Software-Inventar und SBOM für OutSystems:

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

agentbase ag

OutSystems/ Partner Silver

Das Team

Marius Neumann
Senior Consultant

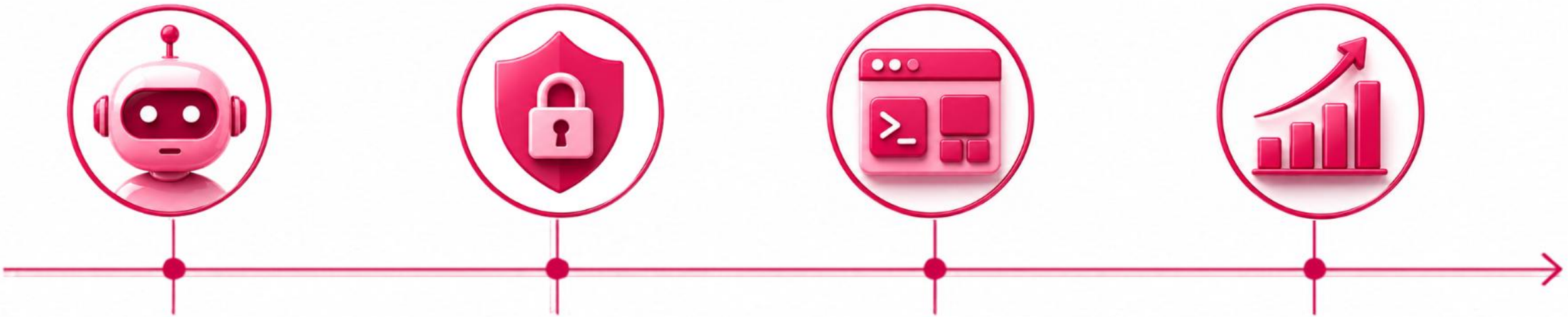
André Ortmann
Consultant

Franziska Surmund
Business Development

agentbase ag

OutSystems/ Partner Silver

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

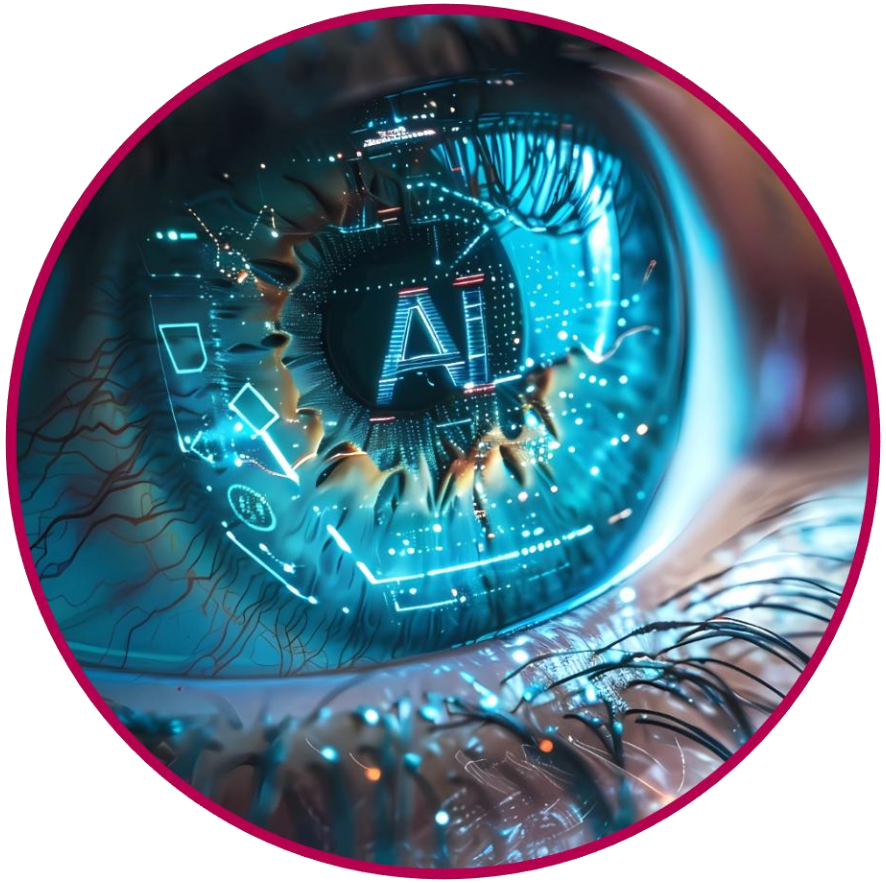
Aufzeichnung anfordern

agentbase ag

OutSystems/ Partner Silver

Über die agentbase

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



