SK shieldus

# Managed Security Services

# on Amazon Web Services

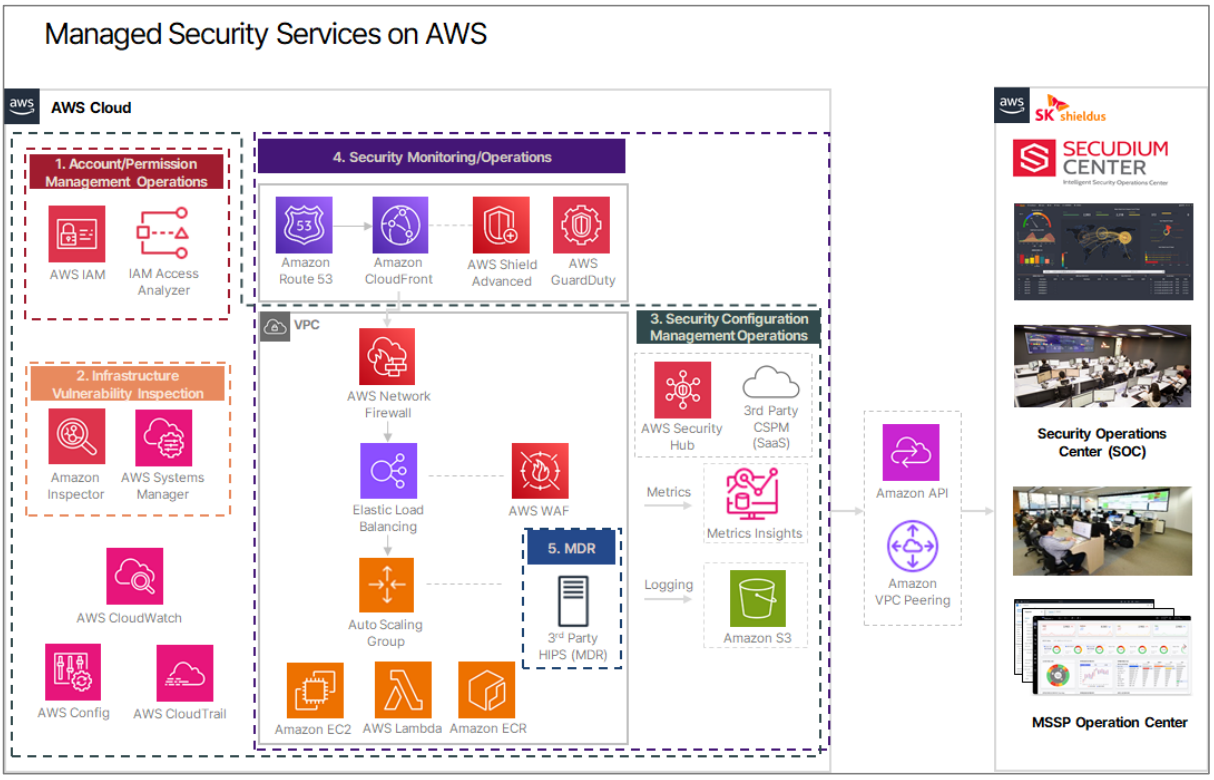
## Contents

# 1. Service Overview

Managed Security Services on AWS by SK shieldus is a specialized service designed for security management in AWS cloud environments. It offers 24/7 monitoring of customer workloads, detects threats, and assists security professionals in responding to incidents accurately and effectively. In addition, the service systematically enhances cloud security through effective compliance management, security policy management, vulnerability assessments, and improvement recommendations. It provides tailored security solutions that are optimized for each customer's unique environment and includes detailed reporting, delivering comprehensive security management services to help customers build safer and more reliable cloud infrastructures.

With the expertise of professionals who leverage the capabilities of AWS's various security services and third-party security tools, customers can efficiently manage and optimize their security in complex cloud environments. This approach reduces the burden of security operations, allowing customers to focus more on their core business in a secure cloud setting.

- Detailed descriptions of Managed Security Services on AWS are provided to customers in five categories, with a brief architecture shown below.
  1. Account/Permission Management Operations
  2. Infrastructure Vulnerability Inspection
  3. Security Configuration Management Operations
  4. Security Monitoring/Operations
  5. MDR Security Solution Implementation




* HIPS: Host based IPS (Intrusion Prevention System)

* MDR: MDR Security Solution Implementation

Managed Security Services on AWS provides an integrated approach to managing the security of AWS cloud environments, supporting the resolution of complex security challenges with ease. This allows customers to build safer and more optimized cloud environments, promoting business growth and enhancing competitiveness through reliability.

# 2. Detailed Service Description

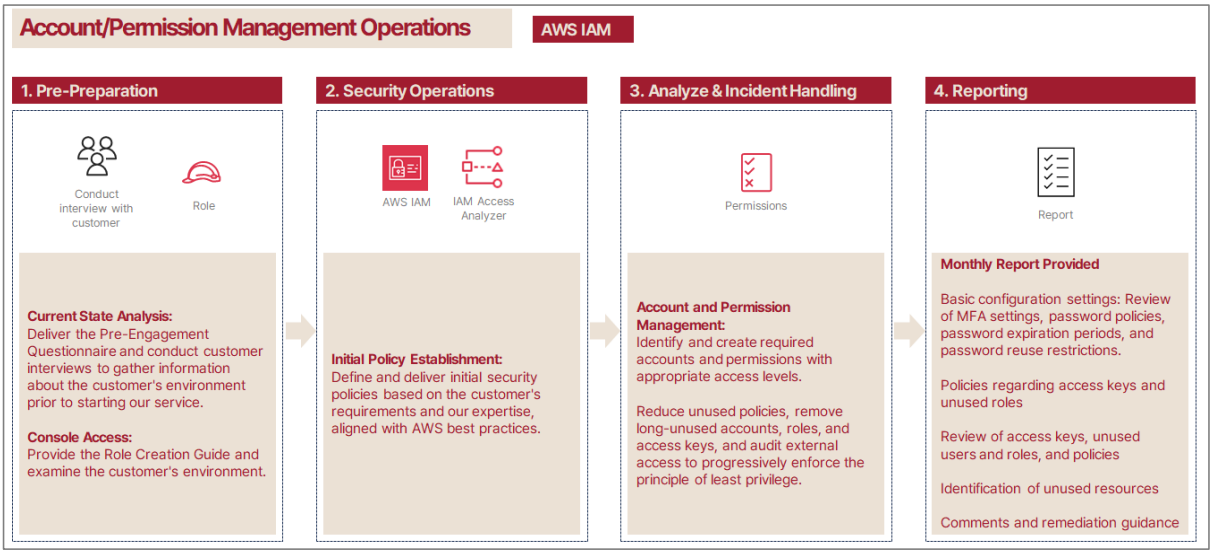
## 2.1. Account/Permission Management Operations

To enhance the security of AWS IAM (Identity and Access Management) accounts and permissions while securely managing access to services and resources, we provide account/permission management operations based on AWS best practices.

