



Smart & Secure DevSecOps

90%

웹 애플리케이션을 통한
해킹 공격 비율

* 출처 : Verizon DBIR

45%

2025년까지 소프트웨어
공급망 공격을 경험할
전 세계 조직 비율

* 출처 : Gartner

20,142건

2021년 신규 취약점 건수

* 출처 : CVE Details

193.1일

초고위험군 취약점을
고치는데 소요되는
평균 기간

* 출처 : NTT Application Security

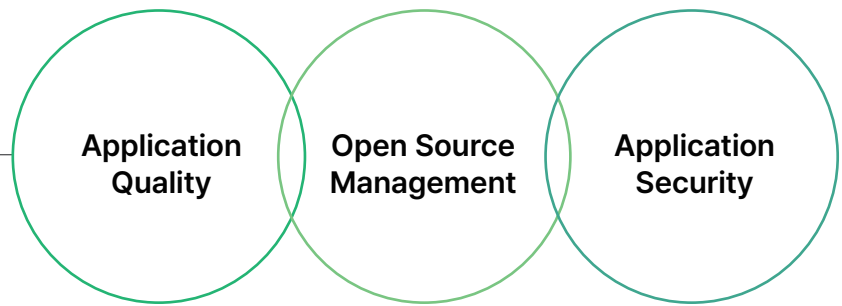
Guarantees Quality & Security of Software!

주식회사 스파로우는

실행 의미 기반의 프로그램 오류 분석 분야에서 국내 최초 GS 인증 획득, 소스코드 보안 약점 분석 도구로 업계 최초 CC 인증 획득, 그리고 국내 업체 중 유일하게 가트너 매직 쿼드런트 애플리케이션 보안 테스트 부문에도 등재되었던 기업입니다.

독자적인 기술력을 바탕으로 소프트웨어 개발 주기의 모든 단계에서 보안 취약점과 품질 이슈를 검출하고 보안 테스트 자동화를 통해 DevSecOps를 구현할 수 있도록 지원하고 있습니다.

스파로우는 사용자가 더욱 안전하게 애플리케이션을 개발하고 활용할 수 있도록 훌륭한 제품을 공급하는 수준을 넘어 소프트웨어의 가치를 높이는 글로벌 기업이 되겠습니다.



포괄적인 제품군

개발, 테스트 및 운영 단계에 걸쳐 애플리케이션 보안과 품질 개선을 위해 필요한 다양한 도구를 제공하여 보다 안전한 개발과 DevSecOps 구현이 가능합니다.

자동화 도구

애플리케이션을 손쉽게 테스트하고 관리할 수 있도록 자동화를 지원하고 보안 취약점과 품질 이슈를 정확하고 빠르게 검출하여 최소한의 시간으로 문제 해결이 가능합니다.

편리한 관리

GUI, CLI, 웹 브라우저를 통해 편리하게 제품을 사용할 수 있으며 다양한 개발 환경과의 연동으로 기존 개발 환경에서도 사용이 가능합니다.

서비스 유연성

고객의 애플리케이션 개발 환경에 맞추어 선택할 수 있도록 온프레미스 및 클라우드 서비스 모두를 지원합니다.

Sparrow SAST/SAQT



소스코드에 존재하는 보안 취약점이나 품질 결함을 정확하고 빠르게 검출하는 정적 분석 도구

Benefit

- 개발 단계에서부터 보안 취약점 및 결함을 발견하여 수정 비용 절감
- 시큐어코딩을 통한 국내외 최신 컴플라이언스에 빠른 대응 가능
- 보안 취약점 선제 대응으로 제품의 시장 경쟁력 강화

강력한 소스코드 분석

- 연관 파일 분석, 함수 호출 관계 분석, 코드 의미 분석 등 다양한 분석 기법 적용
- 취약점이나 품질 결함을 분석하는 2,300개 이상의 체커 제공
- 재분석 시 변경된 소스코드만 분석하여 분석 시간 최소화

편리하고 빠른 취약점 수정

- 취약점 발생 지점, 원인 및 호출 관계를 소스코드 라인 별로 제공
- 실제 소스코드 기반의 수정 예시 제공
- 오탐이 존재할 경우 해당 취약점에 대한 예외 처리 가능

폭넓은 지원 및 다양한 플러그인 연동

- C/C++, Java, Python 등 22개의 언어와 주요 프레임워크 지원
- 행정안전부 보안가이드, 전자금융감독규정, OWASP 등 국내외 주요 컴플라이언스 지원
- 다양한 개발 환경과의 연동 지원으로 기존 개발 환경에서 분석 가능

