SK shieldus

Managed Security Services Provider on Amazon Web Services

목차

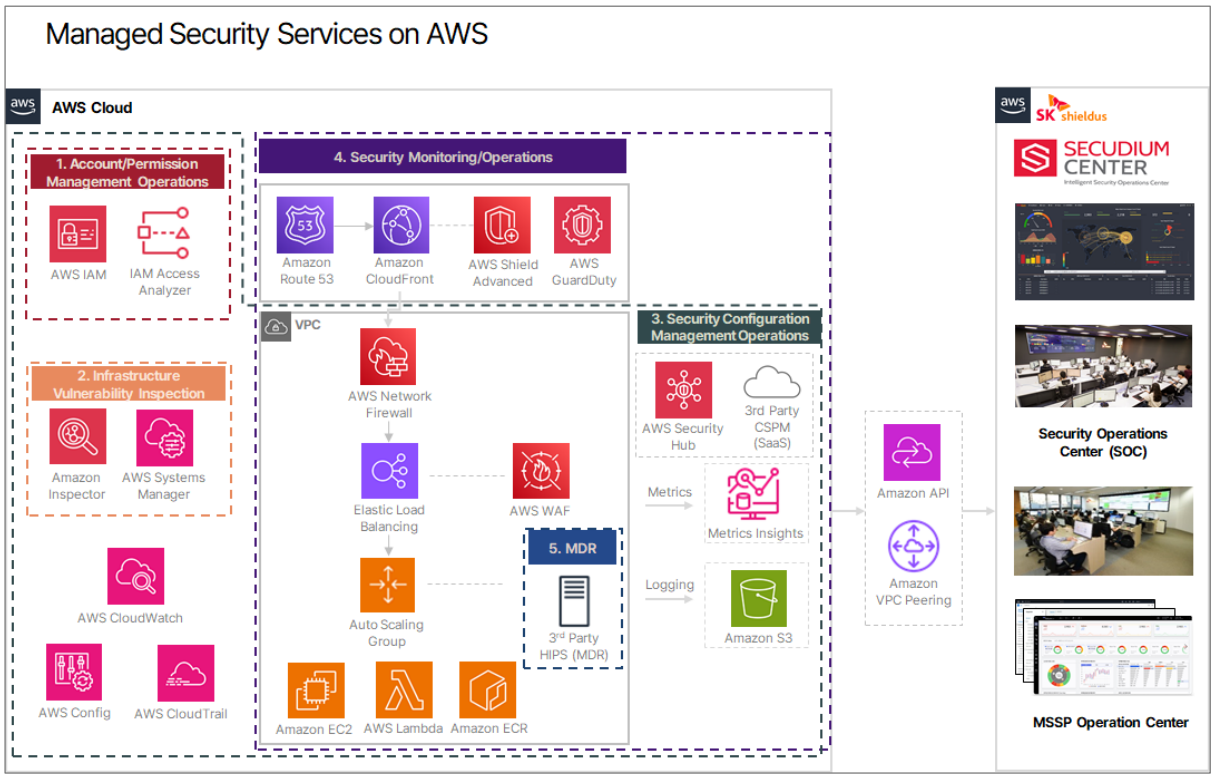
1. 서비스 개요

에스케이쉴더스㈜의 Managed Security Services Provider on AWS는 AWS 클라우드 환경에서의 보안 관리를 전문적으로 제공하는 서비스입니다. 고객의 워크로드를 24/7 모니터링하고, 위협을 탐지하며, 보안 전문가가 정확하고 효과적으로 사고 대응을 지원합니다. 또한, 주요 규정 준수와 보안 정책 관리, 취약점 평가 및 개선 권고를 통해 클라우드 환경의 보안을 체계적으로 강화합니다. 고객 환경에 최적화된 보안 솔루션을 제안하고 상세한 보고서를 제공합니다. 이를 통해 고객이 더욱 안전하고 신뢰할 수 있는 클라우드 인프라를 구축할 수 있도록 돕는 종합적인 보안 관리 서비스를 제공합니다.

AWS의 다양한 보안 서비스 및 서드파티 보안 툴의 기능을 최대한 활용하는 전문가의 도움을 받아 복잡한 클라우드 환경의 보안을 효과적으로 관리하고, 최적화할 수 있습니다. 이를 통해 보안 운영의 부담을 줄이고, 고객은 안전한 클라우드 환경에서 핵심 비즈니스에 더욱 집중할 수 있습니다.

■ **Managed Security Services Provider on AWS에 대한 상세 설명은 고객에게 5가지 카테고리로 제공되며, 아래에 간단한 아키텍처가 표기되어 있습니다.**

1. **계정/권한 관리 운영**
2. **인프라 취약점 점검**
3. **보안 형상 관리 운영**
4. **보안 관제/운영**
5. **MDR 보안 솔루션 구축**



* HIPS: 호스트 기반 IPS (Host based IPS)

* MDR: MDR 보안 솔루션 구축

Managed Security Services Provider on AWS는 고객의 AWS 클라우드 환경의 보안을 통합적으로 관리하여 복잡한 보안 문제를 손쉽게 해결할 수 있도록 지원합니다. 이를 통해 고객은 더욱 안전하고 최적화된 클라우드 환경을 구축할 수 있으며, 안정성을 바탕으로 비즈니스 성장을 촉진하고 경쟁력을 높일 수 있습니다.

