SYNOPSYS®

오픈소스 소프트웨어 위험관리 전략

Synopsys Korea - Software Integrity Group
정성훈 부장

목차

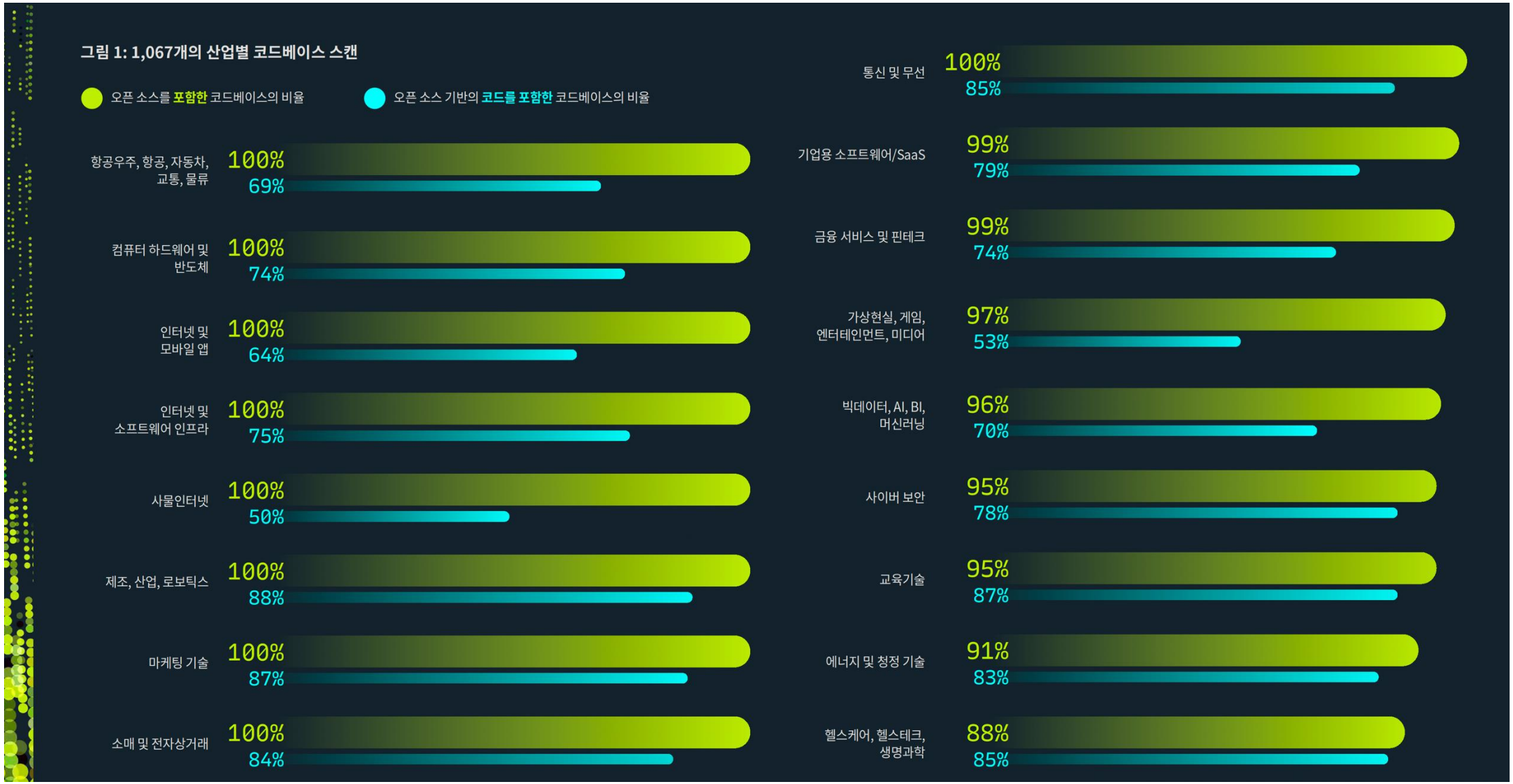
- 왜 오픈소스 소프트웨어에 주목해야 할까요?
- 관리되지 않는 오픈소스 소프트웨어 사용의 위험성
- 국내외 오픈소스 보안 동향
- 오픈소스 소프트웨어 관리를 위한 모범 사례

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

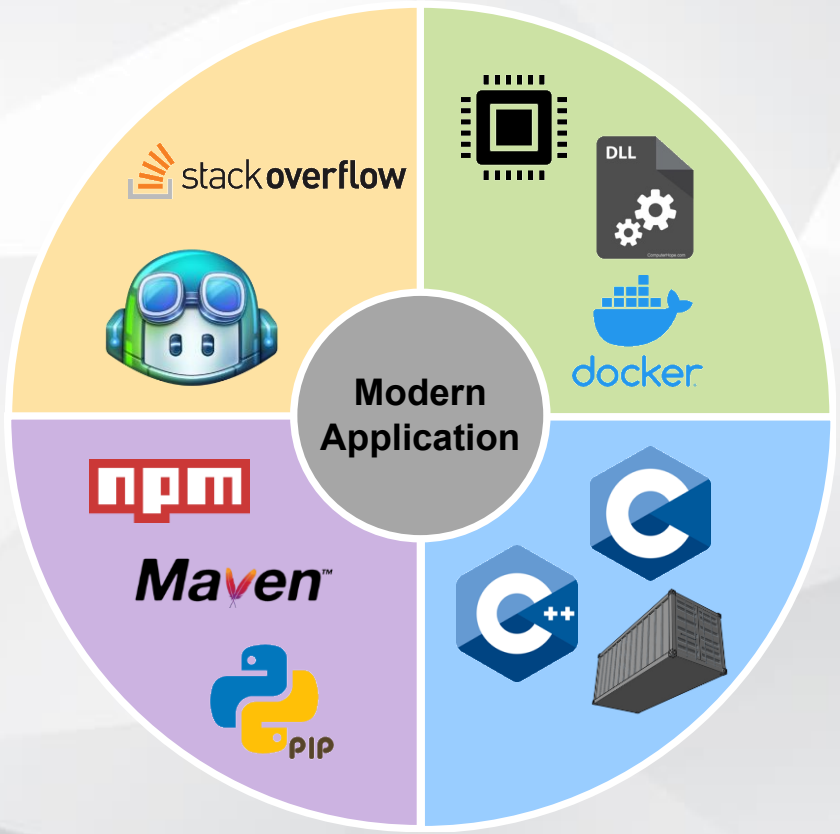
모든 산업은 오픈 소스를 기반으로 합니다.



