정 보 보 호 학 회 지
제 32 권 제5호, 2022. 10

소프트웨어 공급망 관리를 위한 글로벌 솔루션 동향

김 광 준*, 이 만 희**

요 약

2021년 5월 12일, 美 바이든 행정부는 소프트웨어 공급망 보안 강화를 위한 대통령 행정명령 14028을 발표하였다. 이후 연방정부에 납품하는 핵심 소프트웨어에 대해 SBOM(Software bill of materials) 제출이 의무화됨에 따라, 2021년 하반기부터 소프트웨어 공급망 관리를 위한 다양한 솔루션이 빠르게 개발되고 있다. 하지만 활발한 연구 및 산업화가 이루어지고 있는 글로벌 정세와 달리, 국내 산업은 상대적으로 더딘 실정이다. 이에 따라 본 논문에서는 소프트웨어 공급망 및 SBOM 관리를 제공하고 있는 글로벌 기업과 해당 솔루션에 대해 소개한다. 향후 국내 시장도 소프트웨어 공급망 보안 강화를 위해 SBOM 관리 의무화가 예상되는바 관련 솔루션의 개발 연구가 요구된다.

Ⅰ. 서 론

제품 또는 서비스를 공급자로부터 소비자에게 전달하는 과정에서의 인력, 정보, 조직, 자원 등에 대한 전반적인 시스템을 공급망이라고 한다[1]. 그중 소프트웨어의 설계, 개발, 배포, 유지보수의 전 과정에서 사용되는 부속 소프트웨어 및 관리 체계를 통칭하여 소프트웨어 공급망이라 한다. 기업들은 제품의 설계 및 공정 등 다양한 분야에서 요구사항에 맞는 하드웨어 및 소프트웨어를 공급하게 되는데, 이러한 공급 과정에서 발생하는 해킹, 침투, 변조, 악성코드 삽입 등과 같은 각종 보안 위협을 공급망 위협이라 한다.

최근 소프트웨어 공급망 공격이 급증함에 따라 2021년 5월 12일, 美 바이든 행정부는 소프트웨어 공급망 보안 강화를 위한 대통령 행정명령 14028을 발표하였으며, 그 결과 연방정부에 납품하는 핵심 소프트웨어에 대해 SBOM(Software bill of materials) 제출이 의무화되었다[2]. 이후 2021년 하반기부터 소프트웨어 공급망 관리를 위한 다양한 글로벌 솔루션이 빠르게 개발되고 있으나, 국내 산업은 상대적으로 더딘 실정이다.

따라서 본 논문에서는 소프트웨어 공급망 및 SBOM 관리를 제공하고 있는 글로벌 기업과 해당 솔루션에 대해 소개한다. 향후 국제 정세에 맞추어 국내 시장도 소프트웨어 공급망 보안 강화를 위해 SBOM 관리 의무화가 예상되는바 관련 솔루션의 개발 연구가 필요하다.

Ⅱ. 배경지식

2.1. SBOM

소프트웨어 개발의 전 단계에 걸쳐 사용되는 다양한 구성요소 및 외부 요소들을 기록하여 소프트웨어에 대한 공급망 정보를 제공하는 구조화된 명세서를 SBOM(Software Bill of Materials)라 한다[3]. 초기 국립 전기 통신 및 정보 관리청(NTIA, National Telecommunications and Information Administration)에 의하여 주로 의료 기기 제조업체 및 의료 제공 기관을 대상으로 SBOM을 적용하며 가능성을 시험 중에 있었지만, 소프트웨어 공급망 관리의 필요성이 부각되면서 현재 소프트웨어에 대한 신뢰를 보장하고 안전한 공급망 구축 및 운영을 위한 방안으로 주목받고 있다.

SBOM은 공급자 정보, 소프트웨어의 구성요소 정보, 버전, 해시값, 관계 및 SBOM 저자 정보 등을 포함한 3가지의 표준 형식이 존재한다. 첫 번째로 국제 표준 ISO/IEC 1977 기반의 SWID Tag(Software Identification)는 소프트웨어 식별 및 관리를 목적으로

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(2021R1A4A2001810).
* 한남대학교 컴퓨터공학과 (대학원생, kimkwangjun.kr@gmail.com)
** 한남대학교 컴퓨터공학과 (교수, manheelee@hnu.kr)

제작되었다. 두 번째로 리눅스 재단에서 개발한 SPDX(Software Package Data eXchange)는 소프트웨어 및 라이센스 관리를 주된 목적으로 한다. 마지막으로 OWASP 커뮤니티에서 개발한 CycloneDX는 소프트웨어의 보안 요구사항 및 위험 분석을 목적으로 개발하였다. 3가지의 SBOM 표준은 핵심 가치에 차이가 있지만, 소프트웨어 식별과 공급망을 관리한다는 공통 목적을 포함한다.