2. 상세 서비스 소개

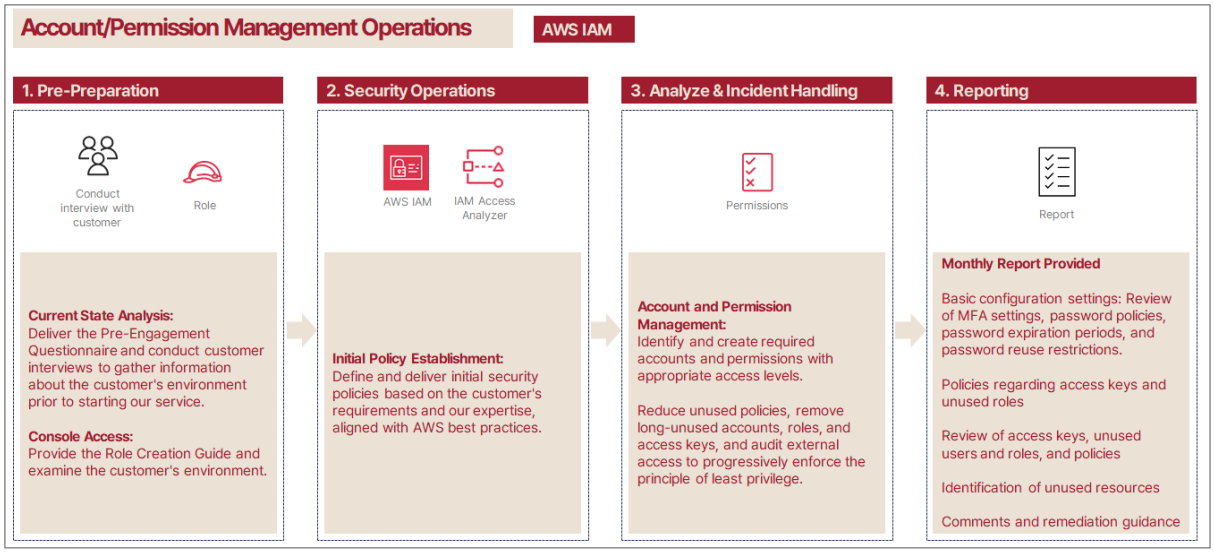
2.1. 계정/권한 관리 운영

AWS IAM (Identity and Access Management) 계정/권한의 보안을 강화하고, 서비스 및 리소스에 대한 접근을 안전하게 관리하기 위하여 AWS 모범사례를 기반으로 한 계정/권한 관리 운영 서비스를 제공합니다.

계정/권한 관리 운영을 위해 임시 자격 증명(AssumeRole)을 사용하여 고객의 AWS Account에 접근하며, AWS IAM 및 IAM Access Analyzer 리소스를 이용하여 계정/권한에 대한 관리와 점검을 수행합니다.

고객의 사용자가 필요로 하는 계정/권한을 확인하고 적절한 범위의 권한을 지정하여 생성합니다. 미사용 정책에 대한 권한 축소, 장기 미사용 계정/역할 및 액세스 키 삭제, 외부 액세스 점검을 통해 점진적으로 최소 권한을 적용하여, 고객의 계정/권한을 보호합니다.

■ 계정/권한 관리 운영 서비스 절차는 아래와 같습니다.

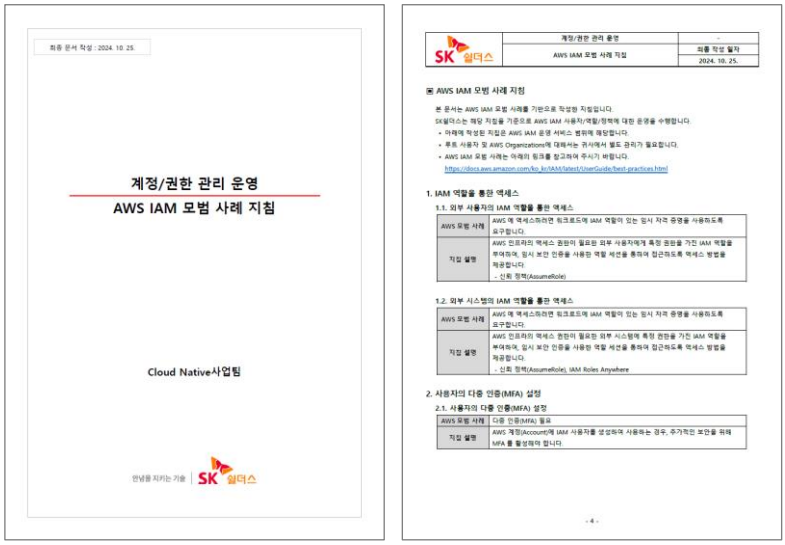


■ 계정/권한 관리 운영 서비스 범위는 아래와 같습니다.

서비스 범위		제공 여부
기술 지원	기술 지원(구성/가이드)	제공
	AWS Support 문의 대응	필요시 제공
계정 및 권한 관리	계정 및 권한 설정/관리	제공
	권한 최적화(커스터마이징)	제공
	백업/복구 관리	제공
	변경 이력 관리	제공
액세스 분석	외부 액세스 분석	제공

운영 관리	운영 현황 관리	제공
	관리 문의 대응	제공
	운영 이력 관리	제공
	정기 점검	제공
리포트	월간 리포트	제공

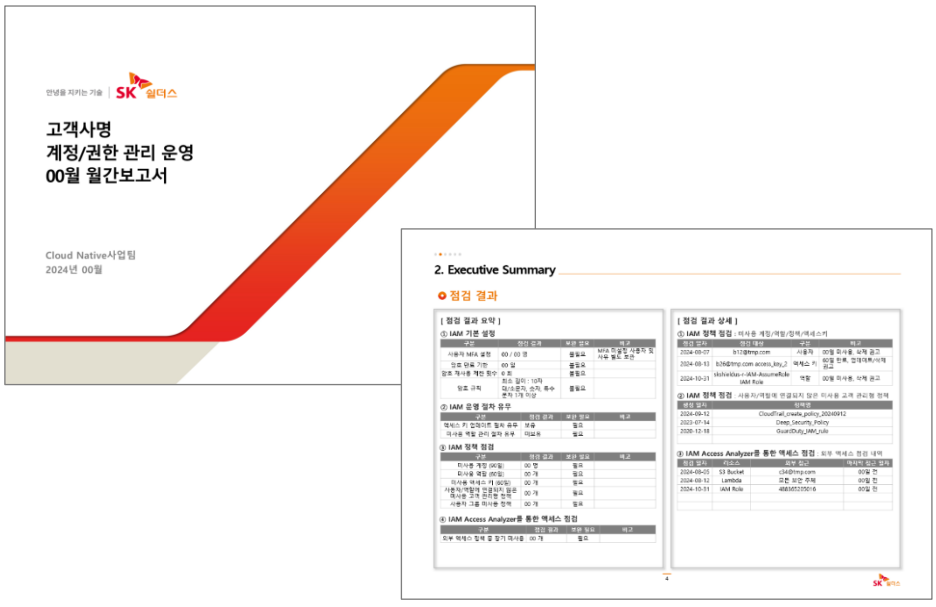
■ AWS IAM 모범 사례 지침 문서를 제공하여, 고객의 관리가 필요한 내용을 전달합니다.



[AWS IAM 모범 사례 지침 문서]

■ 고객의 AWS IAM에 대한 운영을 수행하고, 이에 대한 정기 보고서를 제공합니다.

※ 아래의 이미지는 샘플입니다.



[월간 보고서]

2.2. 인프라 취약점 점검

AWS 인프라 취약점에 대한 식별과 평가, 보완을 위해 AWS Inspector를 이용하여 Amazon Elastic Compute Cloud (Amazon EC2)와 Amazon Elastic Container Registry (Amazon ECR)을 대상으로 보안 취약점 점검 서비스를 제공합니다.

AWS Native 서비스 Inspector의 점검대상 자동 감지 기능의 장점을 활용하여 고객을 대상으로 취약점 점검 서비스를 자동화 형식으로 제공하고 있으며, Inspector에서 제공하고 있는 점검 대상의 여러가지 메타데이터를 포함하여 취약점 점검 결과 보고서 및 취약점 조치 가이드를 제공합니다.

