

SYNOPSYS®

Open Source Management Points in Software Supply Chain

What requires to SCA(Software Composition Analysis)

Byeoung-Joo Je | Sales Engineer Manager

Sep 14, 2023



미국 유럽의 사이버보안 규제

USA – Executive Order 14028

THE WHITE HOUSE

Administration | Priorities | The Record | Briefing Room | Español

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM | PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

EU – Cyber Resilience Act

European Commission

English

Shaping Europe's digital future

Home | Policies | Activities | News | Library | Funding | Calendar | Consultations

Home > Policies > EU Cyber Resilience Act

EU Cyber Resilience Act

New EU cybersecurity rules ensure safer hardware and software.

From baby-monitors to smart-watches, products and software that contain a digital component are omnipresent in our daily lives. Less apparent to many users is the security risk such products and software may present.

The Commission's [proposal for a new Cyber Resilience Act \(CRA\)](#) aims to safeguard consumers and businesses buying or using products or software with a digital component. The Act would see inadequate security features become a thing of the past with the introduction of mandatory cybersecurity requirements for manufacturers and retailers of such products, with this protection extending throughout the product lifecycle.

The problem addressed by the proposed regulation is two-fold. First is the inadequate level of cybersecurity inherent in many products, or inadequate security updates to such products and software. Second is the inability of consumers and businesses to currently determine which products are cybersecure, or to set them up in a way that ensures their cybersecurity is protected.

The proposed Cyber Resilience Act would guarantee:

EU Cyber Resilience Act
For safer & more secure digital products
© European Union

Proposed Regulation - Cyber Resilience Act

Factsheet - Cyber Resilience Act

자동차 시장의 사이버보안 규제

WP-29 – UN Regulation No. 155

E/ECE/TRANS/505/Rev.3/Add.154

4 March 2021

Agreement

Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations*


(Revision 3, including the amendments which entered into force on 14 September 2017)

Addendum 154 – UN Regulation No. 155

Date of entry into force as an annex to the 1958 Agreement: 22 January 2021

Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2020/79 (as amended by ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97).



UNITED NATIONS

ISO/SAE – 21434:2021

ISO Standards About us News Taking part Store

ICS ← 43 ← 43.040 ← 43.040.15

ISO/SAE 21434:2021

Road vehicles — Cybersecurity engineering

[Preview](#)

Abstract

This document specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces.

A framework is defined that includes requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risk.

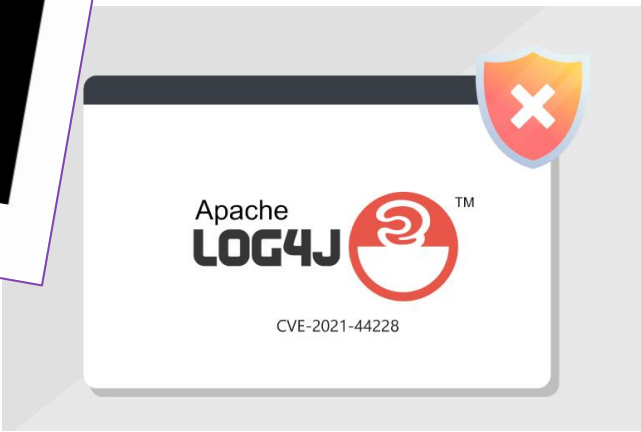
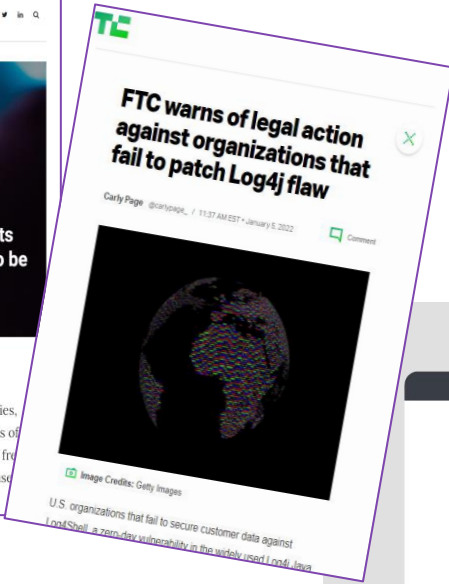
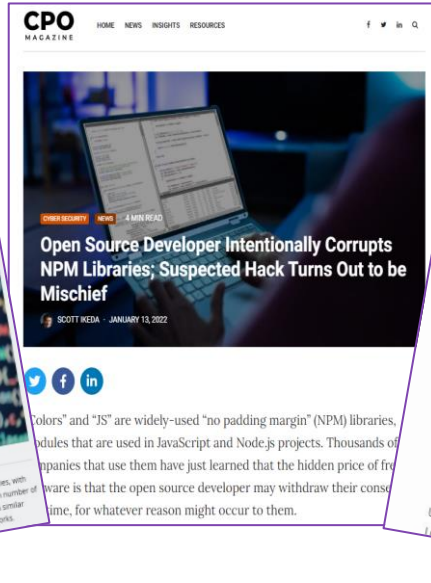
This document is applicable to series production road vehicle E/E systems, including their components and interfaces, whose development or modification began after the publication of this document.

This document does not prescribe specific technology or solutions related to cybersecurity.

General information

Status : Published	Publication date : 2021-08
Edition : 1	Number of pages : 81
Technical Committee : ISO/TC 22/SC 32 Electrical and electronic components and general system aspects	
ICS : 43.040.15 Car informatics. On board computer systems	

왜 사이버보안 규제를 강화할까요?



