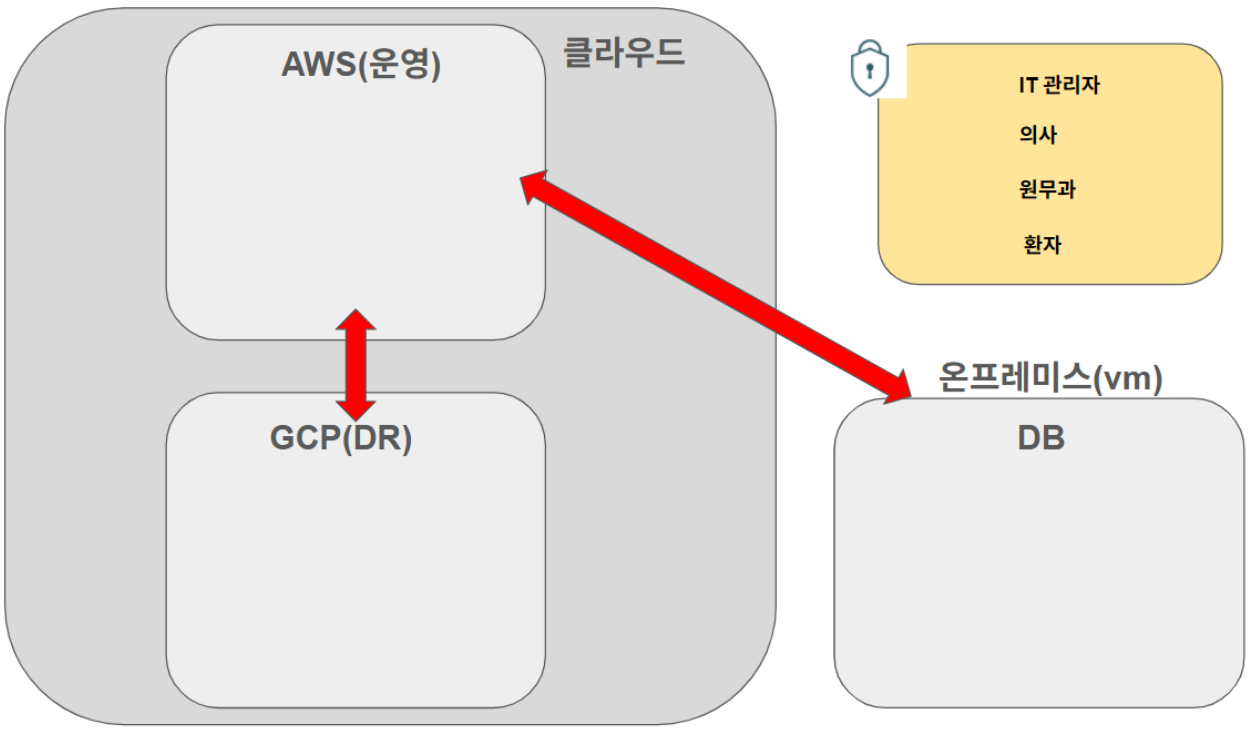
중소형 병원 하이브리드 보안 아키텍처 구축요구서

MSP 과정 최종 팀 프로젝트

Ⅰ. 개요

항목	내용
프로젝트명	중소형 병원 온프레미스 ↔ AWS 하이브리드 보안 아키텍처 구축
시나리오	입원실 및 수술실을 보유한 중소형 병원의 IT 인프라 설계, 보안 구축 및 법적 요건 대응
목적	MSP 과정 최종 프로젝트
수행 기간	2 개월
수행 인원	3 명 (AWS / GCP / Onpremise)
적용 기준	ISMS-P, 개인정보보호법, 의료법 관련 보호 원칙
핵심 설계 원칙	Security by Design — 데이터 분류 정책을 기준으로 아키텍처를 설계하고, 보안관제 및 DR 까지 연계 구현



Ⅱ. 목적 및 구축 범위

- 민감 의료정보는 온프레미스에 우선 배치하고, 대외 서비스는 AWS 에 분리 배치하는 하이브리드 아키텍처를 구축한다.
- 환자 대상 예약·접수 기능과 관리자 대상 운영·보안 관제 기능을 함께 제공한다.
- Wazuh 기반 SIEM 을 통해 온프레미스 및 AWS 로그를 통합 수집하고, 병원 특화 위협 시나리오를 탐지한다.
- 백업·복구 체계와 GCP Cold Standby 기반 긴급 운영모드를 설계·구현하여 핵심 기능 지속성을 확보한다.
- 정책서, 요구사항 정의서, 아키텍처 다이어그램, 테스트 결과서 등 실무형 산출물을 함께 제출한다.

Ⅲ. 주요 구축내용

가. 데이터 분류 기반 하이브리드 병원 인프라 구축

- 병원에서 처리하는 데이터를 민감도 및 업무 목적에 따라 등급별로 구분하고, 해당 분류 기준에 따라 저장 위치와 처리 경계를 설계한다.
- 민감 의료정보는 온프레미스에 우선 저장·관리하고, 예약·공지·대외 서비스와 같은 외부 접점 기능은 AWS 환경에 배치한다.
- 데이터 분류표는 전체 설계의 기준선으로 삼으며, 각 기능 및 인터페이스가 해당 기준을 따르도록 구현한다.