고객의 인프라 취약점에 대한 보안 강화를 위해 1차 초기 점검 및 보완 작업을 진행한 후 2차 이행 점검 서비스도 제공하면서 고객 인프라 취약점으로 인해 보안사고가 발생하지 않도록 보호합니다.

■ 인프라 취약점 점검 서비스 절차는 아래와 같습니다.

■ 인프라 취약점 점검 서비스 범위는 아래와 같습니다.

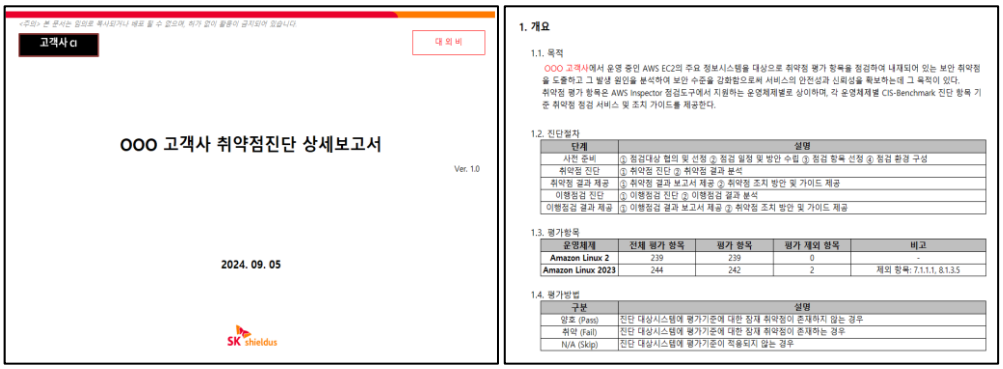
서비스 범위		제공 여부
기술 지원	점검환경 구성 (구성/가이드)	제공
	AWS Support 문의 대응	제공
취약점 점검	초기 점검 (점검/가이드)	제공
	이행 점검 (점검/가이드)	제공
보고서	취약점 점검 결과 보고서	제공
	이행점검 결과 보고서	제공
	취약점 조치 가이드	제공

■ 인프라 취약점 점검 서비스 특장점은 아래와 같습니다.

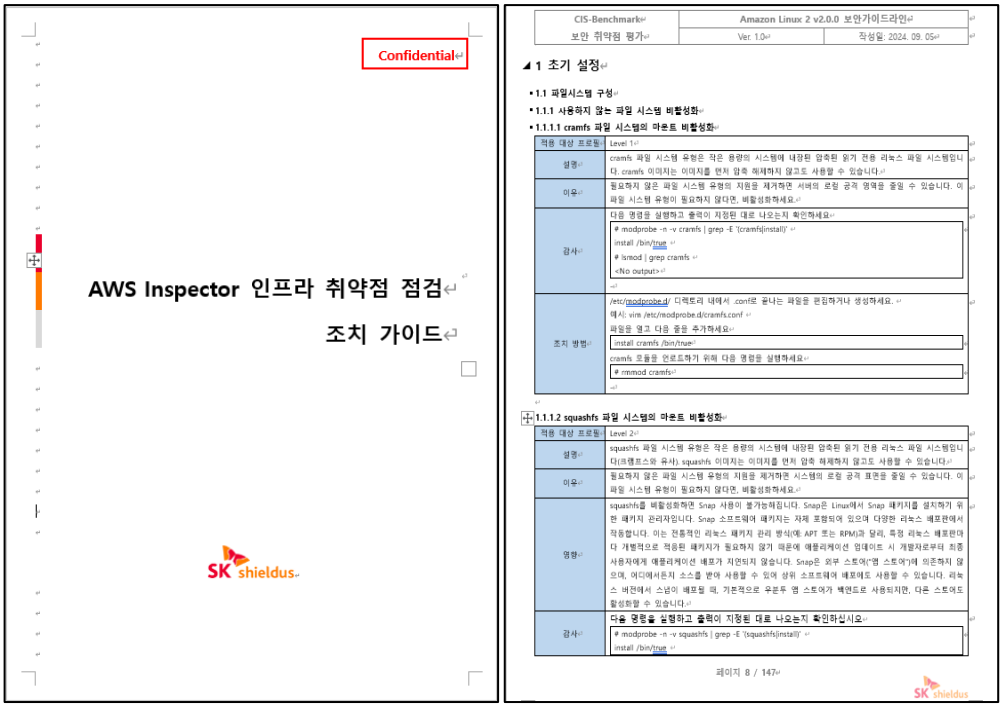
No	특장점	설명
1	업무 시간 단축	취약점 대행 및 보고서 제공 등 신속한 취약점 파악
2	가독성 향상	영문 결과 보고서 및 조치 가이드에 대한 한글 문서 제공
3	고도화 서비스 제공	취약점 설명, 조치 가이드, 기술 지원, 질의 응답 등 서비스 제공
4	점검 최적화	AWS Inspector 활용으로 Cloud Native 점검 최적화
5	최신 취약점 점검	최신 보안 취약점 및 점검 항목 등 AWS Inspector 자동 반영
6	점검 위험도 감소	스크립트 실행 방식이 아닌 AWS 자동화 취약점 점검 실행

■ 인프라 취약점 점검 결과 보고서 및 취약점 조치 가이드를 제공합니다.

※ 아래의 이미지는 샘플입니다.



[취약점 점검 결과 보고서]

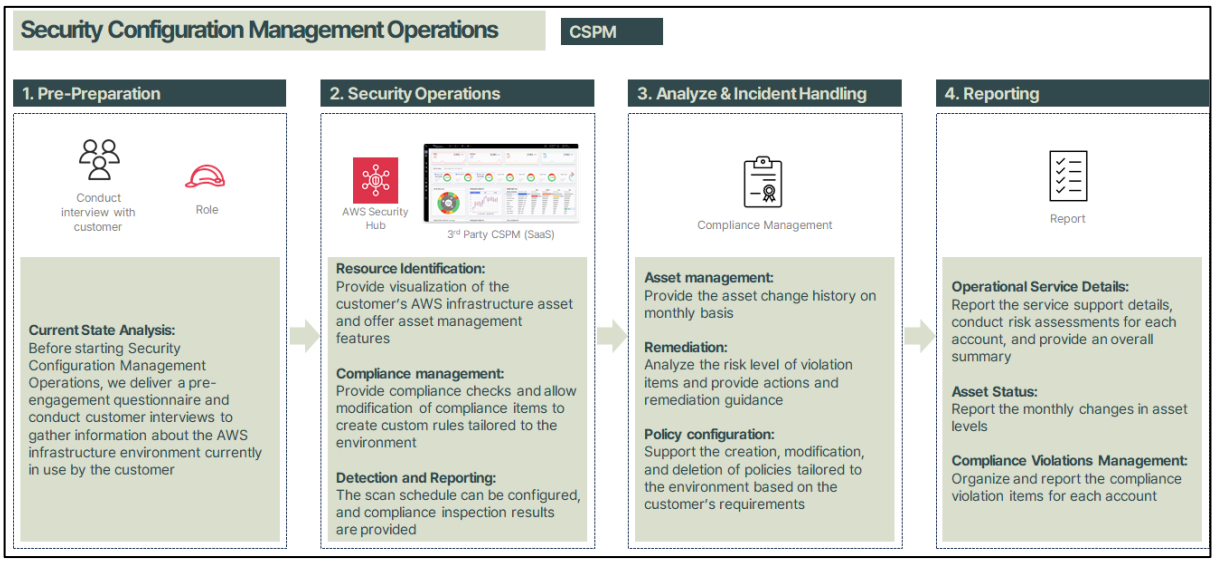


[취약점 조치 가이드]

