윤주혜

취약점 진단 · SAST/DAST 운영 · 개발보안



경력

현대오토에버
2024.07–현재

롯데이노베이트
2022.03–2024.07

SK쉴더스
2020.08–2022.03

보유 역량

웹·앱 모의해킹
웹·앱 애플리케이션 대상 취약점 검출

인프라·AWS 보안 진단
서버·DB 설정과 AWS 보안 설정 점검

소스코드 취약점 진단
소스코드 기반 정오탐 분류

SAST·DAST 운영·자동화
플랫폼 운영·업무 자동화·조치관리

개발보안 기획·기술검증
가이드 제작·점검 체계 기획·PoC

기술 PL· 진단 품질관리
일정 관리·산출물 검토·온보딩

SKILL SET

Security Assessment
Fortify · AppScan · Sparrow

Development Security
Secure SDLC · Secure Coding

Vulnerability Analysis
Web/App · Infra · Source Code · AWS

자격

AI-POT 1급
2026.08

AWS SAA
2026.03

CPPG
2025.09

보안약점 진단원
2023.10

정보처리기사
2019.05

SAST·DAST 운영 및 취약점 관리

점검 서비스 운영 과정에서 대상 관리·정오탐 분류·이행 점검 지원 및 서비스 품질 관리

01 대상 선정·접수

정기점검 대상 선정
보안성 검토 대상 범위 검토

02 점검 진행

SAST · Fortify
소스코드 정적 분석

DAST · AppScan
웹 서비스 동적 점검

설치·계정·실행·접근 설정(SG) 지원

03 정오탐 판단·조치 협의

취약점 및 소스 검토 후 검출 근거 확인
정오탐 분류
※ 확인 필요 시 개발자에게 요청

조치방안 기술 검토·서비스 영향 협의

04 조치·이행점검

개발자 조치 항목 확인
조치 가이드 제공
미이행 항목 조치 독려

05 결과 확인·종료

최종 리포트 검토·승인
조치 결과·예외 확인

전 그룹사 대상 서비스 형태로 운영 중

조치 완료 시까지 반복

검출 항목별 정오탐 판단 사례를 정오탐 가이드에 반영

예외·유예 검토

1차 기술적 검토·결재

반려

승인 예외 반영

진단환경 운영

Fortify·AppScan 서버 운영 및 기술지원

서버·DB 운영

OS·DB 관리 / 솔루션 업데이트
EoS 대응 · 취약점 점검 대응

점검 기술지원

계정·클라이언트·실행 환경
점검 오류·문의·장애 대응

운영 개선·관리

진단 기준 개선	룰셋 검토 및 적용 · 진단자용 정오탐 가이드 최신화
정기점검·현황	소스 정기점검 · 조치 이행 현황 · 그룹 KPI 지원
가이드·매뉴얼	사용자 가이드 · 장애대응 매뉴얼 · 운영 매뉴얼 작성
업무 효율화	**Fortify API** 진단 결과 관리 → **취약점관리 플랫폼** 리포트 연동 → **Teams·Jira** 취약점 추적·알림 → **대시보드** 현황 가시화

기술 취약점 진단

웹·앱 모의해킹과 인프라·AWS 진단을 수행하고, 취약점 검출 및 조치방안 제시

01 진단 범위

진단 대상

주요정보통신기반시설
웹·앱·인프라·AWS 환경
애플리케이션 소스코드

수행 범위

정기·상시 취약점 진단
신규 오픈 시스템 테마점검
취약점 원인·영향 분석
조치방안 안내·이행점검

검증 기준

공격 재현·서비스 영향 확인
조치 후 잔여 취약점 이행점검

02 기술 진단 영역

웹·앱 모의해킹



웹·앱 공격 가능성 검증

웹·앱 애플리케이션 대상 취약점 검출
고객사 결과보고서 전달·보고
개발자에게 조치 요청
개발자 조치 후 이행점검

인프라 취약점 진단



서버·DB 설정 점검

OS·WEB/WAS·DB·Network·보안장비 진단
OS별 버전 스크립트 검증·개정
점검 스크립트·가이드 개정
필요 시 인프라 담당자 인터뷰 진행
담당자 조치 후 이행점검