For account/permission management operations, we access customers' AWS accounts using temporary credentials (AssumeRole) and manage and check the accounts and permissions using AWS IAM and IAM Access Analyzer resources.

We identify the accounts and permissions required by the customer's users and create them with appropriate levels of access. By reducing unused policies, removing long-unused accounts, roles, and access keys, and auditing external access, we gradually enforce the principle of least privilege to secure the customer's accounts and permissions.

■ The procedure of the account/permission management operations is as follows.

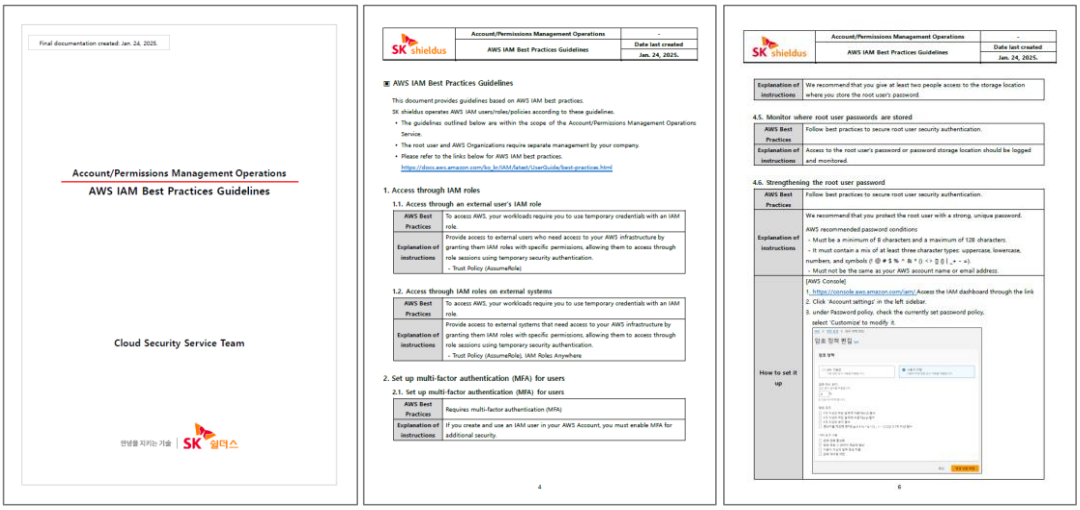



■ The coverage of the account/permission management operations is as follows.

| Coverage | | Provision Status (O : Provided, - : Not Provided) |
|---|---|---|
| **Technical Support** | Technical support (Configuration/Guide) | O |
| | AWS support inquiry responses | O (if needed) |
| **Account and Permission Management** | Account and permission configuration/management | O |
| | Permission optimization (customization) | O |
| | Backup/recovery management | O |
| | Change history management | O |

| | | |
|---|---|---|
| **Access Analysis** | External access analysis | O |
| **Operational Management** | Operational status management | O |
| | Support for management inquiry | O |
| | Operational history management | O |
| | Regular inspections | O |
| **Reports** | Monthly reports | O |

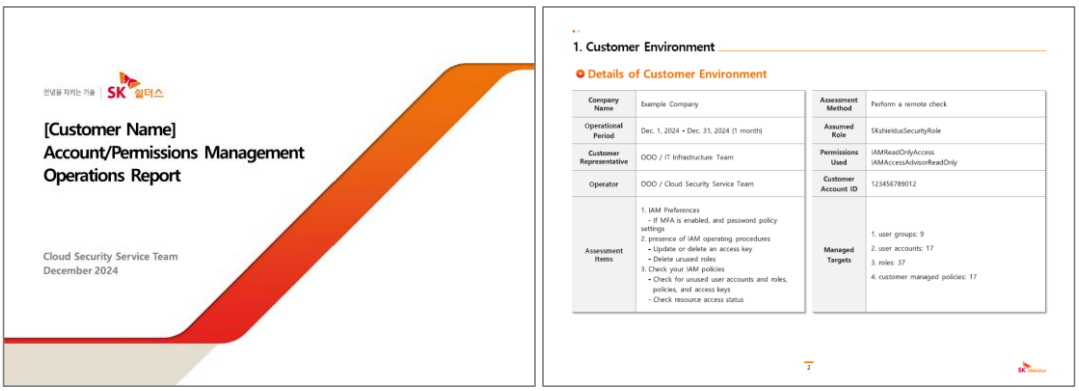
■ We provide an AWS IAM best practices guide to communicate key management responsibilities to the customer.




**[AWS IAM best practices guide]**

■ We perform operations for the customer's AWS IAM and provide regular reports on these operations.

※ The images below are samples.




**[Monthly Report]**

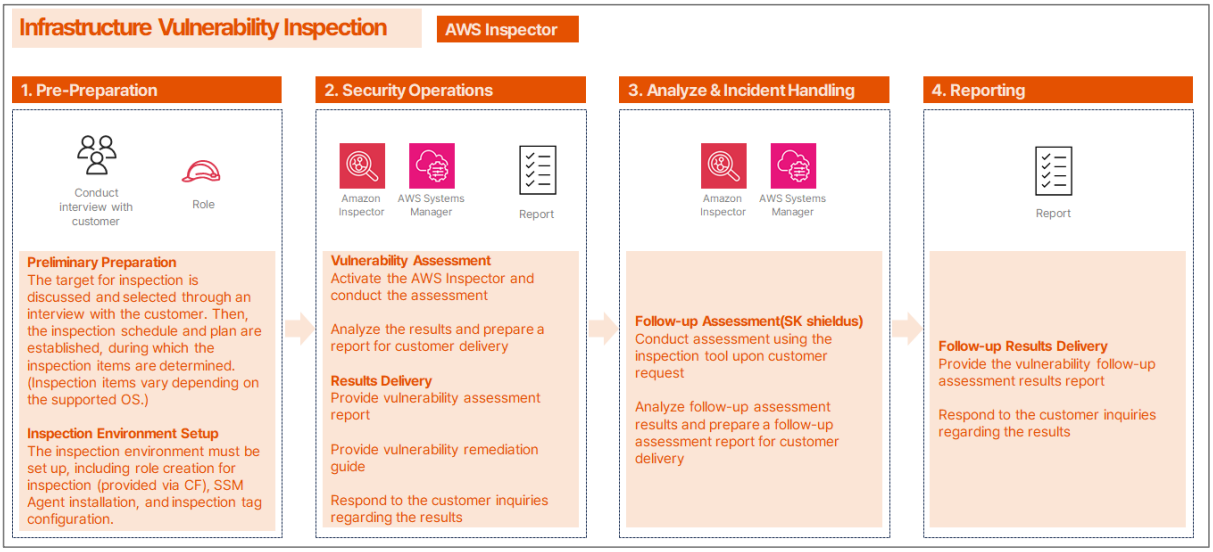
## 2.2. Infrastructure Vulnerability Inspection

We provide security vulnerability inspection for Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Elastic Container Registry (Amazon ECR) using AWS Inspector, to identify, assess, and remediate vulnerabilities in AWS infrastructure.