오픈 소스를 포함시킬 수 있는 다양한 방법

코드 조각

패키지 매니저



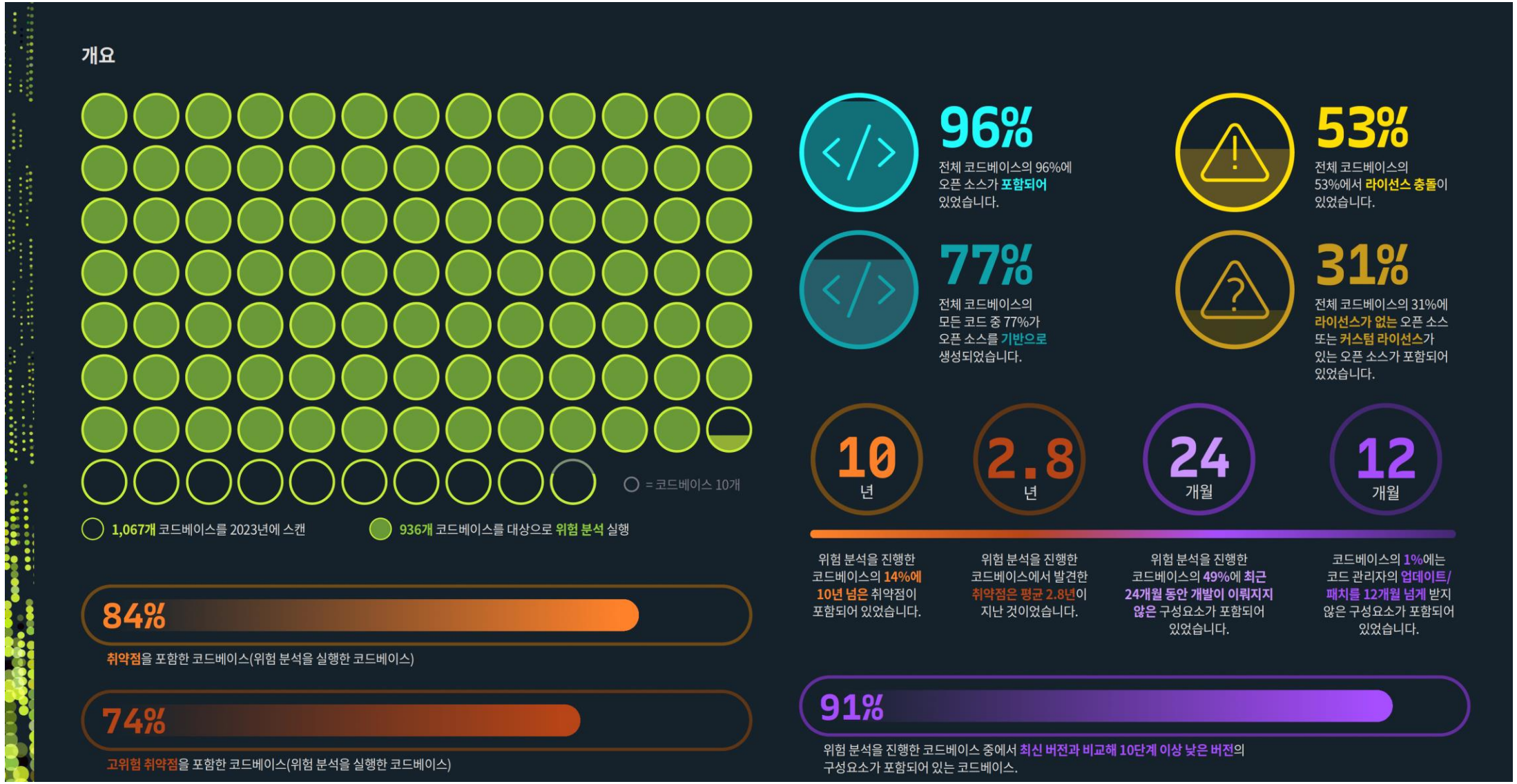
바이너리,라이브러리, 아티팩트, 컨테이너

패키지 매니저에 없는 의존성

관리되지 않는 오픈소스 소프트웨어 사용의 위험성

소프트웨어 공급망 보안을 최우선으로 고려해야 합니다.