2.2. CI/CD

소프트웨어 개발 단계를 자동화하여 보다 빠르게 사용자에게 제공하기 위한 개념을 CI(Continuous Integration)/CD(Continuous Delivery, Continuous Deployment)라고 한다[4]. 소프트웨어 개발 생명주기 전 과정을 자동화하고 이 과정을 모니터링할 수 있으므로, 개발자는 개발에만 집중하면 된다는 장점이 있다.

CI는 개발자를 위한 자동화 프로세스로 지속적인 통합을 의미한다. 소프트웨어의 새로운 코드 변경 상황이 발생할 경우, 자동으로 빌드 및 테스트를 통해 리포지토리에 통합하여 사용자 및 코드 간의 상호 충돌을 예방할 수 있다.

CD는 지속적인 서비스 제공 또는 지속적인 배포를 의미한다. 두 의미 모두 파이프라인의 자동화를 의미한다. 먼저 지속적인 서비스 제공은 개발자들이 소프트웨어를 수정할 경우 버그 테스트를 거쳐 리포지토리에 자동으로 업로드되는 것을 의미한다. 운영팀은 이 리포지토리를 통해 소프트웨어를 실시간으로 프로덕션 환경으로 배포할 수 있게 된다. 지속적인 배포란 개발자의 변경 사항을 리포지토리에서 프로덕션 환경까지 자동으로 릴리즈하는 것을 의미한다. 이는 배포 프로세스를 자동화함으로써, 운영팀의 업무 과부하 문제를 해결할 수 있게 된다.

Ⅲ. 소프트웨어 공급망 관리 솔루션 동향

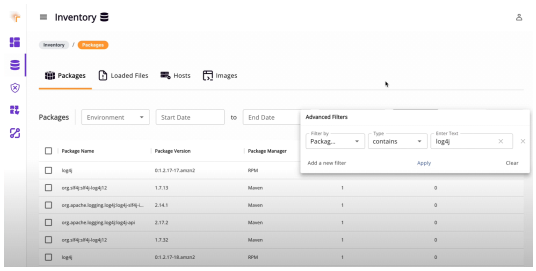
3.1. Dynamic SBOM Platform

Rezilion 社가 개발한 SBOM 관리 솔루션으로 애플리케이션, 라이브러리, 도커 컨테이너 등에 포함된 SBOM을 활용하여 동적으로 소프트웨어의 오픈소스 구성요소 및 취약한 구성요소를 관리한다[5]. 본 솔루션은 CI/CD 및 프로덕션 환경의 모든 소프트웨어 구성 요소에 대한 라이브 인벤토리를 생성하고 지속적으로 업데이트하며 SBOM을 관리한다. 그 후 SBOM을 통해 Log4j와 같이 알려진 취약점 및 악용 가능성을 즉시 검색할 수 있는 특징이 있다. 소프트웨어의 구성요소 및 오픈소스 간의 종속성을 파악하고, 그를 취약점 정보와 연계함으로써 일반적인 취약점 수동 분석에 비해 취약점 관리의 시간을 대폭 절약할 수 있는 강점을 보여준다.

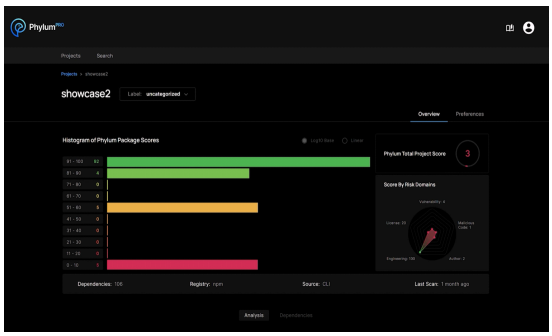
3.2. Phylum

Phylum 社가 개발한 소프트웨어 공급망 보안 솔루션으로 개발 및 CI/CD 환경에서 휴리스틱, 머신러닝을 이용하여 소프트웨어 패키지를 자동으로 식별하고 공급망 위험을 분석하여 5가지 영역으로 분류한다[6].

