

Software-Inventar und SBOM für OutSystems:

Wissen Sie wirklich, was in Ihren
OutSystems-Apps steckt?



Das Team



Marius Neumann
Senior Consultant



André Ortmann
Consultant



Franziska Surmund
Business Development

Unsere Webinar-Reihe im Juli



09.07. | 11:00 Uhr

**Was Agentic
Systems Engineering
für Ihr Unternehmen
bedeutet**



14.07. | 11:00 Uhr

**KI-Agenten sicher
einsetzen – Daten,
Guardrails &
Compliance**



16.07. | 11:00 Uhr

**Vom Prompt zur
fertigen Anwendung
– OutSystems Mentor
live erleben**



21.07. | 11:00 Uhr

**Wie ihr OutSystems-
Team den nächsten
Produktivitätssprung
macht**



Aufzeichnung anfordern



Über die agentbase

- Beratungs- & Implementierungspartner
- seit 2018 OutSystems Partner
- Digitalisierung von Prozessen
- Entwicklung maßgeschneiderter IT-Lösungen
- Full-Service Provider
- Team aus umfangreich zertifizierten Consultants



Supply Chain Attacks Are No Longer Rare Events

Shai-Hulud 2.0

npm ecosystem · November 2025

796

npm packages backdoored

25,000+ malicious GitHub repos, ~14,000 secrets exposed
Self-replicating worm – wiped home directories as fallback

Axios

npm ecosystem · March 2026

100M+

weekly downloads of the affected library

Remote access trojan installed on every npm install
Live for only ~3 hours · attributed to North Korean actor
UNC1069

These attacks don't target your code — they target the libraries you build on.

“We Build Low-Code – This Doesn’t Affect Us.”

Your OutSystems apps & modules

Low-code has a supply chain, too.

Every OutSystems application references code you didn’t write – and by default can’t see.

Your visibility ends here

- C# extensions
- Forge components (unknown sources)
- Third-party .NET libraries
- Transitive dependencies

Remember Log4j (2021)?

The flaw sat deep in transitive references. Tools that couldn’t resolve them could not tell who was affected – for weeks.

