|  |
| --- |
|  |
| **[의료서비스 마이그레이션 프로젝트]** |
| **시스템 취약점 진단 수행계획서** |
| *Version 1.1* |

**2021. 11. 29**



**개 정 이 력**

| 버전 | 변경일 | 변경 사유 | 변경 내용 | 작성자 | 비고 |
| --- | --- | --- | --- | --- | --- |
| 1.0 | 2021-11-25 | 최초작성 | 보고서 최초작성 | 김민지 |  |
| 1.1 | 2021-11-29 | 항목변경 | 진단 항목 업데이트 | 김민지 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**목차**

[1. 목적 5](#_Toc89098214)

[1.1. 수행 목적 5](#_Toc89098215)

[1.2. 수행 일정 5](#_Toc89098216)

[1.3. 수행 인력 6](#_Toc89098217)

[1.4. 수행 환경 6](#_Toc89098218)

[1.5. 수행 대상 6](#_Toc89098219)

[2. 수행방안 7](#_Toc89098220)

[2.1. 수행 절차 7](#_Toc89098221)

[2.2. 수행 방법 8](#_Toc89098222)

[2.3. 수행 도구 8](#_Toc89098223)

[2.4. 진단 기준 9](#_Toc89098224)

[2.5. 진단 항목 10](#_Toc89098225)

[3. 산출물 및 협조사항 21](#_Toc89098226)

[3.1. 수행 산출물 21](#_Toc89098227)

[3.2. 협조 요청 사항 21](#_Toc89098228)

[3.3. 수행 전 업무 협의 사항 22](#_Toc89098229)

[별첨 1. 클라우드 취약점 점검 가이드 – 보안설정(CCE) (Linux) 23](#_Toc89098230)

[별첨 2. 클라우드 보안 가이드(컨테이너 보안) – Docker, Kubernetes 25](#_Toc89098231)

[별첨 3. 클라우드 보안 가이드 – AWS 27](#_Toc89098232)

**표 목차**

[[표 1] 취약점진단 수행 일정 5](#_Toc89098233)

[[표 2] 수행 인력 6](#_Toc89098234)

[[표 3] 수행 환경 6](#_Toc89098235)

[[표 4] 취약점진단 대상 요약 6](#_Toc89098236)

[[표 5] 취약점진단 수행절차 7](#_Toc89098237)

[[표 6] 취약점진단 수행방법 8](#_Toc89098238)

[[표 7] 취약점진단 수행도구 8](#_Toc89098239)

[[표 8] 위험도 9](#_Toc89098240)

[[표 9] 진단등급 9](#_Toc89098241)

[[표 10] 대책적용 시기 9](#_Toc89098242)

[[표 11] Linux 서버 취약점 진단 항목 10](#_Toc89098243)

[[표 12] Docker 취약점 진단 항목 12](#_Toc89098244)

[[표 13] AWS 취약점 진단 항목 13](#_Toc89098245)

[[표 14] 수행 산출물 21](#_Toc89098246)

[[표 15] 업무협조 요청사항 22](#_Toc89098247)

[[표 16] 한국인터넷진흥원의 클라우드 취약점 점검 가이드 – 보안설정(CCE) (Linux) 23](#_Toc89098248)

[[표 17] EQST 클라우드 보안가이드(컨테이너 보안) – Docker, Kubernetes (Docker) 25](#_Toc89098249)

[[표 18] EQST 2021 클라우드 보안가이드 - AWS 27](#_Toc89098250)

**그림 목차**

**그림 목차 항목을 찾을 수 없습니다.**

1. 목적
   1. 수행 목적

1조에서 구성한 정보시스템에 대하여 취약점진단을 수행하고 도출된 취약점에 대하여 취약점의 조치 현황을 점검하여 보안대책을 제시함으로써 신뢰성 확보를 통해 보안대책을 수립 및 시행하고 서비스의 안전성을 확보하는 것에 목적이 있다.