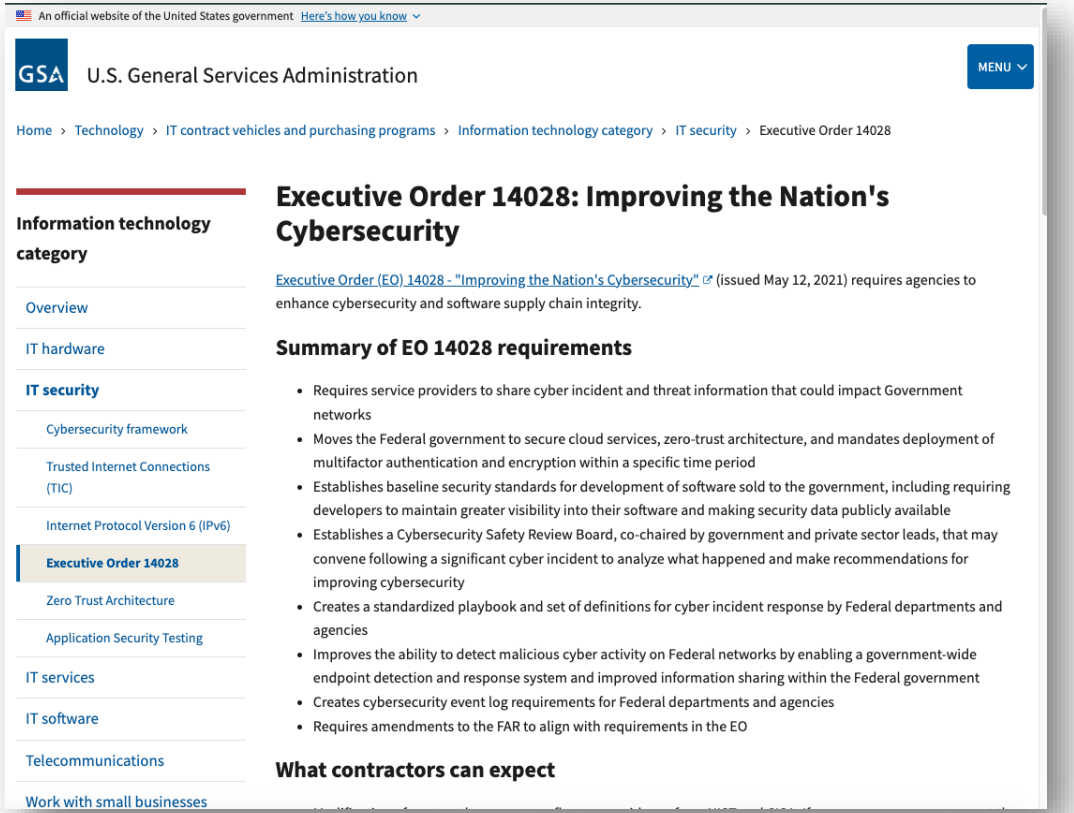
OSSRA 리포트 요약



국내외 오픈소스 보안 동향

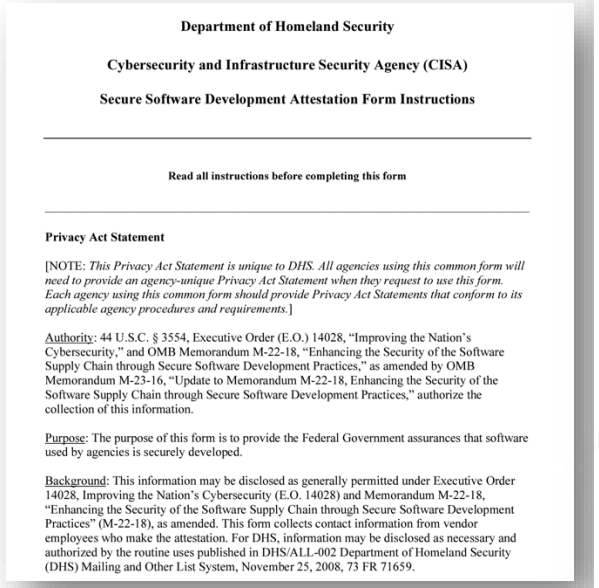
국제 오픈소스 보안 동향

- 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



Department of Homeland Security

Cybersecurity and Infrastructure Security Agency (CISA)

Secure Software Development Attestation Form Instructions

Read all instructions before completing this form

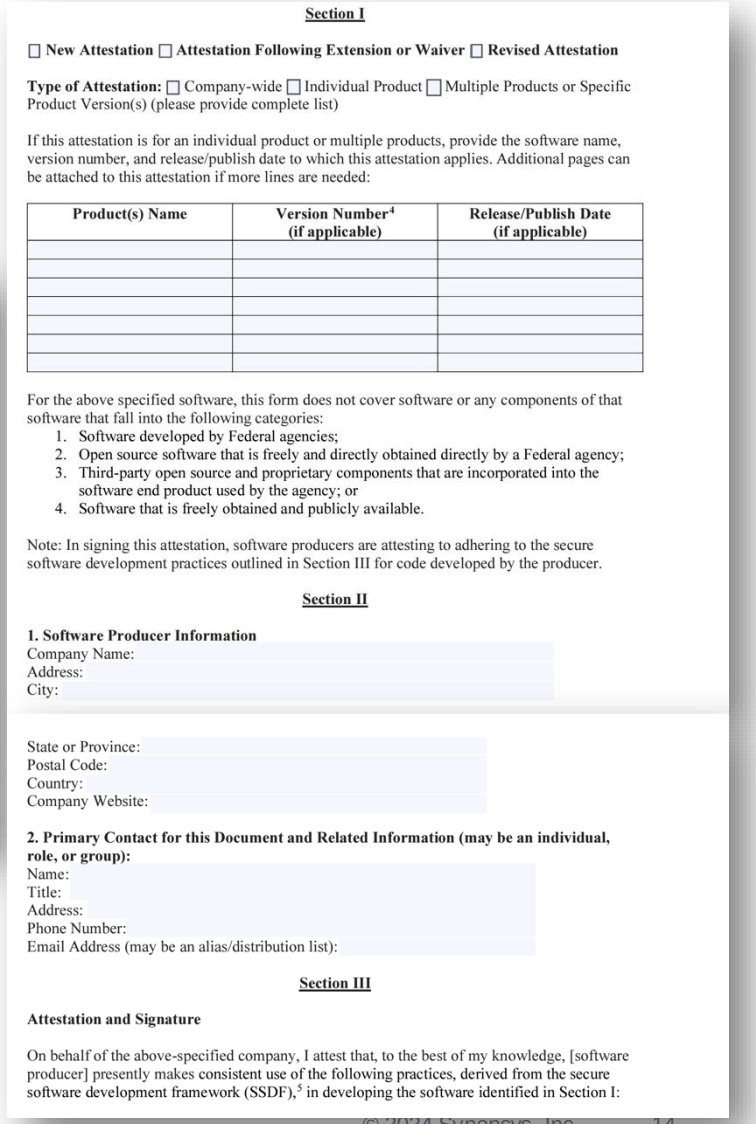
Privacy Act Statement

[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[4] (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

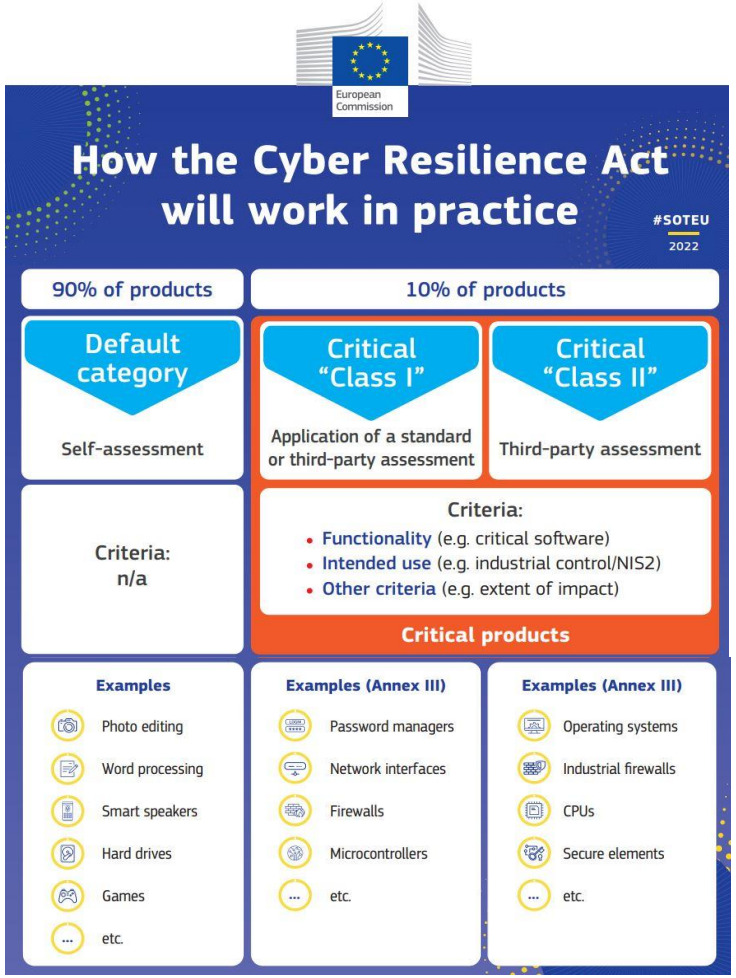
On behalf of the above-specified company, I attest that, to the best of my knowledge, [software producer] presently makes consistent use of the following practices, derived from the secure software development framework (SSDF),[5] in developing the software identified in Section I:

OMB: 관리예산처

CISA: 사이버보안 및 인프라 보안국

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

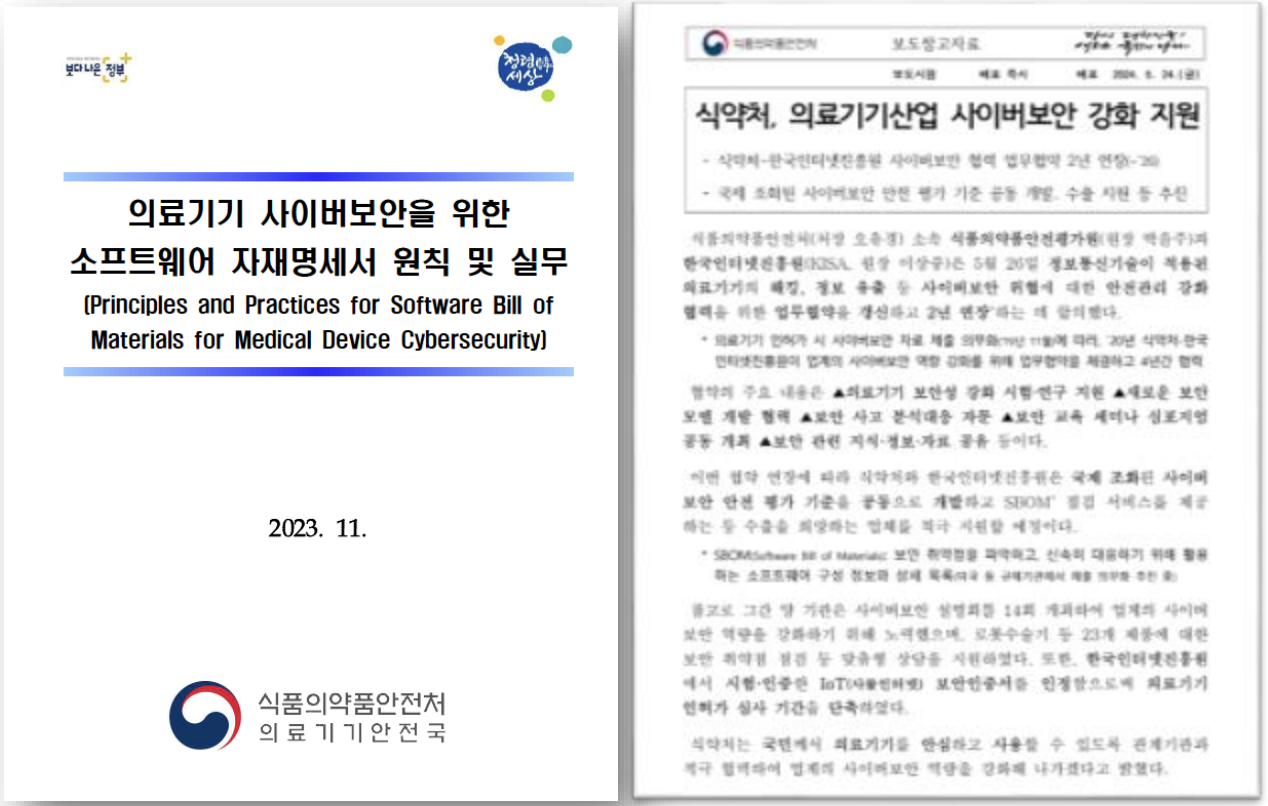


국내 오픈소스 보안 동향 – TTA

- 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

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



보다나은 정부

의료기기 사이버보안을 위한
소프트웨어 자재명세서 원칙 및 실무
(Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity)

2023. 11.