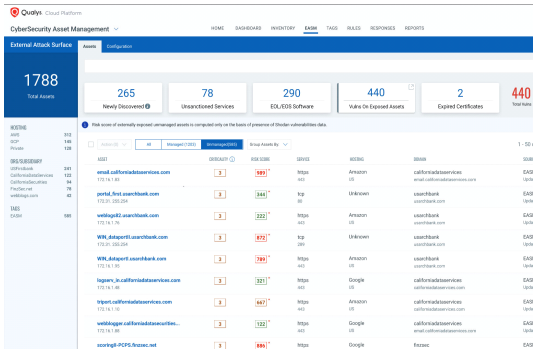
- 악성코드(멀웨어 및 백도어) 위험
- 소스코드 취약점 위험
- 라이센스 오용 위험
- 저자 평판 및 저작권 위험
- 엔지니어링 위험



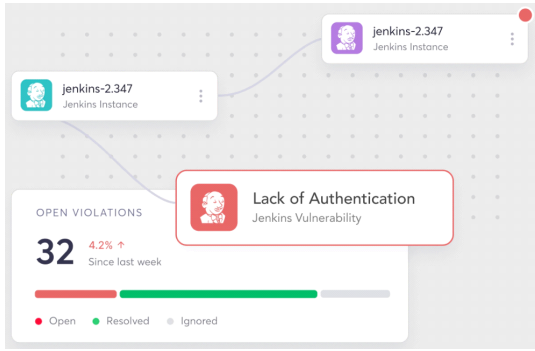
〔그림 1〕 Rezilion - Dynamic SBOM Platform: 등록된 소프트웨어 패키지 중 log4j 구성요소 검색



〔그림 2〕 Phylum: 등록된 프로젝트의 종합적인 위험 점수



〔그림 3〕 Qualys - Cyber Security Asset Management: 등록된 자산의 미확인 도메인 정보



〔그림 4〕 Cycode - NextGen SCA: CI/CD 파이프라인에서 발견된 취약점에 대한 종속성 표기 예시

그 후 각 영역에 대해 연역적 분석을 수행한 뒤, 조직에서 설정한 위험 허용 기준에 따라 식별된 위험의 우선순위를 지정하여 시각적으로 표시한다. 소프트웨어 구성요소의 전반적인 위험도를 사용자가 한눈에 볼 수 있도록 종합적인 점수를 제공한다는 장점이 있다.

3.3. Cyber Security Asset Management

Qualys 社가 개발한 IT 자산 관리 솔루션으로 사이버 보안 태세를 지속해서 측정, 분류, 검색할 수 있도록 고객의 내부 및 외부 IT 자산을 관리할 수 있는 클라우드형 서비스이다[7]. 본 솔루션은 애플리케이션 및 모든 엔드포인트 단말기, 클라우드, 컨테이너, IoT 단말기에서 실시간으로 데이터를 수집하고 가시화함으로써 고객에게 빠른 정보 제공을 목적으로 한다. 또한, 사이버 보안 위험을 관리하기 위해 발견된 자산과 관련 취약성을 바탕으로 고객 비즈니스에 미치는 영향력을 판단하여 위험 우선순위를 책정한다.

본 솔루션은 모든 제조업체 이름, 제품 이름, 모델, 소프트웨어 버전 등에 대한 데이터를 포함하며, 정확한 의사 결정을 위해 정규화된 데이터를 제공한다. 또한, 자산 관리뿐만 아니라 보유하고 있는 자산과 관련된 취약점과 악성 도메인 정보 등을 함께 제공하는 특징이 있다.

3.4. NextGen SCA

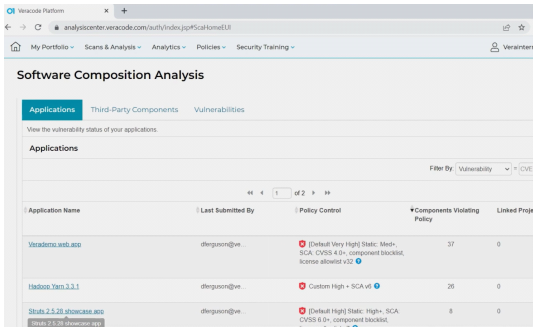
Cycode 社가 개발한 소프트웨어 구성요소의 종속성 관리 도구로 소프트웨어 개발 생명주기(SDLC, Software Development Life Cycle)의 파이프라인 구성 분석(PCA, Pipeline Composition Analysis)을 통해 포함된 구성요소와 종속성을 식별한다[8]. 개발 과정 중 하드 코딩된 비밀번호, 코드 누출, 잘못된 구성 등과 같은 소프트웨어의 보안 문제를 찾기 위한 검색 엔진을 구현하였으며, 소프트웨어 개발 생명 주기 전반에 걸쳐 코드의 무결성과 사용자 활동을 추적하여 이상 징후를 찾고 코드 변조를 방지함으로써 소프트웨어 공급망의 보안성을 향상시킨다.