agentbase ag

OutSystems/ Partner Silver

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

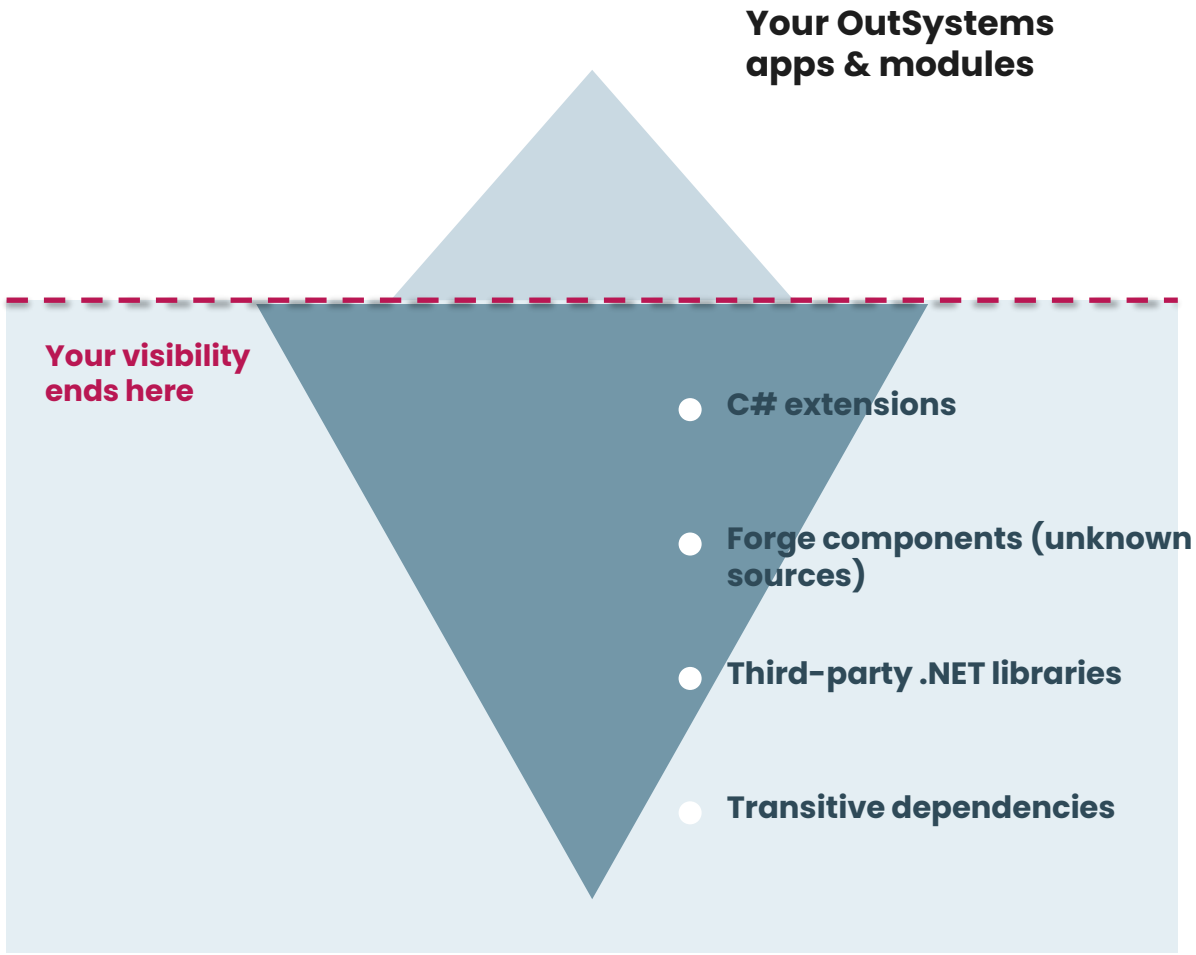
These attacks don't target your code — they target the libraries you build on.

Sources: Unit 42 / Palo Alto Networks (Shai-Hulud 2.0, Nov 2025) · Wiz Research · StepSecurity (Axios, Mar 2026) · Google TIG attribution via Tenable

agentbase ag

OutSystems/ Partner Silver

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



Low-code has a supply chain, too.

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

Remember Log4j (2021)?