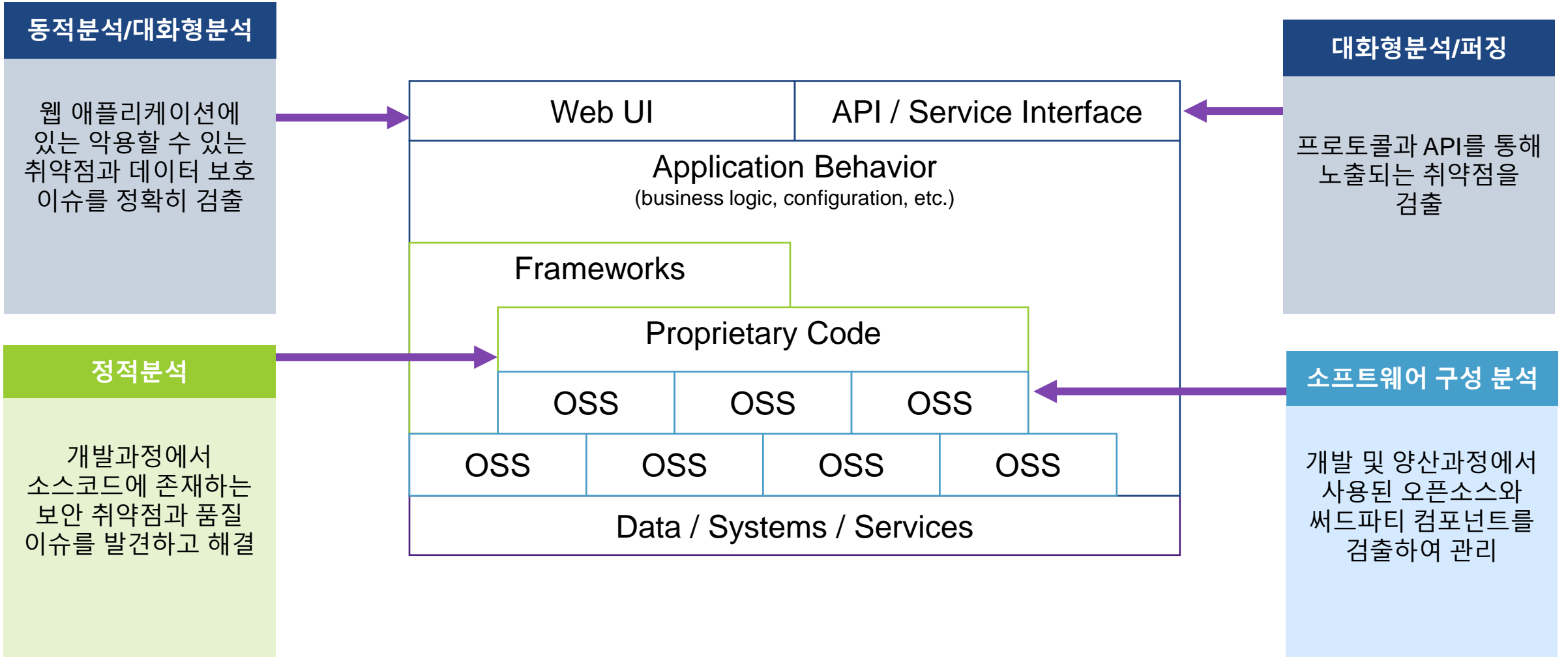
소프트웨어 공급망이
사이버보안에서 가장
취약한 고리입니다.

작년 한 해 동안 61%의
사업이 소프트웨어
공급망 위협으로
피해를 입었습니다.

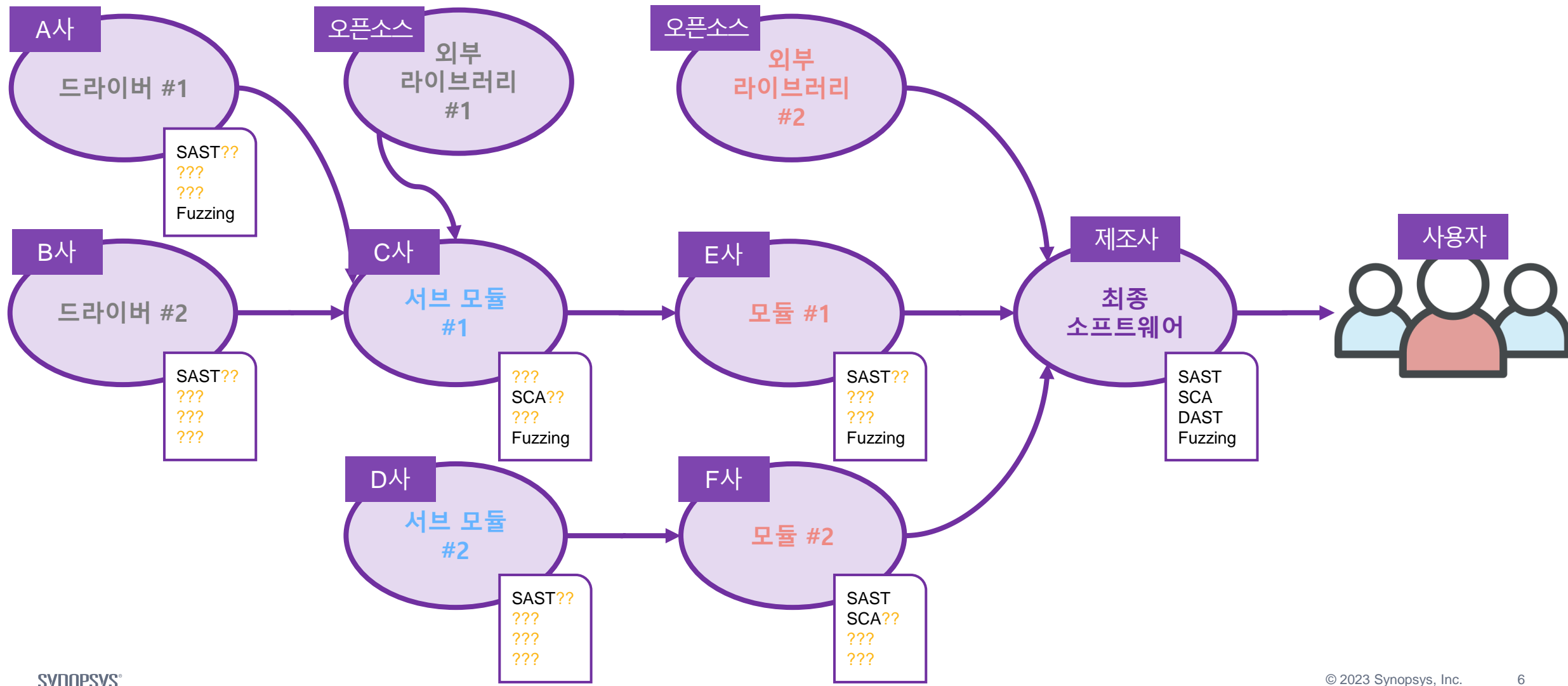
출처:

<https://www.capterra.com/resources/software-supply-chain-attacks/>

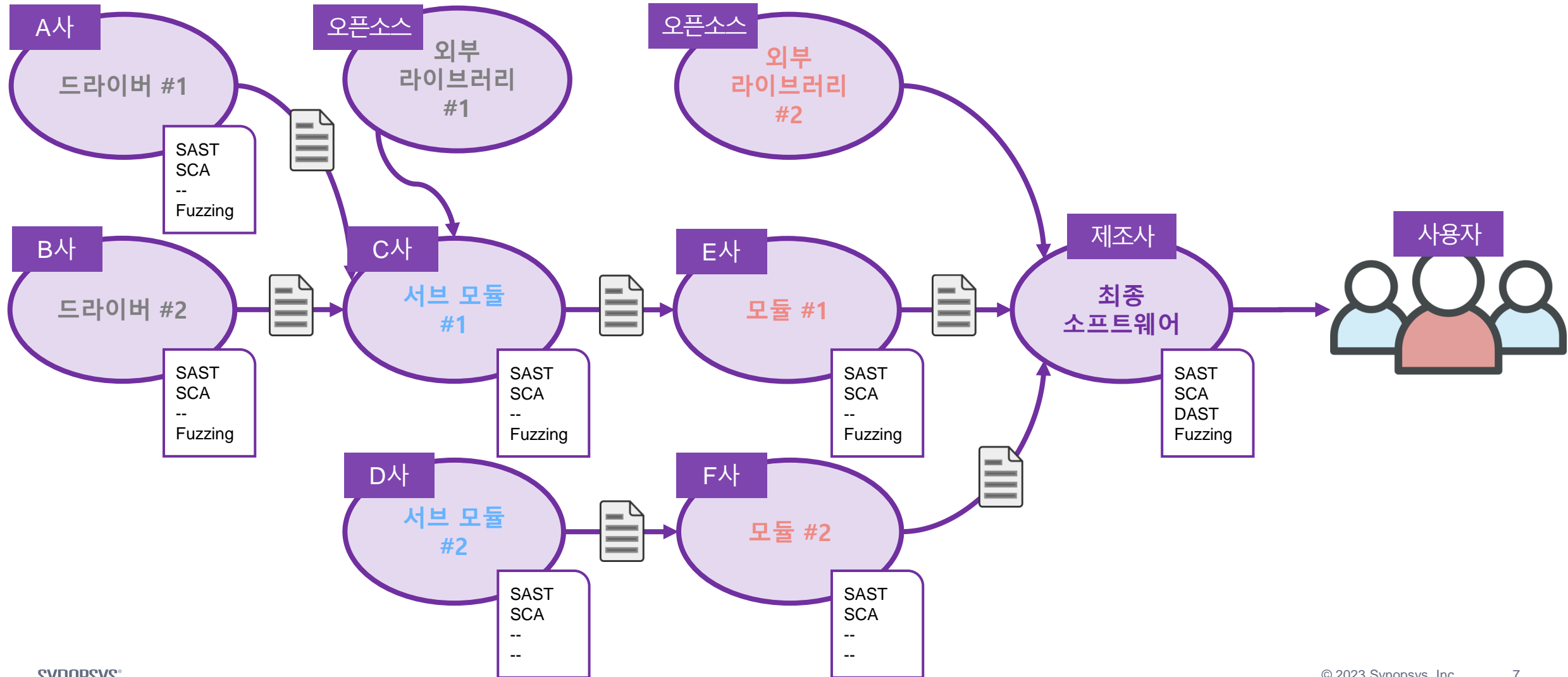
한 회사내의 프로젝트에 대한 사이버보안 대응



소프트웨어 공급망(SSC)에서는...



소프트웨어 공급망(SSC)에서는...



사이버보안 강화를 위한 조치

SSC에서 SAST/DAST/SCA/IAST/Fuzzing 등 Application Security Testing을 강화하고 준수

NIST – IR 8397

2 Recommended Minimum Standard for Developer Testing	4
2.1 Threat Modeling	5
2.2 Automated Testing	6
2.3 Code-Based, or Static, Analysis	6
2.4 Review for Hardcoded Secrets	7
2.5 Run with Language-Provided Checks and Protection	7
2.6 Black Box Test Cases	7
2.7 Code-Based Test Cases	8
2.8 Historical Test Cases	8
2.9 Fuzzing	8
2.10 Web Application Scanning	8
2.11 Check Included Software Components	9

Guidelines on Minimum Standards for Developer Verification of Software
<https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8397.pdf>

