SPARROW

Sparrow Enterprise

애플리케이션 보안 테스팅(AST) 통합 솔루션

First AST Solution
Leading AST Solution

국내 최초 AST 솔루션 제조사이자 안전한 SW 개발을 위해
앞장서는 스패로우가 SW 공급망 보안의 시작과 끝을 함께합니다.

SW 공급망 위협에 선제적으로 대응하는
애플리케이션 보안 테스팅 통합 솔루션

Sparrow Enterprise

SW 공급망 공격이 날로 고도화됨에 따라, 국내외에서는 SW 공급망의 신뢰성을
확보하기 위해 SW 보안 취약점을 조기에 식별하고 지속적으로 관리할 것을 적극 권장하고 있습니다.

Sparrow Enterprise 는
소스코드 · 오픈소스 · 웹 취약점을 하나의 플랫폼에서 분석 및 관리할 수 있는 애플리케이션
보안 테스팅 환경을 제공합니다. SW 개발 단계에서부터 보안 취약점을 조치해 효율적으로 SW 안전을
확보할 수 있으며 오픈소스 라이선스와 보안 취약점 등을 SBOM으로 관리해 SW 공급망 위협 대응이 가능합니다.

주요 기능

Sparrow Enterprise는 SW 개발 전주기에 걸친 보안 취약점 분석 기능과 함께 분석 결과를 효율적으로 관리하기 위한
다양한 기능들을 제공합니다.

대시보드	자산별 이슈 확인 (소스코드, 컴포넌트, 웹 취약점)	전체 자산 확인 (총 자산, 위험한 자산, 컴포넌트)	이슈 검출 현황 확인 (위험도별, 상태별, 기간별)	결재 상태 확인 (진행 중인 결재, 처리할 결재)

분석 기능	소스코드 분석	컴포넌트 분석	웹 취약점 분석	분석 자동화
	보안 약점 분석 품질 결함 분석 이슈 발생 지점 확인 안전한 코드 예시 확인	컴포넌트 식별 라이선스 고지의무 확인 취약점 검출 및 확인 SBOM 생성 및 내보내기	분석 대상 선택 (URL, OpenAPI) 분석 범위 설정 (URL 수집 깊이, 제외 URL 등) 공격 과정 재현	이기종 도구 연동 (형상관리시스템, CI/CD 도구 등) 분석 상태 실시간 확인 (실행, 중지, 완료)

관리 기능	사용자 관리	결재 관리	이슈 상태 관리	이슈 검출 규칙 관리	보고서 관리
	구성원 추가 역할 및 권한 제어 분석 이력 확인	결재선 및 단계 설정 결재 유형 설정 (합의, 결재) 결재 대상 항목 관리 (이슈, 자산, 컴포넌트 등)	검토 담당자 배정 상태 변경 (확인, 미확인, 해결)	정책 기반 검출 규칙 선택 (SW 보안약점 진단 가이드 등) 위험도별 이슈 5단계 구분 (매우 높음, 높음, 보통 등) 사용자 지정 검출 규칙 추가	템플릿 설정 (제목, 로고 등) 포함될 검출 규칙 선택 (SW 보안약점 진단 가이드 등) 포함될 구성요소 선택 (위험도별, 검출 규칙별 등)

AI 기능	오픈소스 AI 모델 사용 여부 식별	소스코드 취약점 조치 방안 제안	취약점 조치 우선 순위 제안

분석 기술

Sparrow Enterprise는 SW 개발부터 운영까지 발생 가능한 소스코드 · 오픈소스 · 웹 취약점을 분석해 한층 더 탄탄한 SW 공급망 보안 체계를 구축할 수 있도록 기여합니다.

소스코드 보안약점 및 품질 결함 분석
SAST/SAQT

소스코드에 잠재하는 보안약점 및 품질 결함을 분석해 시큐어 코딩이 가능합니다.

- C/C++, JAVA, Python 등 25개 이상 언어와 프레임워크, IaC 분석 지원
- 실제 소스코드 기반으로 취약점 발생 지점과 원인 제공
- 점검 결과 조치를 위한 안전한 소스코드 예시 제공
- 분석 대상 내 오픈소스 자산 식별 및 취약점 점검

오픈소스 분석 및 관리
SCA

사용 중인 오픈소스를 식별해 라이선스와 취약점 정보를 제공하고, SW 자재명세서 (SBOM)를 생성합니다.