2.3. 보안 형상 관리 운영

보안 형상 관리 운영은 CSPM 솔루션을 활용하여 고객 AWS 클라우드 인프라 자산에 대한 서비스 구성 및 정책을 모니터링합니다. 이 서비스는 보안 취약점을 식별하고, 검사 결과를 기반으로 조치대응, 자산관리, 정책구성 등을 지원하는 운영 서비스입니다.

■ 보안 형상 관리 운영 절차는 아래와 같습니다.



■ CSPM 솔루션의 주요기능은 아래와 같습니다.

기능명	기능 설명
리소스 식별	리소스 시각화 제공
	리소스 관리기능 제공
컴플라이언스 관리	컴플라이언스 점검 제공 (기본 13개 컴플라이언스 제공)
	컴플라이언스 수정 및 생성 기능 제공
탐지 및 보고	점검 주기 설정 가능
	점검 결과 리포트 제공

■ 보안 형상 관리 운영 서비스 범위는 아래와 같습니다.

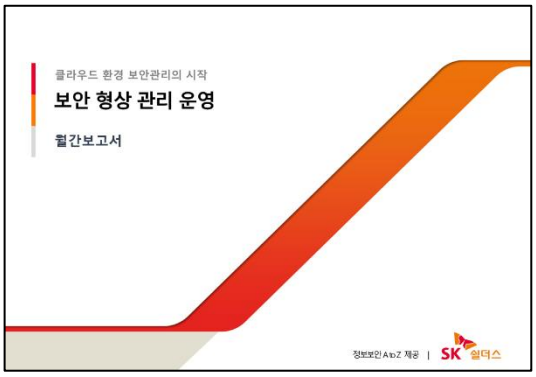
서비스명	서비스 설명	
운영환경설정	구축지원	현황분석 및 계정 연동지원
	초기정책 설정	요구조건에 맞는 정책 설정 지원
운영서비스	자산관리	자산 변동내역 자료제공
	조치대응	조치 및 상세 조치방안 제공
	정책설정	정책 생성, 수정, 삭제 지원
	리포트	주간, 월간 리포트 제공
기술지원	유지보수	이슈 발생 및 버전 패치 지원
	문의대응	기술 Q&A 지원

■ 보안 형상 관리 운영의 특장점은 아래와 같습니다.

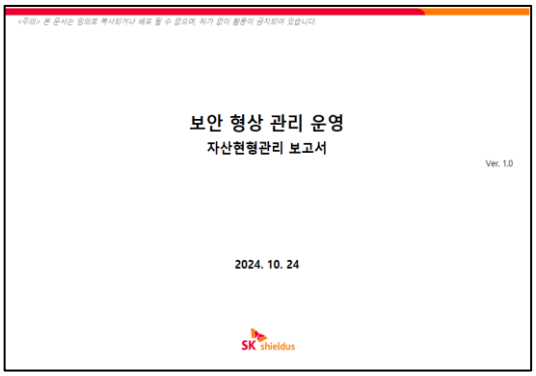
No.	특장점	기능 설명
1	운영 안정성	CSPM 솔루션 운영 노하우를 고객사에 적용함으로써 운영의 안정성과 신뢰성 확보
2	보안관리 효율성	최적화된 운영프로세스 적용으로 신속, 정확한 취약점 관리 및 정확한 취약점 분석 가능
3	업무부담 경감	담당자가 갖춰야 할 역량을 지원함으로써 업무부담 경감 (클라우드 환경에 대한 이해, 컴플라이언스 이해 등)
4	비용절감	운영비용 절감 및 운영인력 공백에 따른 기회비용 최소화

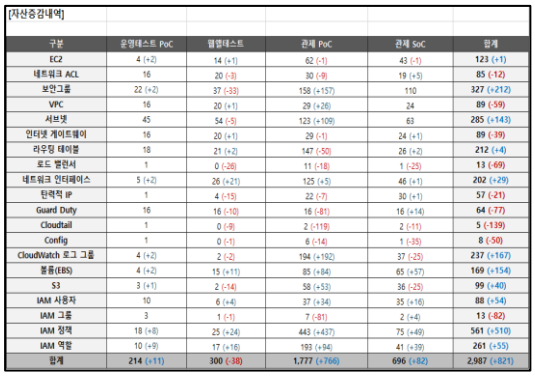
■ 보안 형상 관리 운영은 서비스 운영을 수행하고, 이에 대한 정기 보고서를 제공합니다.

※ 아래의 이미지는 샘플입니다.



[월간보고서]





