Automatisierung regulatorischer Anforderungen des Cyber Resilience Acts

#bfoss24 Workshop

12.09.2024

bitkom

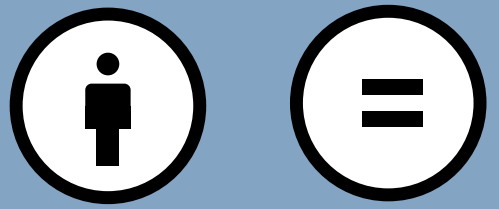
#bfoss24

{metæffekt}

Karsten Klein – CEO {metæffekt} GmbH
https://metaeffekt.com

Hinweise

- Der Inhalt dieser Präsentation ist keine Rechtsberatung. Es dient der allgemeinen Information.
- Diese Präsentation ersetzt keine von zugelassenen Rechtsberatern durchgeführte Rechtsberatung.
- Die in dieser Präsentation einschließlich ihrer Anlagen dargestellten Informationen sind urheberrechtlich geschützt.
- Jede Form der Abwandlung oder Vervielfältigung ist ohne explizite Erlaubnis des Urhebers nicht gestattet.
- Materialien von Dritten sind entsprechend der genutzten Lizenz gekennzeichnet



Referent

Dipl. Inf. Karsten Klein ist seit 24 Jahren in der Software-entwicklung und seit 21 Jahren als Software Architekt tätig.

Bevor er im Juli 2016 die {metæffekt} GmbH gründete, war er 4 Jahre CTO der InterComponentWare AG in Walldorf.

Neben Lizenz-Compliance Themen beschäftigte sich Karsten in den vergangenen 4 Jahren mit Informations- und Cyber-Sicherheit und entsprechenden Regularien.

Als Geschäftsführer und technische Leitung bei der {metæffekt} berät er mit seinem Team Kunden in verschiedenen Industrien.

Karsten ist in nationalen und internationalen Arbeitskreisen aktiv und unterstützt die Anwendung und Entwicklung von Standards.

Unternehmen

{metæffekt}

Die {metæffekt} GmbH hat sich zum Ziel gesetzt Open Source im Unternehmen effizient nutzbar zu machen und erforderliche Abläufe weitestgehend zu automatisieren. Dazu entwickelt sie Prozessabläufe, Richtlinien, Werkzeuge und Datenbanken.

https://metaeffekt.com/

https://github.com/org-metaeffekt

Aktuelle Referenzen / Beiträge / Projekte

Bitkom

- AK Open Source
- Publikationen/Open-Source-Software-Rechtliche-Grundlagen-und-Handlungshinweise
- Publikationen/Open-Source-Leitfaden-Praxisempfehlungen-fuer-Open-Source-Software

SPDX

- https://github.com/spdx/license-list-XML

OSBA

- WG-Continuous License Compliance
- CRA Task Force – Anforderungsanalyse EU Cyber Resilience Act
- BSI TR-03183-2 – Austausch zum Thema SBOM mit dem BSI

{metæffekt} Online Ressourcen / Tools

- https://metaeffekt.com/security/cvss/calculator/
- https://github.com/org-metaeffekt/metaeffekt-universe

Agenda

Einleitung – Einordung Cyber Resilience Act

- Anwendbare Praxis, Normen, Standards und Ableitungen
- Ziele der Automatisierung

Teil 1 – Qualifizierte SBOM

- Ansatz, Inhalte, Anwendungsfälle, Ziele
- Rahmenbedingungen

Teil 2 – Schwachstellen Management

- Identifikation, Kontextualisierung, Bewertung und Reporting
- Prozesse, Richtlinien und Rahmenbedingungen

Teil 3 – Lizenz Compliance

- Erhebung, Bewertung, Reporting
- Prozesse und Richtlinien und Rahmenbedingungen

Q & A

Bitkom OSM#23

{metæffekt}

Experten-Statement: Einordnung des EU Cyber Resilience Act zum OSM#23

Bezug

Mit dem *Cyber Resilience Act* (CRA) [1] strebt die EU die Harmonisierung der Sicherheitsanforderungen von Produkten mit digitalen Elementen im Binnenmarkt an. Der CRA beabsichtigt das Maß an Cybersicherheit dieser Produkte zu erhöhen und Schwachstellen entgegenzutreten.
Der derzeitige Entwurf beinhaltet grundlegende und nachvollziehbare Forderungen zu folgenden Themen:

- Erstellung von *Software Bill of Materials* (SBOM)
- Evaluation und Verwaltung von Sicherheitsaspekten
- Konformitätsnachweise der Hersteller in der Lieferkette
- Verifikation und Validierung von SBOM-Inhalten

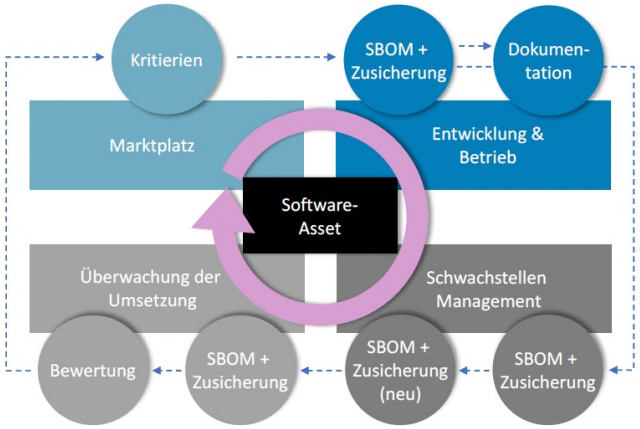
Open Source Software (OSS), sofern im kommerziellen Kontext genutzt, wird von der zukünftigen Verordnung eingeschlossen. Insofern finden sich zentrale Aspekte des CRA im Open Source Monitor der Bitkom (OSM#23) wieder.

Status Quo

Im CRA ausformulierte Maßnahmen und Anforderungen sind bereits heute Treiber für Industrie und Verwaltung. Dies wird an den Kennzahlen des OSM#23 deutlich. So erstellen 38,5 Prozent in der Verwaltung und 31,7 Prozent der befragten Unternehmen eine SBOM. Bei der Verwendung von OSS prüfen 64,3 Prozent in der Verwaltung und 72,8 Prozent in der Industrie die eingesetzten Komponenten auf ihre Sicherheit. Allerdings erfolgt bei nur 13,7 Prozent in der Industrie und 23,5 Prozent in der Verwaltung die Prüfung automatisiert in festgelegten Zeitabständen.