또한, 빌드 파일 뿐만 아니라, Jenkins, GitHub 작업, IaC 템플릿 등에서의 종속성 식별을 지원하며, 빠른 시간 내의 취약점에 대한 종속성 스캔이 가능한 장점이 있다. 부가적으로 소프트웨어와 종속된 구성요소들의 라이센스 유형 및 제한된 라이센스 사용 여부를 식별하고 가시적으로 정보를 제공함으로써 라이센스 위반으로부터 소프트웨어를 보호한다.

3.5. Software Composition Analysis

Veracode 社가 개발한 소프트웨어 구성 분석 솔루션으로 소프트웨어 공급망을 보호하기 위해 구성요소를 분석한 후 라이브러리 내의 취약점을 자동으로 식별한다[9]. CI/CD 파이프라인 및 IDE 등 개발환경에서 즉시 스캔 가능함으로 소프트웨어 개발 생명 주기 초기에 코드의 오류와 취약점을 식별하고 수정할 수 있도록 개발자를 보조한다.

또한, 코드 오류를 분석하여 자동으로 풀 요청 생성 기능을 지원함으로써 더 높은 정확도와 빠른 수정 속도를 제공하는 등 개발자의 편의를 고려한 인터페이스가 이 솔루션의 장점이다. 더불어 다른 솔루션과 마찬가지로 오픈소스의 라이센스 준수 여부를 분석하는 라



〔그림 5〕 Veracode - Software Composition Analysis: 애플리케이션의 정책 검증 현황

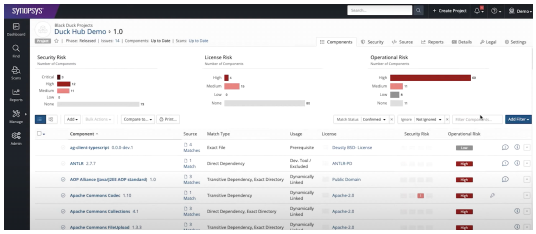
이센스 위험 관리를 함께 제공한다. 이 솔루션은 분석한 소프트웨어 구성요소를 바탕으로 CycloneDX 형식의 SBOM 생성을 지원한다.

3.6. Black Duck Software Composition Analysis

Synopsys 社가 개발한 소프트웨어 구성 분석 솔루션으로 애플리케이션 및 컨테이너에서 오픈소스 또는 타사 코드 사용으로 인해 발생하는 보안, 품질 및 라이센스 규정 준수 위험을 관리하는 기능을 제공한다[10]. 또한, 애플리케이션과 컨테이너를 구축하는 데 사용되는 오픈소스, 타사 및 독점 소프트웨어 구성요소를 분석하여 SPDX 및 CycloneDX 포맷의 SBOM 생성을 지원한다.

본 솔루션의 가장 큰 기능 4가지는 다음과 같다.

- 종속성 분석: Maven 및 Gradle과 같은 빌드 도구와 통합하여 Java 및 C#과 같은 언어로 빌드된 애플리케이션에서 선언된 오픈 소스 종속성과 전이적 오픈 소스 종속성을 식별 및 추적한다.
- 코드프린트 분석: 문자열, 파일 및 디렉터리 정보를 DB와 매핑하여 C 및 C++와 같은 언어를 사용하여 구축된 애플리케이션에서 오픈소스 및 타사 구성요소를 식별한다.
- 바이너리 분석: 컴파일된 애플리케이션 라이브러리 및 실행 파일 내에서 오픈소스를 식별한다.
- 스니펫 분석: 라이센스 위반 및 충돌 등 잠재적으로 위험할 수 있는 오픈소스 코드의 일부를 식별한다.



〔그림 6〕 Synopsys - Black Duck Software Composition Analysis: Demo 프로젝트의 구성요소 및 관련 정보 Overview

본 솔루션은 소프트웨어 개발 생명 주기 전반에 걸쳐 사용할 수 있으며, CI/CD와 통합하여 빌드 단계에서의 정책 위반을 자동 식별한다.

