

Settembre 2026

WEBINAR · SONATYPE

La nuova realtà normativa europea

Come essere conformi alle nuove normative con SBOM e Policy applicate

NIS2

DORA

EU AI ACT

CRA



Speakers:

Giampaolo Flace

DevOps & Product Architect

Profesia - Lynx Group

Giorgio De Vita

Sales & Account Manager

Profesia - Lynx Group

PROFESIA

a company of lynx group

PROFESIA, Polo innovativo del Gruppo Lynx



Il 2026: la svolta normativa

Il 2026 apre una delle **trasformazioni normative più significative** per chi sviluppa e distribuisce software.

NIS2

Infrastrutture e servizi critici

DORA

Settore finanziario

EU AI ACT

Sistemi di intelligenza artificiale

CRA

Prodotti con elementi digitali

Tratti comuni: obblighi di notifica, security by design, responsabilità sulla supply chain, evidenze documentali.

Obiettivo: costruire capacità organizzative e tecniche una volta sola, valide per più normative contemporaneamente.

Perché riguarda quasi tutte le aziende

>90%

delle organizzazioni al mondo
rientra nell'ambito di
applicazione di almeno una di
queste normative.

- Bastano «**impresso sul mercato**» o «**messo a disposizione**».
- **Non serve vendere:** anche il software gratuito rientra nell'ambito applicativo!
- **Open source:** esistono eccezioni, ma usato in servizi commerciali genera obblighi e responsabilità.
- **Calendari diversi,** ma direzione unica per tutte le normative

Direzione: più trasparenza, più responsabilità, più capacità di dimostrazione.

Le date da segnare

Normativa	In vigore	Applicazione degli obblighi
NIS2 Dir. UE 2022/2555	16 gennaio 2023	dal 18 ottobre 2024 — recepimento nazionale; attuazione ancora in evoluzione
DORA Reg. UE 2022/2554	16 gennaio 2023	17 gennaio 2025 — già applicabile
EU AI Act Reg. UE 2024/1689	1 agosto 2024	Divieti 2 febbraio 2025 · GPAI 2 agosto 2025 Trasparenza/etichettatura (Art. 50) 2 agosto 2026 Sistemi ad alto rischio — posticipati dal Digital Omnibus (Reg. UE 2026/1744)
CRA Reg. UE 2024/2847	10 dicembre 2024	11 settembre 2026: obbligo reporting vulnerabilità sfruttate attivamente e incident gravi. 11 dicembre 2027: altri obblighi principali.

11 settembre 2026 — partono gli obblighi di reporting del **CRA** (Art. 14): early warning 24 h → notifica 72 h → report finale.
Vale anche per i prodotti già immessi sul mercato.

Notificare gli incidenti, in tempi certi

24 h

Prima segnalazione

all'autorità competente:
autorità nazionale - CSIRT - ENISA



72 h

Informazioni approfondite

dettagli e valutazione dell'impatto
dell'incidente



Root cause

Analisi della causa principale

conclusione dell'iter di notifica

Capacità richieste: rilevare, comprendere, documentare, comunicare.

Perché: in passato fughe di dati e incidenti presso fornitori terzi sono emersi dai media, non dalle aziende coinvolte. Le normative europee puntano a **trasparenza** e **tutela** di utenti e consumatori.

La software supply chain al centro

≈ 90%

del software è **codice di terze parti**:
librerie, framework, pacchetti,
componenti open source

- **Non basta sapere di usarli**: bisogna assumersene la responsabilità del rischio
- **Vulnerabilità note e sfruttabili** nei componenti = responsabilità dell'organizzazione
- **«Conoscere e controllare la propria software supply chain»**: è il filo rosso di tutte le normative

Ambiti diversi, stessa logica:

NIS2

infrastrutture e servizi critici

AI Act

sistemi AI

DORA

settore finanziario

CRA

prodotti con elementi digitali

Security by design, Vulnerability Management e CVD

Security by design

- configurazioni sicure per impostazione predefinita
- identificare le vulnerabilità note
- correggerle rapidamente
- monitoraggio continuo dei componenti
- tracciamento delle dipendenze
- documentazione delle attività svolte

Programmi richiesti

- **Vulnerability Management** solido e documentato
- **Coordinated Vulnerability Disclosure (CVD)**: ricevere, identificare, valutare, correggere, comunicare, documentare
- **Governance e accountability (es. DORA)**: incidenti, supply chain, fornitori, rischio, continuità, resilienza digitale

Regola d'oro — non basta la policy sulla carta: quando arrivano i regolatori servono **evidenze** che i processi esistono e vengono applicati.

