LGE OSPO

SW 공급망 보안 가이드라인 소개

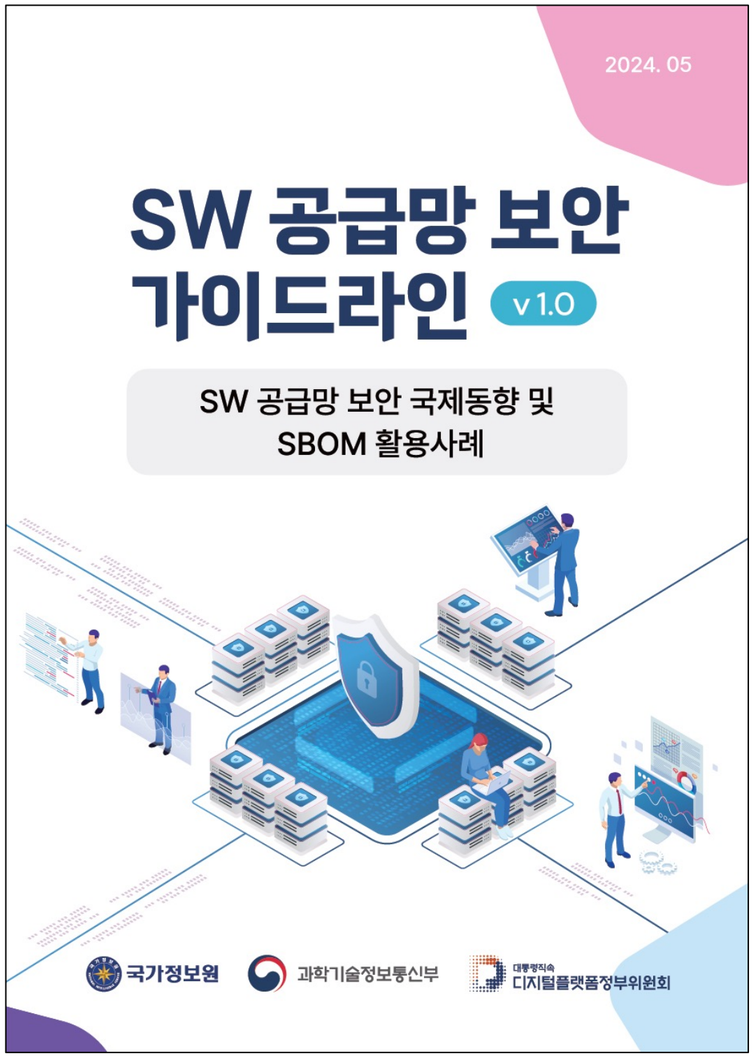
SW 공급망 보안 국제 동향 및 SBOM 활용 사례

LG전자 | SW센터 | 박 원 재

Contents

I. SW 공급망 보안 가이드라인

I. SW 공급망 보안 가이드라인



개요

발행 기관	과학기술정보통신부, 디지털플랫폼정부위원회, 국가정보원
발행일	2024. 05.
주요 내용	이 가이드라인은 소프트웨어(SW) 공급망 보안 관리의 필요성과 주요 국가들의 정책 동향을 검토하고, 기업과 산업, 그리고 국가 차원에서 통합된 위험관리 체계를 구축하는 방안을 제안합니다. 이 체계에서 SBOM은 SW 공급망에서의 SW구성 요소에 대한 신뢰할 수 있는 정보를 공유하는 중요한 수단이 되는데, 본 문서에서는 정부 여러 기관이 운영하는 테스트베드를 통해 SBOM 인프라를 지원하고 있음과 동시에 국내에서 활용 가능한 SBOM 표준에 대해서도 소개합니다.
배포처	한국인터넷진흥원 (KISA) • https://www.kisa.or.kr/2060204/form?postSeq=15&page=1

