 2-3 years ago? Can we judge this as a threat?

Each security controller may make a different judgment regarding the above three matters, and it would be difficult to say that there is a problem with this.

Question 3. How are we responding to new attacks, expanding attack surfaces, new security equipment to detect them, and increasing security logs?

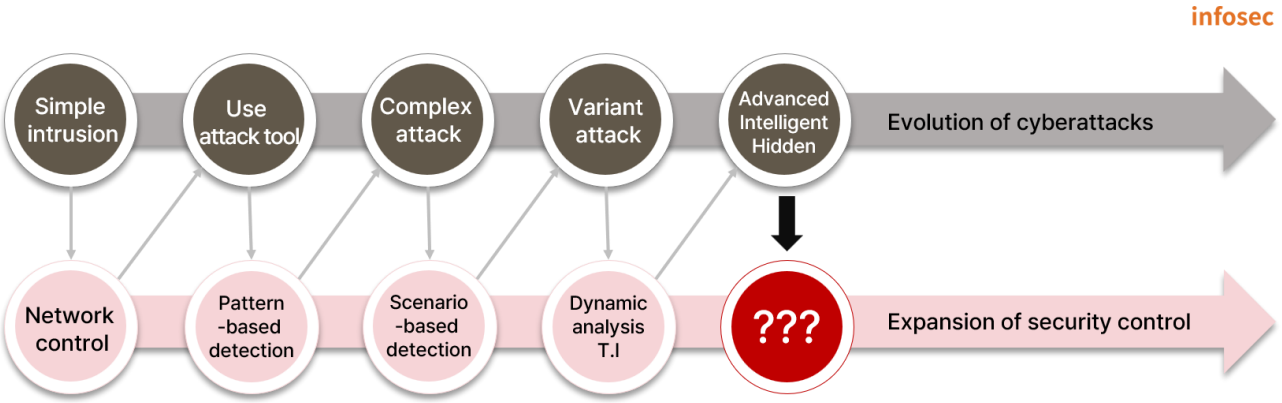


Figure 3. Evolution of cyberattacks and security control

Early simple attacks could be prevented simply by blocking IP through a firewall. When automated tools are used, detection patterns were registered in IDS/IPS/WAF to perform defense, and it was possible to respond to more diverse attack attempts through security log correlation analysis.

For recent malicious file-based attacks, dynamic analysis/T.I(Threat Intelligence). detection, analysis, and response can be performed through APT detection solutions. If so, we need to think about how to respond to advanced/intelligent/hidden attacks using AI in the future.

The vulnerability announced last in 2023 was CVE-2023-24151, and 66 new vulnerabilities were announced daily on average, and security targets are also expanding to Cloud and OT/ICS. Also, to respond to this, new security equipment such as Micro-Segmentation, ASM, and SASE are being expanded as managed security service targets.

Therefore, security service must respond to new threats by analyzing the increasing number of security logs. There are also concerns about whether managed security service can cover everything. An attacker only needs to succeed in one attack, but not a single mistake is allowed to security control.

■ AI-based managed security service

So far, we have looked at the limitations of security control. To make up for the limitations, it is important to "quickly analyze, judge, and respond to all collected events in real time" with the help of machines. In particular, if we combine managed security service with AI, we can get help in overcoming many of the limitations of security control.

To summarize the first question asked earlier, "Are you analyzing all collected/log events?" and the third question, "Increase in new attacks," it could be this question: Is it possible to detect Un-known threats? This is because if the threat is already known, it can be detected through Threat Intelligence by creating a detection pattern or correlation analysis rule. In other words, in order to effectively detect Un-known threats, it is important to monitor whether logs with different characteristics are included in the entire collected logs.

