SIEM-based XDR Implementation Plan

Team Leader, Cloud Infra Business Team, Kim Yi-gon

■ Outline

With the Internet-based environment generalized, the importance of information security is being emphasized. To this end, the intrusion detection system (IDS) and intrusion prevention system (IPS) to detect cyber attacks from firewalls for simple network blocking have spread. In addition, concurrently with the development of IT services, the increase in advanced cyber attacks to threaten such services has led to the introduction of various information security solutions.

Information security in the earlier phase was to block all areas vulnerable to an attack. Recently, however, the security trend is shifting to center around monitoring with service availability and security concurrently taken into consideration. A solution that leads this change is the extended detection and response (XDR) service.

Cyber attacks are being advanced and more sophisticated as of late. A security solution of an independently implemented detection and response model cannot sufficiently respond to the threats. To this end, XDR, which is capable of integrated security incident detection and response, is drawing attention. XDR responds to threats by automatically collecting detection information in various security solutions, identifying and analyzing correlation, and therefore detecting malicious activities.

XDR comprehensively identifies the correlation of data in all vectors, such as email, endpoint, server, cloud workload and network. Therefore, even when an advanced threat occurs, visibility and context[1] can be secured for the overall environment.

[1] Context: The "situation information" or "information of information" that has become necessary by context network to search useful services and information from the massive information network. It refers to a specific situation that is recognized immediately, not an interpretation of simple information such as text.

■ Definition of XDR

XDR was first mentioned by Nir Zuk, the CTO of Palo Alto Networks. At the time, Zuk proposed the XDR concept for detection and response in all data sources through the security silo collapse. Subsequently, Gartner mentioned XDR in a report titled the "Security Monitoring Visibility Triad" and defined it as a security solution providing extensibility and a control function by including various security technologies and solutions in a single platform.

XDR is an open cyber security architecture to integrate security solutions, and security operations in all security layers including user, endpoint, email, application, network, cloud workload and data. Using XDR, even the security solutions that were not originally designed for concurrent operation can be mutually operated for threat prevention, detection, investigation and response.

XDR supports a security team, which is overloaded with work, to solve security issues faster and more effectively by narrowing the visibility gap between security solution and layer. In addition, it supports the team to make better security-related decisions and prevent cyber attacks in the future by capturing more comprehensive context-based data.

The concept of XDR, which was first introduced in 2018, has been continuously developed through active discussions by security experts and industry analysts. In the initial phase, many security experts explained XDR as an EDR extended to encompass all enterprise security layers. Currently, however, experts consider the potential of XDR to be far larger than the sum of the integrated solutions and functions, and emphasize its strengths including the workflow optimized to end-to-end threat visibility, integrated interface, and threat detection, investigation and response.

Analysts and vendors have classified the XDR solution into two types. The first is Native XDR, which is to integrate only the security solutions of the respective vendors, and the second is Open XDR, which is to integrate all security tools within the organization's security ecosystem. However, a growing number of enterprise security teams and security operations centers (SOCs) are hoping for Native XDR to also be an open solution. In other words, they are looking for flexibility to integrate other security solutions that are currently in use or being planned for use in the future.

Type	Characteristics
Open XDR	✓ Open XDR is dependent on the minimized partner (vendor) ✓ It can be linked with the previously implemented security products ✓ It can be implemented and used without replacement of the existing security products (tools)
Native or Closed XDR	✓ It can be integrated with and linked to the security equipment of single vendor ✓ There are limitations in the link to and analysis of other products

Table 1. Classification according to XDR Implementation Method

■ Summary of Detection & Response Technology

Type	Purpose	Scope of Response	Operational Approach
EDR	To conduct real-time endpoint monitoring and advanced threat detection	Endpoint equipment and host	• Real-time organizational endpoint monitoring • Endpoint data correlation analysis - Malicious act, indicator of attack (IoA), indicator of compromise (IoC), signature, machine learning
NDR	To analyze network traffic/user action and identify/investigate suspicious network activities	Traffic between network and device	• Real-time network attack response and blocking • Correlation analysis for user action-related abnormal network operations - Indicator of attack (IoA), anomaly detection, user action, machine learning
MDR	To continuously monitor and respond to threats through skilled security experts (24/7 monitoring, latest threat intelligence, security consulting, security compliance, etc.)	Cyber security experts (in all environments)	• Threat detection and response outsourcing • Data correlation analysis by security experts - Customer system integration through various interfaces* (API, logging, DataLake, etc.)
XDR	To support efficient threat detection/response in all environments of security team (using advanced analysis, machine learning, automation, etc.)	Endpoint host, application, traffic between network and device	• Automated response through various platforms • Integrated analysis of various sources - Machine learning, indicator of attack (IoA), anomaly detection, user action, malicious action, indicator of compromise

