레드펜소프트의 X-SCAN 제품은 소프트웨어 공급망 보안을 위한 솔루션으로, 다양한 기능을 제공합니다. 주요 기능은 다음과 같습니다:

1. \*\*패치 분석 및 검증\*\*: X-SCAN은 소프트웨어 패치의 자동화된 분석 및 검증을 통해 잠재적인 위협을 탐지합니다. 패치의 변경, 추가, 삭제된 내용을 이전 버전과 비교 분석하여 보안 위험을 식별합니다 [[❞]](https://www.redpensoft.com/blank-1-2) [[❞]](https://www.dailysecu.com/news/articleView.html?idxno=156384).

2. \*\*클라우드 컨테이너 이미지 스캐닝 및 분석\*\*: 최근 추가된 기능으로, 클라우드 컨테이너 이미지에 대한 스캐닝 및 분석을 수행합니다. 컨테이너 이미지 내의 비밀 데이터나 구성 오류를 탐지하여 보안 취약점을 사전에 방지할 수 있습니다 [[❞]](https://redpensoft.tistory.com/70) [[❞]](https://byline.network/2024/05/29-271/).

3. \*\*의심 행위 탐지\*\*: 소프트웨어 구성 요소 간의 의존성과 공급망 공격에 주로 사용되는 행위를 분석하여 의심스러운 활동을 탐지합니다 [[❞]](https://www.redpensoft.com/blank-1-2).

4. \*\*제로데이 공격 대응\*\*: 발견되지 않은 취약점을 악용하는 제로데이 공격을 방지하는 기능도 포함되어 있으며, 시스템 보안 업데이트가 지연된 경우에도 보호할 수 있습니다 [[❞]](https://redpensoft.tistory.com/70).

5. \*\*생성형 AI 연계\*\*: 생성형 AI 기술을 활용하여 컨테이너 이미지의 각 레이어에 포함된 명령어의 목적과 기능을 해석해 줍니다. 이는 보안 분석의 정확성을 높이는 데 기여합니다 [[❞]](http://www.hitech.co.kr/news/articleView.html?idxno=31546).

X-SCAN은 금융, 공공, 기업 분야에서 레퍼런스를 확보하고 있으며, 다양한 공인 파트너사들과 협력하여 다수의 POC(Proof of Concept)를 진행 중입니다 [[❞]](https://www.dailysecu.com/news/articleView.html?idxno=156384).

이러한 기능들을 통해 X-SCAN은 소프트웨어 공급망의 보안성을 강화하고, 클라우드 네이티브 환경에서의 보안 취약점을 효과적으로 관리할 수 있습니다.

국내에서 X-SCAN과 유사한 소프트웨어 공급망 보안 솔루션으로는 쿤텍(Kuntek)의 "이지스(AEGIS)"가 있습니다. 이지스는 다양한 기능을 갖추고 있어 소프트웨어 공급망의 보안을 강화하는 데 효과적입니다.

1. \*\*이지스-SCA(Software Component Analysis)\*\*: 이 기능은 외부에서 반입된 오픈소스와 바이너리 파일에 대한 SBOM(Software Bill of Materials)을 생성하고, 취약점 및 라이선스 이슈를 대시보드를 통해 직관적으로 파악할 수 있습니다. 또한 결재 및 승인 프로세스를 통해 손쉽게 관리할 수 있도록 지원합니다 [[❞]](https://www.denews.co.kr/news/articleView.html?idxno=29926).

2. \*\*이지스-SCM(Supply Chain Management)\*\*: 실행 소프트웨어의 바이너리 분석을 통해 악성코드 유입이나 변조 가능성을 확인하고, 다양한 형식의 SBOM을 업로드 및 비교할 수 있습니다. 이를 통해 소프트웨어 공급망을 효과적으로 관리할 수 있습니다 [[❞]](https://www.denews.co.kr/news/articleView.html?idxno=29926) [[❞]](https://www.dailysecu.com/news/articleView.html?idxno=157322).

3. \*\*이지스-RMS(Repository Management System)\*\*: 퍼블릭 및 내부 레파지토리를 고객사의 언어와 환경에 맞게 커스터마이징하여 관리합니다. 패키지 매니저를 통해 요청, 점검, 반입의 원스톱 프로세스를 적용하여 클린 레파지토리를 유지할 수 있습니다 [[❞]](https://www.dailysecu.com/news/articleView.html?idxno=157322).