II. 추진 배경

II. 추진 배경

01 환경 변화

- 초연결 사회의 도래

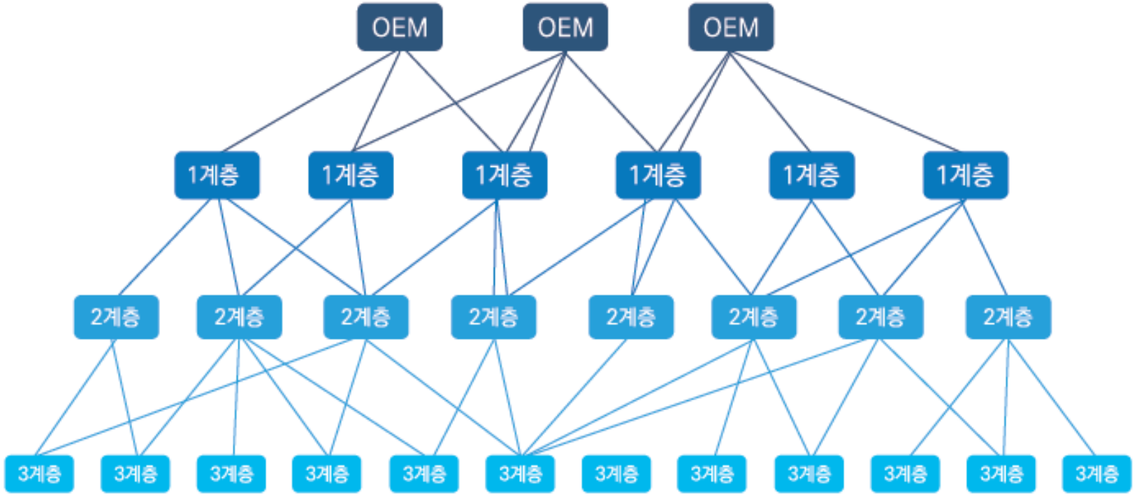


그림 1 공급망 생태계 기본 모형

II. 추진 배경

01 환경 변화

- SW 부품 공급의 분업화 / 공개 SW 사용의 확대

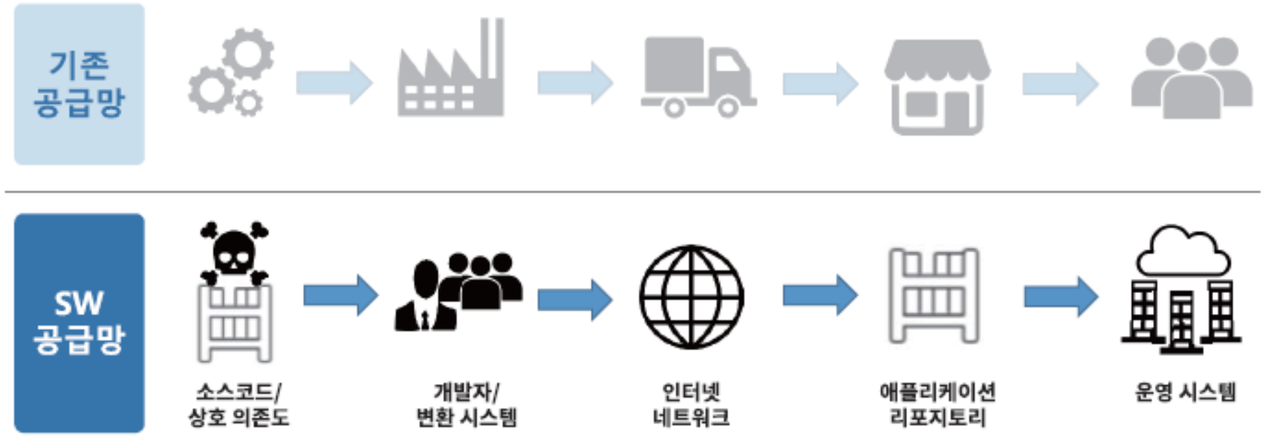


그림 2 전통적인 공급망과 SW 공급망 비교

II. 추진 배경

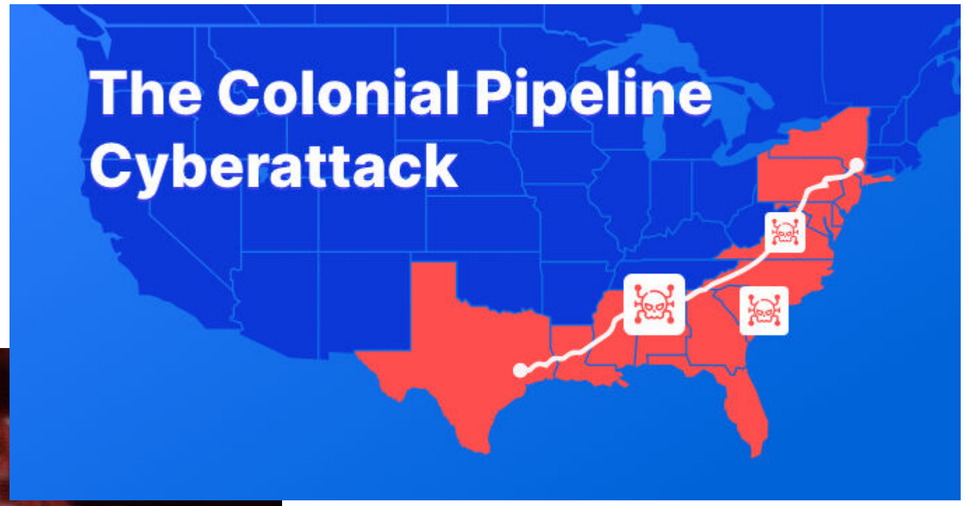
02 SW 공급망 위기 대응의 필요성

- 공격 기법의 고도화

II. 추진 배경

02 SW 공급망 위기 대응의 필요성

- 피해 규모의 대형화



03 주요국 정책 동향 (미국)

- 미국
  - '21.5 | EO14028
  - '22.9 | 관리예산처(OMB) 보안 강화 지침
    - Self-Attestation 제출 요구, SBOM 중요성 부각
  - '23.1 | FDA 의료기기 보안 강화 정책
    - SBOM 제출 요구

- 일본
  - 의료, 자동차, SW 분야에 SBOM 실증(PoC)사업 진행중
  - 공개 SW의 급속한 확대로 통신 분야 공급망에 대한 SBOM 도입 가능성 검토중(2023)

- 유럽
  - '24.3 | 유럽의회 Cyber Resilience Act(CRA) 승인
    - 유통되는 디지털 기기의 SBOM 제출 의무화
    - 이사회의 승인을 거쳐 2026년 하반기 발효될 것으로 예상
  - CE 마크 부착 요건에 Cyber 보안 적합성 포함
    - CE 마크 : KC 마크와 유사한 개념
    - 제품 안정성 관련 인증

- Quad 사이버보안 파트너쉽
  - 미국, 일본, 인도, 호주 4개국 협의체
  - 각국 정부 정책에 '안전한 SW 개발 활동'을 반영하고, 장려하기로 합의
  - 안전한 SW를 위한 공동의 원칙을 마련

III. SW 공급망 위험관리 방안

III. SW 공급망 위험관리 방안

01 C-SCRM 구축 방안

- 공급망 보안 기본 개념 (미국 국립표준기술 연구소, NIST)

공급망 요소 (Supply Chain Element)	시스템 및 구성요소의 연구 및 설계, 개발, 제조, 구입, 배포, 통합, 운영 및 유지보수 또는 폐기에 사용되는 조직과 개체, 도구를 포함
공급망 사이버보안 위험 (Cybersecurity Risks throughout the Supply Chain)	공급자(개발사 및 공급(유통)사), 공급망(개발환경 및 업데이트 전송로), 제품 및 서비스에서 발생할 수 있는 피해와 침해 가능성
공급망 사이버보안 위험평가 (Cybersecurity Supply Chain Risk Assessment)	공급망 전체의 사이버보안 위험, 발생 가능성 및 잠재적 영향에 대한 체계적인 조사
공급망 사이버보안 위험관리 (Cybesecurity Supply Chain Risk Management, C-SCRM)	공급망 전체에서 사이버보안 위험에 대한 노출을 관리하고 적절하게 대응하기 위한 전략, 정책 및 절차 등의 관리체계