Regulators Hold You Accountable for Your Supply Chain

NIS2

In force – EU-wide

Essential & important entities in 18 critical sectors

Supply-chain security is a mandatory measure

Incident early warning within 24 hours

Fines up to €10M or 2% of global turnover
– management personally accountable

DORA

Applies since Jan 2025

Financial sector: banks, insurers, their ICT providers

ICT third-party risk management

Register of all ICT dependencies

Strict incident classification & reporting

CRA

Obligations 2026/2027

All products with digital elements on the EU market

Security by design & vulnerability handling

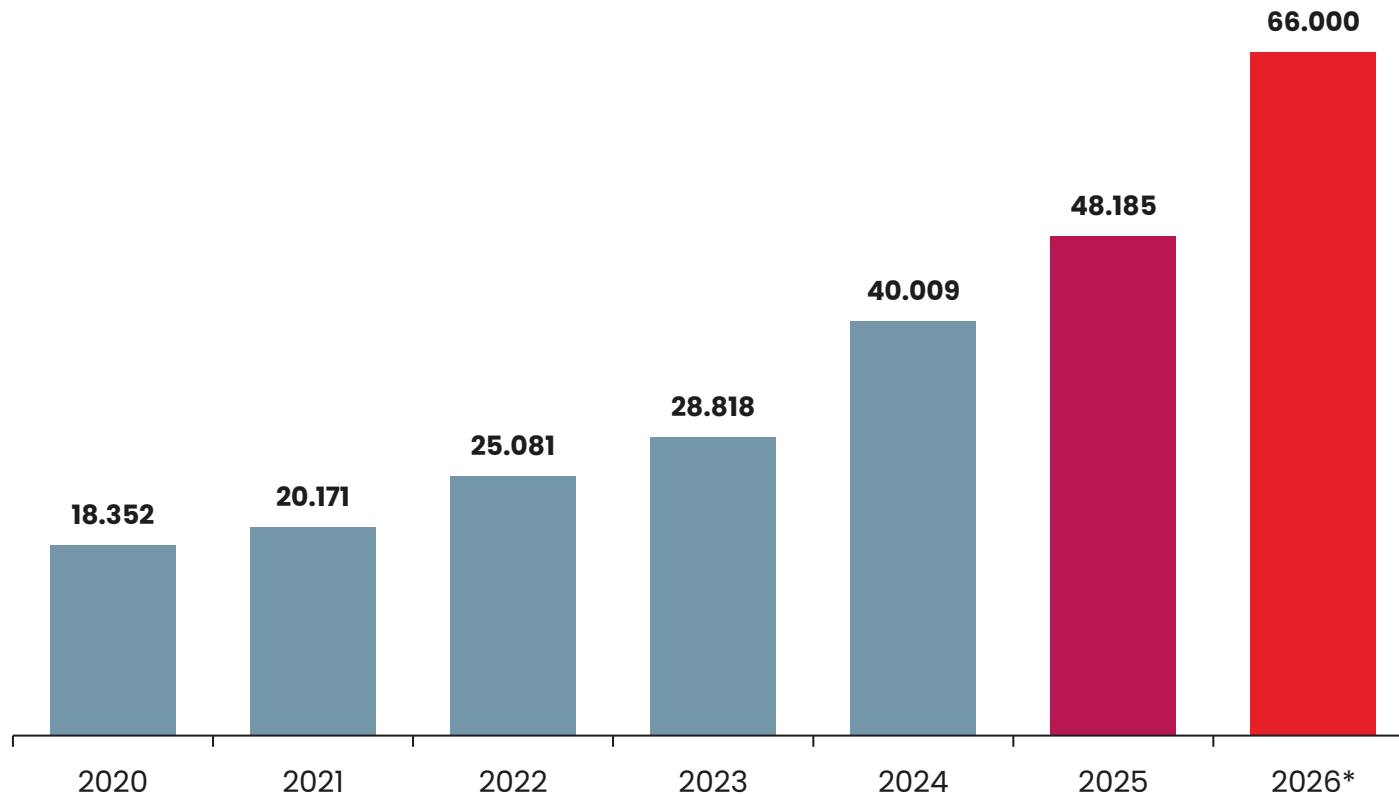
Explicitly requires an SBOM

Fines up to €15M or 2.5% of global turnover

The common denominator: you must know – and document – what is inside your software.

More Vulnerabilities Than Ever – AI Is Accelerating It

CVEs published



48,185

CVEs published in 2025 – an all-time record
(~131 per day)

