SBOM – Technischer Deep Dive

Wie Software-Stücklisten wirklich in Entwicklung und Betrieb ankommen

Dr. Yvette Teiken & Ruben Brick · 06.10.2026



STELLEN SIE SICH VOR …

Sie arbeiten ab heute bei Brenner Gate Technology



Familienunternehmen seit 1958 · heute in 3. Generation

650+
Mitarbeitende

65+
Länder im Einsatz

500.000+
installierte Systeme

Ihr Produkt: der smarte Torantrieb



Antrieb & Steuerung
eigene Firmware

Funkmodul
Zulieferer A

App
Partner B

Cloud-Dienst
Dienstleister C

Open Source
Bibliotheken überall

IHRE ROLLE

Sie sind Hersteller im Sinne des CRA – verantwortlich für das ganze Produkt, auch für alles Zugekaufte.

Ihr Antrieb steckt in Logistikzentren, Flughäfen, Kühlhäusern und Häfen – oft unter fremder Marke.

DER ERNSTFALL

Eine Schlagzeile – und plötzlich ist alles dringend

24 h

Seit 11.09.2026 gilt die CRA-Meldepflicht

Aktiv ausgenutzte Schwachstellen müssen Hersteller innerhalb von 24 Stunden frühwarnend melden.

Sind wir betroffen? Die Fragenkette:

01 Welche Bibliothek nutzen wir – und wo?

02 In welcher Version?

03 Bei welchem Kunden läuft das?

04 Ist der Fix schon drin?

05 Wurde er schon ausgeliefert?

WAS DIE SBOM LEISTET

Von „alle Kunden“ zu „diese fünf Installationen“

Ohne SBOM

Alle Produkte und alle Kunden sind potenziell betroffen. Suchen, fragen, raten.

Mit SBOM

Pro Release dokumentiert: welche Bibliothek, welche Version, in welchem Produkt.

Ergebnis

Eine konkrete Liste betroffener Kundeninstallationen. Fokus statt Hektik.

Wie man da hinkommt – und wo es in der Praxis hakt, zeigt Ruben.

OIXIO

Advisory | IT | Digital | Cyber

Software Bill of Materials

Ruben Brick

6. Oktober 2026

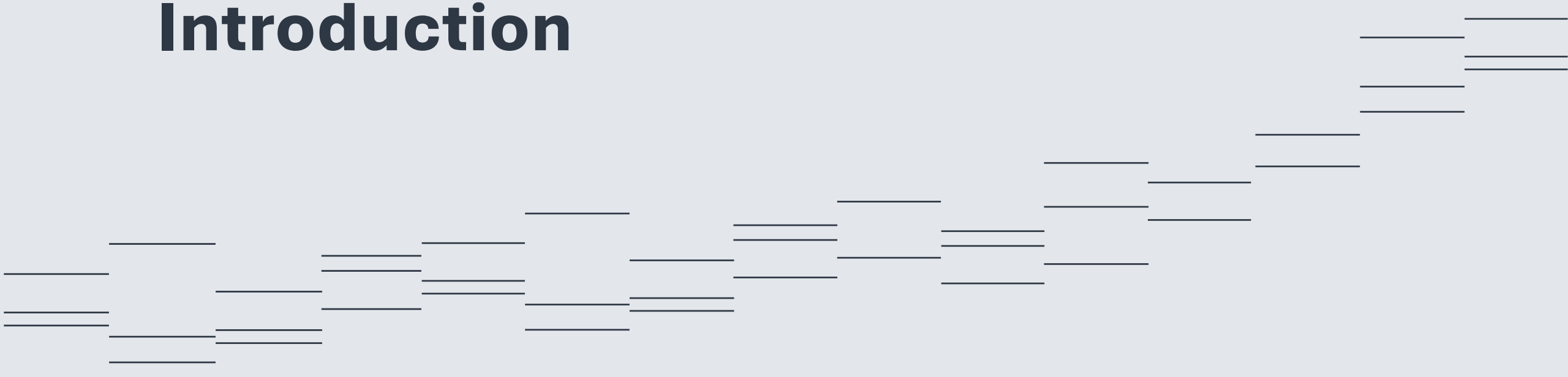


Agenda

OIXIO

- Introduction
- Software Supply Chain
- Beispiel: Log4J
- Software Bill of Materials
- Standards
- Schwachstellen Management
- Demo
- Key Takeaways