01 C-SCRM 구축 방안

- 기업, 기관의 C-SCRM 관리 활동 (NIST)
  - 3개 레벨로 나누어진 다단계 위험관리 체계를 구축할 수 있음

그림 7 다단계 전사적 위험관리(C-SCRM) 개요

표 7 이해관계자의 역할에 따른 주요 C-SCRM 활동 예시

수준	이해관계자	역할	활동
1. 전사	경영진[26]	C-SCRM 활동에 대한 경영진의 감독을 확립	• 전사적 C-SCRM 전략 정의 • 거버넌스 구조 및 운영 모델 수립 • 기업의 위험 구성, 위험관리 방식의 기조 설정 • 대체적인 구현 계획, 정책, 목적, 목표를 정의 • 전사적 수준의 C-SCRM 의사 결정 수행 • C-SCRM PMO(프로젝트 관리조직) 구성
2. 프로세스	비즈니스 관리자[27]	기업의 미션과 비즈니스 프로세스 측면에서 공급망의 사이버보안 위험을 평가, 대응, 모니터링	• 비즈니스 프로세스별 전략 개발 • 정책, 절차, 지침, 제약사항 개발 • 신규 IT 프로젝트에서 보안취약점 감축 • C-SCRM 구현 계획 개발 • 기업의 위험관리 체계를 비즈니스 프로세스에 맞게 조정 (예, 위험 허용 범위 설정) • 비즈니스 프로세스 내 위험관리 • C-SCRM에 관해 레벨1에 보고, 레벨3의 보고에 대한 조치
3. 운영	시스템 관리자[28]	개별 시스템 및 업무에 C-SCRM을 적용하고 운영 및 보고	• C-SCRM 계획 개발 • C-SCRM 정책과 요구사항 구현 • 레벨1과 2에서 제공한 제약사항 준수 • 개별 시스템의 상황에 맞게 C-SCRM을 조정하고 SDLC에 적용 • C-SCRM에 관해 레벨2에 보고

III. SW 공급망 위험관리 방안

01 C-SCRM 구축 방안

- 개발, 운영환경의 C-SCRM 구축 방안 (ESF 권고)
  - 개발사, 공급사, 운영사로 나누어 역할 분배

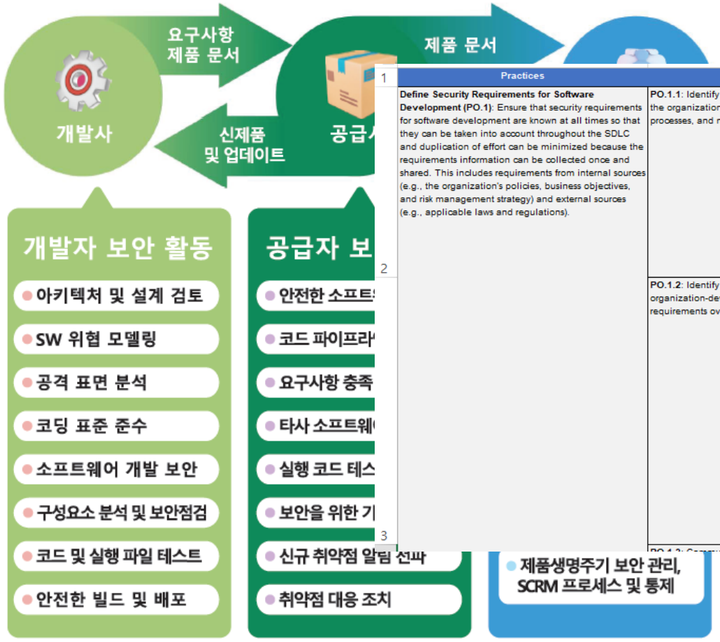
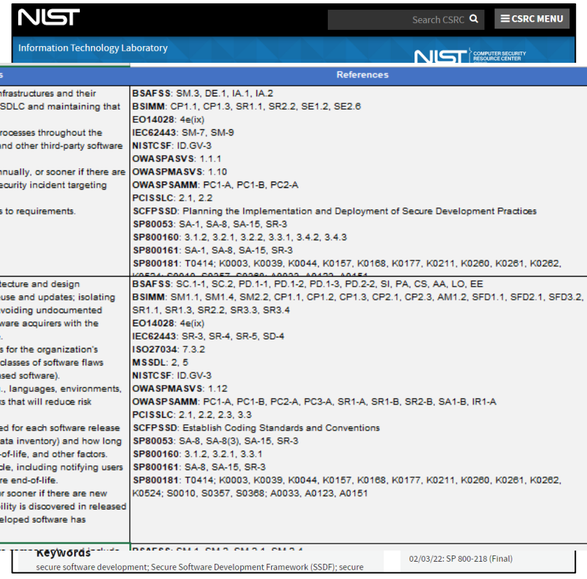


그림 8 SW 공급망 참여자에 따른 보안 활동

- 안전한 SW 개발체계(NIST) 활용 가능 :
  Secure Software Development Framework(SSDF)*


NIST Search CSRC CSRC MENU
Information Technology Laboratory
NIST COMPUTER SECURITY RESOURCE CENTER

Practices	Tasks	Notional Implementation Examples	References
Define Security Requirements for Software Development (PO.1): Ensure that security requirements for software development are known at all times so that they can be taken into account throughout the SDLC and duplication of effort can be minimized because the requirements information can be collected once and shared. This includes requirements from internal sources (e.g., the organization's policies, business objectives, and risk management strategy) and external sources (e.g., applicable laws and regulations).	**PO.1.1**: Identify and document all security requirements for the organization's software development infrastructures and processes, and maintain the requirements over time.	Example 1: Define policies for securing software development infrastructures and their components, including development endpoints, throughout the SDLC and maintaining that security. Example 2: Define policies for securing software development processes throughout the SDLC and maintaining that security, including for open-source and other third-party software components utilized by software being developed. Example 3: Review and update security requirements at least annually, or sooner if there are new requirements from internal or external sources, or a major security incident targeting software development infrastructure has occurred. Example 4: Educate affected individuals on impending changes to requirements.	**BSAFSS**: SM.3, DE.1, IA.1, IA.2 **BSIMM**: CP1.1, CP1.3, SR1.1, SR2.2, SE1.2, SE2.6 **EO14028**: 4e(ix) **IEC62443**: SM-7, SM-9 **NISTCSF**: ID.GV-3 **OWASPASVS**: 1.1.1 **OWASPMASVS**: 1.10 **OWASPSAMM**: PC1-A, PC1-B, PC2-A **PCISSLC**: 2.1, 2.2 **SCFPSSD**: Planning the Implementation and Deployment of Secure Development Practices **SP80053**: SA-1, SA-8, SA-15, SR-3 **SP800160**: 3.1.2, 3.2.1, 3.2.2, 3.3.1, 3.4.2, 3.4.3 **SP800161**: SA-1, SA-8, SA-15, SR-3 **SP800181**: T0414; K0003, K0039, K0044, K0157, K0168, K0177, K0211, K0260, K0261, K0262,
	PO.1.2: Identify and document all security requirements for organization-developed software to meet, and maintain the requirements over time.	Example 1: Define policies that specify risk-based software architecture and design requirements, such as making code modular to facilitate code reuse and updates; isolating security components from other components during execution; avoiding undocumented commands and settings; and providing features that will aid software acquirers with the secure deployment, operation, and maintenance of the software. Example 2: Define policies that specify the security requirements for the organization's software, and verify compliance at key points in the SDLC (e.g., classes of software flaws verified by gates, responses to vulnerabilities discovered in released software). Example 3: Analyze the risk of applicable technology stacks (e.g., languages, environments, deployment models), and recommend or require the use of stacks that will reduce risk compared to others. Example 4: Define policies that specify what needs to be archived for each software release (e.g., code, package files, third-party libraries, documentation, data inventory) and how long it needs to be retained based on the SDLC model, software end-of-life, and other factors. Example 5: Ensure that policies cover the entire software life cycle, including notifying users of the impending end of software support and the date of software end-of-life. Example 6: Review all security requirements at least annually, or sooner if there are new requirements from internal or external sources, a major vulnerability is discovered in released software, or a major security incident targeting organization-developed software has occurred.	**BSAFSS**: SC.1-1, SC.2, PD.1-1, PD.1-2, PD.1-3, PD.2-2, SI, PA, CS, AA, LO, EE **BSIMM**: SM1.1, SM1.4, SM2.2, CP1.1, CP1.2, CP1.3, CP2.1, CP2.2, CP2.3, AM1.2, SFD1.1, SFD2.1, SFD3.2, SR1.1, SR1.3, SR2.2, SR3.3, SR3.4 **EO14028**: 4e(ix) **IEC62443**: SR-3, SR-4, SR-5, SD-4 **ISO27034**: 7.3.2 **MSSDL**: 2, 5 **NISTCSF**: ID.GV-3 **OWASPMASVS**: 1.12 **OWASPSAMM**: PC1-A, PC1-B, PC2-A, PC3-A, SR1-A, SR1-B, SR2-B, SA1-B, IR1-A **PCISSLC**: 2.1, 2.2, 2.3, 3.3 **SCFPSSD**: Establish Coding Standards and Conventions **SP80053**: SA-8, SA-8(3), SA-15, SR-3 **SP800160**: 3.1.2, 3.2.1, 3.3.1 **SP800161**: SA-8, SA-15, SR-3 **SP800181**: T0414; K0003, K0039, K0044, K0157, K0168, K0177, K0211, K0260, K0261, K0262, K0524; S0010, S0357, S0368; A0033, A0123, A0151

