클라우드 취약점 점검 결과보고서

Ver 1.0

2022.06.07

**문서 이력**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **버전** | **주요내용** | **일자** | **작성자** | **검토자** |
| Ver0.1.0 | 템플릿 작성 및 진단 개요 작성 | 2022.06.07 | 석우영 | 김백현 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

목차

[**1.** **진단 개요** 3](#_Toc105509715)

[**가.** **목적** 3](#_Toc105509716)

[**나.** **진단 일정** 3](#_Toc105509717)

[**다.** **진단 인력** 3](#_Toc105509718)

[**라.** **진단 도구 및 방법** 3](#_Toc105509719)

[**2.** **진단 수행 절차** 4](#_Toc105509720)

[**3.** **구성 현황 파악 및 진단 항목 선정** 5](#_Toc105509721)

[**가.** **구성 현황 파악** 5](#_Toc105509722)

[**나.** **체크리스트 항목** 5](#_Toc105509723)

[4. 세부 항목(수동진단 + 분석) 6](#_Toc105509724)

[가. 계정관리 6](#_Toc105509725)

[나. 권한관리 6](#_Toc105509726)

[다. 데이터관리 6](#_Toc105509727)

[라. 가상 리소스 관리 6](#_Toc105509728)

[마. 감사/추적 관리 6](#_Toc105509729)

[5. 진단 결과 6](#_Toc105509730)

[6. 별첨 6](#_Toc105509731)

# **진단 개요**

## **목적**

SK헬스에서 전환한 클라우드 서비스에 존재할 수 있는 위협 요소를 정확하게 분석하여 잠재된 보안 위협을 도출하고, 적절한 보안대책을 수립·적용하여 취약점을 제거하도록 조치한다. 이를 통해 클라우드 서비스의 보안 수준 향상 및 신뢰성을 확보하는데 그 목적이 있다.

## **진단 일정**

2022년 06월 01일부터 2022년 06월 09일까지 9일 간 수행하였다.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **분류** | **내용** | **2022년 6일** | | | | | | | | |
| **1D** | **2D** | **3D** | **4D** | **5D** | **6D** | **7D** | **8D** | **9D** |
| **사전준비** | 대상범위 협의, |  |  |  |  |  |  |  |  |  |
| AWS 구성 |  |  |  |  |  |  |  |  |  |
| **취약점 진단** | 수동진단 및 결과 리뷰 |  |  |  |  |  |  |  |  |  |
| **분석 평가** | 결과 보고서 작성 및 리뷰 |  |  |  |  |  |  |  |  |  |

[표 1] 진단 일정

## **진단 인력**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **이름** | **직급** | **소속** | **담당업무** | **이메일** | **비고** |
| 김다빈 | CTO | 취약점 진단팀 | 취약점 진단 및 분석(총괄) |  |  |
| 석우영 |  | 취약점 진단팀 | 취약점 진단 |  |  |

[표 2] 진단 인력

## **진단 도구 및 방법**

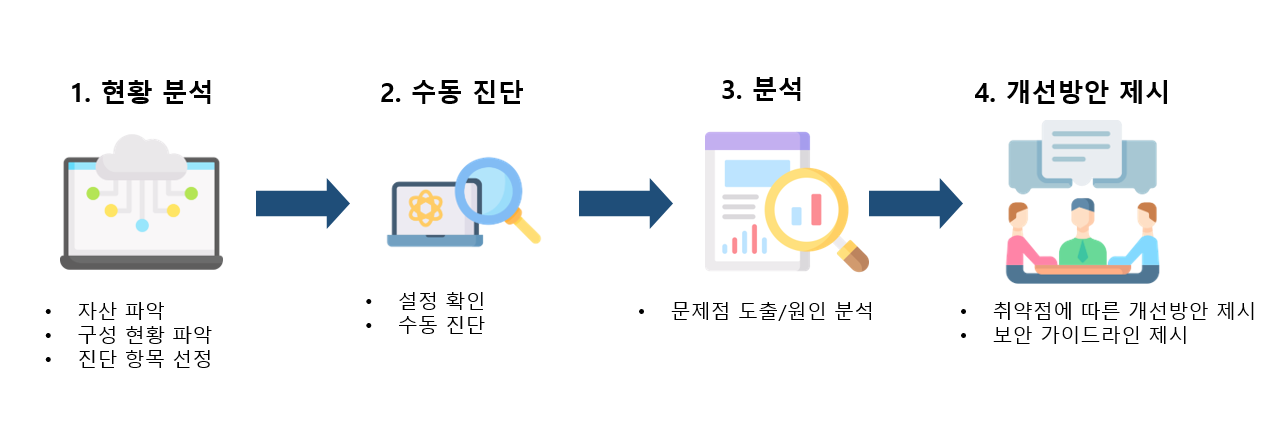
취약점 진단은 수동진단을 통하여 실시하였다.