Introduction



Cyber Resilience Act

Legale Anforderung

Eine maschinenlesbare SBOM, die mindestens die Top-level Dependencies abdeckt

Technische Dokumentation

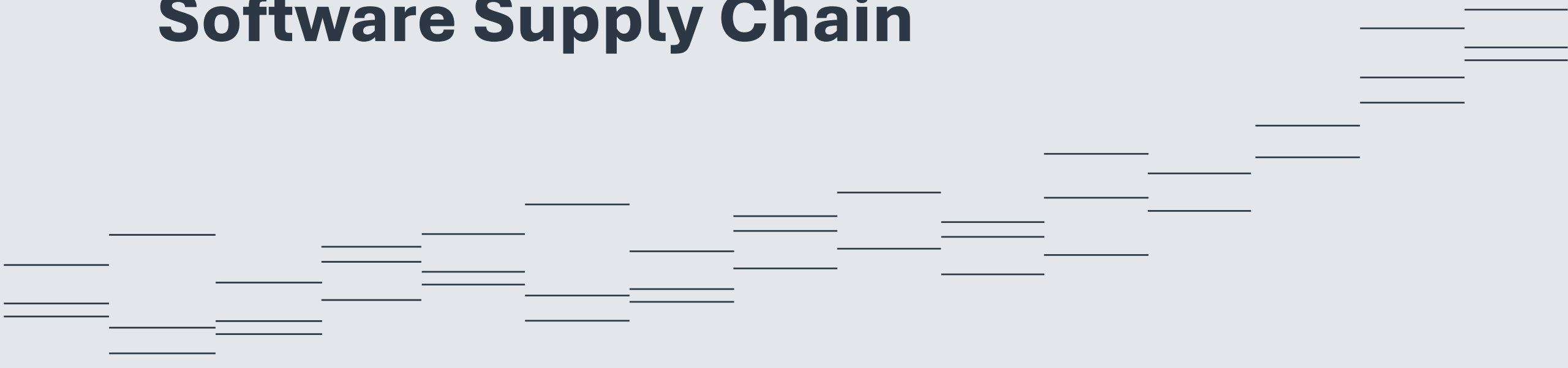
Die SBOM ist Bestandteil der technischen Dokumentation und muss den MSA auf nachfrage zur verfügung gestellt werden