Table 2. Summary of Detection & Response Technology

■ XDR Trend and Major Vendors

In the XDR market, the demand for flexible and extensible solutions that can adapt to the fast changing situation is on the rise. According to this trend, the market is shifting towards service-based models such as XDR-as-a-Service[2]. In addition, as cyber threats are diversifying and becoming more elaborate, XDR is improving its detection and response function through machine learning and using AI technologies.

Gradually adopting multi-cloud strategies, enterprises are demanding an XDR solution capable of providing visibility for only multiple cloud platforms, but also the on-premise environment in order to strengthen their focus on multi-cloud environment security.

From the perspective of automation, as enterprises are experiencing difficulty due to the complexity of management according to the introduction of a number of security solutions and technologies, the importance of an improved orchestration function to integrate and automate security operations in a single platform is increasing.

At the same time, XDR adoption for SecOps[3] is increasing as XDR, which provides an integrated platform for security data collection, analysis and handling, plays a critical role in the SecOps activation.

Additionally, in line with the spread of mobile and IoT devices, the demand for comprehensive security in relation to not only the existing IT assets, but also mobile and IoT devices is increasing.

In line with the changes in market and customer requirements, numerous manufacturers are strengthening their competencies and broadening the scope of response based on the latest technologies. The table below shows the status of solutions of representative companies by XDR type.

[2] XDR-as-a-Service: A cloud-based preemptive cyber threat management service that provides 24/7 monitoring service by security experts through integration with the key operations of XDR (threat hunting, investigation, warning and response)

[3] SecOps(Security Operations): An approach to integrate the organizational security process and IT operation enabling faster and more effective response to security threats by sharing responsibilities related to security maintenance for the organization's digital assets and information, and therefore strengthening cooperation between security and operation teams

Type	Company	Features of Solution
Open XDR	Stellar Cyber	• Open XDR leading company, solution comprising open XDR platform, NG-SIEM[4], Threat Intel, NDR, IDS & Malware Analysis and SOAR • Collecting and analyzing comprehensive data in relation to various IT environments including cloud and heterogenous equipment • Enabling preemptive response and threat element analysis and monitoring in each cyber kill chain stage by establishing a security monitoring portal integrated with the previously implemented security solution, configuring honey pot sensor, and therefore identifying external attack factors
	Elastic	• Took over Endgame in 2019 and launched Elastic Security for endpoint • Collection, detection, defense and direct response through Elastic Agent integrated with open platform • Detecting and blocking unknown malware and ransomware, defending against APT attacks through host-based analysis
	IBM	• QRadar XDR comprising attack surface management (ASM), endpoint detection and response (EDR), security information and event management (SIEM), security orchestration, automation and response (SOAR), etc. • Designed to simplify threat detection, tracking, investigation and response in an integrated environment, automating detection, analysis and response using AI and pre-implemented playbook • Capable of establishing open XDR ecosystem to link to systems and solutions of other companies through QRadar XDR Connect
Native XDR	CrowdStrike	• Cloud-based single lightweight agent with usage of 1% CPU and 50MB or less • Providing high true positive rate through machine learning without requiring signature • Capable of securing visibility for threats through process tree • Providing 24*365 monitoring by overwatch team, and cyber threat information and response guidelines from threat hunting team experts
	SentinelOne	• Launched endpoint solution using machine learning-based action AI as the first in industry • Supporting file header-based analysis using reference and static AI engines before file execution • Capable of analyzing correlations of all related actions from the start to the end of malicious code attack • Preventing, stopping and remedying new malware, changed malware and hacking attacks based on the patented AI machine learning model, autonomously blocking ransomware function • Recently launched Purple AI, a ChatGPT-based search engine, to provide automatic query generation function through AI at natural language input
	TrendMicro	• Providing comprehensive protection with improved extended detection and response (XDR) functions

[4] SIEM(Security Information and Event Management): A solution to collect, analyze and report security data for overall IT infrastructure of the organization supporting security threat detection and response through real-time monitoring, log management and correlation analysis among security events