Ableitung aus dem CRA

Nachfolgend wird der Blick auf das Software-Asset als Bestandteil eines Produkts mit digitalen Elementen und die vier Regulierungsbereiche des CRA gerichtet:



Software-Asset Lebenszyklus

Für ein Software-Asset leiten sich aus dem Markt und dem CRA diverse Kriterien ab, die in Entwicklung und Betrieb zu berücksichtigen sind. Zur Erfassung eines Software-Assets wird eine SBOM verlangt, um individuelle Eigenschaften der detaillierten Bestandteile zuzusichern. Die SBOM wird zur Erzeugung von Dokumentation und zum Management von Schwachstellen herangezogen. Der CRA stellt konkrete Anforderungen an die Regelmäßigkeit von Analyse und Kommunikation der Schwachstellen an die Empfänger des Software-Assets. Die SBOM mit ihren Zusicherungen wird zur Bewertung und Überwachung der Kriterien genutzt.

Open Source in Industrie und Verwaltung

OSS ist zentraler Baustein der modernen Softwareentwicklung und bietet ein kollaboratives Ökosystem. Im OSM#23 wird deutlich, welche Aspekte von OSS für Industrie und Verwaltung eine besondere Rolle spielen. Um OSS in diesem Umfeld voranzutreiben, ist es erforderlich die Verbindlichkeit in Gestaltung und Nutzung zu gewährleisten sowie das Maß an Sicherheit zu erhöhen.
Der CRA kann genügen, die Akteure im Ökosystem auf ein neues Niveau an Sicherheit und Professionalität zu heben. Allerdings erfordert dies eine Mitwirkung aller beteiligten Freiwilligen und Unternehmen.

Fazit

Aus dem OSM#23 lässt sich die Hypothese ableiten, dass die Verwaltung zumindest formal besser aufgestellt ist als die Industrie. Um der Forderung des CRA nach einer unverzüglichen Reaktion auf Schwachstellen nachzukommen, reicht der aktuelle Automatisierungsgrad beider Sektoren jedoch noch nicht aus. Die Qualität der zugrundeliegenden SBOMs steht dabei zunächst noch außer Frage.

Die {metæffekt} GmbH [2] bietet Konzepte, Werkzeuge und Dienstleistungen zur Umsetzung von automatisierten Prozessen im Lebenszyklus von Software-Assets. Sie ist verbindlicher Partner einer maßgeschneiderten Umsetzung.

1 https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
2 https://metaeffekt.com

EU Cyber Resilience Act

- Statistik Zielsetzung/Hintergrund:
  - 48 Seiten
  - 154 Überschriften / Paragrafen / Aufzählungen
  - ~21.000 Wörter
  - Reine Lesedauer: >2h

- Statistik Hauptteil:
  - 83 Seiten
  - 905 Überschriften / Paragrafen / Aufzählungen
  - ~31.000 Wörter
  - Lesedauer: >3h
  - 47 Fußnoten / Links
  - ~30 Adressaten / Rollen

Analyse des Cyber Resilience Acts

	A	B	C	D	E	F
1	Order	Section	CRA Paragraph (EN)	Link	CRA Paragraph (DE)	Primary Target Group
2	155	I General Provisions	CHAPTER I		KAPITEL I	all
3	156	I General Provisions	GENERAL PROVISIONS		ALLGEMEINE BESTIMMUNGEN	all
4	157	I-1 Subject Matter	Article 1		Artikel 1	all
5	158	I-1 Subject Matter	Subject matter		Gegenstand	all
6	159	I-1 Subject Matter	This Regulation lays down:		Mit dieser Verordnung wird Folgendes festgelegt:	all
7	160	I-1 Subject Matter	(a) rules for the ***making available*** on the market of products with digital elements to ensure the cybersecurity of such products;		a) Vorschriften für ***die Bereitstellung auf dem Markt*** von Produkten mit digitalen Elementen, um die Cybersicherheit solcher Produkte zu gewährleisten;	all
8	161	I-1 Subject Matter	(b) essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to those products with respect to cybersecurity;		b) grundlegende Anforderungen an die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Produkte hinsichtlich der Cybersicherheit;	all
9	162	I-1 Subject Matter	(c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the ***time the product is expected to be in use***, and obligations for economic operators in relation to those processes;		c) grundlegende Anforderungen an die von den Herstellern festgelegten Verfahren zur Behandlung von Schwachstellen, um die Cybersicherheit von Produkten mit digitalen Elementen während ***der erwarteten Nutzungsdauer der Produkte*** zu gewährleisten, sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Verfahren;	all
10	163	I-1 Subject Matter	(d) rules on market surveillance***, including monitoring,*** and enforcement of the rules and requirements ***referred to in this Article.***		d) Vorschriften für die Marktüberwachung***, einschließlich Überwachung,*** und die Durchsetzung der ***in diesem Artikel*** genannten Vorschriften und Anforderungen.	all
11	164	I-2 Scope	Article 2		Artikel 2	all
12	165	I-2 Scope	Scope		Anwendungsbereich	all
13	166	I-2 Scope	1. This Regulation applies to products with digital elements ***made available on the market, the*** intended ***purpose*** or reasonably foreseeable use ***of which*** includes a direct or indirect logical or physical data connection to a device or network.		(1) Diese Verordnung gilt für ***auf dem Markt bereitgestellte*** Produkte mit digitalen Elementen, deren ***bestimmungsgemäßer Zweck*** oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt.	all
14	167	I-2 Scope	2. This Regulation does not apply to products with digital elements to which the following Union ***legal*** acts apply:		(2) Diese Verordnung gilt nicht für Produkte mit digitalen Elementen, auf die folgende Rechtsakte der Union Anwendung finden:	all
15	168	I-2 Scope	(a) Regulation (EU) 2017/745;		a) Verordnung (EU) 2017/745,	all
16	169	I-2 Scope	(b) Regulation (EU) 2017/746;		b) Verordnung (EU) 2017/746,	all
17	170	I-2 Scope	(c) Regulation (EU) 2019/2144.		c) Verordnung (EU) 2019/2144.	all
18	171	I-2 Scope	3. This Regulation does not apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139.		(3) Diese Verordnung gilt nicht für Produkte mit digitalen Elementen, die nach der Verordnung (EU) 2018/1139 zertifiziert worden sind.	all
19	172	I-2 Scope	4. This Regulation does not apply to equipment that falls within the scope of Directive 2014/90/EU of the European Parliament and of the Council(38).	https://v	(4) Diese Verordnung gilt nicht für Geräte, die in den Anwendungsbereich der Richtlinie 2014/90/EU des Europäischen Parlaments und des Rates(38) fallen.	all
20	173	I-2 Scope	5. The application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I may be limited or excluded where:		(5) Die Anwendung dieser Verordnung auf Produkte mit digitalen Elementen, die unter andere Rechtsvorschriften der Union mit Anforderungen für alle oder einige der von den grundlegenden Anforderungen in Anhang I abgedeckten Risiken fallen, kann eingeschränkt oder ausgeschlossen werden, wenn	all
21	174	I-2 Scope	(a) such limitation or exclusion is consistent with the overall regulatory framework ***that*** applies to those products; and		a) eine solche Einschränkung oder ein solcher Ausschluss mit dem für diese Produkte geltenden allgemeinen Rechtsrahmen vereinbar ist und	all

