



# 오픈소스 소프트웨어 위험관리 전략

Synopsys Korea - Software Integrity Group

정성훈 부장

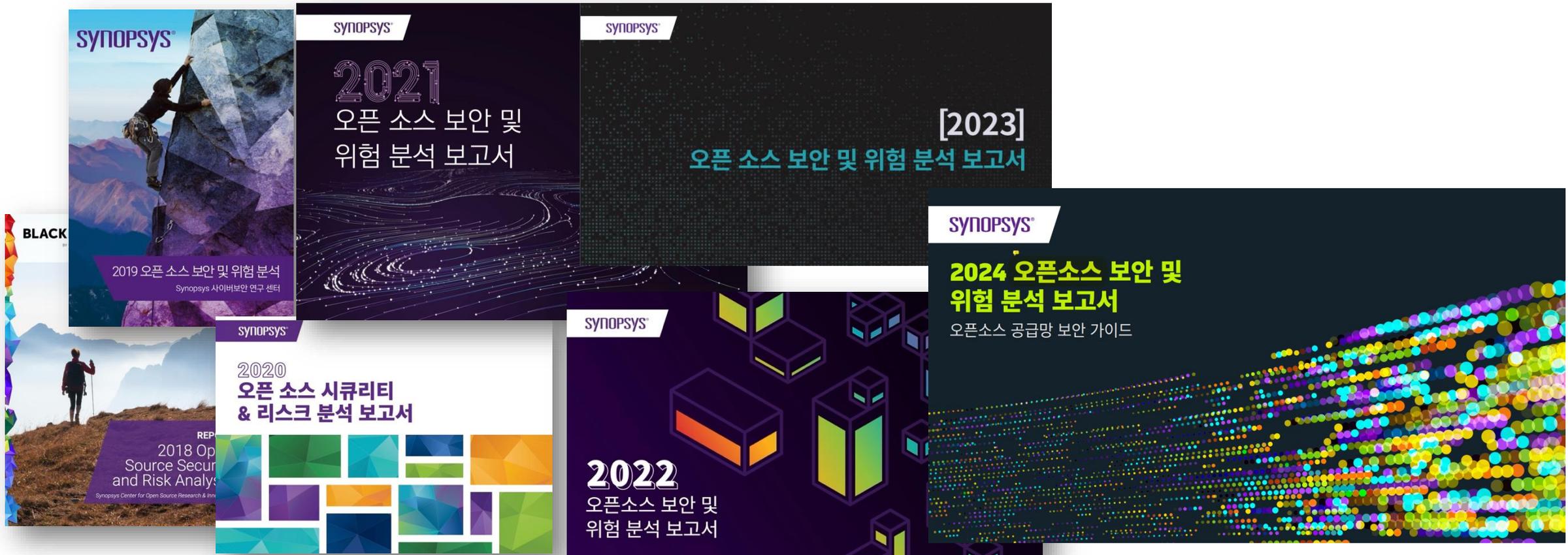
# 목차

- 왜 오픈소스 소프트웨어에 주목해야 할까요?
- 관리되지 않는 오픈소스 소프트웨어 사용의 위험성
- 국내외 오픈소스 보안 동향
- 오픈소스 소프트웨어 관리를 위한 모범 사례

왜 오픈소스 소프트웨어에 주목해야 할까요?

# OSSRA 리포트

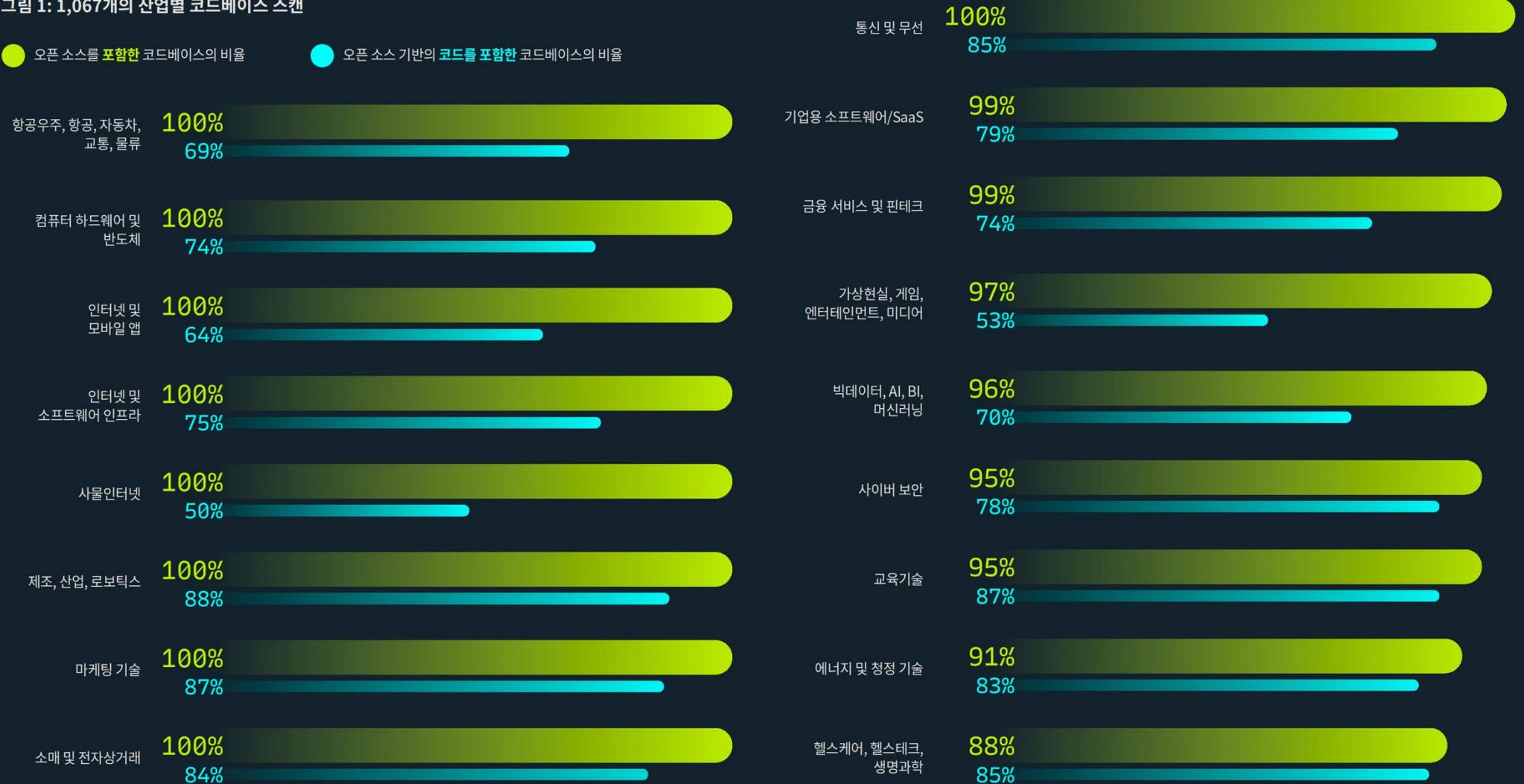
- 상업용 애플리케이션 코드에서 오픈소스의 사용 양상에 대한 조사 결과를 공개
- 2018년부터 매년 발행
- 현재 시놉시스 SIG(Software Integrity Group)의 사이버보안연구센터(CyRC)에서 담당