이 솔루션들은 소프트웨어 공급망 보안의 체계적인 관리를 지원하며, 기업이 자체적으로 관리하기 어려운 SBOM 분석과 취약점 관리를 통합적으로 처리할 수 있도록 돕습니다.

이 외에도 다양한 국내외 솔루션들이 소프트웨어 공급망 보안을 강화하기 위해 지속적으로 발전하고 있습니다.

또 다른 국내 소프트웨어 공급망 보안 솔루션으로는 이글루코퍼레이션의 “Security & Intelligence”가 있습니다. 이 솔루션은 주로 SBOM(Software Bill of Materials)을 활용하여 소프트웨어 구성 요소의 투명성을 확보하고, 공급망 보안의 취약점을 관리하는 데 중점을 둡니다.

이글루코퍼레이션의 솔루션은 CycloneDX 표준을 사용하여 SBOM을 생성합니다. CycloneDX는 메타데이터, 구성 요소, 종속성, 취약점 등을 포함한 다양한 형식의 BOM을 지원하며, 이를 통해 소프트웨어 개발 단계에서부터 배포 및 유지보수 단계에 이르기까지 전반적인 보안을 강화할 수 있습니다 [[❞]](<https://www.igloo.co.kr/security-information/sbom%EC%9D%84-%EC%9D%B4%EC%9A%A9%ED%95%9C-%EA%B3%B5%EA%B8%89%EB%A7%9D-%EB%B3%B4%EC%95%88/>).

또한, 과학기술정보통신부와 한국인터넷진흥원(KISA)에서는 소프트웨어 공급망 보안 가이드라인을 발표하고, 이를 통해 국내 기업들이 SBOM을 효과적으로 활용하여 공급망 보안을 강화할 수 있도록 지원하고 있습니다 [[❞]](<https://www.aitimes.kr/news/articleView.html?idxno=31141>).

이러한 솔루션들은 소프트웨어 개발 및 운영 과정에서 발생할 수 있는 다양한 보안 위협을 사전에 탐지하고 관리함으로써, 보다 안전한 소프트웨어 환경을 제공하는 데 기여하고 있습니다.

해외에서도 소프트웨어 공급망 보안 솔루션이 많이 사용되고 있으며, 대표적인 제품으로는 다음과 같은 것들이 있습니다:

1. \*\*Sonatype Nexus Lifecycle\*\*:

- \*\*기능\*\*: Sonatype의 Nexus Lifecycle은 소프트웨어 개발 파이프라인 내에서 오픈소스 컴포넌트의 보안, 라이선스, 품질 문제를 자동으로 감지하고 보고합니다. SBOM 생성 및 관리 기능을 포함하여 오픈소스 라이브러리의 최신 상태를 유지합니다.

- \*\*특징\*\*: 오픈소스 보안 취약점을 실시간으로 감시하고, 보안 정책을 적용하여 자동으로 문제를 해결합니다.

2. \*\*Snyk\*\*:

- \*\*기능\*\*: Snyk은 오픈소스 라이브러리, 컨테이너, 코드 및 인프라의 보안 취약점을 탐지하고 수정하는 데 중점을 둔 도구입니다. 개발자가 코드 작성 시점에서 보안을 유지할 수 있도록 지원합니다.

- \*\*특징\*\*: 실시간 보안 취약점 탐지, 자동 수정 제안, 통합된 CI/CD 파이프라인 지원을 통해 개발 주기 전반에 걸쳐 보안을 강화합니다.

3. \*\*Black Duck by Synopsys\*\*:

- \*\*기능\*\*: Black Duck은 오픈소스 관리 솔루션으로, 소프트웨어의 오픈소스 사용을 감시하고 취약점 및 라이선스 준수 문제를 관리합니다.

- \*\*특징\*\*: 광범위한 오픈소스 데이터베이스를 기반으로 한 보안 분석, 라이선스 준수 관리, 자동화된 보안 업데이트 기능을 제공합니다.

4. \*\*Veracode\*\*:

- \*\*기능\*\*: Veracode는 애플리케이션 보안을 위한 통합 플랫폼으로, 정적 및 동적 애플리케이션 보안 테스트(SAST/DAST), 소프트웨어 구성 분석(SCA), 펜 테스트 등을 포함합니다.

- \*\*특징\*\*: 통합된 보안 플랫폼으로, 소프트웨어 개발 라이프사이클 전반에 걸쳐 보안 테스트 및 분석을 수행합니다.

