

SBOM e Cyber Resilience Act: come SPDX 3.0 e CycloneDX ridefiniscono la sicurezza della supply chain software



La trasparenza del codice diventa obbligo normativo: analisi degli standard tecnici e delle implicazioni per produttori e operatori europei.

Introduzione: dalla vulnerabilità sistemica alla tracciabilità obbligatoria

L'attacco a SolarWinds del 2020 e la vulnerabilità Log4Shell del dicembre 2021 hanno rappresentato punti di svolta nella percezione del rischio legato alla *supply chain* software. Il rapporto ENISA *Threat Landscape* 2024, pubblicato a settembre 2024, identifica gli attacchi alla catena di approvvigionamento tra le sette minacce principali per la cybersecurity europea, evidenziando come questa tipologia di attacco abbia assunto carattere trasversale, intersecando ransomware, malware e minacce alla disponibilità dei sistemi.

In questo scenario, il concetto di *Software Bill of Materials* (SBOM) emerge come paradigma fondamentale per garantire visibilità e controllo sui componenti che costituiscono qualsiasi prodotto digitale. L'Unione Europea, con l'approvazione definitiva del Regolamento (UE) 2024/2847, noto come *Cyber Resilience Act* (CRA), pubblicato nella Gazzetta Ufficiale il 20 novembre 2024 ed entrato in vigore il 10 dicembre 2024, ha trasformato questa *best practice* in requisito cogente, inaugurando una nuova era di responsabilità

documentata per i produttori di software.

Il *Software Bill of Materials*: anatomia di un inventario critico

Il SBOM costituisce un inventario formale e leggibile da macchina che elenca tutti i componenti, le librerie e le dipendenze presenti in un prodotto software. La National Telecommunications and Information Administration (NTIA) del Dipartimento del Commercio statunitense ha definito nel luglio 2021 gli elementi minimi che un SBOM deve contenere, stabilendo uno standard *de facto* successivamente adottato anche dalle normative europee.

Gli elementi minimi NTIA includono: il nome del fornitore del componente, il nome e la versione del componente stesso, gli identificatori univoci, le relazioni di dipendenza, l'autore del SBOM e il *timestamp* di generazione. Questa struttura apparentemente semplice nasconde una complessità tecnica considerevole quando applicata a software enterprise moderni, che tipicamente integrano centinaia o migliaia di dipendenze transitive.

La distinzione tra dipendenze dirette e transitive assume rilevanza critica nella gestione del rischio. Una dipendenza diretta è un componente esplicitamente incluso dagli sviluppatori; una dipendenza transitiva è un componente richiesto da una dipendenza diretta, spesso invisibile al team di sviluppo ma perfettamente sfruttabile da un attaccatore. Il caso Log4Shell ha dimostrato come una vulnerabilità in una dipendenza transitiva possa propagarsi attraverso l'intero ecosistema software mondiale nel giro di ore.

SPDX 3.0: l'evoluzione dello

standard ISO per la trasparenza software

Il *System Package Data Exchange* (SPDX), sviluppato sotto l'egida della Linux Foundation, rappresenta lo standard più consolidato per la rappresentazione di SBOM. La versione 3.0, rilasciata ufficialmente il 16 aprile 2024, costituisce una riscrittura architetturale completa che risponde alle esigenze emergenti del panorama normativo internazionale.

SPDX gode dello status di standard internazionale attraverso la certificazione ISO/IEC 5962:2021, elemento che ne garantisce l'accettazione in contesti regolamentati e conferisce autorevolezza in procedimenti di *compliance*. La versione 3.0 estende significativamente le capacità dello standard precedente, introducendo un modello dati modulare che consente di rappresentare non solo componenti software, ma anche *dataset*, modelli di intelligenza artificiale, specifiche di *build* e informazioni di sicurezza.

L'architettura SPDX 3.0 si basa su profili specializzati che possono essere combinati in base alle esigenze specifiche. Il profilo *Core* definisce le strutture fondamentali; il profilo *Software* descrive pacchetti, file e *snippet* di codice; il profilo *Security* integra informazioni su vulnerabilità secondo lo standard *Common Vulnerabilities and Exposures* (CVE); il profilo *AI*, particolarmente innovativo, consente di documentare *dataset* di *training* e modelli di *machine learning*.