3.7. Anchore

Anchore 社가 SBOM 관리 솔루션으로 소프트웨어의 종속성을 포함한 모든 구성요소를 식별 및 관리한다[11]. 소스 코드 리포지토리 및 CI/CD 파이프라인, 컨테이너 레지스트리 및 런타임에 이르는 개발 프로세스의 각 단계에서 SBOM 생성을 지원하며, 패키지 및 파일, 구성요소 등의 심층 메타데이터를 활용하여 SBOM 정책 규칙을 생성한다. 이를 통해, 허용되지 않은 소프트웨어가 식별될 경우 개발자에게 알림을 제공한다.

또한, 소프트웨어 배포 후에도 가시성과 지속적인 소프트웨어 모니터링을 위해 생성한 SBOM을 중앙 저장소에 보관 및 검색 기능을 제공한다. 이를 통해 Log4j와 같은 신규 취약점의 빠른 식별 및 사고 대응이 가능하다는 장점이 있으며, 저장된 SBOM을 외부 고객 또는 내부 보안 팀과의 공유를 통해 신뢰 구축이 가능하다는 점이 이 솔루션의 강점이다.

〔그림 7〕 Anchore - Anchore Enterprise: 저장된 샘플 SBOM 정보 가시화

GRAMMATECH CODESentry

Bill of Materials

Component	Component Version	Path	Target	Number of CVEs
cwalk	1.0.0	COTS/cots - shallow/COTS-Software.zip/COTS-Software/PushDirect.dll	PushDirect.dll	0
dcmtk	3.6.5	COTS/cots - shallow/COTS-Software.zip/COTS-Software/CoreGraphics.dll	CoreGraphics.dll	0
easylzma	0.0.7	COTS/cots - shallow/COTS-Software.zip/COTS-Software/PushDirect.dll	PushDirect.dll	0
expat	2.0.1	COTS/cots - shallow/COTS-Software.zip/COTS-Software/program.exe	program.exe	10
freetype	2.8.1	COTS/cots - shallow/COTS-Software.zip/COTS-Software/CoreGraphics.dll	CoreGraphics.dll	0
imagemagick	6.9.7.4	COTS/cots - shallow/COTS-Software.zip/COTS-Software/program.exe	program.exe	71
libflac	1.3.2	COTS/cots - shallow/COTS-Software.zip/COTS-Software/CoreAudioToolbox.dll	CoreAudioToolbox.dll	0
libjpeg	6b2	COTS/cots - shallow/COTS-Software.zip/COTS-Software/CoreGraphics.dll	CoreGraphics.dll	2
libplist	2.1.0	COTS/cots - shallow/COTS-Software.zip/COTS-Software/CFNetwork.dll	CFNetwork.dll	0
libplist	2.1.0	COTS/cots - shallow/COTS-Software.zip/COTS-Software/CoreAudioToolbox.dll	CoreAudioToolbox.dll	0
libpng	1.2.56	COTS/cots - shallow/COTS-Software.zip/COTS-Software/CoreGraphics.dll	CoreGraphics.dll	7
libressl	3.2.0	COTS/cots - shallow/COTS-Software.zip/COTS-Software/program.exe	program.exe	0
libressl	3.2.0	COTS/cots - shallow/COTS-Software.zip/COTS-Software/Admin.dll	Admin.dll	0
libtiff	3.9.4	COTS/cots - shallow/COTS-Software.zip/COTS-Software/CoreGraphics.dll	CoreGraphics.dll	50
libxml	2.9.8	COTS/cots - shallow/COTS-Software.zip/COTS-Software/libtidy.dll	libtidy.dll	0
libxml	2.9.4	COTS/cots - shallow/COTS-Software.zip/COTS-Software/libxml2.dll	libxml2.dll	0
libxml	2.9.4	COTS/cots - shallow/COTS-Software.zip/COTS-Software/WebKit.dll	WebKit.dll	0
libxslt	1.1.28	COTS/cots - shallow/COTS-Software.zip/COTS-Software/libxslt.dll	libxslt.dll	8
lz4	1.9.2	COTS/cots - shallow/COTS-Software.zip/COTS-Software/PushDirect.dll	PushDirect.dll	0
mozjpeg	3.3.1	COTS/cots - shallow/COTS-Software.zip/COTS-Software/CoreGraphics.dll	CoreGraphics.dll	1
openblas	0.3.7	COTS/cots - shallow/COTS-Software.zip/COTS-Software/CoreVideo.dll	CoreVideo.dll	0
openblas	0.3.7	COTS/cots - shallow/COTS-Software.zip/COTS-Software/libtidy.dll	libtidy.dll	0
openblas	0.3.7	COTS/cots - shallow/COTS-Software.zip/COTS-Software/MediaAccessibility.dll	MediaAccessibility.dll	0
openblas	0.3.7	COTS/cots - shallow/COTS-Software.zip/COTS-Software/CoreGraphics.dll	CoreGraphics.dll	0
openblas	0.3.7	COTS/cots - shallow/COTS-Software.zip/COTS-Software/CoreText.dll	CoreText.dll	0