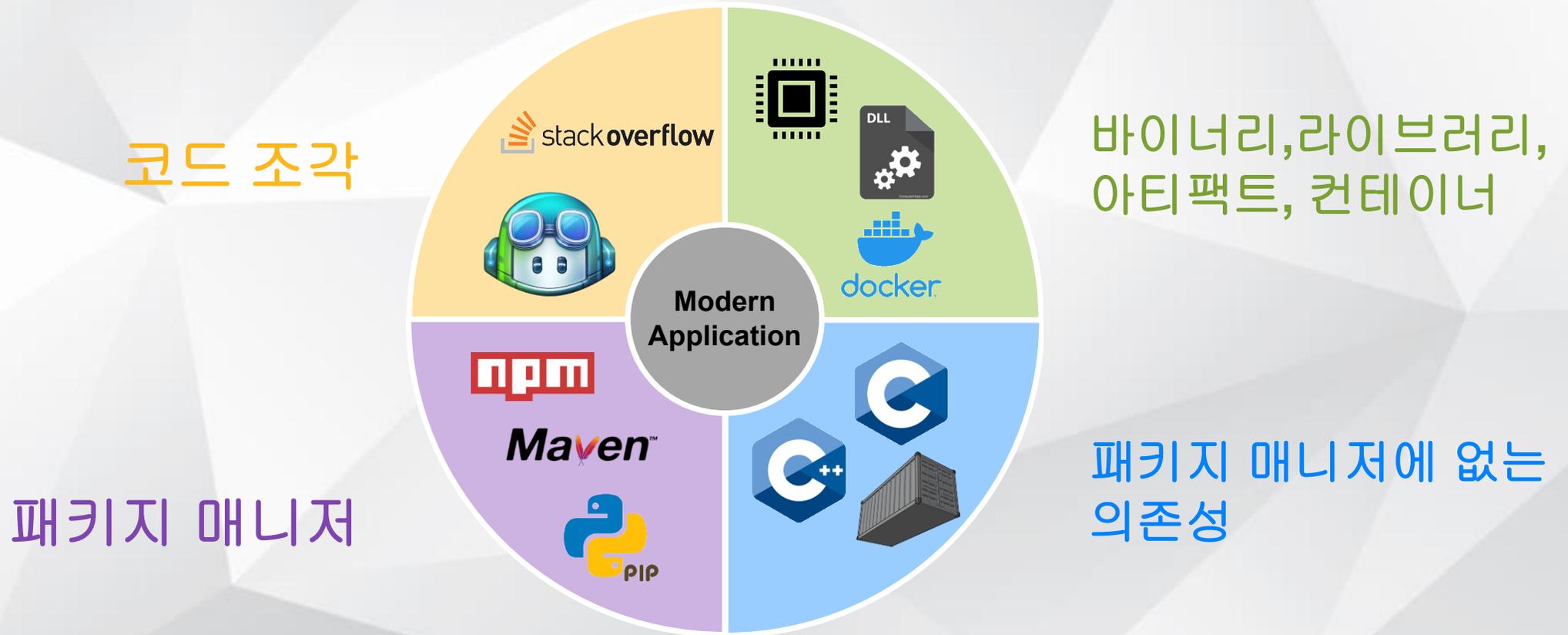
# 모든 산업은 오픈 소스를 기반으로 합니다.

그림 1: 1,067개의 산업별 코드베이스 스캔

● 오픈 소스를 포함한 코드베이스의 비율    ● 오픈 소스 기반의 코드를 포함한 코드베이스의 비율



# 오픈 소스를 포함시킬 수 있는 다양한 방법



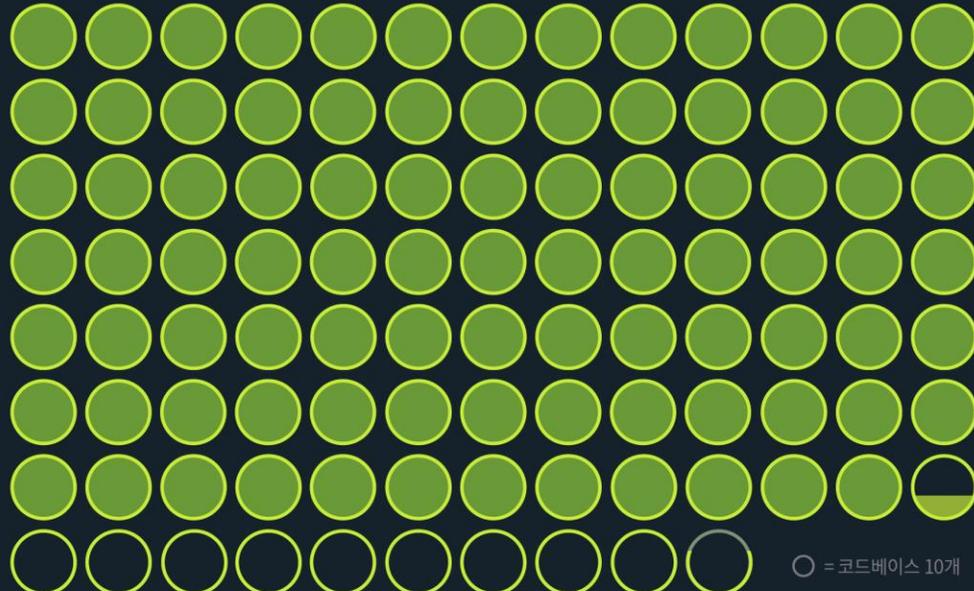
# 관리되지 않는 오픈소스 소프트웨어 사용의 위험성

소프트웨어 공급망 보안을 최우선으로 고려해야 합니다.



# OSSRA 리포트 요약

## 개요



○ 1,067개 코드베이스를 2023년에 스캔      ● 936개 코드베이스를 대상으로 위험 분석 실행

84%

취약점을 포함한 코드베이스(위험 분석을 실행한 코드베이스)

74%

고위험 취약점을 포함한 코드베이스(위험 분석을 실행한 코드베이스)



96%

전체 코드베이스의 96%에  
오픈 소스가 포함되어  
있었습니다.



