EQST insight

Corporate cyber security advancement strategy using MDR service

■ Outline

Cyber attack is rapidly increasing around the world and the importance of cyber security is growing. As remote work increases and reliance on digital technology increases, touchpoints widen and new vulnerabilities continue to be discovered. Therefore, it is more important than ever for companies to effectively implement cyber security countermeasures. Recently, a hacking incident occurred that exploited the vulnerability of the financial security authentication software (INISAFE CrossWeb EX V3) used by many people in Korea, resulting in damage to more than 210 PCs in 60 major domestic institutions. As it is estimated that more than 10 million PCs are using this software in Korea, it is expected that related damage will continue to occur.

In addition, the number of ransomware reports filed with the Korea Internet & Security Agency (KISA) increased more than 14 times from 22 cases in 2018 to 325 cases in 2022, and small and medium-sized enterprises in the manufacturing sector are known to suffer a lot of damage. As a result, voices are growing that companies should change to advanced defense and response systems against cyber attacks that are becoming more advanced and intelligent.

The MDR service is an advanced cyber security analysis service that provides enterprises with 24x7 monitoring, real-time threat detection/analysis and quick response to security incidents. This headline introduces the overview, features, components, implementation and actual cases of the MDR service. To help companies understand the importance of the MDR service in the recent threat environment, and to reduce the risk of cyber attacks, we would like to present preventive insights to protect important assets.

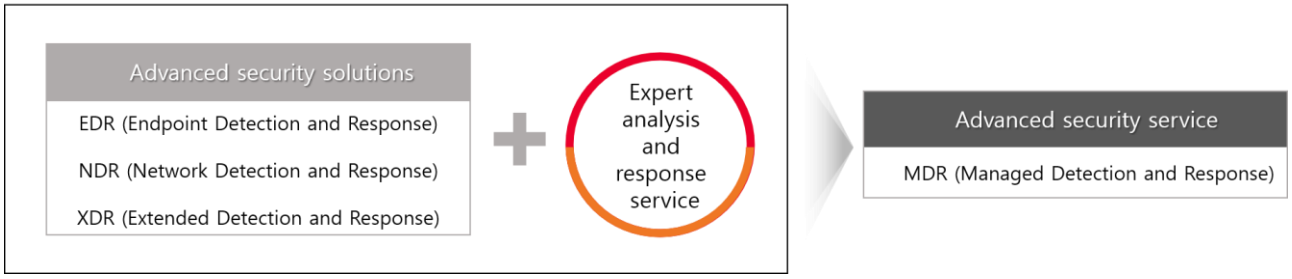

SK 실더스

■ What is MDR (Managed Detection and Response) service?

The MDR service is an advanced cyber security service that combines technologies, processes and expert knowledge to provide 24x7 threat monitoring, analysis, incidents response and reporting. By detecting and responding to security threats in real time, it supports companies to enable them to block cyber threats in advance. The MDR service is designed to detect threats and provide the visibility of attacks through various cyber security solutions such as EDR, NDR, and XDR, and to respond to incidents quickly.

The MDR service described above is briefly defined as follows:

infosec



■ Features of the MDR service

The MDR service has several features such as real-time threat detection, quick response to security incidents, reduction of cyber attack risks, and proactive prevention. So it supports companies to enable them to minimize damage caused by cyber attacks.

① 24x7 monitoring: It continuously monitors the network and endpoints to make it possible to detect and respond to potential threats in real time. This shortens the time it takes to detect and respond to security incidents, thereby reducing the attacker's dwell time and minimizing the potential impact of the attack.

② Advanced threat detection: The MDR service uses advanced security technology to protect companies from a wide range of cyber threats by identifying potential threats including Zero-day attacks, Fileless Malware and insider threats.

③ Quick response to incidents: The MDR service provides a quick incident response function to enable enterprises to quickly contain and resolve security events. Through this, damage caused by intrusion can be minimized and the risk of data loss can be reduced.

④ Expert support: The MDR service can receive support from experts in malware analysis, intrusion incident analysis, and solutions. This includes threat hunting, incident response and security policy reinforcement. Enterprises can enhance security and reduce the risk of cyber attacks by utilizing the expert knowledge of the MDR service.

