Confidential

클라우드 취약점진단 수행계획서

2025. 08. 13.

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 SK쉴더스에서 작성을 하였으며, 정보보호 서약에 대한 사항을 준수합니다.

- 목 차 -

1. 개요 4

1.1. 진단목적 4

1.2. 진단대상 4

1.3. 진단일정 5

2. 클라우드 취약점 진단 6

2.1. 주요 취약점 및 진단항목 6

2.2. 수행 산출물 7

3. 협조사항 8

3.1. 진단 수행 간의 협조 사항 8

3.2. 담당자에게 협조를 구하는 사항 8

1. 개요

1.1. 진단목적

본 클라우드 진단은 "**J.W.P. MagicShop**"의 서비스가 동작하는 클라우드 환경에 대해서 취약점 진단을 수행하고, 발견된 취약점이 시스템에 미치는 영향을 파악하여 보안대책을 제시함으로써, 침해사고 예방 및 서비스의 안정성을 확보하는 데 그 목적이 있습니다.

1.2. 진단대상

클라우드 취약점 진단 대상 계정의 상세 내역은 다음과 같습니다.

No	계정	비고
1	team3	관리자

[표 1 – 진단대상]

1.3. 진단일정

진단 일정은 다음과 같습니다.

업무 수행 내역	일정
사전준비 및 대상 관련 자료 수령	2025.08.01 ~ 2025.08.09
클라우드 취약점 진단 수행	2025.08.11 ~ 2025.09.05
결과 분석 및 결과 보고서 작성	2025.09.05 ~ 2025.09.17
보고서 최종 수정 및 완료	2025.09.17 (종료)

[표 2 – 진단일정]

2. 클라우드 취약점 진단

2.1. 주요 취약점 및 진단항목

클라우드 진단 항목은 SK Shieldus 에서 고시한 "2024 클라우드 보안 가이드(AWS)"를 반영하여, 아래와 같이 진단항목을 선정합니다.

구분	NO.	대상항목
1.계정 관리	1	사용자 계정 관리
	2	IAM 사용자 계정 단일화 관리
	3	IAM 사용자 계정 식별 관리
	4	IAM 그룹 사용자 계정 관리
	5	Key Pair 접근 관리
	6	Key Pair 보관 관리
	7	Admin Console 관리자 정책 관리
	8	Admin Console 계정 Access Key 활성화 및 사용주기 관리
	9	MFA(Multi-Factor Authentication) 설정
	10	AWS 계정 패스워드 정책 관리
	11	EKS 사용자 관리
	12	EKS 서비스 어카운트 관리
	13	EKS 불필요한 익명 접근 관리
2.권한 관리	1	인스턴스 서비스 정책 관리
	2	네트워크 서비스 정책 관리
	3	기타 서비스 정책 관리
3.가상 리소스 관리	1	보안 그룹 인/아웃바운드 ANY 설정 관리
	2	보안 그룹 인/아웃바운드 불필요 정책 관리
	3	네트워크 ACL 인/아웃바운드 트래픽 정책 관리
	4	라우팅 테이블 정책 관리
	5	인터넷 게이트웨이 연결 관리
	6	NAT 게이트웨이 연결 관리
	7	S3 버킷/객체 접근 관리
	8	RDS 서브넷 가용 영역 관리
	9	EKS Pod 보안 정책 관리
	10	ELB(Elastic Load Balancing) 연결 관리

구분	NO.	대상항목
4.운영 관리	1	EBS 및 볼륨 암호화 설정
	2	RDS 암호화 설정
	3	S3 암호화 설정
	4	통신구간 암호화 설정
	5	CloudTrail 암호화 설정
	6	CloudWatch 암호화 설정
	7	AWS 사용자 계정 로깅 설정
	8	인스턴스 로깅 설정
	9	RDS 로깅 설정
	10	S3 버킷 로깅 설정
	11	VPC 플로우 로깅 설정
	12	로그 보관 기간 설정
	13	백업 사용 여부
	14	EKS Cluster 제어 플레인 로깅 설정
	15	EKS Cluster 암호화 설정

[표 3 – 주요 진단 항목]

2.2. 수행 산출물

산출물	제출 시기	비고
클라우드 취약점진단 수행계획서	진단 수행 전	본 문서
클라우드 취약점진단 결과보고서	진단 수행 후	대상 정보시스템의 취약점진단 진단과정, 결과에 대한 개선안의 설명서
클라우드 이행점검 결과보고서	조치 이행 후	대상 정보시스템의 점검 결과에 대한 설명서

[표 4 – 수행 산출물]

3. 협조사항

비인가자로 인한 해킹의 위협을 테스트 하기 위하여 고객사의 내부 서비스용 시스템을 대상으로 아래와 같은 환경에서 테스트를 실시합니다.

3.1. 진단 수행 간의 협조 사항

(1) 대상 도메인의 URL 정보

(2) 진단 수행간의 발생한 흔적 삭제

(3) 대상 시스템의 정상 작동 확인

3.2. 담당자에게 협조를 구하는 사항

(1) 담당하고 있는 대상에 대한 취약점 진단 일정 숙지

(2) 비상 사태에 대비하여 주요 데이터에 대한 백업 수행

(3) 취약점 진단 수행기간 동안 특이사항 발생에 대비한 담당자 대기