식품의약품안전처
의료기기안전국

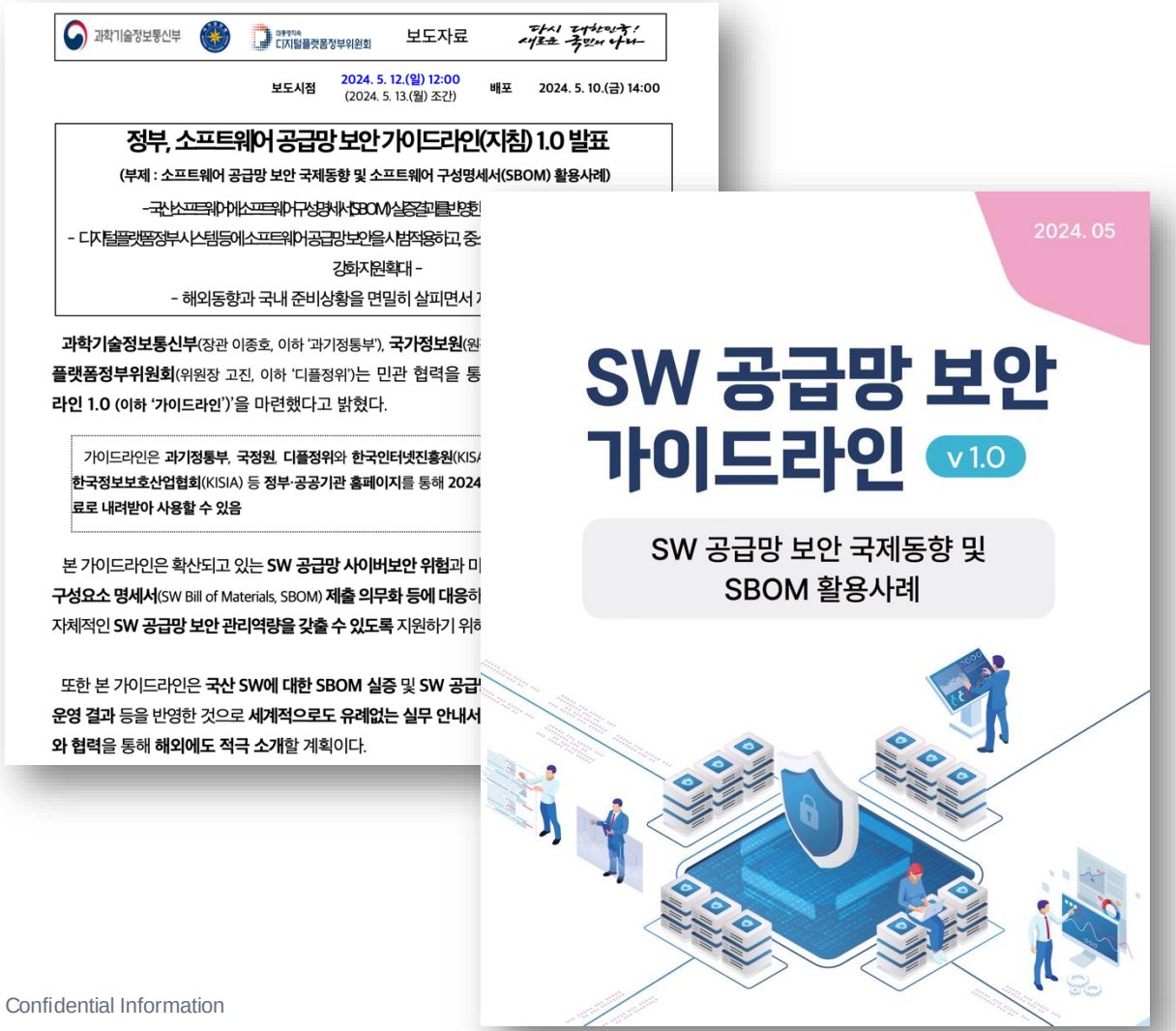
보도참고자료

식약처, 의료기기산업 사이버보안 강화 지원

- 식약처-한국인터넷진흥원 사이버보안 협력 업무협약 2년 연장(~'26)
- 국제 조화된 사이버보안 안전 평가 기준 공동 개발, 수출 지원 등 추진

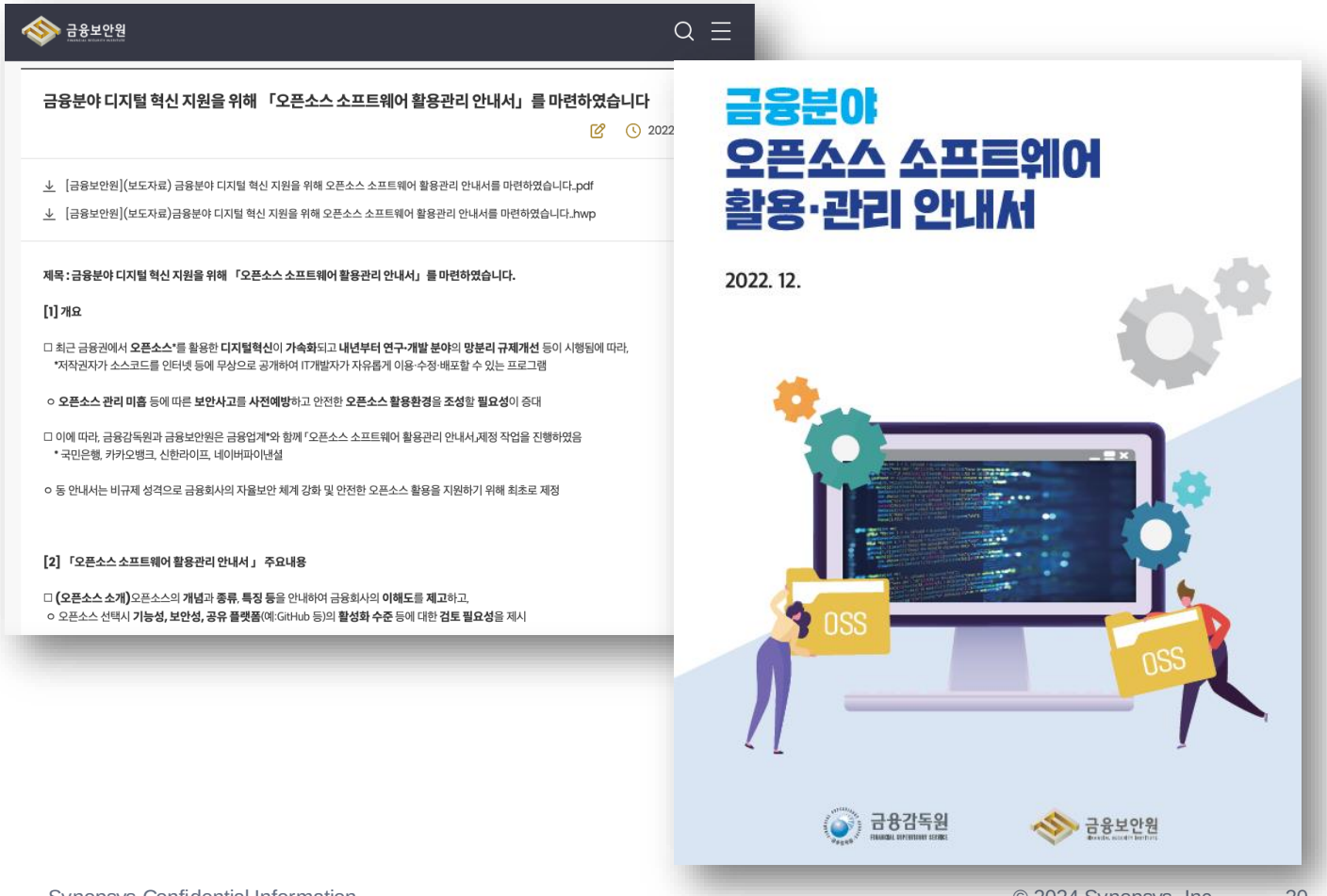
국내 오픈소스 보안 동향 - 정부

- 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)