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

Sources: Log4Shell: CVE-2021-44228, NIST NVD

agentbase ag

OutSystems/ Partner Silver

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

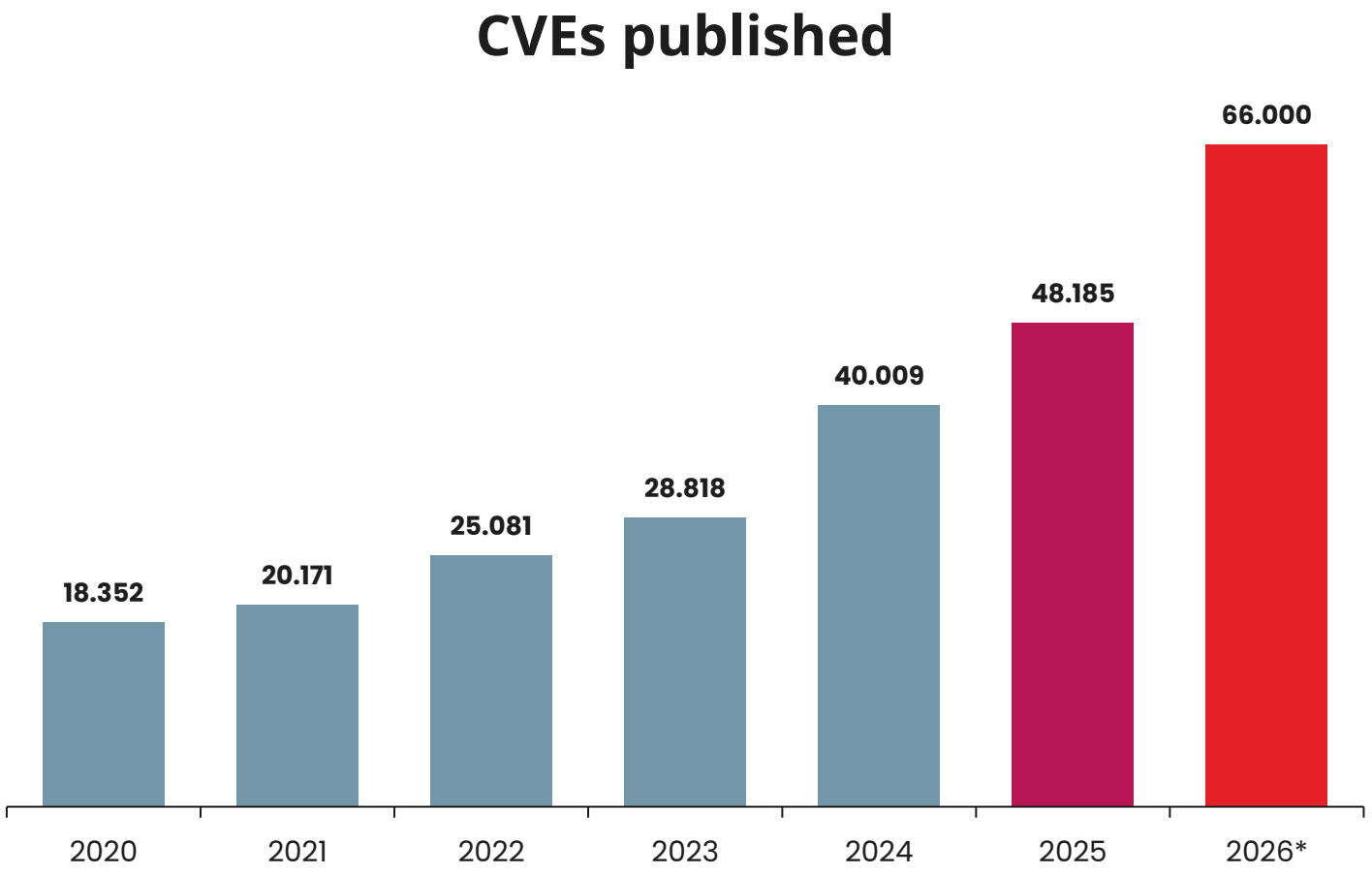
The common denominator: you must know – and document – what is inside your software.

Sources: Directive (EU) 2022/2555 (NIS2) · Regulation (EU) 2022/2554 (DORA) · Regulation (EU) 2024/2847 (CRA) · European Commission: NIS2 Directive