By leveraging the automatic detection feature of the AWS Native service, Inspector, we offer an automated vulnerability inspection to customers. This includes various metadata from the inspection targets, as well as vulnerability assessment reports and remediation guides.

To strengthen the security of customer infrastructure vulnerabilities, we conduct an initial inspection and remediation process followed by a secondary implementation inspection, ensuring that no security incidents occur due to infrastructure vulnerabilities.

■ The procedure for the infrastructure vulnerability inspection is as follows.




■ The coverage of the infrastructure vulnerability inspection is as follows.

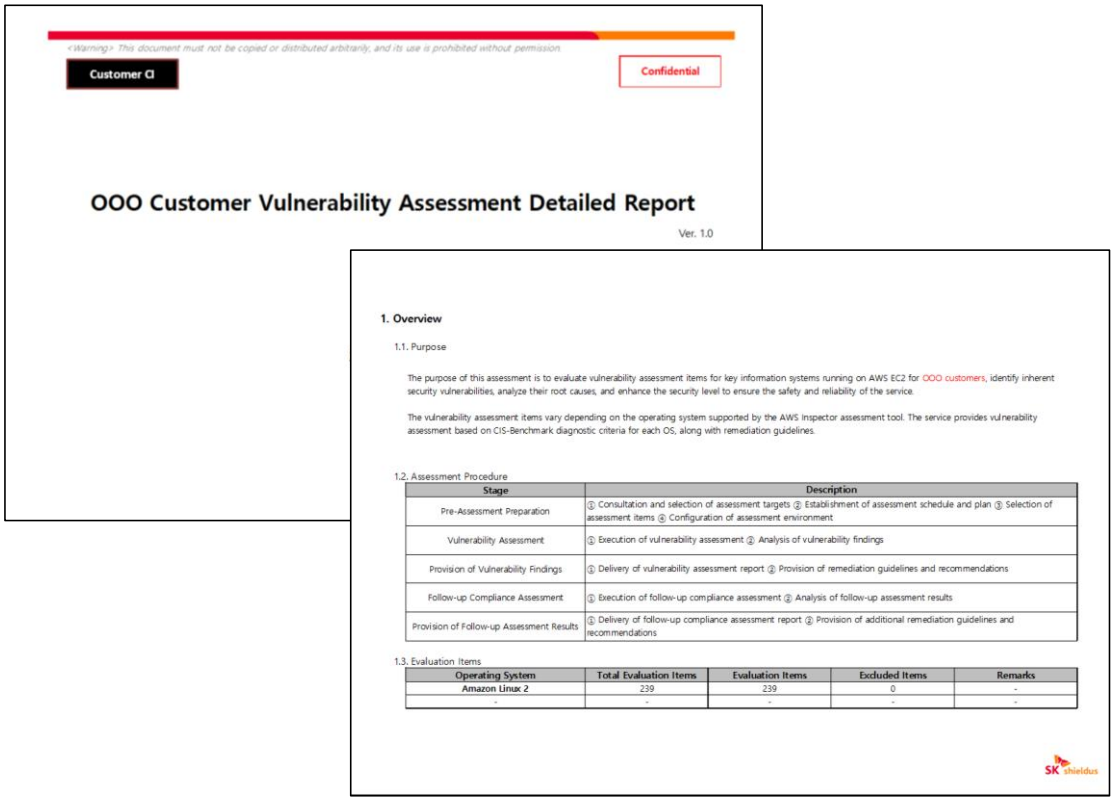
| Coverage | | Provision Status (O : Provided - : Not Provided) |
|---|---|---|
| **Technical Support** | Configuration of the inspection environment (Configuration/Guide) | O |
| | AWS support inquiry responses | O |
| **Vulnerability inspection** | Initial inspection (Inspection/Guide) | O |
| | Implementation inspection (Inspection/Guide) | O |
| **Reports** | Vulnerability inspection results report | O |
| | Implementation inspection results report | O |
| | Vulnerability remediation guide | O |

■ The advantages of the infrastructure vulnerability inspection are as follows.

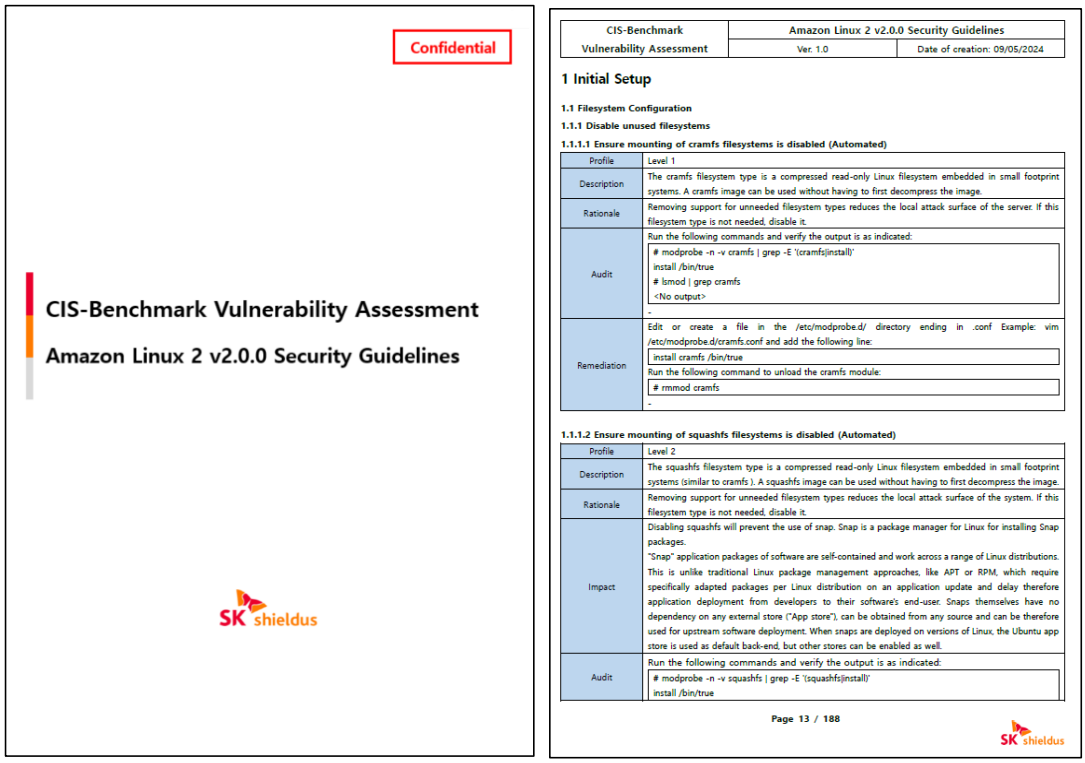
| No | Key Benefits | Description |
|---|---|---|
| 1 | **Reduced Working Hours** | Quick identification of vulnerabilities, including delegation of vulnerability inspection and report creation. |
| 2 | **Improved Readability** | Provides the result reports and remediation guides written in English as Korean-language documents |
| 3 | **Advanced Services** | Provides vulnerability explanations, remediation guides, technical support, and Q&A services. |
| 4 | **Optimized Inspection** | Cloud-native inspection optimization using AWS Inspector |
| 5 | **Up-to-date Vulnerability Inspection** | Automatic integration of the latest security vulnerabilities and inspection criteria through AWS Inspector. |
| 6 | **Reduced Inspection Risks** | Vulnerability inspections are executed using AWS automation rather than script-based execution. |

■ We provide infrastructure vulnerability inspection result reports and remediation guides.