Verpflichtend ab

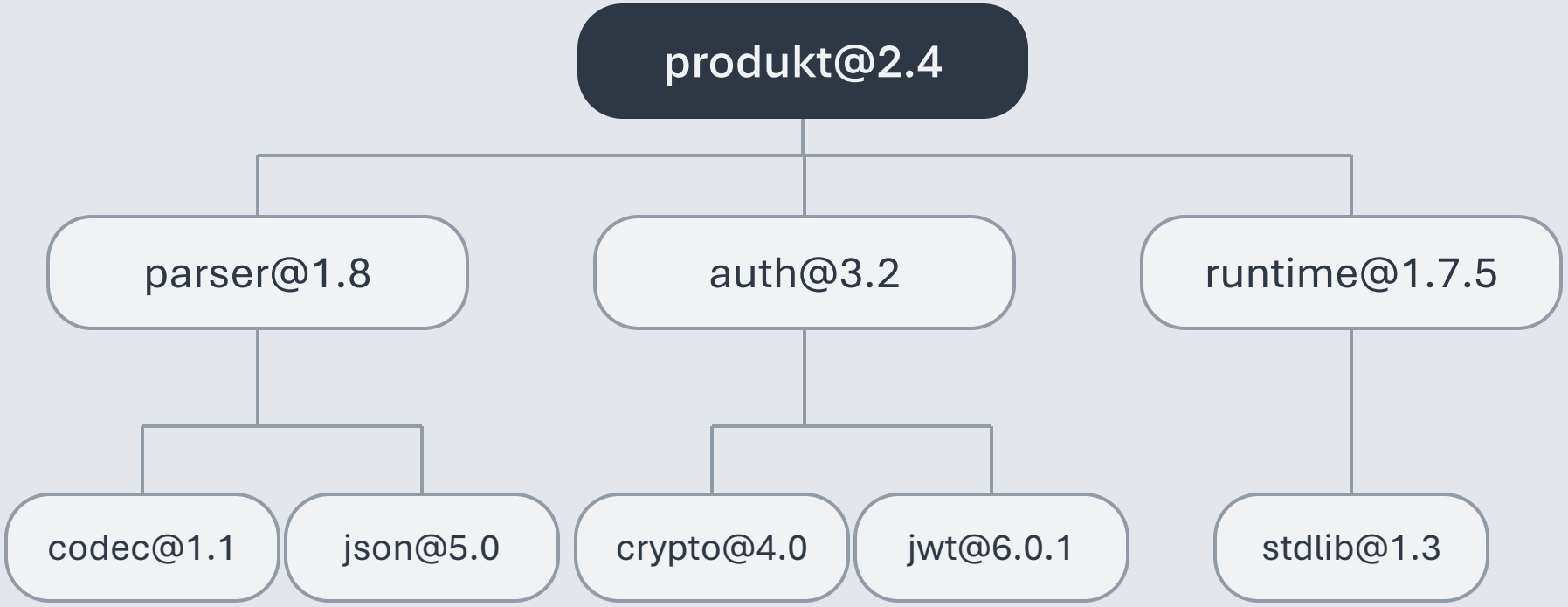
11. Dezember 2027

OIXIO

Software Supply Chain



Software Supply Chain



EBENEN

0 Release Komponente

1 Direkte Abhängigkeiten

2 Transitive Abhängigkeiten

Software Supply Chain

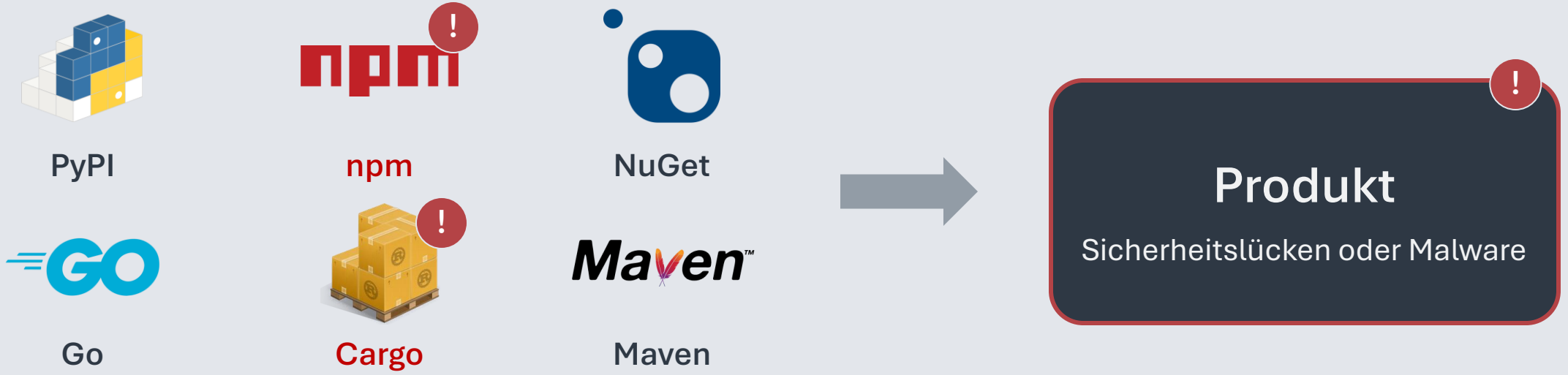
Viele Pakete aus gängigen Ecosystems sind Bestandteil nahezu aller Softwareprodukte.