* 1. 수행 일정

1조 취약점 진단 담당자와 협의를 통해 11월23일부터 12월 10일까지 03주간 진행하며 진단 중 문제 발생 시 운영 시스템의 영향을 최소화 하기 위해서 1조 시스템 운영팀의 대응이 빠른 일과 시간 (9:00 ~ 18:00) 중에 수행합니다. 추가 진단이 필요할 경우 야간 진단(18:00 ~ 04:00)을 수행합니다.

[표 1] 취약점진단 수행 일정

| 구분 | 내역 | 기간 | 일정 | Owner |
| --- | --- | --- | --- | --- |
| 사전준비 | 정보시스템 보안관리 현황 분석 | OW | 11. 23 ~ 11. 26 | 1조 |
| 진단대상 확인 및 확정 |
| 진단 일정 계획 수립 |
| 취약점 점검 | 시스템 취약점진단(서버/DB/NW/APP.) | OW | 11. 29 ~ 12. 03 | 1조 |
| 보고서 작성 | 진단결과 분석 | OW | 12. 07 ~ 12. 10 | 1조 |
| 진단 보고서 작성 | OW | 12. 07 ~ 12. 10 | 1조 |
| 보안 취약점 조치 | 취약점에 대한 조치 지원 | - | - | 1조 |

* 1. 수행 인력

취약점진단 수행 인력은 다음과 같음

[표 2] 수행 인력

| 담당업무 | 수행원 | 직급 | 연락처 | 이메일 |
| --- | --- | --- | --- | --- |
| 취약점진단 | 조상우 |  | 010-9934-6348 |  |
| 취약점진단 | 김민지 |  | 010-8785-1501 | happy0652@naver.com |
| 취약점진단 | 배슬기 |  | 010-4760-6408 |  |

* 1. 수행 환경

취약점진단 수행 환경은 다음과 같음

[표 3] 수행 환경

| 구분 | 수행원 | IP | 진단 장소 |
| --- | --- | --- | --- |
| 시스템 취약점진단 | 조상우 | 223.38.22.161 XXX.XXX.XXX.XXX | 재택 동국대학교 |
| 시스템 취약점진단 | 김민지 | 182.217.209.120 XXX.XXX.XXX.XXX | 재택 동국대학교 |
| 시스템 취약점진단 | 배슬기 | 220.117.34.169 XXX.XXX.XXX.XXX | 재택 동국대학교 |

* 1. 수행 대상

취약점진단 수행 대상은 다음과 같음

[표 4] 취약점진단 대상 요약

|  |  |  |
| --- | --- | --- |
| 구분 | | 수량 |
| 서버 | Linux | 09 |
| 미들웨어 | Docker | 12 |
| AWS | | 01 |
| **합계** | | **23** |

주) 주요 진단 대상 및 범위는 상호 협의하여 확정

1. 수행방안
   1. 수행 절차

[표 5] 취약점진단 수행절차

| 단계 | 내용 | 기법/도구 |
| --- | --- | --- |
| 사전준비 | 요구사항 및 제약 사항 파악  담당자와 협의하여 진단대상 선정  각 OS, APP Engine별 체크리스트 작성 및 확정 | 운영 문서 검토 |
| 취약점진단 | OS, APP Engine, 네트워크 장비에 대하여 진단 체크리스트를 기반으로 한 수동 진단  보안시스템 정책 및 환경설정에 대한 취약점을 진단하며, 운영상의 문제점을 파악  네트워크/보안시스템 진단수행 시 장비의 직접적인 로그인은 필요없음  (필요 시 계정 요청함)  제공된 운영 configuration(텍스트)을 체크리스트에 의거하여 수행원이 분석하는 형태로 진행 | OS, APP Engine, 네트워크 장비 수동 점검  네트워크 및 보안 솔루션 구성도 검토 |
| 결과 분석 및 인터뷰 | 진단 결과에 대한 취약점 결과 분석 및 원인 분석 | 점검로그 분석 |
| 대응방안 수립 | 발견된 취약점에 대한 보안 강화 방안 수립 및 보고서 작성 |  |
| 이행지원 | 발견된 취약점 중 Quick Fix 항목에 대한 이행 시 진단 대상별 20~30%비율로 직접 조치 공동 수행을 통한 기술전수 및 이행지원 |  |