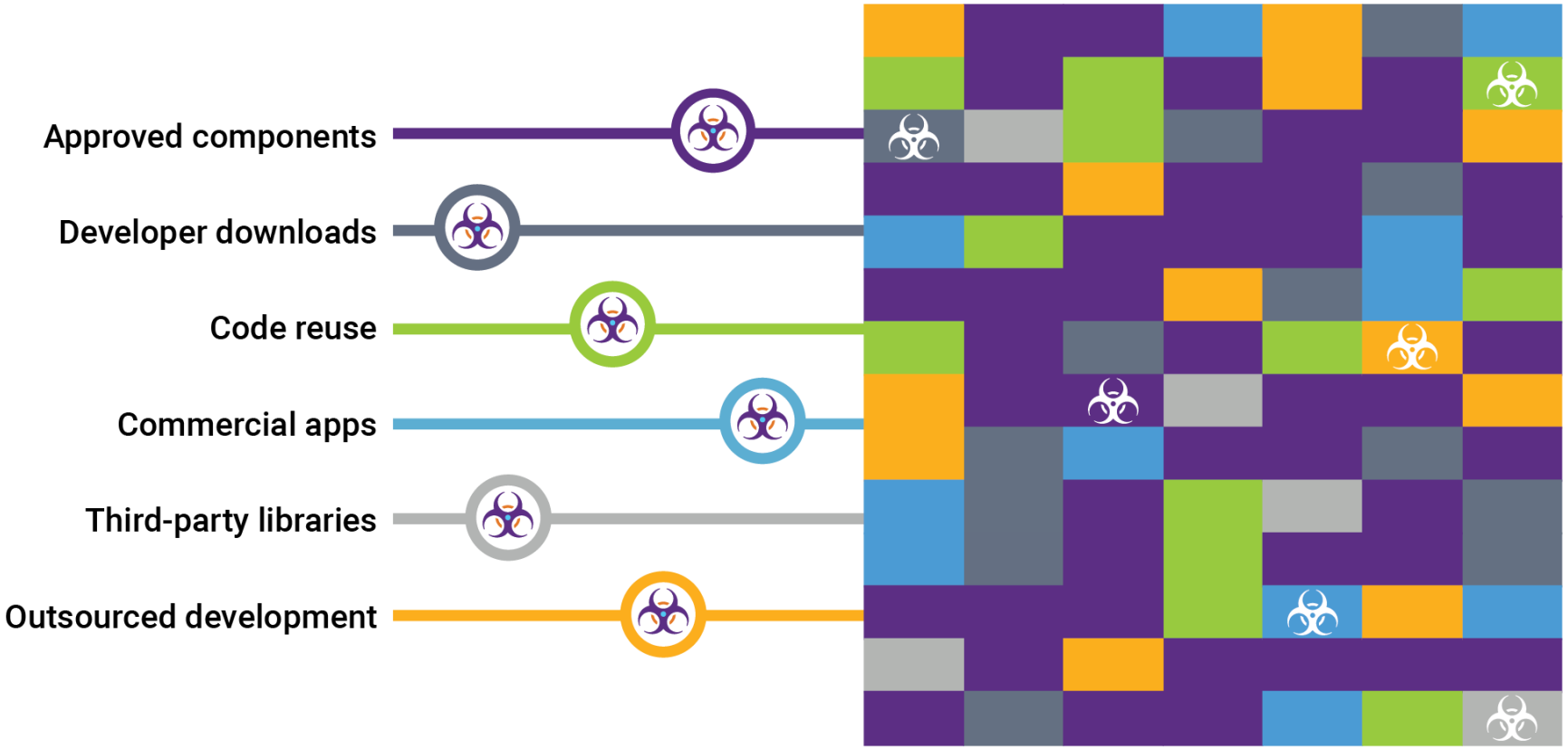
국내 오픈소스 보안 동향 - 금융보안원

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

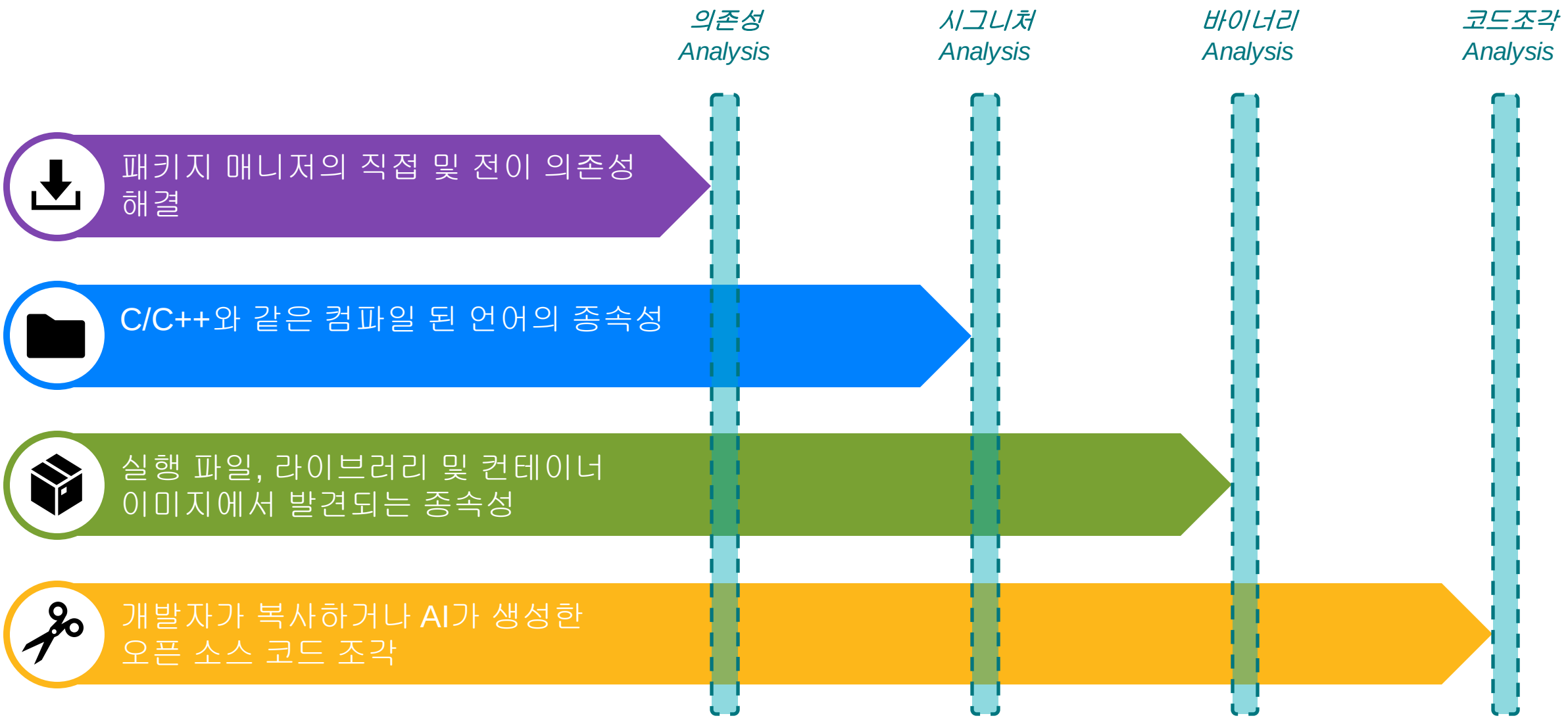


오픈 소스 관리를 위한 모범 사례

현대 애플리케이션 구성의 복잡성

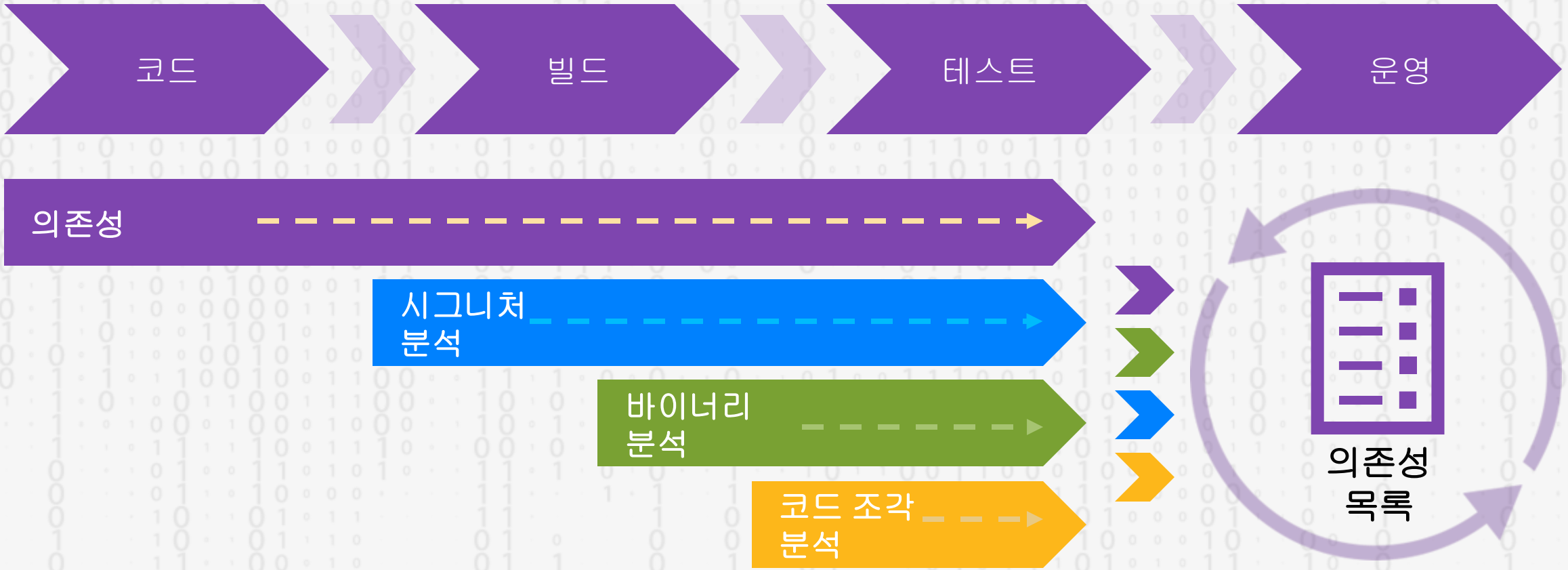


SCA를 통한 가시성 확보

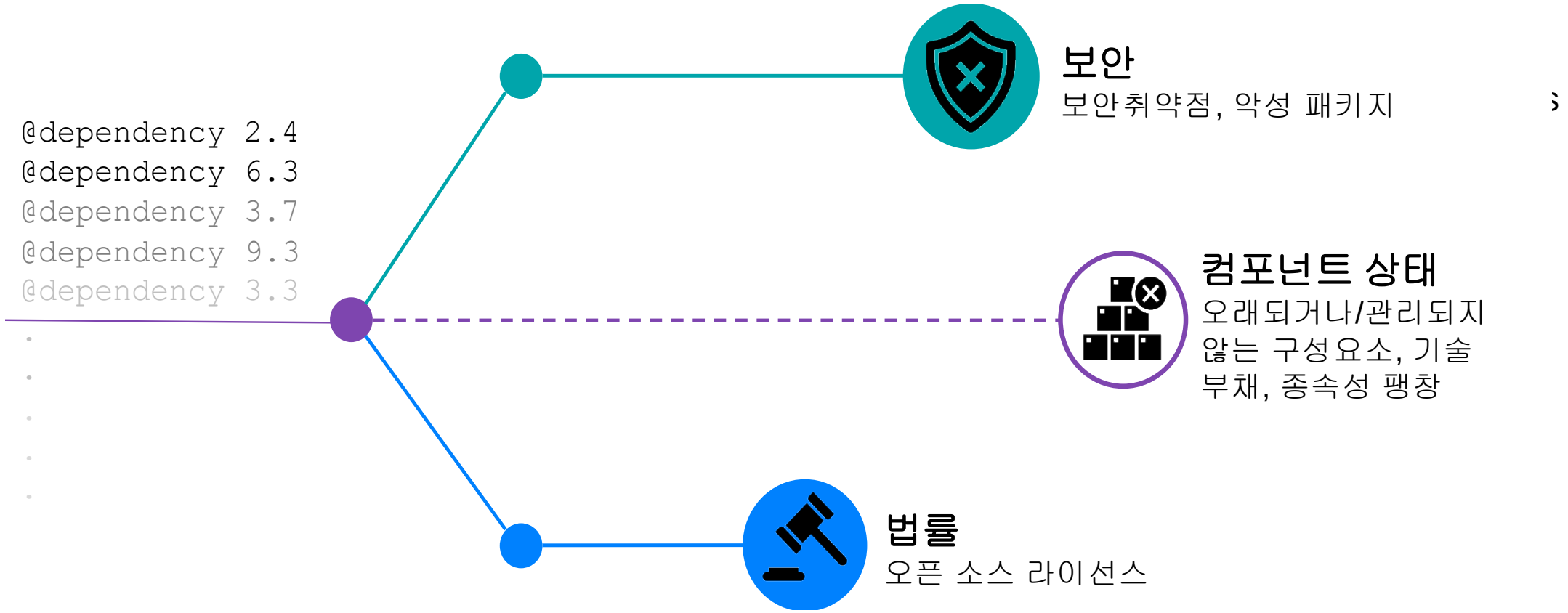


SDLC에 종속성 분석 과정을 구축