Keywords: secure software development; Secure Software Development Framework (SSDF); secure
02/03/22: SP 800-218 (Final)

https://csrc.nist.gov/pubs/sp/800/218/final

- SSDF의 특징
  - SW 개발에 관한 지식 없이도 이해할 수 있는 프레임워크
  - 사용하는 SDLC 모델, 기술, 플랫폼, 프로그래밍 언어, 운영환경과 관계 없이 적용 가능

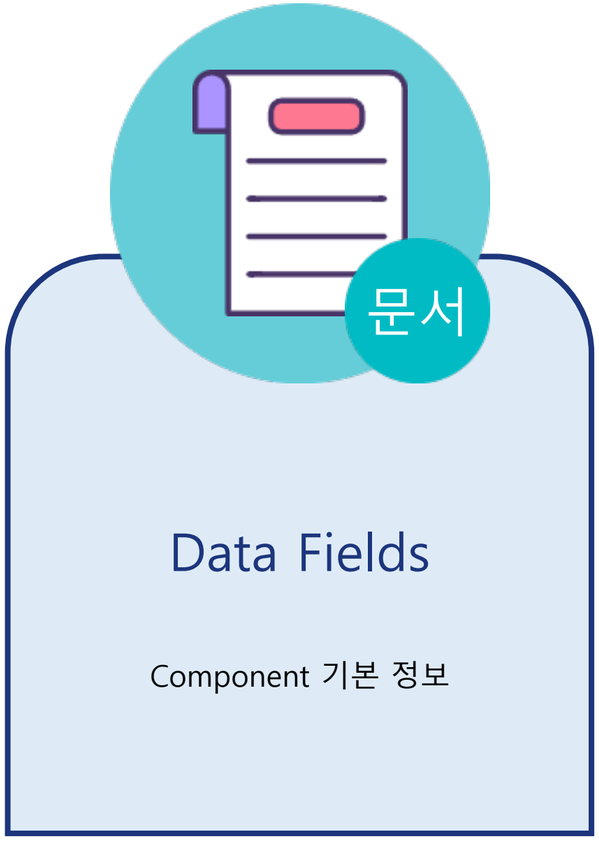
02 SW 구성요소의 신뢰성 확보 방안

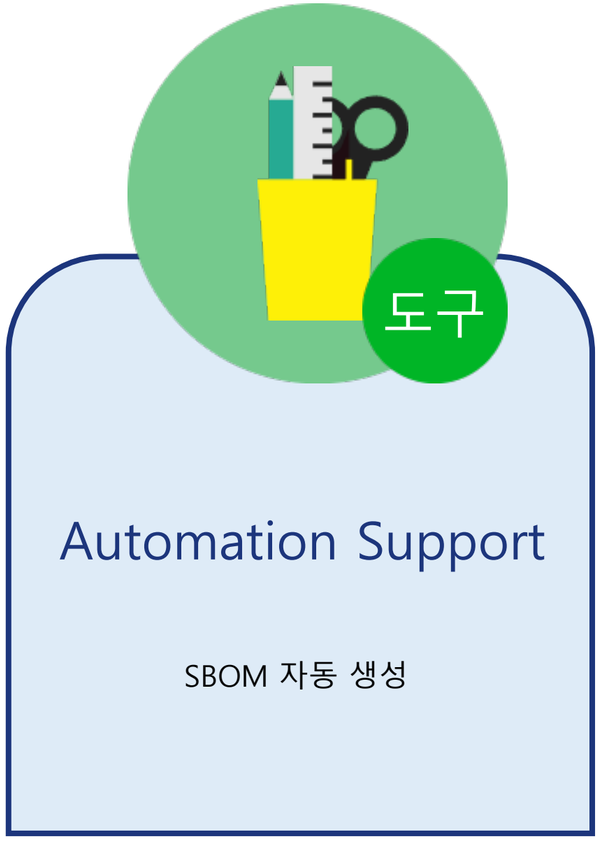
- Software Bill of Materials (SBOM)
  - SW 전체의 구성요소를 목록화한 문서