La serializzazione in SPDX 3.0 supporta formati multipli: JSON-LD per l'interoperabilità semantica, RDF per l'integrazione con *knowledge graph*, XML per la compatibilità con sistemi *legacy*. Questa flessibilità risponde alle diverse esigenze di ecosistemi tecnologici eterogenei, facilitando l'adozione sia in ambienti enterprise tradizionali sia in *pipeline* DevOps moderne.

CycloneDX: lo standard OWASP per la sicurezza applicativa

CycloneDX, sviluppato dalla *Open Worldwide Application Security Project* (OWASP), nasce con una vocazione specificamente orientata alla sicurezza applicativa. A differenza di SPDX, che ha origine nel contesto della gestione licenze open source, CycloneDX è stato progettato fin dall'inizio per supportare l'analisi di vulnerabilità e la gestione del rischio nella *supply chain* software.

La versione 1.6 dello standard, rilasciata il 9 aprile 2024, introduce capacità avanzate per la documentazione di attestazioni crittografiche, certificazioni di conformità e metadati relativi all'approvvigionamento. Il formato supporta nativamente la rappresentazione di *Vulnerability Exploitability eXchange* (VEX), un meccanismo standardizzato che consente ai produttori di comunicare se e come una determinata vulnerabilità impatta effettivamente i propri prodotti.

Un elemento distintivo di CycloneDX è il supporto nativo per diversi tipi di BOM oltre al software: *Hardware Bill of Materials* (HBOM), *Manufacturing Bill of Materials* (MBOM), *Software-as-a-Service BOM* (SaaS BOM) e *Cryptography BOM* (CBOM). Quest'ultima tipologia, sviluppata da IBM Research, assume rilevanza crescente nel contesto della migrazione verso algoritmi *post-quantum*, consentendo alle organizzazioni di inventariare gli algoritmi crittografici utilizzati e pianificare la transizione.

Lo standard CycloneDX è riconosciuto come standard internazionale Ecma ECMA-424, acquisendo uno *status* di standardizzazione formale che ne rafforza la posizione in contesti normativi europei e internazionali.

Cyber Resilience Act: il framework normativo europeo

Il Regolamento (UE) 2024/2847, noto come *Cyber Resilience Act*, è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il 20 novembre 2024 ed è entrato in vigore il 10 dicembre 2024. Il regolamento stabilisce requisiti orizzontali di cybersecurity per tutti i prodotti con elementi digitali immessi sul mercato europeo, introducendo obblighi che si estendono lungo l'intero ciclo di vita del prodotto.

L'Allegato I, Parte II del CRA definisce i requisiti essenziali di cybersecurity per la gestione delle vulnerabilità. Al punto (1) specifica che i fabbricanti devono "identificare e documentare le vulnerabilità e i componenti contenuti nel prodotto, anche redigendo una distinta base del software (*software bill of materials*) in un formato comunemente usato e leggibile da una macchina, che includa almeno le dipendenze di primo livello del prodotto".

Il regolamento distingue tra prodotti "importanti" e prodotti "critici", applicando requisiti di conformità proporzionati al livello di rischio. Per i prodotti critici, che includono sistemi operativi, ipervisori, infrastrutture a chiave pubblica e componenti di sicurezza di rete, è richiesta la valutazione di conformità da parte di organismi terzi accreditati. Per i prodotti importanti di Classe I, è ammessa l'autovalutazione seguendo standard armonizzati.

La *timeline* di applicazione prevede periodi transitori differenziati. Gli obblighi di segnalazione delle vulnerabilità attivamente sfruttate diventano applicabili dall'11 settembre 2026. I requisiti essenziali e gli obblighi di valutazione della conformità diventano applicabili dall'11 dicembre 2027. Questo scaglionamento intende consentire agli operatori economici di adeguare processi e tecnologie.