* 1. 수행 방법

[표 6] 취약점진단 수행방법

| 수행방법 | 내용 |
| --- | --- |
| 문서 검토 | 서버, APP Engine 관련 문서에 대한 검토 및 서버, APP Engine 보안관리 검토  전체 네트워크 구성도, 보안시스템 구성도, 네트워크 장비 configuration, 보안시스템 정책 및 환경설정에 대한 검토 |
| 수동진단 | 자동진단 도구에서 도출할 수 없는 부분에 대해 서버, APP Engine에 로그인 후 시스템 운영 환경에 대한 수동 정밀 분석  (시스템 관리자 권한으로 로그인 필요)  라우터, 스위치 등 네트워크 장비의 특권을 이용하여 보안설정에 대한 취약점진단(필요 시)  보안시스템의 Rule Set, 환경 설정 값에 대한 분석 |
| 네트워크 및 보안솔루션 구성도 검토 | 네트워크, 보안시스템의 구조 및 접근통제 등에 대한 검토 |

* 1. 수행 도구

시스템 보안진단은 수작업을 통하여 종합적인 보안 현황을 파악합니다.

[표 ] 취약점진단 수행도구

| 수행도구 | 설명 |
| --- | --- |
| 수동진단 | 진단 도구로 찾기 어려운 시스템 취약성들은 전문 컨설턴트의 수동진단을 통해 분석함  John the Ripper = 패스워드 보안성을 테스트하기 위한 패스워드 크래킹 도구로 수동 진단시 사용됨 |

* 1. 진단 기준
     1. 위험도

[표 ] 위험도

| 위험도 | 설 명 | 가중치 |
| --- | --- | --- |
| 상 | 취약점을 이용하여 관리자 권한을 획득하거나 시스템 정지 가능 | 3 |
| 중 | 취약점을 이용하여 일반권한을 획득하거나, 직접적인 취약점으로 이용될 수 있는 정보 유출 가능 | 2 |
| 하 | 취약점을 이용하여 정보 유출 가능 | 1 |

* + 1. 진단등급

[표 ] 진단등급

| 진단등급 | 설 명 | 가중치 |
| --- | --- | --- |
| 양호 | 취약점이 존재하지 않음. 안전함. | 0 |
| 취약 | 취약점이 존재하며 보안대책 적용 필요 | 1 |
| N/A | 해당 사항 없음(점검 불가) | - |

* + 1. 대책적용 시기

[표 ] 대책적용 시기

| 적용시기 | 설 명 | 기간 |
| --- | --- | --- |
| 단기 | 대상 장비의 리부팅이 없거나, 구성 변경이 간단하거나, 대책 적용으로 인한 영향도가 낮음. | 1개월 이내 |
| 중기 | 대상 장비의 리부팅이 있거나, 구성 변경이 다소 복잡하거나, 대책 적용으로 인한 영향도가 다소 높음. | 5개월 이내 |
| 장기 | 대상 장비의 리부팅이 있고, 구성 변경이 매우 복잡하거나, 대책 적용으로 인한 영향도가 매우 높은 경우, 대책 적용 전 OS 또는 Data 를 백업해야 함. | 6개월 이상 |

* 1. 진단 항목

진단 항목은 KISA 클라우드 취약점 점검 가이드 – 보안설정(CCE), EQST 클라우드 보안 가이드(컨테이너 보안) – Docker, Kubernetes, EQST 2021 클라우드 보안 가이드 - AWS 항목을 기준으로 점검함