※ The images below are samples.




**[Vulnerability Inspection Result Report]**



Confidential

CIS-Benchmark Vulnerability Assessment

Amazon Linux 2 v2.0.0 Security Guidelines

SK shieldus

| CIS-Benchmark Vulnerability Assessment | Amazon Linux 2 v2.0.0 Security Guidelines | |
|---|---|---|
| | Ver. 1.0 | Date of creation: 09/05/2024 |

## 1 Initial Setup

### 1.1 Filesystem Configuration

### 1.1.1 Disable unused filesystems

#### 1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Automated)

| | |
|---|---|
| Profile | Level 1 |
| Description | The cramfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A cramfs image can be used without having to first decompress the image. |
| Rationale | Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it. |
| Audit | Run the following commands and verify the output is as indicated:<br># modprobe -n -v cramfs \| grep -E '(cramfs\|install)'<br>install /bin/true<br># lsmod \| grep cramfs<br><No output><br>- |
| Remediation | Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/cramfs.conf and add the following line:<br>install cramfs /bin/true<br>Run the following command to unload the cramfs module:<br># rmmod cramfs<br>- |

#### 1.1.1.2 Ensure mounting of squashfs filesystems is disabled (Automated)

| | |
|---|---|
| Profile | Level 2 |
| Description | The squashfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems (similar to cramfs ). A squashfs image can be used without having to first decompress the image. |
| Rationale | Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it. |
| Impact | Disabling squashfs will prevent the use of snap. Snap is a package manager for Linux for installing Snap packages.<br>"Snap" application packages of software are self-contained and work across a range of Linux distributions. This is unlike traditional Linux package management approaches, like APT or RPM, which require specifically adapted packages per Linux distribution on an application update and delay therefore application deployment from developers to their software's end-user. Snaps themselves have no dependency on any external store ("App store"), can be obtained from any source and can be therefore used for upstream software deployment. When snaps are deployed on versions of Linux, the Ubuntu app store is used as default back-end, but other stores can be enabled as well. |
| Audit | Run the following commands and verify the output is as indicated:<br># modprobe -n -v squashfs \| grep -E '(squashfs\|install)'<br>install /bin/true |

Page 13 / 188

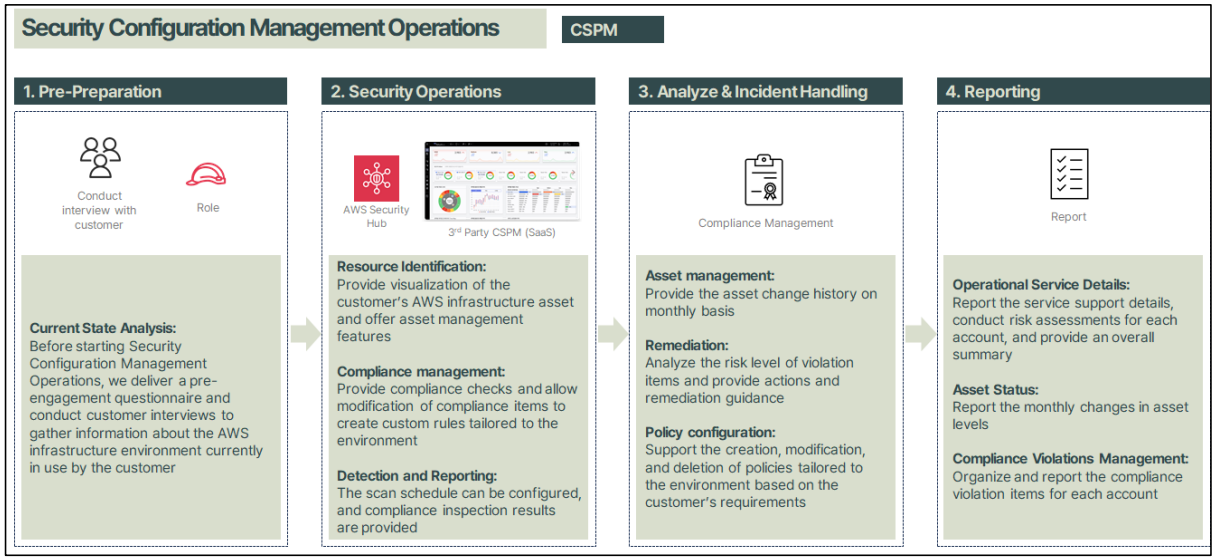
SK shieldus

**[Vulnerability Inspection Remediation Guide]**

## 2.3. Security Configuration Management Operations

Security configuration management operations utilize a CSPM solution to monitor service configurations and policies for customer AWS cloud infrastructure assets. Customers can choose either AWS-native Security Hub or a third-party CSPM solution, as SK shieldus supports both. This service identifies security vulnerabilities, and provide operations including remediation, asset management, and policy configuration based on inspection results.

■ The procedure of security configuration management operations is as follows.




■ Key features of security configuration management operations are as follows.

| Key Features | Description |
|---|---|
| **Resource Identification** | Provides resource visualization |
| | Provides resource management functions |
| **Compliance Management** | Provides compliance checks (default 13 compliance) |
| | Provides compliance modifications and creation |
| **Detection and Reporting** | Provides setting inspection cycle |
| | Provides inspection result reports |

■ The coverage of security configuration management operations is as follows.

| Coverage | Description | |
|---|---|---|
| **Operational Environment Setup** | Build support | Supports for status analysis and account integration |
| | Initial policy configuration | Supports for policy configuration based on requirements |
| **Operations** | Asset management | Provides asset change history |
| | Remediation | Provides remediation actions and detailed action plans |