〔그림 8〕 GrammaTech - CodeSentry: 바이너리 분석을 통한 소프트웨어 구성요소 SBOM 예시

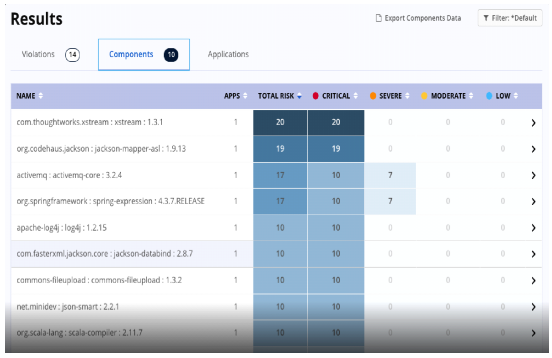
3.8. CodeSentry

GrammaTech 社가 개발한 바이너리 소프트웨어 구성 분석 도구는 바이너리 분석을 통하여 SBOM을 생성하고 종속성을 포함하여 탐지된 구성요소에서 알려진 취약점(NVD, National Vulnerabilities Database)을 식별한다[12]. 이를 위해 본 제품은 다양한 ISA(Instruction Set Architecture) 및 컴파일러에서 구성요소 식별을 위한 알고리즘을 개발하였다.

또한, 개발 환경의 CI/CD 파이프라인을 지원함으로 소프트웨어 수명 주기 전반에 걸쳐 발생할 수 있는 취약점을 지속적으로 추적하고 SBOM을 최신 상태로 유지할 수 있는 장점이 있다. 본 솔루션은 소스코드 없이도 오픈소스 및 상용 소프트웨어의 취약점을 탐지할 수 있다는 차별화된 특징이 있다.

3.9. Nexus Lifecycle

Sonatype 社가 개발한 오픈소스 보안 및 종속성 관리 제품으로 소프트웨어 수명 주기 전반에서 오픈 소스 취약점을 자동으로 식별 및 수정하는 기능을 제공



〔그림 9〕 Sonatype - Nexus Lifecycle: SBOM 정보를 통해 식별한 오픈소스 구성요소 예시

한다[13]. 대중적인 모든 파이프라인 및 개발도구를 통합 지원하므로 별도의 프로그램을 사용하지 않아도 되며, 취약점 발견과 같은 정책 위반 상황이 발생할 경우 구성요소에 대한 풀 요청을 자동으로 생성한다. 이때, 잘못된 구성요소나 취약점의 수정 방법을 자세히 명시해주어 개발자의 업무를 돕는 장점이 있다.

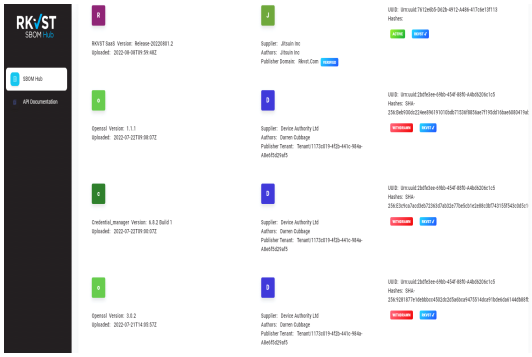
또한, 소프트웨어 수명 주기 전반에서 SBOM을 생성하여 종속성과 함께 모든 오픈소스의 구성요소를 식별한다. 부가적으로 오픈소스의 라이센스를 관리하고 이를 정책화할 수 있는 기능을 제공함으로써 라이센스 위반으로부터 소프트웨어를 보호한다.

3.10. RKVST

RKVST 社가 개발한 SBOM 관리 플랫폼으로 자산 정보를 지속적으로 증명하기 위해 블록체인 기반의 데이터 교환 및 보증기술을 사용한다[14]. 이를 위해 RKVST 社는 SBOM을 쉽게 저장 및 검색할 수 있도록 RKVST SBOM Hub를 무료로 제공한다. 현재 SBOM 생성 기능은 제공하지 않는다.