High-Level Ableitungen aus dem CRA

- Beschreibung Konzeption, Entwicklung und Herstellung des Produkts
- Beschreibung des Verfahrens zur
  - Behandlung von Schwachstellen
  - Erstellung der Software Bill of Materials (SBOM)
  - Offenlegung und Meldung von Schwachstellen
  - Sicherung der Prozesse
- Umsetzung der o.g. Prozesse inklusive Risiko-Behandlung
- Bewertung der Sicherheitsrisiken in der Herstellung und Handhabung
- Erstellung Software Bill of Materials (SBOM)
- Offenlegung von Schwachstellen
- Erstellung von Prüf- und Testberichten

Relevante Normen, Standards und Regulierung

- EU Cyber Resilience Act (CRA)
- Network and Information Security Directive (NIS2)
- BSI TR-03183-2 – Cyber Resilience Requirement / SBOM
  - ISO/IEC 5692:2021 – System Package Data Exchange (SPDX)
  - ECMA-424 – CycloneDX Bill of Materials (CycloneDX BOM)
  - (Common Security Advisory Framework (CSAF) inkl. VEX)
- ISO/IEC 27001:2022 – Information Security Management System (ISMS)
- ISA/IEC 62443 – Industrial Automation Control System (IACS)
- ISO/IEC 31000:2018 – Information Security Management System (ISMS)
- BSI IT-Grundschutz Kompendium
- ISO/IEC 5230:2020 – OpenChain; Standard für Open Source Compliance
- ISO/IEC 18974:2023 – OpenChain; Standard für Open Source Security
- Executive Order 14028 – Improving the Nation's Cybersecurity / NTIA The Minimum Elements For a SBOMs
- EVB-IT Basis- und Standardverträge
- Open CoDE SPDX Conformance

https://github.com/org-metaeffekt/metaeffekt-bom-essentials/blob/main/README.md#external-references