- 오픈소스 AI 모델을 비롯한 오픈소스 라이선스 자동 식별 및 고지 의무 여부 제공
- 취약점 정보 제공 및 안전한 버전으로의 업데이트 안내
- SPDX, CycloneDX 등 다양한 형식의 SBOM 생성
- 컨테이너를 포함한 다양한 오픈소스 소프트웨어 및 SBOM 분석 지원

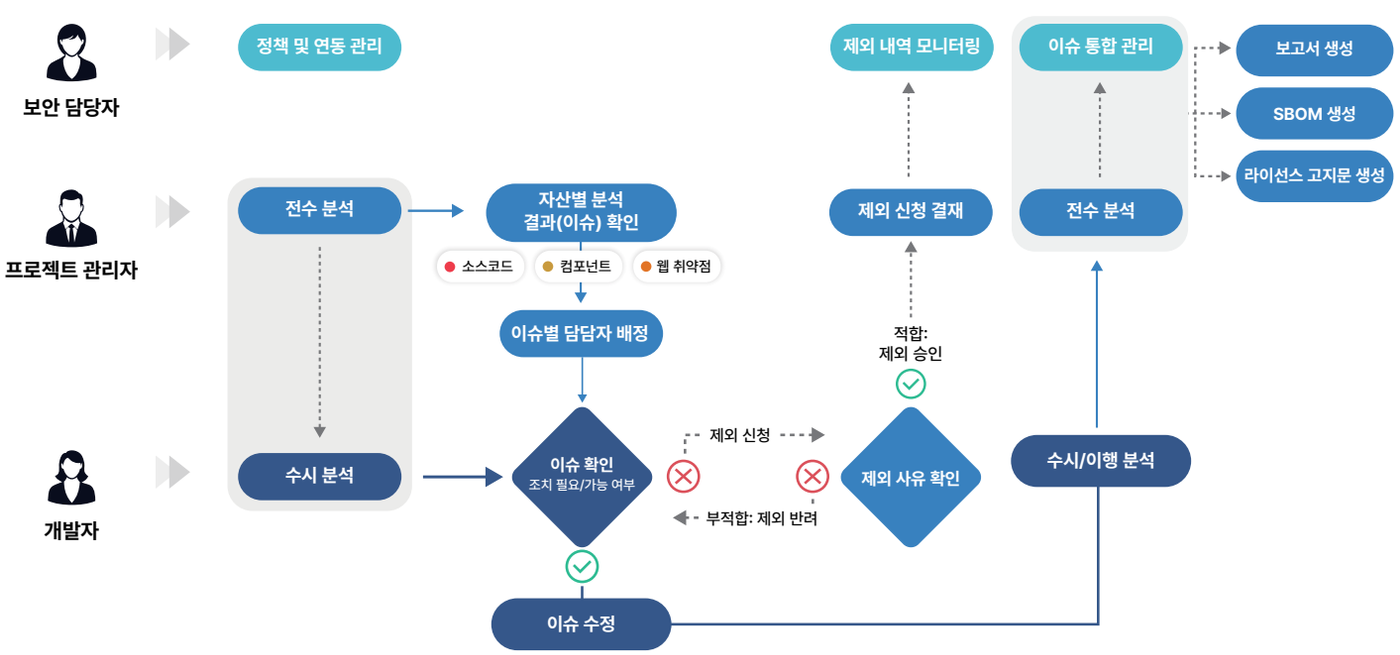
웹 애플리케이션 취약점 동적 분석
DAST

소스코드 분석으로 발견하지 못하는 웹 애플리케이션 실행 과정에서의 취약점을 테스트 단계에서 검출합니다.

- 웹사이트 최상위 URL 또는 OpenAPI 명세 기반 분석 수행
- URL 분석 깊이 조절, SSL 인증서 사용 등 세부 옵션 제공
- 발견된 취약점 설명과 함께 해결 방안 제시
- API 보안을 위한 OWASP API Top 10 기반 분석 지원

분석 및 이슈 처리 과정

SW 개발 전주기에 걸친 일관된 보안 정책을 설정하고, 사용자 별로 역할 및 권한을 차등 부여해 주기적인 전수/수시 분석이 가능합니다. 프로젝트별 분석 결과를 이슈별로 관리함으로써 보안 위협에 효과적으로 대응합니다.