FDA – Cybersecurity in Medical devices

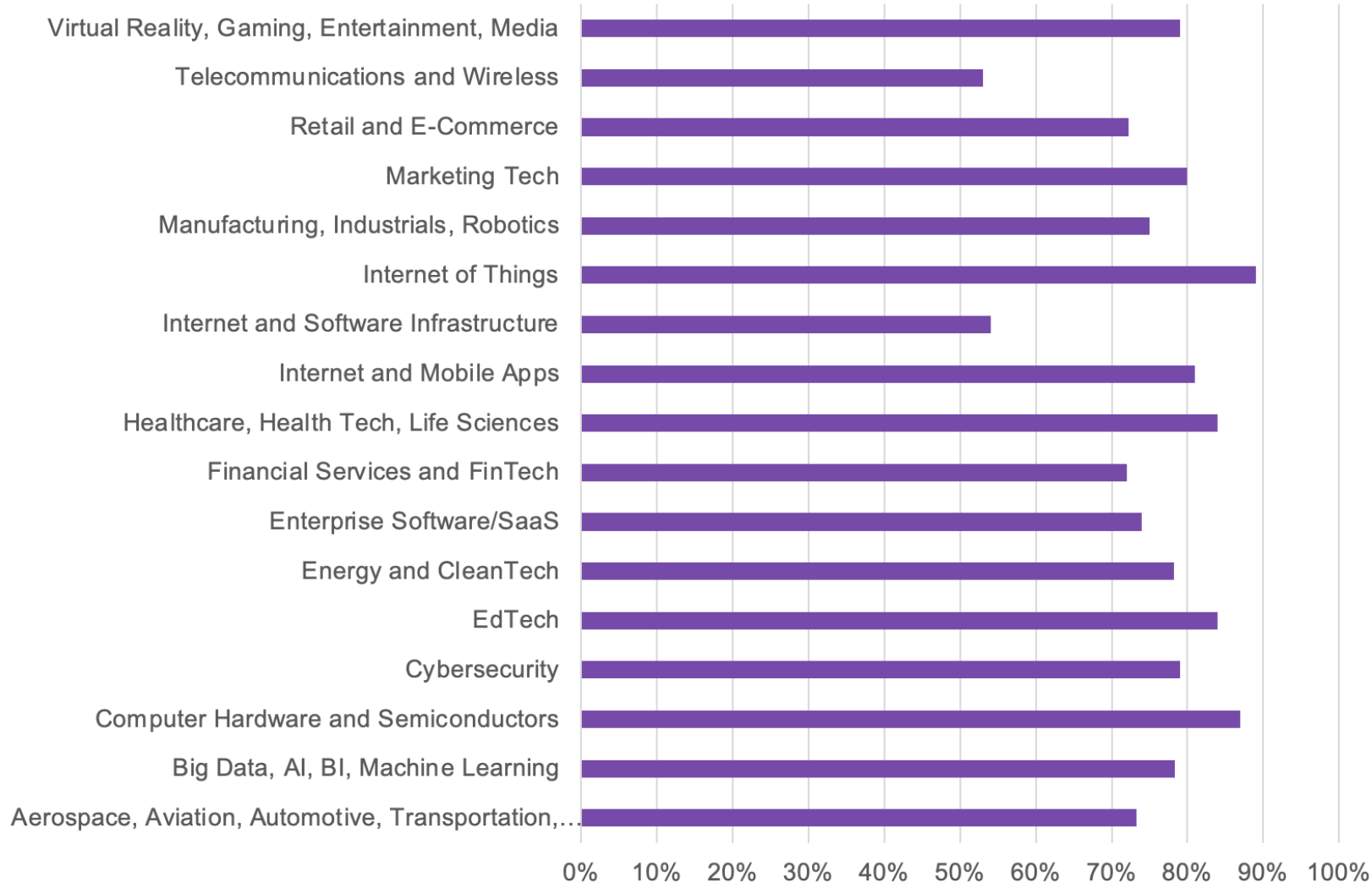
C. Cybersecurity Testing

805	
806	
807	As with other areas of product development, testing is used to demonstrate the effectiveness of
808	design controls. While software development and cybersecurity are closely related disciplines,
809	cybersecurity controls require testing beyond standard software verification and validation
810	activities to demonstrate the effectiveness of the controls in a proper security context to therefore
811	demonstrate that the device has a reasonable assurance of safety and effectiveness.
840	c. Vulnerability Testing (such as section 9.4 of ANSI/ISA 62443-4-1)
841	o Manufacturers should provide details and evidence ⁴⁶ of the following testing
842	pertaining to known vulnerabilities:
843	▪ Abuse case, malformed, and unexpected inputs,
844	• Robustness
845	• Fuzz testing
846	▪ Attack surface analysis,
847	▪ Vulnerability chaining,
848	▪ Closed box testing of known vulnerability scanning,
849	▪ Software composition analysis of binary executable files, and
850	▪ Static and dynamic code analysis, including testing for credentials that are
851	“hardcoded,” default, easily-guessed, and easily compromised.

<https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions>

**왜 오픈소스가
소프트웨어 공급망 위험 관리에서
중요할까요?**

Percentage of Codebases That Is Open Source



76%

전체 프로젝트 코드
중 오픈 소스
코드의 평균적인 양

96%

상용 프로젝트가
오픈 소스를 포함

참조: 2023 Open Source Software Risk Analysis Report <https://www.synopsys.com/ko-kr/software-integrity/em/ossra.html>

OSSRA 리포트

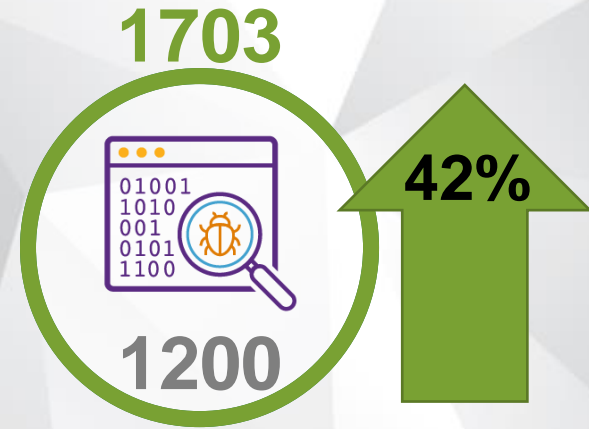
- 상업용 프로젝트 코드에서 오픈 소스의 사용 양상에 대해 조사
- 2018년부터 매년 발행
- 시놉시스 SIG의 CyRC(Cybersecurity Research Center)에서 담당



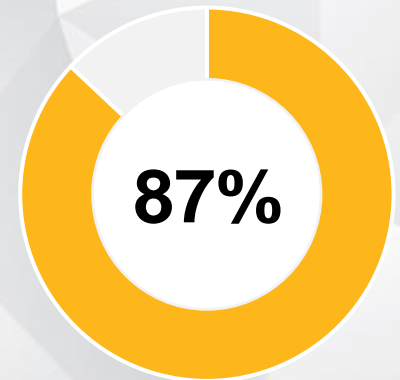
OSSRA 리포트의 데이터 소스

M&A로 인한 1703 개 프로젝트에 대한 감사

Industry	Distribution
Enterprise Software/SaaS	29%
Financial Services & FinTech	11%
Big Data, AI, BI, Machine Learning	10%
Healthcare, Health Tech, Life Sciences	9%
Internet and Mobile Apps	7%
Internet & Software Infrastructure	6%
Marketing Tech	5%
Retail & E-Commerce	5%
Manufacturing, Industrials, Robotics	4%
Cybersecurity	3%
Virtual Reality, Gaming, Entertainment, Media	2%
Telecommunications & Wireless	2%
Aerospace, Aviation, Automotive, Transportation, Logistics	2%
EdTech	2%
Internet of Things	2%
Energy & CleanTech	1%
Computer Hardware & Semiconductors	1%



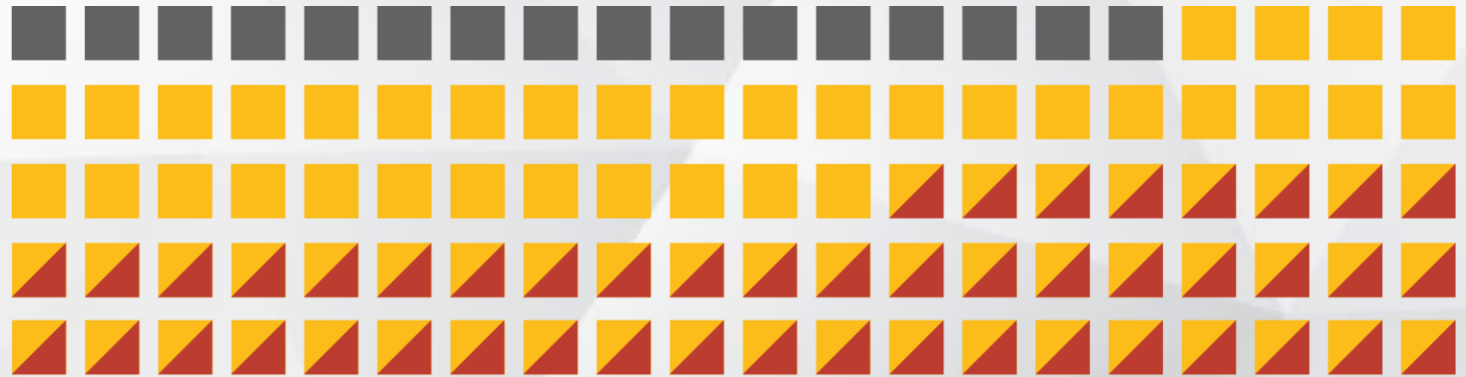
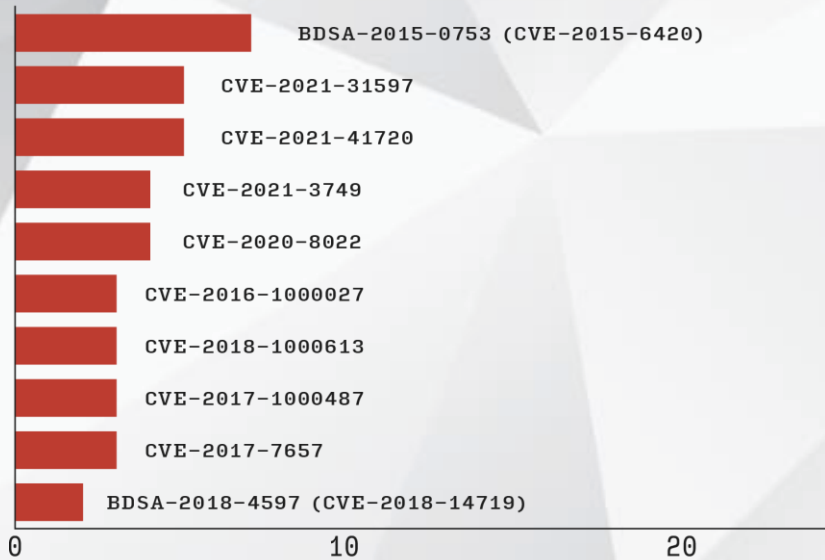
2019년 대비 감사 대상
프로젝트의 성장