Requisiti tecnici SBOM nel CRA: interpretazione operativa

L'articolo 13 del CRA impone ai fabbricanti di effettuare una valutazione dei rischi di cybersecurity prima dell'immissione sul mercato e di integrare nel prodotto meccanismi che consentano l'identificazione e la documentazione delle vulnerabilità. La generazione e manutenzione del SBOM diventa strumento necessario per adempiere a questi obblighi.

La formulazione "dipendenze di primo livello" nell'Allegato I, Parte II solleva questioni interpretative rilevanti. Una lettura restrittiva limiterebbe l'obbligo alle sole dipendenze dirette; una lettura teleologica, orientata all'effettività della protezione, estenderebbe l'obbligo alle dipendenze transitive essenziali per la gestione del rischio. Le linee guida tecniche che CEN/CENELEC sta sviluppando chiariranno questo aspetto cruciale, con uno standard orizzontale atteso entro metà 2026.

Il considerando 37 del regolamento specifica che il SBOM non deve essere reso pubblico ma deve essere messo a disposizione delle autorità di vigilanza del mercato su richiesta motivata. Questa scelta riflette un bilanciamento tra trasparenza e protezione di informazioni commerciali sensibili, ma potrebbe limitare l'utilità del SBOM per gli utenti finali nella gestione del rischio.

L'interazione con il quadro di gestione delle vulnerabilità impone che il SBOM sia mantenuto aggiornato durante l'intero periodo di supporto del prodotto, che il regolamento fissa in minimo cinque anni o nella durata attesa di utilizzo, se superiore. Questo requisito implica l'implementazione di processi continui di *Software Composition Analysis* (SCA) integrati nelle *pipeline* di sviluppo.

Analisi comparativa: SPDX 3.0 versus CycloneDX 1.6

La scelta tra SPDX e CycloneDX dipende da fattori tecnici, organizzativi e strategici che meritano analisi approfondita. Entrambi gli standard soddisfano i requisiti minimi NTIA e sono compatibili con gli obblighi del *Cyber Resilience Act*, ma presentano caratteristiche distintive che li rendono preferibili in contesti specifici.

SPDX eccelle nella gestione delle informazioni di licenza, offrendo un *repository* standardizzato di oltre 500 identificatori di licenza riconosciuti. Questa caratteristica lo rende particolarmente adatto per organizzazioni con significativa esposizione a tematiche di *compliance* open source e rischio legale. La certificazione ISO conferisce inoltre vantaggi in settori regolamentati che richiedono l'adozione di standard internazionali riconosciuti.

CycloneDX presenta vantaggi significativi nell'integrazione con *workflow* DevSecOps e strumenti di sicurezza applicativa. Il supporto nativo per VEX consente una comunicazione efficace dello stato di sfruttabilità delle vulnerabilità, riducendo il carico operativo dei team di sicurezza nella gestione dei falsi positivi. L'architettura orientata alla sicurezza facilita l'integrazione con piattaforme SIEM e SOAR.

La serializzazione rappresenta un elemento differenziante. CycloneDX supporta JSON, XML e *Protocol Buffers*, quest'ultimo particolarmente efficiente per trasmissioni in ambienti a banda limitata. SPDX 3.0 introduce JSON-LD con supporto per *linked data*, abilitando scenari avanzati di interrogazione semantica e integrazione con *knowledge graph*.

Sul piano dell'adozione industriale, analisi condotte dal Linux Foundation Research indicano una crescita parallela di entrambi gli standard, con SPDX prevalente in contesti

enterprise tradizionali e CycloneDX dominante in ambienti *cloud-native* e DevOps. La tendenza emergente è verso l'adozione di approcci multi-formato, con generazione simultanea di SBOM in entrambi i formati per massimizzare l'interoperabilità.

Implementazione tecnica: architetture e strumenti

L'implementazione di un programma SBOM conforme al CRA richiede l'integrazione di strumenti e processi lungo l'intera catena di sviluppo. L'analisi delle soluzioni disponibili evidenzia un ecosistema maturo che include opzioni open source di livello enterprise.

Syft, sviluppato da Anchore, rappresenta la soluzione open source più diffusa per la generazione di SBOM da immagini container e *filesystem*. Lo strumento supporta nativamente SPDX e CycloneDX, con capacità di rilevamento per oltre 15 ecosistemi di pacchetti inclusi npm, PyPI, Maven, NuGet e Alpine. L'integrazione con Gripe, *scanner* di vulnerabilità dello stesso produttore, consente *workflow* completi di analisi.