연동	사내 시스템	DevOps 도구
	인사관리 시스템, 메일/메신저, 인증 솔루션 등	형상 관리 시스템, CI/CD 도구, 이슈 트래킹 시스템 등

도입효과

애플리케이션 취약점을 단일 플랫폼에서 분석하고 통합 관리해 보안 운영 효율성을 제고합니다.
기업별 보안 요구사항을 반영한 정책 설정으로 체계적인 취약점 관리 프로세스를 구축해 보안 위협을 사전 예방할 수 있습니다.

1 Point 통합 분석으로 보안 사각지대 최소화

소스코드 보안약점 분석, SW 구성요소 분석, 웹 애플리케이션 취약점 동적 분석을 하나로 통합하여 SW 개발 전주기에 걸친 보안 위협을 탐지합니다. 상호 작용 분석으로 개별 도구로는 놓치기 쉬운 취약점까지 폭넓게 점검해 보안 사각지대를 최소화하고 결재 기능을 통해 취약점 조치 여부를 체계적으로 관리할 수 있습니다.

2 Point DevSecOps 기반의 선제적 취약점 조치

형상관리부터 배포까지 DevOps 파이프라인과 연동해 일관된 보안 정책 기반으로 개발부터 운영까지 각 단계별 보안 테스트를 자동화합니다. 이를 통해 취약점을 조기에 식별 및 조치함과 동시에 개발팀과 보안팀이 동일한 기준으로 대응하며 개발 속도와 보안의 균형을 유지하는 DevSecOps를 실현할 수 있습니다.

3 Point 통합 관리를 통한 가시성 확보 및 운영 효율 향상

분석 결과를 통합 관리해 자산별 보안 상태와 취약점 조치 현황을 한눈에 파악할 수 있습니다.
또한, 조치 우선순위 제안과 취약점 재현 기능 등을 통해 중요한 이슈부터 신속하게 대응함으로써 취약점 조치 시간을 단축하고 보안 운영 효율성과 관리 편의성을 높일 수 있습니다.

고객사

뛰어난 분석력과 높은 편의성으로 많은 공공기관과 기업의 선택을 받아 SW 공급망을 안전하게 보호하고 있습니다.

공공 법무부, 성평등가족부, 고용노동부, 외교부, 통일부, 산업통상부, 대법원, 조달청, 기상청, 국가데이터처, 지식재산처, 국세청, 관세청, 경찰청, 국회사무처, 한국인터넷진흥원, 대한지방행정공제회, 인천국제공항공사, 한국공항공사, 한국자산관리공사, 예금보험공사, 한국전력기술, 한국가스공사, 한국수자원공사, 한국남부발전, 한국동서발전, 한국남동발전, 한국중부발전, 사회보장정보원, 한국재정정보원, 한국신용정보원, 한국주택금융공사, 주택도시보증공사, 코레일, 한국방송공사, 강원테크노파크, 더케이교직원나라

금융 금융감독원, 금융결제원, 한국은행, KB국민은행, 신한은행, 농협은행, KDB산업은행, IM뱅크, 한국투자증권, 키움증권, 신한투자증권, 대신증권, 교보증권, SK증권, NH투자증권, 카카오페이증권, KB국민카드, 우리카드, 롯데카드, 농협카드, KB손해보험, 농협손해보험, AXA손해보험, 롯데손해보험, 코리안리재보험, 삼성생명, DB생명, 한화생명, 농협생명, 하나생명, 한국투자캐피탈, 신한캐피탈, KB캐피탈, KDB캐피탈, 메리츠캐피탈, 다날, 핀크, 코스콤, 나이스평가정보, SBI저축은행, 한국투자저축은행, IBK저축은행, MG새마을금고

기업 SK텔레콤, 케이티, 삼성SDS, 네이버클라우드, CJ올리브네트웍스, SK네트웍스, 효성, 카카오엔터프라이즈, NHN, 롯데이노베이트, 엔씨소프트, 네오플, 현대자동차, GS칼텍스, 포스코, SK케미칼, 현대로템, 한화에어로스페이스, 세메스, 42dot, 한화오션, HMM, STX엔진, SK브로드밴드, CJ대한통운, 티맵모빌리티, GS리테일, 홈플러스, 동국제강, 골프존, KT&G, SK인텔릭스, 효성티앤에스

국방 육군, 해군, 공군, 방위사업청, 병무청, 사이버작전사령부, 국군지휘통신사령부, 한국국방연구원, 국방기술품질원, 국가보안기술연구소, LIG넥스원, 한화시스템

자세한 상담이 필요하다면,
지금 바로 문의주세요!

✉ E. marketing@sparrow.im
🎧 T. 02-6263-7400

스패로우 홈페이지