나. 온프레미스 의료정보 보호 환경 구축

- 온프레미스 영역에는 EMR 모의 서버, 내부 데이터 저장소, 보안 로그 수집 대상, 방화벽 정책을 포함한 내부 보호 구역을 구성한다.
- 민감정보 원본은 외부 클라우드에 직접 복제하거나 무차별 반출하지 않으며, 외부 서비스와의 연계가 필요한 경우 비식별 또는 최소화 처리 후 전달한다.
- 온프레미스는 제한된 물리 장비를 활용하되, 실제 중소형 병원 내부 서버실을 모사하는 수준의 구조를 갖추도록 한다.

다. AWS 기반 예약·접수 서비스 구축

- 환자 및 외부 사용자가 접근하는 예약·알림·공지 기능은 AWS 환경에 구축한다.
- 외래 예약, 입원 예약 요청, 초진/재진 구분, 예약 변경·취소, 예약 상태 조회, 예약 알림 기능을 포함한다.
- AWS 예약 시스템은 온프레미스 원본 차트를 직접 저장하지 않고, 필요한 경우 보안 통신을 통해 최소 정보만 참조하도록 한다.

라. 권한 기반 접근통제 및 인증 체계 구축

- 환자, 접수직원, 의료진, 운영자, 관리자 역할별로 화면·기능·데이터 접근 권한을 구분한다.
- 관리자 및 중요 계정에는 MFA 적용을 우선 고려하고, 최소권한 원칙에 기반한 IAM 정책을 수립한다.
- 권한 변경, 계정 잠금, 주요 설정 변경 행위는 반드시 감사로그로 남도록 한다.

마. 보안관제(SIEM) 및 위협 탐지 체계 구축

- 온프레미스 로그와 AWS CloudTrail 로그를 Wazuh 로 수집하여 단일 보안관제 체계를 구성한다.
- 병원 환경을 고려하여 비정상 시간대 대량 조회, 권한 외 진료영역 접근, USB 반출 시도, 관리자 이상 로그인 등 대표 시나리오를 탐지한다.
- 탐지 규칙, 이벤트 분류 기준, 경보 우선순위와 인시던트 대응 절차를 문서화한다.

바. 백업 및 복구 체계 구축

- 예약 데이터, 주요 설정, 보안 로그를 정기 백업하고, 암호화된 저장소에 이중 보관한다.
- 장애 또는 데이터 손상 발생 시 복구 가능한 절차를 문서화하고, 최소 1 회 이상의 복구 시나리오를 테스트한다.
- 복구 우선순위와 목표 복구시간을 정의하여 운영 관점의 복구 Runbook 을 작성한다.

사. GCP 기반 Cold Standby DR 구축

- AWS 장애 시 전체 서비스를 복제하는 대신, 핵심 예약 접수와 긴급 공지만 유지하는 경량 DR 구조를 GCP 에 구축한다.
- GCP 환경은 평상시 최소 리소스만 유지하거나 비활성 상태로 대기하고, 장애 시 운영자 승인 또는 정의된 절차에 따라 활성화한다.

• 복구 후 GCP 에서 생성된 최소 운영 데이터는 병합 또는 정리 절차를 통해 원복한다.

Ⅳ. 요구사항 분류

순번	요구사항 분류	ID 부여 규칙	요구사항 수
1	기능 요구사항	SFR-000	15
2	성능 요구사항	PER-000	5
3	시스템 장비구성 요구사항	ECR-000	3
4	인터페이스 요구사항	INR-000	4
5	데이터 요구사항	DAR-000	4
6	테스트 요구사항	TER-000	6
7	보안 요구사항	SER-000	6

Ⅶ. 상세 요구사항

▶ 기능 요구사항 (System Function Requirement)

요구사항 분류	기능 요구사항		
요구사항 고유번호	SFR-001	**요구사항 명칭**	예약시스템 기능
요구사항 상세설명	**정의**	초진/재진/입원/수술 전 예약 및 알림 기능 구현	
	세부 내용	○ 환자는 웹 기반 예약 포털을 통해 외래 예약, 입원 예약 요청, 예약 변경 및 취소를 수행할 수 있어야 한다. ○ 초진 예약은 진료과 선택, 날짜/시간 선택, 접수 흐름으로 구성하고 EMR 직접 참조 없이 처리할 수 있어야 한다. ○ 재진 예약은 환자 식별용 내부 키를 활용하여 담당의 일정 또는 최근 방문 이력을 최소 정보 기준으로 참조할 수 있어야 한다. ○ 입원 예약은 병상 또는 입원 가능 여부를 반영한 요청 흐름을 제공하여야 한다. ○ 수술 전 예약은 사전 검사 일정과 연계될 수 있도록 구성하되, 수술 이력 및 알레르기 정보는 비식별 또는 코드화 후 최소 범위만 활용하여야 한다. ○ 예약 완료, 변경, 취소 시 AWS SNS/SES 또는 동등한 방식의 알림 기능을 제공하여야 한다.	