NIS2 — Sicurezza delle reti e dei sistemi informativi

In vigore · 16 gen 2023

Recepimento · 17 ott 2024

Applicazione · dal 18 ott 2024

attuazione nazionale ancora in evoluzione

Ambito ampliato

Infrastrutture critiche, banche e servizi finanziari, sanità, manifattura, tecnologia e software, servizi crittografici, ...

Notifica incidenti gravi

Servizio indisponibile, danni digitali o fisici →

Notifica entro 24h ad autorità competente, poi analisi approfondita e **Root Cause Analysis**

Pilastri di conformità

- Politiche di gestione del rischio
- Sicurezza della supply chain
- Gestione dei fornitori
- Incident management
- Continuità operativa e disaster recovery
- Crisis management

Sanzioni: fino a ~10 M€ o 2% del fatturato globale - **responsabilità personale dei dirigenti**, fino alla sospensione dall'attività.

DORA — Digital Operational Resilience Act

In vigore · 16 gen 2023

Applicabile · 17 gen 2025

banche, istituzioni finanziarie, enti interessati

Incidente maggiore

Notifica iniziale **entro 4 ore** dalla classificazione come grave, e comunque **entro 24 ore**

Da documentare

- Sistemi IT, hardware, reti
- Dipendenze di terze parti
- ... anche la supply chain dei propri fornitori

Gestione del rischio ICT

- Incident response, recovery, business continuity
- Gestione fornitori e dipendenze tecnologiche
- Identificazione degli asset

Effetti a valle

SBOM richieste ai fornitori.

Secondary compliance: la conformità si propaga lungo la supply chain.

Chi fornisce servizi a un soggetto DORA può essere obbligato contrattualmente a requisiti analoghi, anche senza esservi direttamente soggetto.

EU AI Act — Il regolamento sull'intelligenza artificiale

In vigore · 1 ago 2024 con applicazione a scaglioni

2 feb 2025

Divieti sulle pratiche AI inaccettabili + AI literacy

2 ago 2025

Obblighi GPAI, governance, sanzioni

2 ago 2026

Trasparenza ed etichettatura (Art. 50) — già applicabile

2 dic 2027

Sistemi alto rischio (Allegato III) — posticipati dal Digital Omnibus (Reg. UE 2026/1744)

2 ago 2028

Alto rischio integrato in prodotti regolamentati (Allegato I)

Obblighi principali

- Sistema di gestione del rischio
- Governance dei dati e qualità dei dataset
- Trasparenza e informazione agli utenti
- Documentazione tecnica, registri, cybersecurity
- Logging automatizzato del ciclo di vita

Etichettatura AI

Contenuti generati o modificati da AI identificabili come tali: deepfake, chatbot, sistemi agentici, riconoscimento emozioni, ecc.

CRA — Cyber Resilience Act: ambito e requisiti

In vigore · 10 dic 2024

Reporting · 11 set 2026

Obblighi principali · 11 dic 2027

Può riguardare ~90% del software reso disponibile sul mercato UE: software · dispositivi IoT · sistemi operativi · prodotti con elementi digitali — obblighi anche per importatori e distributori

Requisiti minimi

Security by design, configurazioni sicure, assenza di vulnerabilità note sfruttabili, gestione delle vulnerabilità.

Evidenze e tracciabilità

SBOM, raccolta delle evidenze, gestione degli incidenti · tracciabilità delle release.

Aggiornamenti di sicurezza

Garantiti per almeno 5 anni, o per la durata del ciclo di vita del prodotto se più breve.

Marcatura CE

Autodichiarazione per la maggior parte dei prodotti, mentre per le categorie più critiche servono controlli o valutazioni da parte di organismi notificati.

Reporting, open source e responsabilità

1

Reporting

Piattaforma centralizzata europea (ENISA + CSIRT):

Early Warning 24 h → notifica 72 h → report finale.