Per ambienti enterprise, FOSSA e Snyk offrono piattaforme integrate che combinano generazione SBOM, analisi di vulnerabilità e gestione della *compliance* licenze. Queste soluzioni includono funzionalità di monitoraggio continuo delle dipendenze e *alerting* automatizzato su nuove vulnerabilità, requisiti impliciti nel *framework* CRA.

L'architettura raccomandata prevede la generazione di SBOM in fase di *build* attraverso integrazione con sistemi CI/CD, l'archiviazione in *repository* centralizzati con versionamento, l'integrazione con sistemi di *vulnerability management* per correlazione automatica con database CVE, e la predisposizione di API per l'esposizione controllata alle autorità di

vigilanza.

La firma crittografica dei SBOM, sebbene non esplicitamente richiesta dal CRA, costituisce *best practice* per garantire integrità e non ripudio. Entrambi gli standard supportano meccanismi di firma basati su *JSON Web Signature* (JWS) o *XML Signature*, con raccomandazione di utilizzo di chiavi gestite attraverso infrastrutture PKI aziendali.

Prospettive evolutive: verso un ecosistema di trasparenza software

Il panorama normativo internazionale converge verso l'adozione sistemica dei SBOM. Negli Stati Uniti, l'*Executive Order* 14028 del 12 maggio 2021 ha imposto requisiti SBOM per il software venduto alle agenzie federali. La *Food and Drug Administration* (FDA) richiede SBOM per dispositivi medici connessi. Il *National Institute of Standards and Technology* (NIST) ha pubblicato linee guida dettagliate sulla generazione e utilizzo dei SBOM.

L'interazione tra SBOM e intelligenza artificiale apre scenari innovativi. I profili AI di SPDX 3.0 consentono la documentazione di *dataset* di *training* e modelli, anticipando requisiti che l'AI Act europeo potrebbe rendere cogenti per sistemi ad alto rischio. La tracciabilità della provenienza dei dati diventa elemento critico per la *compliance* con il principio di trasparenza algoritmica.

L'evoluzione verso *framework* di sicurezza della *supply chain* software vede l'integrazione dei SBOM con altri artefatti di attestazione. Il *framework* SLSA (*Supply-chain Levels for Software Artifacts*), proposto da Google nel 2021 e ora gestito dalla OpenSSF sotto la Linux Foundation, definisce livelli di maturità che includono la generazione di SBOM come requisito fondamentale. L'integrazione con Sigstore per la firma *keyless* dei *build* rappresenta la frontiera emergente della sicurezza

della *supply chain*.

Conclusioni: dalla *compliance* alla resilienza sistemica

Il *Cyber Resilience Act* trasforma il SBOM da strumento di visibilità opzionale a requisito normativo vincolante per l'accesso al mercato europeo. Questa transizione impone alle organizzazioni un ripensamento dei processi di sviluppo software che trascende la mera adozione di strumenti tecnici.

La scelta tra SPDX 3.0 e CycloneDX 1.6 non deve essere formulata in termini di esclusione reciproca. L'approccio ottimale prevede la capacità di generare e consumare SBOM in entrambi i formati, garantendo interoperabilità con l'intero ecosistema di fornitori, clienti e autorità di vigilanza. Gli investimenti in automazione della generazione e gestione dei SBOM costituiscono prerequisito per la sostenibilità operativa degli obblighi CRA nel lungo periodo.

La visione sottesa al regolamento europeo trascende la protezione del singolo prodotto per abbracciare la resilienza dell'intero ecosistema digitale. In un mondo dove ogni prodotto software eredita vulnerabilità e rischi dalle proprie dipendenze, la trasparenza documentata rappresenta condizione necessaria per la gestione sistemica del rischio cyber. Le organizzazioni che sapranno integrare questa visione nella propria cultura di sviluppo acquisiranno vantaggio competitivo duraturo in un mercato dove la sicurezza diventa progressivamente criterio di selezione primario.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/spdx-3-0/>