		○ 예약 취소 및 변경은 본인 확인 절차를 거쳐 수행할 수 있어야 한다. ○ 수술실 상세 스케줄링, 보험 청구 연동, 의료진 근무표 고도화는 시나리오 설계 범위로 한정할 수 있다. ○ 환자는 자신의 예약 내역, 예약 상태, 변경 이력을 조회할 수 있어야 한다. ○ 예약 완료, 변경, 취소 시 SMS 또는 이메일 방식의 알림 기능을 제공하여야 한다. (AWS SNS/SES 활용)

요구사항 분류	기능 요구사항		
요구사항 고유번호	SFR-002	**요구사항 명칭**	사용자 인증 및 권한관리
요구사항 상세설명	**정의**	역할 기반 접근제어(RBAC) 및 MFA 적용	
	세부 내용	○ 사용자는 환자, 직원(간호사·의사·원무), 관리자 역할로 구분하여 메뉴 및 기능 접근권한을 차등 적용하여야 한다. ○ 직원 및 관리자 계정에는 MFA 적용을 우선 고려하여야 한다. ○ 비밀번호 정책은 최소 길이, 복잡도, 변경 주기를 포함하여 정의하여야 한다. ○ 비활성 세션은 일정 시간 경과 시 자동 만료되어야 한다. ○ 로그인 실패가 반복될 경우 계정 잠금 및 관리자 알림 기능을 제공할 수 있어야 한다. ○ AWS IAM 은 최소권한 원칙을 적용하고, 과도한 와일드카드 권한 부여를 지양하여야 한다. ○ 각 역할에 따라 메뉴, 버튼, 조회 가능한 데이터 범위, 수행 가능한 행위가 차등 적용되어야 한다.	

요구사항 분류	기능 요구사항		
요구사항 고유번호	SFR-003	**요구사항 명칭**	데이터 분류 및 저장 정책
요구사항 상세설명	**정의**	데이터 등급 분류 및 저장 위치 통제	
	세부 내용	○ 민감도와 업무 목적에 따라 데이터를 1 등급, 2 등급, 3 등급으로 분류하여야 한다. ○ EMR, 수술기록 등 민감한 의료정보는 온프레미스에 우선 저장·관리하여야 한다.	

		○ 민감정보 원본과 외부 전달용 가공정보의 경계가 데이터 분류 정책서에 문서화되어야 한다. ○ 예약정보, 비식별 통계, 알림 로그 등은 암호화 및 보호조치를 전제로 AWS 활용 범위에 포함할 수 있다. ○ 공지사항, 비의료 콘텐츠 등은 클라우드 환경에서 자유롭게 운영할 수 있다. ○ 데이터 분류 정책서는 별도 산출물로 제출되어야 하며, 이후 설계·구현의 기준선이 되어야 한다.

요구사항 분류	기능 요구사항		
요구사항 고유번호	SFR-004	**요구사항 명칭**	비식별화 처리(API 마스킹)
요구사항 상세설명	**정의**	온프레미스 EMR → AWS 전달 시 예약 유형별 비식별화 규칙 적용	
	세부 내용	○ 비식별화 처리는 온프레미스 내부에서 수행한 뒤 API 를 통해 최소 정보만 AWS 로 전달하여야 한다. ○ 초진 예약은 EMR 참조 없이 처리하는 것을 기본으로 한다. ○ 재진 예약은 최근 방문 진료과와 같은 최소 수준의 정보만 코드화하여 참조할 수 있어야 한다. ○ 입원 예약은 기저질환 여부 등 위험도 판단에 필요한 최소 정보만 마스킹 후 활용할 수 있어야 한다. ('만성질환 있음/없음' 수준으로 마스킹) ○ 수술 전 예약은 수술 이력 및 알레르기 정보를 코드 체계로 치환하고, 원본 진단명 또는 자유서술 원문은 전달하지 않아야 한다. ○ API Gateway 또는 동등한 수신 계층에서 허용 스키마 검증 및 비허용 필드 차단 기능을 적용하여야 한다. ○ 환자명, 주민번호, 원문 진단명 등 직접 식별정보는 온프레미스 외부로 전송하여서는 안 된다.	

요구사항 분류	기능 요구사항		
요구사항 고유번호	SFR-005	**요구사항 명칭**	SIEM 위협 탐지
요구사항 상세설명	**정의**	Wazuh 기반 내부자 위협 및 랜섬웨어 탐지 룰 구현	
	세부 내용	○ 비정상 시간대 대량 조회, 권한 외 진료영역 접근, 관리자 이상 로그인 시도 등을 탐지할 수 있어야 한다.	

		○ 대표적인 병원 내부자 위협 시나리오를 최소 2 건 이상 선정하여 탐지 룰을 구현하여야 한다. ○ USB 대량 복사 또는 이동식 저장매체 반출 시도 탐지는 가능한 범위에서 온프레미스 로그 기반으로 구현할 수 있어야 한다. ○ 랜섬웨어 관련 대량 파일 변경 또는 비정상 프로세스 실행 패턴을 보조 시나리오로 추가할 수 있다. ○ 탐지 룰은 Wazuh 규칙 문법 또는 동등한 형식으로 관리하고, 별도 룰셋 문서로 제출하여야 한다.

요구사항 분류	기능 요구사항		
요구사항 고유번호	SFR-006	**요구사항 명칭**	시간 동기화 (NTP)
요구사항 상세설명	**정의**	로그 및 보안 이벤트 분석 정확도 확보를 위한 시스템 시간 동기화	
	세부 내용	○ AWS, 온프레미스, GCP 를 포함한 모든 시스템은 동일한 기준 시간(NTP)을 사용하여 동기화하여야 한다. ○ 로그 간 시간 불일치로 인한 분석 오류를 방지하기 위하여 표준 시간 서버를 기준으로 설정하여야 한다. ○ 시간 동기화 실패 시 경고 또는 알림이 발생하도록 구성할 수 있어야 한다.	