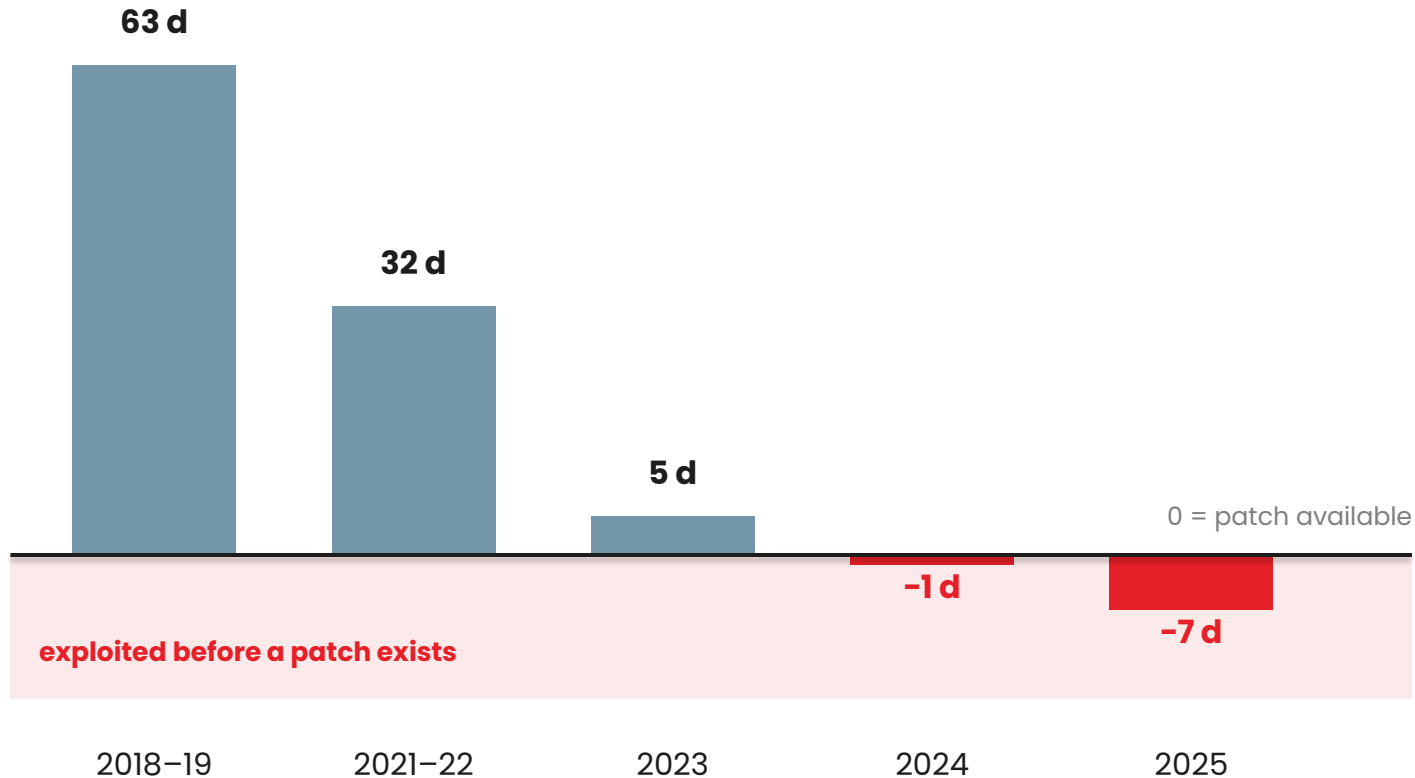
3.5×

the previous monthly record of high/critical
CVEs since AI models entered vulnerability
research (June 2026)

* 2026: ~66,000 forecast

Exploited Before You Can Patch

Average days from disclosure to exploitation



-7 days

average time-to-exploit in 2025: the average vulnerability is exploited before a patch exists

24 hours

is what NIS2 gives you for the first incident warning – manual dependency analysis takes weeks

What a Successful Attack Costs

Case: MOVEit (2023)

One vulnerability in one file-transfer product

2,700+

organizations breached worldwide

93.3M

individuals' personal data exposed –
names, addresses, SSNs, financial data

Total damage estimates run into the billions (up to \$12.15B).

\$160

average cost per compromised customer record – and 53%
of all breaches expose customer PII

Quick math for your applications:

250,000 customer records

× \$160 ≈ \$40M potential exposure

The average supply-chain breach: \$4.91M – and 267 days to identify and contain.

What is OSIS?

- **“OutSystems Software Inventory & SBOM”**

- Platform to build a full picture of **assets and their relationships** in OutSystems and referenced third party libraries
- Full **automation** from development to complete license and vulnerability management and escalation
- Possible integration into **CI/CD pipelines**
- Also covering OutSystems **Forge assets**, often coming from unknown sources
- Support of **SBOM standard** CycloneDX to allow easy integration in tools for further processing
- **Ad-hoc** available