Open-Source- und kommerzielle Komponenten

Software Supply Chain

Viele Pakete aus gängigen Ecosystems sind Bestandteil nahezu aller Softwareprodukte.



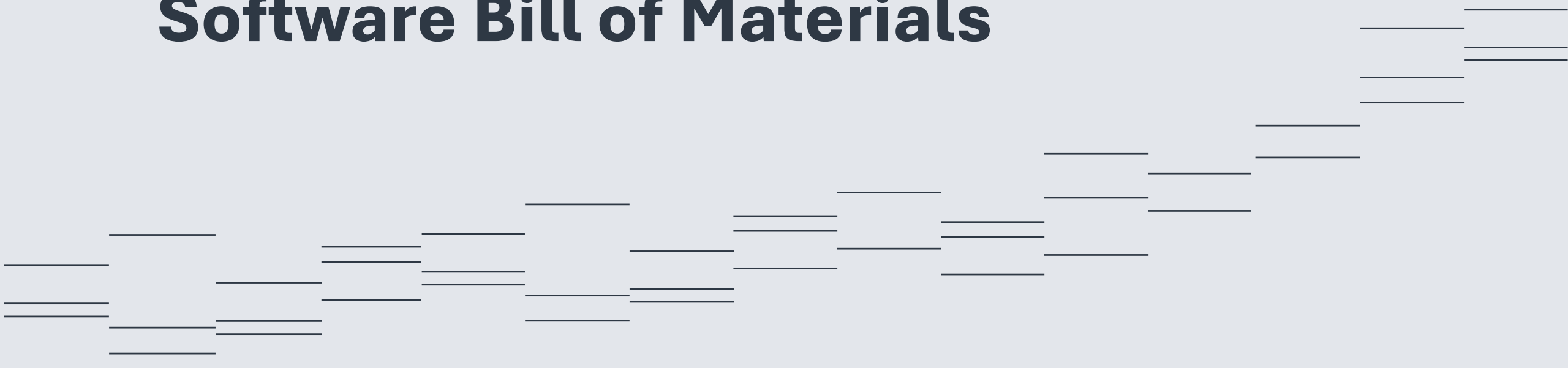
Open-Source- und kommerzielle Komponenten

Beispiel: Log4J

- „Log4Shell“ (CVE-2021-44228)
- **~40** Millionen Downloads der betroffenen Version in **2025**
- Meistens als Transitive abhängigkeit

OIXIO

Software Bill of Materials



Inhalt einer SBOM

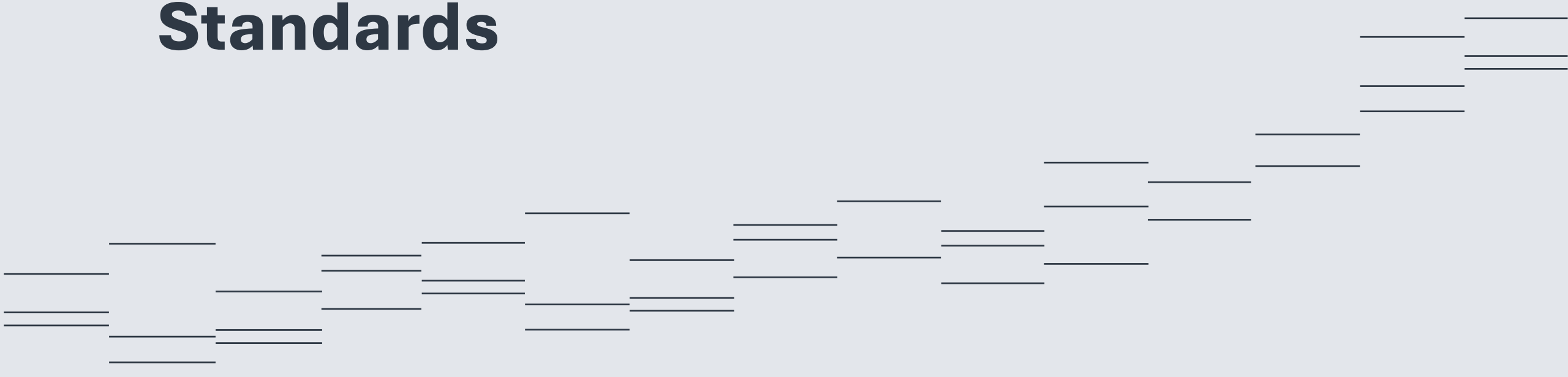
Speichert für jede Komponente mindestens:

- Autor
- Name
- Version
- Lizenzinformationen
- Package Identifier
- Hash
- Beziehungen

Was bringt eine SBOM?