|  |  |  |
| --- | --- | --- |
| **구분** | **설명** | **비고** |
| 수동진단 | 진단 대상 시스템의 운영현황, 특성 등으로 인하여 스크립트로 진단이 어려울 경우 취약점진단 인력이 시스템에 직접 접근하여 점검을 수행  ※ 시스템운영자 등 고객사의 관리·감독 하에 수행 | 공통 |

[표 3] 진단 도구

# **진단 수행 절차**

취약점 분석 수행 절차는 아래 그림과 같이 “현황분석”, “수동 진단”, “분석”, “개선방안 제시”를 수행하여 최종 취약점 분석 보고서를 작성한다.



[그림 1] 취약점 분석 평가 수행절차

· **현황 분석**

인프라 구조를 파악하고 AWS 구성 현황을 분석한다. 이 후 취약점 분석 대상 항목을 선정하여 전반적인 보안 현황을 파악한다.

· **수동 진단**

SK쉴더스에서 제공한 2021 클라우드 보안 가이드-AWS 기준으로 인프라 환경에 대한 보안 취약점을 진단한다.

· **분석**

진단 단계에서 식별된 취약점을 분석하여 문제점을 도출하고, 현재 취약점의 보안수준을 평가하여 미칠 수 있는 위험을 분석 평가한다.

· **개선방안 제시**

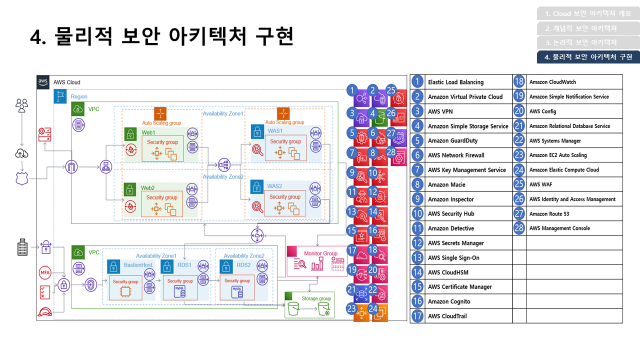
취약점 분석 평가를 통해 도출된 취약점에 대한 보안설정 가이드라인을 제공하고, 필요 시 적절한 보호대책을 제시한다.

# **구성 현황 파악 및 진단 항목 선정**

## **구성 현황 파악**

SK헬스의 인프라 구성을 파악하고 보안 요건 정의서와 STRM을 근거로 클라우드 보안 현황을 분석한다.

SK헬스의 AWS 구성도는 다음과 같다



[그림 2] SK헬스 AWS 구성도

## **체크리스트 항목**

SK쉴더스 발간 ‘2021 클라우드 보안 가이드 – AWS’ 기준의 취약점 점검항목으로 선정하였다.

|  |  |  |
| --- | --- | --- |
| **영역** | **평가항목(개)** | **비고** |
| 계정관리 | 7 | - |
| 권한관리 | 6 | - |
| 데이터관리 | 3 | - |
| 가상 리소스 관리 | 10 | - |
| 감사/추적 관리 | 4 | - |
| **합계** | **30** | **-** |

# **세부 항목**

다음은 진단에 사용될 SK쉴더스 발간 ‘2021 클라우드 보안 가이드 – AWS’ 기준의 취약점 상세 체크리스트이다.