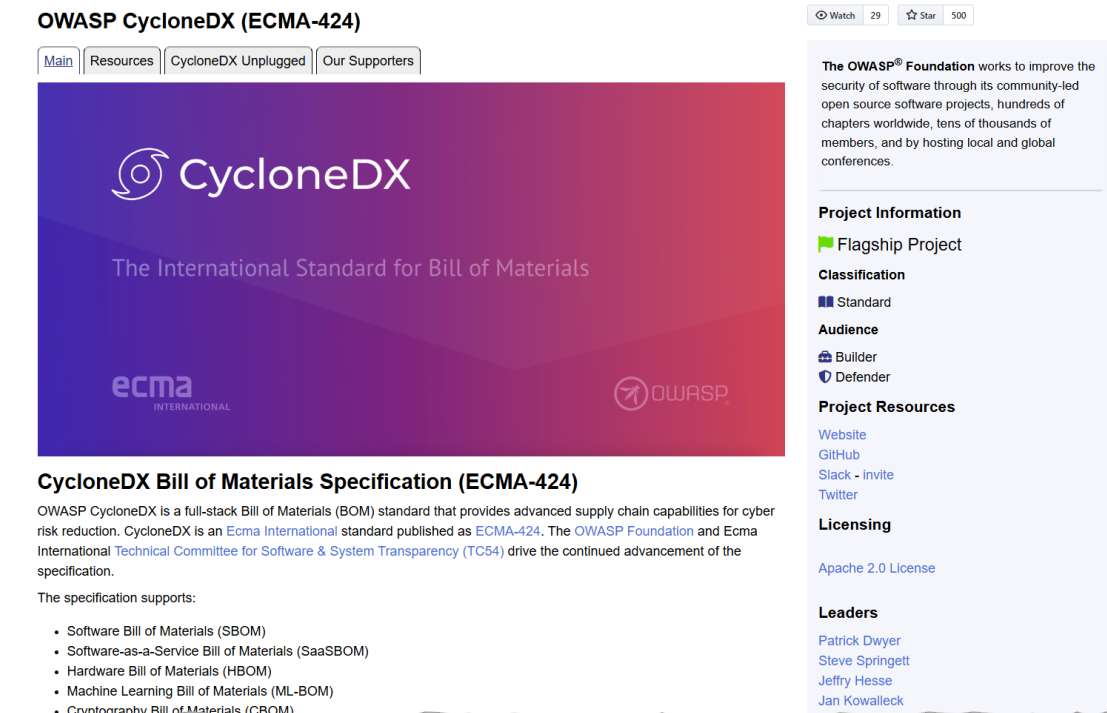
- In practice is useful for

- **Security teams**, for transparency of components and alerting of **up-to-date vulnerabilities**.
- **Developers**, for tracking and **identifying dependencies** more clearly
- **Compliance teams**, for checking **license** and **supply-chain requirements**.

What is SBOM ?

SBOM stands for a **Software Bill of Materials**. It is a detailed inventory of the software's building blocks, such as third-party libraries, open-source components, and other dependencies used inside an application.

OSIS supports the **CycloneDX** SBOM format, which is one of the leading formats provided by OWASP. Under **Apache 2.0 Licence** publically commercially usable.



The screenshot shows the GitHub repository page for OWASP CycloneDX (ECMA-424). The page features a navigation bar with links to Main, Resources, CycloneDX Unplugged, and Our Supporters. The main content area has a large banner with the CycloneDX logo and the text "The International Standard for Bill of Materials", along with the ECMA International and OWASP logos. Below the banner, the title "CycloneDX Bill of Materials Specification (ECMA-424)" is followed by a detailed description of the standard and its purpose. A list of supported specifications is provided, including SBOM, SaaSOM, HBOM, ML-BOM, and CBOM. On the right side, there is a sidebar with project information, including a description of the OWASP Foundation, project classification as a "Flagship Project", audience (Builder and Defender), project resources (Website, GitHub, Slack, Twitter), licensing (Apache 2.0 License), and a list of leaders (Patrick Dwyer, Steve Springett, Jeffrey Hesse, Jan Kowalleck).

OWASP CycloneDX (ECMA-424)

[Main](#) | [Resources](#) | [CycloneDX Unplugged](#) | [Our Supporters](#)

CycloneDX
The International Standard for Bill of Materials

ecma INTERNATIONAL | OWASP

CycloneDX Bill of Materials Specification (ECMA-424)

OWASP CycloneDX is a full-stack Bill of Materials (BOM) standard that provides advanced supply chain capabilities for cyber risk reduction. CycloneDX is an [Ecma International](#) standard published as [ECMA-424](#). The [OWASP Foundation](#) and [Ecma International Technical Committee for Software & System Transparency \(TC54\)](#) drive the continued advancement of the specification.