- Supply Chain Transparenz
- Schwachstellen Management
- Incident Response
- Lizenz Compliance

Standards



Standards





SBOM Tools

Generierung



cdxgen
Open Source



Trivy
Open Source



Syft
Open Source



Snyk CLI SBOM
Kommerziell

Qualitätsbewertung



sbomqs
Open Source

Ingestion & Analyse



Dependency-Track
Open Source



FOSSA
Kommerziell, Free-Tier



Sonatype SBOM Manager
Kommerziell

Weitere Tools unter: https://cyclonedx.org/tool-center/

SBOM generieren

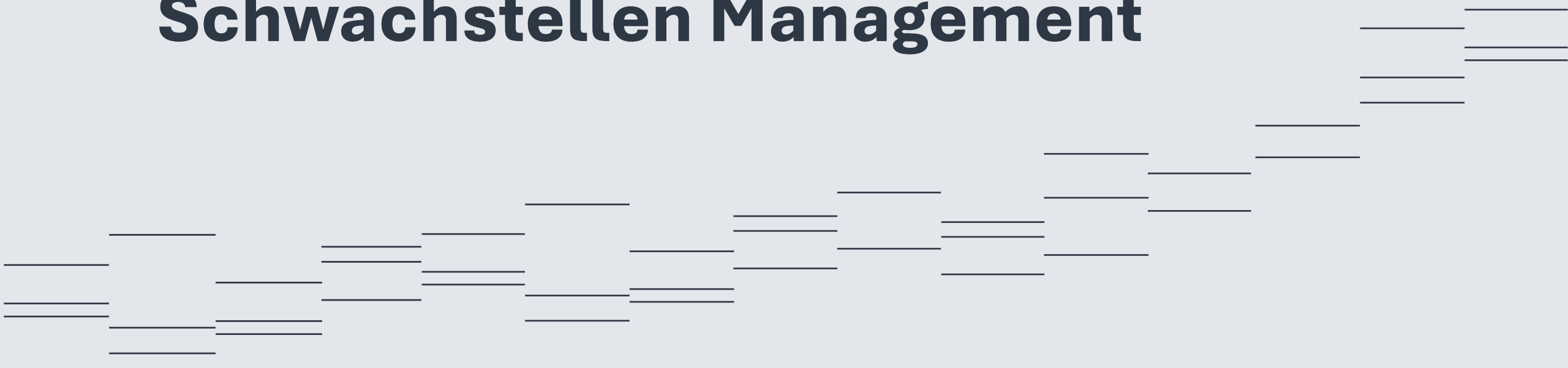
Beispiel für ein .NET-Projekt mit cdxgen




```
cdxgen -t dotnet --spec-version 1.6 -o sbom.cdx.json .
```

MyApp.csproj	Deklarierte direkte NuGet-Packages
obj/project.assets.json	Aufgelöste Versionen und transitive Dependencies
packages.lock.json	Optionales Lockfile mit aufgelösten Packages

Schwachstellen Management



Schwachstellen Management

Wie?

Komponenten mit Datenbanken abgleichen mithilfe von:

- Name & Version
- CPE oder PURL

Datenbanken

- NIST NVD
- ENISA EUVD
- Google OSV

Was sind CPEs und PURLs?