		• Generative AI assistant companion, providing preemptive attack surface risk management (ASRM) based on the principle of zero trust • Capable of automatic response to high-risk warnings through playbook • Reducing silo through correlation analysis among security vectors, and detecting and responding to suspicious action, malware, ransomware, interference and other important attacks
	Palo Alto Networks	• Focusing on improving security operation across endpoint, network and cloud • Providing Cortex XSOAR for automatic attack response, Cortex Xpanse for overall Internet attack surface management and protection, and Cortex XSIAM, an AI-based SOC operating platform • Providing MDR, the managed security service, through Unit42, a professional security service
	Cybereason	• Capable of detecting and responding to unknown attacks using machine learning technologies based only on the action data through end point and host data collection, capable of remedy in all attack stages through single click • Comprising endpoint protection providing NGAV and EDR functions in MalOp engine, cloud, extended attack protection for network, threat hunting, security operation optimization providing MDR service, digital forensic and incident management providing incident response service
	Trellix	• Focusing on security event correlation analysis and automation • Conducting comprehensive collection and analysis also for endpoint events • Offering visibility for the flow of an attack by accurately providing an event with correlation analyzed as single threat
	Genians	• Expanded XDR business in 2021 through investment and business cooperation with ZDR and NDR specialist Xabyss • Solution comprising multi-layer detection engine for IOC detection (file), ML detection (file), XBA detection (action) and CTI (reference check) • Providing step-by-step detailed visibility covering from user action to data level
	Ahnlab	• Focusing on effective risk management under the assumption that the degree of risk of threats can vary depending on the organizational situation • Providing advanced risk scenario rules to identify and index risk priorities, reflect scenarios that have occurred and continuously update new scenarios, internal impact monitoring based on threat intelligence and linked analysis of heterogenous logs • Supporting open platform, etc. that can be linked to third-party solution

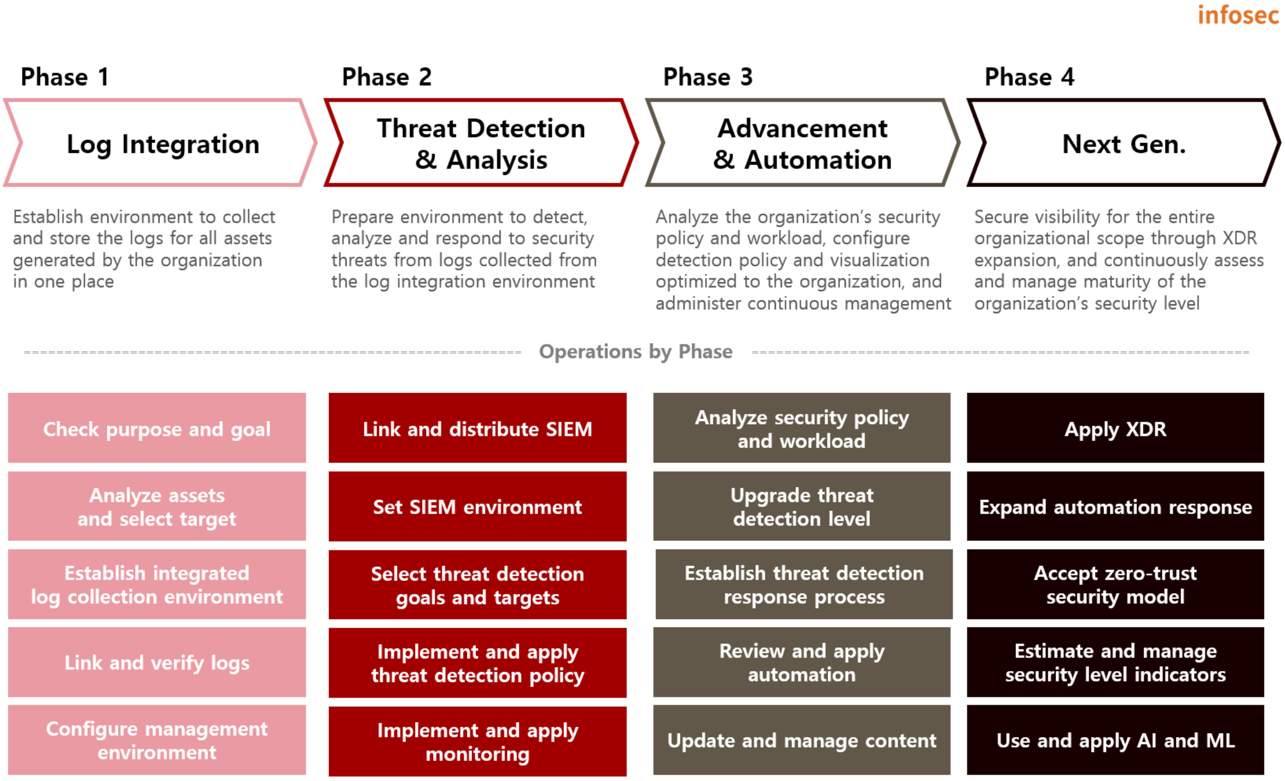
Table 3. Features of XDR Solutions by Vendor