77%

전체 코드베이스의  
모든 코드 중 77%가  
오픈 소스를 기반으로  
생성되었습니다.



53%

전체 코드베이스의  
53%에서 라이선스 충돌이  
있었습니다.



31%

전체 코드베이스의 31%에  
라이선스가 없는 오픈 소스  
또는 커스텀 라이선스가  
있는 오픈 소스가 포함되어  
있었습니다.

10

년

위험 분석을 진행한  
코드베이스의 14%에  
10년 넘는 취약점이  
포함되어 있었습니다.

2.8

년

위험 분석을 진행한  
코드베이스에서 발견한  
취약점은 평균 2.8년이  
지난 것이었습니다.

24

개월

위험 분석을 진행한  
코드베이스의 49%에 최근  
24개월 동안 개발이 이뤄지지  
않은 구성요소가 포함되어  
있었습니다.

12

개월

코드베이스의 1%에는  
코드 관리자의 업데이트/  
패치를 12개월 넘게 받지  
않은 구성요소가 포함되어  
있었습니다.

91%

위험 분석을 진행한 코드베이스 중에서 최신 버전과 비교해 10단계 이상 낮은 버전의  
구성요소가 포함되어 있는 코드베이스.

# 국내외 오픈소스 보안 동향

# 국제 오픈소스 보안 동향

- 미 연방 정부(U.S. Federal Government)

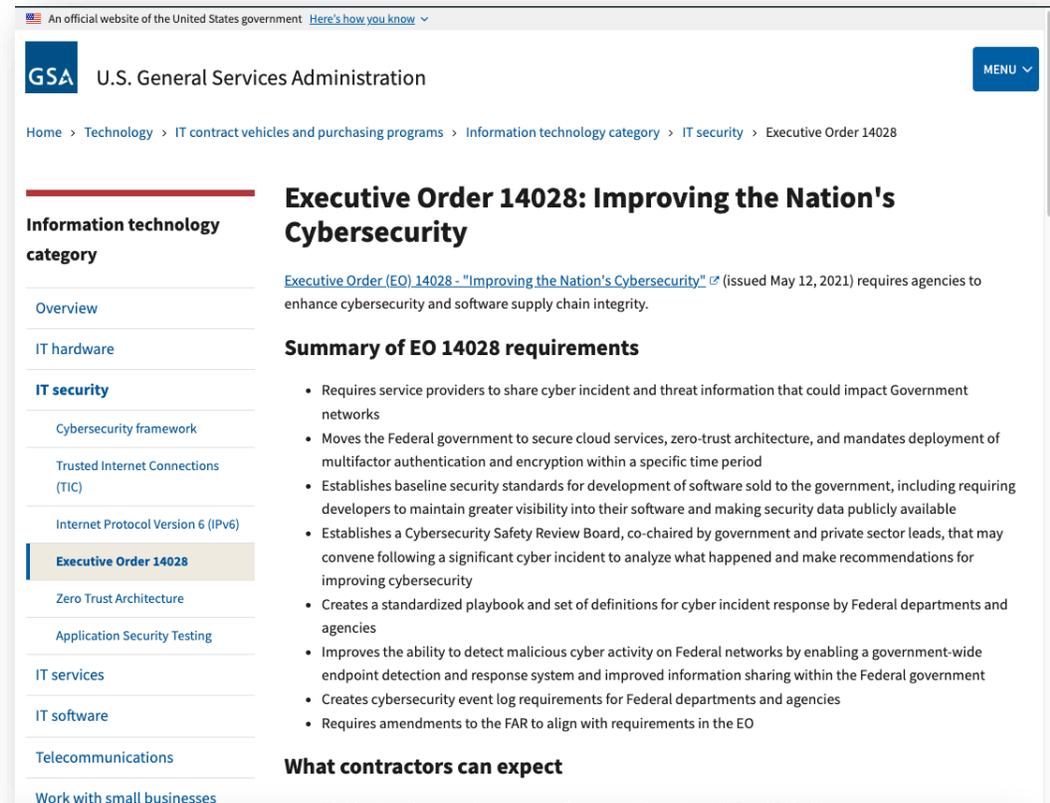
- 행정명령 14028 (5/2021)

- 국립 표준 기술 연구소(NIST)에 SBOM에 대한 지침 개발 지시

- 연방 조달 프로세스에 SBOM 사용 기준 설정

- CISA (사이버보안 및 인프라 보안국)

- 보안 지침의 일부로 SBOM을 사용할 것을 권장



# 국제 오픈소스 보안 동향

- 미 연방 정부(U.S. Federal Government)
  - Secure Software Development Attestation
    - CISA와 OMB 배포 (3/11/2024)
    - 미국 공급망 보안정책으로 의무사항
    - 소프트웨어가 안전하게 개발 되었음을 연방 정부에 보증하는 것
    - 기관은 소프트웨어 제공자에게 SBOM 혹은 3rd Party 인증서 등 추가 증명 문서 요구 가능

OMB: 관리예산처

CISA: 사이버보안 및 인프라 보안국

**Department of Homeland Security**  
**Cybersecurity and Infrastructure Security Agency (CISA)**  
**Secure Software Development Attestation Form Instructions**

---

Read all instructions before completing this form

---

**Privacy Act Statement**

[NOTE: This Privacy Act Statement is unique to DHS. All agencies using this common form will need to provide an agency-unique Privacy Act Statement when they request to use this form. Each agency using this common form should provide Privacy Act Statements that conform to its applicable agency procedures and requirements.]

**Authority:** 44 U.S.C. § 3554, Executive Order (E.O.) 14028, "Improving the Nation's Cybersecurity," and OMB Memorandum M-22-18, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices," as amended by OMB Memorandum M-23-16, "Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices," authorize the collection of this information.

**Purpose:** The purpose of this form is to provide the Federal Government assurances that software used by agencies is securely developed.

**Background:** This information may be disclosed as generally permitted under Executive Order 14028, Improving the Nation's Cybersecurity (E.O. 14028) and Memorandum M-22-18, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices" (M-22-18), as amended. This form collects contact information from vendor employees who make the attestation. For DHS, information may be disclosed as necessary and authorized by the routine uses published in DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other List System, November 25, 2008, 73 FR 71659.

**Section I**

New Attestation  Attestation Following Extension or Waiver  Revised Attestation

**Type of Attestation:**  Company-wide  Individual Product  Multiple Products or Specific Product Version(s) (please provide complete list)

If this attestation is for an individual product or multiple products, provide the software name, version number, and release/publish date to which this attestation applies. Additional pages can be attached to this attestation if more lines are needed:

Product(s) Name	Version Number <sup>1</sup> (if applicable)	Release/Publish Date (if applicable)

For the above specified software, this form does not cover software or any components of that software that fall into the following categories:

1. Software developed by Federal agencies;
2. Open source software that is freely and directly obtained directly by a Federal agency;
3. Third-party open source and proprietary components that are incorporated into the software end product used by the agency; or
4. Software that is freely obtained and publicly available.