요구사항 분류	기능 요구사항		
요구사항 고유번호	SFR-007	**요구사항 명칭**	로그 수집 및 통합 관리
요구사항 상세설명	**정의**	온프레미스 및 AWS 로그를 Wazuh 로 통합 수집·분석	
	세부 내용	○ 온프레미스 로그는 Wazuh Agent 를 통해 EMR 서버, 방화벽, 엔드포인트 등에서 직접 수집할 수 있어야 한다. ○ AWS 로그는 CloudTrail, VPC Flow Logs, CloudWatch 등에서 수집하여 Wazuh 또는 중앙분석 체계와 연계할 수 있어야 한다. ○ 로그는 온프레미스와 AWS 를 구분하여 수집하되, 중앙 대시보드에서 통합 조회할 수 있어야 한다.	

		○ 주요 로그는 별도 저장소에 이중 보관할 수 있어야 하며, GCP 로그 백업 구조와 연계할 수 있어야 한다.

요구사항 분류	기능 요구사항		
요구사항 고유번호	SFR-008	**요구사항 명칭**	인시던트 대응 플로우
요구사항 상세설명	**정의**	위협 탐지 이후 대응 절차 설계 및 문서화	
	세부 내용	○ 탐지 이벤트 발생 시 알림, 1 차 분류, 차단·격리, 원인 분석, 복구 절차를 포함한 대응 플로우를 정의하여야 한다. ○ 내부자 위협 탐지 시 해당 계정 잠금, 담당자 통보, 증적 로그 보존 절차를 포함할 수 있어야 한다. ○ 랜섬웨어 탐지 시 감염 서버 격리, 백업 복구 절차 개시 등 대응 절차를 문서화하여야 한다. ○ 인시던트 대응 플로우는 다이어그램 포함 산출물로 제출하여야 하며, 대표 시나리오 1 회 이상 모의 실행 결과를 첨부하여야 한다. ○ 인시던트 대응 절차는 개념적인 흐름에 그치지 않고, 실제 운영자가 즉시 수행할 수 있는 단계별 실행 지침(Runbook) 형태로 문서화하여야 한다.	

요구사항 분류	기능 요구사항		
요구사항 고유번호	SFR-009	**요구사항 명칭**	DR — GCP Cold Standby
요구사항 상세설명	**정의**	AWS 전체 장애 시 GCP 긴급 운영모드 전환 구성	
	세부 내용	○ 평상시 GCP 리소스는 최소 수준으로 유지하거나 비활성 상태로 둘 수 있어야 한다. ○ 장애 감지는 Route 53 헬스체크, CloudWatch Alarm, Lambda 또는 동등한 방식으로 구현할 수 있다. ○ 전환 후 GCP 에서 제공하는 기능은 예약 접수 최소 기능 및 긴급 공지 기능으로 제한할 수 있어야 한다. ○ 목표 RTO 는 약 10 분 이내로 설정하고, 실측 결과를 문서화하여야 한다. ○ 목표 RPO 는 5 분 이내를 기준으로 설정하여야 하며, 데이터 손실 범위를 최소화하도록 설계하여야 한다.	

		○ 보안 감사 및 사후 분석을 위해 주요 로그는 GCP 저장소에 이중화할 수 있어야 한다.

요구사항 분류	기능 요구사항		
요구사항 고유번호	SFR-010	**요구사항 명칭**	AWS 가용성 구성
요구사항 상세설명	**정의**	예약 시스템 고가용성을 위한 AWS 기본 가용성 구성	
	세부 내용	○ RDS 는 Multi-AZ 또는 이에 준하는 가용성 구성을 고려하여야 한다. ○ ALB 헬스체크를 활용하여 장애 인스턴스로의 트래픽을 자동 우회할 수 있어야 한다. ○ 트래픽 변동에 대응하기 위한 Auto Scaling Group 또는 동등한 확장 구조를 적용할 수 있어야 한다. ○ S3 암호화 백업 및 버전 관리 기능을 활성화할 수 있어야 한다. ○ AWS Backup 또는 동등한 방식으로 백업 정책을 구성할 수 있어야 한다.	

요구사항 분류	기능 요구사항		
요구사항 고유번호	SFR-011	**요구사항 명칭**	ISMS-P 컴플라이언스 산출물
요구사항 상세설명	**정의**	ISMS-P 기준 핵심 통제항목 이행 및 문서 산출물 생성	
	세부 내용	○ 데이터 분류 정책서, 접근통제 정책서, 로그 보존 정책서, 인시던트 대응 플로우를 포함한 핵심 문서를 작성하여야 한다. ○ 통제항목별 이행 여부와 근거를 연결한 갭 분석표를 작성할 수 있어야 한다. ○ 문서는 단순 설명 자료가 아니라 실제 구현 항목과 연결되는 형태여야 한다.	

요구사항 분류	기능 요구사항		
요구사항 고유번호	SFR-012	**요구사항 명칭**	운영자 통합관리 대시보드
요구사항 상세설명	**정의**	ISMS-P 기준 핵심 통제 MSP 운영 관점의 시스템 상태·보안·백업·DR 현황 통합 조회 기능 구현	

	세부 내용	○ 운영자는 단일 화면 또는 통합 메뉴를 통해 온프레미스, AWS, GCP 의 주요 상태를 확인할 수 있어야 한다. ○ 예약 서비스 상태, 백업 수행 여부, 보안 이벤트, 장애 상태, DR 대기 상태를 통합 조회할 수 있어야 한다. ○ 주요 장애 또는 경보 발생 시 즉시 판단할 수 있도록 핵심 정보와 이력 정보를 함께 확인할 수 있어야 한다.