효율성과 정확성을 고려한 합리적 운영



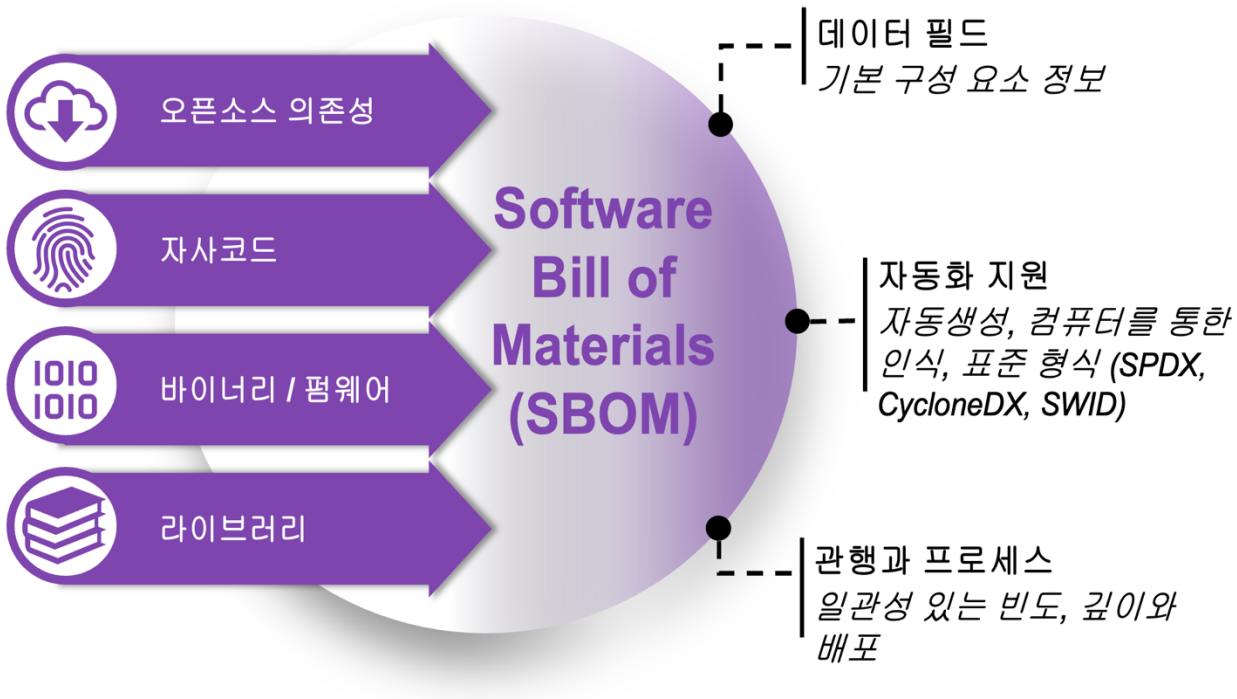
포괄적인 목록 구성을 통한 위험 관리



소프트웨어 자재 명세서 (SBOM - Software Bill of Materials)

- 소프트웨어 재료 목록 (구성요소)
  - 자체개발 코드
  - 오픈소스 소프트웨어 (OSS)
  - 3rd Party 소프트웨어 (상용)

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



소프트웨어 자재 명세서 (SBOM - Software Bill of Materials)