* + 1. Linux 진단 항목

[표 ] Linux 서버 취약점 진단 항목

| 진단 구분 | 취약점 진단 항목 |
| --- | --- |
| 계정 관리 | root 계정 원격 접속 제한 |
| 패스워드 복잡성 설정 |
| 계정 잠금 임계값 설정 |
| 패스워드 최대 사용 기간 설정 |
| 패스워드 파일 보호 |
| 파일 및 디렉토리 관리 | root 홈, 패스 디렉터리 권한 및 패스 설정 |
| 파일 및 디렉터리 소유자 설정 |
| /etc/passwd 파일 소유자 및 권한 설정 |
| /etc/shadow 파일 소유자 및 권한 설정 |
| /etc/hosts 파일 소유자 및 권한 설정 |
| /etc/(x)inetd.conf 파일 소유자 및 권한 설정 |
| /etc/(r)syslog.conf 파일 소유자 및 권한 설정 |
| /etc/services 파일 소유자 및 권한 설정 |
| SUID, SGID, Sticky bit 설정 파일 점검 |
| 사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정 |
| world writable 파일 점검 |
| $HOME/.rhosts, hosts.equiv 사용 금지 |
| 접속 IP 및 포트 제한 |
| cron 파일 소유자 및 권한 설정 |
| 서비스 관리 | Finger 서비스 비활성화 |
| Anonymous FTP 비활성화 |
| r 계열 서비스 비활성화 |
| DoS 공격에 취약한 서비스 비활성화 |
| NFS 서비스 비활성화 |
| NFS 접근통제 |
| automountd 제거 |
| RPC 서비스 확인 |
| NIS, NIS+ 점검 |
| tftp, talk 서비스 비활성화 |
| Sendmail 버전 점검 |
| 스팸 메일 릴레이 제한 |
| 일반사용자의 Sendmail 실행 방지 |
| DNS 보안 버전 패치 |
| DNS ZoneTransfer 설정 |
| 패치 및 로그 관리 | 최신 보안 패치 및 벤더 권고사항 적용 |
| 로그의 정기적 검토 및 보고 |

* + 1. Docker 진단 항목

[표 ] Docker 취약점 진단 항목

| 진단 구분 | 취약점 진단 항목 |
| --- | --- |
| Docker  Configuration | 호스트 OS 주요 자원 접근 제어 |
| 인증-권한 제어 |
| SSL/TLS 적용 |
| 네임스페이스 관리 |
| 컨테이너 네트워크 제어 |
| 컨테이너 리소스 제어 |
| 컨테이너 권한 제어 |
| 컨테이너 보안 정책 |
| 로그 관리 |
| 호스트 OS | 설정 파일 및 주요 디렉터리 권한 설정 |
| audit 설정 |
| 이미지 | Dockerfile Config |
| 이미지 취약점 및 구성 결함 |
| 레지스트리 운영 관리 |
| Docker Swarm | 인증제어 |
| SSL/TLS 적용 |
| 네트워크 제어 |
| 기타 | 중요도 수준에 따른 격리 운영 |
| 앱 취약점 |
| 보안 패치 적용 |