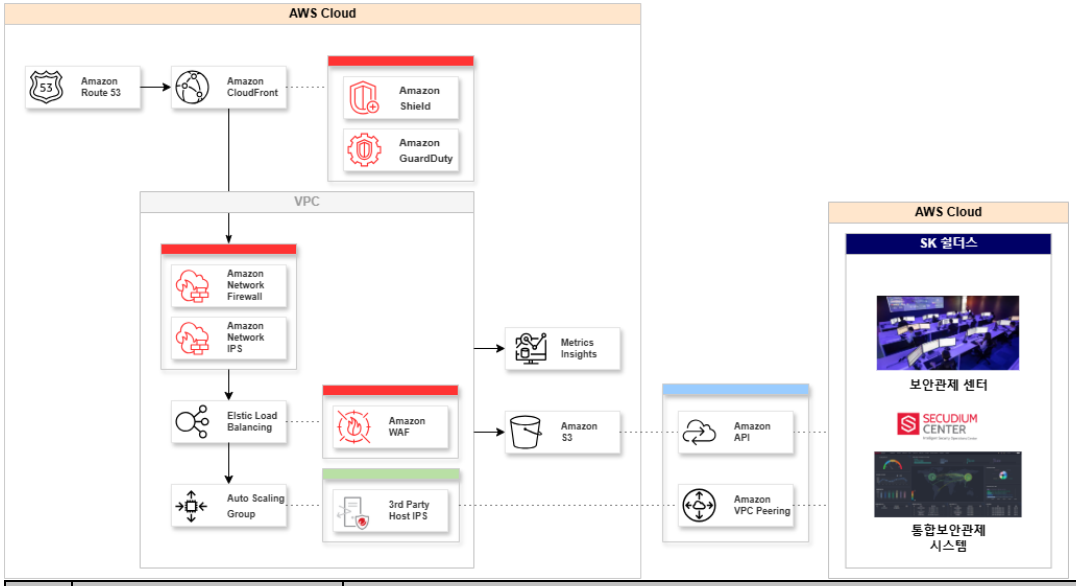
구분	운영테스트 PoC	랩엔테스트	관제 PoC	관제 SoC	합계
EC2	4 (+2)	14 (+1)	62 (-1)	43 (-1)	123 (+1)
네트워크 ACL	16	20 (-3)	30 (-9)	19 (+5)	85 (-12)
보안그룹	22 (+2)	37 (-33)	158 (+157)	110	327 (+212)
VPC	16	20 (+1)	29 (+26)	24	89 (-59)
서브넷	45	54 (-5)	123 (+109)	63	285 (+143)
인터넷 게이트웨이	16	20 (+1)	29 (-1)	24 (+1)	89 (-39)
라우팅 테이블	18	21 (+2)	147 (-50)	26 (+2)	212 (+4)
로드 밸런서	1	0 (-26)	11 (-18)	1 (-25)	13 (-69)
네트워크 인터페이스	5 (+2)	26 (+21)	125 (+5)	46 (+1)	202 (+29)
탄력적 IP	1	4 (-15)	22 (-7)	30 (+1)	57 (-21)
Guard Duty	16	16 (-10)	16 (-81)	16 (+14)	64 (-77)
Cloudtail	1	0 (-9)	2 (-119)	2 (-11)	5 (-139)
Config	1	0 (-1)	6 (-14)	1 (-35)	8 (-50)
CloudWatch 로그 그룹	4 (+2)	2 (-2)	194 (+192)	37 (-25)	237 (+167)
볼륨(EBS)	4 (+2)	15 (+11)	85 (+84)	65 (+57)	169 (+154)
S3	3 (+1)	2 (-14)	58 (+53)	36 (-25)	99 (+40)
IAM 사용자	10	6 (+4)	37 (+34)	35 (+16)	88 (+54)
IAM 그룹	3	1 (-1)	7 (-81)	2 (+4)	13 (-82)
IAM 정책	18 (+8)	25 (+24)	443 (+437)	75 (+49)	561 (+510)
IAM 역할	10 (+9)	17 (+16)	193 (+94)	41 (+39)	261 (+55)
합계	214 (+11)	300 (-38)	1,777 (+766)	696 (+82)	2,987 (+821)

[자산현황 보고서]

2.4. 보안 관제/운영

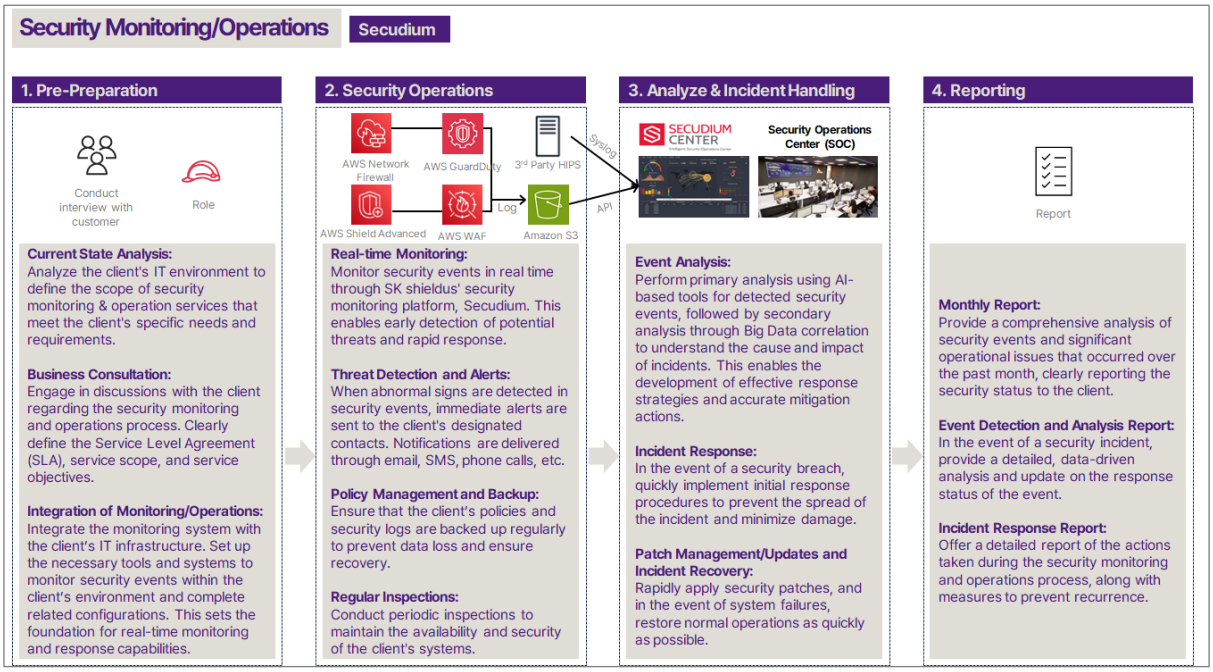
SK쉴더스는 고도화되는 사이버 위협으로 고객 서비스를 안전하게 보호하기 위해 축적된 노하우(Know-How)를 활용하여 AWS Cloud Native Service와 3rd Party 솔루션을 아우르는 24/365 무중단 보안 관제 서비스를 제공하며, 검증된 AWS 파트너로서 풍부한 경험과 전문성을 바탕으로 AWS Native 보안 운영 서비스와 고객사의 다양한 환경에 맞춘 클라우드 솔루션 파견 운영 서비스를 통해 안정적이고 효율적인 클라우드 운영을 지원합니다.

■ 보안 관제/운영 주요 제공 서비스는 아래와 같습니다.



