OSIMS로 더욱 스마트 해지는 오픈소스 관리혁신

2024. 9. 23

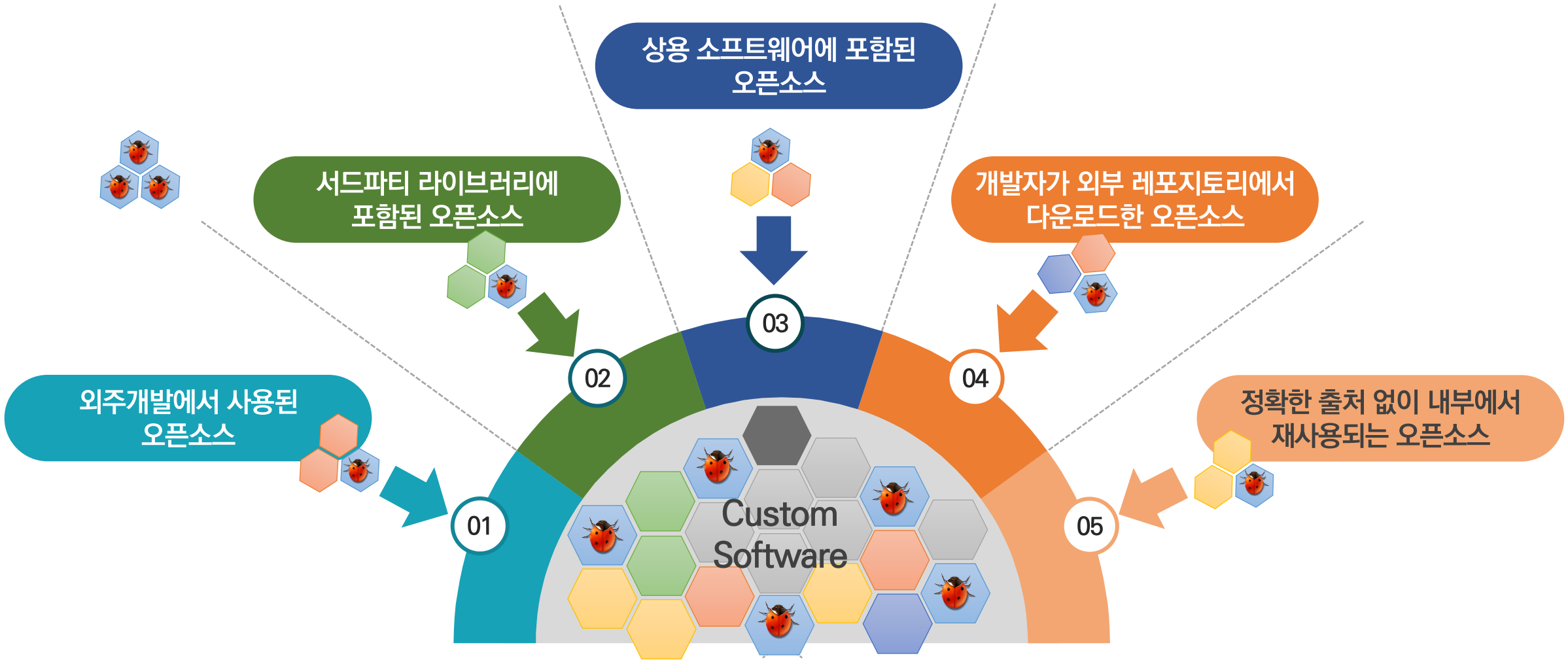
OSBC

목 차

OSBC

오픈소스 관리의 어려움

다양한 오픈소스의 유입경로로 인해 오픈소스 가시화 어려움



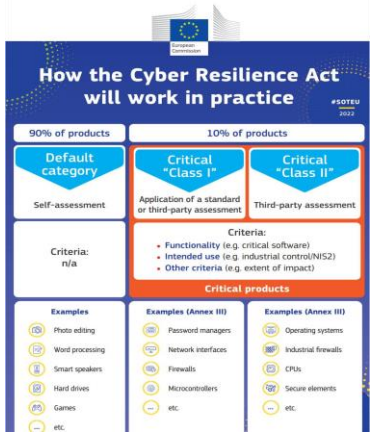
SBOM 대두로 인한 오픈소스 가시화의 필요성

미국

- 행정 명령 14028
- 보안 소프트웨어 개발 프레임워크
- 의료 기기에 대한 FDA 요구 사항

유럽

- 사이버 복원력 법
- SBOM은 "디지털 요소"가 있는 모든 제품에 필요



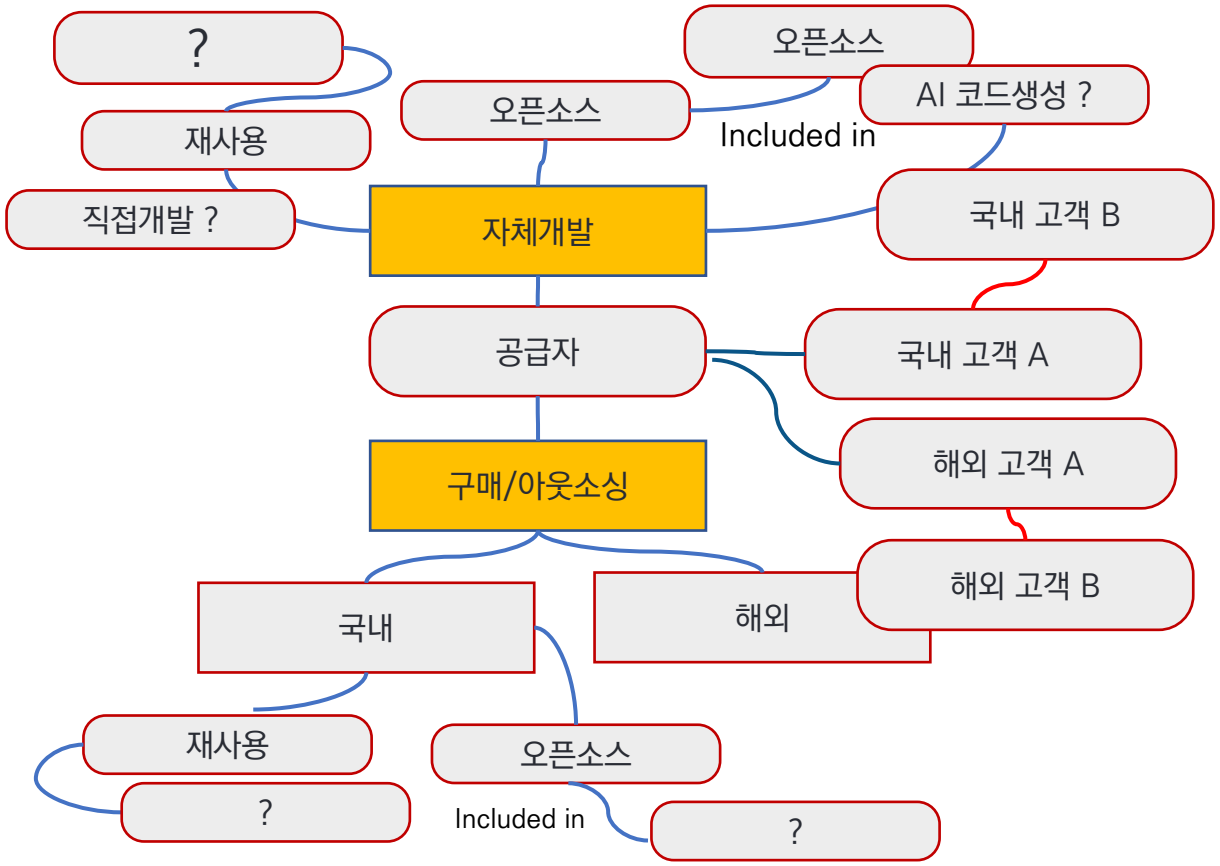
아시아

- 한국: SW 공급망 보안 가이드라인
- 일본: 소프트웨어 BOM(Bill of Materials) 구현 가이드

SBOM 관리의 어려움

다양한 공급망 환경과 비즈니스 모델에 적합한 SBOM 관리범위를 정의하고 구성요소를 관리해야 함

공급망 환경



비즈니스 모델

- 시스템/미들웨어/어플리케이션 SW
- 임베디드 SW
- 서비스
- ...

SBOM 관리 영역

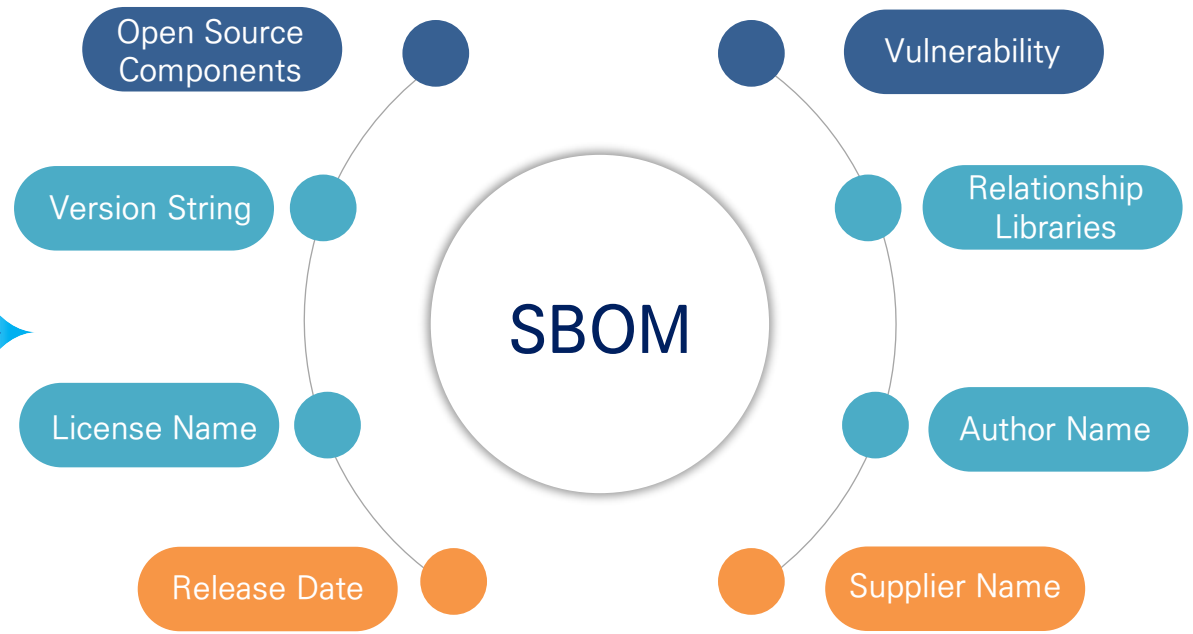
- 소스코드 버그 및 취약점 : 정적분석
- 오픈소스 관계성 : 오픈소스 종속성 분석
- 오픈소스 컨테이너 : 오픈소스 컨테이너 분석
- 소스코드 내 오픈소스 라이선스 및 취약점 : 소스코드 분석
- 바이너리 내 오픈소스 라이선스 및 취약점 : 바이너리 분석

SBOM을 통한 오픈소스 가시성 확보 필요

소프트웨어 구성요소 및 공급망에 대한 가시성 확보를 통한 신속한 대응

소프트웨어 공급망 공격 특징

- 보안이 강화된 최종 대상보다 상태적으로 허술한 조직의 보안 관리 악용
- 한번의 공격으로 잠재적인 여러 고객사에 보다 많은 공격 가능
- 고도의 기술과 많은 시간이 필요하지만, 성공시 은밀하고 지속적인 공격 가능



오픈소스 SBOM (예)

SBOM 생성도구

Attribute	SPDX	CycloneDX	SWID
Author Name	Creator	metadata/authors/author	<Entity> @role (tagCreator), @name
Timestamp	Created	metadata/timestamp	<Meta>
Supplier Name	PackageSupplier	Supplier publisher	<Entity> @role (softwareCreator/publisher), @name
Component Name	PackageName	name	<softwareIdentity> @name
Version String	PackageVersion	version	<softwareIdentity> @version
Component Hash	PackageChecksum Or VerificationCode	Hash "alg"	<Payload>/../<File> @[hash-algorithm]:hash
Unique Identifier	DocumentNamespace combined with SPDXID	bom/serialNumber component/bom-ref	<softwareIdentity> @tagID
Relationship	Relationship: DESCRIBES; CONTAINS	(Inherent in nested assembly/subassembly and/or dependency graphs)	<Link> @rel, @href

Table 1: A mapping between SPDX, CycloneDX, and SWID to capture the core fields discussed in the "baseline component information" SBOM.