Photo by Chelsea Gates on Unsplash

Einordnung CRA

Verständnis, Fragen, Diskurs

Zusammenfassung

Teil 1

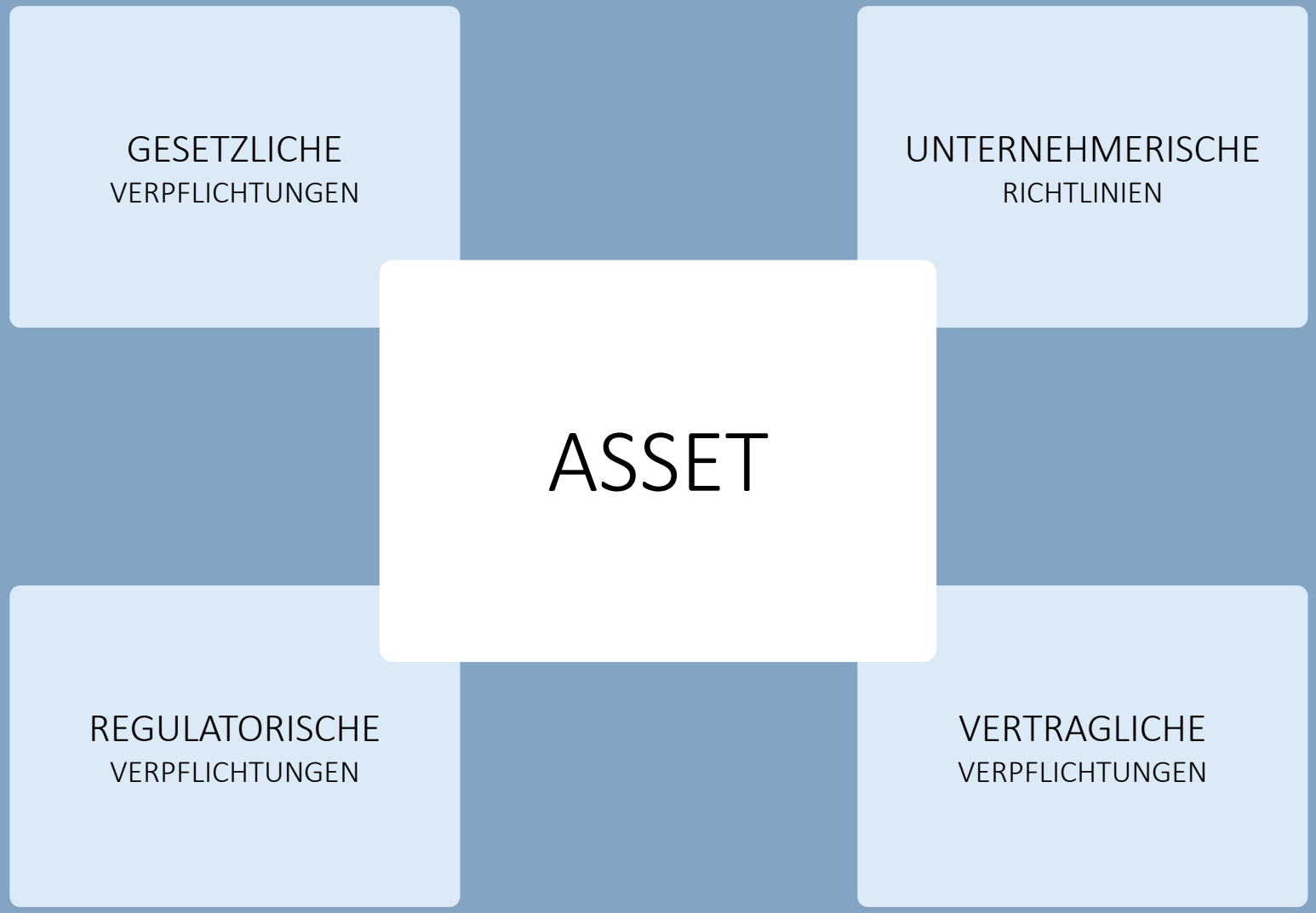
Qualifizierte SBOM

Ansatz, Inhalte, Anwendungsfälle, Ziele
Rahmenbedingungen

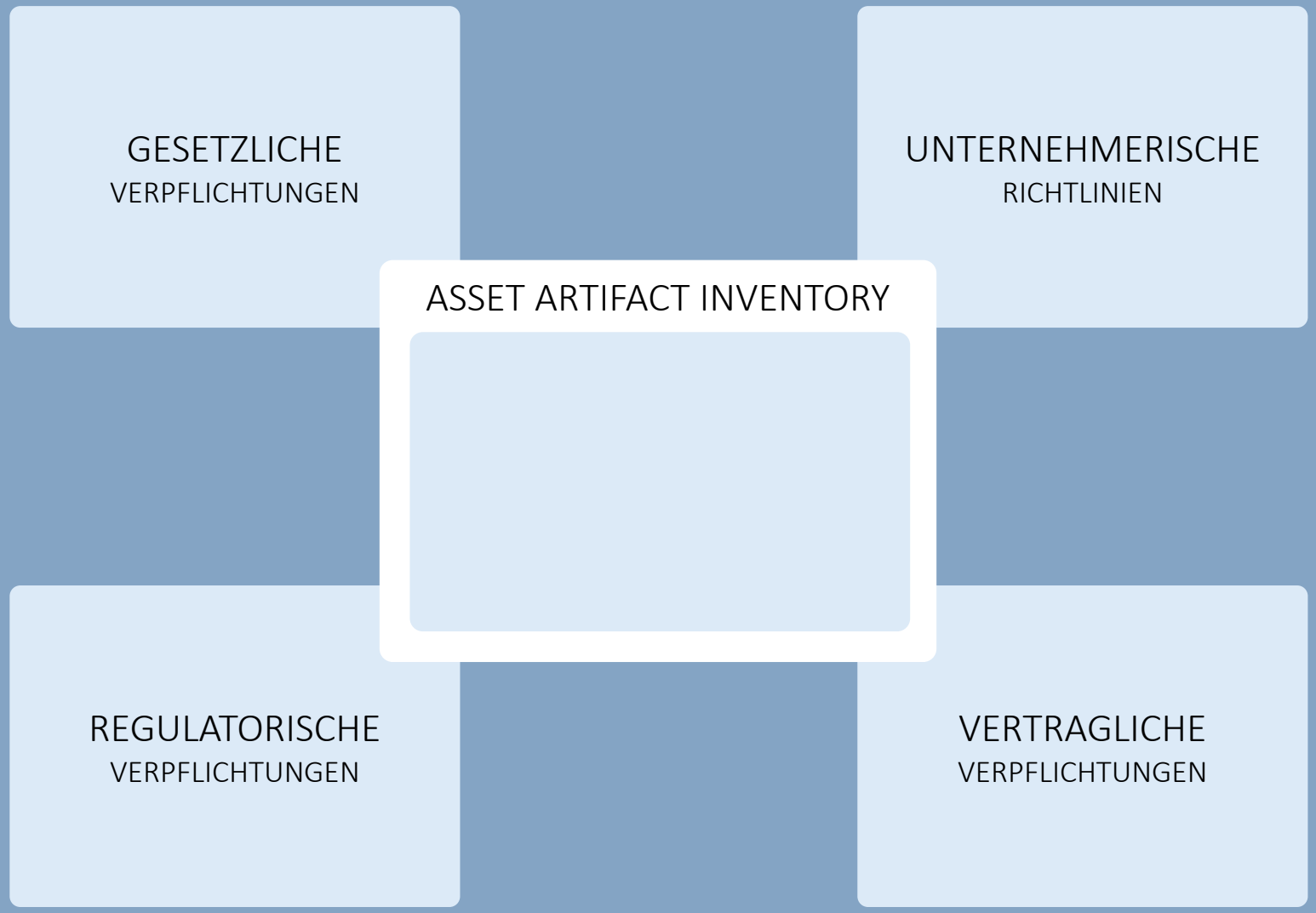
Exkurs – Asset

ASSET

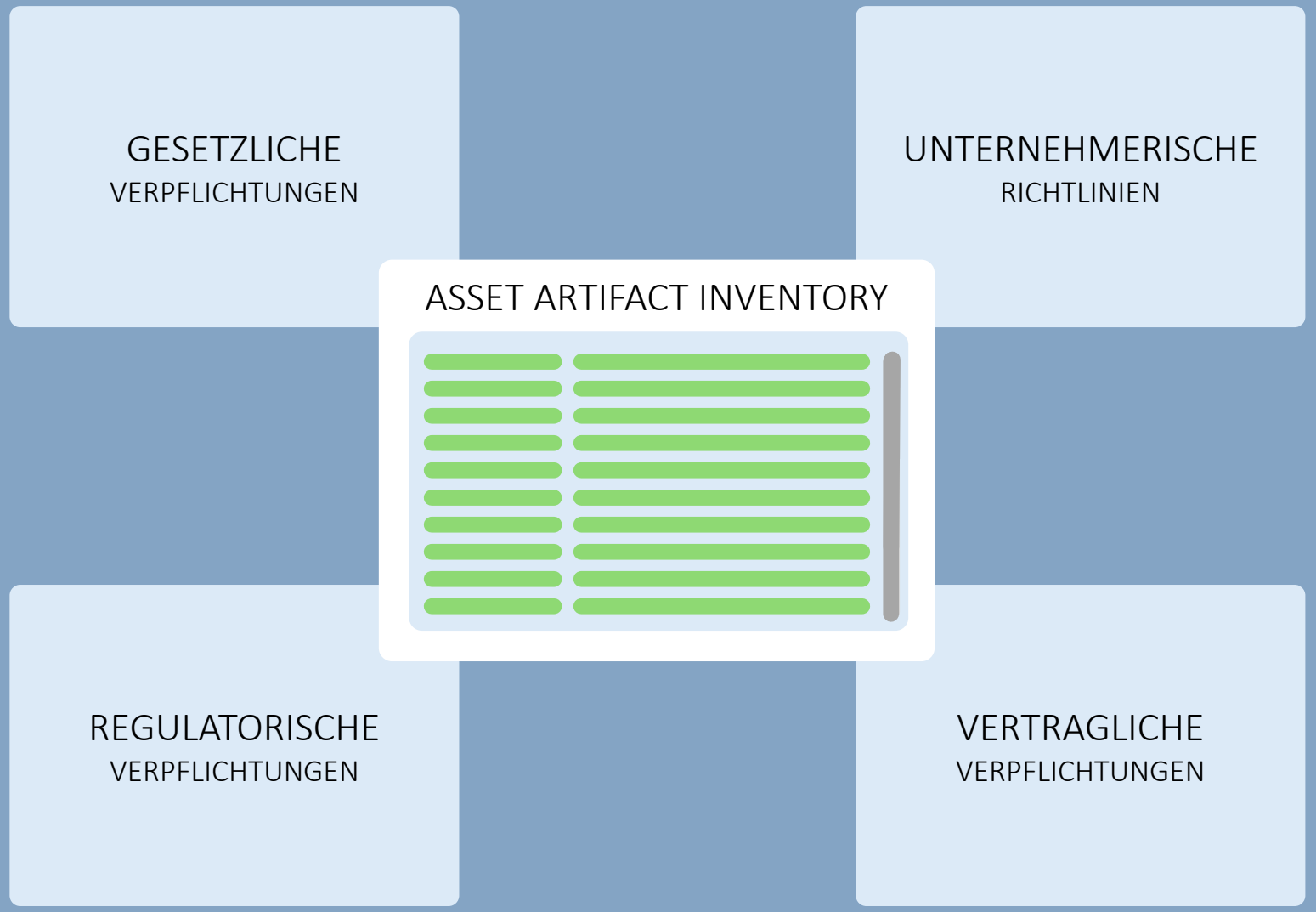
Exkurs – Asset



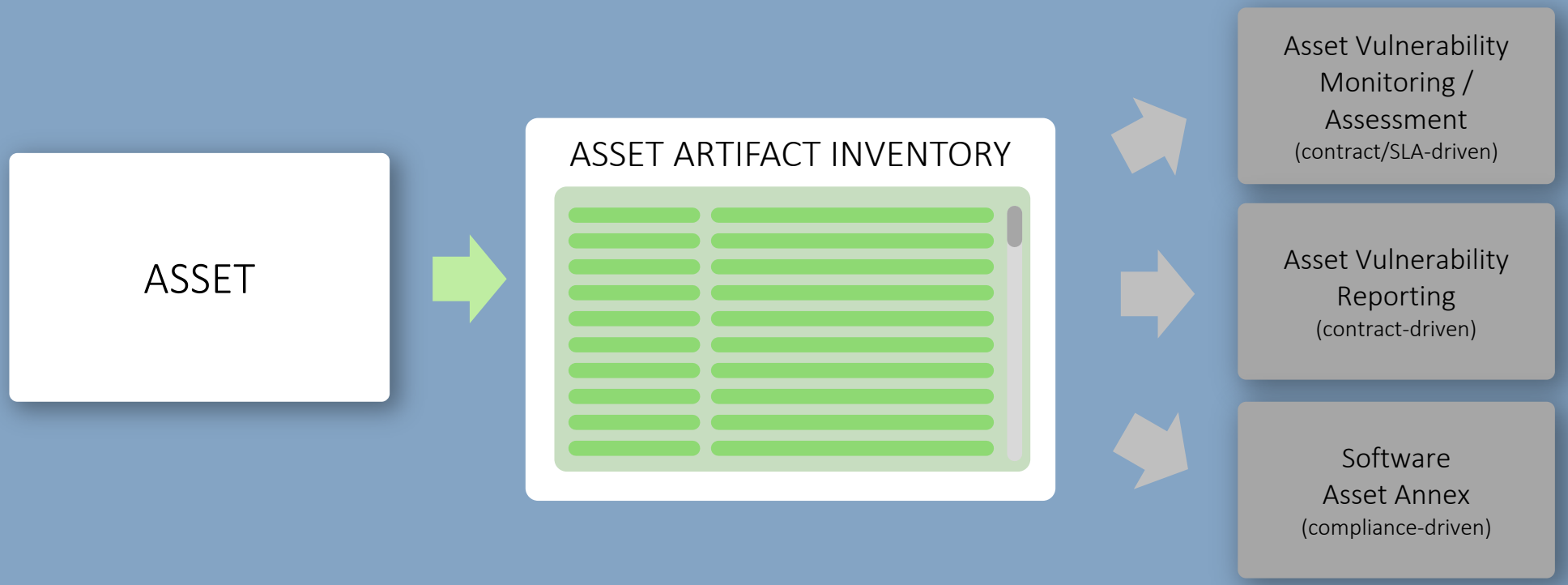
Asset – Analyse



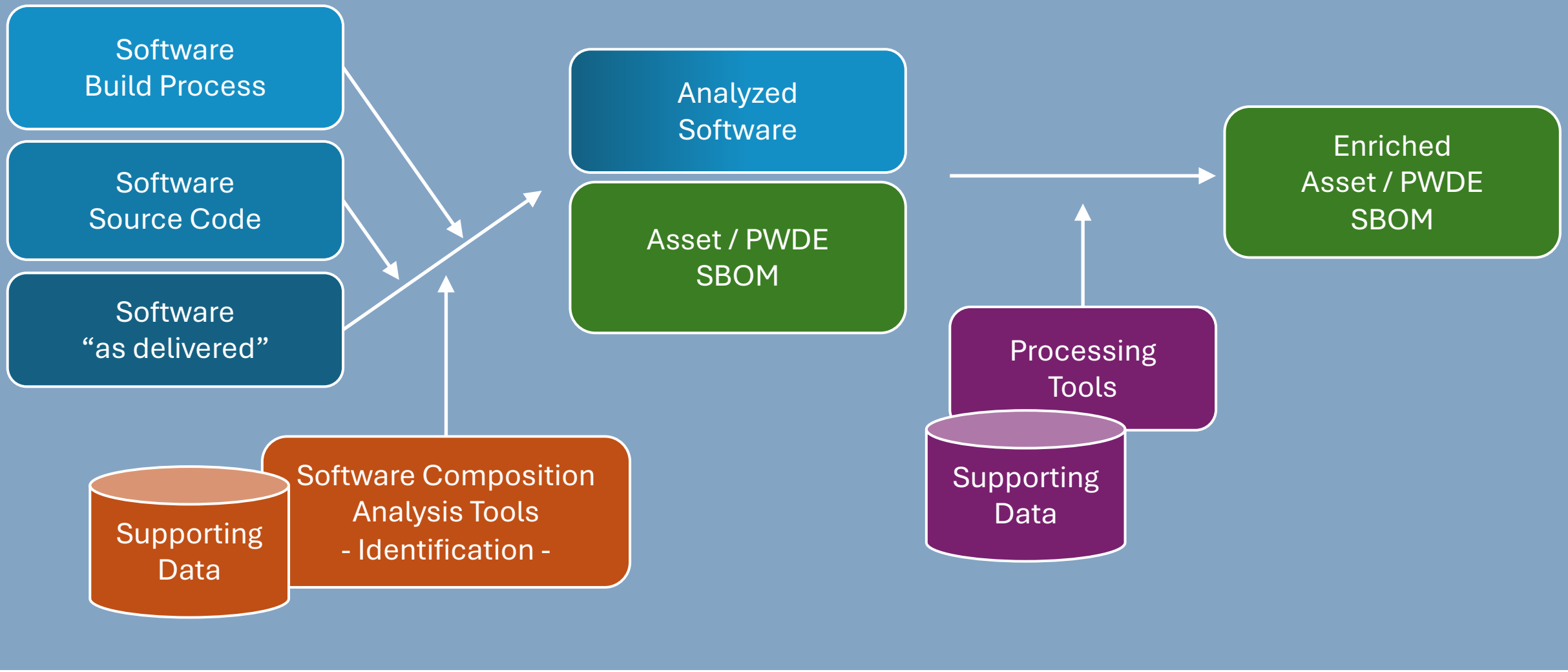
Asset – Analyse



Automatisierungsansätze – SBOM / Inventory als Basis



SBOM Erhebung & Anreicherung



SBOM-zentrische Anwendungsfälle

- SBOM als maschinen-lesbares Format zur Identifikation von Software
- SBOM als maschinen-lesbares Format zur Benennung der Lizenzen
- SBOM als Teil bzw. Basis der technischen Dokumentation
- SBOM basierte Prüfungen und Prüfberichte
- Qualitätssicherung auf Prüfergebnissen
- SBOM-basierte Konformitätsprüfungen durch Marktüberwachungsbehörde

→ Wie sieht eine solche qualifizierte SBOM konkret aus?
→ Was muss eine SBOM bei der Konformitätsprüfung leisten?