Servono **processi automatizzati**: rilevare vulnerabilità, valutare l'impatto, classificare, segnalare.

Vale anche per prodotti già immessi sul mercato.

2

Open source

Usarlo non trasferisce il rischio: il produttore del prodotto finale deve conoscere e gestire i componenti incorporati e le loro **vulnerabilità**.

3

Product liability

Esteso ai prodotti digitali: se non dimostri la **conformità** emergono responsabilità legali (*le clausole contrattuali non bastano*).

Sanzioni per grave non conformità: fino al 2,5% del fatturato annuo globale o almeno 15M €

La conformità diventa tecnica

Per ogni build

- Conoscere tutte le dipendenze e la loro provenienza
- Generare o verificare la SBOM
- Identificare ed eliminare le vulnerabilità sfruttabili
- Applicare le policy di security by design
- Pianificare gli aggiornamenti di sicurezza
- Conservare SBOM + evidenze con ogni release

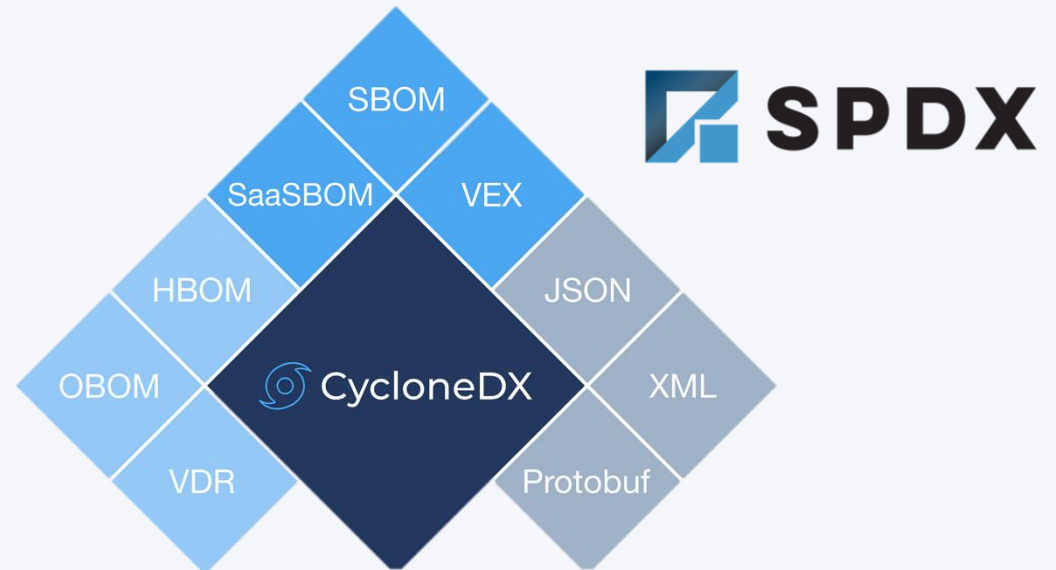
La normativa diventa tecnica e prescrittiva:

le autorità specificano quali evidenze produrre e in quale formato.
Non basta dire che «la sicurezza è gestita»!

Tecniche richieste

SCA · SAST · DAST · Security Testing Continuo

Formati SBOM Machine-Readable



Il ciclo continuo e le quattro priorità



i risultati alimentano nuovamente le policy: un ciclo continuo

1

Conoscere le dipendenze

Componenti, provenienza, versioni, vulnerabilità, fornitori software.

2

Prevenire il rischio

Blocchi automatici e dependency firewall, anche sulle dipendenze introdotte dall'AI.

3

Eliminare le vulnerabilità gravi

Security gate nell'SDLC: zero spazio alle vulnerabilità critiche in produzione.