Survey of Existing SBOM Formats and Standards – Version 2021, NTIA Multistakeholder Process on Software Component Transparency Standards and Formats Working Grou

TTA 오픈소스 SBOM 규격

구분(Baseline)	속성 (Attribution)
SBOM 검증 도구 (SBOM Validation Tool Name)	ex) Folosology
공급자 (Supplier Name)	ComponentSupplier:
저작권자 (Author Name)	Component Author:
콤포넌트 (Component Name)	ComponentName:
버전 (Version String)	ComponentVersion:
고유식별자(Unique Identifier)	FormatID:
콤포넌트 해쉬 (Component Hash)	FileChecksum:
라이선스 명 (License Name)	Component License:
라이선스 결합형태(License Usage)	Dynamic/Satic Linking:
보안취약점 DB(Vulnerability DB)	VulnerabilityDB : NVD
관계성 (Relationship)	IncludeComponent, ImportComponent
릴리즈 날짜(Release Date)	ReleaseDate:
CWE	CWE-89
CVE ID	CVE-Year-Serial Number
CVSS Base Score	Base : , Impact : , Exploitability :
CVSS Severity	CVSS Severity: High, Medium, Low, None

TTAK.KO-11.0309(공개 소프트웨어 공급망 관리를 위한 소프트웨어 목록 구성(SBOM) 속성 규격)

목 차

OSBC

왜 오픈소스 관리 시스템이 필요한가?

- 오픈소스 검증도구는 사용하기 쉽지 않다.
  - Clarity, FossID, Snyk, Black Duck 등 필요는 하지만, 효율적으로 사용하기 어렵다
  - 익숙하지 않은 언어와 용어, 조금씩 다른 사용법을 쉽게 통일할 필요가 있다.
- 물리적 공간이 분리된 상태에서 일어나는 워크플로우는 불편하다.
  - 관리자와 개발자는 다른 공간에서 작업하며 이를 아우르는 워크플로우는 복잡하다
  - 누구나 쉽게 접근하고 업무를 편리하게 지원하는 시스템이 필요하다
- 회사마다 다른 워크플로우를 가지고 있으며 조직 구성도 다르다.
  - 대부분의 회사는 독특한 워크플로우를 가지고 있고, 조직을 운영하는 방식도 다르다
  - 원하는 워크플로우에 맞춰 기능을 제공 받기를 원한다.

OSBC

어떤 기능들이 요구되는가?

- 허용되는 라이선스/취약점의 기준이 경우에 따라 많이 다르다
  - 회사의 정책에 따라, 프로젝트의 특성에 따라 허용가능한 라이선스/취약점 기준이 바뀐다
  - 정책이 편집 가능하고, 정책에 따라 특정 라이선스/취약점의 사용을 통제할 수 있어야 한다
- 보안 위험이 있는 오픈소스를 사용한 프로젝트를 찾기가 어렵다
  - 보안 위험이 발견된 경우 기존의 많은 프로젝트에서 해당하는 프로젝트를 찾기가 쉽지 않다
  - 새로운 보안 위험과 관련된 프로젝트를 자동으로 검색하고 알람을 제공해야 한다
- 요구되는 SBOM의 형식에 맞춰 재 가공이 필요한 경우가 있다.
  - 표준을 포함한 다양한 SBOM 형식을 지원해야 한다.

OSBC

기존의 오픈소스 관리시템

- 오픈소스 관리 및 관련 프로세스를 한눈에 보기 쉽게.
- 불필요한 과정을 단순화 하고, 관리 프로세스를 자동화.
- 자산, 인력 등 회사의 다양한 시스템과 연동.
- 오픈소스 사용을 체계적으로 관리.
- 보기 쉬운 다양한 대시보드 제공.
- 새롭게 발생하는 오픈소스 이슈에 빠르게 대응 가능.

OSBC

목 차

OSBC

사용자 편의 기능 개선

- 화면과 기능이 복잡해요. 좀 더 쉽게 사용하고 싶어요.
  - 많은 기능을 한꺼번에 보여주는 것은 복잡하다는 느낌을 줌
  - 간결하고 직관적인 화면으로 필요한 기능만 사용하기 원함
- 다양한 SBOM 형식을 지원해 주세요.
  - 용도와 목적에 따라서 요구되는 SBOM의 형식이 다름
  - 엑셀 형식 이외에 JSON, XML 형식을 제공하고, de facto standard인 SPDX, CycloneDX 지원
- 우리도 쓰고 싶어요. 다양한 외국어.
  - 국내 사용자 뿐만 아니라 해외 사용자, 혹은 지역과 상관 없이 다양한 언어 지원 필요