No	구분		설명
1	**AWS Shield Advanced**		DDoS 공격에 대한 가시성과 복원력을 강화하여 애플리케이션의 가용성을 높이고, 재무적 손실과 보안 위협으로 인한 위험을 효과적으로 줄일 수 있습니다.
2	**AWS Network Firewall**		AWS F/W 구성을 기반으로 내/외부간 Traffic 에 대한 접근제어 정책 관리를 통해 고객 내부 자산을 비인가 된 접근으로부터 안전하게 보호하는 원격 운영을 지원합니다.
3	**IPS**	**AWS Network Firewall** (Network-based)	AWS F/W 구성을 기반으로 내부 시스템을 대상으로 한 내·외부 공격을 실시간으로 탐지 및 분석하여 내부 자산을 보호하고, 서비스 가용성을 안정적으로 보장합니다.
		Third-party (Host-based)	AWS 기반 Endpoint 에 에이전트를 구축하여 이상 행위나 알려진 위협 패턴에 효과적으로 탐지 및 방지함으로써, 전반적인 보안 태세를 한층 강화합니다.
4	**AWS WAF**		AWS WAF 를 활용해 웹 애플리케이션을 대상으로 한 다양한 공격을 실시간으로 탐지 및 차단하며, 고객사의 정보 자산을 보호하는 원격 보안 관제 서비스입니다.
5	**AWS Guard duty**		AWS IAM, S3, EC2 등에서 발생하는 이상 행위와 잘못된 권한 설정을 실시간으로 탐지하고 분석합니다.

■ 보안 관제/운영 서비스 절차는 아래와 같습니다.



■ 보안 관제/운영 서비스 범위는 아래와 같습니다.

서비스 구분	AWS Shield Advanced	AWS Network Firewall	IPS		AWS WAF	AWS GuardDuty
			AWS Network	3rd Party Host		
기술지원 (구축/구성)	제공	제공	제공	제공	제공	제공
로그관리	제공	-	제공	제공	제공	제공
정책관리	제공	제공	제공	제공	제공	-
가용성 관리	제공	-	-	제공	-	-
운영관리	제공	제공	-	-	-	제공
모니터링 (*24x365)	제공	-	제공	제공	제공	제공
리포트	제공	제공	제공	제공	제공	제공

■ 보안 관제/운영 서비스 특장점은 아래와 같습니다.

No	특장점	설명
1	**전문 보안관제 인력 및 역량 보유**	업계 최다 전문 보안관제 및 침해사고 대응 전담 인력(Top-CERT)을 보유하고 프로젝트 관리 조직을 운영하여 체계적인 사고 대응으로 정보 자산의 손실을 최소화하고 고객 신뢰도를 높이는 맞춤형 보안 서비스를 제공합니다.
2	**국내 1 위 보안관제 노하우**	24/365 무중단 보안관제 서비스를 통해 지속적으로 위협을 탐지 및 차단함으로써 보안 사각지대를 제거하고 서비스 연속성을 유지하는 안정적인 운영 환경을 제공합니다. (3,000여 고객 대상, 5,200여개 보안 장비 연동)
		자체 개발한 통합 보안관제 시스템(Secudium)을 활용하여 고객 환경에 최적화된 관제 서비스를 제공하며, 유연한 대응과 높은 운영 효율성을 보장합니다.
		원격관제 방법론(ISMM)을 기반으로 6,000 여 개의 침해 패턴을 탐지하여 다양한 공격 시나리오에 대비한 포괄적인 방어 체계를 제공합니다.
		AI 기반 분석과 빅데이터 처리 기술을 통해 탐지 정확도를 높이고 운영 비용을 절감하며, 보안관제 업무의 효율성을 극대화합니다.
3	**Cloud 특화 보안관제 서비스 제공**	관제 Coverage 확대를 통해 다수의 AWS Native 서비스 확장

[보안 관제 서비스]

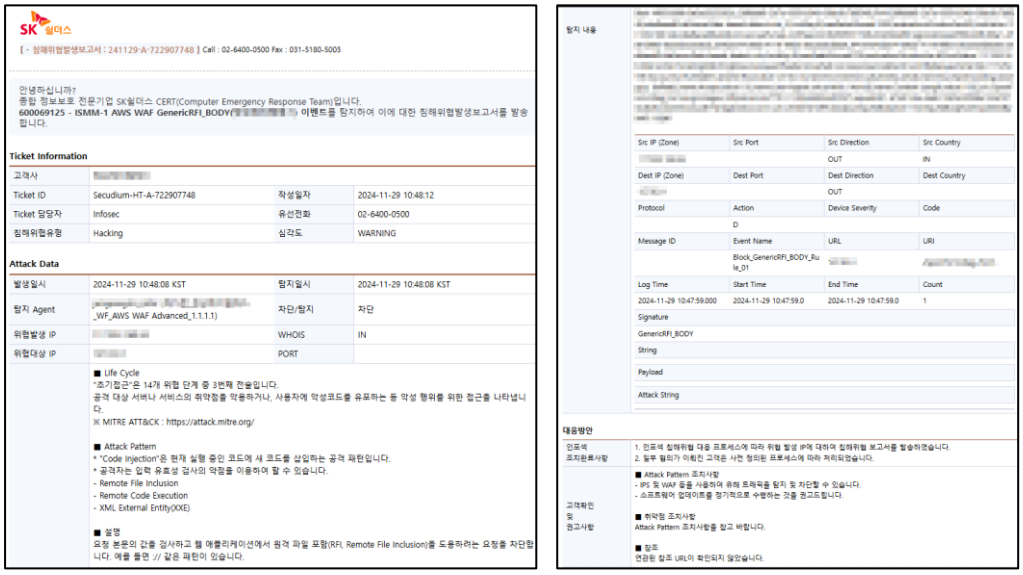
No	특장점	설명
1	**검증된 AWS 전문 보안 운영 기술력**	Advanced Tier 파트너로서 국내 보안 업계에서 "Perimeter Protection MSSP" 자격을 획득하여 신뢰성과 전문성을 인정받았습니다.
		AWS 보안 전문가를 직접 지원하여 고객의 클라우드 보안 요구사항에 최적화된 솔루션을 제공합니다.
		국내 최초로 AWS DDoS 운영 서비스를 런칭하여 강력한 분산 서비스 거부(DoS) 완화 체계를 구축했습니다.
2	**SK 쉴더스의 전문 보안 운영 노하우**	운영 관리, 보안 관리, 이슈 및 장애 처리, 변경 관리, 백업 및 복구 관리를 포함한 체계적인 보안운영 서비스를 제공합니다.
3	**Cloud 보안 운영 서비스 제공**	AWS Native 환경에서 원격으로 보안운영 서비스를 제공하여 효율적인 클라우드 보안 관리를 지원합니다
		클라우드 환경 내에서 솔루션 파견 운영 서비스를 통해 고객 맞춤형 보안 솔루션을 제공하고 운영 효율성을 극대화합니다.