■ SIEM-based XDR Implementation Plan

Currently, many enterprises and organizations are performing log integration and security monitoring by using the SIEM solutions, and introducing EDR and NDR to strengthen their security levels. Under the circumstances, they have come to face the mega trend of XDR.

As explained earlier, XDR is implemented as Open XDR or Native XDR. Although each has different strengths and weaknesses, Native XDR may involve difficulties in its configuration due to the large cost and resource investment considering the substantial organizational security environments at the moment.

The operations by phase from the SIEM establishment to the XDR expansion are summarized below.



Phase 1 – Log Integration: Establish environment to collect and store the logs for all assets generated by the organization in one place

Phase 2 – Threat Detection & Analysis: Prepare environment to detect, analyze and respond to security threats from logs collected from the log integration environment

Phase 3 – Advancement & Automation: Analyze the organization's security policy and workload, configure detection policy and visualization optimized to the organization, and administer continuous management

Phase 4 – Next Gen.: Secure visibility for the entire organizational scope through XDR expansion, and continuously assess and manage maturity of the organization's security level

Operations by Phase

Phase 1	Phase 2	Phase 3	Phase 4
Check purpose and goal	Link and distribute SIEM	Analyze security policy and workload	Apply XDR
Analyze assets and select target	Set SIEM environment	Upgrade threat detection level	Expand automation response
Establish integrated log collection environment	Select threat detection goals and targets	Establish threat detection response process	Accept zero-trust security model
Link and verify logs	Implement and apply threat detection policy	Review and apply automation	Estimate and manage security level indicators
Configure management environment	Implement and apply monitoring	Update and manage content	Use and apply AI and ML

Figure 1. SIEM Implementation by Phase

Phase 1 – Log Integration

In the phase of log integration, an environment to collect/store the logs for all assets generated within an organization is established. In general, the main purpose is to collect logs for compliance.

Phase 2 – Threat Detection and Analysis

The threat detection and analysis phase is where security threat detection, analysis and response policies are established in relation to the logs collected following log integration. This is a critical phase where the key functions of SIEM are set. For the detection rules established in this phase, the importance of assets, environment, etc. must be taken into consideration.

Phase 3 – Advancement and Automation

The advancement and automation phase is where detection accuracy is enhanced based on the fine-tuning of the established rules through advancement of the detection policy established in the threat detection and analysis phase, and the organization's SIEM operating maturity is continuously improved for response to the changing security environment. In addition, the efficiency of security response must be maximized by establishing a response process according to the detection result, and automating the post-detection response operations through application of the established process to SOAR functions.