The specification supports:

- Software Bill of Materials (SBOM)
- Software-as-a-Service Bill of Materials (SaaSOM)
- Hardware Bill of Materials (HBOM)
- Machine Learning Bill of Materials (ML-BOM)
- Cryptographic Bill of Materials (CBOM)

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

Project Information

Flagship Project

Classification

Standard

Audience

Builder
Defender

Project Resources

[Website](#)
[GitHub](#)
[Slack - invite](#)
[Twitter](#)

Licensing

[Apache 2.0 License](#)

Leaders

[Patrick Dwyer](#)
[Steve Springett](#)
[Jeffrey Hesse](#)
[Jan Kowalleck](#)

What is OSIS?

OSIS Applications

Issue Tracker

JWT Library

Local Notifications Plugin

OneSignal Plugin

OpenAI Connector

OpenAI Test

OSIS - OutSystems Software Inventory & SBOM

OSIS Test App 1

OSIS Test App 2

OutSystems Charts

OutSystems Charts V

OSIS Applications

OutSystems Now

OutSystems Sample Data

OutSystems Templat

OutSystems UI

OutSystems UI Web

Platform Extensibility

QuizApp

Randomizer Number Generator

ReactFilePondUploa

49 to 72 of 89 items

OSIS Test App 1

Description

Temporarily for MN

Modules

Dependencies

SBOM

OSISApp1Module1

OSISApp1Module2

OSISApp1Module3

Application overview and details



What is OSIS?



OSIS Applications



OSIS - OutSystems Software Inventory & SBOM

Description

OSIS provides a centralized dashboard to monitor all applications, modules, and dependencies across the OutSystems factory. The platform automates the discovery of assets and streamlines compliance via a one-click SBOM engine.

Modules Dependencies **SBOM**

Create SBOM

File Name Created On Created By

[SBOM-OSIS - OutSystems Software Inventory & SBOM2026-04-16-16-48.json \(7673B\)](#)

16 Apr 2026 16:48



[SBOM-OSIS - OutSystems Software Inventory & SBOM2026-04-16-16-49.json \(24117B\)](#)

16 Apr 2026 16:49



1 to 2 of 2 items



OSIS Applications



OSIS Test App 1

Description

Temporarily for MN

Modules Dependencies **SBOM**

Create SBOM

File Name Created On Created By

[SBOM-OSIS Test App 12026-04-17-16-30.json \(1231B\)](#)