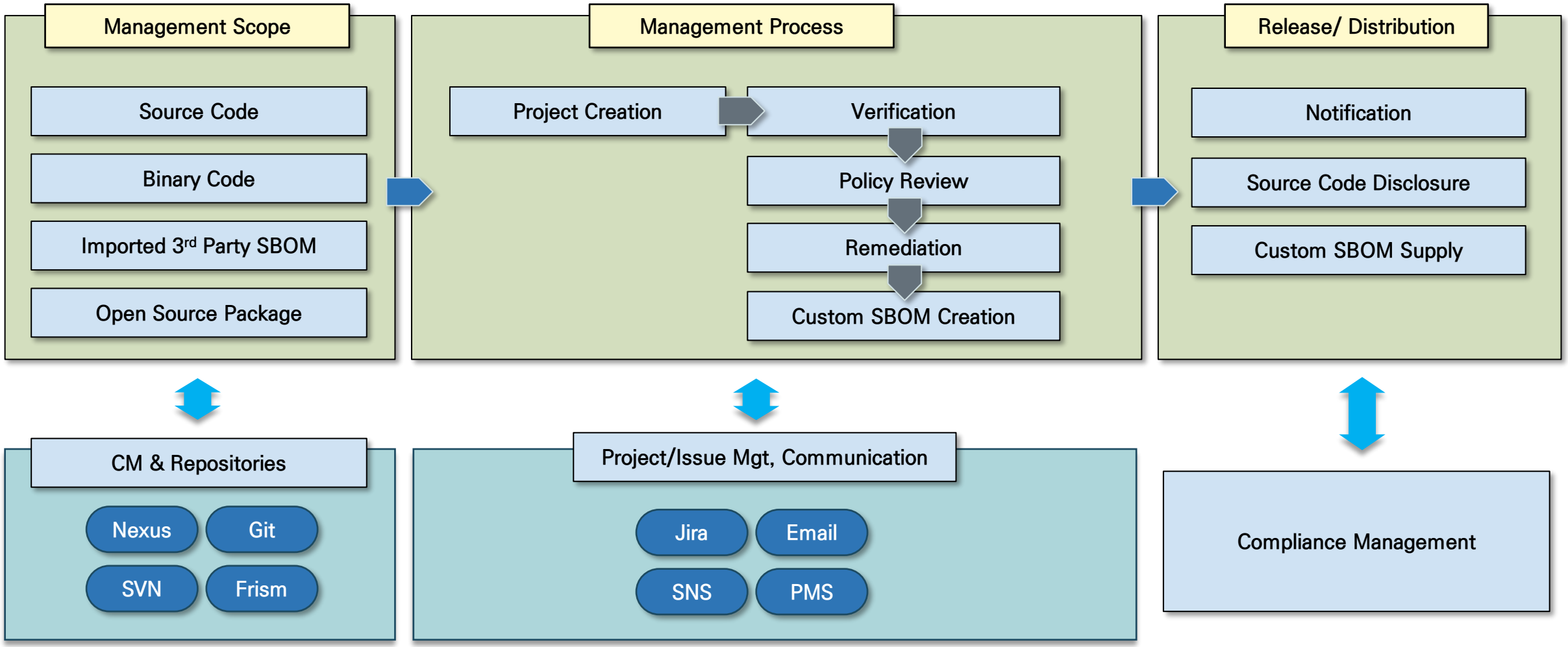
OSBC

커스터 마이징 기능개선

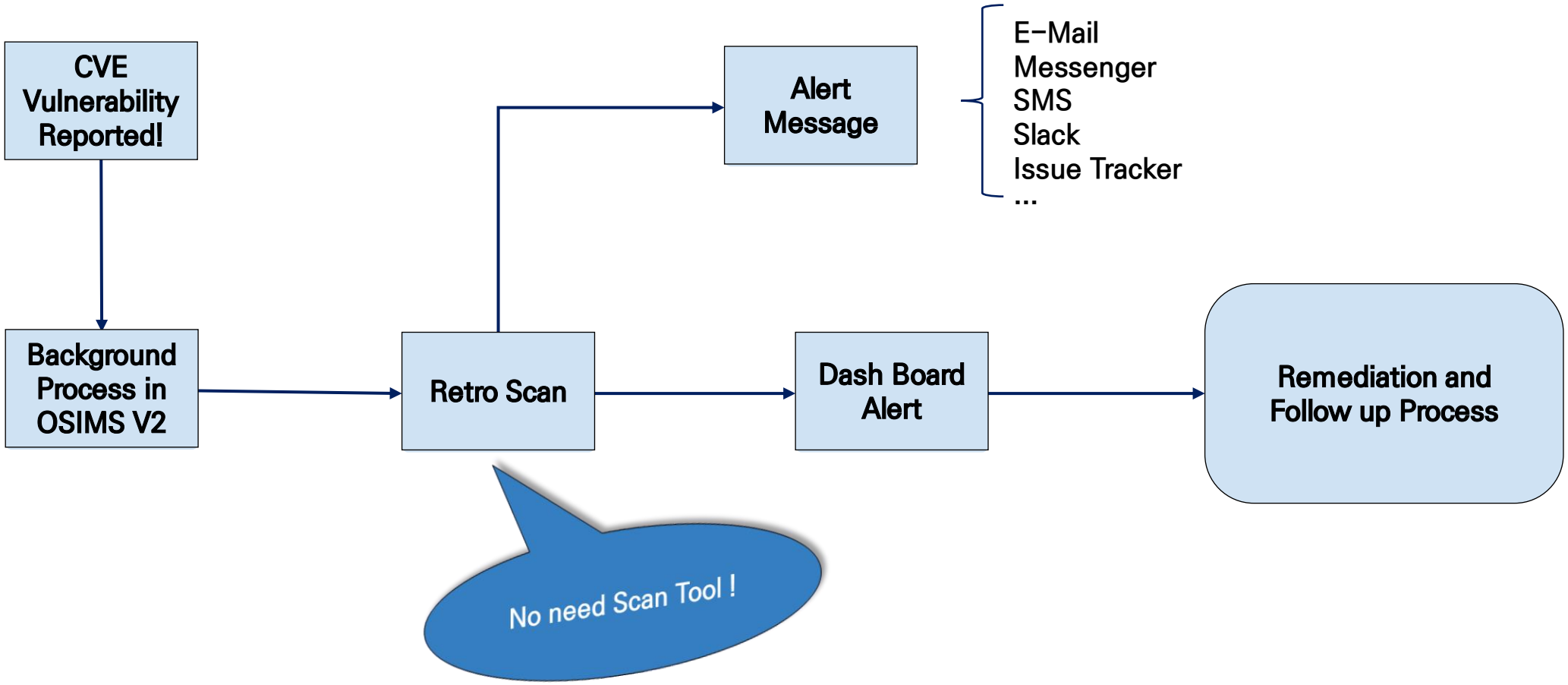
- 설치가 쉬우면 좋겠어요.
  - 제품 설치가 간단하고 쉬울수록 관리 비용 절감
  - 리셀러의 경우 제품 설치 및 관리의 난이도는 중요
- 새로운 Scan 솔루션도 쉽게 적용 가능하면 좋겠어요.
  - 다양한 Scan 솔루션을 지원할 뿐 아니라 쉽게 변경, 추가 등이 가능
- 워크플로우를 변경하거나 확장이 쉬우면 좋겠어요.
  - 회사마다 다른 워크플로우를 설정으로 쉽게 변경 가능
  - Atlassian의 JIRA같은 제품과 연동 가능

OSBC

OSIM를 통한 프로젝트 관리



OSIM를 통한 실시간 취약점 모니터링



OSBC

OSiMS 개요

SW 공급망 관리를 위한 유연하고 (Flexible), 확장 가능한(Scalable) SBOM 관리 통합 플랫폼 OSiMS

소프트웨어 자산과 위험의 가시화 확보 (Ensure Visibility)

- 소프트웨어 자산 (퍼스트파티, 서드파티, 오픈소스)에 대한 라이선스/취약점 위험 가시화

다양환 공급망 환경과 비즈니스 모델을 위한 유연한 정책 관리 (Flexible Policy Management)

- 고객의 SBOM 요구사항과 소프트웨어 유형(임베디드, 솔루션, 서비스 등) 최적화된 정책 관리

SDLC 기반의 유연한 워크플로우 관리 (Flexible Workflow Management)