[보안 운영 서비스]

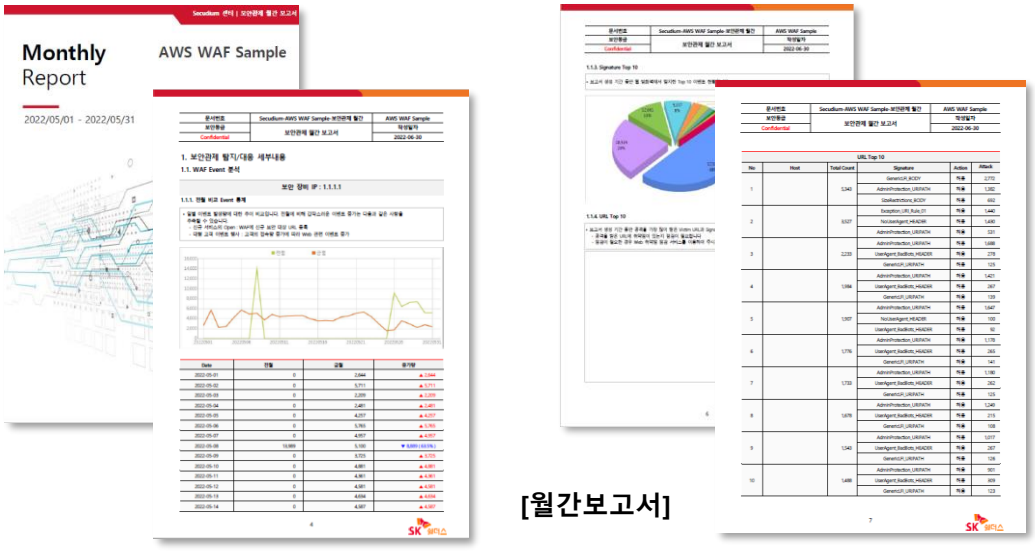
■ 보안관제/운영 서비스 리포트를 아래와 같이 제공합니다.

※ 아래의 이미지는 샘플입니다.

[“Secudium” 대시보드]



[침해위협 발송 보고서]

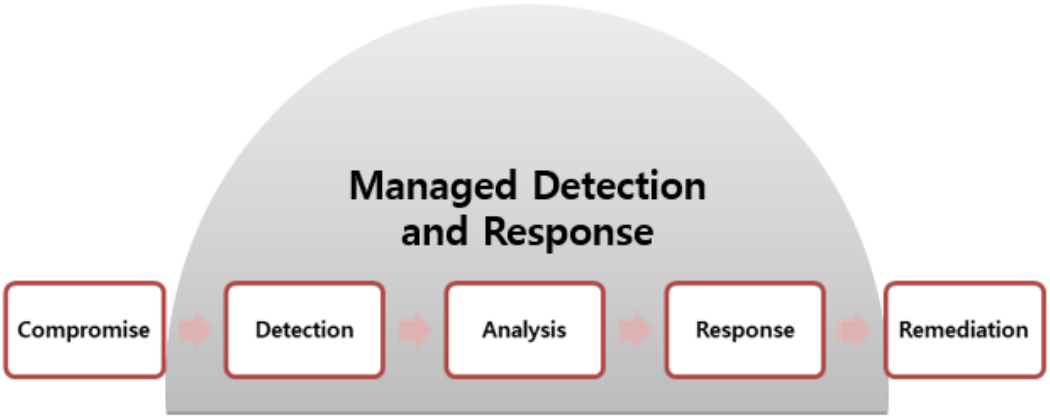


[월간보고서]

2.5. MDR 보안솔루션 구축

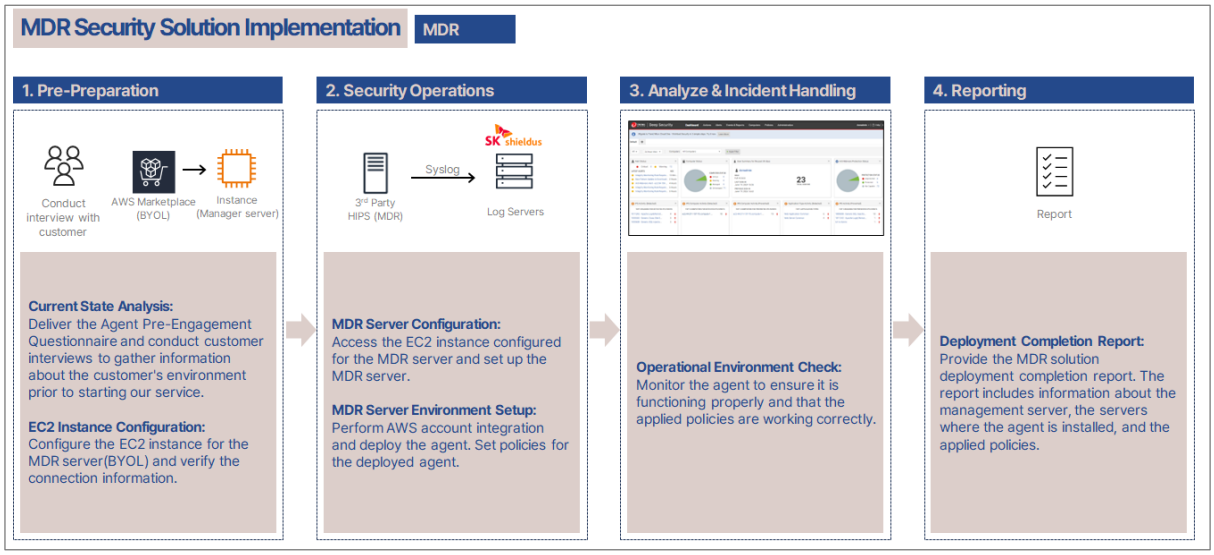
SK쉴더스는 조직의 보안 위협을 탐지하고 대응하는 Trend Micro의 MDR (Managed Detection and Response) 구축 서비스를 제공합니다. Trend Micro의 MDR은 경고 모니터링, 경고 우선순위 지정, 조사, 위협 탐색 등 다양한 보안 서비스를 제공합니다. 인공지능 모델을 사용하여 엔드-포인트, 네트워크 및 서버 데이터에 적용하여 고급 위협을 상호 연관시키고 우선순위를 지정합니다.

MDR 보안솔루션 도입을 통해 위협 탐지(Detection), 위협 대응(Response), 사고 분석(Investigation)을 수행할 수 있도록 솔루션 구축 서비스를 제공합니다.



No	Features	Description
1	**탐지(Detection)**	조직의 네트워크 및 엔드포인트 데이터를 지속적으로 모니터링하며, 특정 침해 지표를 탐색하기 위해 위협 점검을 수행합니다. 이를 바탕으로 위협의 우선순위를 결정합니다.
2	**분석(Analysis)**	탐지된 잠재적 위협이 상관관계 분석 및 우선순위 지정된 후, 공격의 출처와 범위를 조사합니다. 이후 위협 및 그 영향에 대한 상세한 분석을 수행합니다.
3	**대응(Response)**	조직에 사건 발생을 알리고, 근본 원인 분석, 완화 권장 사항, 그리고 사건을 처리하는 데 도움을 줄 도구 키트를 제공합니다.