SBOM 배포 시 생성한 SBOM의 공개 여부에 따라 공공의 용도라면 RKVST SBOM Hub를 통해 SBOM을 배포하고, 사적인 용도라면 접근 정책을 정의한 후 선택한 사용자와 RKVST를 통해 SBOM을 공유한다. 사용자는 RKVST SBOM Hub의 웹 UI를 통해 모든 사용자가 게시한 SBOM 정보를 검색할 수 있으며, 미국 전기통신 및 정보청(NTIA, National Telecommunications and Information Administration)이 고시한 최소 권장 메타데이터 필드 검색을 지원한다.

앞서 언급한 솔루션과는 달리 개발 생명주기 및

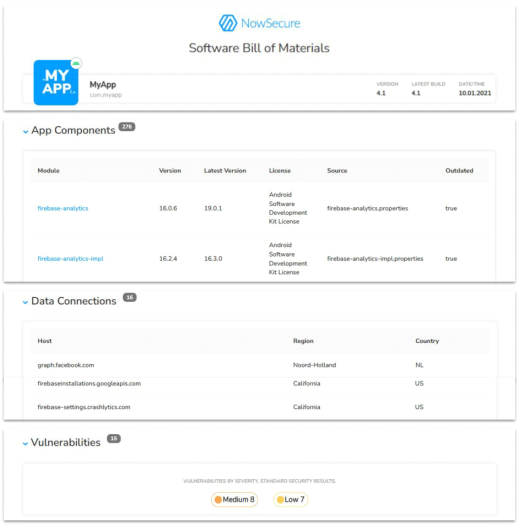


〔그림 10〕 RKVST - RKVST SBOM Hub: 등록된 SBOM 리스트

CI/CD 환경에서의 소프트웨어 구성요소 식별, 취약점 진단의 기능은 제공하지 않으나, SBOM의 유통과정을 지속적으로 증명하기 위해 블록체인 기술을 접목한 것은 차별화된 장점으로 해석된다.

3.11. NowSecure Platform SBOM

NowSecure 社가 개발한 모바일 SBOM 보안 솔루션으로 iOS(.ipa) 및 Android(.apk) 장치에서 실행되는 모바일 앱 바이너리를 정적/동적 분석하여 라이브러리, 프레임워크, API 정보, 네트워크 통신지 및 취약성 정보 등에 대한 정보를 생성한다[15]. 모바일 중심의 Agile 및 DevSecOps 프로그램을 위해 제작되었으며,



〔그림 11〕 NowSecure - NowSecure Platform SBOM: 샘플 App의 구성요소 SBOM 예시

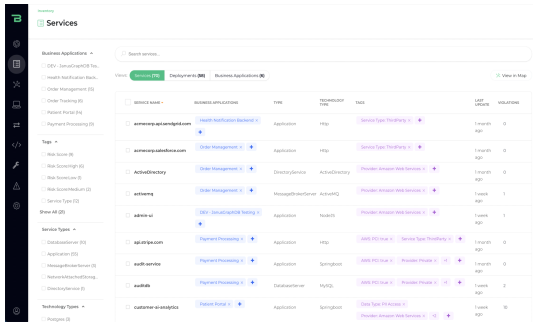
모바일 앱의 소프트웨어 개발 생명주기 내에 온디맨드 또는 Jenkins, Azure DevOps와 같은 CI/CD 파이프라인을 지원한다.

본 솔루션은 모바일 앱에 포함된 라이브러리 및 프레임워크를 식별하고, 사용되지 않는 불필요한 구성요소 식별을 지원한다. 또한, 내/외부 정책을 위반하는 구성요소 라이센스를 식별하여 라이센스 위반으로부터 소프트웨어를 보호한다. 그 외에도 승인되지 않은 API 정보와 네트워크 통신지에 대한 정보, 추가 테스트 및 분석이 필요한 코드 취약성 정보 등을 제공한다. 위 정보들은 PDF 보고서와 SBOM 포맷인 CycloneDX을 통해 제공된다. 세계 최초로 모바일 SBOM 관리를 제공하는 것이 이 솔루션의 강점이다.

3.12. Application Security Posture Management (ASPM)

Bionic 社가 개발한 프로덕션 애플리케이션의 보안성 향상을 위한 통합 보안 관리 솔루션이다[16]. 기존의 CI/CD 파이프라인을 다루는 소프트웨어 구성 분석(SCA, Software Composition Analysis)과 정적 애플리케이션 보안 테스트(SAST, Static Application Security Testing), 동적 애플리케이션 보안 테스트(DAST, Dynamic Application Security Testing) 등의 기능을 모두 포함한다.