그림 11 SBOM 활용의 효과성

02 SW 구성요소의 신뢰성 확보 방안

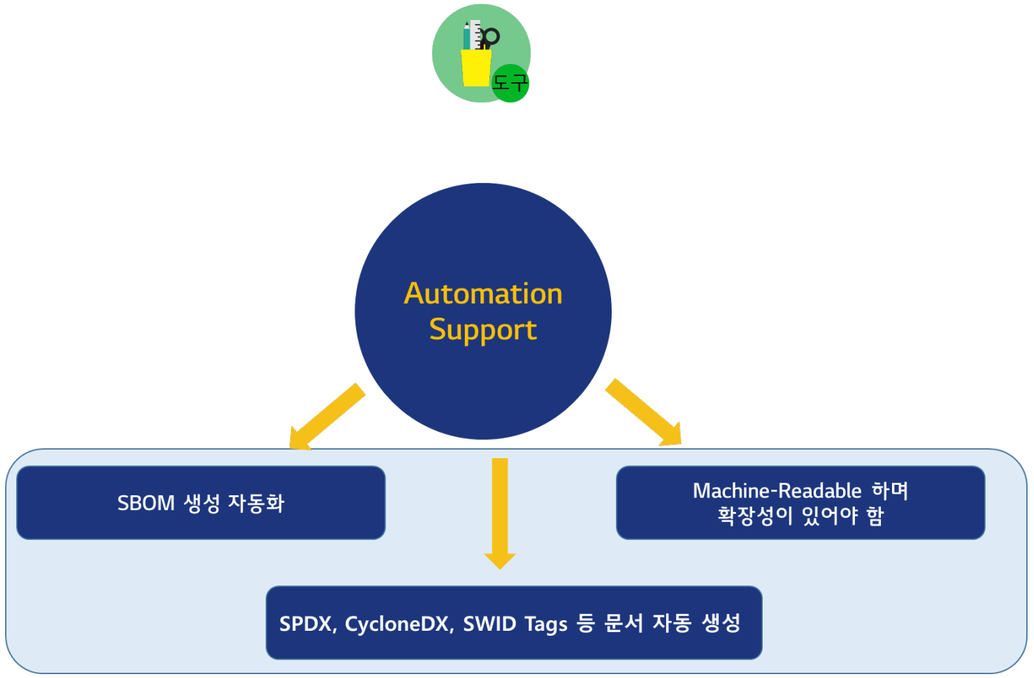
- NTIA의 SBOM 최소 요건

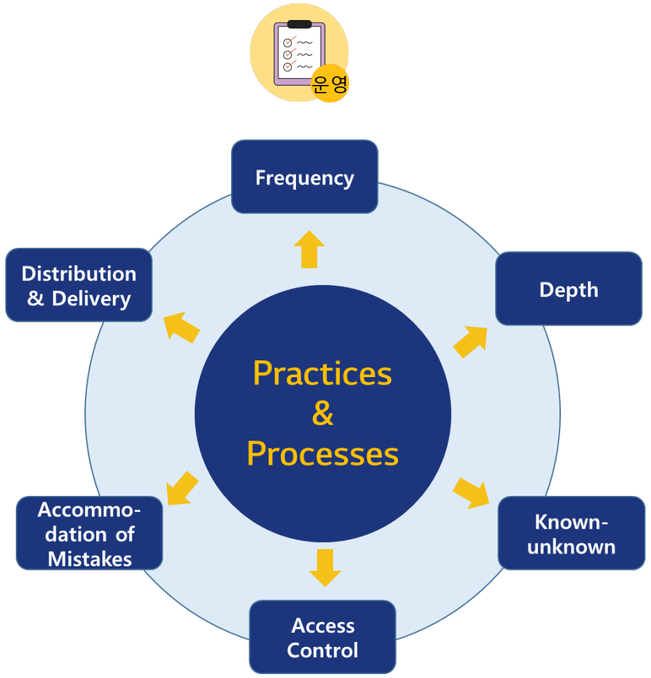




02 SW 구성요소의 신뢰성 확보 방안

- NTIA의 SBOM 최소 요건





02 SW 구성요소의 신뢰성 확보 방안

- SBOM 활용 영역
  - 보안취약점 관리
  - 공개 SW 라이선스 관리

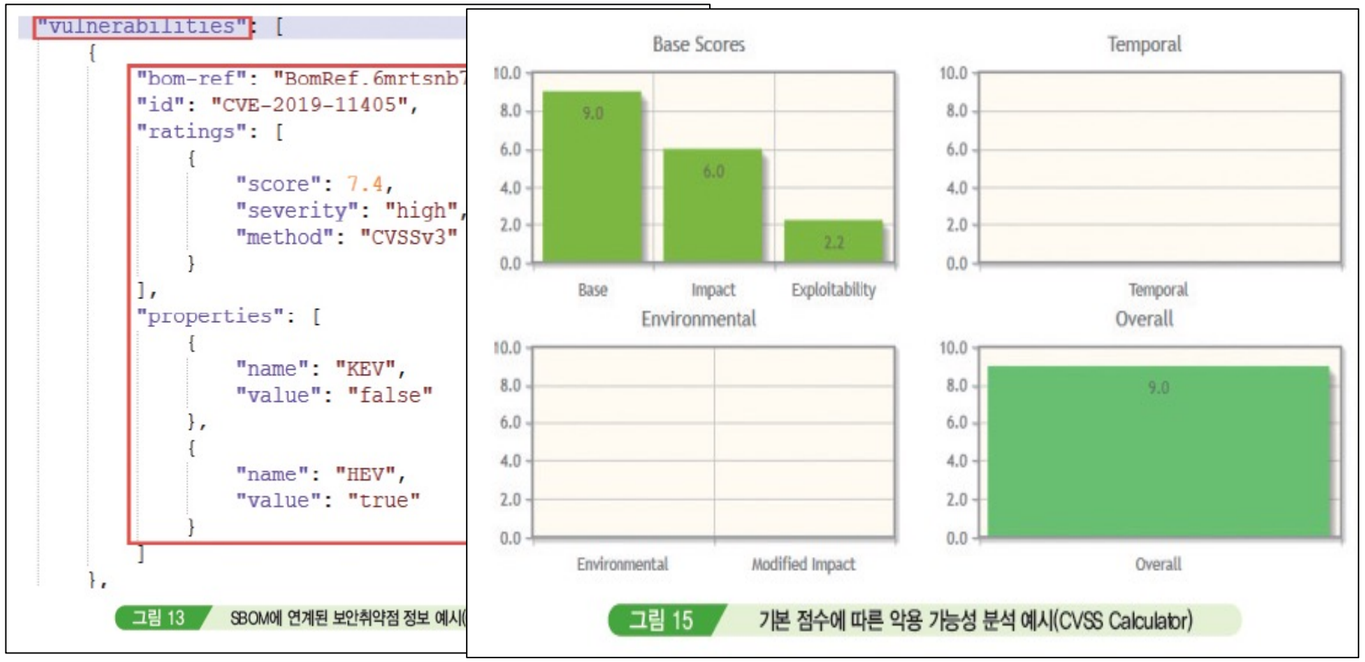


그림 13 SBOM에 연계된 보안취약점 정보 예시(

그림 15 기본 점수에 따른 악용 가능성 분석 예시(CVSS Calculator)