* + 1. AWS 진단 항목

[표 ] AWS 취약점 진단 항목

| 진단 구분 | | 취약점 진단 항목 |
| --- | --- | --- |
| Identity&Crypto | IAM | 루트 사용자 계정의 액세스 키 제거 |
| 루트 사용자 계정의 MFA 활성화 |
| 복잡한 비밀번호 규칙 설정 |
| 비밀번호 재사용 제한 |
| 모든 사용자 계정 MFA 활성화 |
| 초기 액세스 키 사용 제한 |
| 90일 이상 사용하지 않는 자격 증명 비활성화 |
| 액세스 키 개수 제한 |
| 액세스 키 90일 이내 교체 |
| IAM 정책 설정 시 그룹으로 권한 관리 |
| "\*:\*" administrative 권한 제거 |
| IAM 역할을 통한 리소스 액세스 제어 |
| 만료된 SSL/TLS 인증서 삭제 |
| IAM 액세스 분석기 활성화 |
| 90일 이상 미접속 계정 삭제 |
| iam:CreatePolicyVersion 권한 해제 |
| iam:SetDefaultPolicyVersion 권한 해제 |
| iam:PassRole, ec2:RunInstances 권한 해제 |
| iam:CreateAccessKey 권한 해제 |
| iam:CreateLoginProfile 권한 해제 |
| iam:UpdateLoginProfile 권한 해제 |
| iam:AttachUserPolicy 권한 해제 |
| iam:AttachGroupPolicy 권한 해제 |
| iam:AttachRolePolicy, sts:AssumeRole 권한 해제 |
| iam:PutUserPolicy 권한 해제 |
| iam:PutGroupPolicy 권한 해제 |
| iam:PutRolePolicy, sts:AssumeRole 권한 해제 |
| iam:AddUserToGroup 권한 해제 |
| iam:UpdateAssumeRolePolicy, sts:AssumeRole 권한 해제 |
| iam:PassRole, lambda:CreateFunction, lambda:InvokeFunction 권한 해제 |
| iam:PassRole, lambda:CreateFunction, lambda:CreateEventSourceMapping, dynamodb:CreateTable, dynamodb:PutItem 권한 해제 |
| iam:PassRole, lambda:CreateFunction, lambda:CreateEventSourceMapping 권한 해제 |
| iam:PassRole, glue:CreateDevEndpoint 권한 해제 |
| glue:UpdateDevEndpoint 권한 해제 |
| iam:PassRole, cloudformation:CreateStack 권한 해제 |
| iam:PassRole, datapipeline:CreatePipeline, datapipeline:PutPipelineDefinition 권한 해제 |
| lambda:UpdateFunctionCode 권한 해제 |
| 고객 관리형 정책에서 kms:ReEncryptFrom, kms:Decrypt 권한 해제 |
| 인라인 정책에서 kms:ReEncryptFrom, kms:Decrypt 권한 해제 |
| IAM 사용자에 태그 지정 |
| KMS | 삭제가 예약된 키 여부 검토 |
| 고객 관리형 키 자동 교체 설정 |
| Secrets Manager | Secrets Manager 보안 암호 자동 교체 활성화 |
| Compute | EC2 | EC2 인스턴스 세부 모니터링 활성화 |
| EC2 종료 방지 활성화 |
| EC2 리소스 태그 지정 |
| EC2 인스턴스에 키 페어 액세스 설정 |
| EC2 인스턴스 메타데이터 버전 설정 |
| EBS 최적화 설정 |
| Lambda | Lambda 함수 인터넷 노출 제한 |
| Lamdba 함수 VPC 액세스 설정 |
| Lambda 함수에 배달 못한 편지 대기열 구성 |
| Lambda 함수의 리소스 기반 정책 설정 |
| Storage | S3 | S3 버킷 기본 암호화 설정 |
| S3 버킷 정책 HTTP 요청 거부 설정 |
| S3 버킷의 MFA 삭제 활성화 |
| Macie 활성화 |
| 퍼블릭 액세스 차단 설정 |
| S3 버킷 태그 지정 |
| S3 버킷 버전 관리 설정 |
| S3 버킷의 객체 수준 로깅 이벤트 쓰기 설정 |
| S3 버킷의 객체 수준 로깅 이벤트 읽기 설정 |
| S3 버킷 객체 잠금 활성화 |
| S3 버킷 정책 설정 |
| S3 버킷 교차 리전 복제 활성화 |
| EBS | EBS 볼륨 암호화 설정 |
| EBS 스냅샷 Private 설정 |
| EBS 백업 계획 설정 |
| EBS 삭제 대기 상태 설정 |
| EFS | EFS 자동 백업 설정 |
| EFS 암호화 설정 |
| EFS 백업 계획 설정 |
| Database | RDS | RDS 데이터베이스 퍼블릭 액세스 제한 |
| RDS 데이터베이스 암호화 설정 |