- SDLC 기반의 설계(사전검토), 개발(실시간 검토), 릴리즈(지속적인 관리) 위한 탄력적 워크플로우

안전한 SW 공급망 관리를 위한 지속적인 실시간 취약점 모니터링 (Continuous Real-time Vulnerability Monitoring)

- 소프트웨어 자산에 대한 레트로 스캔(Retro-Scan)을 통한 실시간 취약점 모니터링

SBOM국제 표준 포맷 및 맞춤 정의 포맷으로 확장 가능한 SBOM 관리 (Expanded, Standardized, Custom-Defined SBOM Management)

- 국제 표준화 SBOM 포맷은 물론, 특정 Scanner와 에 독립적으로 및 맞춤 정의된 모든 SBOM 데이터 필드 관리 (오픈/상용 소스코드, 바이너리 SCA, Repository 등)

OSiMS는 OSBC의 17년간의 소프트웨어 구성요소 분석(SCA) 및 관리에 대한 노하우를 기반으로 개발된 SW 공급망 관리를 위한 유연하고 확장가능한 SBOM 통합 관리 플랫폼입니다.

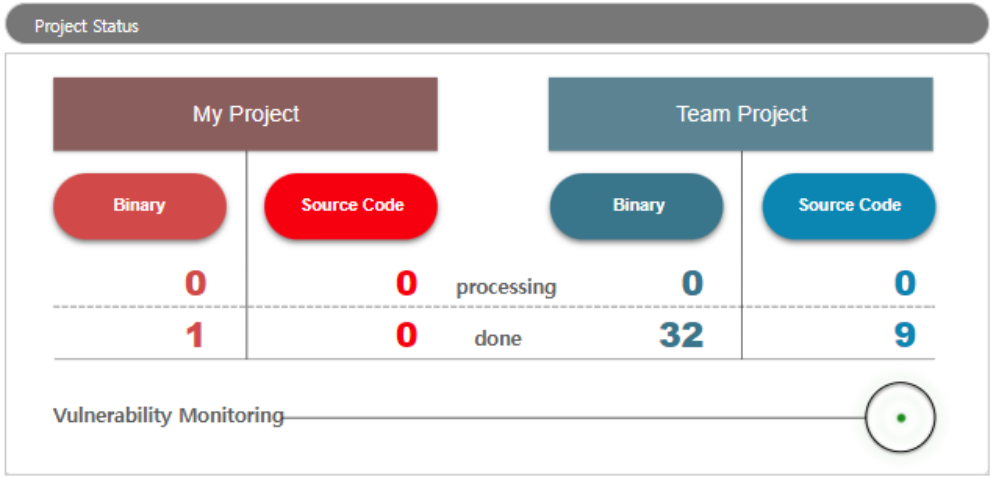
OSiMS는 개별 소프트웨어의 구성요소를 분석 및 식별 관리하는 일반적인 SCA 시스템과 달리 조직의 다양한 공급망 환경과 비즈니스 모델에 적합한 정책과 워크플로우를 유연하게 관리하게 함으로서 소프트웨어 공급망 내에서 필요시되는 최적화된 투명성과 추적성을 보장하여 조직이 잠재적인 보안 취약성과 규정준수 위험을 식별하고 예방할 수 있도록 지원합니다.
특히, 미국 NTIA에서 권장하고 있는 국제 표준화된 SBOM 데이터 필드 관리와 다양한 스캔 분석도구 지원을 통한 SBOM 자동생성 및 관리는 OSiMS의 글로벌 SBOM 관리 통합 플랫폼으로서의 핵심 컨셉입니다.
무엇보다도 OSiMS에서 지원하고 있는 SBOM에 대한 실시간 취약점 모니터링은 소프트웨어 공급망 위험으로 부터 조직의 소프트웨어 자산과 위험 관리를 지속적으로 보장하는 SBOM 관리 목적의 중요한 역할을 수행하게 됩니다.

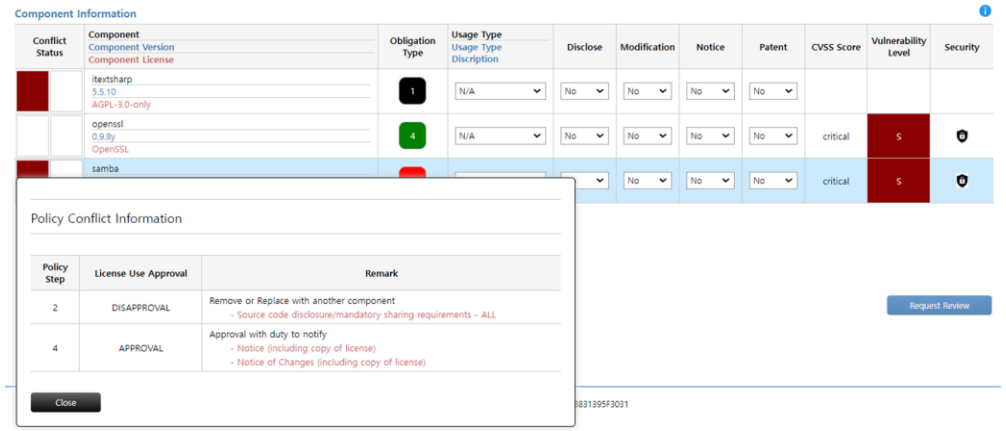
OSiMS 기능

소프트웨어 자산과 위험의 가시화 확보 (Ensure Visibility)

소프트웨어 자산 (퍼스트파티, 서드파티, 오픈소스)에 대한 라이선스/취약점 위험 가시화

- 조직내에서 개발된 퍼스트 파티, 자회사에서 개발된 세컨드 파티, 협력업체에서 개발된 서드 파티 코드와 개발에 사용된 오픈소스까지 소프트웨어 공급망을 구성하고 있는 모든 소프트웨어 자산에 대한 구성요소 별 라이선스 및 보안 취약점 현황과 위험에 대한 가시화를 제공합니다.
- 조직 컴플라이언스 및 보안 정책에 위반된 구성요소와 위반 현황에 대한 상세내용을 시각적으로 쉽게 인지할 수 있도록 표시해 드립니다.
- 모든 영역의 소프트웨어 공급망 영역을 관리하기 위해 다양한 스캔 툴과의 연동을 지원하고 다양한 스캔 툴에서 생성된 SBOM 간의 비교 분석 자료를 제공합니다.
- 소프트웨어 구성요소에 대한 사용자 맞춤식 대시보드를 제공하여 현황 모니터링과 추적을 용이하게 하여 긴급한 취약점에 대응하여 손쉬운 패치가 이루어 될 수 있도록 지원합니다.