⑤ Regulatory level: The MDR service allows companies to meet compliance requirements including ISO 27001, PCI DSS and ISMS-P authentication. Meeting these requirements is very important for companies that process sensitive data such as personal information, and the MDR service supports companies to meet these requirements.

⑥ Reasonable cost: Instead of investing in expensive cyber security technology and hiring a dedicated security team, companies using the MDR service can protect their critical assets by leveraging the professional knowledge of the MDR service provider.

⑦ Scalability: As the MDR service has excellent scalability, it can also flexibly respond to the increase in corporate requirements. In other words, enterprises can quickly respond to changing threats and change security services to meet business requirements.

By utilizing the features of the MDR service as above, companies can reduce the risk of cyber attacks and proactively respond to intelligent attacks.

Features of the MDR service

Use the MDR security expert service of SK Shieldus to improve security level

24 x 7 monitoring

- Detect and respond to potential threats in real time
- Reduce the dwell time of the attacker and minimize impact of the attack

Detection of advanced threats

- Identify potential threats including Zero-Day attack, Fileless Malware and insider threat

Quick incident response

- Skilled analysis/operation experts quick response
- Support to make it possible to suppress events quickly and find a solution

Expert support

- Experts in malware analysis, analysis of security breaches
- Threat hunting, incident response and reinforcement of the security policy

Compliance with regulations

- It is possible to meet compliance requirements, such as ISO 27001, PCI DSS and ISMP-P.

Reasonable cost/scalability

- It is possible to use the expert knowledge of the MDR service provider to reduce investments in expensive solutions and high-quality manpower.
- It can be scaled up easily according to the increasing requirements of enterprises.

■ Components of the MDR service

The MDR service consists of key elements such as monitoring, analysis, incident response and reporting. Monitoring includes 24x7 threat monitoring and alerts, and analysis must include detailed analysis to determine the severity of the threat. An incident should be investigated immediately, and an attack pattern should be identified and the analysis result should be reported in writing.

The MDR service provides services with various advanced components to provide a comprehensive cyber security solution. The components are as follows:

① Threat intelligence: To prepare for cyber attacks, threat intelligence must be used to detect potential threats and respond to them promptly. Threat intelligence includes information on the latest cyber threats, vulnerabilities and attack tactics used to identify and determine security risks.

② Response to incidents: The MDR service provides incident response functions including interception, isolation and detailed analysis. This allows enterprises to respond quickly to security incidents and minimize damage from attacks.

③ Threat hunting: It also includes the threat hunting function that proactively finds threats that exist on the network and endpoints. Through this, it is possible to prevent damage and strengthen security by identifying and removing threats that infiltrated the system.

④ Security analysis: The MDR service uses security analysis to identify patterns and anomalies in network and endpoint activities. This can help detect potential threats and provide insight into the effectiveness of cybersecurity measures.

⑤ Reporting: The MDR service provides regular reporting on cyber security threats and incidents, including attack trends, vulnerabilities and security improvement recommendations. Through this, companies can continuously obtain information about potential threats and take proactive measures to mitigate the risks.