요구사항 분류	기능 요구사항		
요구사항 고유번호	SFR-013	**요구사항 명칭**	비용 최적화
요구사항 상세설명	**정의**	ISMS-P 기준 핵심 통제 MSP 운영 관점의 시스템 상태·보안·백업·DR 현황 통합 조회 기능 구현	
	세부 내용	○ 사용하지 않는, 빈도가 적은 자원은 자동으로 삭제하거나 관리자에게 알림을 보내도록 한다. ○ 빈번하게 조회되지 않는 3 개월 이상의 로그는 고가의 표준 스토리지에서 **GCP Archive Storage** 또는 **AWS S3 Glacier** 로 자동 이동시켜 보관 비용 절감할 수 있어야 한다. ○ **AIOps** 기능을 통해 매주/매월 사용된 비용의 패턴을 분석하고, 이상 비용 발생 시(예: 갑작스러운 트래픽 증가로 인한 비용 폭증) AI 가 원인을 요약하여 리포트로 발송해야 한다.	

요구사항 분류	기능 요구사항		
요구사항 고유번호	SFR-014	**요구사항 명칭**	운영 자동화 및 효율화 (DevOps/IaC)
요구사항 상세설명	**정의**	ISMS-P 기준 핵심 통제 MSP 운영 관점의 시스템 상태·보안·백업·DR 현황 통합 조회 기능 구현	
	세부 내용	○ Terraform 을 사용하여 AWS 및 GCP 의 다중 클라우드 자원을 코드로 정의하고, **프로비저닝을 자동화**하여 개발·운영 환경 간의 **인프라 일관성**을 100% 유지해야 한다. ○ CI/CD 프로세스로 소스 코드 및 설정 변경 시 **자동 빌드·테스트**를 수행해야한다.	

요구사항 분류	기능 요구사항		
요구사항 고유번호	SFR-015	요구사항 명칭	키 관리
요구사항 상세설명	정의	의사의 DB 접근 및 보안 설정을 위한 **키 관리**	
	세부 내용	○ **플랫폼별 독립 키 관리**: AWS 와 GCP 등 각 클라우드에서 사용하는 비밀키는 외부 공유 없이 해당 플랫폼의 전용 보안 서비스(KMS 등)를 통해 개별적으로 관리한다. ○ **세션 기반 임시 권한 부여**: 의사가 DB 에 접근할 때마다 HashiCorp Vault 또는 AWS Secrets Manager 를 통해 **30 분~60 분간만 유효한** 임시 접속 자격 증명을 동적으로 생성한다. ○ **권한 자동 회수 및 통제**: 진료 세션 종료 또는 정해진 시간이 만료되면 부여된 권한을 시스템이 자동으로 회수하여, 내부자에 의한 데이터 오남용 및 키 유출 리스크를 원천 차단한다.	

▶ 성능 요구사항 (Performance Requirement)

요구사항 분류	성능 요구사항		
요구사항 고유번호	PER-001	요구사항 명칭	응답시간
요구사항 상세설명	정의	사용자 요청에 대한 시스템 응답 완료 시간 기준	
	세부 내용	○ 예약 목록 조회 및 메인 화면은 일반적인 사용자 체감 기준에서 지연 없이 동작하여야 한다. ○ 예약 신청·변경·취소 처리 기능은 안정적으로 수행되어야 하며, 지연 시 처리 중 안내를 제공하여야 한다. ○ 대표 화면은 3 초 이내 응답을 목표로 하고, 실패 시 명확한 안내 메시지를 제공하여야 한다.	

요구사항 분류	성능 요구사항		
요구사항 고유번호	PER-002	요구사항 명칭	가용성
요구사항 상세설명	정의	서비스 지속 가능성 및 장애 복구 목표	

	세부 내용	○ AWS 예약 시스템 정상 운영 시 가용성 목표를 정의하고, 기본 가용성 구성을 적용하여야 한다. ○ RDS Multi-AZ 또는 동등한 구조를 통해 DB 장애 시 서비스 중단을 최소화하여야 한다. ○ GCP Cold Standby DR 전환 목표 시간은 약 10 분 수준으로 설정하고, 실측 결과를 기록하여야 한다. ○ 온프레미스 핵심 노드도 목표 가용성을 정의하고 운영 정책을 수립하여야 한다.

요구사항 분류	성능 요구사항		
요구사항 고유번호	PER-003	**요구사항 명칭**	예약 동시성
요구사항 상세설명	**정의**	동일 예약 자원에 대한 중복 처리 방지 및 일관성 유지	
	세부 내용	○ 동일 시간대, 동일 예약 자원에 대해 중복 예약이 발생하지 않도록 하여야 한다. ○ 예약 처리 시 충돌 방지, 재검증, 저장 일관성 보장을 위한 트랜잭션 및 잠금 로직을 제공하여야 한다. ○ 시스템은 예약 성공/실패 결과를 명확히 반환하여 사용자의 혼선을 줄여야 한다.	

요구사항 분류	성능 요구사항		
요구사항 고유번호	PER-004	**요구사항 명칭**	SIEM 탐지 성능
요구사항 상세설명	**정의**	위협 탐지 및 알림 처리 응답 시간	
	세부 내용	○ Wazuh 탐지 룰 매칭 후 알림 발송까지의 목표 시간을 정의하여야 한다. ○ CloudTrail 등 외부 로그가 중앙 관제 체계에 반영되는 허용 시간을 정의하여야 한다. ○ 동일 시간대 복수 이벤트 발생 시 누락 없이 순차 또는 정책 기반으로 처리되어야 한다.	