17 Apr 2026 16:30

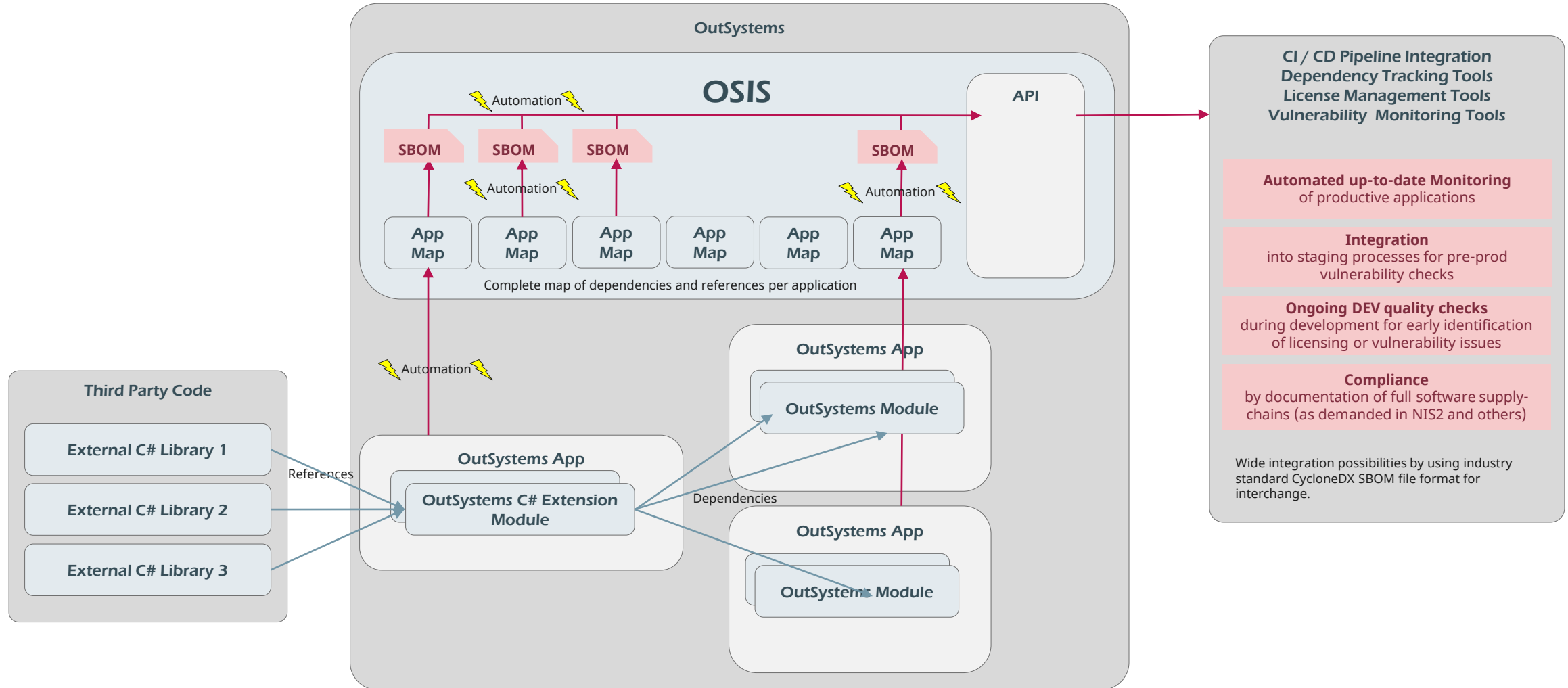


1 to 1 of 1 items

Automated generation of SBOM on application and module level

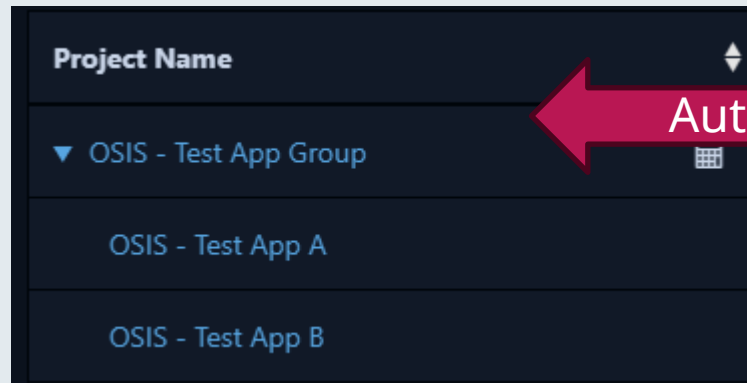


High-Level Overview OSIS

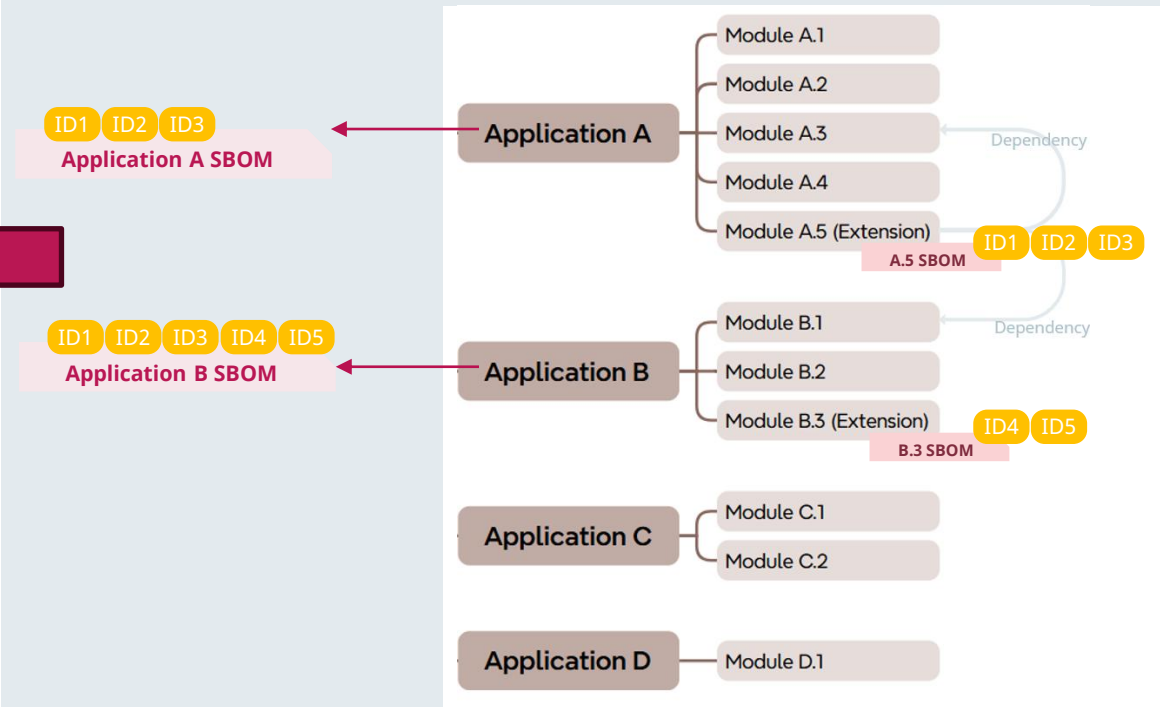


Creation of OS App SBOMs and automated Propagation

Dependency Tracking Tool
(e. g. *Dependency Tracker*)



OSIS



Visibility of incoming vulnerabilities

+ Create Project

x

Show inactive projects

x

Show flat project view

Search

Project Name	Tags	Version	Latest	Classifier	Last BOM Import	BOM Format	Risk Score	Active	Components	Policy Violations	Vulnerabilities
▼ OSIS - Test App Group				Application	-	-	0		8	7 7	0
OSIS - Test App A				Application	17 Apr 2026 at 22:07:59	CycloneDX 1.6	0		4	4 4	0
OSIS - Test App B				Application	17 Apr 2026 at 16:54:17	CycloneDX 1.6	0		4	3 3	0