agentbase ag

OutSystems/ Partner Silver

More Vulnerabilities Than Ever – AI Is Accelerating It



48,185

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

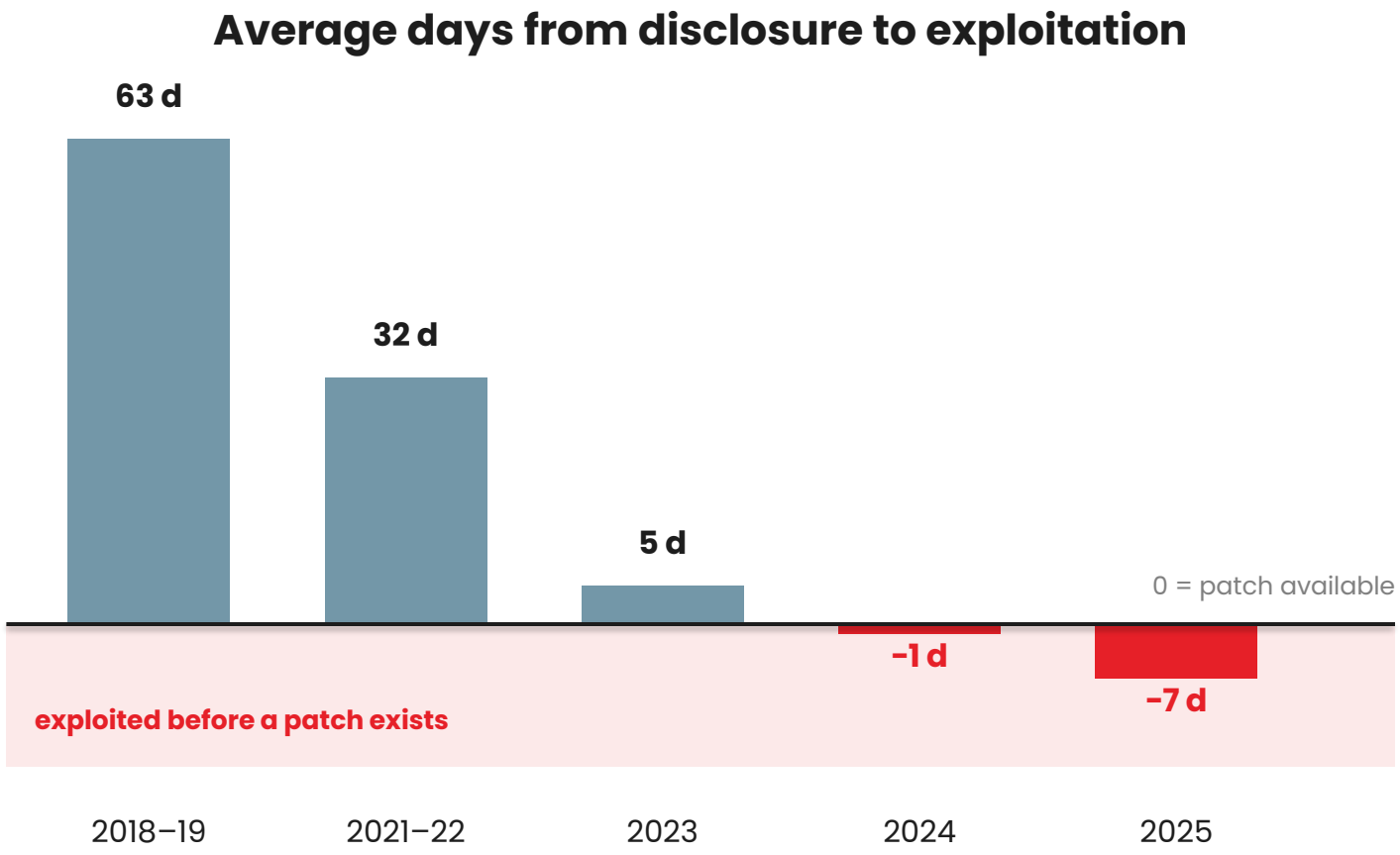
3.5×

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

* 2026: ~66,000 forecast

Sources: CVE Program / NIST NVD · The Stack: CVEs in 2025 · FIRST CVE Forecast 2026 · Epoch AI: 3.5× spike after Claude Mythos

Exploited Before You Can Patch



-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

Sources: Google Mandiant M-Trends 2026 / Google TIG (time-to-exploit) · Directive (EU) 2022/2555, Art. 23 (24h early warning)

agentbase ag

OutSystems/ Partner Silver

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.

Sources: IBM Cost of a Data Breach Report 2025 · Emsisoft: "Unpacking the MOVEit Breach" (cost & victim estimates)

agentbase ag

OutSystems/ Partner Silver

What is OSIS?

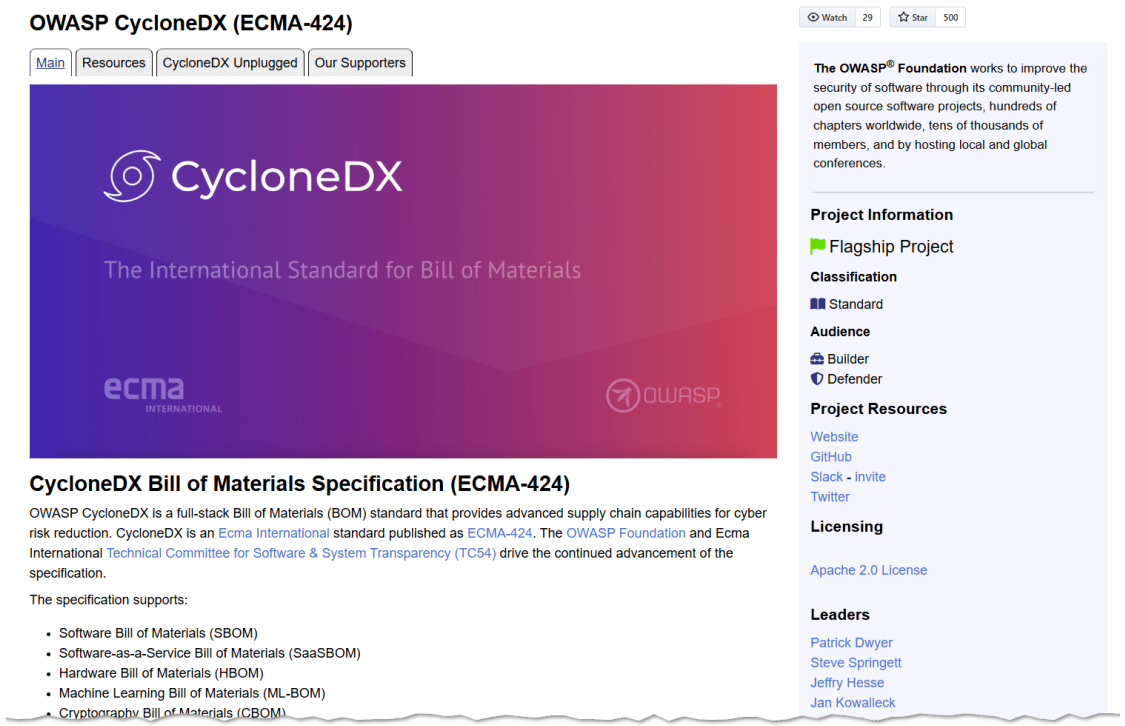
- "**OutSystems Software Inventory & SBOM**"
  - Platform to build a full picture of **assets and their relationships** in OutSystems and referenced third party libraries
  - Full **automation** from development to complete license and vulnerability management and escalation
  - Possible integration 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 vulnerabilites**.
  - **Developers**, for tracking and **identifying dependencies** more clearly
  - **Compliance teams,** for checking **license** and **supply-chain requirements**.