그중 코드 변경 사항이 CI/CD 파이프라인에 푸시될 때, 본 솔루션은 애플리케이션의 아티팩트를 수집하고 리버스 엔지니어링 하여 SBOM을 실시간으로 동적으로 생성한다. 그 후 실시간으로 자산 인벤토리를 생성하여 소프트웨어 내에 존재하는 구성요소를 검색할 수 있는 기능을 제공한다. 또한, 자산 인벤토리 내에



〔그림 12〕 Bionic - ASPM 중 인벤토리에 표시된 서비스 SBOM 예시

취약한 서비스가 있는지 식별하는 기능을 제공한다.

Ⅳ. 결 론

본 논문에서는 소프트웨어 공급망 및 SBOM 관리 기능을 제공하고 있는 글로벌 기업 및 솔루션에 대해 소개하였다. 美 바이든 행정부가 행정명령 14028을 발표한 이후 전 세계적으로 소프트웨어 공급망 보안 강화를 위한 연구 개발이 활발히 이루어지고 있다. 현재 미 연방정부에 납품하는 핵심 소프트웨어에 대한 SBOM 제출이 의무화됨에 따라, 향후 국내 공급망 보안 정책 역시 SBOM 관리 의무화가 예상된다. 따라서 국제 정세에 맞추어 향후 국내 시장도 소프트웨어 공급망 보안 강화를 위한 활발한 솔루션 연구 개발이 이루어지길 기대한다.

참 고 문 헌

[1] KISA, "Cyber-treat Trends Report," Jul. 2018.

[2] Executive Office of the President of U.S., "Improving of Nation's Cybersecurity (Executive Order 14028)," May. 2021.

[3] National Telecommunications and Information Administration, "Framing Software Component Transparency: Establishing a Common Software Bill of Material," NOV. 2019

[4] Redhat, "CI/CD: Concepts, Methods, Benefits, Implementation Process," https://www.redhat.com/ko/topics/devops/what-is-ci-cd

[5] Rezilion, "Dynamic SBOM Solution Overview," https://www.rezilion.com/resource/dynamic-sbom-solution-overview

[6] Phylum, "Product Overview," https://www.phylum.io/why-phylum

[7] Qualys, "CyberSecurity Asset Management (CSAM) v2.0," https://www.qualys.com/apps/cybersecurity-asset-management

[8] Cycode, "NextGen SCA - Pipeline Composition Analysis," https://cycode.com/sca-software-composition-analysis

[9] Veracode, "Software Composition Analysis (SCA)," https://www.veracode.com/products/software-composition-analysis

[10] Synopsys, "Black Duck Software Composition Analysis," https://www.synopsys.com/software-integrity/security-testing/software-composition-analysis.html

[11] Anchore, "SOFTWARE BILL OF MATERIALS (SBOM) MANAGEMENT," https://anchore.com/sbom

[12] GrammaTech, "CodeSentry," https://www.grammatech.com/codesentry-sca

[13] Sonatype, "Nexus Lifecycle," https://www.sonatype.com/products/open-source-security-dependency-management

[14] RKVST, "Share Your Software Bill of Materials," https://www.rkvst.com/share-sboms

[15] NowSecure, "Announcing the World's First Dynamic Software Bill of Materials (SBOM) for Mobile Apps," Oct, 2021.

[16] Bionic, "Static SBOMs become out-of-date as you push code changes," https://bionic.ai/dynamic-bom

〈저 자 소 개〉

김 광 준 (Kwang-jun Kim)

학생회원

2017년 2월 : 한남대학교 컴퓨터공학과 학사
2019년 2월 : 한남대학교 컴퓨터공학과 석사
2019년 3월~현재 : 한남대학교 컴퓨터공학과 박사과정
<관심분야> 정보보호, 침입 탐지, 네트워크/시스템/공급망 보안

이 만 희 (Man-hee Lee)

종신회원

1995년 2월 : 경북대학교 컴퓨터공학과 공학사
1997년 2월 : 경북대학교 공학석사
2008년 8월 : Texas A&M 대학교 컴퓨터공학과 공학박사
1997년~2003년 : 한국과학기술정보연구원 연구원
2008년~2009년 : Cisco Systems, San Jose
2010년~2012년 : 국가보안기술연구소 선임연구원
2012년~현재 : 한남대학교 교수
<관심분야> 네트워크/시스템/스마트폰/공급망 보안, 고성능 시스템, 컴퓨터교육