소프트웨어 공급망 전반의 보안 신뢰를 향상시키는 전략

비즈니스 화이트 페이퍼

주식회사 스패로우

SPARROW

CONTENTS

소프트웨어 공급망 전반의 보안 신뢰를 향상시키는 전략

개발 과정에서 사용된 오픈소스 라이브러리나 외부 패키지에 취약점이나 악성 코드가 포함되어 있는 경우 최종 제품에도 동일한 문제가 발생하거나 보안 위협에 노출될 수 있습니다. 오픈소스 소프트웨어에 대한 의존도가 높아짐에 따라 최근 이러한 취약점을 노린 해킹 사고와 함께 공급망 보안에 대한 필요성이 강조되고 있습니다.

하지만 소프트웨어 공급망 보안에 대한 통일된 기준은 아직 정립되지 않은 상태입니다. 여기에는 다양한 원인이 있습니다. 우선 공급망 보안을 확인하기 위해 사용되는 가장 기본적인 자료인 SBOM 포맷의 표준이 SPDX, CycloneDX 등으로 나눠져 있고 제공하는 정보의 종류가 일치하지 않습니다. SBOM으로 소프트웨어 구성 요소를 확인하더라도 오픈소스, 상용 소프트웨어, 클라우드 등 다양한 형태의 프로그램이 혼재되어 있기에 처리 기준이 다를 수밖에 없습니다.

이렇게 공급망 구조가 복잡해짐으로써 소프트웨어의 구성 요소를 확인하는 과정도 어려워졌습니다. 공급 단계에 따라 구성 요소가 끊임없이 변경되는 것은 물론이고 소프트웨어 공급자도 더 이상 단일 주체가 아니게 되었습니다. 소프트웨어 공급망을 관리하기 위해서는 공급망의 흐름에 따라 소프트웨어 구성 요소의 변화를 추적하고 공급망 참여자를 구분해야 합니다. 공급망 단계에 추가적으로 소프트웨어의 종속성 및 서드파티를 고려한다면 소프트웨어 공급망은 더 세분화됩니다.

공급망 보안의 복잡성을 해소하는 가장 효과적인 방법은 SBOM(Software Bill of Materials)을 활용한 검증입니다. SBOM을 통해 소프트웨어 공급망을 통해 보안 위협이 전파되거나 미확인 상태로 남는 위험을 사전에 방지할 수 있습니다. Sparrow SecureHub는 소프트웨어를 생산하는 과정에서 산출된 SBOM을 하나의 플랫폼으로 관리함으로써 공급망 전반의 가시성과 추적 가능성을 크게 향상시킵니다.

상호 신뢰를 위한 SBOM 공유 플랫폼

Sparrow SecureHub는 클라우드 기반 SBOM 등록·서명·공유 플랫폼으로, SBOM을 통해 소프트웨어 공급망 전반의 신뢰를 확보하기 위해 설계되었습니다. Sparrow SecureHub는 단순히 SBOM을 저장하는 도구가 아니라, 소프트웨어 구성 요소의 출처를 기록하고, SBOM의 무결성을 검증하며, 취약점과 같은 위험 정보를 관리함으로써 공급망 전체의 보안 신뢰 체인(Security Trust Chain)을 완성합니다.

투명한 공급망 관리

SBOM은 소프트웨어 구성 요소의 관계를 명확히 드러내는 데이터입니다. 다만 사람이 직접 읽기 위해서가 아니라, 보안 및 개발 도구에서 정보를 교환하기 위해 작성된 기술 명세서라고 볼 수 있습니다. 따라서 SBOM 파일을 직접 읽는 방식으로는 소프트웨어를 명확하게 파악하기가 어렵습니다. Sparrow SecureHub는 SBOM 파일을 파싱하고 데이터테이블 형식으로 표시함으로써 구조화된 데이터에 가시성(Visibility)을 부여합니다.