→ Was kann sinnvoll automatisiert werden?

https://github.com/org-metaeffekt/metaeffekt-bom-essentials/blob/main/README.md#external-references

Prüfbare SBOM / Ansatz

- Alle Bestandteile (Dateien/Inhalte) der Software können den Komponenten in der SBOM zugeordnet werden.
- Zu jeder Komponente der SBOM kann eine Datei oder Inhalt zugeordnet werden.
- Regeln für die Abbildung sind nachvollziehbar und ggf. standardisiert.

→Kanonische SBOM

- Detailierung / Standardisierung der Repräsentationen in SBOMs
- Prüfbarkeit gegenüber der Software Repräsentation
- SPDX / CycloneDX Ausprägung

Photo by Alex Siale on Unsplash

Qualifizierte SBOM

Ansatz, Inhalte, Anwendungsfälle, Ziele

Rahmenbedingungen

Teil 1 – Zusammenfassung

Teil 2

Schwachstellen Management

Identifikation, Kontextualisierung, Bewertung und Reporting

Prozesse, Richtlinien und Rahmenbedingungen

Problemstellung

[…] 'exploitable vulnerability' means a vulnerability that has the potential to be effectively used by an adversary under practical operational conditions;

[…] On the basis of the *cybersecurity risk assessment* referred to in Article 13(2) and where applicable, products with digital elements shall:

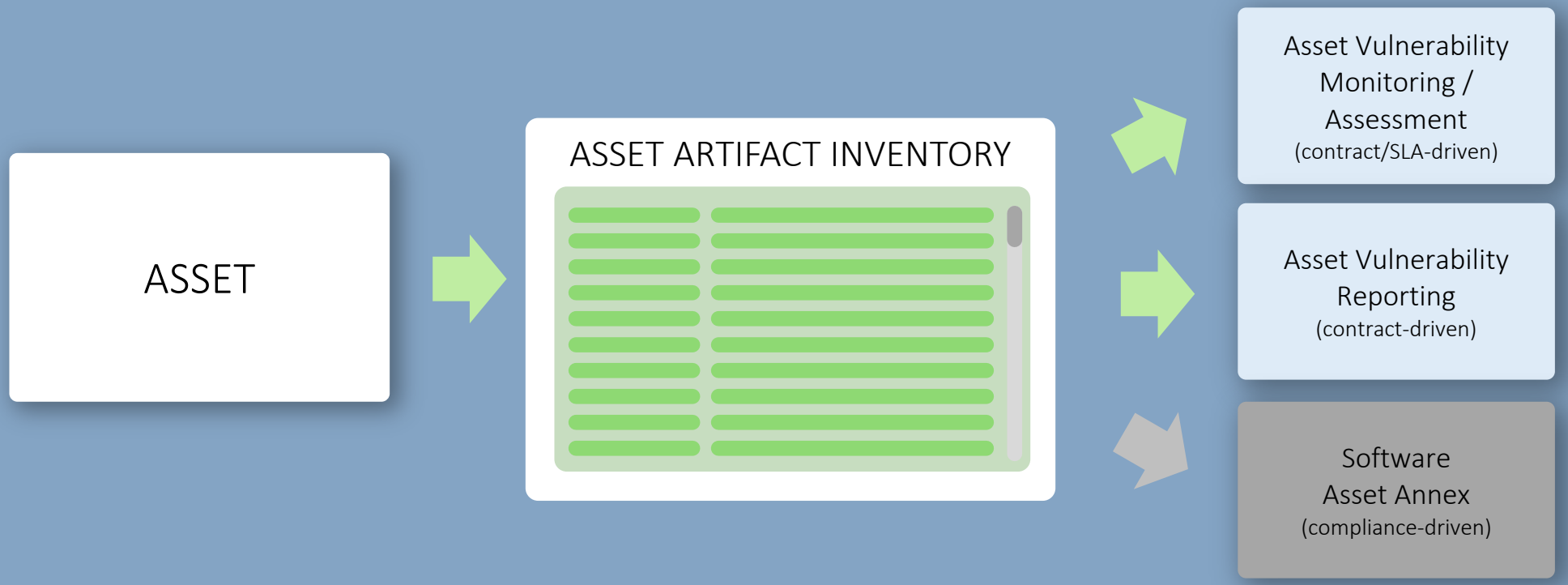
[…] be made available on the market without known exploitable vulnerabilities […]

[…] „ausnutzbare Schwachstelle“ eine Schwachstelle, die von einem Gegner unter praktischen Betriebsbedingungen wirksam genutzt werden kann;

[…] auf der Grundlage der *Bewertung der Cybersicherheitsrisiken* gemäß Artikel 13 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend,

[…] ohne bekannte ausnutzbare Schwachstellen auf dem Markt bereitgestellt werden, […]

Automatisierungsansätze – Schwachstellen Monitoring / Reporting



Ansatz

- Ableitung einer Richtlinie zur Bewertung zur Schwachstellen
  - Kontextualisierung (kontextbasierter CVSS Modulation)
  - Abschichtung (MUST, SHOULD, COULD / CRITICAL/HIGH/INSIGNIFICANT)
  - Priorisierung (ESCALATE, DUE, ELEVATED)
- Festlegung des Hersteller-Anforderungen auf Basis einer solchen Richtlinie
- Erforderliche Datenquellen einfordern, schaffen und bereitstellen

