JM COMPANY-VA-클라우드진단수행계획서

Confidentia
l

클라우드진단 수행계획서

2023. 07. 26.

SK shieldus

Confidentiality Agreements

본 보고서는 시스템 정보와 관련한 비공개 사항이 포함되어 있으므로, 열람권한은 우선적으로 정보보안 책임자로 제한되며, 이외의 열람자격은 정보보안 책임자가 허락한 최소한의 인원으로 제한하여 주시기 바랍니다.

본 보고서는 양사간의 사전 협의 없이 어떠한 목적으로도 외부로 유출되거나 무단 복제, 무단 사용될 수 없으며, 기밀성을 유지한다는 전제하에 사용이 엄격 하게 제한됩니다.

본 보고서는 인포섹㈜에서 작성을 하였으며, 정보보호 서약에 대한 사항을 준수 합니다.

- 목 차 -

1.개요

1.1.목적

본 클라우드 진단은 **"JM COMPANY"**에서 운영 중인 클라우드서비스에 대해 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조 제2항에 따라 정보보호 기준의 준수 여부를 확인을 인증기관에 요청하는 경우 인증기관은 이를 평가·인증하며, 내부 직원이나 내부망에 거점을 확보한 자가 악용할 수 있는 취약성이 존재하는지를 점검하고, 발견된 취약성에 대한 대응책을 수립하여 안전하고 신뢰할 수 있는 정보시스템 구축 및 운영을 위한 기반을 마련 및 보안 수준 향상을 위한 방법을 제시하고자 합니다.

1.2.진단방법

정보시스템 관리/운영 부문과 기술적 부문에 대한 취약성을 진단하고 관리자 인터뷰를 통해 대상 시스템을 점검합니다.

- ○ SK쉴더스 '클라우드 보안 가이드 – AWS(ver.2023)' 체크리스트 기반 진단 및 분석 수행
- ○ 클라우드 서비스 담당자 인터뷰 수행을 통한 현황 파악 및 분석 수행

1.3.진단일정

클라우드 취약점 진단 수행 일정은 사전 준비 및 공조체계 마련, 서버 취약점 점검, 점검 결과 분석, 보고서 작성의 4단계로 수행하며, 세부 일정은 다음과 같습니다.

구분	내용	일정
사전준비	대상협의 및 환경분석	2023.07.28 이전
취약점 점검	취약점 점검 수행(수동)	2023.07.28 ~ 2023.08.04
결과분석 / 보고서	결과분석 및 보고서 작성	2023.08.17
결과보고서 제출	최종 결과보고서 제출	2023.08.31 (종료)

[표 1 – 진단일정]

1.4.진단대상

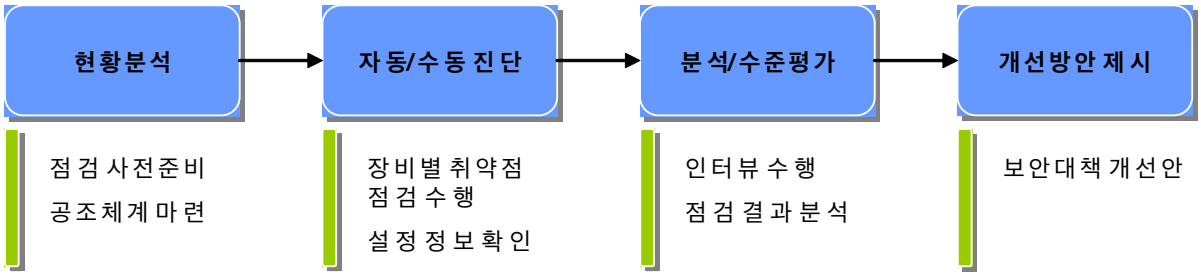
클라우드 진단 대상의 상세 내역은 다음과 같습니다.

No	구분	계정	비고
1	AWS	sk401-team	리전 –오하이오

[표 2 – 클라우드 진단대상]

1.5.진단절차

클라우드 진단 수행 절차는 아래 그림과 같이 "현황 분석", "수동 진단", "분석/수준평가", "개선방안 제시"를 수행하여 최종 취약점 분석 보고서를 작성합니다.



[그림 1 – 취약성 진단 수행 절차]

1. 현황 분석
원활한 진단을 수행하기 위하여 실제 진단 전에 입수된 자료와 담당자 인터뷰 등을 통해 대상 웹서버에 대한 정보(IP, Hostname, Service, WA S정보, 웹 구조, 네트워크 Config 등)를 수집하며 전반적인 보안 현황을 파악합니다.

2. 수동 진단
실제 장비의 취약점을 진단하는 단계로 시큐어코딩, 모의 침투 테스트 등을 이용한 서버 점검 및 네트워크 Config 점검을 수행합니다.

3. 분석/수준 평가
진단 단계에서 식별된 취약점을 분석하여 문제점을 도출하고, 현재 취약점의 보안 수준을 평가하여 각 장비의 취약점이 미칠 수 있는 위험을 분석 평가합니다.