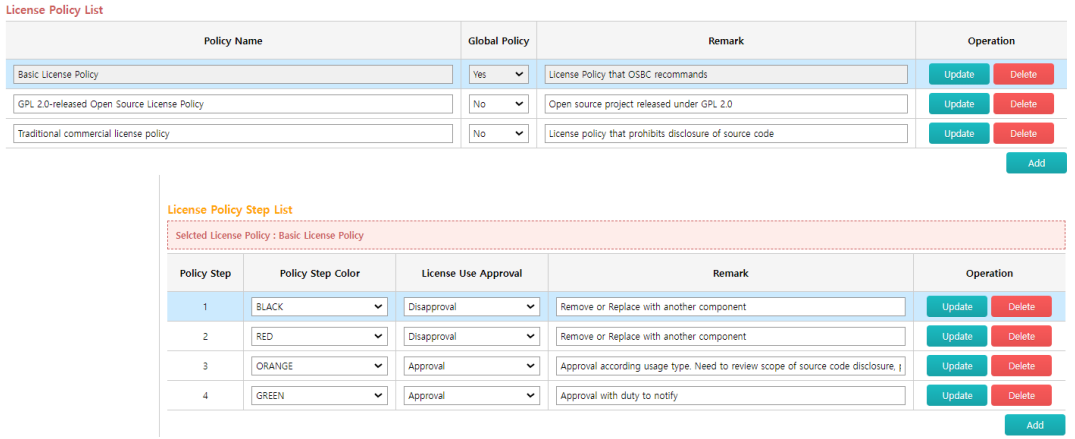


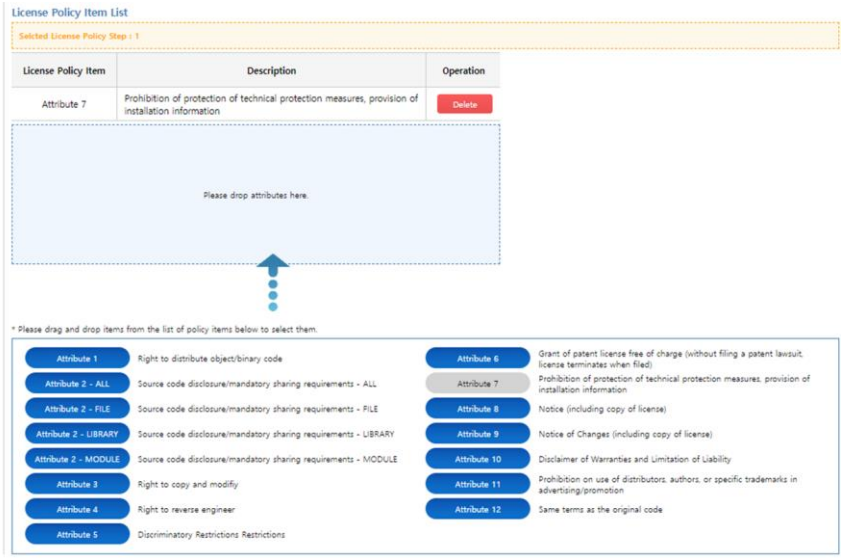


다양환 공급망 환경과 비즈니스 모델을 위한 유연한 정책 관리 (Flexible Policy Management)

고객의 SBOM 요구사항과 소프트웨어 유형(임베디드, 솔루션, 서비스 등) 최적화된 정책 관리

- 조직의 글로벌/로컬 컴플라이언스 및 보안정책 수립과 적용이 가능합니다.
- 공급망 환경 및 프로젝트 배포 및 비즈니스 모델에 부합한 유연한 소프트웨어 공급망 정책수립과 적용이 가능합니다.
- 조직에서 수용 가능한 컴플라이언스와 보안 정책 수준을 기반으로 정책 위반에 대한 임계치를 설정하여 제품별/프로젝트별/구성요소별 위반 현황에 대한 실시간 모니터링과 추적이 가능합니다.
- 오픈소스 컴플라이언스 정책 수립의 경우 OSiMS에 학습되어 있는 수백개의 오픈소스 라이선스 의무사항에 대한 속성 값을 기반으로 손쉽게 조직에서 사용가능 혹은 조건부 사용가능, 사용 불가능한 오픈소스를 식별 및 추적할 수 있습니다. 또한, OSiMS에 학습된 라이선스 의무사항에 대한 속성 값을 통해 라이선스에 대한 전문 지식이 없더라도 손쉽게 해당 의무사항을 식별하여 이행 할 수 있습니다. 조직의 라이선스 전문가는 조직의 라이선스 및 오픈소스 라이선스를 추가, 수정할 수 있어 조직 내 모든 소프트웨어자산에 대한 지적재산권 관리를 용이하게 합니다.
- 오픈소스 보안취약점 정책 수립의 경우 조직의 주요 자산에 대한 보안 중요도를 OSiMS에 반영하여 자산 중요도에 따른 취약점을 자동으로 분류 하여 정책에 반영된 심각도에 따라 단계별로 시정조치 할 수 있도록 가이드를 제공합니다. 이러한 OSiMS의 자산 중요도에 따른 취약점 분류 기능은 하나의 구성요소에서도 수천개씩 발견될 수 있는 보안 취약점을 자산 중요도에 따른 심각도를 우선순위로 분류하여 단계별로 위험에 대처 및 예방할 수 있도록 지원합니다.