- Standardisierte Namensschemata für Software und Hardware

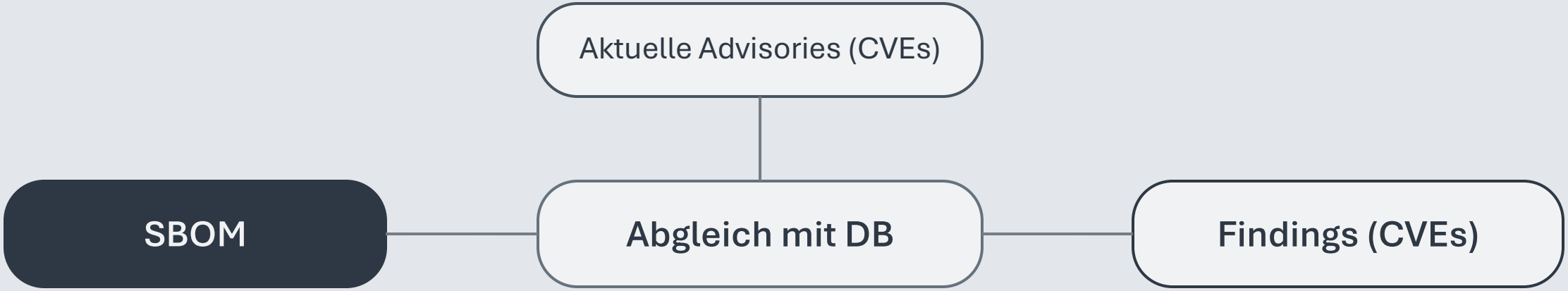
Package URL (PURL)

pkg:type/namespace/name@version?qualifiers#subpath

Common Platform Enumeration (CPE)

cpe:2.3:part:vendor:product:version:update:edition:language:sw_edition:target_sw:target_hw:other

SBOM Ingestion



PURL, CPE, Name, Version

Vulnerability Triage



Prüfen

Komponente und betroffene Version bestätigen

Bewerten

Betroffenheit überprüfen, False-positives aussortieren

Beheben

Updaten, mitigieren und ein Security Advisory veröffentlichen

Workflow mit CI/CD











Anwendung

Nuget Pakete

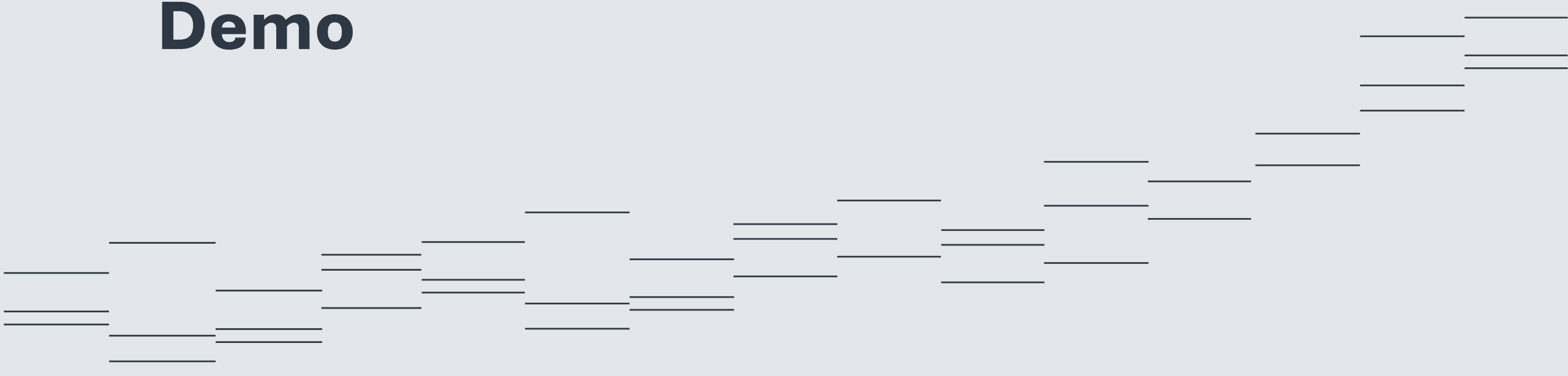
Azure DevOps

SBOM generieren

Dependency-Track

SBOM ingestieren
und mit DB abgleichen

Demo



UND WENN ES ERNST WIRD?