요구사항 분류	성능 요구사항		
요구사항 고유번호	PER-005	**요구사항 명칭**	장애 전환 시간

요구사항 상세설명	정의	AWS 장애 발생 시 GCP 긴급 운영모드 전환 소요 시간
	세부 내용	○ AWS 장애 발생 시 GCP 긴급 운영 기능이 목표 시간 내 가동될 수 있도록 설계하여야 한다. ○ 본 프로젝트의 목표 RTO 는 10 분 이내를 기준으로 설정한다. (Route 53 감지 + Lambda 기동 + DNS 전파 포함) ○ 전환 시간은 실제 테스트를 통해 측정하고 결과를 문서로 제출하여야 한다.

▶ 시스템 장비구성 요구사항 (Equipment Composition Requirement)

요구사항 분류	시스템 장비구성 요구사항		
요구사항 고유번호	ECR-001	요구사항 명칭	온프레미스 환경 구성
요구사항 상세설명	정의	물리 서버 대역 노트북 기반 온프레미스 환경 구성	
	세부 내용	○ 운영 OS 는 Ubuntu 22.04 LTS 또는 이에 준하는 안정 버전을 적용할 수 있어야 한다. ○ EMR 시뮬레이션 서버, Wazuh Manager, 방화벽 또는 네트워크 통제 기능, API 처리 서버 역할을 구성할 수 있어야 한다. ○ 내부망, DMZ, 관리망 분리 설계를 적용할 수 있어야 한다. ○ 제한된 장비 사양 내에서 실제 병원 내부 서버실을 모사하는 구성을 목표로 한다.	

요구사항 분류	시스템 장비구성 요구사항		
요구사항 고유번호	ECR-002	요구사항 명칭	AWS 클라우드 환경 구성
요구사항 상세설명	정의	예약 시스템 및 보안 모니터링을 위한 AWS 인프라 구성	
	세부 내용	○ VPC 는 Public/Private Subnet 분리, NAT Gateway, Internet Gateway 또는 동등 구조를 포함할 수 있어야 한다. ○ 예약 시스템은 ALB, EC2, RDS 를 기준으로 구성하거나 동등한 관리형 서비스를 사용할 수 있어야 한다. ○ 보안 구성으로 WAF, GuardDuty, Security Group 최소 포트 정책, CloudTrail, VPC Flow Logs 를 포함할 수 있어야 한다. ○ 온프레미스와의 연계는 Site-to-Site VPN 또는 동등한 구조를 활용할 수 있어야 한다.	

요구사항 분류	시스템 장비구성 요구사항		
요구사항 고유번호	ECR-003	요구사항 명칭	GCP 클라우드 환경 구성
요구사항 상세설명	정의	Cold Standby DR 및 로그 백업을 위한 GCP 최소 구성	
	세부 내용	○ Compute Engine 또는 동등한 실행 환경은 평상시 최소 리소스 또는 비활성 상태로 유지할 수 있어야 한다. ○ 장애 시 예약 접수 최소 기능만 제공하도록 구성하여야 한다. ○ Cloud Storage 또는 동등한 저장소를 활용하여 Wazuh 로그 이중화 백업을 수행할 수 있어야 한다. ○ 자동 또는 반자동 전환에 필요한 방화벽 및 외부 접속 정책을 최소 범위로 구성하여야 한다.	

▶ 인터페이스 요구사항 (Interface Requirement)

요구사항 분류	인터페이스 요구사항		
요구사항 고유번호	INR-001	요구사항 명칭	하이브리드 연동 인터페이스
요구사항 상세설명	정의	온프레미스 ↔ AWS ↔ GCP 간 데이터 연동 방식 정의	
	세부 내용	○ 온프레미스와 AWS 간 데이터 전송은 VPN 및 TLS 1.2 이상 암호화를 적용하여야 한다. ○ EMR 에서 예약 시스템으로 전달되는 데이터 흐름은 비식별 처리 후 API Gateway 또는 동등한 계층을 통해 전달되어야 한다. ○ 요청/응답 스키마 정의 문서를 산출물로 제출하여야 한다. ○ 연동 구간 장애 시 타임아웃 및 재시도 로직을 고려하여야 한다.	

요구사항 분류	인터페이스 요구사항		
요구사항 고유번호	INR-002	요구사항 명칭	SIEM 대시보드 인터페이스
요구사항 상세설명	정의	Wazuh 대시보드를 통한 통합 모니터링 화면 구성	
	세부 내용	○ 온프레미스 로그와 AWS 로그를 단일 대시보드에서 통합 조회할 수 있어야 한다.	

		○ 탐지 이벤트 목록, 심각도, 발생 시간, 대상 자산 정보를 시각적으로 표시하여야 한다. ○ 내부자 위협 탐지와 랜섬웨어 탐지를 구분하여 확인할 수 있는 뷰를 제공할 수 있어야 한다. ○ 탐지 이벤트는 이메일 또는 협업 도구 알림과 연계할 수 있어야 한다.

요구사항 분류	인터페이스 요구사항		
요구사항 고유번호	INR-003	**요구사항 명칭**	예약 시스템 UI
요구사항 상세설명	**정의**	환자용 예약 인터페이스 기본 요건	
	세부 내용	○ 예약 유형 선택, 진료과 선택, 날짜·시간 선택, 접수 완료 흐름을 직관적으로 제공하여야 한다. ○ 재진 예약 시 환자 식별용 내부 키를 통한 최소 정보 기반 조회를 제공할 수 있어야 한다. ○ 예약 완료 후 SMS 또는 이메일 알림을 자동 발송할 수 있어야 한다. ○ 예약 취소 및 변경은 본인 확인 후 처리할 수 있어야 한다.	