| RDS 클러스터 자동 백업 설정 |
| RDS 스냅샷 퍼블릭 액세스 제한 |
| RDS 클러스터 삭제 방지 활성화 |
| RDS 백업 계획 설정 |
| RDS 로깅 활성화 |
| RDS 데이터베이스 확장 모니터링 활성화 |
| RDS 스냅샷 암호화 |
| RDS 데이터베이스 다중 AZ 배포 설정 |
| RDS 리소스 태그 지정 |
| Redshift | Redshift 클러스터 공개적 액세스 설정 |
| Redshift 클러스터 암호화 설정 |
| Redshift 클러스터 로깅 활성화 |
| Redshift 클러스터 버전 업그레이드 설정 |
| Redshift 클러스터 전송 중 암호화 설정 |
| DynamoDB | DynamoDB 암호화 설정 |
| DynamoDB 특정 시점으로 복구 활성화 |
| DynamoDB 리소스 태그 지정 |
| DynamoDB 백업 계획 설정 |
| ElastiCache | ElastiCache Redis 클러스터 자동 백업 설정 |
| Logging | CloudTrail | CloudTrail 로그 파일 검증 활성화 |
| S3 버킷 정책 및 ACL의 퍼블릭 액세스 차단 설정 |
| CloudTrail 추적과 Cloudwatch Logs 통합 설정 |
| CloudTrail S3 버킷의 서버 액세스 로깅 활성화 |
| CloudTrail 로그 보관 시 고객 마스터 키로 암호화 |
| Monitoring | CloudWatch | 인증되지 않은 API 호출에 대한 로그 지표 및 경보 설정 |
| MFA 없이 관리 콘솔 로그인에 대한 로그 지표 및 경보 설정 |
| 루트 계정 사용에 대한 로그 지표 및 경보 설정 |
| IAM 정책 변경사항에 대한 로그 지표 및 경보 설정 |
| CloudTrail 설정 변경사항에 대한 로그 지표 및 경보 설정 |
| AWS 관리 콘솔 인증 실패에 대한 로그 지표 및 경보 설정 |
| 사용자가 생성한 CMK 비활성화 또는 삭제 예약에 대한 로그 지표 및 경보 설정 |
| S3 버킷 정책 변경사항에 대한 로그 지표 및 경보 설정 |
| AWS Config 설정 변경사항에 대한 로그 지표 및 경보 설정 |
| 보안 그룹 변경사항에 대한 로그 지표 및 경보 설정 |
| 네트워크 ACL 변경사항에 대한 로그 지표 및 경보 설정 |
| 네트워크 게이트웨이 변경사항에 대한 로그 지표 및 경보 설정 |
| 라우팅 테이블 변경사항에 대한 로그 지표 및 경보 설정 |
| VPC 변경사항에 대한 로그 지표 및 경보 설정 |
| AWS Organizations 변경사항에 대한 로그 지표 및 경보 설정 |
| SNS | SNS 주제 액세스 정책 설정 |
| SNS 주제 암호화 설정 |
| Networking | VPC | 네트워크 ACL에서 인터넷 원격 접속 제한 |
| 인스턴스 보안 그룹에서 인터넷 원격 접속 제한 |
| 기본 보안 그룹 사용 제한 |
| VPC 내 멀티 서브넷 구성 |
| 인스턴스 보안 그룹에서 80/443 포트 외 인터넷 노출 제한 |
| 네트워크 ACL에서 80/443 포트 외 인터넷 노출 제한 |
| VPC 플로우 로그 활성화 |
| 사이트 간 VPN 연결의 터널 작동 상태 설정 |
| NAT 게이트웨이 관리 |
| 인터넷 게이트웨이 관리 |
| CloudFront | CloudFront 전송 중 데이터 암호화 |
| CloudFront OAI 설정 |
| CloudFront 로깅 활성화 |
| ELB | ELB 보안 정책 최신 버전 설정 |
| ELB에 사용된 인증서 갱신 |
| CLB 교차 영역 로드 밸런싱 활성화 |
| ELB 삭제 방지 활성화 |
| ELB 액세스 로깅 활성화 |
| ELB HTTPS 리스너 설정 |
| ALB 잘못된 헤더 필드 삭제 설정 |
| ALB HTTP-HTTPS 리다이렉션 설정 |
| ALB에 WAF 활성화 |
| Route 53 | Route53 도메인 자동 갱신 활성화 |
| Route53 도메인 이전 잠금 설정 |
| API Gateway | API 게이트웨이 캐싱 활성화 |
| Analytics | Elasticsearch Service | Elasticsearch 도메인 퍼블릭 액세스 노출 제한 |
| Elasticsearch 노드 간 암호화 설정 |
| Elasticsearch 유휴 시 데이터 암호화 설정 |
| Elasticsearch 도메인의 VPC 엔드포인트 설정 |
| EMR | EMR 퍼블릭 액세스 차단 |
| EKS | Control Plance Configuration | EKS 감사 로깅 활성화 |
| CMK를 사용한 Kubernetes Secrets 암호화 설정 |
| Control Plane Endpoint 접근 제어 |
| 클러스터 전용 보안 그룹 설정 |
| 클러스터 보안 그룹 규칙 중 인터넷 노출 제한 |
| Security&Compliance | Security Hub | Security Hub 활성화 |
| WAF | WAF의 Web ACL 로깅 활성화 |