What is SBOM ?

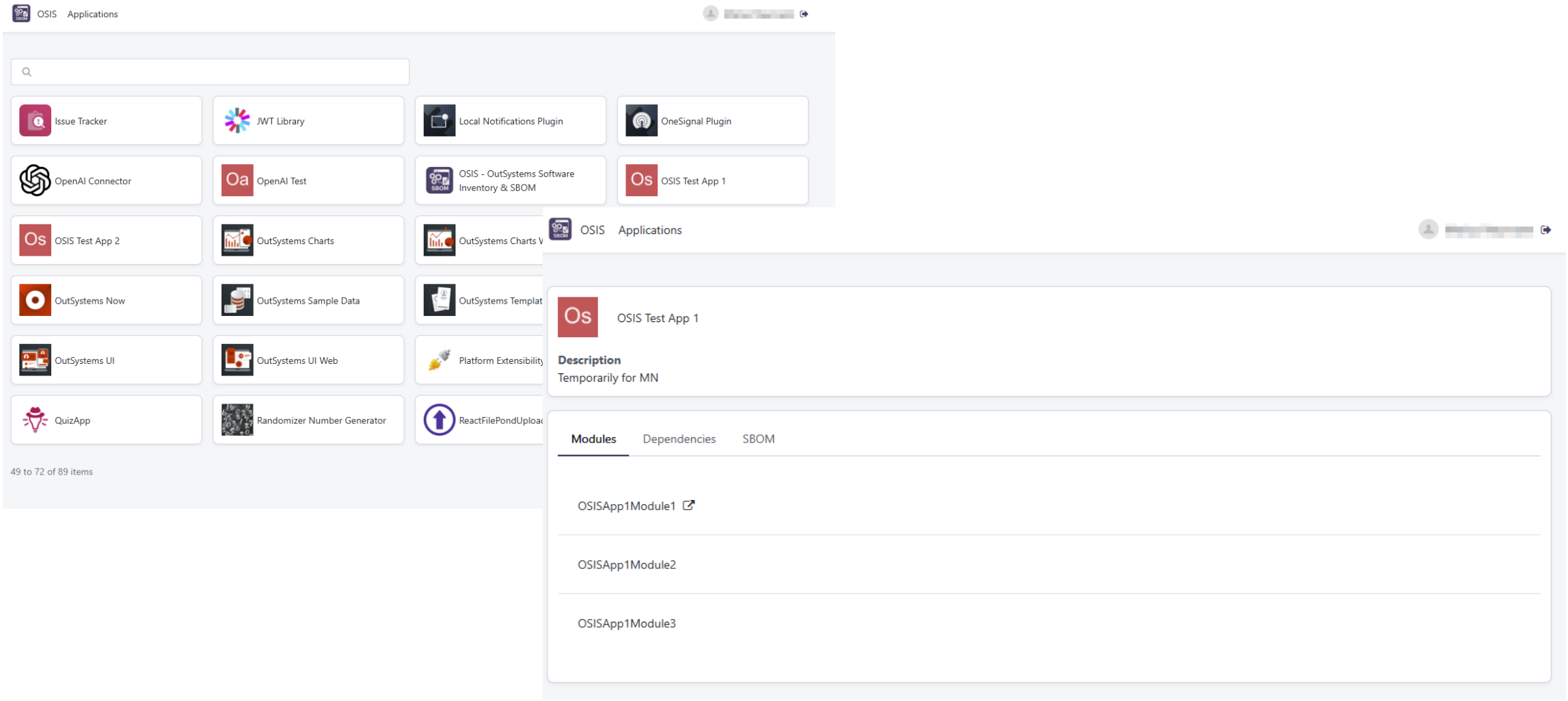
SBOM stands for a **Software Bill of Materials**. It is a detailed inventory of the software's building blocks, such as third-party libraries, open-source components, and other dependencies used inside an application.