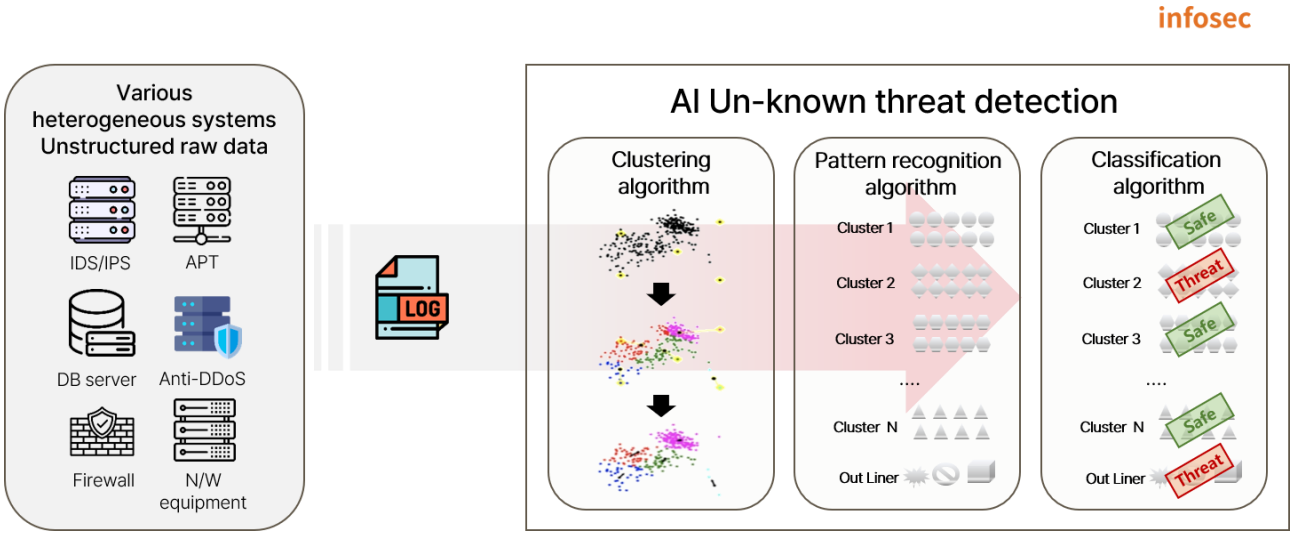


Figure 4. AI-based detection of Un-known threats

AI has an excellent 'clustering' function that separates similar items. To achieve this, AI learning and utilization is possible through the following steps.

- Initially, data is collected over a certain period of time and an initial learning model is performed. Labeling is performed for each classified cluster to determine whether it is safe or a threat.
- Then, logs that may become threats are analyzed through Labeling.
- As learning continues, Out-Liners that were not initially included in any cluster are continuously reduced. Afterwards, monitoring can detect/analyze Un-known threats by detecting/analyzing "Labeled threats" and "Out-Liners."

The second question, **"Is consistency in threat detection/analysis maintained?"** is about controllers' judgment of true and false positives. Because threat judgment requires experience, the judgments of new controllers and those of controllers with more than 3 to 4 years of experience may be different.

Where is the judgment based on experience? The previously determined true and false positive results reflect experience. True and false positive detection is basically the same as AI that distinguishes between dogs and cats.

