DevSecOps 파이프라인 연동형 SBOM 자동 관리 체계 구축

Sparrow SAST | Sparrow SCA

개요

I사는 **국내 대표 데이터 솔루션 및 오픈소스 DB 전문 기업**으로 금융권 핵심 시스템을 대상으로 고가용성 DB 환경을 구축 및 운영하고 있습니다. 데이터의 생성부터 저장, 관리, 활용까지 전 주기를 아우르는 솔루션 라인업을 보유한 만큼, 금융 산업의 엄격한 안정성·보안성·규제 대응 역량이 기업 경쟁력인 환경에서 높은 신뢰를 확보하고 있습니다. 최근 금융권의 소프트웨어 공급망 보안 가이드라인이 강화됨에 따라, 오픈소스 라이선스 식별과 SBOM(Software Bill of Materials) 제출 체계를 실무 프로세스에 내재화 하는 고도화가 주요 과제로 부상했습니다.

목표

단순한 SCA 도입이 아닌 개발 전 단계에 걸친 자동화 파이프라인 구현

- **DevSecOps 거버넌스 확립:** CI/CD 파이프라인에 보안 정책 자동 적용
- **보안 게이트 구현:** CVSS 기반 보안 기준 미달 시 빌드 자동 차단
- **SBOM 라이프사이클 자동화:** 분석 결과 기반 SBOM 자동 생성 및 중앙 관리
- **규제 대응력 강화:** 금융권 요구 규격에 부합하는 SBOM 리포팅 체계 확보
- **End-to-End 추적성 확보:** 취약점 탐지부터 조치 완료까지 이력 관리 자동화

기존 문제

'사후 점검'에서 '선제적 방어'로 패러다임 전환

기존에는 개발 단계에서 보안이 고려되지 않은 채 오픈소스 라이선스 관리와 보안 점검이 개발 완료 후 배포 직전에 이루어지는 체크리스트 형태의 수동 점검에 의존하고 있었습니다.

- 오픈소스 라이선스 및 취약점 점검 수작업 수행으로 이슈 누락 위험 존재
- 분석 결과와 SBOM 산출물 간의 정합성 확보 어려움 및 문서화 작업의 비효율성
- 취약점 발견 시 수동 이슈 등록 및 개별 추적으로 인한 수정 조치 지연
- 빌드 완료 후에 보안 검증으로 보안 결함이 포함된 SW가 배포될 가능성 상존

특히 금융권 고객사의 SBOM 제출 요구가 권고에서 필수로 전환됨에 따라, 보안을 개발의 부가적인 단계가 아닌 빌드 승인을 위한 필수 조건으로 전환하는 DevSecOps 체계 구축이 시급했습니다.

해결 방안

보안 승인 기반 DevSecOps 구현

스패로우의 보안 취약점 분석 솔루션(Sparrow SAST, Sparrow SCA)을 개발 환경에 유기적으로 결합하여, 취약점 분석을 자동화하고 개발-빌드-배포 전 과정에 보안 게이트를 시스템적으로 구현했습니다.

✔ 개발 단계에서 소스코드 보안 취약점 선제적 대응

개발 초기 단계에서 Sparrow SAST를 통해 소스코드 내 보안 약점을 정밀 분석합니다. 이를 통해 잠재적 위협을 조기에 제거하고, 소스코드 품질과 보안성을 상향 평준화 했습니다.

✔ 빌드 단계에서 CVSS 기준 보안 게이트 구현

Jenkins CI/CD 파이프라인에서 Sparrow SCA를 통해 오픈소스 분석을 자동으로 수행하고, CVSS 기준 보안 평가 점수 기준을 충족하는 경우 빌드가 수행되며 기준을 초과하는 취약점이 존재할 경우 빌드가 중단되도록 구현했습니다. 이를 통해 보안 검증이 완료된 산출물만 배포 단계로 진입하도록 통제합니다.

✔ SBOM 자동 생성 및 정합성 보장

소프트웨어 패키지 빌드에 대해 최신 점검 결과를 바탕으로 SBOM을 자동 생성합니다. 생성된 문서는 중앙 관리 솔루션에 자동 업로드되며, 배포 패키지와 SBOM 간의 1:1 정합성을 보장하여 문서 위변조 및 관리 누락 문제를 원천 차단했습니다.

✔ Redmine 연동을 통해 이슈 추적 자동화

취약점이 발견될 경우, Redmine에 자동으로 이슈가 등록되며 수정 후 재빌드 시 조치 상태가 시스템에 실시간으로 업데이트 됩니다. 또한 소프트웨어 버전별 취약점 이력 관리를 통해 차후 금융권 감사 및 규제 대응을 위한 객관적인 근거 자료를 확보했습니다.

성과

공급망 보안 자동화 및 신뢰성 극대화

- **보안 내재화 완성:** 보안 분석이 개발 워크플로우의 일부로 통합되어 수동 점검 대비 리소스 절감
- **SBOM 신뢰성 확보:** SBOM 자동 생성 프로세스를 통해 배포 산출물과 SBOM 간의 정합성 불일치 리스크 제거
- **금융권 규제 선제적 대응:** 금융권의 강화된 공급망 보안 가이드라인에 즉시 대응 가능한 표준 모델 확립
- **취약점 이력 관리 효율화:** 보안 이슈 자동 추적 및 이력 관리를 통해 소프트웨어 릴리즈 전 과정의 투명성 확보

결론

SBOM을 단순 문서가 아닌 '운영 프로세스'로 정의

이번 프로젝트의 핵심은 단순히 SBOM을 생성하는 체계를 구축한 것이 아닌, DevSecOps 파이프라인에 보안 정책을 통합하고 보안 승인 기반 배포 통제 모델을 구현했다는 점에 있습니다. 금융권을 비롯한 규제 산업군에서 SBOM 제출 요구가 확대되는 가운데 해당 기업은 보안을 개발 흐름 안에 통합함으로써 기술 경쟁력과 보안 신뢰성을 확보하게 되었습니다.