Die SBOM ist der Anfang – nicht schon die Antwort

01

Betroffen?

Die SBOM zeigt Produkt, Version und Kundeninstallation.

02

Patchstatus

Fix integriert? Teil eines Releases? Beim Kunden ausgeliefert?

03

Threat Model

Wird die Funktion genutzt? Ist das System exponiert? Praktisch angreifbar?

04

Kommunikation

Kunden klar, ehrlich und aktiv informieren – bevor sie fragen.

WAS WIR KUNDEN SAGEN KÖNNEN

Klare Antworten statt Erklärungsnot

Kein Handlungsbedarf

„Ihr System nutzt die Bibliothek, aber nicht die betroffene Version."

Betroffen – Fix kommt

„Wir haben die gepatchte Version getestet. Die Auslieferung erfolgt morgen."

Noch kein Fix

„Ihr Nutzungsszenario ist nicht angreifbar. Wir beobachten eng und informieren Sie aktiv."

Statt Unsicherheit zeigen wir Übersicht – das stärkt Vertrauen, gerade im kritischen Moment.

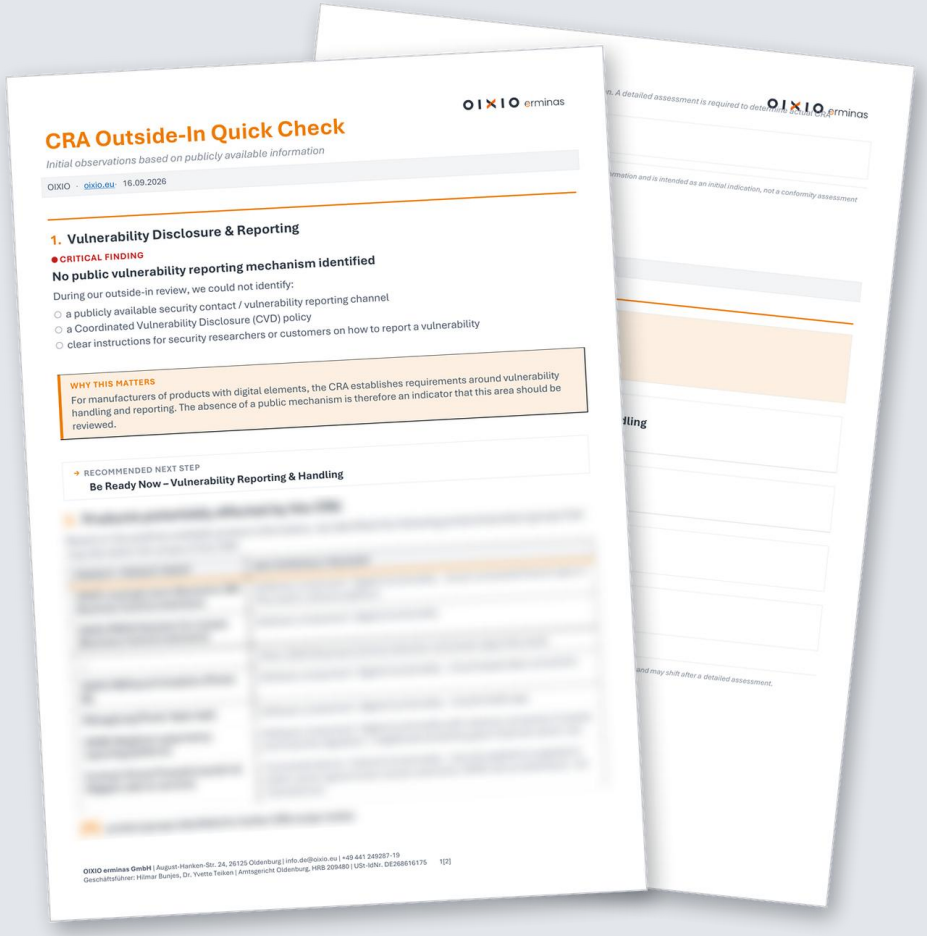
Key Takeaways

- Supply Chain Transparenz und Sicherheit
- Lizenz Compliance
- Viele verschiedene Tools

- EUVD unterstützt noch keine PURLs/CPEs
- Kein einheitlicher Package Identifier

KOSTENFREIER CRA QUICK CHECK

Wo steht Ihr Unternehmen beim CRA?