소프트웨어 최종 생산자 혹은 솔루션 제공자는 공급망 단계에 따라 시스템의 SBOM을 Sparrow SecureHub에 등록함으로써 SBOM을 중앙에서 통합 관리할 수 있습니다. 자사 제품에 어떤 오픈소스 라이브러리, 외부 모듈, 서드파티 컴포넌트가 포함되어 있는지를 명확히 파악할 수 있습니다. 이를 통해 무엇을 사용하는가를 모르는 위험을 제거할 수 있습니다. 또한, 특정 구성 요소가 언제 어느 단계에서 추가되었는지를 추적함으로써 소프트웨어의 변경 이력을 명확히 기록하고 책임 있는 공급망 체계를 마련할 수 있습니다.

SBOM 표준 지원

Sparrow SecureHub는 CycloneDX, SPDX, SWID Tag 등 국제 SBOM 표준 포맷을 완벽히 지원합니다. 따라서 개발사가 생성한 SBOM을 쉽게 가져올 수 있고, 외부 파트너나 고객 환경으로 전달해야 하는 경우에도 입력한 형식의 SBOM을 그대로 제공함으로써 표준화된 방식으로 데이터를 공유할 수 있습니다.

디지털 서명 및 무결성 보장

SBOM 파일은 텍스트 기반이라 내용을 수정할 수 있으므로 공유 과정에서 손상되거나 변조될 위험이 있습니다. 따라서 특정 파일을 공유할 때 검증된 파일임을 증명하기 위해 디지털 서명을 추가하게 됩니다. Sparrow SecureHub에서는 SBOM을 등록한 후에 서명을 추가할 수 있도록 계정 사용자의 이름으로 서명할 수 있는 기능을 지원합니다. 서명된 SBOM을 공유함으로써 해당 파일의 검증 여부를 명확하게 보증할 수 있습니다.

또한 Sparrow Enterprise와 Sparrow Cloud에서에서 분석한 결과의 SBOM을 Sparrow SecureHub로 보내는 경우 SBOM이 생성된 시점에 즉시 서명이 추가됩니다. 그러면 SBOM 생성 도구를 통해 만들어진 SBOM 원본을 수정하지 않은 상태이기 때문에 서명의 무결성을 더욱 신뢰할 수 있습니다.

취약점 정보 확인

Sparrow SecureHub는 등록된 SBOM에서 취약점 정보를 파싱하여 SBOM에 어떤 취약점이 포함되어 있는지를 표시합니다. 사용자는 SBOM에 작성된 취약점 ID, 취약점의 URL, 심각도 및 해당 취약점 정보의 DB를 확인하고 해당 정보를 통해 소프트웨어 공급망에 직접적으로 영향을 줄 수 있는 보안 위협에 대해 사전에 대응할 수 있습니다.

적용 사례 및 방법

Sparrow SecureHub를 활용하는 가장 좋은 방법은 Sparrow Enterprise 혹은 Sparrow Cloud를 통해 분석을 수행하는 것입니다. 일련의 제품을 통해 가장 효율적으로 오픈소스 컴포넌트 분석을 수행하고 SBOM을 공유할 수 있습니다. 다음과 같은 설정을 수행하세요.

1. a, b 중에서 하나의 방법을 선택 가능
   a. Sparrow Enterprise에서 Sparrow SecureHub 연동을 활성화하고 프로젝트에서 패키지를 분석
   b. Sparrow Cloud에서 Github 계정으로 로그인하고 프로젝트에 Github 브랜치를 분석
2. Sparrow Enterprise 혹은 Sparrow Cloud에서 Sparrow SecureHub로 SBOM 내보내기를 수행
3. Sparrow SecureHub의 시스템 목록에 동일한 이름의 시스템 및 SBOM 등록됨

베스트 시나리오

Sparrow Enterprise의 경우 소프트웨어 공급자가 개발 완료된 패키지를 분석합니다. 컴포넌트 분석이 완료되면 패키지에 포함된 소프트웨어 컴포넌트 및 컴포넌트에 포함된 라이선스와 알려진 취약점이 이슈 목록에 표시됩니다. 분석 결과를 확인하면서 SBOM 내보내기를 클릭하고 Sparrow SecureHub로 안전하게 내보내기를 선택합니다. 그러면 Sparrow Enterprise에서 분석한 SBOM이 Sparrow SecureHub에 등록됩니다.