4

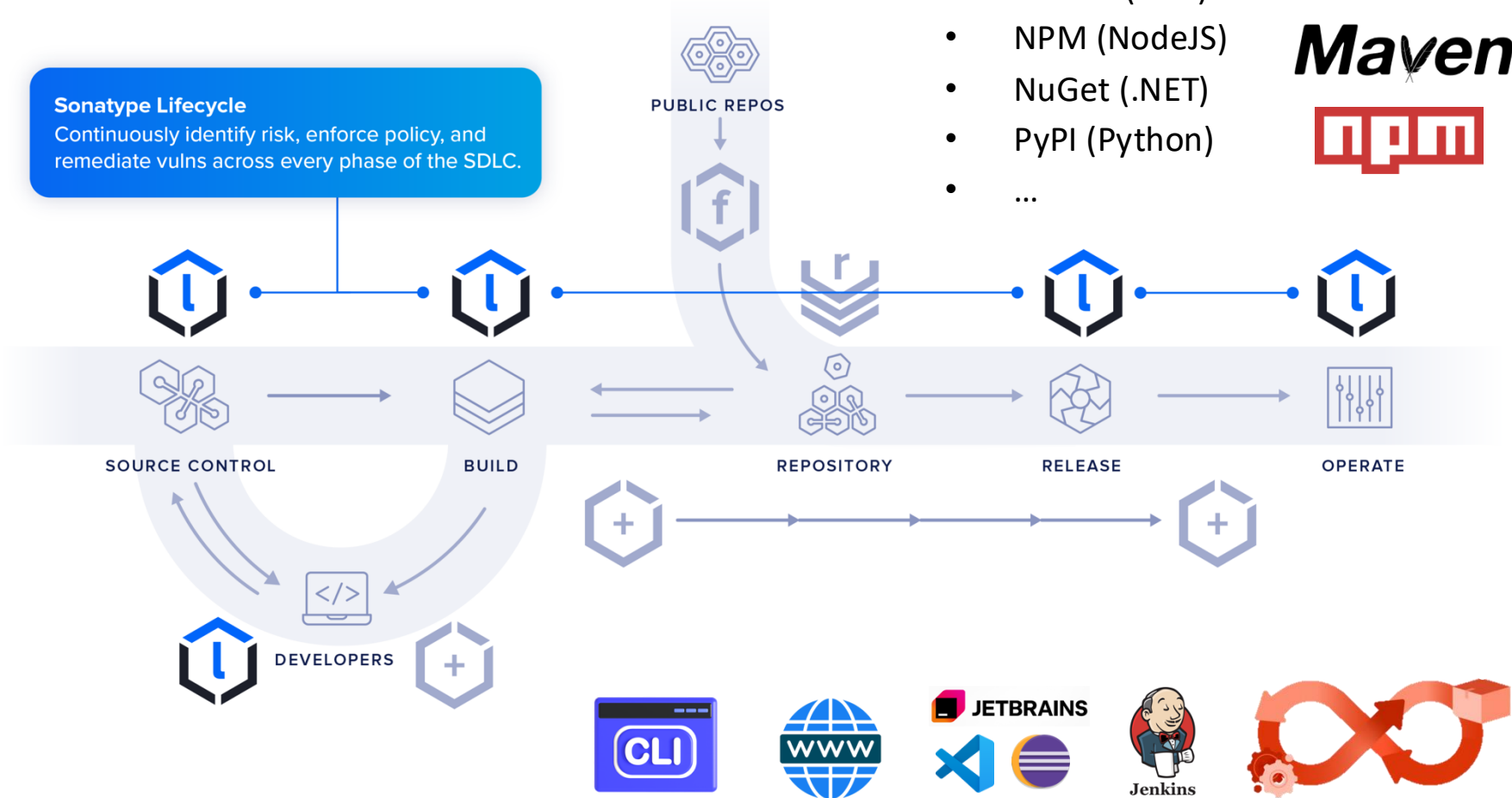
Attestare ogni artefatto

Cosa, con quali componenti, quali controlli, quali policy applicate.

Da **abbiamo una policy di sicurezza** a **la pipeline applica la policy, genera le evidenze e dimostra la conformità.**

Sonatype Lifecycle / Repository Firewall / Guide — intelligence su open source, malware, vulnerabilità, licenze · SBOM · SCA · governance AI/open source

Sonatype Lifecycle (SCA)