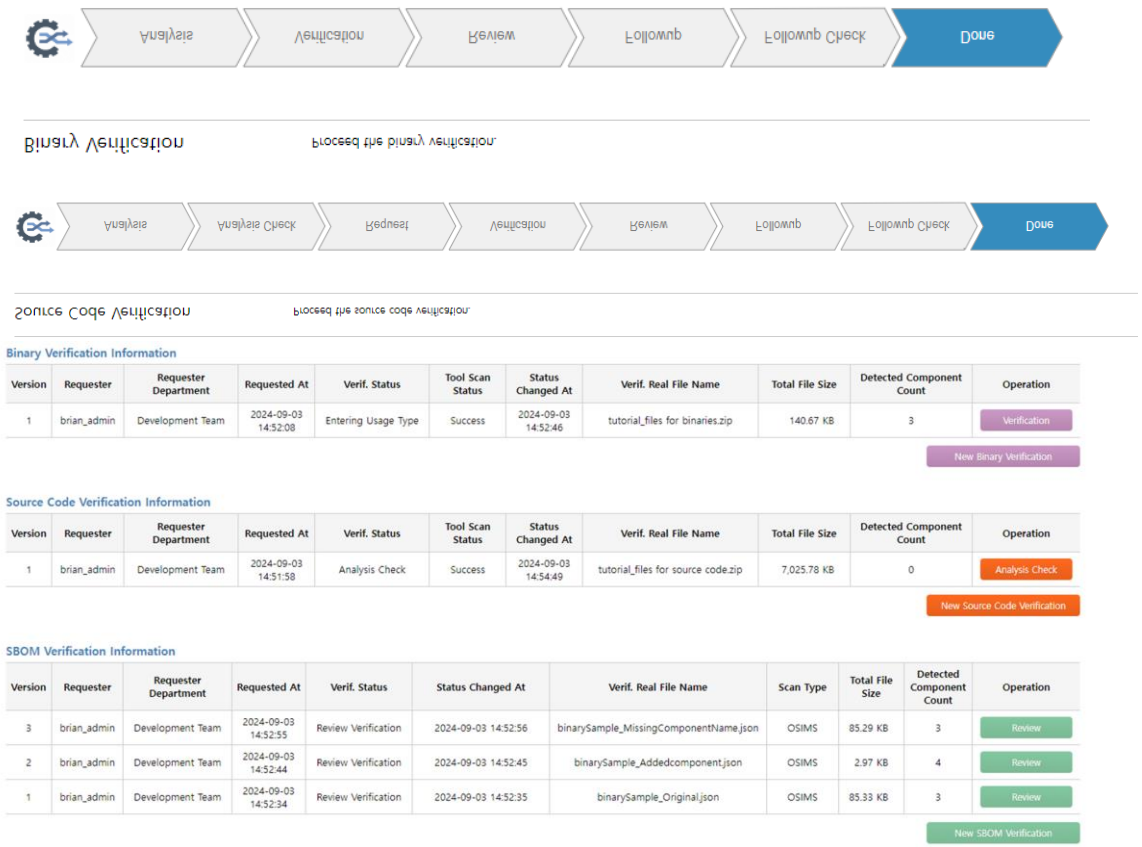




SDLC 기반의 유연한 워크플로우 관리 (Flexible Workflow Management)

SDLC or DevOps 기반의 설계(사전검토), 개발(실시간 검토), 릴리즈(지속적인 관리) 위한 탄력적 워크플로우

- 조직의 SDLC 혹은 DevOps 환경에 따라 선택적 유연한 워크플로우 적용이 가능합니다.
- 조직의 소프트웨어 개발 및 관리프로세스에 따라 OSiMS에서 제공하고 있는 SBOM 관리 워크플로우인 사전검토 워크플로우, 검증 워크플로우, 이행 워크플로우를 선택적으로 적용할 수 있습니다.
- 특정 제품/소프트웨어의 릴리즈 이후에도 동일한 오픈소스 구성요소에서 보안취약점이 발견될 경우 실시간으로 탐지하여 자산 중요도에 따라 새로운 워크플로우를 생성하여 관리할 수 있습니다.
- OSiMS에서는 조직내 퍼스트 파티 SBOM관리를 위한 워크플로우 뿐 아니라 서드파티 SBOM 관리를 위한 서드파티 워크플로우를 지원합니다. 국제 표준화된 SBOM 포맷 뿐 아니라 맞춤 정의된 SBOM 포맷도 손쉽게 Import 하여 관리할 수 있습니다.
- GIT이나 NEXUS 등 다양한 리파지토리와도 손쉽게 연동하여 오픈소스 반입 워크플로우 관리가 가능합니다. 정책에 부합되지 않는 오픈소스의 사용이 불가피 할 경우 선택적으로 예외처리 워크플로우 적용을 통해 오픈소스의 유연한 사용과 추적을 지원합니다.



OSiMS 기능

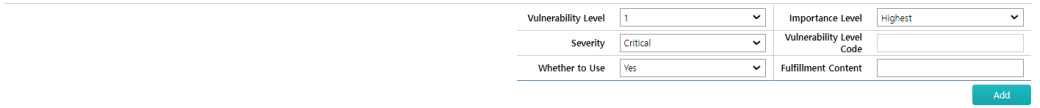
안전한 SW 공급망 관리를 위한 지속적인 실시간 취약점 모니터링 (Continuous Real-time Vulnerability Monitoring)

✔ 소프트웨어 자산에 대한 레트로 스캔(Retro-Scan)을 통한 실시간 취약점 모니터링

- OSiMS에서 관리되고 있는 조직내 모든 SBOM을 대상으로 정기적인 Retro-Scan*을 실행하여 신규 취약점 발생여부를 실시간으로 탐지합니다.
  * Retro-Scan은 소프트웨어 구성요소가 가지고 있는 메타데이타를 기반으로 스캐너에 의한 반복적인 스캔 없이 취약점 정보를 실시간 확인할 수 있는 기능으로 OSBC의 고유 상표입니다.

- Retro-Scan을 통해 취약점이 발견된 경우 OSiMS에 적용된 자산중요도에 따른 취약점 분류 정책에 따라 위반 심각도가 자동 분류되고 대시보드 및 이메일, 메시지 등을 통해 권한 별 설정된 이해관계자들에게 실시간으로 전달하여 제로데이 어택에 대비하여 빠른 긴급 패치가 이루어 질 수 있도록 지원합니다.

- OSiMS의 Retro-Scan은 제품/소프트웨어의 릴리즈 후나 서드파티 SBOM import 단계에서 발견되지 않았던 취약점을 모니터링함으로써 지속적인 소프트웨어 공급망 안전을 가능하게 합니다.