효율적인 분석 결과 관리

- 사용자 편의성을 고려하여 구성된 직관적인 대시보드
- 취약점의 위험도를 5단계로 구분하여 위험도 순으로 해결 가능
- 분석 결과 공유를 위한 사용자 맞춤형 보고서 지원



Sparrow SCA



오픈소스 소프트웨어의 라이선스를 식별하고 보안 취약점을 진단하는 오픈소스 관리 도구

Benefit

- SBOM(소프트웨어 자재명세서)을 통해 효율적인 소프트웨어 공급망 관리 가능
- 라이선스 관리를 통해 발생할 수 있는 법적 분쟁 방지
- 오픈소스에 존재하는 보안 취약점을 검출하여 보안 문제에 빠른 대처 가능



다양한 오픈소스 탐지 방식

- 소스코드, 압축파일, 바이너리 등 다양한 형태의 소프트웨어 분석 지원
- 의존성 파일 분석과 코드 스니펫 분석 지원

보안 취약점 진단

- 취약점 정보와 취약점이 발견된 컴포넌트 정보 제공
- 취약점의 위험성을 나타내는 CVSS 점수 제공으로 심각성 확인 가능

오픈소스 소프트웨어 라이선스 식별

- 사용 중인 오픈소스 소프트웨어 및 라이선스 자동 식별
- 국제 표준인 SPDX 및 CycloneDX, SWID의 형식을 사용해 상세한 소프트웨어 구성 컴포넌트 정보를 포함한 SBOM 생성
- 라이선스 현황을 한눈에 확인할 수 있는 라이선스 정보 차트 제공

빠른 결과 공유 및 연동 지원

- 웹 기반 UI로 빠른 분석 및 결과 공유 가능
- 분석 수행과 진단 결과 확인을 위한 API 제공

Sparrow IHUB



애플리케이션 구현, 테스트, 운영 단계에서 보안을 적용할 수 있도록 도와주는 DevSecOps 관리 도구

맞춤형 DevSecOps 프로세스 정의

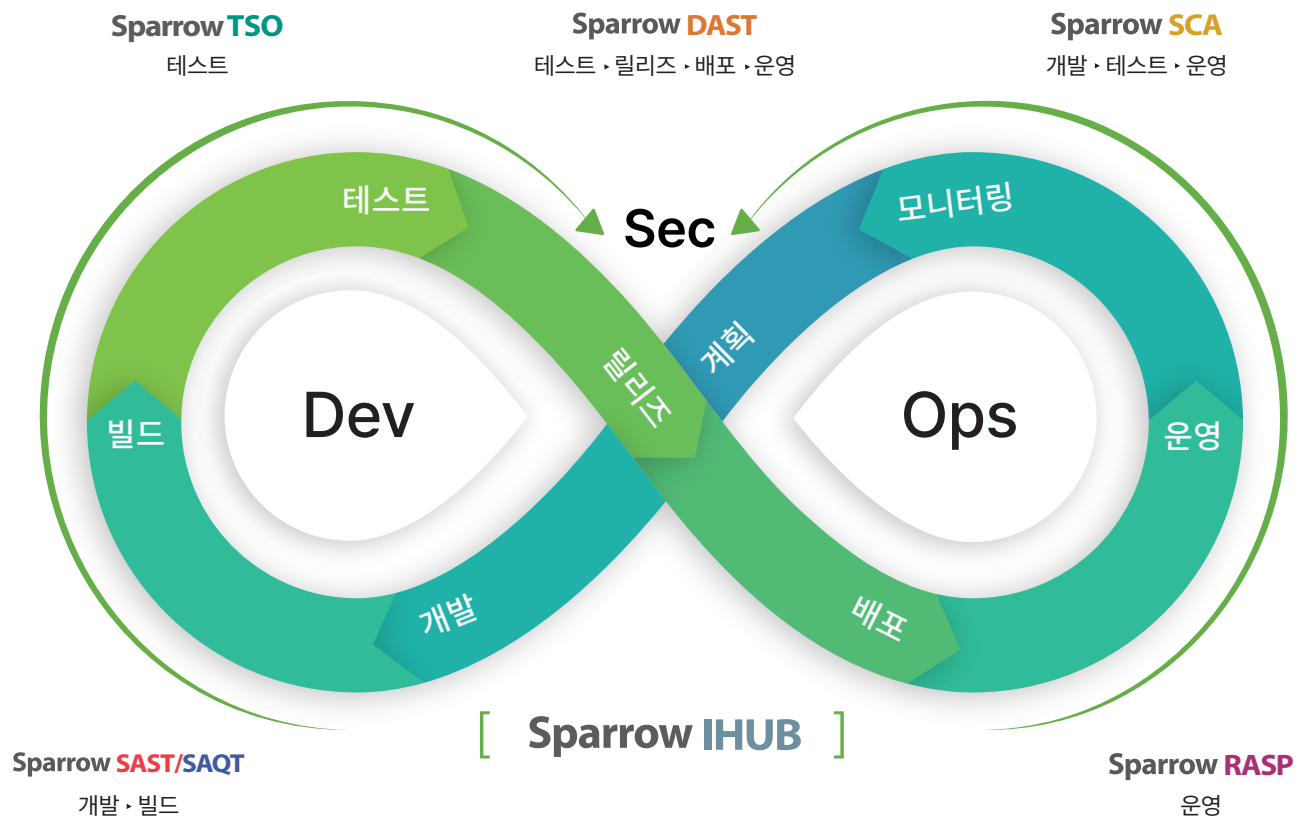
- 개발 환경에 알맞은 DevSecOps 작업 흐름 및 단계별 활동 내용 수립 가능