Controllo **licenze** dipendenze OSS



Generazione
Report + SBOM

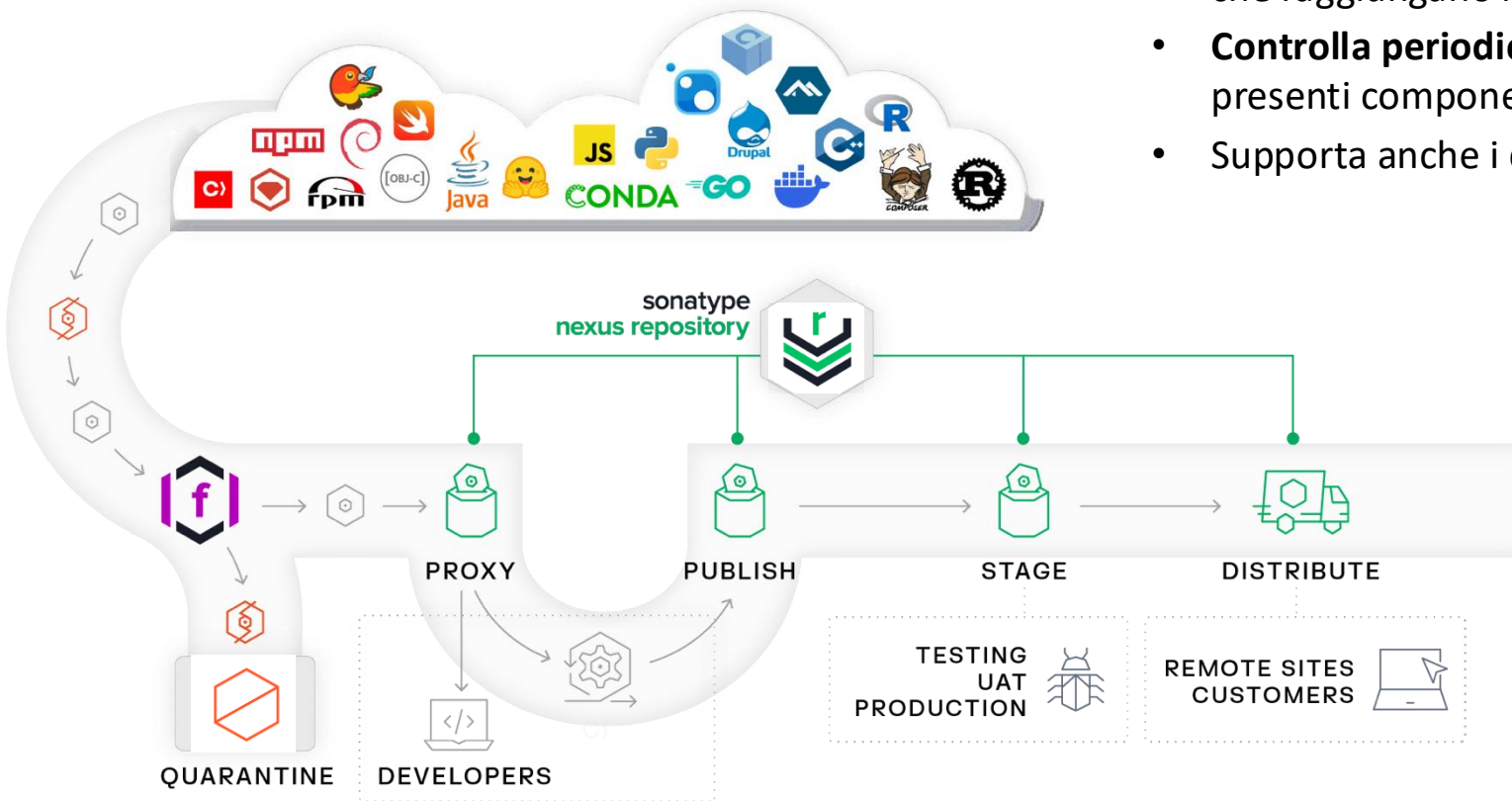


Scan vulnerabilità su
**immagini Docker e
modelli di AI**



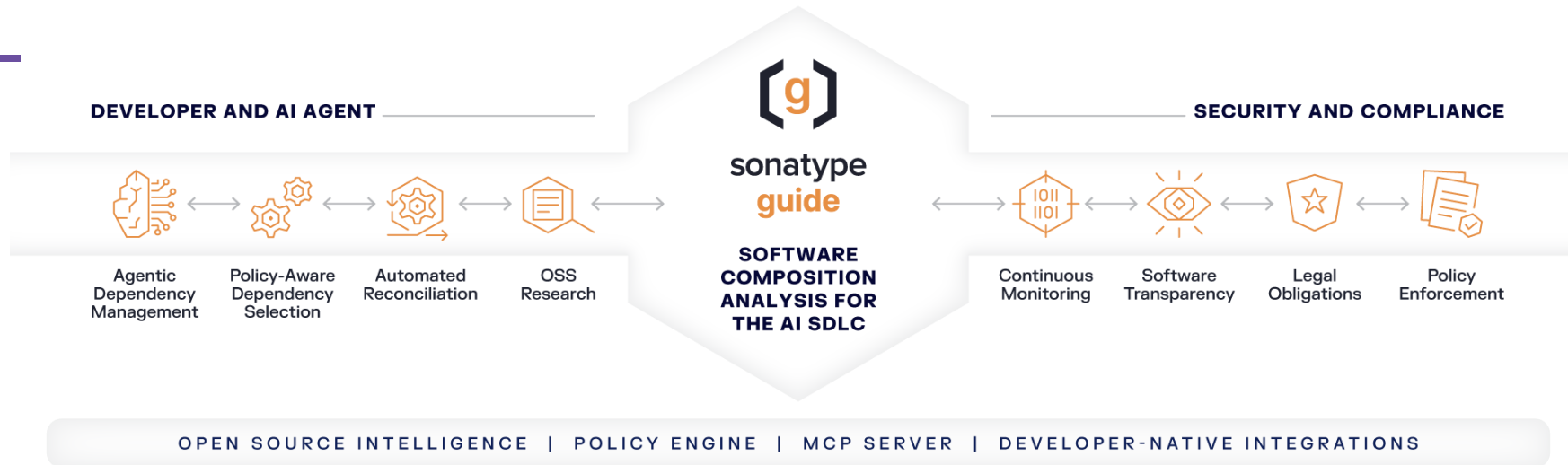
Monitoraggio continuo delle
dipendenze precedentemente
analizzate;

Sonatype Repository Firewall



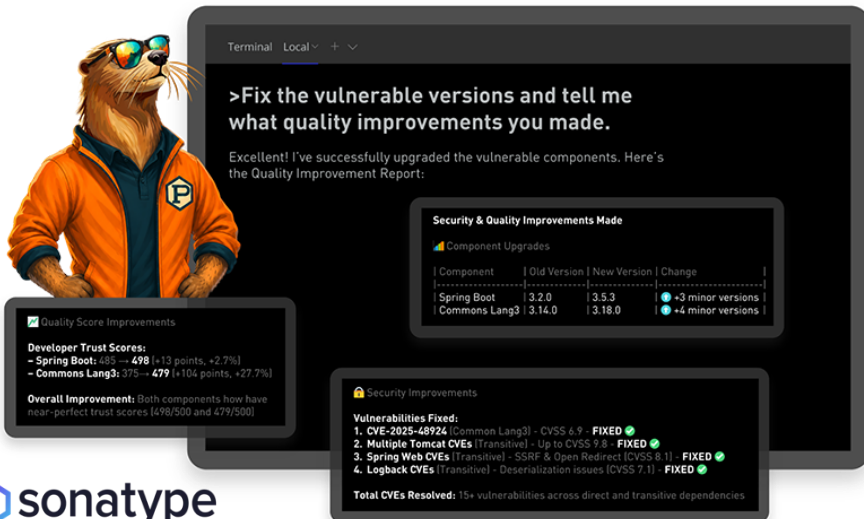
- Si integra su:
 - **Nexus Repository;**
 - **Artifactory** (plugin);
 - **Blocca** le componenti OSS vulnerabili prima che raggiungano i **repository proxy / remote;**
 - **Controlla periodicamente** se nei repository proxy sono presenti componenti vulnerabili.
 - Supporta anche i **docker repository proxy.**
- Le componenti vulnerabili finiscono in una zona di **quarantena** piuttosto che nella cache dei proxy repository.
 - Tramite una **waiver** può essere aggiunta una componente vulnerabile in whitelist.
 - Passiamo da un modello reattivo (damage control dopo l'infezione) a un **modello preventivo**, bloccando la minaccia all'origine.