Beispiel: Outside-In Quick Check (2 Seiten)

- Gibt es einen öffentlichen Meldeweg für Schwachstellen?
- Welche Ihrer Produkte fallen voraussichtlich unter den CRA?
- Was sind Ihre nächsten Schritte?

Auf Basis öffentlich verfügbarer Informationen – ohne Aufwand für Sie. Den Report erstelle ich individuell und schicke ihn Ihnen persönlich.

Scannen & anfragen

Lieber direkt sprechen? Dr. Yvette Teiken · +49 441 249287-19 · yvette.teiken@oixio.eu oder Ruben Brick ruben.brick@oixio.eu

OIXIO erminas · Individuelle Softwareentwicklung

Wenn Standardsoftware nicht reicht, entwickeln wir Ihre Lösung

Seit über 19 Jahren bauen wir in Oldenburg Software, die genau zu Ihren Prozessen passt – von der Maschine über die App bis zum fertigen Produkt. Wir denken vom Business Case her, nicht von der Technologie.

Industrial IoT & Retrofit

Maschinendaten erfassen – auch bei geschlossenen Steuerungen. Mit unserer Plattform erPUB.

Referenz: CEWE · HCCR (HHLA)

Enterprise Apps

Web, Windows, iOS und Android. Papierlose Abläufe, angebunden an ERP und Logistik.

Referenz: Amagno · Chemie-Intralogistik

Produktentwicklung

Vom Prototyp zur Serie: Software und Cloud. Fertigungspartner finden und steuern wir.

Referenz: E+S (YOLii) · DÜPERTHAL connect

KI & Datenanalyse

Bildanalyse, Dokumenten-erkennung und vorausschauende Wartung.

Referenz: Projekte in Produktion und Logistik

So arbeiten wir

Vom Business Case her
Nutzen zuerst, Technologie danach

Ihr Team wird befähigt
Übergabe und Weiterentwicklung im Haus

Datenhoheit bei Ihnen
Ihre Daten, Ihre Systeme

Projekt anfragen
yvette.teiken@oixio.eu

OIXIO erminas · Seit 1. Juli 2026 Teil der OIXIO Group

Jetzt mit OIXIO: von der Maschine bis zum sicheren Betrieb aus einer Hand

Ab einer gewissen Projektgröße wird die Abstimmung zwischen mehreren Dienstleistern selbst zum Risiko. Gemeinsam mit der OIXIO Group übernehmen wir die Verantwortung für das Gesamtbild.

Das bleibt

Team, Geschäftsführung und Standort Oldenburg

Ihre Ansprechpartner, Verträge und Konditionen

erminas wird Kompetenzzentrum der Gruppe für Industrial IoT und Business Applications

Das kommt dazu

Cyber Security

Vom Audit bis zum 24/7-SOC, inkl. NIS2 und CRA

Managed IT Services

Betrieb der Infrastruktur aus derselben Hand

Microsoft in voller Breite

Azure, Dynamics 365, Power Platform und Copilot

BI & KI

Reporting und KI, die im Alltag genutzt werden

Advisory

Prozessberatung vor dem Projekt

Internationale Roll-outs

Teams in mehreren Ländern, auch über mehrere Werke

300 Mitarbeitende (rund)

7 Standorte in Estland, Litauen, Deutschland

1.000+ aktive Kunden

EU Recht und Datenhaltung

Wer heute Strukturen schafft, reduziert den Stress von morgen.

Der CRA fordert Nachvollziehbarkeit – keine Perfektion.

Pragmatische Ansätze für KMU: EU-Projekt CRACoWi.

Fragen & Austausch: Dr. Yvette Teiken · Ruben Brick