Schwachstellen Management

Identifikation, Kontextualisierung, Bewertung und Reporting

Verständnis, Fragen, Diskurs

Photo by Micaela Parente on Unsplash

Teil 2 – Zusammenfassung

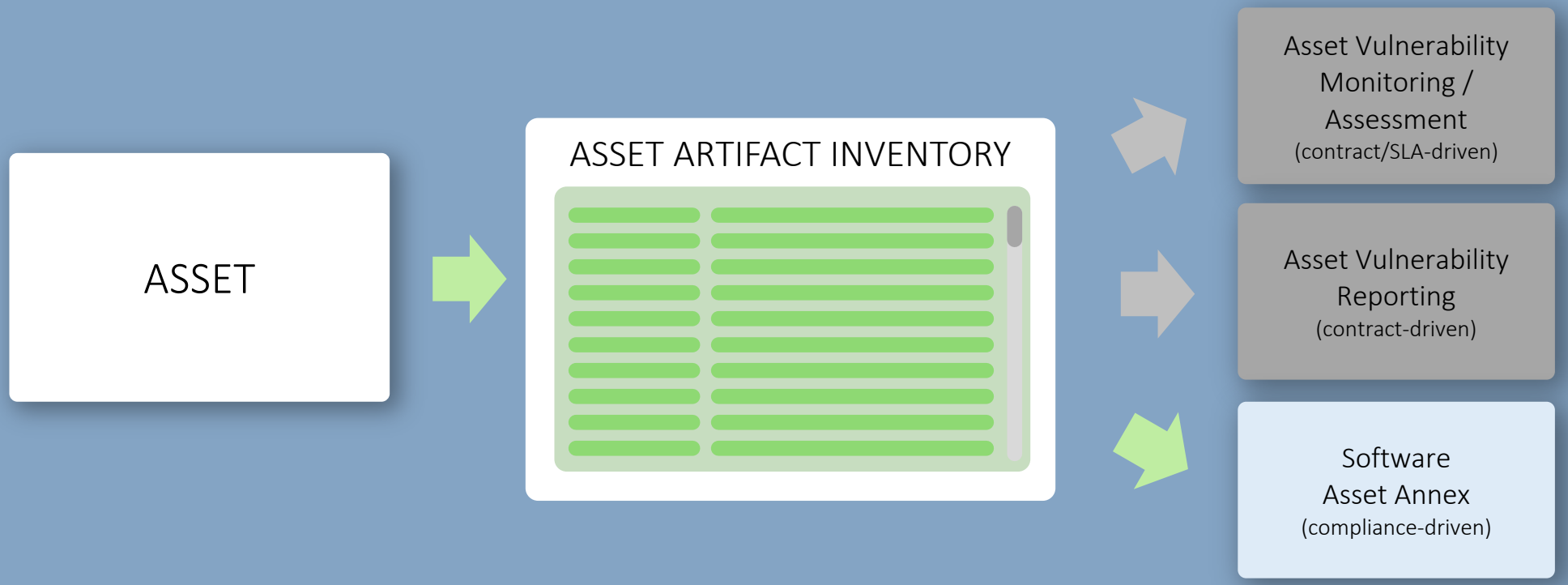
Teil 3

License Compliance

Erhebung, Bewertung, Reporting

Prozesse und Richtlinien und Rahmenbedingungen

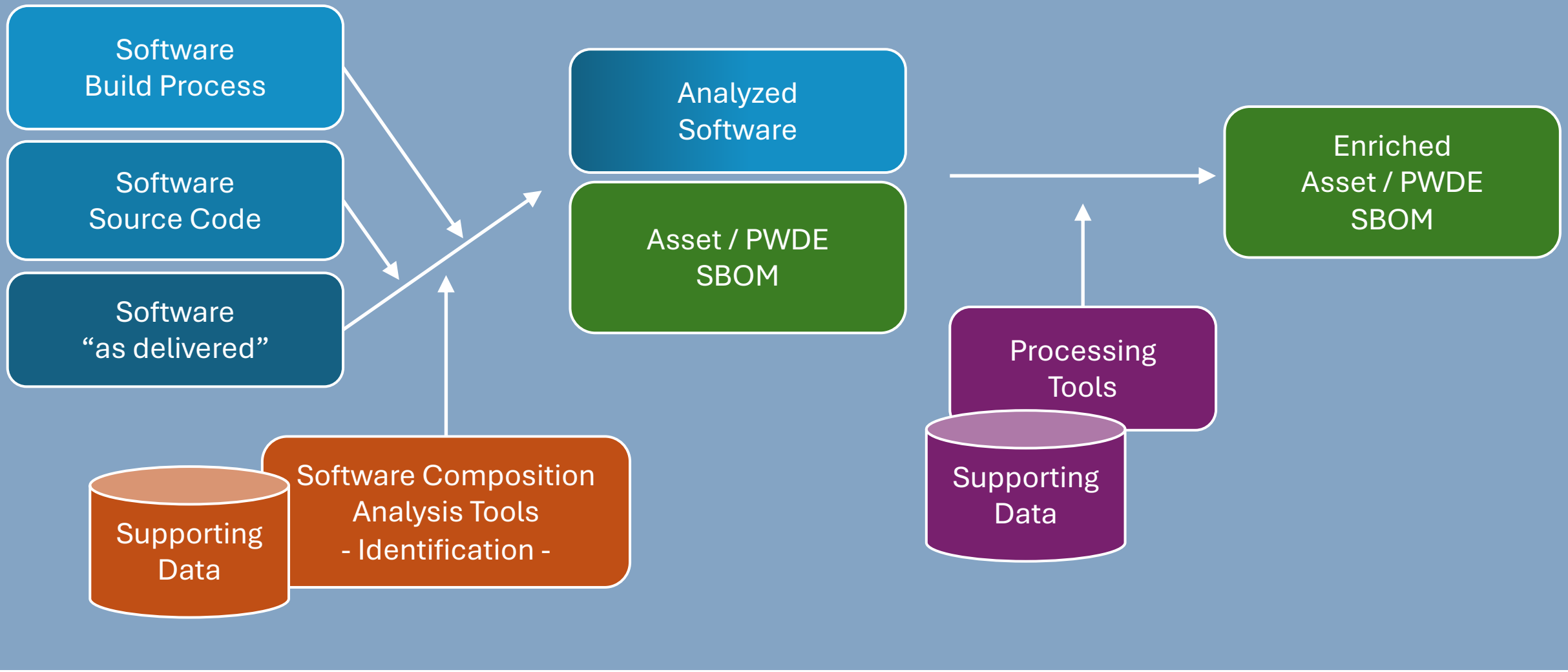
Automatisierungsansätze – „Software Asset Annex“