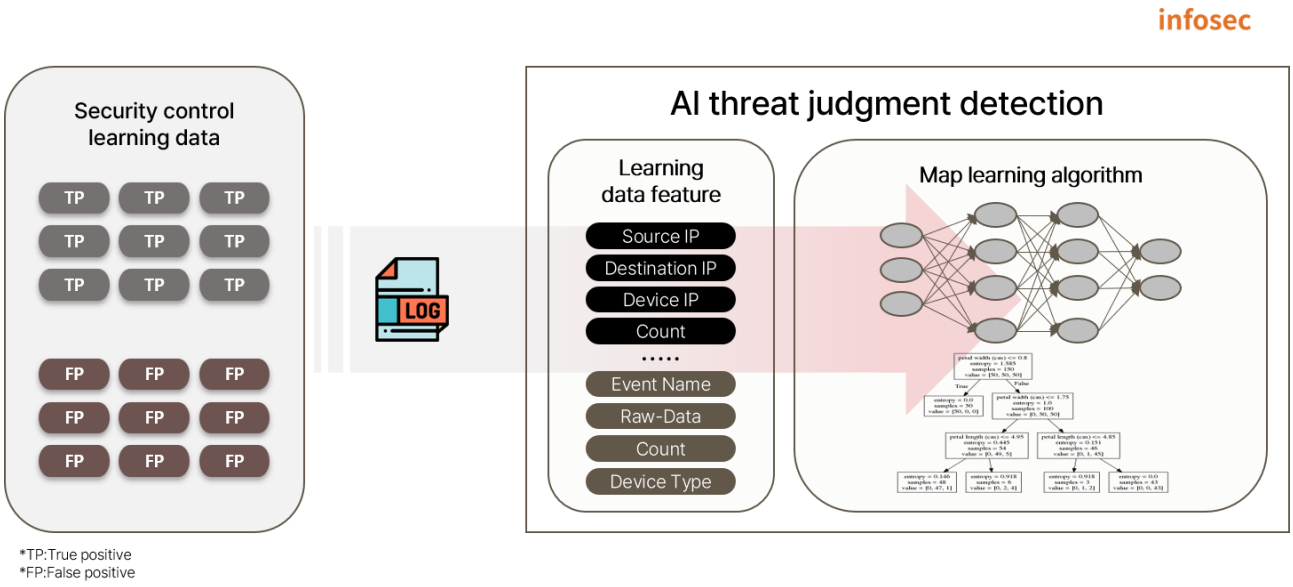


Figure 5. AI threat judgment detection through data learning

- Secure data for AI learning is the most important. Accurate true and false positive judgment result data is secured and learning is conducted.
- Conduct learning various data to prevent overfitting[1] and underfitting[2].
- Preparation of Training Data and TEST Data
  - Training Data and Test Data must have the same ratio of true and false positive distributions.
  - Training Data and TEST Data should not have duplicate data..

So far, we have looked at the limitations of managed security service mentioned above and ways to solve them through AI. This was examined from the perspective of threat detection. Actual managed security service involves **tasks such as threat analysis, emergency response, and result reporting** after detection. In particular, we expect that generative AI, which has recently been attracting attention, will be of great help.

[1] Overfitting: A phenomenon in which judgment on new data cannot be made due to excessive optimization for learning data

[2] Underfitting: A phenomenon in which the structure/pattern of data cannot be reflected due to insufficient learning

Generative AI can recognize natural language and perform various actions. In the analysis process, it can perform various inquiries and write codes for verification, and in the response process, it can implement real-time threat response measures in conjunction with SOAR(Security Orchestration, Automation and Response), establish a response strategy, and evaluate the threat level. In addition, it is expected to be able to communicate with customers through Chat, respond to inquiries, and write reports to report results.

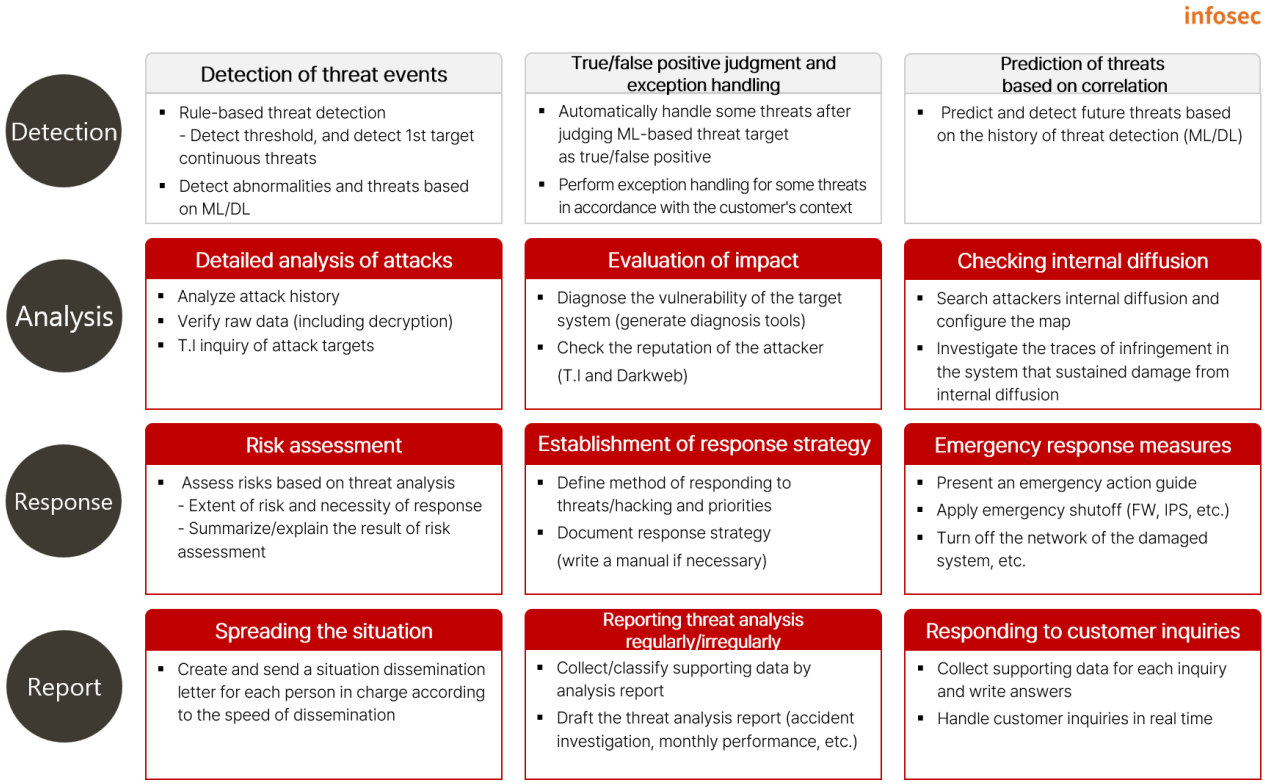
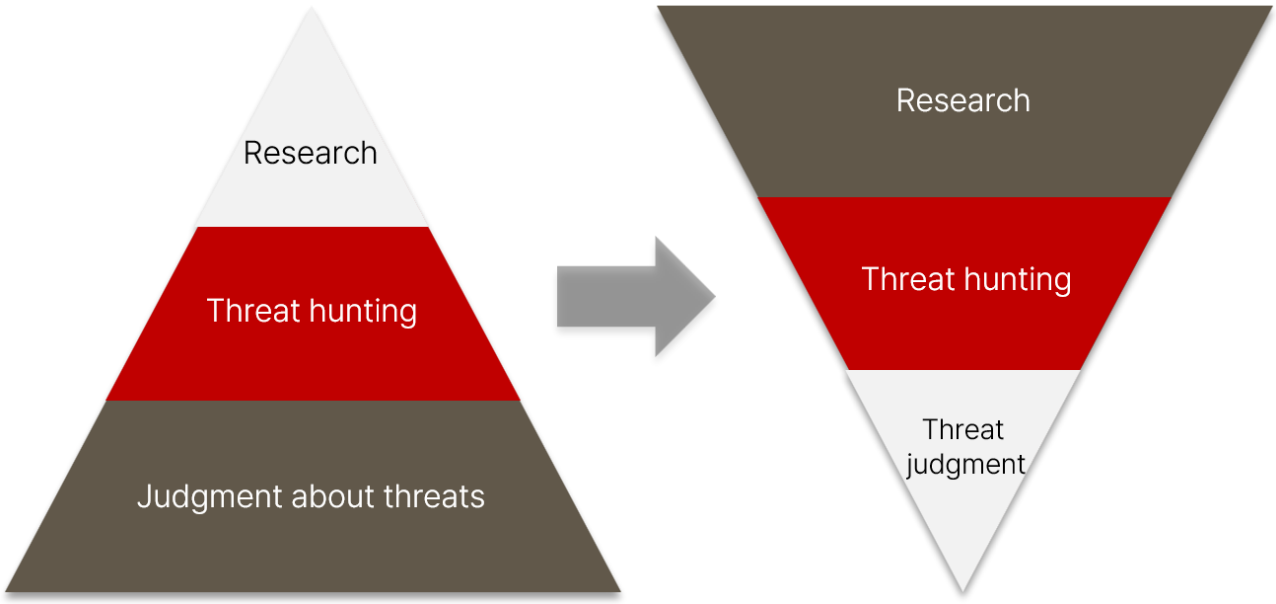