AWS 클라우드 보안 진단



계정 내 리소스별 보안 설정 점검
진단 결과·개선방안 정리
담당자 조치 후 이행점검

소스코드 연계 검증

소스코드 원인 확인 ⟷ **모의해킹 공격 가능성**

소스코드 진단 후 모의해킹 악용 가능성 교차 검증
실제 공격 재현 여부 확인
하드코딩 항목은 전체 소스코드에서 확인하여 미탐 최소화

소스코드 진단



Sparrow 기반 소스코드 취약점 진단
코드 플로우 기반 정오탐 판정
취약점 원인·수정 방안 안내
수정 코드 기준 조치 여부 확인

03 공통 진단·검증 과정

01 범위·환경 확인
대상·범위·접근 환경

→

02 기술 진단 수행
영역별 취약점 진단

→

03 취약점 검증
발생 조건·정오탐 분류

→

04 결과 보고·조치 요청
고객사 보고·담당자 조치 요청

→

05 조치 이행점검
수정 내용·조치 여부 확인

기술 PL 및 진단 품질관리

프로젝트 전반적인 일정 관리 및 진단 품질 관리·개선 지원

01 기술 PL 역할

프로젝트 계획·WBS 관리

고객사 범위·일정 협의
WBS·진행 현황 관리

업무 배치·수행 지원

기술 인력 프로젝트 업무 배치
인원별 수행 현황 확인

고객 협의·보고

착수·종료보고·기술 이슈 설명
이행점검 일정 협의

산출물 품질 검토

진단 근거·판정 타당성 확인
보고서·조치방안 품질 검토

조치 협의·이행관리

개발자와 조치 협의
개선방안 전달 및 이행점검

신규 진단원 온보딩

모의해킹·소스코드·인프라 OJT
진단 기준·수행 방법 교육

02 진단 품질관리·개선

프로젝트 수행·검토

범위·일정 협의 → 업무 배치·진단 수행 → 산출물 검토 근거·판정 확인 → 조치방안 협의 → 이행 점검 조치 결과 확인 → 종료 보고

외부 인력 점검 결과 교차검증

외주 업체·파트너사 진단 결과 → 기술적 타당성 확인 → 보완 요청·결과 정리

진단 품질 개선

스크립트·룰셋 개선
인프라 점검 스크립트 / 소스코드 탐지 룰 개정

가이드·보고서 표준화
보안가이드·보고서 양식 개선

진단 사례·교육 공유
시큐어코딩 자료 제작·교육·진단 사례 공유

03 주요 성과

조치 이행 개선

50% 미만 → 약 93%

특정 차세대 프로젝트에서 실시간 조치 협의·이행점검

진단 인력 육성

3명 → 6명

소스코드 진단 OJT 통해 점검 인력 증가 기여

결과 품질·기준 개선

스크립트·룰셋·가이드 개선
보고서 템플릿·점검 기준 통일화

개발보안 업무 수행

사내 개발보안 체계 수립을 위한 전사 업무 수행

01 전사 보안지침 개정 지원

시스템 보안지침 개정안에서 개발보안 조항 검토

지침 개정안을 개발보안 관점에서 검토

개발팀이 실제로 적용할 수 있도록 조항 수정안을 정보보안팀에 제안

산출물 개발보안 조항 검토 의견·수정안 제시

02 신규 취약점 검토·대응자료 배포

신규 이슈의 적용 환경·발생 조건·영향·대응 검토

JWT 취약점 검토 → JWT 보안가이드 신규 작성·전사 배포

LiteLLM 등 신규 보안 이슈 검토·대응자료 배포

산출물 JWT 보안가이드 / 신규 이슈 대응자료·활용 지침

03 반복 취약점 원인 분석(RCA)·공통 보안 모듈 설계 기획

분석 목적 여러 서비스에서 동일 취약점이 반복적으로 발견되는 원인을 비교해, 공통적으로 해결할 수 있는 방안 마련

반복 사례 분류
취약점 유형·발생 위치 확인

→

재발 원인 분석
유사 코드·기존 조치 범위 비교

→

공통 적용 범위 정의
위험도·재사용성 기준 우선순위

→

설계 초안·검증 계획
기능 요건·파일럿 검증 방안

우선 추진 과제 공통 보안 모듈 설계 기획 → [1차 설계 대상] 파일 업로드 검증·XSS

R&R 제안

보안팀(SA) | 보안 요건·적용 기준 정의, 모듈 배포·교육

개발팀 | 모듈 상세 설계·구현·단위테스트

법무팀 | 외주 계약·과업 범위에 보안 요건 반영 가능 여부 검토

산출물 RCA 분석자료 / 재발 방지 개선안 / 공통 보안 모듈 요건·설계 초안

04 해외법인 정기점검 체계 기획

소스코드 점검 운영 기준과 오픈소스 정기 점검 도입안 기획

자산리스트 작성 및 점검 영역별 대상 검토, 영문 신청서·가이드 마련

오픈소스 도구 견적·라이선스 도입 방안 및 도입 일정 협의

운영 설계 점검 신청·결과 검토·조치 확인 절차와 현지·본사 간 R&R 정리

산출물 정기점검 절차·R&R / RACI

05 설계·구현 단계 가이드·교육자료

설계 단계 설계단계 보안 가이드 작성·전사 배포

구현 단계 Java 최신 예제·교육자료 제작·전사 배포

주요 보안약점 위주 취약점 설명·안전한 코드·안전하지 않은 코드·수정 방안 반영

매년 교육자료 개정·전사 배포 (C/C++/Python 추가 제작 예정)