위험도 평가도 같이 수행한
프로젝트

오픈소스에서 이미 알려진 보안 취약점의 현황은...


High-Risk CVEs/BDSAs



84% of codebases scanned for risk assessment contained security vulnerabilities. **48%** of these contained high-risk vulnerabilities.

보안 취약점에 대해 자세히 들여다 봅시다

CVE-2015-6420: 7% 의 코드베이스에서 발견

 Black Duck Security Advisory
Apache Commons Collections (ACC) Library Vulnerable to Arbitrary Code Execution via Deserialization of Untrusted Input

BDSA | BDSA-2015-0753 | [CVE-2015-6420](#) | Published May 3, 2019 | Updated Apr 21, 2020

[Overview](#) | [Affected Projects](#) | [Technical](#) | [Components](#) | [CVE References](#)


CRITICAL 9.1
BDSA

Fix Available
Nov 20, 2015

Exploit Available
Jan 27, 2015

2,676 Days
Vulnerability Age

The apache commons collection (ACC) library, when utilized in an application that deserializes untrusted user input, is vulnerable to a remote attacker executing arbitrary code.

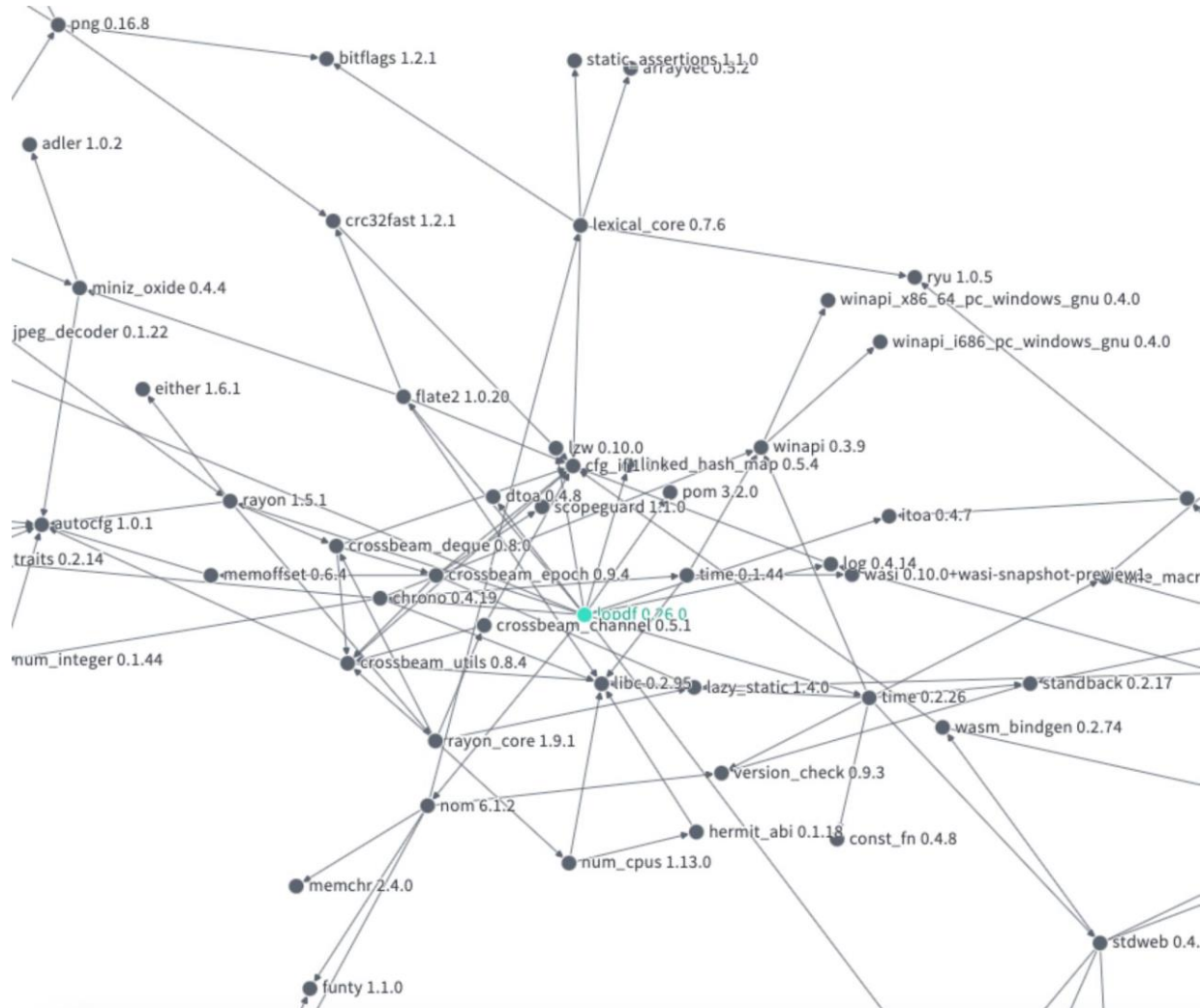
 **Zero-click Remote Code Execution**
This vulnerability can result in the execution of code on the system, triggered by a remote attacker without requiring or relying on any third party action.

Common Weakness Enumeration (CWE)

CWE-502 - Deserialization of Untrusted Data

The application deserializes untrusted data without sufficiently verifying that the resulting data will be valid.

“보이지 않는” 의존성



595

프로젝트 당
평균 오픈 소스
컴포넌트 개수

소프트웨어 공급망의 사이버보안을 위해
오픈소스는 어떻게 관리해야 할까요?