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



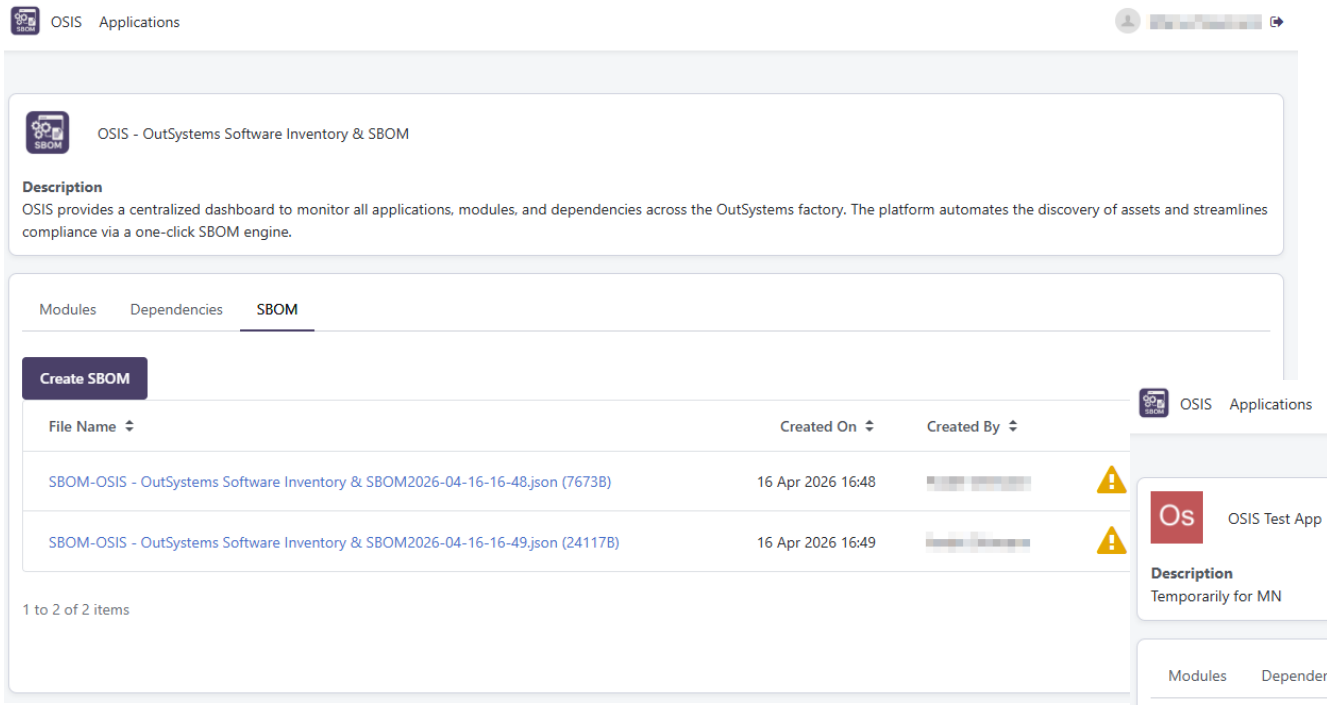
Source: https://owasp.org/www-project-cyclonedx/

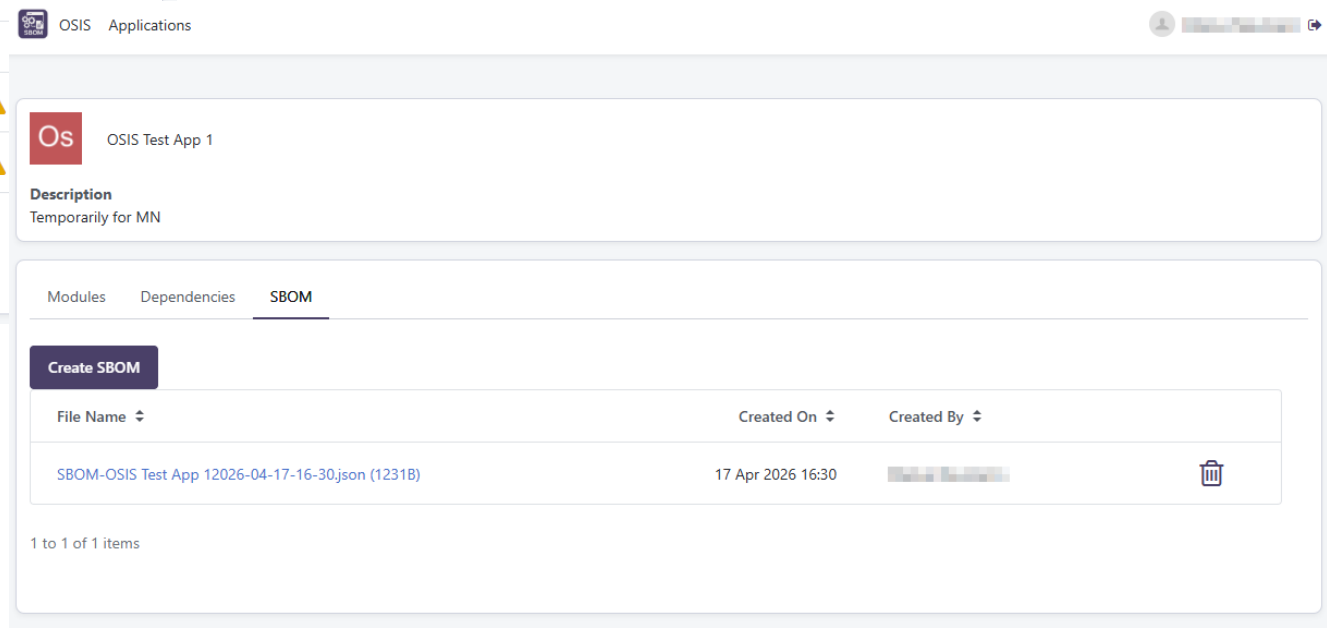
What is OSIS?