Sparrow Cloud의 경우 소프트웨어 공급자가 개발 완료된 패키지를 Github에 올려둡니다. Sparrow Cloud에서 저장소를 분석하면 미리 설정된 해당 브랜치에서 분석이 수행됩니다. 오픈소스 분석이 완료되면 해당 패키지에 포함된 소프트웨어 컴포넌트 및 컴포넌트에 포함된 라이선스와 알려진 취약점이 이슈 목록에 표시됩니다. 분석 결과를 확인하면서 SBOM 내보내기를 클릭하고 SecureHub로 안전하게 내보내기를 선택합니다. 그러면 Sparrow Cloud에서 분석한 SBOM에 서명이 추가되어 Sparrow SecureHub에 등록됩니다.

이미 SBOM을 다른 도구로 생성한 경우에는 Sparrow SecureHub에서 직접 등록하기 버튼을 클릭하고 로컬에 있는 SBOM을 선택하여 업로드합니다. 그리고 등록한 SBOM의 정보를 확인한 다음, 서명하기를 클릭하여 업로드한 파일의 무결성을 증명해야 합니다. 서명하지 않은 SBOM 파일도 공유할 수 있지만, 이 경우 해당 파일은 공유한 사용자가 보증하는 SBOM이라는 것을 확인할 수 없습니다.

공급망 참여자나 최종 생산자에게 공유된 파일은 Sparrow SecureHub를 통해 파일의 출처가 명시되기 때문에 단일 파일로 공유하는 방법보다 신뢰할 수 있습니다. 플랫폼이 없는 경우, 파일이 실제 어떤 공급자로부터 왔고 어떤 버전과 어떤 구성 요소가 포함되어 있는지 확인하는 검증 과정에서 오류나 불확실성이 발생할 수 있습니다. 반면 Sparrow SecureHub를 사용하면 SBOM의 생성자, 서명 정보, 각 구성 요소의 해시 등 메타데이터가 SBOM과 함께 제공되므로, 별도의 작업 없이 파일의 출처와 무결성을 확인할 수 있습니다.

SBOM 공유를 통해 소프트웨어 공급자는 자신이 제공한 소프트웨어의 구성 요소가 안전하다는 것을 증명하고 소프트웨어 최종 생산자 혹은 솔루션 제공자는 공유받은 SBOM의 출처 및 무결성을 확인합니다.

SBOM 트러스트 체인의 허브

SBOM 표준 평가 지표

Sparrow SecureHub는 향후 SBOM 평가 지표를 추가하여 공유된 SBOM이 표준 형식에 부합하는지 자동으로 확인할 예정입니다. NTIA(National Telecommunications and Information Administration)에서 지정한 SBOM 최소 요소를 기준으로 SBOM의 구조와 메타데이터의 정확성을 검증함으로써 수신자는 SBOM이 신뢰할 수 있는 형식으로 작성되었는지를 수치로 확인할 수 있게 됩니다. 즉, SBOM 평가 지표를 통해 잘못된 SBOM이 소프트웨어 공급망에 전파되어 발생할 수 있는 혼란과 오류를 사전에 방지할 수 있습니다.

사용자 정책 기반 SBOM 검증

또한 SBOM 컴포넌트에서 위험한 컴포넌트 및 라이선스를 분석하고 사용자가 정의한 정책에 따라 SBOM 등록을 제한하는 기능을 추가할 것입니다. 사용자는 필요한 경우 금지된 컴포넌트 혹은 특정 라이선스를 포함하거나 지정된 CVSS(Common Vulnerability Scoring System) 점수를 초과하는 컴포넌트가 SBOM에 포함된 경우 해당 SBOM을 Sparrow SecureHub에 등록할 수 없도록 설정할 수 있게 됩니다.

소프트웨어 생태계를 연결하는 허브

이외에도 SBOM과 실제 소프트웨어 산출물 간의 일치성 검증 등 공급망 신뢰를 강화하기 위해서는 아직 핵심적인 문제가 남아있습니다. Sparrow SecureHub는 손쉽게 무결성과 출처를 확인할 수 있도록 검증 가능성(verifiability)을 보장하는 워크플로우를 수립해 나갈 것입니다. 소프트웨어 공급자와 수신자 간의 공급망을 안전하게 연결하고 Sparrow Enterprise와 Sparrow Cloud를 연결하는 트러스트 체인의 허브로써 더욱 발전할 계획입니다.