4. 개선방안 제시
분석 평가된 취약점에 따른 개선방안을 도출하여 이에 따른 보안 가이드를 제시합니다.

1.6.진단항목

클라우드 진단항목은 “2023 클라우드 보안 가이드 – AWS”을 기반으로 계정 관리(10개 항목), 권한 관리(3개 항목), 가상 리소스 관리(8개 항목), 운영 관리(13개항목)으로 총 4개 영역에서 34개 항목으로 되어 있으며 상세 진단항목은 다음과 같습니다.

구분	NO.	대상항목
1. 계정 관리	1.1	사용자 계정 관리
	1.2	IAM 사용자 계정 단일화 관리
	1.3	IAM 사용자 계정 식별 관리
	1.4	IAM 그룹 사용자 계정 관리
	1.5	Key Pair 접근 관리
	1.6	Key Pair 보관 관리
	1.7	Admin Console 관리자 정책 관리
	1.8	Admin Console 계정 Access Key 활성화 및 사용주기 관리
	1.9	MFA (Multi-Factor Authentication) 설정
	1.10	AWS 계정 패스워드 정책 관리
2. 권한 관리	2.1	인스턴스 서비스 정책 관리
	2.2	네트워크 서비스 정책 관리
	2.3	기타 서비스 정책 관리
3. 가상 리소스 관리	3.1	보안 그룹 인/아웃바운드 ANY 설정 관리
	3.2	보안 그룹 인/아웃바운드 불필요 정책 관리
	3.3	네트워크 ACL 인/아웃바운드 트래픽 정책 관리
	3.4	라우팅 테이블 정책 관리
	3.5	인터넷 게이트웨이 연결 관리
	3.6	NAT 게이트웨이 연결 관리
	3.7	S3 버킷/객체 접근 관리
	3.8	RDS 서브넷 가용 영역 관리
	4.1	EBS 및 볼륨 암호화 설정
	4.2	RDS 암호화 설정
	4.3	S3 암호화 설정
	4.4	통신구간 암호화 설정
	4.5	CloudTrail 암호화 설정
	4.6	CloudWatch 암호화 설정

구분	NO.	대상항목
4. 운영 관리	4.7	AWS 사용자 계정 로깅 설정
	4.8	인스턴스 로깅 설정
	4.9	RDS 로깅 설정
	4.10	S3 버킷 로깅 설정
	4.11	VPC 플로우 로깅 설정
	4.12	로그 보관 기간 설정
	4.13	백업 사용 여부

[표 3– 클라우드 진단항목]

1.7.진단 평가 기준

보안 등급	A (안전)	B (양호)	C (보통)	D (취약)	E (위험)
보안수준 점수(%)	85 이상~ 100 미만	70 이상~ 85 미만	55 이상~ 70 미만	40 이상~ 55 미만	0 이상~ 40 미만
해커공격 대응수준	고급해커 120시간 공격에 대응	고급해커 48시간 공격에 대응	중급해커 120시간 공격에 대응	초급해커 120시간 공격에 대응	초급해커 48시간 공격에 대응

[표 4 – 보안 평가등급(TCSEC)]

※ 평가등급 (TCSEC): 미 국방성 (DoD)의 컴퓨터시스템 보안등급 기준인 TCSEC (Trusted Computer System Evaluation Criteria) 의 개념에 기반하며, 기술적 영역에 대한 기업의 보안환경을 분석하여 그 수준을 진단하고 등급을 평가하는 기준. 기술적 보안에 대해 A ~ E 5 단계 등급과 100점 만점의 보안수준 점수로서 평가

2.진단결과

2.1.수행 산출물

클라우드 보안진단을 통하여 제공되는 산출물은 다음과 같습니다.

No	작업 산출물	제출시기	비 고
1	클라우드진단 수행계획서	진단 수행 전	본 문서
2	클라우드진단 결과보고서	진단 수행 후	서버 취약점 분석평가 결과

[표 5– 수행 산출물]

2.2.수행 후의 조치사항

1) 작업 수행 완료 후 특권 획득 표시 및 기타 흔적들의 삭제(예: /upload/infosec.jsp)
2) 대상 시스템의 정상작동 확인

2.3.협조 및 유의사항

서버 취약점 진단의 효율 및 정확성을 보장하기 위하여 다음 사항에 대한 지원을 요청합니다.

1) 대상 서버 중 내부망에 위치한 서버 취약점 진단을 위한 점검용 node 및 IP Address 부여
2) 서버 취약점 진단을 위한 대상 서버의 Administrator 또는 root 계정 확보 요청
3) 서버 별 실무담당자 연락처 요청 (ex. 시스템 담당, 응용 담당, 유지 보수 담당자 등)
4) 진단 컨설턴트가 사용할 수 있는 Remote 또는 Local Network Segment 환경의 제공
5) 진단 스크립트 업로드를 위한 FTP, 터미널 서비스 오픈 요청