Note: In signing this attestation, software producers are attesting to adhering to the secure software development practices outlined in Section III for code developed by the producer.

**Section II**

**1. Software Producer Information**

Company Name: \_\_\_\_\_  
 Address: \_\_\_\_\_  
 City: \_\_\_\_\_

State or Province: \_\_\_\_\_  
 Postal Code: \_\_\_\_\_  
 Country: \_\_\_\_\_  
 Company Website: \_\_\_\_\_

**2. Primary Contact for this Document and Related Information (may be an individual, role, or group):**

Name: \_\_\_\_\_  
 Title: \_\_\_\_\_  
 Address: \_\_\_\_\_  
 Phone Number: \_\_\_\_\_  
 Email Address (may be an alias/distribution list): \_\_\_\_\_

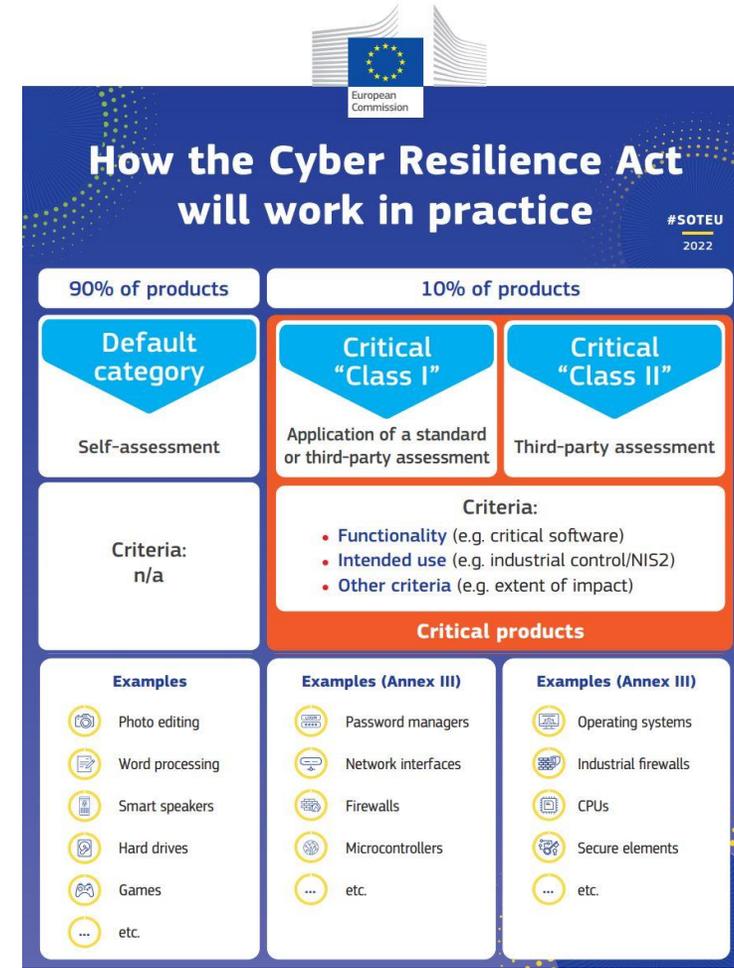
**Section III**

**Attestation and Signature**

On behalf of the above-specified company, I attest that, to the best of my knowledge, [software producer] presently makes consistent use of the following practices, derived from the secure software development framework (SSDF),<sup>2</sup> in developing the software identified in Section I:

# 국제 오픈소스 보안 동향

- 유럽연합 사이버 복원력법 (EU Cyber Resilience Act)
  - EU 집행위원회 발의(9/2022)
  - CRA 필수 사이버보안 요건
    - 사이버보안을 보장하는 안전한 개발 및 운영 관행
    - 지속적인 취약성 대응 및 보고
    - 소프트웨어 업데이트 제공
    - 빌드/개발 환경 보호
    - 지원 수명 관련 투명성
    - 데이터 보호/암호화
    - 보안 테스트
    - **SBOM(Software Bill of Materials) 생성 의무**
    - 소프트웨어 공급망 투명성
    - 보안 테스트 및 승인 보고서
    - 규정 준수 문서



# 국내 오픈소스 보안 동향 - TTA

- TTA (한국정보통신기술협회)
  - 오픈소스 거버넌스 구성요소 (TTAK.KO-11.0321)
    - 오픈소스 거버넌스 활동을 위한 정책, 프로세스, 조직, 도구, 교육 등등 기술
  - 오픈소스 SBOM 거버넌스 관리 지침 (TTAK.KO-11.0322)
    - SBOM 관리목적 도출, 요구사항에 부합한 SBOM 속성 도출 등

The screenshot shows the TTA website interface for the standard TTA.KO-11.0321. It includes a search bar, navigation tabs, and a detailed information table.

No.	표준번호	표준명	제/개정일
27	TTAK.KO-11.0321	오픈소스 거버넌스 구성요소	2023-12-06
26	TTAK.KO-	오픈소스 SBOM 거버넌스 관리 지침	2023-12-06