1. 산출물 및 협조사항
   1. 수행 산출물

[표 14] 수행 산출물

| 산출물 | 제출 시기 | 주요 내용 |
| --- | --- | --- |
| 수행 계획서 | 수행 전 | - 수행 목적 및 범위  - 수행 일정 및 인력투입 계획  - 수행방안 및 산출물 목록  - 사업추진에 필요한 협조 요청 사항 및 선결 사항 등 |
| 결과 보고서 | 종료 시 | - 취약점진단 총평 및 결과 상세 |
| 가이드라인 | 종료 시 | - 취약점진단 항목별 상세 조치 가이드 |

* 1. 협조 요청 사항

취약점 진단 작업 시 시스템에 영향을 줄 수 있는 해킹시도를 수행하지 않으나, 부득이한 경우 시스템에 문제가 발생할 가능성에 대비하여 담당자와 시스템 영향력에 대한 사전 협조 및 동의를 구합니다. 문제 발생 시 담당자에게 연락을 하여 긴급히 정상화 시킬 수 있도록 담당자가 항시 모니터링 수행을 하도록 권장합니다.

* 1. 수행 전 업무 협의 사항

취약점 진단 수행 중 발생 가능한 안전사고를 예방하며 효율적인 진단을 수행하기 위해 필요함. 진단 수행전 고객사 담당자와 협의를 통해 진단 대상 및 환경과 요구 사항을 전달받고 진단대상 요청 목록과 협조 사항을 전달함.

[표 15] 업무협조 요청사항

| No. | 업무협조요청 | 내용 | 비고 |
| --- | --- | --- | --- |
| 1 | 네트워크 Config 정보 | 네트워크 진단시 Config 정보를 분석해야 하므로 네트워크 Config를 텍스트파일로 요청함  (예: show running-config) |  |
| 2 | 보안장비 룰셋팅 정보 | 방화벽의 정책설정 분석에 필요한 자료를 요청함  (예: 엑셀문서, 스크린샷 등) |  |

별첨 1. 클라우드 취약점 점검 가이드 – 보안설정(CCE) (Linux)

[표 ] 한국인터넷진흥원의 클라우드 취약점 점검 가이드 – 보안설정(CCE) (Linux)