Application overview and details

What is OSIS?



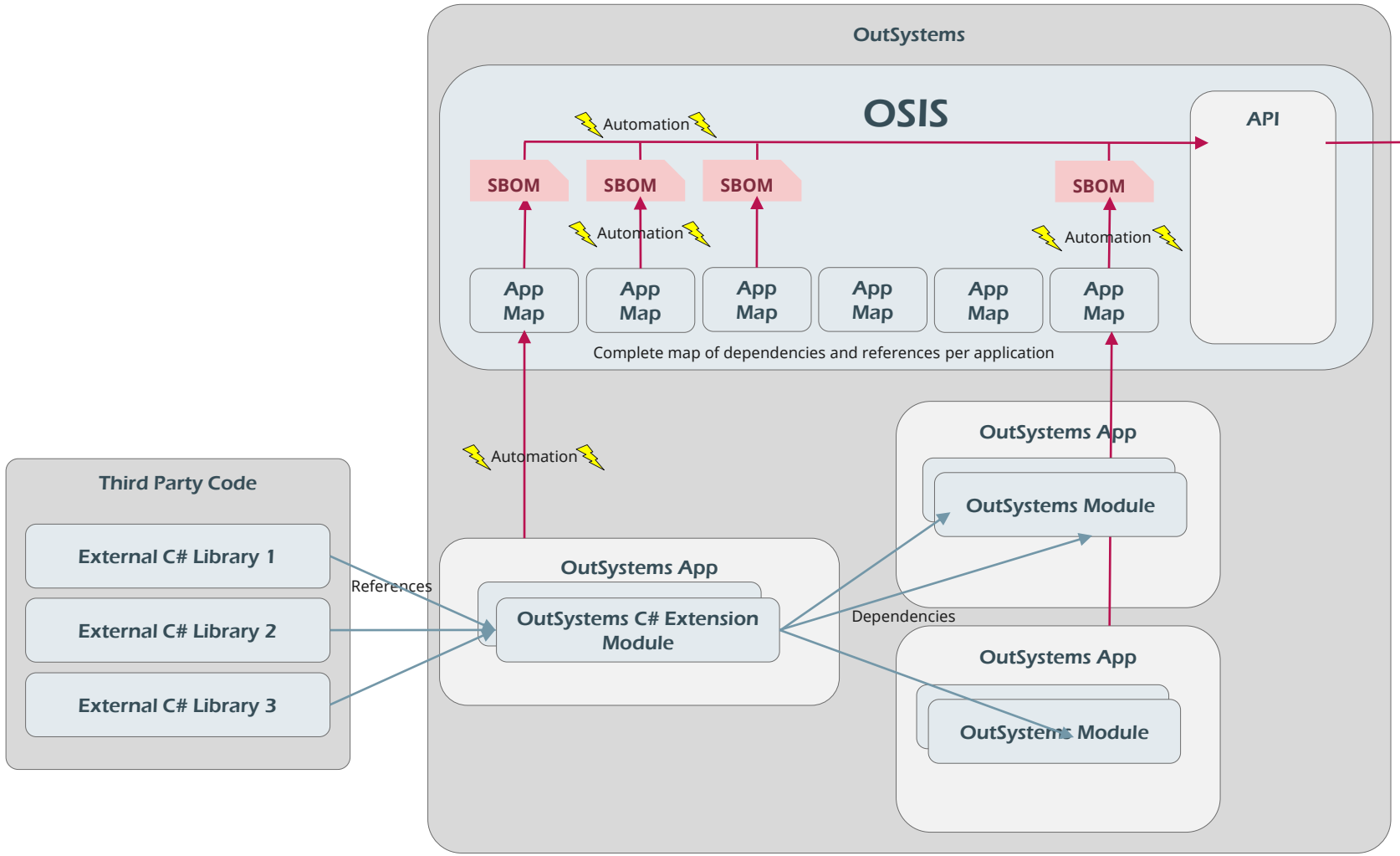


Automated generation of SBOM on application and module level

agentbase ag

OutSystems/ Partner Silver

High-Level Overview OSIS



CI / CD Pipeline Integration
Dependency Tracking Tools
License Management Tools
Vulnerability Monitoring Tools