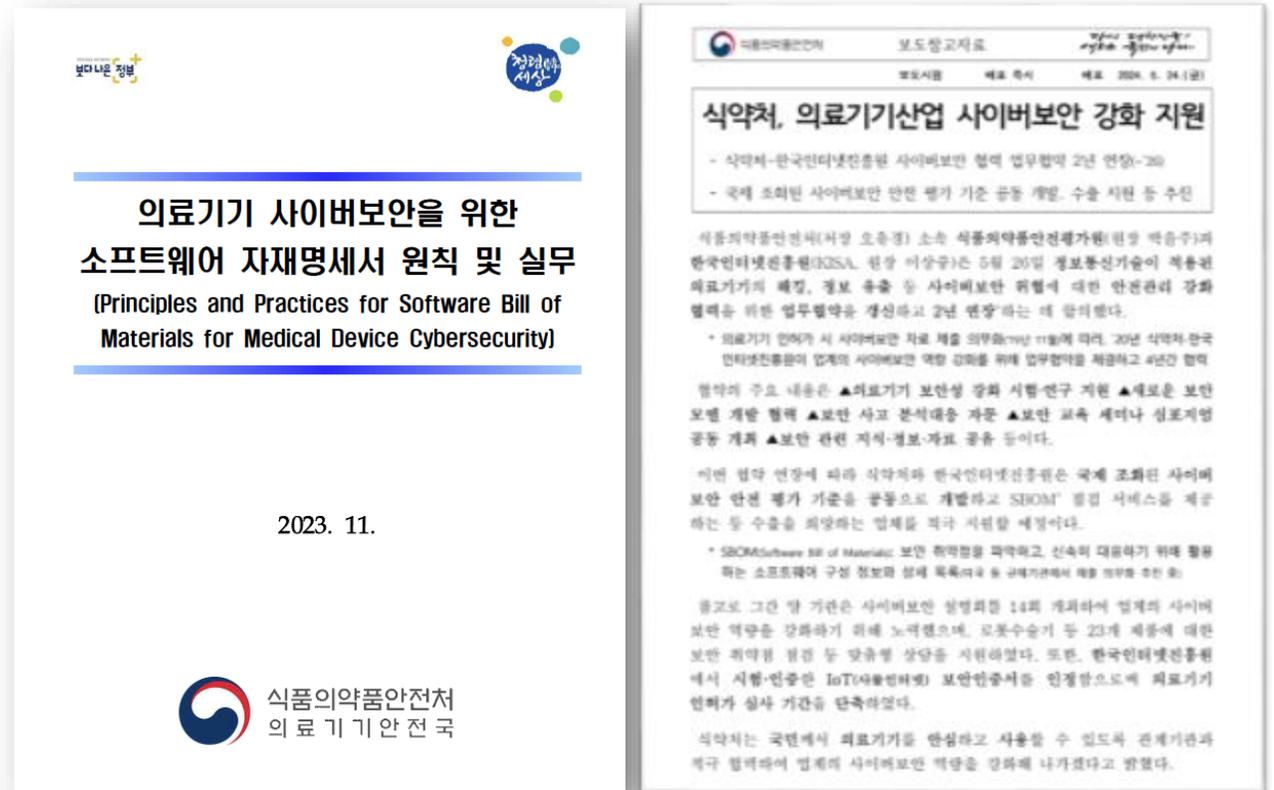
  

표준종류	정보통신단체표준(TTAS)						
표준번호	TTAK.KO-11.0321	구 표준번호					
제개정일	2023-12-06	총 페이지	11				
한글 표준명	오픈소스 거버넌스 구성요소						
영문 표준명	Open Source Governance Component						
한글 내용요약	오픈소스 거버넌스 활동을 위한 정책, 프로세스, 조직, 도구, 교육, 평가 등에 대한 정의, 활동, 필요 역량 등을 기술한다.						
영문 내용요약	The standard describes policies, processes, organizations, tools, definitions of training, evaluation, activities, and required capabilities, which are components of open source governance to systematically and effectively carry out open source-related tasks.						
관련 IPR 협약서	접수된 IPR 협약서 없음						
관련파일	TTAK.KO-11.0321.pdf						
표준이력	표준명	표준번호	제개정일	구분	유효 여부	IPR 협약서	파일
	오픈소스 거버넌스 구성요소	TTAK.KO-11.0321	2023-12-06	제정	유효	없음	

# 국내 오픈소스 보안 동향 - 식품의약품안전처

## • 식품의약품안전처

- 의료기기 사이버보안을 위한 소프트웨어 자재명세서 원칙 및 실무 (11/1/2023)
  - SBOM 프레임워크 개요
  - MDM(Medical Device Manufacturers)의 SBOM 관리를 위한 고려사항 등
- 식약처-한국인터넷진흥원 업무협약 연장 (5/24/2024)
  - 사이버 보안 안전 평가 기준의 공동 개발
  - SBOM 점검 서비스 제공



# 국내 오픈소스 보안 동향 - 정부

## • 정부

- 과학기술정보통신부, 국가정보원, 디지털플랫폼정부위원회 가 협력하여 소프트웨어 공급망보안 가이드라인(지침) 1.0 발표 (5/12/2024)
- SBOM기반 소프트웨어 공급망 보안 관리체계 구축 및 기업 지원 서비스
  - 기업지원허브(판교)
  - 디지털헬스케어 보안리빙랩(원주)
  - 국가사이버보안협력센터 기술공유실(판교)

과학기술정보통신부, 국가정보원, 디지털플랫폼정부위원회 보도자료

2024. 5. 12. (월) 12:00 (2024. 5. 13. (월) 초간) 배포 2024. 5. 10. (금) 14:00

### 정부, 소프트웨어공급망보안가이드라인(지침) 1.0 발표

(부제: 소프트웨어공급망보안 국제동향 및 소프트웨어구성명세서(SBOM)활용사례)

- 국산 소프트웨어에 SBOM 실증 결과를 반영  
- 디지털플랫폼정부시스템등에 소프트웨어공급망보안을 사전 적용하고, 중  
강화 지원 확대 -  
- 해외동향과 국내 준비상황을 면밀히 살펴면서 가

과학기술정보통신부(장관 이종호, 이하 '과기정통부'), 국가정보원(원  
플랫폼정부위원회(위원장 고진, 이하 '디플정위')는 민관 협력을 통  
가이드라인 1.0 (이하 '가이드라인')을 마련했다고 밝혔다.

가이드라인은 과기정통부, 국정원, 디플정위와 한국인터넷진흥원(KISA),  
한국정보보호산업협회(KISIA) 등 정부-공공기관 홈페이지를 통해 2024  
료로 내려받아 사용할 수 있음

본 가이드라인은 확산되고 있는 SW 공급망 사이버보안 위험과 미  
구성요소 명세서(SW Bill of Materials, SBOM) 제출 의무화 등에 대응하  
자체적인 SW 공급망 보안 관리역량을 갖추 수 있도록 지원하기 위하

또한 본 가이드라인은 국산 SW에 대한 SBOM 실증 및 SW 공급  
운영 결과 등을 반영한 것으로 세계적으로도 유례없는 실무 안에서  
와 협력을 통해 해외에도 적극 소개할 계획이다.