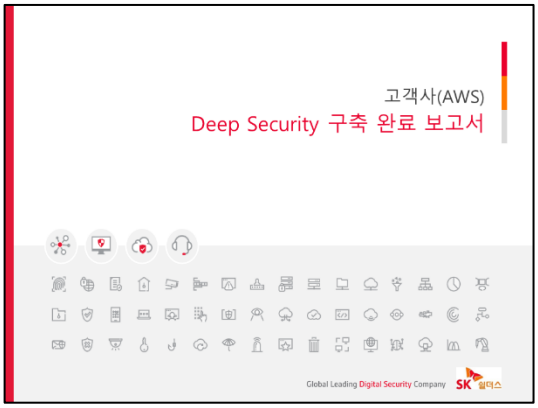
■ 솔루션 구축 절차

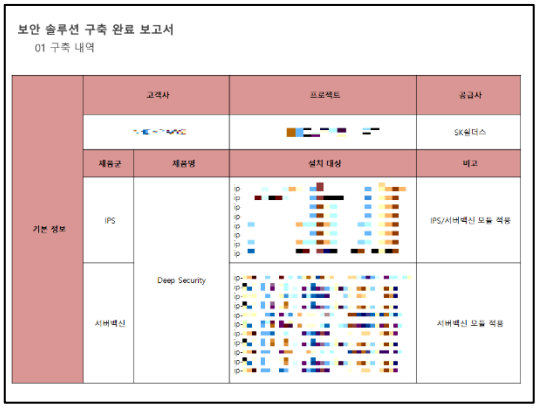


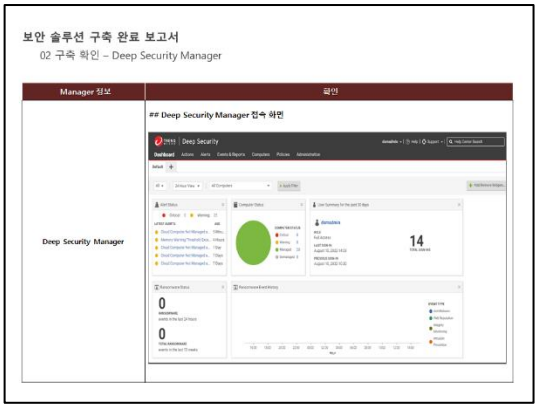
■ 솔루션 구축 시 기대 효과

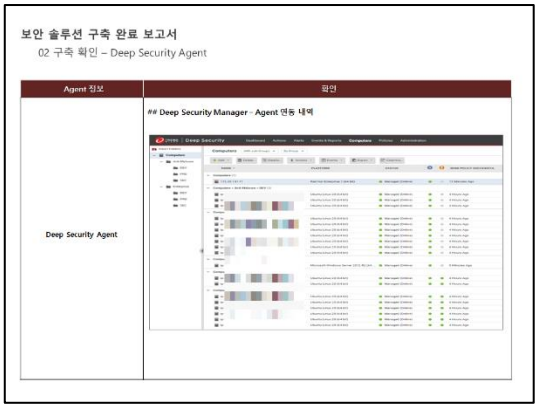
- AWS Account 내 인스턴스 자산 식별
  - ✓ 에이전트 설치 인스턴스 : 메타데이터(Public/Private DNS, Instance ID 등) 확인 가능
  - ✓ 에이전트 미설치 인스턴스 : 솔루션과 연동된 AWS Account의 모든 리전에 존재하는 인스턴스 확인 가능
- 보안 인시던트 탐지: 예측 머신 러닝, 위협 인텔리전스, 행동 모니터링을 통해 탐지 가능
- 엔드포인트에서의 인시던트 억제: 위의 탐지 기술을 통해 탐지된 멀웨어는 멀웨어 유형에 의해 삭제 혹은 차단되며, 차단된 파일들은 Anti-alware Events > Identified Fires에서 확인 가능
- 보안 인시던트 조사: 발생한 세부 멀웨어 이벤트(파일 경로, 발생한 프로세스 이름, 멀웨어 공격 표적, 멀웨어 타입 등)를 확인 가능
- 문제 해결 지침 제공: Windows에선 몇몇 유형(Virus)을 처리하고 치료할 수 없는 것은 격리. Linux는 격리만 가능

■ 구축 완료 보고서(Sample)









3. SK쉴더스 소개

에스케이쉴더스(주)의 급변하는 클라우드 환경의 지능형 사이버 위협에 대비해 유연하고 민첩하게 대응할 수 있는 최적의 솔루션을 제공합니다. 사이버 공격 위협에 대한 보안컨설팅부터 솔루션 구축, 관제/운영까지 Full Service Cycle 을 갖추고 있으며, Cloud 환경에서의 보안 서비스까지 한국 사이버 보안 업계 1 위 사업자로의 전문성과 노하우를 기반으로 최상의 서비스를 제공합니다.

■ SK쉴더스 Cloud 환경 주요 서비스 아래와 같습니다.

No	Features	Description
1	**원격 보안관제**	Cloud Native Security Service 및 3rd party Solution 를 대상으로 네트워크 보안 분야에 대한 통합 서비스를 제공합니다. 원격 보안관제 서비스는 24 시간 365 일 보안관제, 침해사고 예방 및 발생 시 사고 조사 및 분석 서비스를 제공합니다.
2	**SI/Solution**	기업의 다양한 클라우드 환경에 적합한 보안 솔루션을 구축합니다. • N/W, DB, 데이터, 애플리케이션, 엔드유저에 대한 3rd Party 보안솔루션 구축 • CSP(Cloud Service Provider)에서 제공하는 보안서비스 구축 • 보안 서비스 및 솔루션에 대한 통합 서비스 구축 • Cloud Oriented 보안 솔루션 제공(SWG, CWPP, CSPM)
3	**보안 컨설팅**	클라우드 도입 시 기본이 되는 서비스 • Cloud 보안인증 • Cloud Security Migration • Cloud Security Architecting • 메타버스 플랫폼 보안성 검토 • Cloud Data Security • Cloud Security 관리체계 수립 • Cloud Security 진단
4	**운영 서비스**	24시간 365일 보안 장비를 안전하게 보호하며, 긴급 상황 시 원격보안관제 센터의 콜센터를 통해 우선 지원합니다.

4. Support/Contact Point

아래 연락처로 문의 사항을 보내주시면 최대한 빨리 연락 드리겠습니다. 감사합니다.

1. Service-related Inquiries

- E-Mail: infocloudtech@skshieldus.com / infocloudops@skshieldus.com

2. Technology-related Inquiries

- E-Mail: infocloudtech@skshieldus.com / infocloudops@skshieldus.com