산출물 설계단계 보안 가이드 / Java 기반 시큐어코딩 교육자료

개발보안 솔루션 PoC

솔루션 검증 환경 구성부터 기능 검증·결과 보고 수행

01 개요

검증 분야

개발보안 솔루션

검증 목표

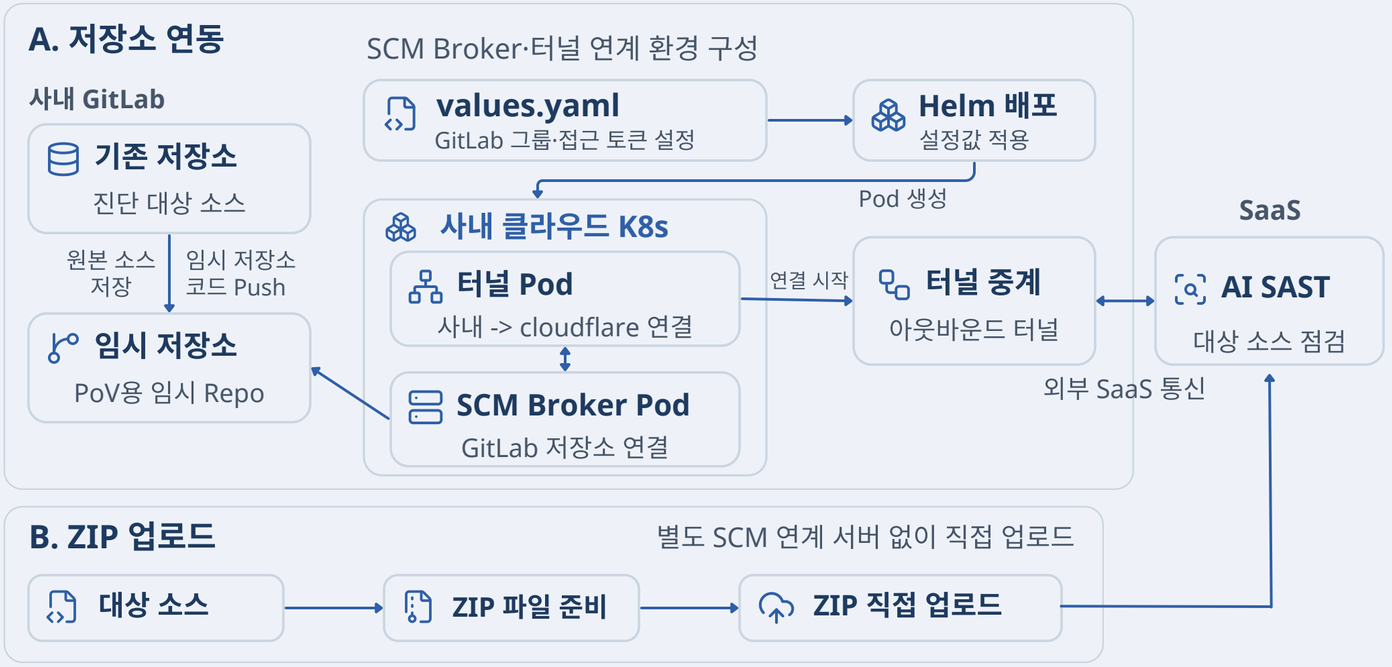
진단 효과·업무 활용성 검증
사내 환경 적합성 검토

수행 역할

환경 구성·검증 설계
결과 분석·최종 보고

02 대표 사례

PoV 환경 구성



03 대표 사례 검증 결과

원본 소스 교차검증
호출·도달성·보상통제 확인

보고서 보완
분석 근거·패치 제안 및 데이터 가공

결과 검증
정오탐·조치방안 타당성 검토

개발자 조치 요청
코드 근거·영향·개선방안 전달

주요 산출물

소스·보고서 교차검증 체크리스트
취약점별 정오탐 분석 보고서
- 소스 근거·동일 원인 그룹화·보완 설명

취약점 원인·조치 가이드

04 PoC 공통 수행 과정

01 대상·범위 협의	02 검증 환경 구성	03 기능·진단 검증	04 결과 검증·판단	05 조치 요청	06 결과 보고
대상 서비스·검증 범위 협의	솔루션별 설치 요건 반영	시나리오·점검 실행	근거·기존 점검 비교 데이터 타당성 검토	확인 취약점·개선방안 전달	검증 결과·적용 제약 정리