2024. 05

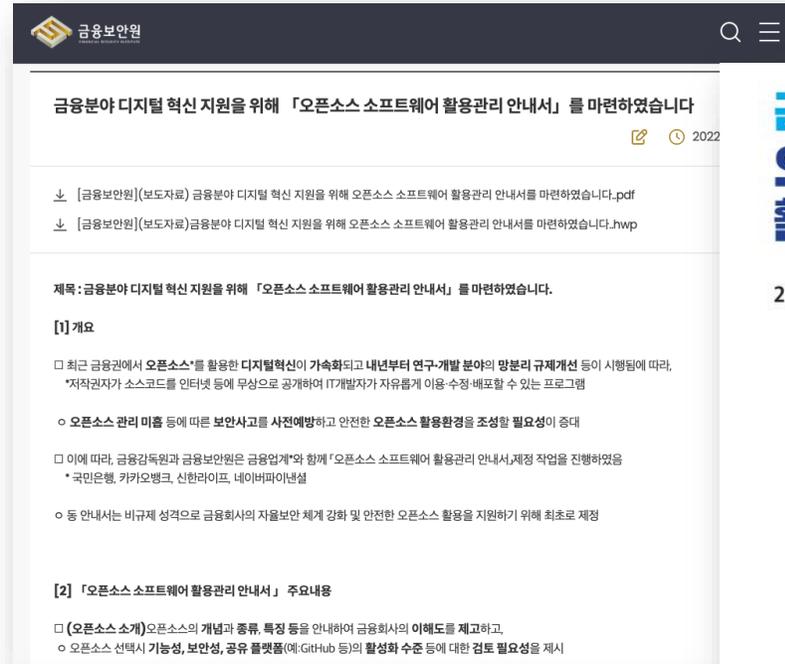
## SW 공급망 보안 가이드라인 v1.0

SW 공급망 보안 국제동향 및 SBOM 활용사례

# 국내 오픈소스 보안 동향 - 금융보안원

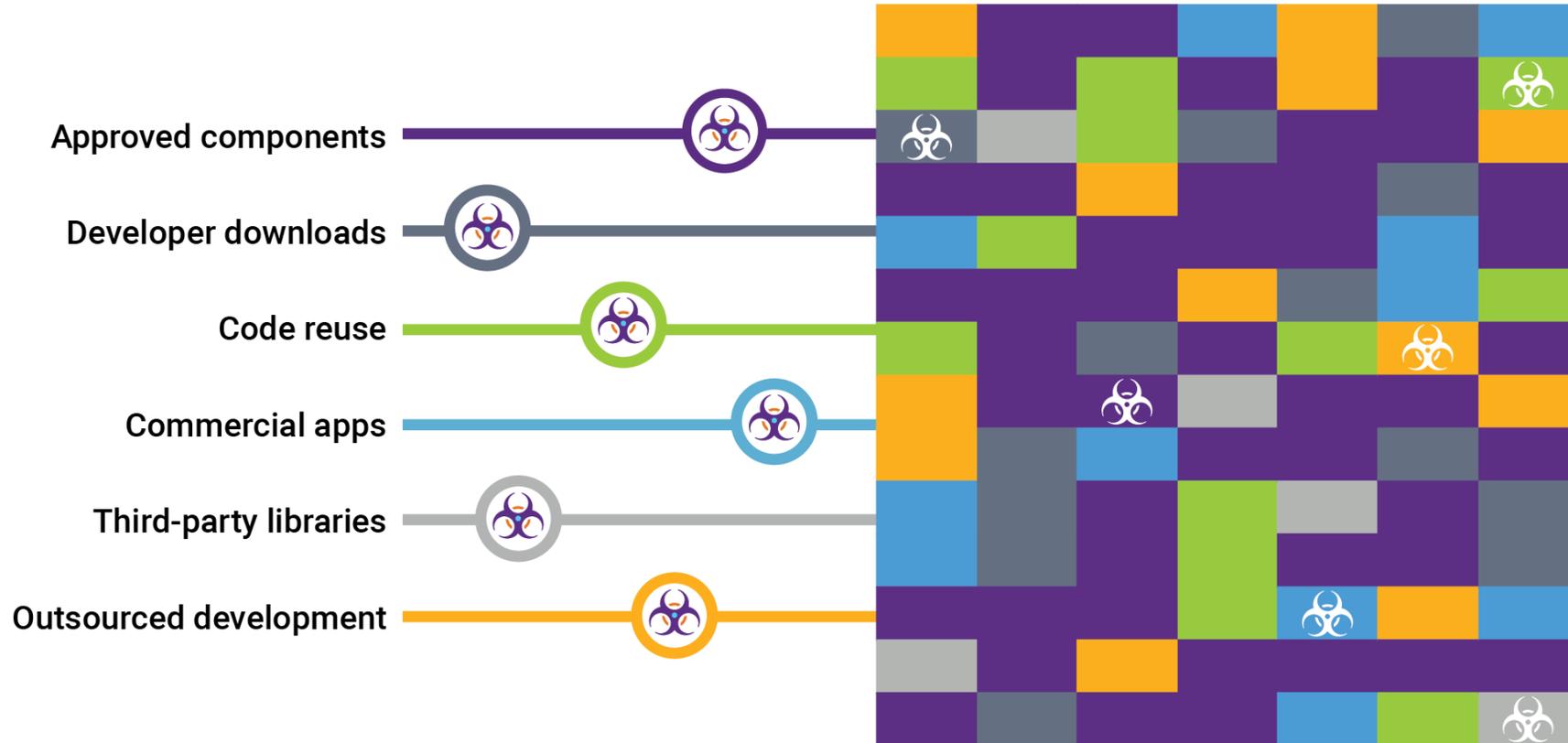
## • 금융보안원

- 오픈소스 소프트웨어 활용관리 안내서 (12/8/2022)
  - 오픈소스 소프트웨어 소개
  - 오픈소스 소프트웨어 보안성관리
  - 오픈소스 소프트웨어 관리절차



