DevSecOps 기반 SBOM 무결성 검증 및 디지털 서명 체계 구축

Sparrow Enterprise | Sparrow SecureHub

개요

H사는 **국내 망연계 보안 시장의 높은 점유율을 보유한 기업**으로 망분리 환경에서 안전한 데이터 전송을 가능하게 하는 솔루션을 제공합니다. 특히 보안이 최우선인 폐쇄망 및 망분리 환경에서의 안전한 데이터 전송 기술을 보유하고 있으며 연구 중심의 자체 개발 역량을 기반으로 제품의 신뢰성과 안정성을 지속적으로 고도화하고 있습니다.

최근 공급망 보안에 대한 고객사의 요구가 고도화됨에 따라, 개발 단계의 상시 보안 검증부터 배포 단계의 디지털 서명된 SBOM 제공까지 아우르는 '신뢰 기반 DevSecOps' 체계를 구축했습니다.

목표

Jenkins CI/CD 파이프라인 기반의 자동 보안 검증 프로세스 구현

- **품질 게이트 구축:** 개발자 수정 및 팀장 승인이 연계된 상시 보안 분석 체계 확립
- **지속적 검증:** Jenkins CI/CD 파이프라인 기반의 자동 보안 검증 프로세스 구현
- **End-to-End 무결성 보장:** 배포 단계에서 디지털 서명된 SBOM 생성 및 암호화를 통한 위변조 방지
- **정합성 기반 리포팅:** 취약점 분석 결과와 SBOM 간의 일치성 확보
- **전체 공급망 네트워크 가시화:** 내부 개발 SW와 외부 도입 SW를 통합하는 SBOM 거버넌스 구축

기존 문제

SBOM의 '신뢰성' 문제와 증명의 한계

망연계 보안 솔루션의 특성상 고객사는 공급받는 SW의 구성 요소에 대해 매우 엄격한 검증을 요구합니다. 그러나 기존 체계에서는 다음과 같은 한계가 있었습니다.

검증의 단절	무결성 증명 한계
개발 단계의 취약점 분석과 최종 SBOM 산출물 간의 유기적 연동 부족	고객사에 전달되는 SBOM 문서가 실제 배포된 바이너리와 동일함을 기술적으로 입증할 장치 미흡
승인 절차의 수동화	**공급망 사각지대**
보안 결함 수정 여부에 대한 관리적 승인 프로세스가 시스템화 되지 않아 인적 오류 가능성 상존	내부 코드 외에 도입되는 3rd Party 구성 요소에 대한 체계적인 검증 데이터 부족

이에 H사는 단순한 SBOM 생성을 넘어 검증된 SBOM에 대한 요구가 강했으며, 이를 기술적으로 증명할 수 있는 고도화된 모델이 필요했습니다.

해결 방안

보안 검증과 SBOM 증명의 일원화

기존 개발 환경에 스패로우의 보안 취약점 분석 도구(Sparrow Enterprise, Sparrow SecureHub)를 밀도 있게 배치해 통합 보안 분석 체계를 마련하고, SBOM 생성 및 배포 단계까지 자동화했습니다.

✓ 승인 기반의 상시 취약점 대응

단순 분석에 그치지 않고 '선 조치 후 승인' 체계를 확립했습니다. 개발자는 Sparrow SAST, Sparrow SCA를 통해 수시로 코드를 점검하고, 발견된 취약점을 즉시 수정해야 합니다. 수정 완료 후 개발 팀장/QA의 승인을 거쳐야만 형상 관리 서버(Gerrit)에서 Jenkins CI/CD 파이프라인으로 진입할 수 있도록 설계하여 보안 책임을 강화했습니다.

✓ CI/CD 파이프라인 연계 통합 보안 검증

Jenkins CI/CD 파이프라인 환경에서 스패로우의 보안 취약점 분석 도구가 자동 실행됩니다.

1) **Sparrow SAST, Sparrow SCA:** 소스코드 및 오픈소스 취약점과 라이선스 규정 준수 여부 진단
2) **Sparrow DAST:** 런타임 환경의 웹 취약점 동적 분석 수행
3) **Binary Analysis:** 클라이언트 빌드 단계에서의 바이너리 분석을 통한 최종 구성 요소 재검증

✓ 디지털 서명 및 암호화된 SBOM 배포

배포 서버(Web) 단계에서 SBOM의 신뢰성을 확정 짓는 핵심 기술을 적용했습니다. 분석된 데이터를 기반으로 자동 생성된 SBOM에 디지털 서명(Digital Signature)을 부여하고 동형 암호화 기술 등을 활용해 보호합니다. 고객사는 전달 받은 SBOM의 서명을 확인하여 위변조 여부를 즉시 검증할 수 있으며, 이는 곧 제품의 무결성을 증명하는 보증서 역할을 합니다.

성과

보안 제조사의 품격을 높이는 '무결성 거버넌스'

SBOM 신뢰도 극대화	보안 선순환 구조 확립
디지털 서명 기술 적용으로 SBOM 무결성에 대한 대외적 공신력 확보	개발-수정-승인-빌드로 이어지는 프로세스 정착으로 취약점 잔존 가능성 최소화
컴플라이언스 대응 속도 향상	**공급망 통제 범위 확장**
고객사의 SBOM 제출 요구에 즉각 대응하며, 검증된 취약점 리포트를 함께 제공하여 고객 만족도 제고	3rd Party SW까지 포함한 통합 관리로 외부 유입 보안 리스크 전면 통제

결론

SBOM, 고객 신뢰를 증명하는 보안 자산으로 전환

이번 프로젝트는 공급망 보안이 단순한 규제 대응을 넘어, 어떻게 기업의 기술적 신뢰 자산으로 변모할 수 있는지를 보여줍니다. H사는 보안 소프트웨어 전문 기업으로서 규제 가이드라인을 충족하기 위해 DevSecOps 환경을 선제적으로 구축한 선도 사례이며, 개발 단계의 엄격한 품질 통제와 배포 단계의 디지털 증명 체계는 기술적 신뢰성과 브랜드 경쟁력을 동시에 강화하는 기업의 핵심 동력이 되었습니다.