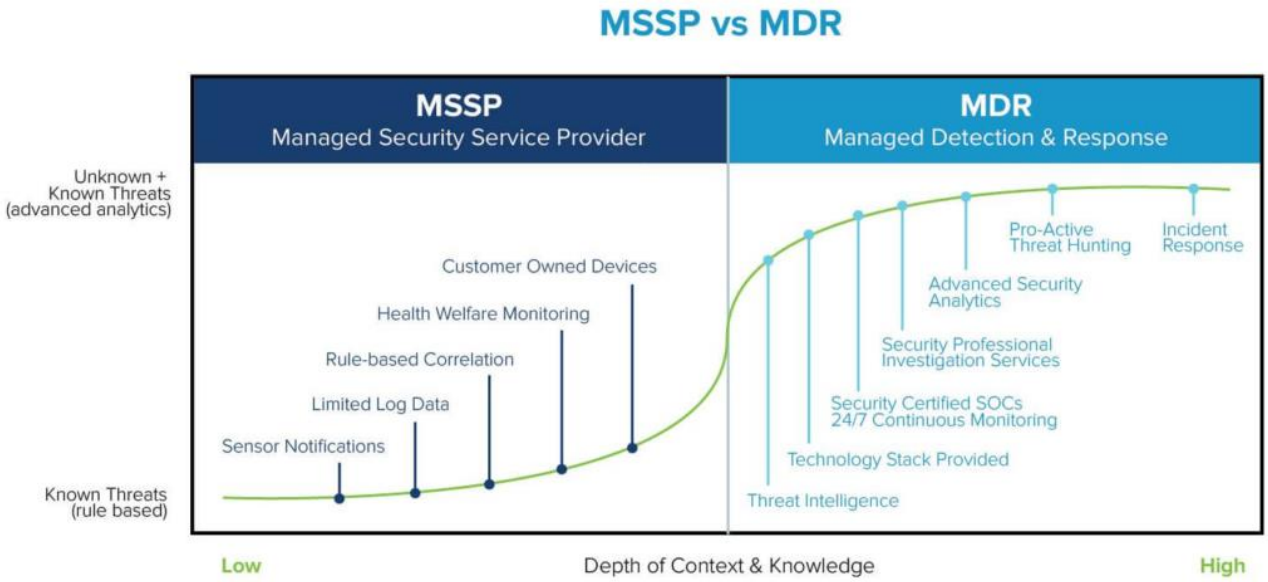
The MDR service utilizes these components to provide companies with a comprehensive cyber security service that reduces the risk of cyber attacks and protects critical assets.

■ MDR service vs security control service

The MDR service is differentiated from the MSS (Managed Security Service), which focuses on event monitoring and correlation analysis to prevent cyber attacks, in that the former provides detailed analysis of real-time threat detection and specific response functions.

- MSSP (Managed Security Service Provider): The MSSP provides enterprises with security services such as network-based security solution management and intrusion detection. It collects and analyzes security data from various paths including network security equipment, servers and applications by utilizing SIEM (security information and event management). In addition, it is an indispensable service for enterprises to meet security requirements, and what differentiates it from the MDR service is whether it provides an intelligent threat detection and incident response function.

Although the line between MSS and MDR is becoming more and more blurred, the difference in terms of results is clearer. MSS monitors boundaries to find known threats and manages assets, but as targeted attacks can bypass it, it is necessary to respond to targeted attacks at a more advanced level through the MDR service. It seems necessary to check the characteristics of each service and select a service suitable for the company's environment. SK Shieldus, as an operator that comprehensively provides both services, provides services by making full use of the characteristics of each.



* Source: https://techgenix.com/mdr-vs-mssp-guide/

■ Plan to implement the MDR service

The implementation of the MDR service includes several steps such as selecting the scope of the MDR service, selecting a supplier, and drawing up an implementation plan. The challenges in building the MDR service include cost, complexity, and the need for expert knowledge. Successful implementation requires participation of all stakeholders, establishment of a realistic implementation plan, and an MDR service test prior to implementation.

In general, the MDR service implementation generally requires the following steps:

① Self-assessment: The first step to implement the MDR service is to perform a security assessment of the network and endpoints. Through this, it is confirmed that potential security threats, vulnerabilities and threats can be identified, and self-assessment is conducted by determining whether security control through existing security solutions is effective in mitigating risks.

② Establishment of a plan: The next step is to establish an MDR service implementation plan based on the assessment results. This involves identifying the components of the MDR service required to address specific security requirements, and defining necessary resources such as implementation scope and WBS.

③ Implementation: When the plan is completed, the next step is to implement the MDR service. This step includes deploying the necessary hardware and software components, configuring the system, and integrating it with existing security controls.