Sonatype Guide (Agent P)



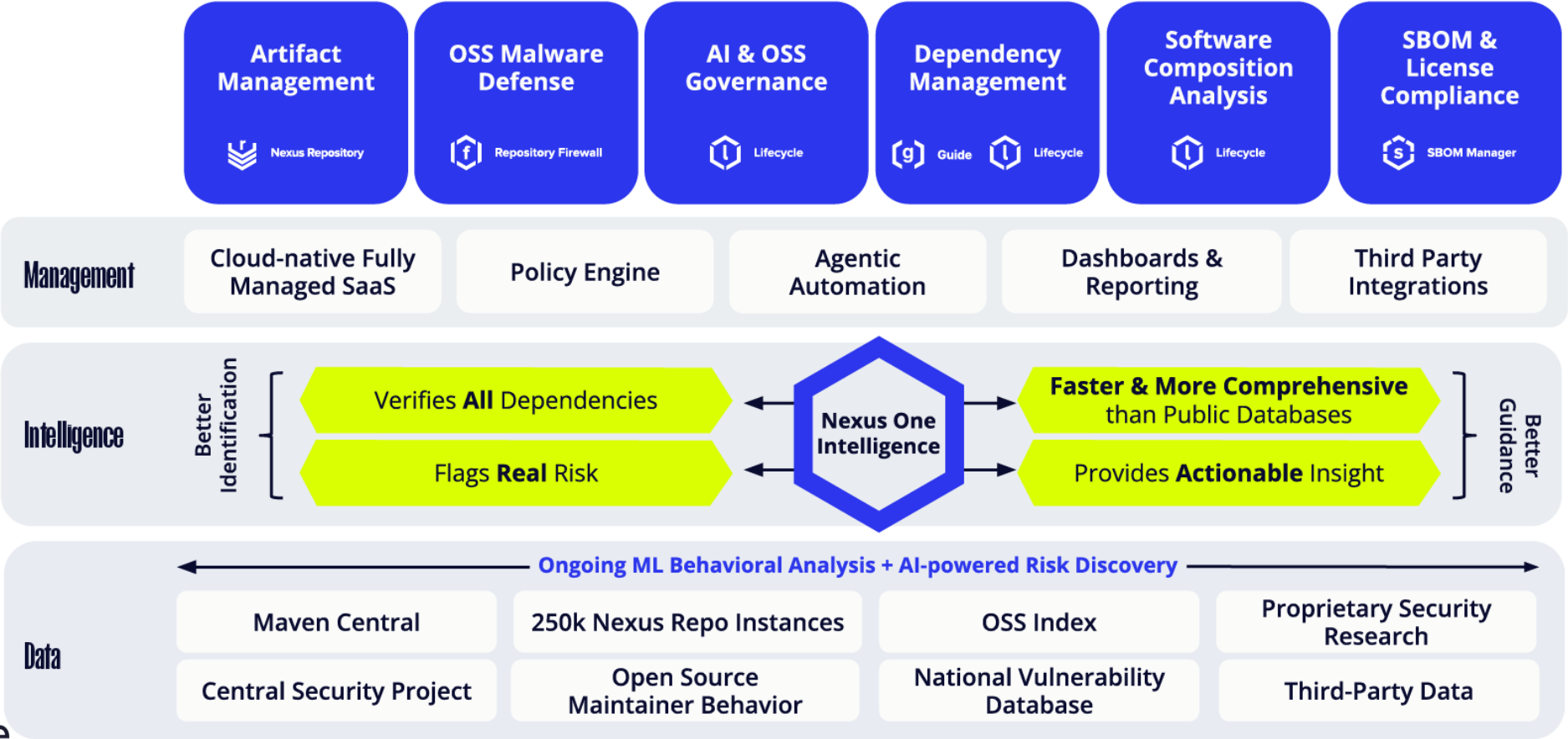
Agent P, tramite **Sonatype Guide MCP**, porta l'intelligence sulle dipendenze direttamente negli assistenti AI di coding.

- Seleziona le versioni migliori prive di vulnerabilità;
- Applica e valida gli aggiornamenti;
- Mantiene le dipendenze continuamente aggiornate;
- Riduce il lavoro manuale degli sviluppatori.



Sonatype Nexus One Platform

Nexus One Platform



Grazie per l'attenzione!

Q&A?

sales@profesia.it

PR  FESIA

a company of lynx group

 sonatype®

THANK YOU!