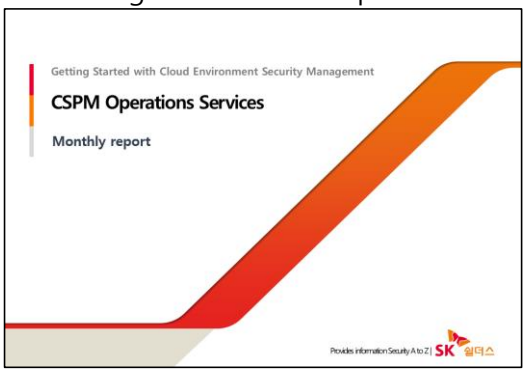
| | | |
|---|---|---|
| | Policy configuration | Supports creation, modification, and deletion of policies |
| | Reports | Provides Weekly and monthly reports |
| **Technical Support** | Maintenance support | Supports issue resolution and version patching |
| | Inquiry response | Supports Technical Q&A |

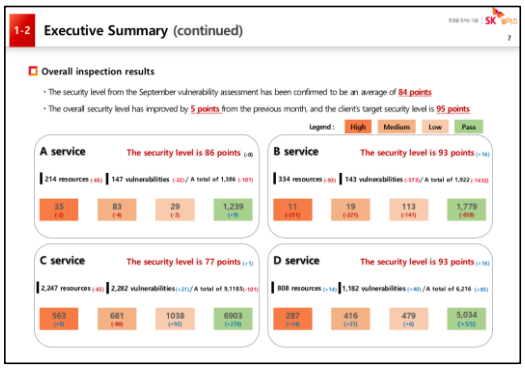
■ The advantages of security configuration management operations are as follows.

| No. | Key Benefits | Description |
|---|---|---|
| 1 | **Operational Stability** | Achieves operational stability and reliability by applying CSPM solution operational know-how to the customer |
| 2 | **Security Management Efficiency** | Enables quick, accurate vulnerability management and precise vulnerability analysis by applying optimized operational processes. |
| 3 | **Reduced Workload** | Reduces workload by supporting the expertise (e.g., understanding cloud environments, compliance). |
| 4 | **Cost Reduction** | Reduces operational costs and minimizes opportunity costs due to gaps in operating staffs. |

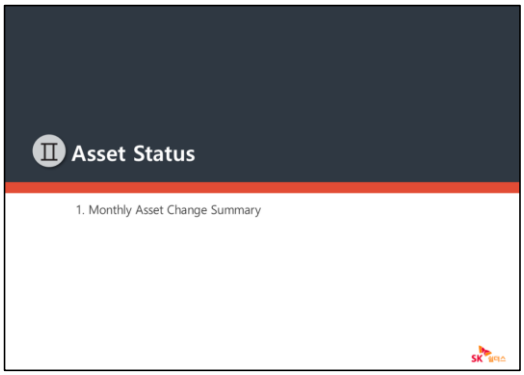
■ We perform operations for security configuration management operations and provide regular reports on them.

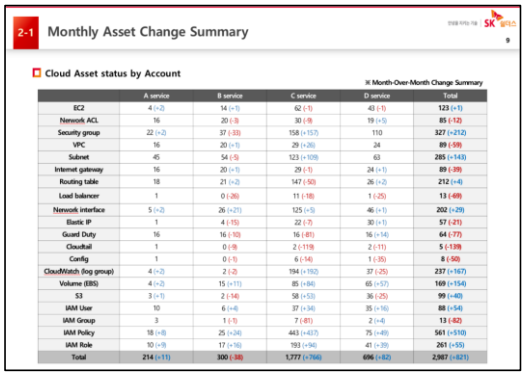
※ The images below are samples.