| 진단 구분 | 취약점 진단 항목 |
| --- | --- |
| 계정 관리 | root 계정 원격 접속 제한 |
| 패스워드 복잡성 설정 |
| 계정 잠금 임계값 설정 |
| 패스워드 최대 사용 기간 설정 |
| 패스워드 파일 보호 |
| 파일 및 디렉토리 관리 | root 홈, 패스 디렉터리 권한 및 패스 설정 |
| 파일 및 디렉터리 소유자 설정 |
| /etc/passwd 파일 소유자 및 권한 설정 |
| /etc/shadow 파일 소유자 및 권한 설정 |
| /etc/hosts 파일 소유자 및 권한 설정 |
| /etc/(x)inetd.conf 파일 소유자 및 권한 설정 |
| /etc/(r)syslog.conf 파일 소유자 및 권한 설정 |
| /etc/services 파일 소유자 및 권한 설정 |
| SUID, SGID, Sticky bit 설정 파일 점검 |
| 사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정 |
| world writable 파일 점검 |
| $HOME/.rhosts, hosts.equiv 사용 금지 |
| 접속 IP 및 포트 제한 |
| cron 파일 소유자 및 권한 설정 |
| 서비스 관리 | Finger 서비스 비활성화 |
| Anonymous FTP 비활성화 |
| r 계열 서비스 비활성화 |
| DoS 공격에 취약한 서비스 비활성화 |
| NFS 서비스 비활성화 |
| NFS 접근통제 |
| automountd 제거 |
| RPC 서비스 확인 |
| NIS, NIS+ 점검 |
| tftp, talk 서비스 비활성화 |
| Sendmail 버전 점검 |
| 스팸 메일 릴레이 제한 |
| 일반사용자의 Sendmail 실행 방지 |
| DNS 보안 버전 패치 |
| DNS ZoneTransfer 설정 |
| 패치 및 로그 관리 | 최신 보안 패치 및 벤더 권고사항 적용 |
| 로그의 정기적 검토 및 보고 |

별첨 2. 클라우드 보안 가이드(컨테이너 보안) – Docker, Kubernetes

[표 ] EQST 클라우드 보안가이드(컨테이너 보안) – Docker, Kubernetes (Docker)

| 진단 구분 | 취약점 진단 항목 |
| --- | --- |
| Docker  Configuration | 호스트 OS 주요 자원 접근 제어 |
| 인증-권한 제어 |
| SSL/TLS 적용 |
| 네임스페이스 관리 |
| 컨테이너 네트워크 제어 |
| 컨테이너 리소스 제어 |
| 컨테이너 권한 제어 |
| 컨테이너 보안 정책 |
| 로그 관리 |
| 호스트 OS | 설정 파일 및 주요 디렉터리 권한 설정 |
| audit 설정 |
| 이미지 | Dockerfile Config |
| 이미지 취약점 및 구성 결함 |
| 레지스트리 운영 관리 |
| Docker Swarm | 인증제어 |
| SSL/TLS 적용 |
| 네트워크 제어 |
| 기타 | 중요도 수준에 따른 격리 운영 |
| 앱 취약점 |
| 보안 패치 적용 |

별첨 3. 클라우드 보안 가이드 – AWS

[표 ] EQST 2021 클라우드 보안가이드 - AWS

| 진단 구분 | 취약점 진단 항목 |
| --- | --- |
| 계정 관리 | 관리자 계정 최소화 관리 |
| IAM 사용자 계정 단일화 관리 |
| IAM 사용자 계정 식별 관리 |
| Key Pair 접근 관리 |
| Key Pair 보관 관리 |
| MFA(Multi-Factor Authentication) |
| 패스워드 정책 관리 |
| 권한관리 | 인스턴스 보안 정책 관리 |
| RDS 보안 정책 관리 |
| S3 보안 정책 관리 |
| Access Key 정책 관리 |
| Admin Console 관리자 정책 관리 |
| IAM 사용자 및 그룹 정책 관리 |
| 데이터 관리 | 인스턴스 암호화 설정 |
| RDS 암호화 설정 |
| S3 암호화 설정 |
| 가상 리소스 관리 | 보안그룹 인/아웃바운드 ANY 설정 관리 |
| 보안그룹 인/아웃바운드 불필요 정책 관리 |
| ACL 네트워크 인/아웃바운드 트래픽 정책 관리 |
| 라우팅 테이블 정책 관리 |
| NAT 게이트웨이 연결 관리 |
| 인터넷 게이트웨이 연결 관리 |
| S3 버킷 접근 관리 |
| RDS 리소스 액세스 권한 관리 |
| RDS API 작업 권한 관리 |
| RDS 서브넷 가용 영역 관리 |
| 감사/추적 관리 | AWS 사용자 계정 로깅 설정 |
| 가상 인스턴스 로깅 설정 |
| RDS 로깅 설정 |
| S3 버킷 로깅 설정 하 |