

Sparrow 통합 보안 진단 컨설팅

소프트웨어 개발 전주기와 공급망 전반의 보안 수준을 진단하고,
SSDF 기반의 개발 보안 체계를 수립·점검·고도화하는 통합 보안 컨설팅 서비스입니다.

안전한 소프트웨어 개발을 위한 기준, SSDF*

* SSDF(Secure Software Development Framework)는
미국 NIST에서 제시한 안전한 소프트웨어 개발을 위한 보안
프레임워크(NIST SP 800-218)입니다.

현재 오픈소스 활용 확대와 복잡한 개발 생태계로 인해 소프트웨어 공급망 공격이 주요 보안 위협으로 부상하고 있는 가운데 개발 생태계의 복잡성은 곧 보안의 사각 지대를 의미합니다. 이에 따라 개발 이후에 보안을 점검하는 방식만으로는 위험을 효과적으로 관리하기 어려워졌습니다.

보안은 이제 개발 완료 이후의 점검으로 끝나는 것이 아니라 소프트웨어 개발 생명주기(SDLC) 전 과정에 내재화되어야 하는 핵심 요소가 되었습니다.

SSDF는 안전한 소프트웨어 개발 프레임워크로 소프트웨어 개발 생명주기(SDLC) 전반에 걸쳐 보안을 통합하기 위해 미국 국립표준기술연구소(NIST)가 제정한 가이드라인입니다. 조직, 개발 프로세스, 보안 점검 활동을 통합적으로 관리하여 안전한 소프트웨어 개발 체계를 구축하기 위한 실무 지침을 제공합니다.

이제 기업은 단순한 취약점 점검을 넘어 SSDF 기반의 체계적인 보안 개발 프로세스 구축이 필수입니다.

서비스 소개

✓ 개발 환경 전반의 통합 보안 진단

소스코드, 실행 환경, 오픈소스 의존성 등 소프트웨어 개발 전반의 보안 리스크를 통합적으로 진단합니다.

✓ 실행 가능한 보안 개선 로드맵 제공

발견된 취약점과 보안 리스크를 분석하여 우선순위를 도출하고 실질적인 개선 계획을 제공합니다.

✓ 지속적인 보안 관리 체계 구축 지원

Sparrow 보안 분석 도구와 연계를 통해 지속적인 취약점 관리와 개발 보안 체계 운영을 지원합니다.

자동화 보안 분석 도구와 전문가 분석을 결합한 통합 보안 진단

전문가를 통한
진단 서비스 제공

전체 SW 개발 환경 진단

분석 결과 통합 해석

보안 리스크 우선순위 도출

자체 개발
분석 도구 활용

SAST (소스코드)

소스코드 보안 약점
및 품질 결합 분석

DAST (웹취약점)

자동화 동적 취약점 분석

SCA (오픈소스)

오픈소스 소프트웨어 라이선스
식별 및 보안 취약점 진단

모의해킹

전문 인력이 공격
시나리오 기반 검증 수행

오픈소스 의존성 식별과
SBOM 생성 및 관리

프로세스



표준 진단 기준 적용

소프트웨어 개발 환경과 보안 수준을 체계적으로 평가하기 위해 국내외 주요 컴플라이언스 기반으로 보안 수준을 점검하고 진단합니다.

+ 행정안전부 소프트웨어 보안약점 진단가이드, 주요정보통신기반시설 취약점 분석·평가 기준, 소프트웨어 개발보안 점검 기준 등



통합 보안 진단 보고서 제공

개별 진단 결과를 단순히 나열하는 것이 아니라, 개발 및 운영 환경에 대한 보안 수준을 종합적으로 진단하고 잠재적 취약 요소를 사전에 식별해 통합적인 관점의 진단 보고서를 제공합니다.

1

진단 접수

- 사전 계획 수립
- 점검 기준
 - 분석 대상
 - 수행 일정

2

진단 준비

- 진단 환경 조사
- 개발 환경
 - 개발 언어
 - 오픈소스

3

최초 진단

- 유형별 진단
결과 리뷰
보고서 작성

4

보완 조치

- 보완 조치 수행
문의 대응

5

이행 진단

- 보안 이행 진단 수행
조치 내역 확인
미조치건 개선 권고

기대효과



01 소프트웨어 품질 및 보안 수준 향상

보안이 적용된 개발·운영 환경을 구축하여 소프트웨어 품질을 높이고 중요 데이터 및 개인정보 보호 수준을 향상시켜 비즈니스 신뢰도를 확보합니다.



02 소프트웨어 공급망 보안 강화

전방위적인 보안 진단을 통해 소프트웨어 개발 환경과 공급망 전반의 보안 리스크를 식별하고 조직 환경의 보안 수준을 강화합니다.



03 보안 분석 솔루션과 전문가 기반 통합 컨설팅

보안 분석 솔루션을 통한 객관적인 데이터와 보안 전문가의 분석을 결합하여 보다 정확하고 신뢰할 수 있는 보안 진단과 개선 방향을 제공합니다.



04 지속 가능한 보안 관리 체계 구축

단발성 진단에 그치지 않고 지속적인 취약점 관리와 보안 개선 활동을 통해 안정적인 서비스 운영과 업무 연속성을 지원합니다.

자세한 상담이 필요하다면,
지금 바로 문의주세요!

✉ E. marketing@sparrow.im

📞 T. 02-6263-7400



스파로우 홈페이지