오픈소스 의존성



자사 코드



바이너리 / 펌웨어



라이브러리

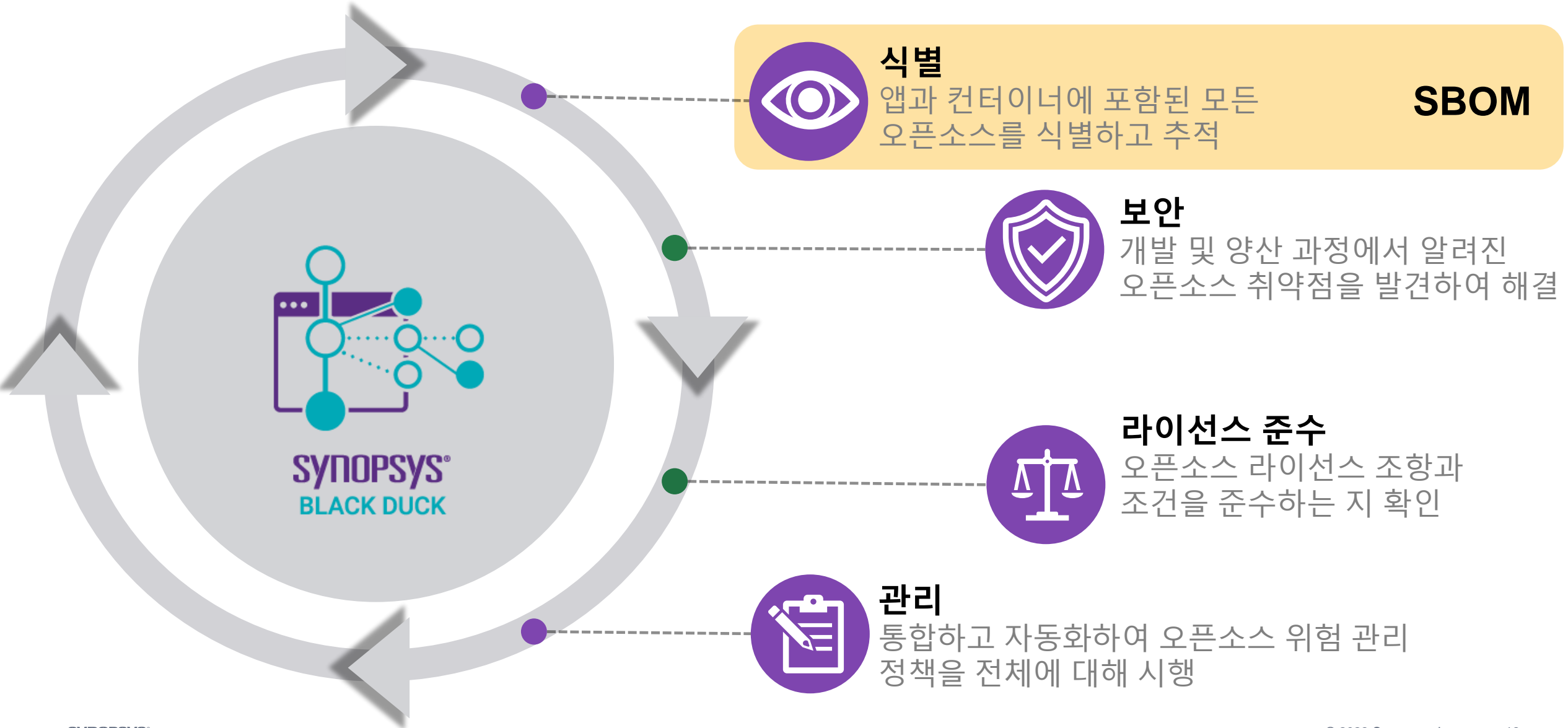
Software Bill of Materials (SBOM)

데이터 필드
기본 컴포넌트 정보

자동화 지원
자동 생성, 컴퓨터를 통한 인식,
표준형식 (SPDX, CycloneDX,
SWID)

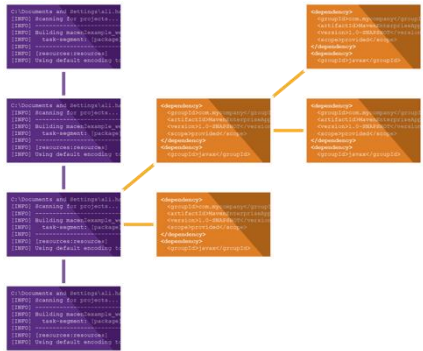
실행 및 프로세스
일관성 있는 빈도, 깊이 및 분포

SBOM은 SCA의 한 부분



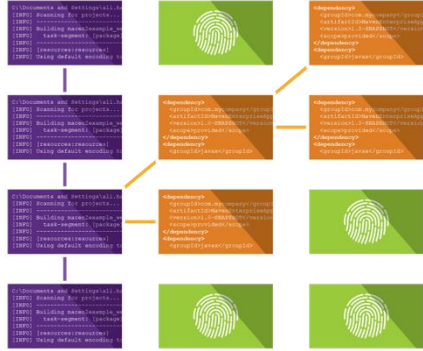
필요한 오픈소스 식별 방법 - Black Duck

의존성 분석



선언된 컴포넌트와 동적으로 빌드된 의존성들을 추적

코드프린트 분석



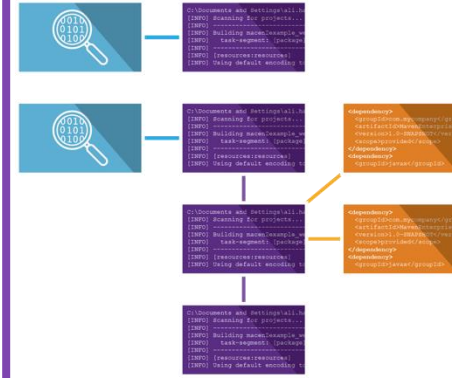
파일/디렉토리 메타데이터 & SHA파일 시그니처를 분석하여, 미선언, 수정, 부분적 오픈소스를 발견