5. \*\*Jfrog Xray\*\*:

- \*\*기능\*\*: Jfrog Xray는 아티팩트 리포지토리 관리 솔루션으로, 소프트웨어 구성 요소의 보안 및 라이선스 준수를 모니터링합니다.

- \*\*특징\*\*: 지속적인 보안 스캔, 실시간 위협 탐지, 심층적인 아티팩트 분석을 통해 소프트웨어 공급망의 보안을 유지합니다.

이러한 해외 솔루션들은 소프트웨어 개발 과정에서 발생할 수 있는 다양한 보안 취약점을 실시간으로 모니터링하고 관리하여, 안전한 소프트웨어 공급망을 유지하는 데 중요한 역할을 하고 있습니다.

한국에서 사용되고 있는 해외 소프트웨어 공급망 보안 솔루션 중 하나는 \*\*Sonatype Nexus Lifecycle\*\*입니다. 이 제품은 오픈소스 컴포넌트의 보안 및 라이선스 문제를 관리하고, 소프트웨어 개발 라이프사이클(SDLC) 전반에 걸쳐 보안을 강화하는 데 중점을 둡니다. Sonatype Nexus Lifecycle은 한국에서 공식 총판인 OSC Korea를 통해 제공되고 있습니다 [[❞]](<https://www.osckorea.com/solution/sonatype>) [[❞]](<https://www.sonatype.com/products/open-source-security-dependency-management>).

또한, \*\*Snyk\*\*는 국내에서도 많이 사용되는 솔루션으로, 오픈소스 라이브러리, 컨테이너, 코드 및 인프라의 보안 취약점을 탐지하고 수정하는 기능을 제공합니다. Snyk는 다양한 개발 도구와 통합되어 개발자가 코드 작성 시점에서 보안을 유지할 수 있도록 돕습니다.

\*\*Black Duck by Synopsys\*\* 역시 국내에서 활용되는 대표적인 제품으로, 오픈소스 관리 솔루션을 통해 소프트웨어의 오픈소스 사용을 감시하고, 취약점 및 라이선스 준수 문제를 관리합니다.

이와 같은 제품들은 한국의 다양한 기업과 기관에서 소프트웨어 공급망 보안을 강화하기 위해 사용되고 있으며, 각 제품의 특성에 따라 맞춤형 보안 솔루션을 제공하고 있습니다.

다음은 국내에서 사용되고 있는 주요 해외 소프트웨어 공급망 보안 솔루션과 그 총판에 관한 정보입니다:

1. \*\*Sonatype Nexus Lifecycle\*\*:

- \*\*총판\*\*: OSC Korea

- \*\*기능\*\*: 오픈소스 컴포넌트의 보안 취약점 및 라이선스 문제를 관리하며, 소프트웨어 개발 라이프사이클 전반에 걸쳐 보안을 강화합니다. SBOM 생성 및 관리, 지속적인 취약점 모니터링을 제공합니다 [[❞]](<https://www.osckorea.com/solution/sonatype>) [[❞]](<https://www.sonatype.com/products/open-source-security-dependency-management>).

2. \*\*Snyk\*\*:

- \*\*총판\*\*: OSBC (Open Source Business Consulting)

- \*\*기능\*\*: 오픈소스 라이브러리, 컨테이너, 코드 및 인프라의 보안 취약점을 탐지하고 수정하는 기능을 제공합니다. 다양한 개발 도구와의 통합을 통해 코드 작성 시점에서 보안을 유지할 수 있도록 돕습니다 [[❞]](<https://www.trendmicro.com/ko_kr/business/products.html>) [[❞]](<https://www.techtradeasia.com/2022/01/snyk-enters-south-korea.html#:~:text=URL%3A%20https%3A%2F%2Fwww.techtradeasia.com%2F2022%2F01%2Fsnyk>).

3. \*\*Black Duck by Synopsys\*\*:

- \*\*총판\*\*: 정보가 명확히 확인되지 않았으나, Synopsys의 다양한 제품들은 한국 내 여러 파트너사를 통해 제공되고 있습니다.

- \*\*기능\*\*: 오픈소스 소프트웨어 구성 요소의 취약점을 분석하고, 라이선스 준수를 관리합니다.

이러한 솔루션들은 한국의 다양한 기업과 기관에서 소프트웨어 공급망 보안을 강화하기 위해 사용되고 있으며, 각 제품의 특성에 따라 맞춤형 보안 솔루션을 제공하고 있습니다.