DevSecOps 활동 모니터링

- 진행 중인 작업 상태와 취약점 현황 모니터링 가능

유연한 도구 연동

- REST API 및 CLI를 통한 각종 도구 실행 및 결과값 가져오기 지원



Sparrow TSO



소프트웨어의 변경으로 영향을 받는 테스트 케이스를 찾는 테스트 스위트 최적화 도구

소스코드-애플리케이션 연관 분석

- 변경된 소스코드로 영향을 받는 테스트 케이스 및 애플리케이션 기능 파악

최소한의 테스트 케이스 선별

- 소스코드 변경에 따라 수행해야 하는 최소한의 테스트 케이스 선별로 테스트 시간 단축

테스트 도구와의 연동 (지원 예정)

- 운영 중인 테스트 자동화 프레임워크와의 연동 지원

Sparrow DAST



웹 애플리케이션에 존재하는 보안 취약점을 검출하는 동적 분석 도구

Benefit

- 웹 애플리케이션 실행 과정에서 발생할 수 있는 공격에 대비
- 정적 분석으로 발견되지 않은 보안 취약점을 테스트 단계에서 검출 가능
- 행정안전부 보안가이드, OWASP 등 국내외 주요 컴플라이언스 대응



강력한 분석 능력

- 기본적인 HTTP 메시지 분석에서 Ajax 분석까지 지원
- 분석하는 동안 공격받는 웹 애플리케이션의 내부 동작 확인 가능
- 취약점을 분석하는 1,400개 이상의 테스트 규칙 제공

보안 취약점 자동 검출

- 웹 애플리케이션의 URL로부터 포함된 하위 경로를 자동 수집
- SQL 삽입, XSS 등 수집된 경로에 존재하는 보안 취약점 검출
- 발견된 취약점에 대한 설명과 해결 방법 제시

편리한 취약점 관리

- 수행한 이벤트를 기록하고 재현하여 취약점 검출 과정 가시화
- 특정 취약점만 재분석하여 취약점이 해결되었는지 빠르게 확인 가능
- 취약점의 위험도를 5단계로 구분하여 위험도 순으로 해결 가능

높은 사용 편의성

- 웹 페이지에서 수행 가능한 이벤트 순서를 녹화하고 분석 시 활용
- 별도 설치 없이 웹 브라우저를 통해 손쉽게 분석 가능
- 취약점별 분석 결과 및 해결 방법을 제공하는 상세 보고서 지원

Sparrow RASP



운영 중인 웹 애플리케이션에 대한 공격을 실시간으로 탐지하고 차단하는 자가 방어 도구

Benefit

- 개발 및 테스트 단계에서 대응하지 못한 취약점 방어 가능
- 웹 애플리케이션 실행 중에 발생하는 실시간 공격 대응
 - 레거시 시스템 보호로 추가적인 개발 비용 절감



실시간 공격 모니터링 및 차단

- 모든 외부 요청을 모니터링하여 실시간으로 보안 위협을 방어

자가 방어 규칙 관리

- 스스로 공격을 탐지하고 차단하는
자가 방어 규칙을 웹 애플리케이션마다 적용 가능

취약점 검출 및 관리

- 주요 보안 취약점 검출 기준으로 공격 탐지 및
검출된 취약점 이력 관리

▶ 바로가기 QR code 카메라 앱 > QR코드 스캔



Homepage



Web brochure

주소 : 서울특별시 마포구 월드컵북로 396 17층 (상암동, 누리꿈스퀘어)

전화번호 : 02-300-9100 팩스 : 02-300-9200

이메일 : 제품 관련 문의 sales@sparrowfasoo.com, 기술지원 문의 cs@sparrowfasoo.com

홈페이지 : <https://www.sparrowfasoo.com>