요구사항 분류	인터페이스 요구사항		
요구사항 고유번호	INR-004	**요구사항 명칭**	관리자 인터페이스
요구사항 상세설명	**정의**	병원 관리자용 기능 인터페이스 요건	
	세부 내용	○ 예약 현황 조회, 취소·변경, 수동 등록 등 운영 기능을 제공할 수 있어야 한다. ○ 사용자 계정 생성·수정·잠금·삭제 기능을 포함할 수 있어야 한다. ○ SIEM 탐지 이벤트 확인 및 처리 상태 갱신 기능을 제공할 수 있어야 한다. ○ DR 상태 모니터링 화면에서 AWS 정상/장애 여부와 GCP 대기 상태를 조회할 수 있어야 한다.	

▶ 데이터 요구사항 (Data Requirement)

요구사항 분류	데이터 요구사항

요구사항 고유번호	DAR-001	요구사항 명칭	데이터 분류 및 저장
요구사항 상세설명	정의	데이터 등급별 저장 위치 및 접근 통제 기준	
	세부 내용	○ 1 등급 데이터는 온프레미스에 우선 저장하고, 외부 전송 시 비식별화 절차를 적용하여야 한다. ○ 2 등급 데이터는 암호화 및 접근통제 적용 후 AWS 저장이 가능할 수 있어야 한다. ○ 3 등급 데이터는 AWS 에서 자유롭게 운영할 수 있다. ○ 각 등급별 접근 가능 역할을 권한 정책과 연계하여 정의하여야 한다.	

요구사항 분류	데이터 요구사항		
요구사항 고유번호	DAR-002	요구사항 명칭	데이터 암호화
요구사항 상세설명	정의	전송 중 및 저장 중 데이터 암호화 기준	
	세부 내용	○ 전송 중 암호화는 TLS 1.2 이상을 적용하여야 한다. ○ 저장 중 암호화는 S3, RDS 등 클라우드 저장소와 온프레미스 저장소에 적절한 암호화 방식을 적용하여야 한다. ○ 민감정보 저장 위치에는 파일시스템 또는 DB 수준의 보호 방안을 고려하여야 한다.	

요구사항 분류	데이터 요구사항		
요구사항 고유번호	DAR-003	요구사항 명칭	데이터 백업 및 보존
요구사항 상세설명	정의	백업 정책 및 의료·운영 기준 보존 기간 준수	
	세부 내용	○ 백업 주기와 보존 기간은 데이터 중요도에 따라 정의하여야 한다. ○ RDS, S3, 로그 저장소 등 각각의 보존 정책을 수립하여야 한다. ○ 백업 복구 테스트를 최소 1 회 이상 수행하고 결과를 문서화하여야 한다.	

요구사항 분류	데이터 요구사항

요구사항 고유번호	DAR-004	요구사항 명칭	데이터 마이그레이션
요구사항 상세설명	정의	샘플 데이터 생성 및 정합성 검증 절차	
	세부 내용	○ 시뮬레이션용 샘플 데이터는 실제 환자 정보를 사용하지 않고 가상 데이터로 생성하여야 한다. ○ 온프레미스와 AWS 간 연동 검증 시 비식별화 필드 정합성을 확인하여야 한다. ○ 이관 또는 연동 완료 후 데이터 일치 여부 검증 절차를 수립하여야 한다.	

▶ 테스트 요구사항 (Test Requirement)

요구사항 분류	테스트 요구사항		
요구사항 고유번호	TER-001	요구사항 명칭	예약 기능 테스트
요구사항 상세설명	정의	예약 생성·변경·취소·조회 기능의 정상 동작 검증	
	세부 내용	○ 초진/재진/입원/수술 전 예약이 정상적으로 수행되는지 확인하여야 한다. ○ 예약 충돌, 변경, 취소 흐름 및 알림 발송 여부를 포함하여 테스트하여야 한다.	

요구사항 분류	테스트 요구사항		
요구사항 고유번호	TER-002	요구사항 명칭	SIEM 탐지 룰 테스트
요구사항 상세설명	정의	내부자 위협 및 랜섬웨어 탐지 룰 유효성 검증	
	세부 내용	○ 각 탐지 시나리오별 모의 이벤트를 발생시켜 탐지 성공 여부를 확인하여야 한다. ○ 야간 대량 조회, 권한 외 접근 등 대표 시나리오를 포함하여야 한다. ○ 탐지 결과 스크린샷 및 이벤트 로그 캡처를 산출물로 제출하여야 한다.	

요구사항 분류	테스트 요구사항

요구사항 고유번호	TER-003	요구사항 명칭	DR 페일오버 테스트
요구사항 상세설명	정의	GCP Cold Standby 전환 시나리오 실증	
	세부 내용	○ AWS 예약 시스템 중단을 가정한 장애 전환 테스트를 수행하여야 한다. ○ 헬스체크 감지, 전환 트리거, GCP 기동, 서비스 접근 가능 여부를 단계별로 확인하여야 한다. ○ 전체 RTO 실측 수치를 측정하고 문서화하여야 한다. ○ 복구 후 DNS 원복 또는 운영 복귀 절차도 함께 검증하여야 한다.	