Figure 6. Utilizing AI in security control

SK Shieldus' Secudium Center developed AI for the purpose of minimizing false negative and false positives, and has been operating it by applying it to a platform since June 2022. It performs work automatically using AI for 47% of all detected threats, and for this purpose, 78 million cases of data were used for learning.

■ Closing



So far, we have learned about the difficulties of managed security service work and the advancement strategy and development direction of AI-based security control. When AI is applied to security control, 'efficiency' may be the first thing that comes to mind. This is due to expectations that it will be possible to reduce manpower and costs in the control center as AI is utilized.

However, AI is an auxiliary tool that helps controllers perform their work. Even if AI is used, the final decision must be made by the controller. Currently, controllers perform the most repetitive 'threat positive/false positive judgment' work. Now these repetitive and simple tasks must be left to AI, and controllers must conduct threat hunting to analyze advanced threats and conduct research on the countless latest threats. Through this, they must make efforts to raise managed security service to a higher level and create a safe cyber world.

SK Shieldus, Korea's No. 1 information security company, provides information managed security service services for safe protection of companies' business environments 24 hours a day, 365 days a year. Through the remote managed security service service, it collects logs and events occurring in various security systems to detect/respond to intelligent cyber threats.

In particular, through the Secudium Center, its own global-level managed security service center, it provides comprehensive managed security service remotely, including installation/connection of corporate security solutions and systems, infringement prevention activities, monitoring and analysis, response, and reporting. By introducing SK Shieldus' security control, you can respond to cyber threats easily and quickly at a reasonable cost without the need for cumbersome procedures such as separate professional manpower or system construction.

SK Shieldus has the largest number of professional managed security service and incident response personnel in the industry. In addition, it has a managed security service framework and its own proven managed security service methodology ISMM. For more information on security control, visit the website of SK Shieldus.