|  |  |  |  |
| --- | --- | --- | --- |
| **영역** | **항목코드** | **항목명** | **중요도** |
| 계정관리 | 1.1 | 관리자 계정 최소화 관리 | **상** |
| 1.2 | IAM 사용자 계정 단일화 관리 | **상** |
| 1.3 | IAM 사용자 계정 식별 관리 | **중** |
| 1.4 | Key Pair 접근 관리 | **상** |
| 1.5 | Key Pair 보관 관리 | **상** |
| 1.6 | MFA (Multi-Factor Authentication) 설정 | **중** |
| 1.7 | 패스워드 정책 관리 | **중** |
| 권한 관리 | 2.1 | 인스턴스 보안 정책 관리 | **상** |
| 2.2 | RDS 보안 정책 관리 | **상** |
| 2.3 | S3 보안 정책 관리 | **상** |
| 2.4 | Access Key 정책 관리 | **중** |
| 2.5 | Admin Console 관리자 정책 관리 | **중** |
| 2.6 | IAM 사용자 및 그룹 정책 관리 | **중** |
| 데이터 관리 | 3.1 | 인스턴스 암호화 설정 | **중** |
| 3.2 | RDS 암호화 설정 | **중** |
| 3.3 | S3 암호화 설정 | **중** |
| 가상 리소스  관리 | 4.1 | 보안그룹 인/아웃바운드 ANY 설정 관리 | **중** |
| 4.2 | 보안그룹 인/아웃바운드 불필요 정책 관리 | **중** |
| 4.3 | ACL 네트워크 인/아웃바운드 트래픽 정책 관리 | **상** |
| 4.4 | 라우팅 테이블 정책 관리 | **중** |
| 4.5 | NAT 게이트웨이 연결 관리 | **중** |
| 4.6 | 인터넷 게이트웨이 연결 관리 | **하** |
| 4.7 | S3 버킷 접근 관리 | **중** |
| 4.8 | RDS 리소스 액세스 권한 관리 | **중** |
| 4.9 | RDS API 작업 권한 관리 | **중** |
| 4.10 | RDS 서브넷 가용 영역 관리 | **중** |
| 감사/추적관리 | 5.1 | AWS 사용자 계정 로깅 설정 | **하** |
| 5.2 | 가상 인스턴스 로깅 설정 | **하** |
| 5.3 | RDS 로깅 설정 | **하** |
| 5.4 | S3 버킷 로깅 설정 | **하** |

[표 4] AWS 보안 진단 체크리스트

각 취약점으로 인해 발생 가능한 피해에 대하여 위험도 산정을 통해 상, 중, 하 3단계로 분류함.

|  |  |  |
| --- | --- | --- |
| **위험도** | **내 용** | **비고** |
| **상** | 관리자 계정 및 주요정보 유출로 인한 치명적인 피해 발생 |  |
| **중** | 노출된 정보를 통해 서비스/시스템 관련 추가 정보 유출 발생 우려 |  |
| **하** | 타 취약점과 연계 가능한 잠재적인 위협 내재 |  |

[표 5] 위험도 분류

## **계정관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | 계정관리 | **중요도** | **상** |
| **점검 날짜** |  | **결과** |  |
| **항목명** | 관리자 계정 최소화 관리 | | |
| **항목 설명**  **(SK 쉴더스 클라우드 보안 가이드)** | 모든 AWS 리소스는 AWS 계정의 소유이고, 리소스 생성 또는 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉, 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있으며 적절한 권한을 통한 서비스 관리가 이루어져야 합니다.  1. AWS 관리형 정책  서비스 내 FULL ACCESS 등과 같이 중요도가 높은 AWS 관리형 정책은 EC2 서비스 관리/운영자 및 관련 담당자 외에 다른 IAM 계정에 아래와 같은 권한 할당이 되지 않도록 해야합니다. 그중에서도 AWS Root 관리자 인 “Administratoraccess” 권한은 다수의 IAM 계정에 설정되지 않도록 관리조치가 필요합니다.  **(\*) “Administratoraccess” 및 "Full Access" 권한이 부여된 다수의 계정이 존재할 경우 담당자 확인이 필요함** | | |
| **진단 기준** | **양호기준**  관리자 권한이 사용 목적에 맞게 지정된 사용자가 부여되어 있을 경우  **취약기준**  관리자 권한이 사용 목적에 맞지 않은 사용자에게 불필요하게 부여되어 있을 경우 | | |
| **점검 내용** |  | | |

## 권한관리

## 데이터관리

## 가상 리소스 관리

## 감사/추적 관리

# 진단 결과

# 별첨