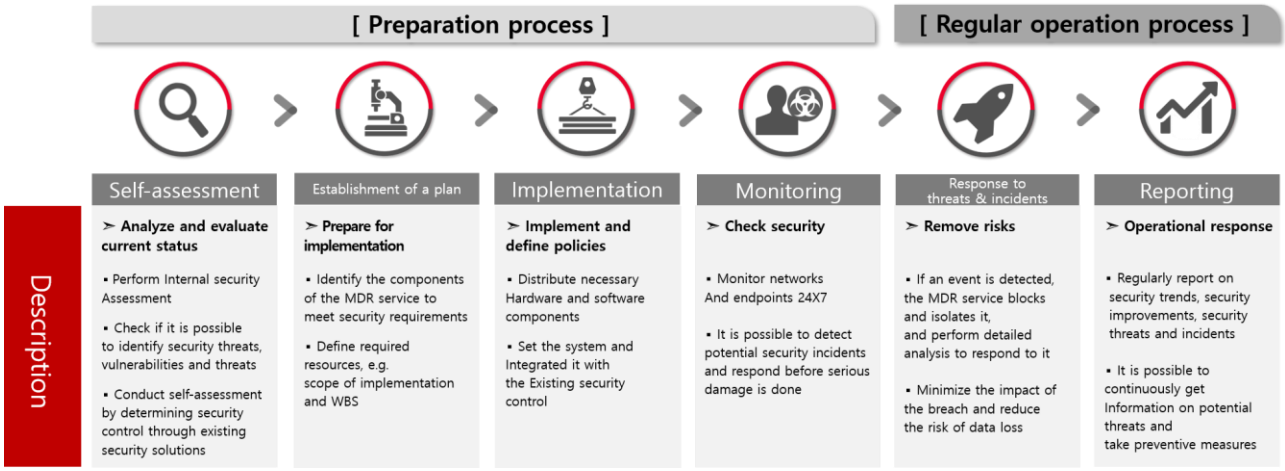
④ Monitoring: After implementation, the MDR service provides real-time monitoring of the network and endpoints 24x7. This allows you to detect potential security incidents and respond to them before they cause serious damage.

⑤ Response to threats and incidents: When a security event is detected, the MDR service responds to the incident, e.g., blocking, quarantine and detailed analysis. This minimizes the impact of security breach and reduces the risk of data loss.

⑥ Reporting: The MDR service provides regular reports on security trends, vulnerabilities and security improvements, cyber security threats and incidents. This allows companies to stay informed about potential threats and take proactive actions to mitigate risks.

Implementing the MDR service can be complex and time consuming, but it is very important for businesses that want to protect their critical assets. Accordingly, if a partnership is formed with an experienced MDR service provider such as SK Shieldus, companies can effectively advance and strengthen their security systems.

Procedure for implementing MDR (Managed Detection Response)



■ Cases of the MDR service

Customers operating global manufacturing plants implemented the MDR service to strengthen security against various cyber threats, including constantly increasing malware, phishing and ransomware attacks. They could prevent threats of cyber attacks occurring in the same industry and enhance their systems to proactive security systems. The MDR service provided customers with the following security enhancements.

① Real-time threat detection: It was possible to detect potential security incidents and respond promptly through the real-time threat detection function even overseas without time and space constraints.

② Response to incidents: Even for small threats occurring at the endpoint, through detailed analysis, it was possible to identify the inflow path and the scope of influence (internal diffusion, etc.) and create an active response plan at the regular incident response level.

③ Threat hunting: A threat hunting function was provided based on the recent breach IoC, and specific ransomware attack groups' access for scanning was fundamentally blocked. Attacks were prevented by detecting potential threats and vulnerabilities in advance through the ASM (Attack Surface Management) function.