**[Monthly Report]**



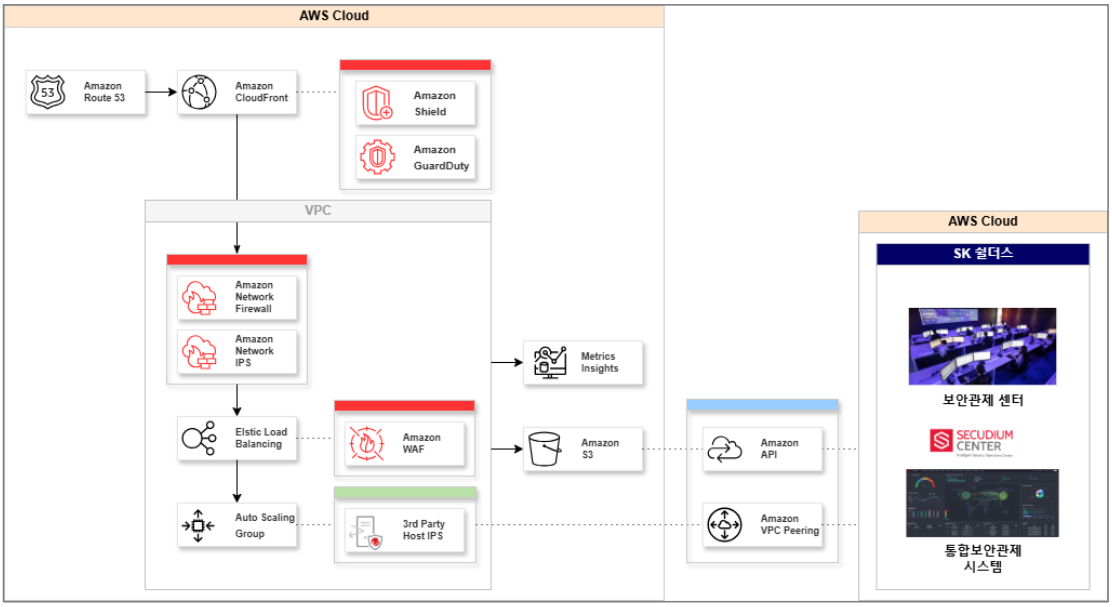




**[Asset Status Report]**

## 2.4. Security Monitoring/Operations

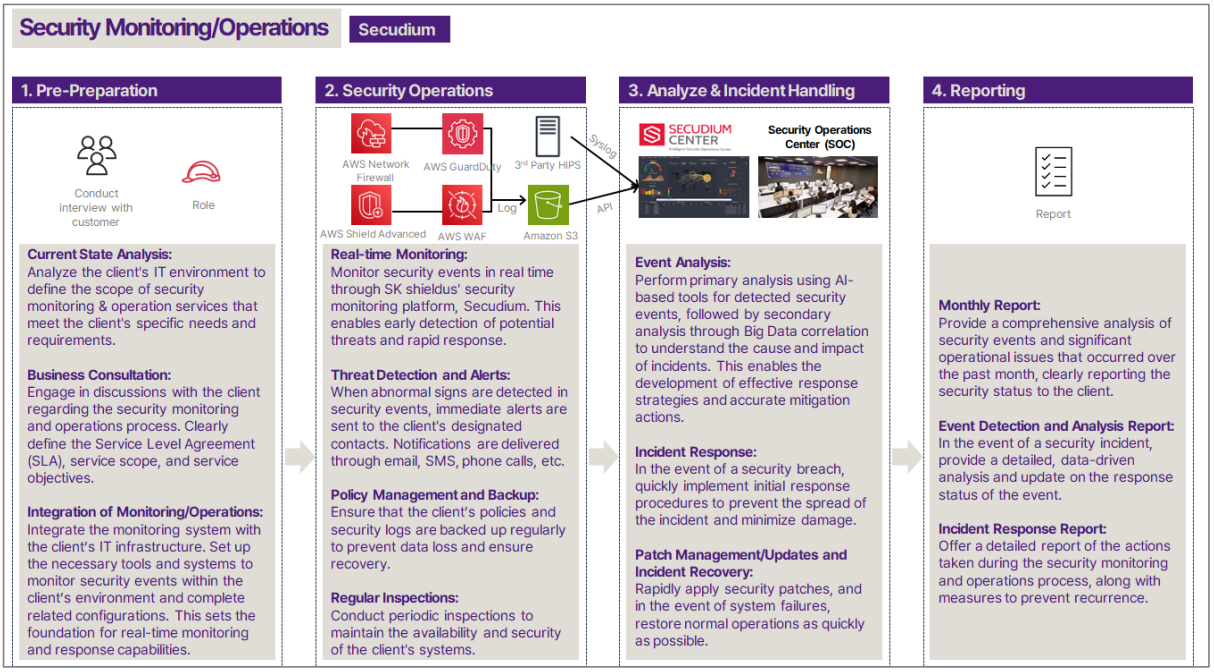
SK shieldus leverages its accumulated know-how to provide 24/7 continuous security monitoring, protecting customer services against advanced cyber threats. By integrating AWS native services with third-party solutions, we deliver comprehensive security management. As a certified AWS partner with extensive experience and expertise, we ensure stable and efficient cloud operations through AWS-native security operations and customized cloud solution deployments tailored to various customer environments.

■ The key features of security monitoring/operations are as follows.




| No | Features | | Description |
|---|---|---|---|
| 1 | **AWS Shield Advanced** | | Enhances visibility and resilience against DDoS attacks, improving application availability while effectively reducing risks associated with financial loss and security threats. |
| 2 | **AWS Network Firewall** | | Supports remote operations by managing access control policies for internal and external traffic, protecting internal assets from unauthorized access. |
| 3 | **IPS** | **AWS Network Firewall** (Network-based) | Detects and analyzes internal and external attacks in real-time, to protect internal assets and ensure service availability. |
| | | **Third-party** (Host-based) | Strengthens security posture by deploying agents on AWS-based endpoints to detect and prevent anomalous activities and known threat patterns effectively. |
| 4 | **AWS WAF** | | Provides remote security monitoring by detecting and blocking a wide range of attacks targeting web applications in real-time, protecting customer information assets. |
| 5 | **AWS Guard duty** | | Detects and notificates anomalous behaviors and misconfigured permissions in AWS IAM, S3, EC2, and other services in real-time. |

■ The procedure of the security monitoring/operations is as follows.




■ The coverage of security monitoring/operations is as follows.

| Features | AWS Shield Advanced | AWS Network Firewall | IPS | | AWS WAF | AWS GuardDuty |
|---|---|---|---|---|---|---|
| | | | AWS Network Firewall (Network-based) | Third-party (Host-based) | | |
| | (O : Provided, - : Not Provided) | | | | | |
| Technical Support (Implementation / Configuration) | O | O | O | O | O | O |
| Log Management | O | - | O | O | O | O |
| Policy Management | O | O | O | O | O | - |
| Availability Management | O | - | - | O | - | - |
| Operational Management | O | O | - | - | - | O |
| Monitoring (24x7) | O | - | O | O | O | O |
| Reports | O | O | O | O | O | O |

■ The key advantages of security monitoring/operations are as follows.

| No | Key Benefits | Description |
|---|---|---|
| 1 | **Expert Security Monitoring Staffs and Capabilities** | We have the largest number of specialized security monitoring and incident response personnel (Top-CERT) in the security industry and respond to incidents in a systematic manner, minimizing the loss of information assets and enhancing customer trust through customized security services. |
| 2 | **No. 1 Security Monitoring Expertise in Korea** | By continuously detecting and blocking threats through 24/7 continuous monitoring, we minimize security blind spots and provide a stable operational environment that ensures service continuity (serving over 3,000 clients and integrating with over 5,200 security devices). |
| | | We provide optimized monitoring for customer environments using our in-house developed integrated security monitoring system, ensuring flexible response and high operational efficiency. |
| | | By detecting over 6,000 attack patterns based on our proprietary ISMM (Infosec* Security Monitoring Methodology), we provide a comprehensive defense system to address various attack scenarios. (Infosec*: SK Shields' cybersecurity brand name) |
| | | We enhance detection accuracy, reduce operational costs, and maximize the efficiency of security monitoring operations through AI-based analysis and big data technologies. |
| 3 | **Cloud-Specific Security Monitoring** | We expand monitoring coverage to include a wide range of AWS Native services. |

**[Security Monitoring]**

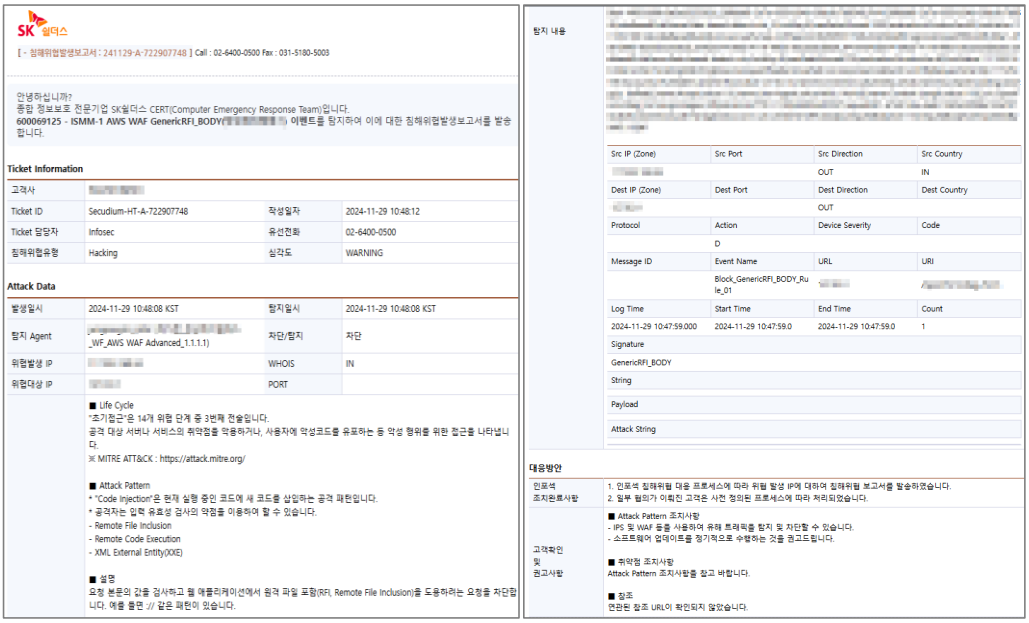
| No | Key Benefits | Description |
|---|---|---|
| 1 | **Verified AWS Security Operations Expertise** | As an Advanced Tier partner, we have earned the "Perimeter Protection MSSP" qualification, recognized for our reliability and expertise. |
| | | We provide solutions optimized for customer cloud security requirements by directly supporting AWS security experts. |
| | | We launched the first AWS DDoS mitigation service in Korea, establishing a robust Distributed Denial of Service (DDoS) mitigation system |
| 2 | **SK shieldus' Specialized Security Operations Expertise** | We offer structured security operations including operational management, security management, issue, and incident handling, change history management, and backup and recovery management. |
| 3 | **Cloud Security Operations** | We provide remote security operations within the AWS Native environment, supporting efficient cloud security management. |
| | | We provide customized security solutions through solution deployment and operations within the cloud environment, maximizing operational efficiency. |