스니펫 매칭



코드에 내장된 오픈소스 코드조각을 식별하여, 잠재적인 저작권 및 라이선스 의무사항을 찾아냄

바이너리 분석



소스코드 접근없이 컴파일된 소프트웨어, 펌웨어 혹은 설치 프로그램 등을 분석

커스텀 컴포넌트 분석



문자열 검색과 코드 프린트로 오픈소스가 아닌 내부 혹은 써드파티 상업용 컴포넌트 식별

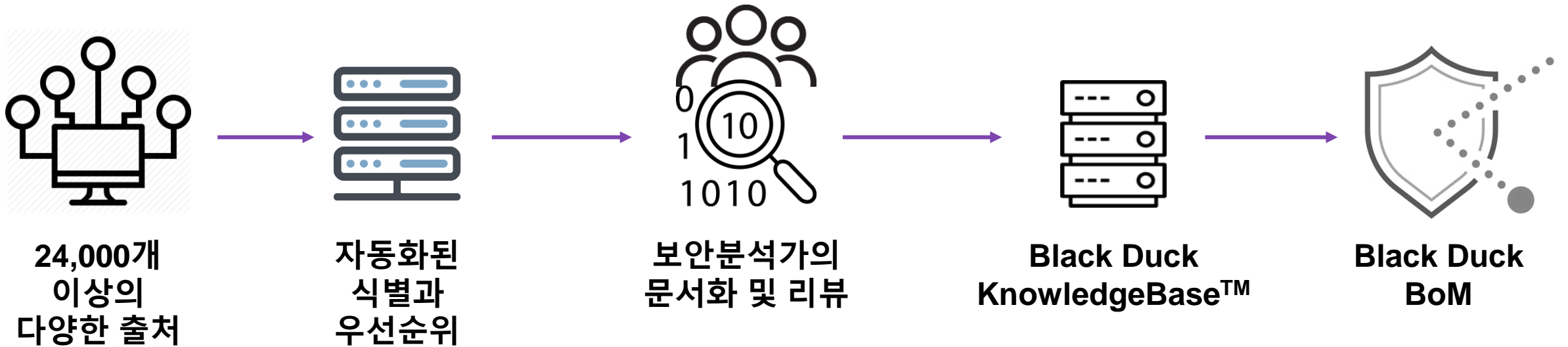
완벽한 소프트웨어 구성 명세서 (SBOM)

개발 파이프라인에서 SBOM 생성

Black Duck SCA



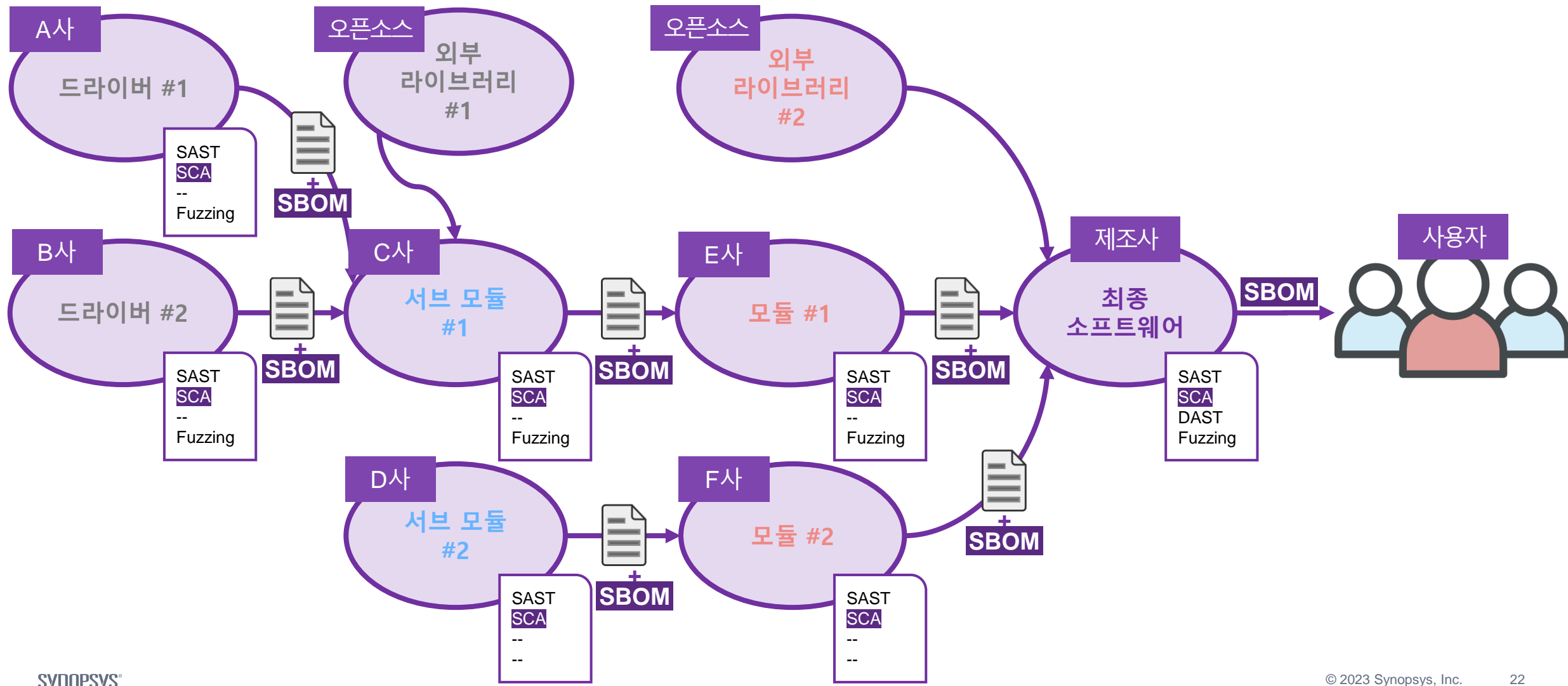
SBOM 컴퍼넌트를 Risk Insights에 연결



최초 취약점 출처에서 BOM에 업데이트까지 4 시간

BDSA는 NVD 보다 수 일 이상 빠르게 취약점을 업데이트

소프트웨어 공급망(SSC)에서 SBOM을 통한 오픈소스 관리



SBOM을 통한 오픈소스 가시성의 사례



이 컴포넌트를 사용하는가?

어떤 버전을 사용하는가?

자사 소프트웨어 중 어느 버전이 영향을 받는가?

취약점이 대중에 공개

가시성 미확보

어떻게 발생한 취약점을 해결해야 하는가?

실질적으로 취약점을 해결했는가?

SBOM을 통한 가시성 확보

가시성 확보

이 컴포넌트를 사용하는가?

어떤 버전을 사용하는가?

자사 소프트웨어 중 어느 버전이 영향을 받는가?

어떻게 발생한 취약점을 해결해야 하는가?

실질적으로 취약점을 해결했는가?

소프트웨어 공급망에서 오픈소스 보안은 모두의 몫!!!



It is your responsibility to track open source components, licenses, and vulnerabilities, and their associated risk, in your supply chain.