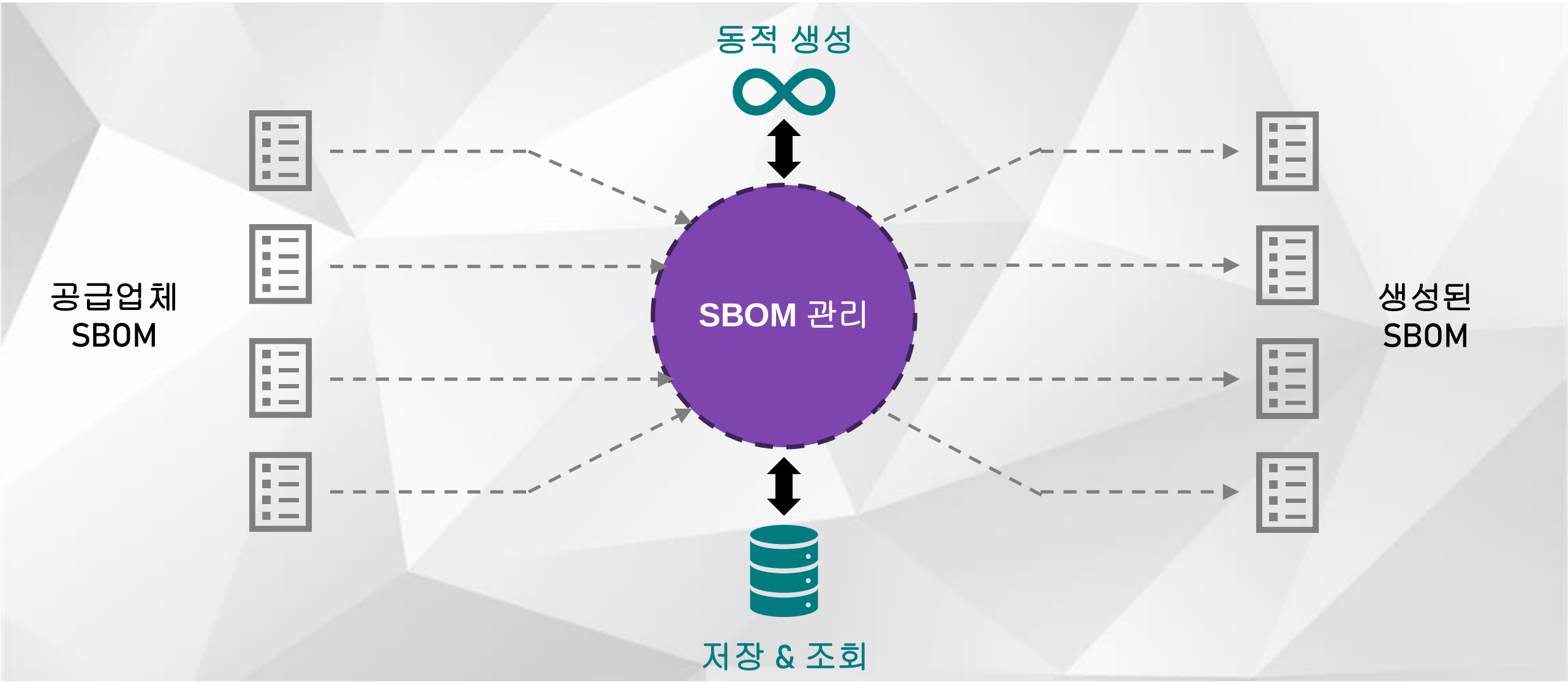
- SBOM 포함 정보
  - Supplier name (컴포넌트 버전)
  - Component name (컴포넌트 이름)
  - Unique identifier (고유식별자)
  - Version string (버전)
  - Relationship (종속관계)
  - Author name (작성자 이름)
  - Timestamp (타임스탬프)

- 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



SYNOPSYS®

감사합니다.