요구사항 분류	테스트 요구사항		
요구사항 고유번호	TER-004	요구사항 명칭	통합 연동 테스트
요구사항 상세설명	정의	온프레미스 ↔ AWS ↔ GCP 연동 정합성 검증	
	세부 내용	○ VPN 터널 연결 상태와 암호화 통신을 검증하여야 한다. ○ 비식별화 API 정합성 테스트를 통해 예약 유형별 마스킹 결과를 검증하여야 한다. ○ CloudTrail 로그 수집과 GCP 로그 백업 동기화가 정상 동작하는지 확인하여야 한다.	

요구사항 분류	테스트 요구사항		
요구사항 고유번호	TER-005	요구사항 명칭	백업 복구 테스트
요구사항 상세설명	정의	데이터 백업 및 복구 절차 유효성 검증	
	세부 내용	○ RDS 스냅샷 또는 동등한 방식의 복구 테스트를 수행하여야 한다. ○ S3 버전 관리 또는 동등한 방식의 파일 복원 테스트를 수행할 수 있어야 한다. ○ 복구 결과, 소요 시간, 정합성 확인 결과를 문서화하여야 한다.	

요구사항 분류	테스트 요구사항

요구사항 고유번호	TER-006	요구사항 명칭	권한 테스트
요구사항 상세설명	정의	역할별 접근 가능 화면 및 기능 차등 적용 검증	
	세부 내용	○ 환자, 접수직원, 의료진, 보안운영자, 관리자별 권한 차이가 정상 동작하는지 확인하여야 한다. ○ 비인가 사용자의 접근 차단 및 화면 비노출 여부를 검증하여야 한다.	

▶ 보안 요구사항 (Security Requirement)

요구사항 분류	보안 요구사항		
요구사항 고유번호	SER-001	요구사항 명칭	ISMS-P 통제항목 이행
요구사항 상세설명	정의	ISMS-P 인증 기준 핵심 통제항목 적용	
	세부 내용	○ 접근통제, 암호화, 로그 관리, 인시던트 대응, 백업 및 복구, 개인정보 처리 항목을 중심으로 통제사항을 반영하여야 한다. ○ 각 통제항목은 설계·구현·운영 문서와 연결되어야 한다.	

요구사항 분류	보안 요구사항		
요구사항 고유번호	SER-002	요구사항 명칭	네트워크 보안
요구사항 상세설명	정의	온프레미스 및 AWS 네트워크 보안 설계	
	세부 내용	○ 온프레미스 방화벽은 내부망, DMZ, 관리망 분리와 최소 포트 허용 원칙을 적용하여야 한다. ○ AWS Security Group 은 최소 포트 원칙과 인바운드 규칙 명시적 허용만 적용하여야 한다. ○ AWS WAF, GuardDuty, VPC Flow Logs 를 활용한 클라우드 보안 레이어를 구성하여야 한다. ○ SSH 접근은 키 기반 인증을 기본으로 고려하여야 한다.	

요구사항 분류	보안 요구사항		
요구사항 고유번호	SER-003	요구사항 명칭	개인정보 보호

요구사항 상세설명	정의	개인정보보호법 기준 의료 개인정보 처리 방침
	세부 내용	○ 환자 성명, 주민번호, 원문 진단명 등 직접 식별정보는 온프레미스 외부 전송을 금지하여야 한다. ○ AWS 전달 데이터는 비식별화 처리 후 최소 정보만 전달하여야 한다. ○ 개인정보 접근 이력은 조회·수정·삭제 전 항목에 대해 감사로그를 남길 수 있어야 한다. ○ 시뮬레이션용 데이터는 실제 환자 정보 대신 가상 데이터만 사용하여야 한다. ○ 환자 본인의 진료 기록이 어디에 저장되고 누가 봤는지 알 수 있어야 한다.

요구사항 분류	보안 요구사항		
요구사항 고유번호	SER-004	요구사항 명칭	취약점 관리
요구사항 상세설명	정의	시스템 취약점 점검 및 패치 관리	
	세부 내용	○ 온프레미스 OS 보안 패치를 정기적으로 적용하여야 한다. ○ AWS Patch Manager 또는 동등한 방식으로 패치 기준선과 업데이트 정책을 운영할 수 있어야 한다. ○ 불필요 서비스 및 포트 비활성화, SSH 루트 로그인 금지, Fail2ban 등 기본 보안 강화를 적용할 수 있어야 한다.	

요구사항 분류	보안 요구사항		
요구사항 고유번호	SER-005	요구사항 명칭	감사 로그
요구사항 상세설명	정의	보안 감사를 위한 로그 수집·보존 기준	
	세부 내용	○ 기록 대상은 로그인/로그아웃, 권한 변경, 데이터 조회·수정·삭제, 설정 변경 등을 포함하여야 한다. ○ 로그는 위변조 방지 및 별도 저장소 분리 원칙을 고려하여야 한다. ○ AWS CloudTrail 은 관리 이벤트 및 필요한 범위의 데이터 이벤트를 기록하여야 한다.	

요구사항 분류	보안 요구사항		
요구사항 고유번호	SER-006	**요구사항 명칭**	온프레미스-AWS 및 사용자 접근 구간의 암호화 보호
요구사항 상세설명	**정의**	온프레미스-AWS 및 사용자 접근 구간의 암호화 보호	
	세부 내용	○ 온프레미스와 AWS 간 통신은 Site-to-Site VPN 을 통한 암호화 전용 통신 경로를 사용하여야 한다. ○ 웹 서비스 구간은 TLS 1.2 이상의 HTTPS 를 적용하여야 한다. ○ API Gateway 수신 데이터에 스키마 검증 및 비허용 필드 차단 로직을 적용하여야 한다.	