Automated up-to-date Monitoring
of productive applications

Integration
into staging processes for pre-prod vulnerability checks

Ongoing DEV quality checks
during development for early identification of licensing or vulnerability issues

Compliance
by documentation of full software supply-chains (as demanded in NIS2 and others)

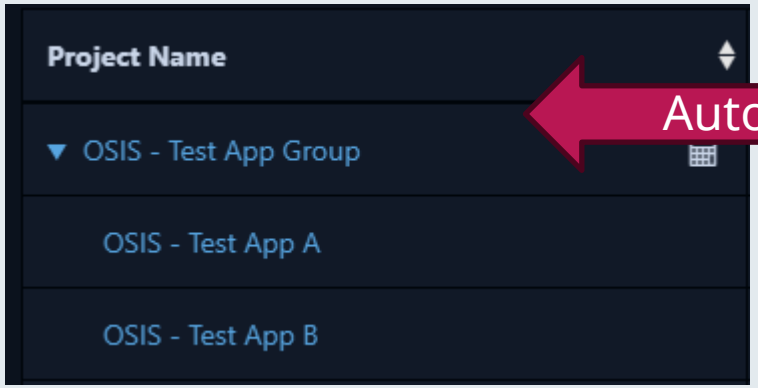
Wide integration possibilities by using industry standard CycloneDX SBOM file format for interchange.

agentbase ag

OutSystems/ Partner Silver

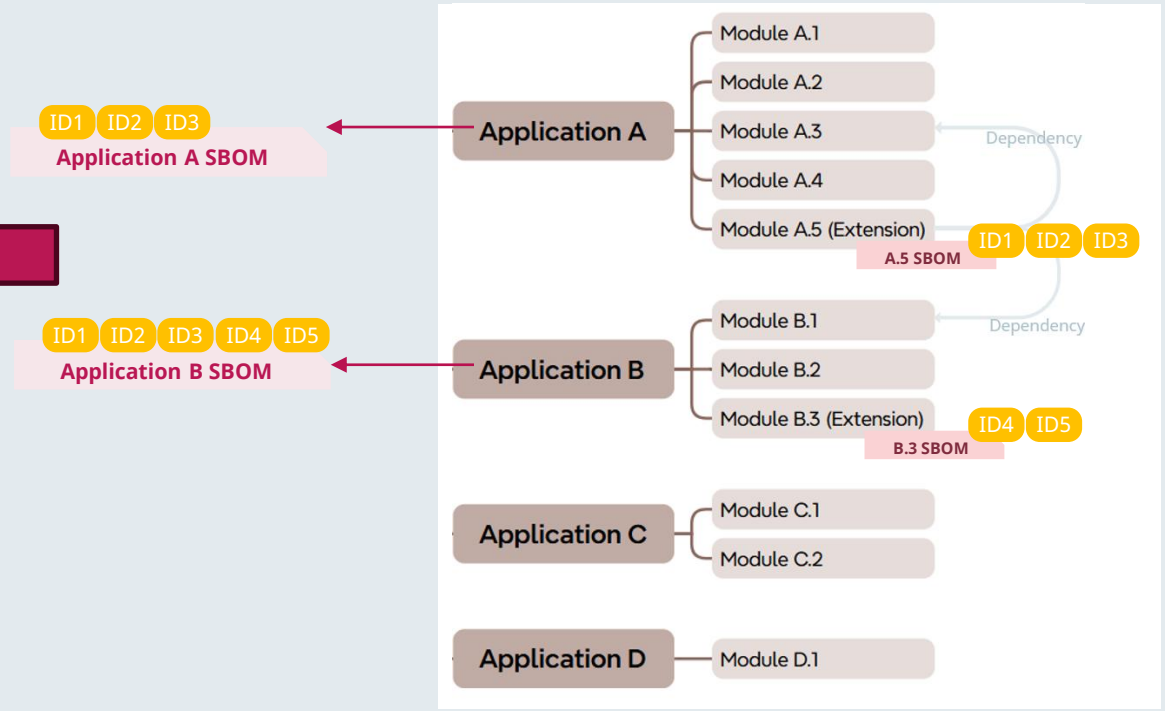
Creation of OS App SBOMs and automated Propagation

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



Automation

OSIS



Visibility of incoming vulnerabilities

Before adding libraries with affected packages

After adding libraries with affected packages

agentbase ag

OutSystems/ Partner Silver

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

agentbase ag

OutSystems/ Partner Silver

Vielen Dank
für Ihre Aufmerksamkeit

agentbase AG
Eggertstraße 7
33100 Paderborn

+49 5251 547 2600

www.agentbase.de

info@agentbase.de

agentbase ag

FRANZISKA SURMUND
Business Development

+49 5251 547 2614

Franziska.Surmund@agentbase.de

www.agentbase.de

Eggertstraße 7
33100 Paderborn

Erstgespräch buchen

agentbase ag

OutSystems/ Partner Silver