Showing 1 to 1 of 1 rows

Before adding libraries with affected packages

+ Create Project

☐ x Show inactive projects

☐ x Show flat project view

Search

Project Name	Tags	Version	Latest	Classifier	Last BOM Import	BOM Format	Risk Score	Active	Components	Policy Violations	Vulnerabilities
▼ OSIS - Test App Group				Application	-	-	15	☒	10	8 8	1 1
OSIS - Test App A				Application	17 Apr 2026 at 22:31:37	CycloneDX 1.6	15	☒	6	5 5	1 1
OSIS - Test App B				Application	17 Apr 2026 at 16:54:17	CycloneDX 1.6	0	☒	4	3 3	0

Showing 1 to 1 of 1 rows

After adding libraries with affected packages

Vulnerability Management Scenarios



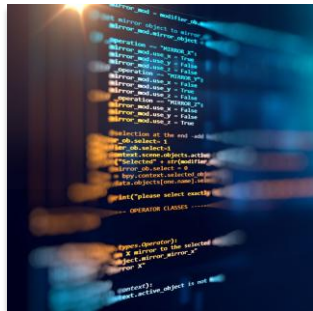
Continuous Infrastructure Monitoring

Monitor application infrastructure regularly, set alerts for vulnerabilities, and document actions taken for improved security.