# 오픈 소스 관리를 위한 모범 사례

# 현대 애플리케이션 구성의 복잡성



# SCA를 통한 가시성 확보

의존성  
Analysis

시그니처  
Analysis

바이너리  
Analysis

코드조각  
Analysis



패키지 매니저의 직접 및 전이 의존성  
해결



C/C++와 같은 컴파일 된 언어의 종속성



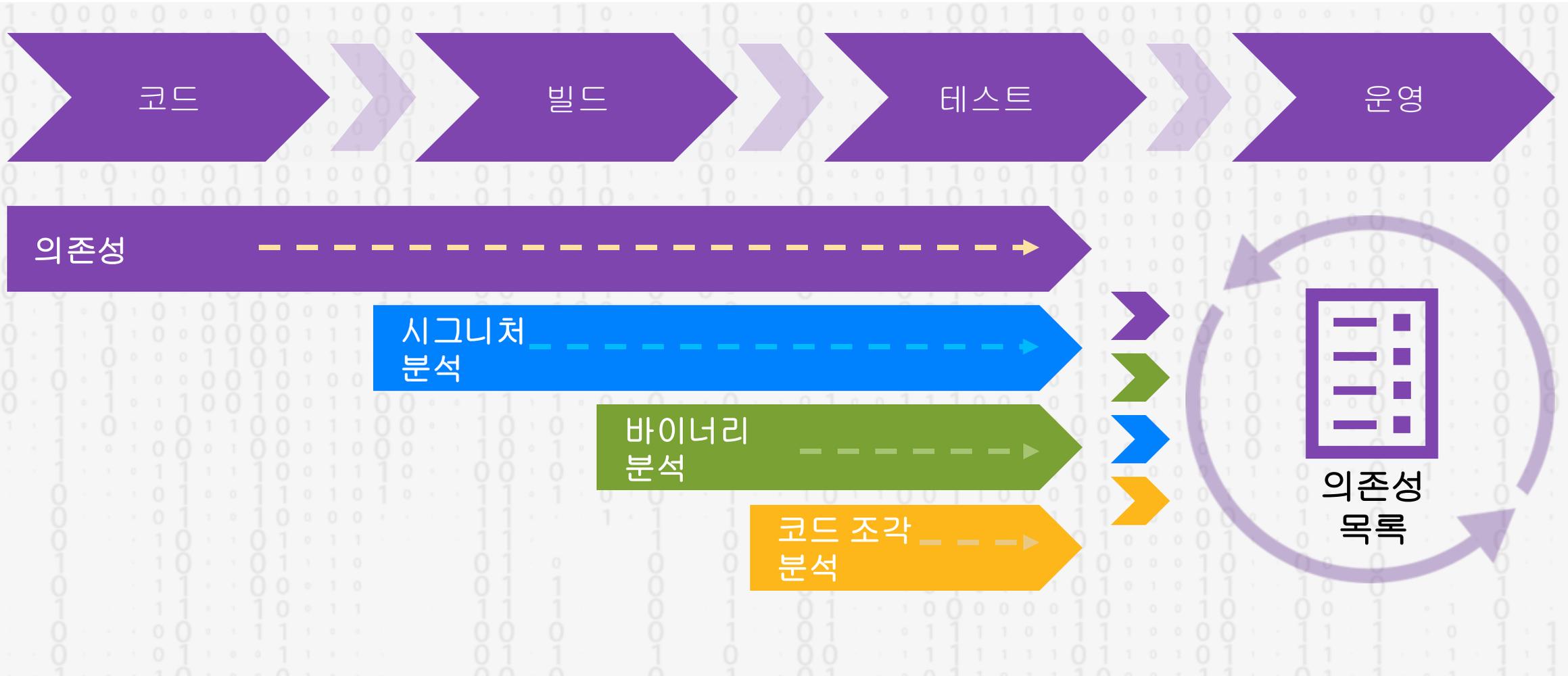
실행 파일, 라이브러리 및 컨테이너  
이미지에서 발견되는 종속성



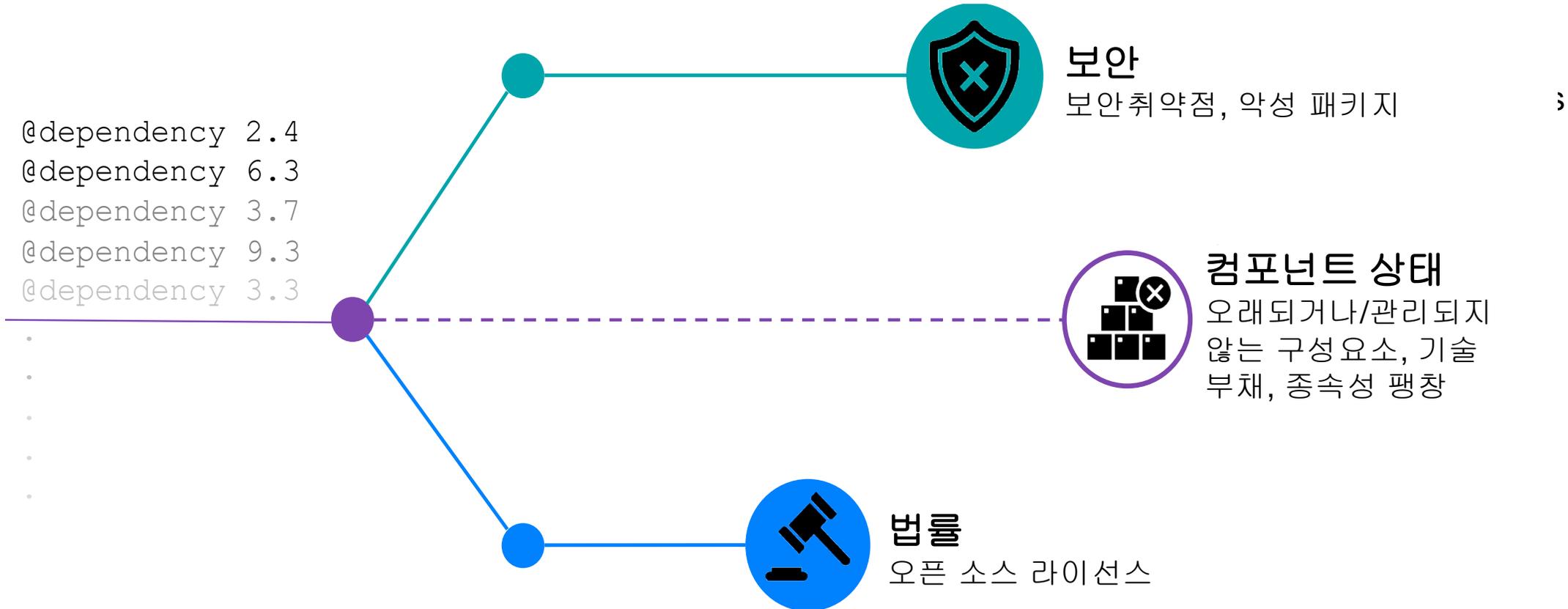
개발자가 복사하거나 AI가 생성한  
오픈 소스 코드 조각

# SDLC에 종속성 분석 과정을 구축

효율성과 정확성을 고려한 합리적 운영



# 포괄적인 목록 구성을 통한 위험 관리



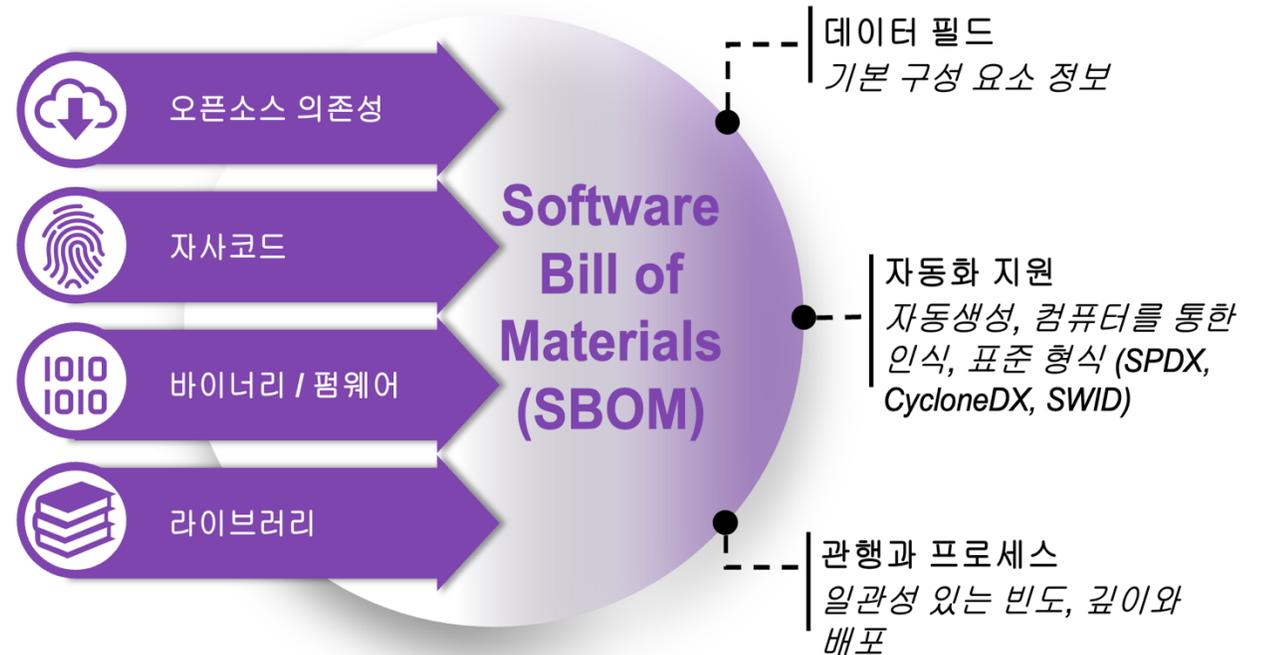
# 소프트웨어 자재 명세서 (SBOM - Software Bill of Materials )

- 소프트웨어 재료 목록 (구성요소)

- 자체개발 코드
- 오픈소스 소프트웨어 (OSS)
- 3<sup>rd</sup> Party 소프트웨어 (상용)

- 왜 필요한가?