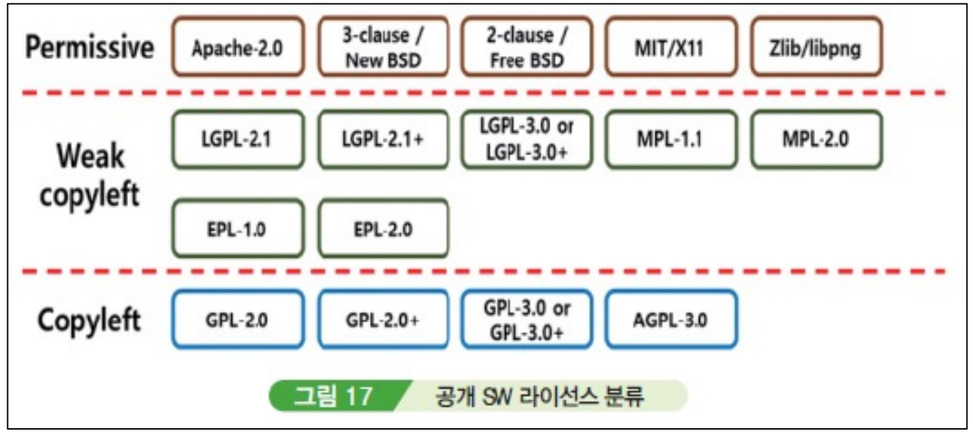


그림 17 공개 SW 라이선스 분류

III. SW 공급망 위험관리 방안

03 SBOM 기반 공급망 보안 강화 방안

- 주체별 보안 강화 방안

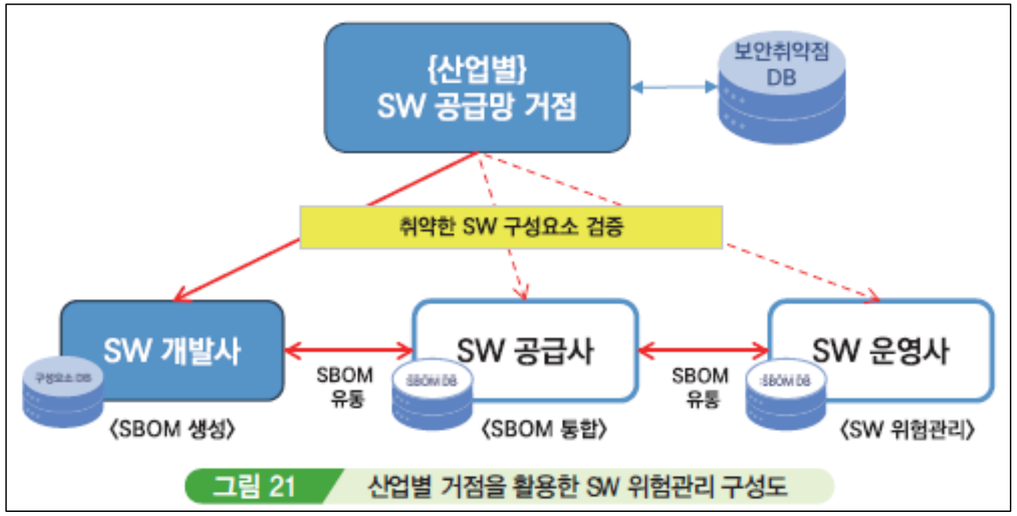


그림 21 산업별 거점을 활용한 SW 위험관리 구성도

개발사	• SBOM 생성을 위한 필수 설비 구축 필요 (SBOM 도구 등)
공급사 및 운영사	• SBOM 공급(유통)체계 구축 • 정부/공공기관/협회/단체 등에 산업별 SW 공급망 거점을 구축

III. SW 공급망 위험관리 방안

03 SBOM 기반 공급망 보안 강화 방안

- 주체별 보안 강화 방안

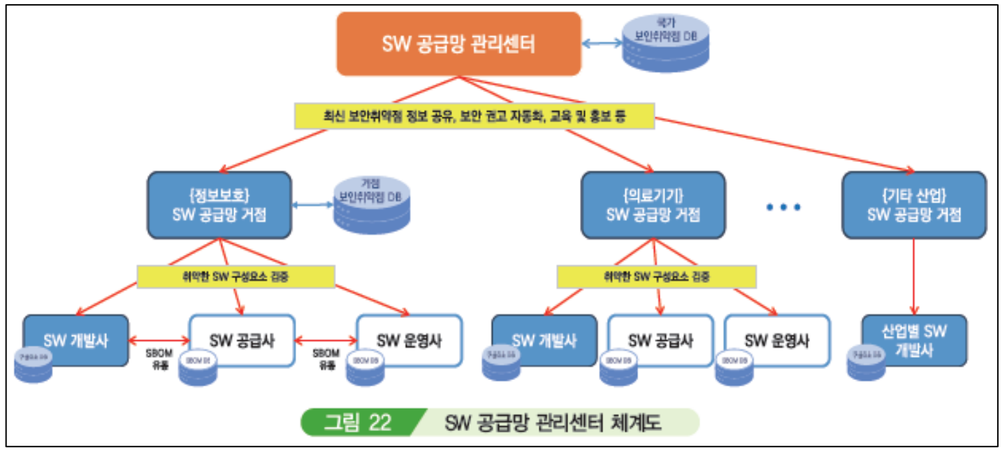


그림 22 SW 공급망 관리센터 체계도

개발사	• SBOM 생성을 위한 필수 설비 구축 필요 (SBOM 도구 등)
공급사 및 운영사	• SBOM 공급(유통)체계 구축 • 정부/공공기관/협회/단체 등에 산업별 SW 공급망 거점을 구축
산업별 SW 공급망 거점 / SW공급망 관리센터	• 산업 생태계 스스로 SBOM 유통할 수 있도록 지원 • 위험 발생 시 산업 전반에서 빠르게 조치 할 수 있도록 지원 • 통합하여 국가 단위로 관리