CI/CD Security Integration

Integrate security checks in CI/CD pipelines to detect vulnerabilities before deploying applications to production environments.



Development Level Vulnerability Scans

Conduct ongoing vulnerability scans during development for early detection and remediation, ensuring safer code releases.

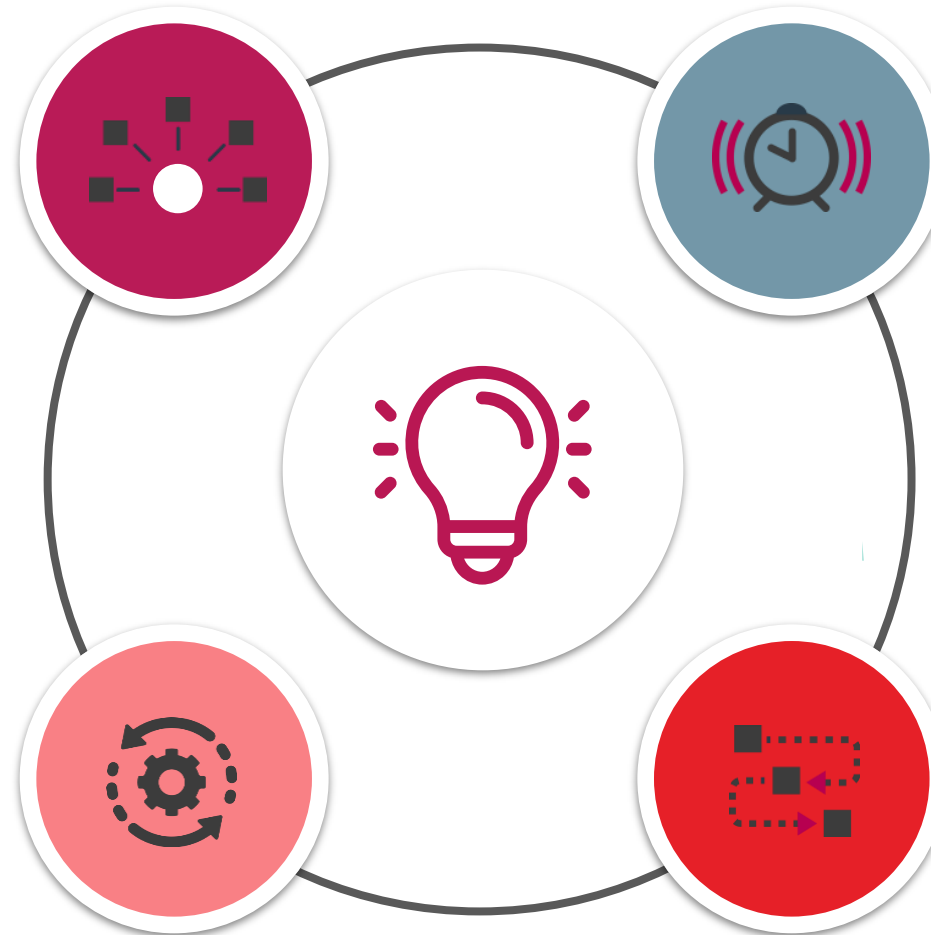
OSIS Service Options

Documentation

- Full Supply Chain
- Licensing
- Which actions have been taken before?

Continuous Monitoring

- Automated SBOM creation
- Seamless integration into tracking tools



Escalation

- Managed Service Agreements to provide quick evaluation and response

Action

- Taking quick and qualified action for emerging security vulnerabilities and license violations

Vielen Dank für Ihre Aufmerksamkeit



agentbase AG
Eggertstraße 7
33100 Paderborn



+49 5251 547 2600



www.agentbase.de



info@agentbase.de



FRANZISKA SURMUND
Business Development



-  +49 5251 547 2614
-  Franziska.Surmund@agentbase.de
-  www.agentbase.de
-  Eggertstraße 7
33100 Paderborn

Erstgespräch buchen