SBOM의 미래

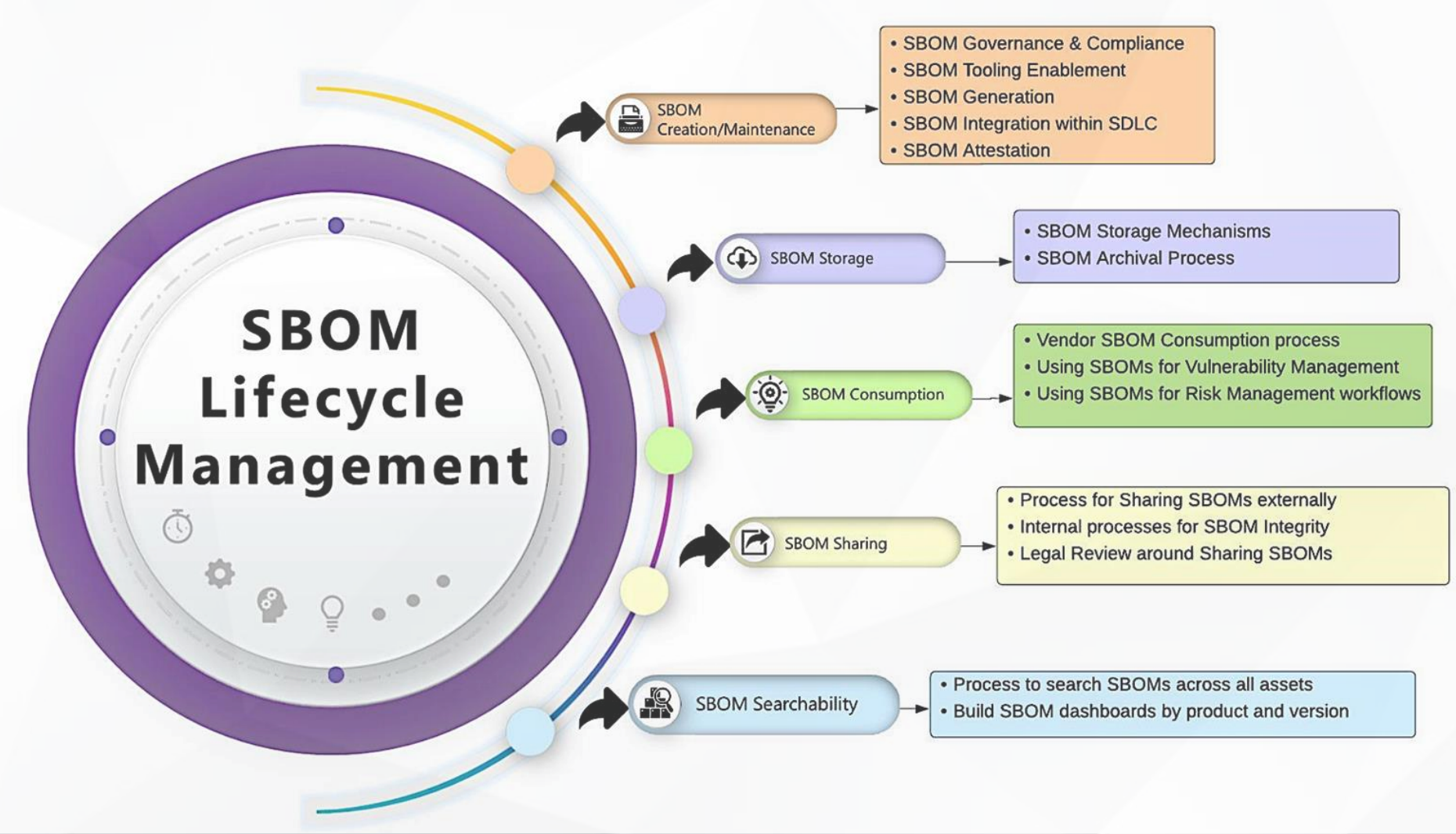


현재

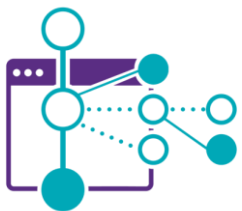
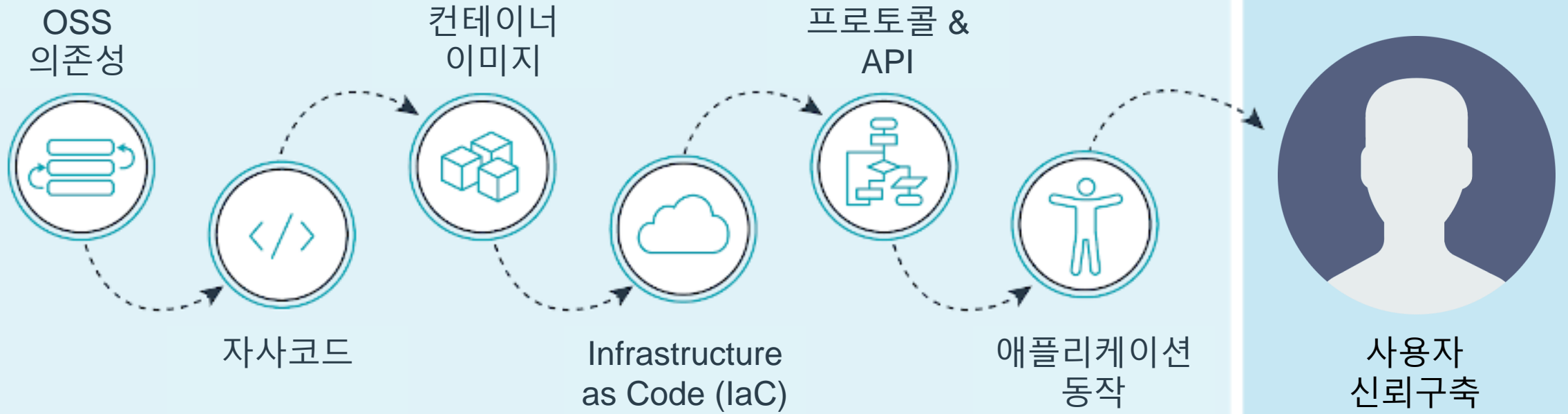
12-15 개월 후

18-24 개월 후

SBOM의 미래



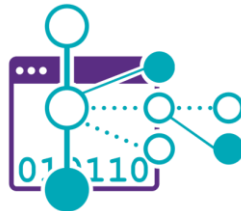
Trusted Software Supply Chain



Black Duck
SCA



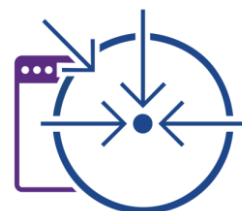
Coverity
SAST



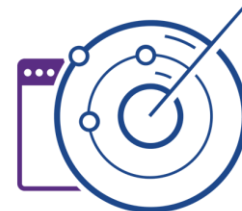
Black Duck
Binary



Rapid Scan
Static



Defensics &
WhiteHat
DAST



Seeker
IAST



Thank You

SYNOPSYS[®]