IV. SBOM 기반
SW 공급망 보안 실증 사례

IV. SBOM 기반 SW 공급망 보안 실증 사례

01 SBOM 생성, 활용 실증

의료, 보안 분야 SW 3종을 활용한 실증

- SBOM 생성 과정에서 SBOM 유효성 검증

표 18 SBOM 유효성 검증 단계에서 데이터 누락·중복 사례

컴포넌트 (Component Name)	버전 (Component Version)	공급자 (Supplier Name)	라이선스명·버전 (License Name·Version)
commons-io	1.3.2	정보누락	정보누락
commons-io	2.2		
commons-io: commons-io	2.2		Apache-2.0
commons-io: commons-io	2.1		Apache-2.0
commons-io: commons-io	1.3.2		Apache-2.0
commons-io: commons-io	1.3		Apache-2.0

표 19 SBOM 데이터를 수정·보완한 사례

컴포넌트 (Component Name)	버전 (Component Version)	공급자 (Supplier Name)	라이선스명·버전 (License Name·Version)
commons-io	1.3.2	apache	Apache-2.0
commons-io	1.3	apache	Apache-2.0
commons-io	2.1	apache	Apache-2.0
commons-io	2.2	apache	Apache-2.0

- 자동 생성 과정에서는 SBOM 항목 중 누락, 중복이 필연적으로 발생
- 검색을 통해 수작업으로 보완 필요

IV. SBOM 기반 SW 공급망 보안 실증 사례

01 SBOM 생성, 활용 실증

- SBOM 도구를 활용한 컴포넌트 관리
  - Source 분석 도구는 편차가 상대적으로 적음
  - Binary 분석 도구는 편차가 큼
  - 2종 이상의 도구 사용을 권장

- SBOM을 활용한 보안 취약점 탐지 및 조치
  - SBOM 생성을 통한 컴포넌트 관리가 취약점 탐지 및 조치에 중요
  - 분석 도구에 따라 컴포넌트 정보가 달라지고, 취약점 정보도 달라지므로 주지 필요
  - 분석 도구에 따라 CVE-ID, 출처, 조치 방안 등이 다르게 표현됨
  - 즉, 경험의 축적이 필요

IV. SBOM 기반 SW 공급망 보안 실증 사례

02 SW 공급망 보안 관리 체계 점검 실증

- 개요
  - 미국 가이드를 참조해 54개 세부항목을 만들고, 인터뷰 진행
- 실증 결과
  - 대상 중소기업은 SW 공급망 보안 관리 인식 부족했음
  - 상당수 대기업들은 SW 투명성/안정성을 위한 SBOM 기반 체계를 구축하고 운영중
  - 보안취약점 관리 보다 라이선스 관리에 중점을 두고 있음

표 21 SW 공급망 보안 점검 실증 항목 일부

보안 요구 분야	점검 항목(예)
안전한 제품 관리 (12개)	• 정기적인 SW 보안 교육 여부 • 모의해킹, 보안취약점 진단 등 보안을 위한 활동 여부
보안코드|개발 (13개)	• 빌드 관리 및 보안성 검토 수행 여부 • 빌드단계에서의 보안요구사항 확인 여부
타사 구성요소 확인 (7개)	• 공개 SW, 상용 SW의 보안요구사항 확인 여부 • 취약성, 라이선스 만료 확인 여부
개발환경 보안 (16개)	• 빌드 환경에 대한 공격 표면 조사 및 위협 모델링 수행 여부 • 개발환경에 대한 접근제어, 인터넷 차단 등 조치 수행 여부
보안코드 전달 (6개)	• 패키지 바이너리의 전자서명 생성 여부 • 계약 명기 시, SBOM 전달 여부

표 22 SW 공급망 보안 점검 상세 결과

보안 요구사항	전체 항목	Y(양호)	P(부분양호)	N(취약)	N/A
안전한 제품 관리	12	5	6	1	0
보안 코드 개발	13	4	5	4	0
타사 구성요소 확인	7	5	1	1	0
개발환경 보안	16	7	3	4	2
보안 코드 전달	6	3	1	2	0
합계	54	24	16	12	2

V. SBOM 기반
SW 공급망 보안 활성화 지원

V. SBOM 기반 SW 공급망 보안 실증 사례

01 SW 보안 취약점 점검 지원 테스트베드

- 기업지원허브(판교)
  - 가전, 금융, 스마트도시, 의료 등 다양한 분야에 대한 사이버보안 위협 시연
  - 보안취약점 점검 도구 활용 지원
  - 학생, 일반인 등을 대상 견학 및 교육 프로그램 운영

그림 28 기업지원허브 IoT 기기 사이버보안 위협 시연시설

V. SBOM 기반 SW 공급망 보안 실증 사례

01 SW 보안 취약점 점검 지원 테스트베드

- 디지털헬스케어 보안 리빙랩(원주)
  - 환자 의료정보 시스템 변조, 개인의료장비 트래픽 변조 등 디지털헬스케어 기기에 대한 사이버위협 시연
  - SW 의료기기를 포함한 다양한 디지털헬스케어 의료기기에 대한 보안취약점 점검을 지원
  - SW가 포함된 의료기기 인·허가 시 의료기기 인허가 지원