**[Security Operations]**

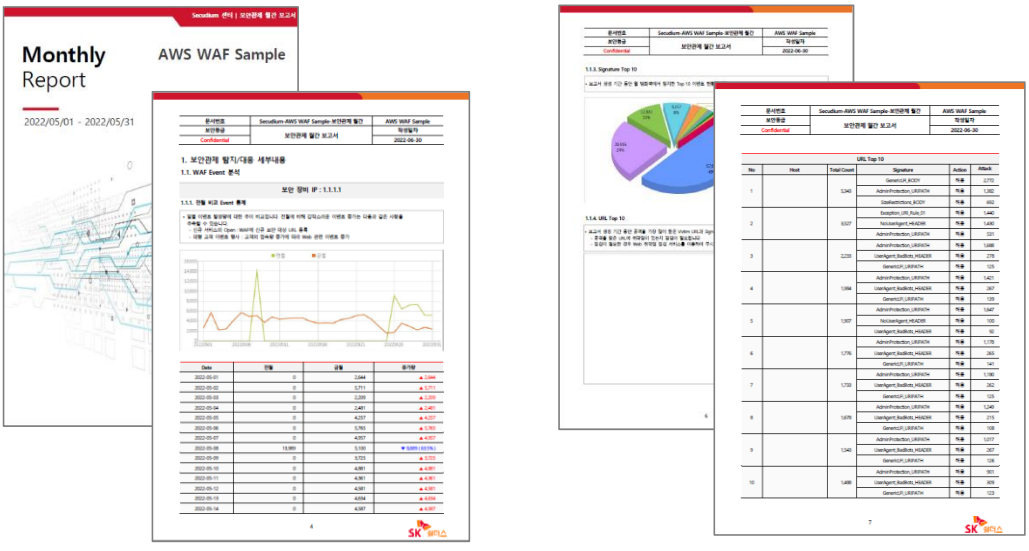
■ We provide security monitoring/operations reports as follows.

※ The images below are samples.


**[Secudium Dashboard]**




**[Threat Incident Report]**



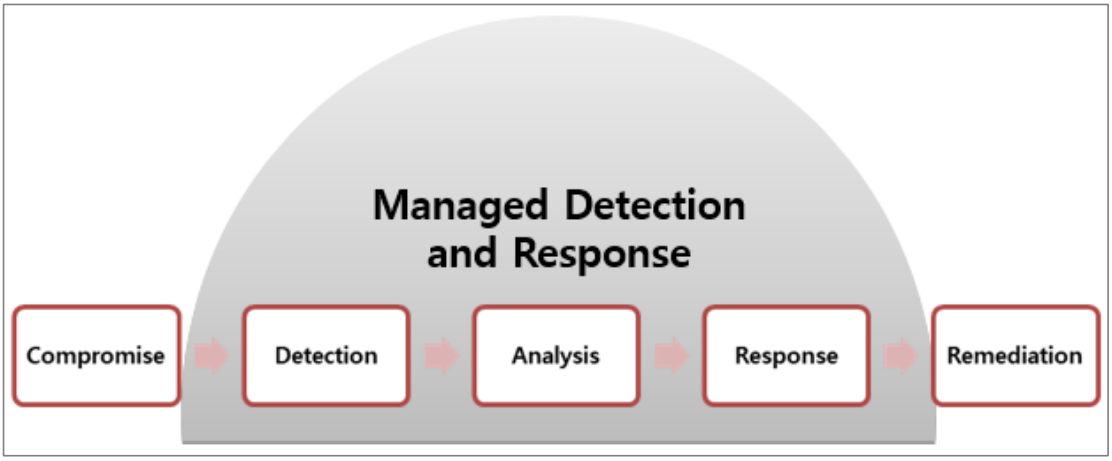

**[Monthly Report]**

## 2.5. MDR Security Solution Implementation

SK shieldus offers Trend Micro's MDR implementation that detects and responds to security threats within an organization.

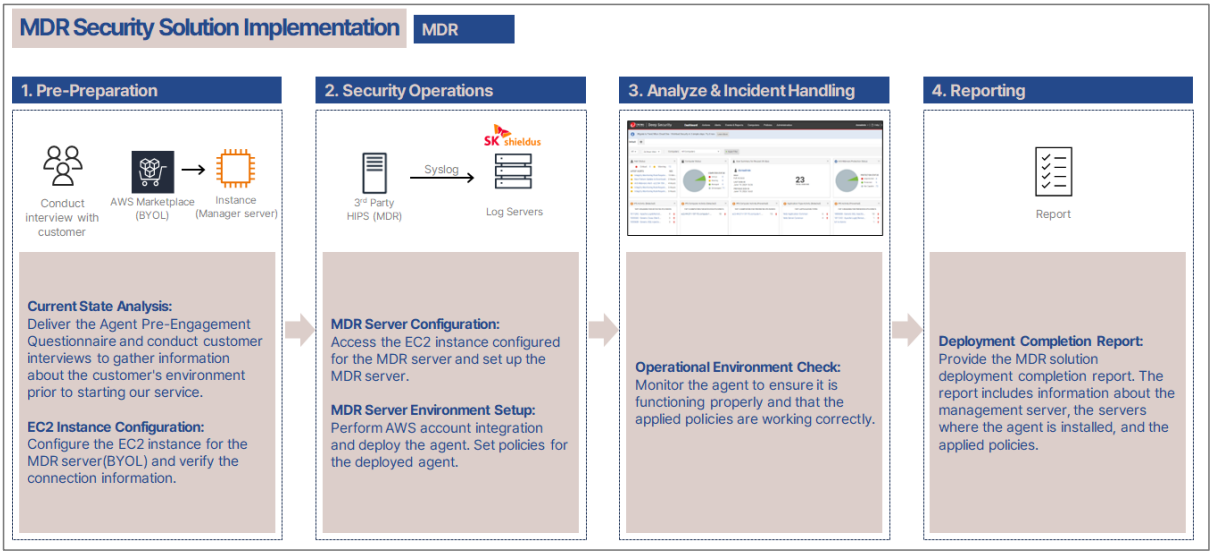
Trend Micro's MDR provides a wide array of security services, including alert monitoring, alert prioritization, investigation, and threat hunting. It uses artificial intelligence models and applies them to endpoint, network, and server data to correlate and prioritize advanced threats.

