SW 생애주기별 취약점 사전 식별 및 공급망 통합 대응 모델 구축

Sparrow Enterprise

개요

S사는 **도로 및 철도 교통의 정보 시스템 구축 및 유지보수를 주력으로 하며 국내 교통 인프라 혁신을 선도하고 있는 기업**입니다. 국가 기반 시설과 직결된 교통 관제, 요금 징수, 차량 제어 시스템을 운영하는 만큼, 시스템의 무결성과 가용성 확보는 타협할 수 없는 필수 과제입니다. 최근 미국 교통 안전 센터를 비롯한 글로벌 시장에서 소프트웨어 공급망 보안 및 SBOM 제출 의무화가 강력히 요구됨에 따라, S사는 글로벌 표준에 부합하는 통합 보안 관리 체계 고도화에 착수했습니다.

목표

단일 보안 도구의 도입이 아닌, 공급망 전반에 대한 통합 관리 체계 구축

- **통합 취약점 분석 자동화**: SAST, SCA, DAST를 아우르는 다각도 분석 체계 구축
- **3rd Party SW 검증 강화**: 외부 도입 SW에 대한 SBOM 기반 교차 검증 및 가시성 확보
- **Shift-Left 보안 내재화**: 개발 초기 단계부터 취약점을 조기 식별하는 DevSecOps 구현
- **글로벌 컴플라이언스 대응**: 글로벌 규제 요구에 대응 가능한 SBOM 관리 환경 구축
- **위험 모델링 기반 거버넌스**: 위협 모델링 프레임워크와 연동된 체계적인 대응 프로세스 수립

기존 문제

파편화된 보안 점검에서 벗어나 전방위 통제 체계 필요성 대두

기존의 보안 점검은 개발 모든 단계에서 고려되지 않은 채 분리되어 비효율적으로 운영되었으며, 공급망 전체를 관통하는 통합적인 위험 관리에 한계가 있었습니다.

보안 사각지대 존재	분석 도구의 파편화
내부 개발 코드 위주의 점검으로 인해 외부에서 유입되는 3rd Party SW에 대한 검증 프로세스 부재	SAST(정적), SCA(오픈소스), DAST(동적) 분석이 유기적으로 연동되지 못해 통합적인 리스크 파악 지연
글로벌 규제 대응 한계	**사후 대응의 고비용 구조**
미국 등 해외 프로젝트 수행 시 요구되는 정교한 SBOM 생성 및 이력 관리 체계 미비	운영 단계에서 발견되는 취약점으로 인한 조치 비용 및 시스템 다운 타임 리스크 상존

이에 S사는 단순 도구 도입에서 벗어나, 내부 개발과 외부 공급이라는 두 갈래의 공급망을 통합 관리할 수 있는 End-to-End 보안 파이프라인 구축을 결정했습니다.

해결 방안

공급망 전반을 아우르는 통합 보안 파이프라인 구현

스패로우의 애플리케이션 보안 테스팅 통합 솔루션(Sparrow Enterprise)을 기반으로 개발 환경부터 운영, 그리고 외부 공급망까지 통제하는 입체적인 보안 모델을 구현했습니다.

✓ 개발 · 빌드 단계의 Full-Stack 자동 분석

개발자가 GitLab에 코드를 푸쉬한 이후, Jenkins CI/CD를 통한 빌드 요청 시 파이프라인을 통해 1)Sparrow SCA를 통한 오픈소스 취약점 및 라이선스 분석, 2)Sparrow SAST를 통한 소스코드 정적 분석, 3)Sparrow DAST를 통한 런타임 환경에서의 웹 애플리케이션 취약점 동적 진단이 자동으로 수행됩니다. 이를 통해 SW 릴리즈 전, 보안 결함을 점검하여 배포 이전 단계에서 보안을 완료하는 구조를 확립했습니다.

✓ 3rd Party SW에 대한 SBOM 기반 교차 검증

가장 차별화된 부분으로, 외부 솔루션 공급사로부터 받은 SW에 대한 철저한 검증 프로세스를 추가했습니다. 3rd Party SW의 SBOM을 제공받아 시스템에 업로드 하고, SBOM 상의 정보와 실제 분석 결과 간의 교차 검증을 통해 숨겨진 취약점이나 허위 기재된 라이선스를 식별하여 외부 공급망 리스크를 원천 차단했습니다.

✓ SBOM DB 기반의 중앙 집중형 자산 관리

모든 분석 결과(내부+외부)는 중앙 SBOM DB로 통합됩니다. 소프트웨어 버전별 이력 관리 및 변경 사항 추적을 통해 글로벌 규제 기관이 요구하는 투명성을 확보했으며, 위협 모델링 프레임워크와 연계하여 식별된 취약점에 대한 체계적인 우선순위 대응이 가능해졌습니다.

성과

글로벌 시장 확장을 위한 DevSecOps 수립

글로벌 컴플라이언스 대응	공급망 가시성(Visibility) 획기적 개선
미국 교통 안전 센터의 SBOM 제출 요구사항을 완벽히 충족하며 글로벌 사업 경쟁력 강화	내부 개발 코드 뿐만 아니라 외부 도입 SW까지 포함한 전체 SW 자산에 대한 보안 지도 완성
취약점 사전 식별을 통한 비용 절감	**통합 보안 거버넌스 체계 정립**
운영 단계의 보안 사고를 예방하고 수동 점검 대비 취약점 조치 속도 대폭 향상	위협 모델링부터 동적 분석까지 연결되는 고도화된 보안 운영 모델 확보

결론

공급망 전반을 통합 관리하는 보안 거버넌스 체계로의 전환

이번 프로젝트는 단순한 취약점 분석 도구의 도입 사례가 아닙니다. 국가 인프라 시스템이 갖춰야 할 '보안 거버넌스'의 표본을 보여줍니다. 내부와 외부를 가리지 않는 철저한 SBOM 기반 검증 체계는 글로벌 시장 진출을 위한 강력한 무기가 되었으며, 이는 기술 경쟁력을 넘어 신뢰라는 무형의 가치를 창출하는 핵심 자산이 되었습니다.