Vulnerability Level Setup

Importance Level \ Severity	Low	Medium	High	Critical
Highest	I	D	A	S
High	J	E	B	C
Medium	K	F	G	H
Low	L	M	N	O

Asset Classification List

Asset Classification Name	Asset Importance Level	Remark	Operation
SaSS Service	Highest	System for SaSS	Update Delete
ERP System	Medium	Systems operating in a network seperation environment	Update Delete

Add

Vulnerability Policy List

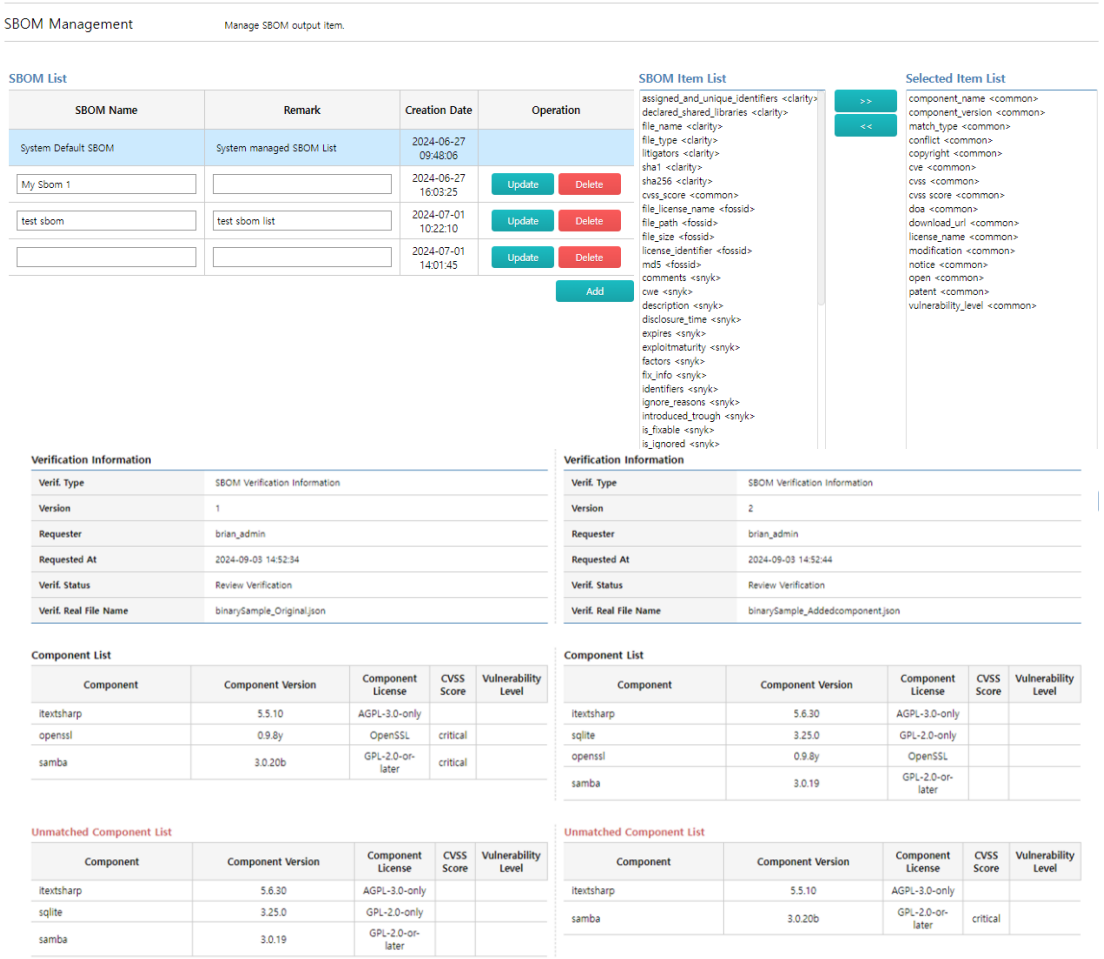
Vulnerability Level	Importance Level	Severity	Level	Vulnerability Level Code	Whether to Use	Fulfillment Content	Operation
1	Highest	Critical		S	No	Remove or Use Other Components	Update Delete
2	Highest	High		A	No	Emergency Patch Required	Update Delete
2	High	High		B	No	Emergency Patch Required	Update Delete
2	High	Critical		C	No	Emergency Patch Required	Update Delete
3	Highest	Medium		D	Yes	Patch Recommandation	Update Delete
3	High	Medium		E	Yes	Patch Recommandation	Update Delete
3	Medium	Medium		F	Yes	Patch Recommandation	Update Delete
3	Medium	High		G	Yes	Patch Recommandation	Update Delete
3	Medium	Critical		H	Yes	Patch Recommandation	Update Delete
4	Highest	Low		I	Yes	Periodic Monitoring Required	Update Delete
4	High	Low		J	Yes	Periodic Monitoring Required	Update Delete
4	Medium	Low		K	Yes	Periodic Monitoring Required	Update Delete
4	Low	Low		L	Yes	Periodic Monitoring Required	Update Delete
4	Low	Medium		M	Yes	Periodic Monitoring Required	Update Delete

OSiMS 기능

SBOM국제 표준 포맷 및 맞춤 정의 포맷으로 확장 가능한 SBOM 관리 (Expanded, Standardized, Custom-Defined SBOM Management)

- 국제 표준화 SBOM 포맷은 물론, 특정 Scanner와 에 독립적으로 및 맞춤 정의된 모든 SBOM 데이터 필드 관리 (오픈/상용 소스코드, 바이너리 SCA, Repository 등)

- OSiMS는 국제 표준인 SPDX, CycloneDX 뿐 아니라 국내 표준인 TTA SBOM과 NIS SBOM 및 사용자 맞춤식 정의된 SBOM 데이터 필드의 Import 및 생성이 가능합니다.
- OSiMS는 현재 FOSSID, Clarity, Snyk과 같은 상용 SCA 도구 뿐 아니라 Sonatype Nexus Repository를 지원하고 있고 향후 OSV Scanner, FOSSLight Scanner와 같은 오픈소스 SCA와 기타 상용 및 오픈소스 정적분석 도구도 지원할 예정입니다.
- OSiMS의 SBOM Management 기능을 통해 조직은 소프트웨어 공급망 환경과 비즈니스 모델에 따라 다양하게 요구 되어 질 수 있는 SBOM 데이터 필드를 다양한 스캐너 및 표준/사전 정의된 포맷으로 입력된 데이터 필드 저장소에서 선택적으로 적용하여 SBOM 생성이 가능합니다. 이러한 SBOM Management 기능은 미국 FDA의 Ensuring Cybersecurity of Medical Devices, SEC Regulation, NIST의 Secure Software Self Attestation Common Form 등과 유럽의 Cyber Resilience Act, Product Liability Directive 등과 같은 규정에 대응하기 위해 제품 및 소프트웨어 별로 필요한 SBOM 생성에 효과적으로 적용될 수 있습니다.



OSBC

감사합니다

오에스비씨(주)
김광섭 연구소장
kskim@osbc.co.kr