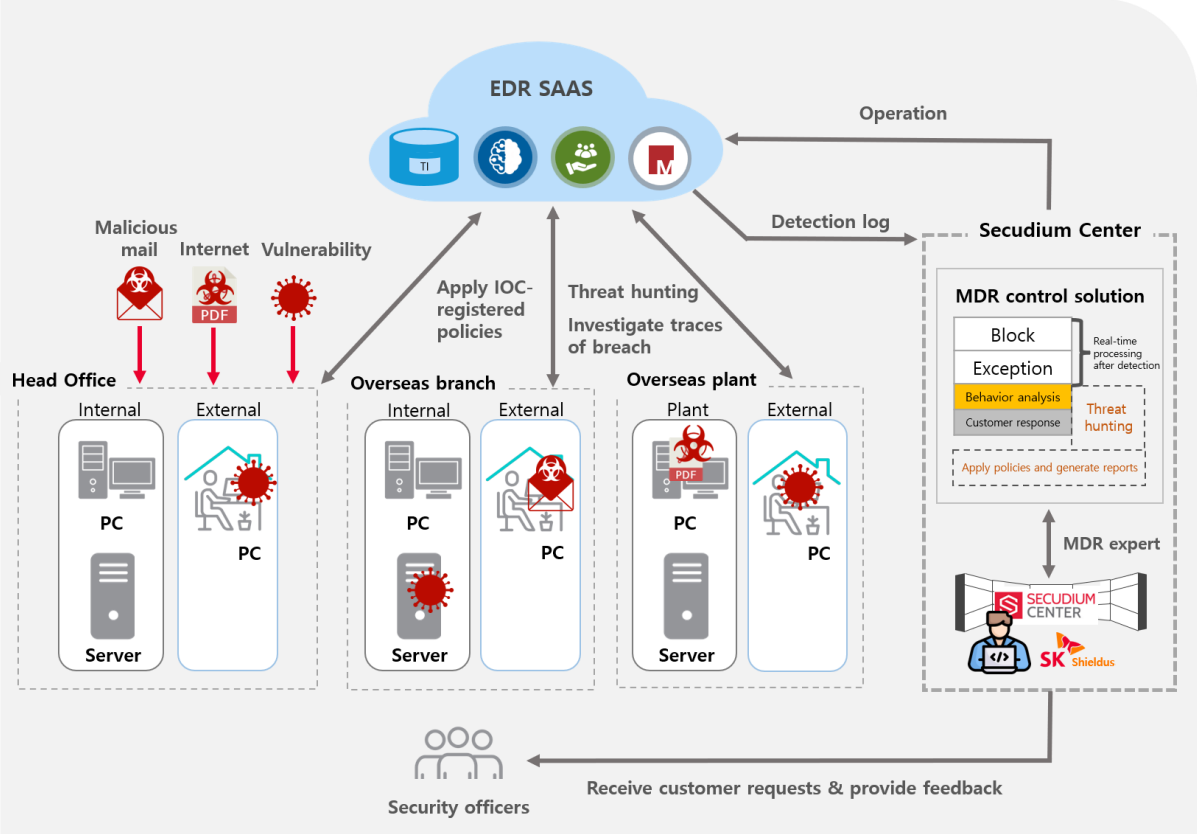
④ Threat information and reporting: Continuous system inspection is conducted based on regular reports on security trends, security threats and incidents occurring in the same manufacturing industry, and information on service vulnerabilities. This allowed affected customers to take proactive steps to mitigate potential threats.

As a result, customers were able to significantly strengthen their cyber security systems and reduce the risk of various attacks. In addition, by increasing the visibility of potential threats and vulnerabilities of networks and endpoints, they were able to minimize threats and ensure the continuity of business operations.

The following is the service configuration based on the above case above.

infosec

Configuration of the MDR service



■ Conclusion and recommendations

The MDR service is an essential component of cyber security for enterprises to detect and respond to threats in real time. It is recommended to reduce the threat of cyber attacks and strengthen the overall cyber security level through the MDR service.

The MDR service is a cyber security service suitable for enterprises of all sizes and variety because it provides comprehensive and proactive approach to cyber security. The MDR service utilizes advanced technologies such as AI and machine learning to enable enterprises to detect, response to and mitigate potential security threats in real time.

In conclusion, companies that want to protect critical assets and maintain business continuity should consider building the MDR service. If three or more of the following items apply, please contact the MDR Service Team of SK Shieldus.

① It is impossible to analyze and respond to threats to endpoints inside the company.

② Malicious e-mails are constantly flowing in and the company had been infected with malware like ransomware before.

③ Did not perform Vulnerability diagnosis regularly or has never been performed.

④ There are cases where the PC is used outside for telecommuting or on a business trip.

⑤ Only firewall or vaccines are in operation and the APT solution is not in use.

⑥ Security incidents occurred, but intrusion incidents were not investigated.