Through the implementation of the MDR security solution, we provide solution implementation that enable threat detection, response, and incident investigation.




| No | Features | Description |
|---|---|---|
| 1 | **Detection** | Trend Micro threat researchers continuously monitor an organization's network and endpoint data — performing threat sweeps to look for specific indicators of compromise — and from there make decisions in terms of threat prioritization. |
| 2 | **Analysis** | Once a detected potential threat is correlated and prioritized, a team of qualified security operations center (SOC) personnel investigate the origin and scope of the attack, after which a detailed analysis of the threat and its impact is determined. |
| 3 | **Response** | Trend Micro threat researchers will alert the organization of the incident, and will also provide root cause analysis, mitigation recommendations, and toolkits to help the organization handle the incident. |

■ The procedure of the MDR Security Solution Implementation is as follows.

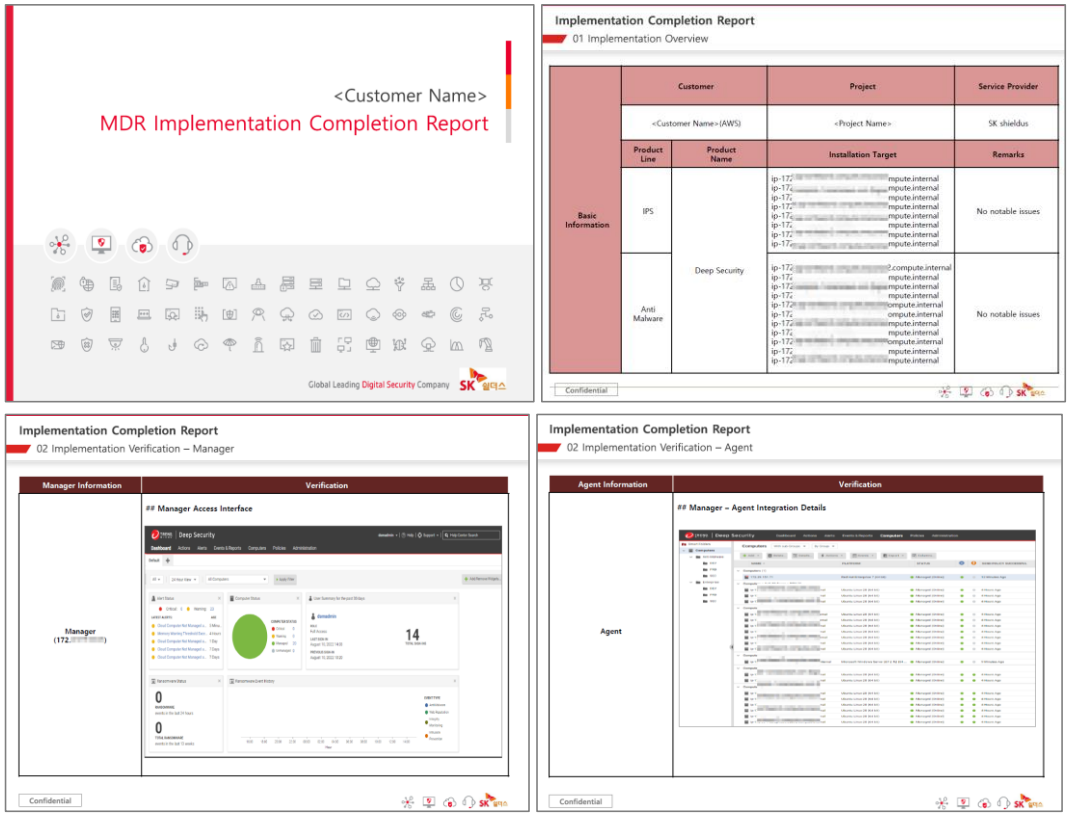



■ Key features of the MDR Security Solution Implementation are as follows.

- Identify instance assets within the AWS account
  - ✓ Agent installed instance: Metadata(Public/Private DNS, Instance ID, and others) can be verified
  - ✓ Agent uninstalled instance: Instances across all regions in the AWS Account linked to the solution can be verified
- Detection of Security Incidents: Detectable through Predictive Machine Learning, Threat Intelligence, Behavior Monitoring
- Containment of Incidents at the Endpoint: Malware detected through the above detection technology is detected/blocked according to the malware type (see ActiveAction default settings), and blocked files can be checked in Anti-Malware Events > Identified Files.
- Investigation of Security Incidents: Possible to view detailed malware events that occurred (file location, process name that occurred, malware attack target, malware type, etc.) can be identified.
- Provision of Remediation Guidance: Windows can treat some types (Virus) and isolate those that cannot be cured; Linux can only quarantine (see ActiveAction)

■ We provide implementation completion report.

※ The images below are samples




**[Implementation Completion Report]**

## 3. SK shieldus Overview

It is the optimal solution for flexible and agile responses to rapidly changing advanced cyber threats.

24/7 monitoring and protection against cyber-attacks, provision of telecommuting infrastructure, information protection service support, etc. We provide thorough security services to prevent and respond to viruses and hacking faster.

■ **Main Features**

| No | Features | Description |
|---|---|---|
| 1 | **Remote Security Monitoring** | We provide integrated services for network security, targeting both Cloud Native Security Services and third-party solutions. The remote security monitoring service offers 24/7 security surveillance, threat prevention, and incident investigation and analysis services in the event of a security breach. |

| | | |
|---|---|---|
| **2** | **SI/Solution** | We build security solutions tailored to diverse cloud environments for enterprises.<br>• Implementation of third-party security solutions for network, databases, data, applications, and end-users.<br>• Deployment of security services provided by Cloud Service Provider (CSP).<br>• Integrated service establishment for security services and solutions.<br>• Providing Cloud-Oriented Security Solutions (SWG, CWPP, CSPM). |
| **3** | **Security Consulting** | Fundamental services when adopting cloud technology:<br>• Cloud Security Certification<br>• Cloud Security Migration<br>• Cloud Security Architecture Design<br>• Metaverse Platform Security Review<br>• Cloud Data Security<br>• Establishment of Cloud Security Management Framework<br>• Cloud Security Assessment |
| **4** | **Operational Services** | We provide 24/7 protection for security equipment, and in emergency situations, we prioritize support through the remote security monitoring center's call center. |

## 4. Support/Contact Point

Should you have any inquiries, please do not hesitate to reach out to us. We will get back to you as soon as possible. Thank you.

1. Service-related Inquiries
   - E-Mail: infocloudtech@skshieldus.com / infocloudops@skshieldus.com
2. Technology-related Inquiries
   - E-Mail: infocloudtech@skshieldus.com / infocloudops@skshieldus.com