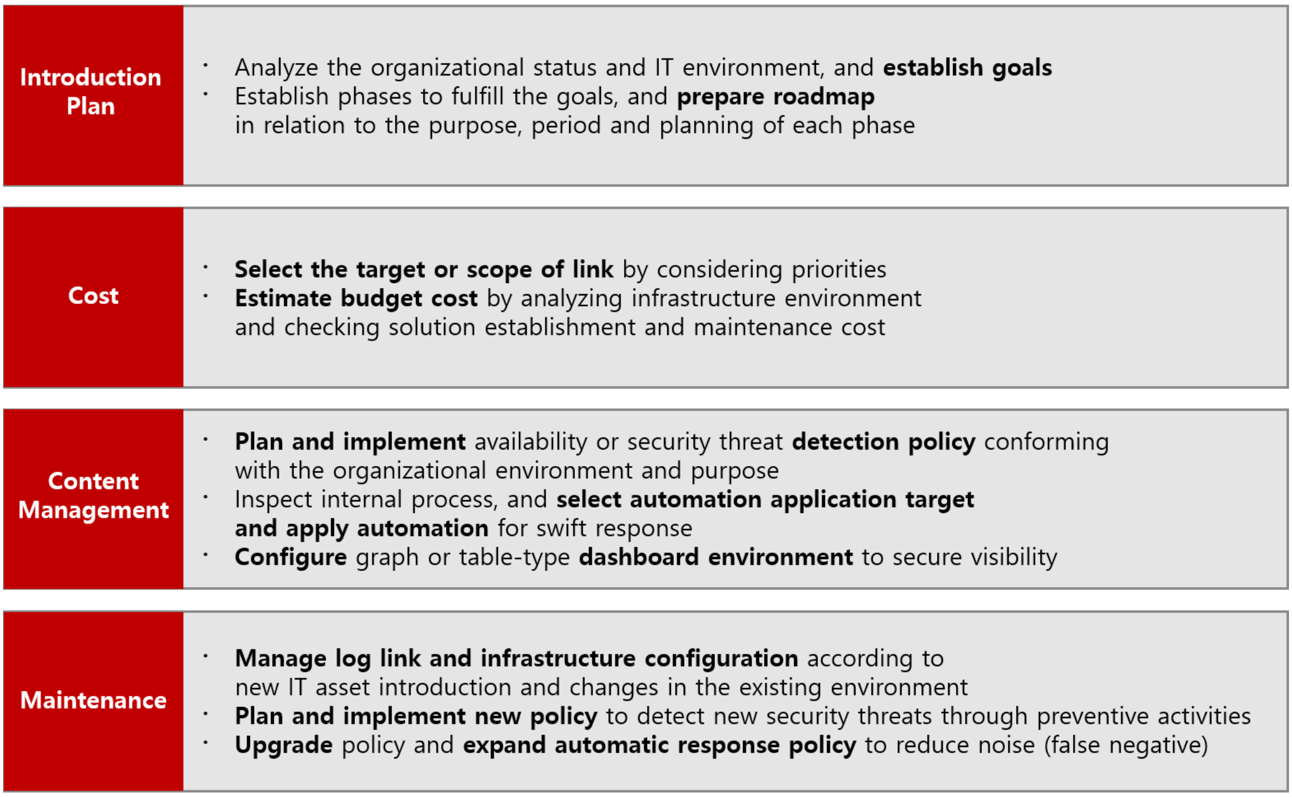
Phase 4 – Next Gen.

In the next gen. phase, the latest trend, such as XDR and zero-trust, is applied using SIEM and SOAR while the organization's maturity for security threat detection, analysis and response is heightened.

■ Conclusion

So far, the phases from the initial SIEM establishment to the establishment of XDR, which is of the latest trend, have been defined. For SIEM, a platform to collect, save, and analyze the log data of heterogenous systems, the value of use in various fields amplifies when the amount of the collected data increases.

To make an effective use of this solution, the following must be taken into consideration.



infosec

Introduction Plan	· Analyze the organizational status and IT environment, and **establish goals** · Establish phases to fulfill the goals, and **prepare roadmap** in relation to the purpose, period and planning of each phase
Cost	· **Select the target or scope of link** by considering priorities · **Estimate budget cost** by analyzing infrastructure environment and checking solution establishment and maintenance cost
Content Management	· **Plan and implement** availability or security threat **detection policy** conforming with the organizational environment and purpose · Inspect internal process, and **select automation application target and apply automation** for swift response · **Configure** graph or table-type **dashboard environment** to secure visibility
Maintenance	· **Manage log link and infrastructure configuration** according to new IT asset introduction and changes in the existing environment · **Plan and implement new policy** to detect new security threats through preventive activities · **Upgrade** policy and **expand automatic response policy** to reduce noise (false negative)

Figure 2. Considerations for SIEM Introduction

It is desirable to establish an organizational security threat response system through the configuration of an SIEM-based security threat response environment by reviewing the considerations for solution introduction and implementation plans for each phase as discussed earlier.

In the zero-trust era, SK Shieldus, Korea's No. 1 information security service provider, is operating information security and security operation service-based detection/response solutions dedicated to WebShell on the basis of its top-tier security competency and infrastructure in Korea. It is providing various security services including not only security SI consulting, but also security level management support, integrated security monitoring and business environment optimization. The details of the security solution introduction, such as SIEM introduction and XDR implementation, can be found on the SK shieldus official website or through professional consulting service (1800-6400).