- 소프트웨어 버전 전반에 걸쳐 SDLC 내에서 테스트 데이터의 유지 및 의사소통을 목적
- 소프트웨어 규정 준수
- 보안 위험의 설명, 공유 및 모니터링하는 방식의 혁신



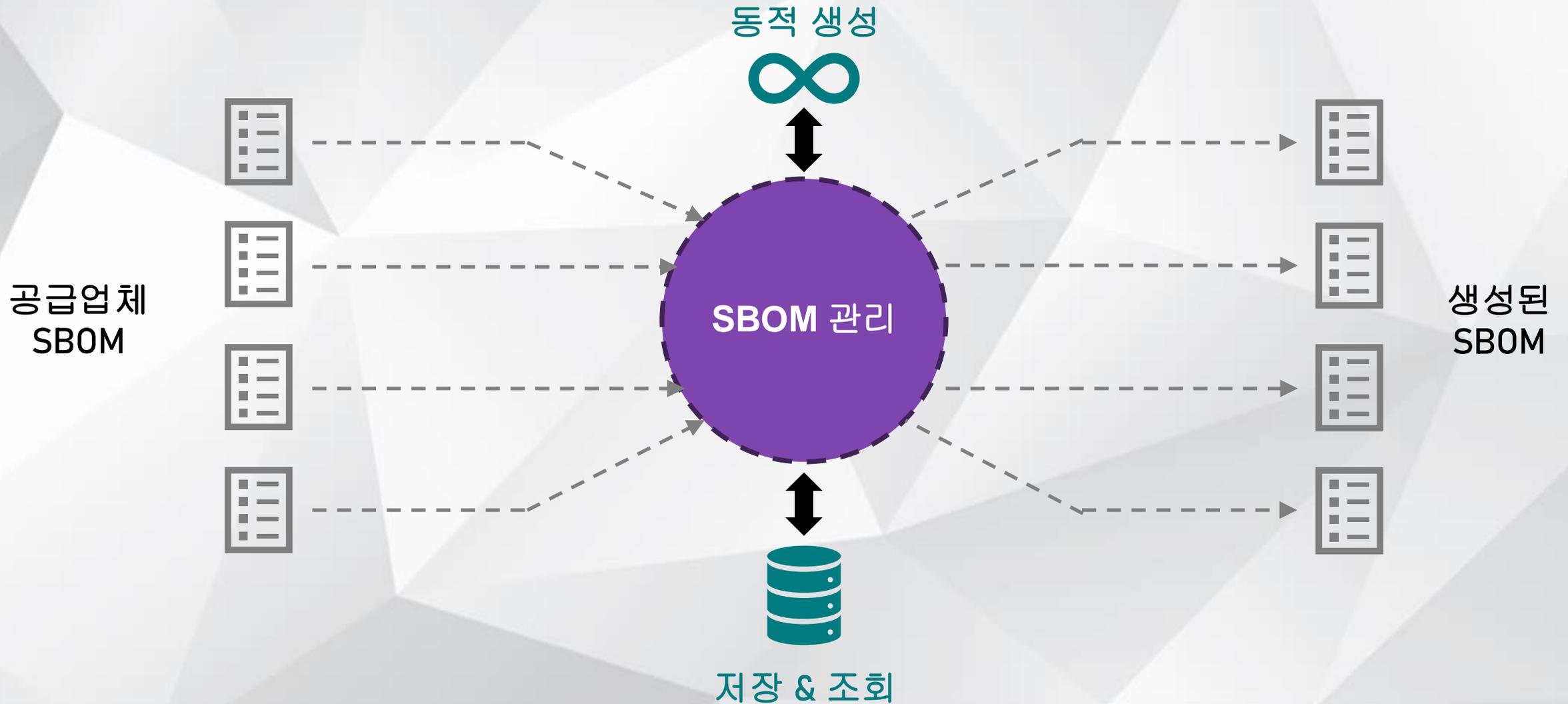
# 소프트웨어 자재 명세서 (SBOM - Software Bill of Materials )

- SBOM 포함 정보
  - Supplier name (컴포넌트 버전)
  - Component name (컴포넌트 이름)
  - Unique identifier (고유식별자)
  - Version string (버전)
  - Relationship (종속관계)
  - Author name (작성자 이름)
  - Timestamp (타임스탬프)
- SBOM 표준 형식
  - SPDX
  - Cyclone DX
- NTIA
  - Minimum fields

\* 데이터필드에는 추적 및 유지 관리해야 하는 각 구성 요소에 대한 기준 정보가 포함

\* 취약점 및 운영 정보는 최소 SBOM 정보에는 포함되어 있지 않고 필요시 취약점/라이선스 데이터베이스에 매핑 할 수 있는 최소 정보 제공

# 지속적인 공급망 가시성 확보



감사합니다.