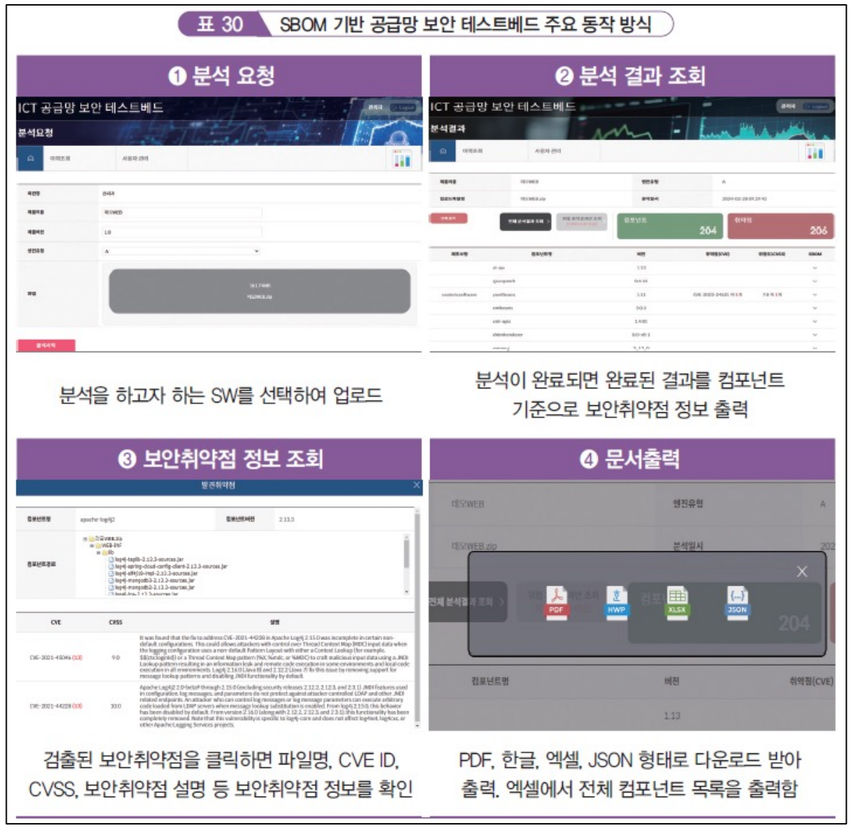
그림 30 디지털헬스케어 보안리빙랩 현장

V. SBOM 기반 SW 공급망 보안 실증 사례

01 SW 보안 취약점 점검 지원 테스트베드

- 국가사이버안보협력센터 기술공유실(판교)
  - SBOM 생성 자동화, SBOM 관리, SW 보안취약점 추적/관리 실증을 위한 테스트베드 구축
  - 테스트베드를 활용한 SBOM 출력

표 30 SBOM 기반 공급망 보안 테스트베드 주요 동작 방식



02 SW 공급망 보안을 위한 SBOM 개발

표 33 SBOM 관련 국내외 표준 현황

구 분	개발기구	국제표준	국내표준	
			국가표준	단체표준
SPDX	리눅스재단	ISO/IEC5962 ('21)	–	TTAK.KO-11.0182('15) ※ SPDX v2.0 일부 참조
CycloneDX	OWASP	–	–	–
SWID	ISO/IEC 19770-2 ('09제정,'15개정)		KS X ISO/IEC 19770-2('21)	–

V. SBOM 기반 SW 공급망 보안 실증 사례

02 SW 공급망 보안을 위한 SBOM 개발

- 정보통신기술협회(TTA)
  - SBOM 단체표준(TTAK.KO-11.0182)
  - SPDX v2.0을 기반으로 국내 실정에 맞게 개선

표 34 정보통신 단체표준 SBOM 속성 규격

구분(Baseline)	속성(Attribution)
① SBOM 검증 도구(SBOM Validation Tool Name)	ex) Folosology
② 공급자(Supplier Name)	ComponentSupplier
③ 저작권자(Author Name)	ComponentAuthor
④ 컴포넌트(Component Name)	ComponentName
⑤ 버전(Version String)	ComponentVersion
⑥ 고유식별자(Unique Identifier)	FormatID
⑦ 컴포넌트 해시(Component Hash)	FileChecksum
⑧ 라이선스 명(License Name)	Component License
⑨ 라이선스 결합 형태(License Usage)	Dynamic/Satic Linking
⑩ 보안취약점 DB(Vulnerability DB)	VulnerabilityDB, NVD
⑪ 관계성(Relationship)	IncludeComponent, ImportComponent
⑫ 릴리즈 날짜(Release Date)	ReleaseDate
⑬ CVE ID	CVE-Year-Serial Number
⑭ CVSS Base Score	Base, Impact, Exploitability
⑮ CVSS Severity	CVSS Severity : High, Medium, Low, None

V. SBOM 기반 SW 공급망 보안 실증 사례

02 SW 공급망 보안을 위한 SBOM 개발

- 국립전파연구원
  - 국가 표준(KS X ISO/IEC 19770-2)
  - SWID(ISO/IEC 19770-2)을 한글 표준으로 도입

  * SW 보안취약점 관리에 SWID가 널리 활용되지 않고 있음

V. SBOM 기반 SW 공급망 보안 실증 사례

02 SW 공급망 보안을 위한 SBOM 개발

- 국가정보원
  - SBOM 기본항목 제안
  - 국제적으로 통용되고 있는 SBOM 데이터 교환 표맷(CycloneDX, SPDX)을 개선하고자 함
    - 항목이 지나치게 많거나 보안취약점 정보를 제공하지 않음
    - NTIA의 데이터 필드는 항목이 부족함

표 35 NIS-SBOM 기본항목 (* : 자체 선정)

구분	속성
① SBOM Standard*	NIS / SPDX / CycloneDX / TTA 등 SBOM 표준
② SBOM Type*	개발 / 유통 등 SBOM 생성단계
③ CycloneDXNo.	CycloneDX번호
④ SPDX Doc. ID	SPDX 문서번호
⑤ SBOM ID*	SBOM 문서번호
⑥ Product Name*	제품 이름
⑦ Product Version*	제품 버전
⑧ Component Name	컴포넌트 이름
⑨ Component Alias*	컴포넌트 별칭
⑩ Component Version	컴포넌트 버전
⑪ Component Supplier Name	컴포넌트 공급자 이름
⑫ Component Hash	컴포넌트 해시(SHA-256 이상 사용)
⑬ Component Path*	컴포넌트 경로(컴포넌트 실제 위치 식별)
⑭ SBOM Author Name	SBOM 작성자
⑮ Unique Identifier	컴포넌트 버전 외에 조회가 가능한 고유 식별자 (CPE, PURL 등)
⑯ Dependency Relationship	상위 컴포넌트와의 종속 관계
⑰ Timestamp	SBOM 생성일시
⑱ License Name·Version	라이선스 이름·버전
⑲ Vul. DB	NVD(CVE), CISA(KEV) 등 보안취약점 DB
⑳ Vul. Info	CVE 식별자 및 CVSS 보안취약점 등급

VI. 시사점

VI. 시사점

01 SW 공급망 관리의 중요성 증대

- 주요 국가에서의 법제화, 규제 강화
- SW 개발환경의 변화에 따른 복잡성 증가
- 공급망 관리를 통한 SW Licensing / 보안 관리

02 공급망 전체의 인식 제고

- 개별 기업이 아니라 공급망 전체의 관점에서의 접근
- 공급망에서의 컨센서스

03 SBOM 생성 효율화 필요

- 분석 도구 기능 고도화
- SBOM 생성 시 수작업 최소화
- 컴포넌트 정보 큐레이션

04 SBOM 유통 효율화 필요

- SBOM 표준 양식 활용

LGE OSPO

감사합니다