Rahmenbedingungen Herausforderungen

- Vielzahl der Technologien / Technologie-Interpretation
- Moderne Entwicklungsmethoden = viele Abhängigkeiten
- Viele Abhängigkeiten → breites Lizenzgefüge
- Umfang der Lizenzdatenbanken wächst
  Siehe auch https://github.com/org-metaeffekt/metaeffekt-universe
- Neue umfassende Regulierung, neue Standards
- Zugriff auf Daten / Repositories

SBOM Erhebung & Anreicherung



Automatisierungsansätze

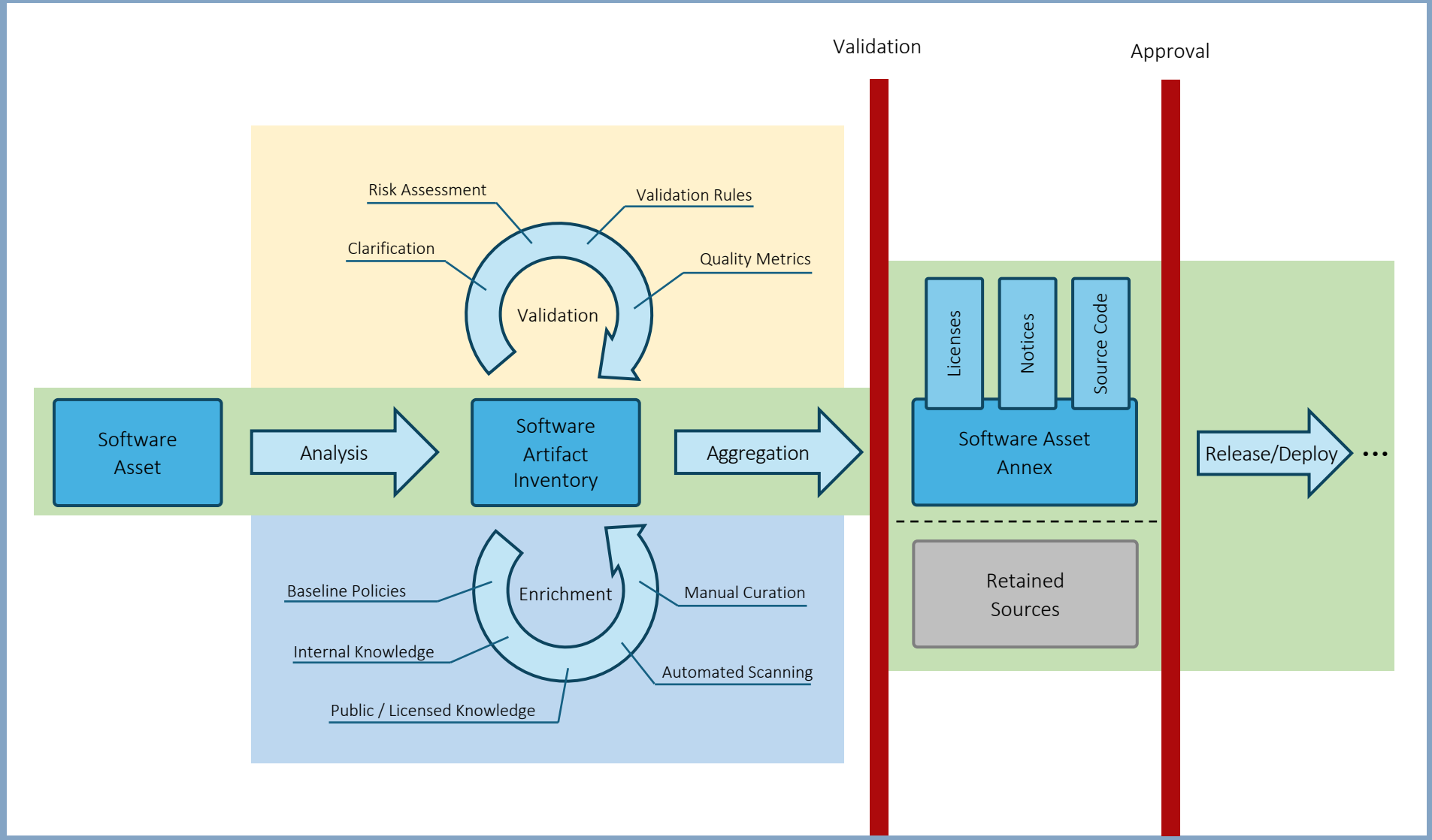


Photo by Samuel Clara on Unsplash

License Compliance

Erhebung, Bewertung, Reporting

Prozesse und Richtlinien und Rahmenbedingungen

Verständnis, Fragen, Diskurs

Teil 3 – Zusammenfassung

Bausteine und aktuelle Lizenzierung / Aktivitäten

- Extractor
  - {metæffekt} Extractor (Apache License 2.0; private repo)
- Resolver
  - {metæffekt} Resolver / 3rd-Party Indices (unterschiedliche Lizenz-Modelle)
- Lizenzdatenbanken
  - {metæffekt} Kosmos (CC-BY-4.0)
  - {metæffekt} Universe (Subskription); basiert auf {metæffekt} Kosmos
  - ScanCode Toolkit (CC-BY-4.0)
- Scanner
  - {metæffekt} Scanner (Apache License 2.0 ; private repo)
  - ScanCode Toolkit (Apache License 2.0)
  - ScanCode Service (Apache License 2.0; private repo)
- Vulnerability Monitoring / Assessment
  - {metæffekt} Vulnerability Dashboard Generator (Apache License 2.0)
  - {metæffekt} Universal CVSS Calculator
- Reporter
  - {metæffekt} Notice Engine (Apache License 2.0; private repo)
  - {metæffekt} Document Generator / Templates (Apache License 2.0)
- Policy Documents
  - Vulnerability Assessment Policy (CC-BY-4.0; not yet published)

Q & A

Photo by Samuel Clara on Unsplash

Questions & Answers

Aufruf zur Mitgestaltung

- Problem verstehen und lösen; Kompetenzen und Wertverständnis aufbauen
- Gemeinsames Wissen sammeln; Gemeinsam souverän auftreten.
- Best Effort / Continuous Improvement
- Proaktiv Festlegungen treffen, Vorschläge für Richtlinien/Umsetzung ableiten
- Feedback geben / Feedback einsammeln
- Über FOSS hinausdenken; kommerzielles Umfeld und Regularien
- Ausgestaltung eines konsortialen Ansatzes; primär für die Datenerhebung und Bewertung
- Schließlich gemeinsam in die Verbindlichkeit / Haftung treten

Photo by Alexas_Fotos on Unsplash

Vielen Dank für Ihre Aufmerksamkeit
im Namen des gesamte Teams der
{metæffekt} GmbH!

karsten.klein@metaeffekt.com

{metæffekt}

Weitere Links

- https://github.com/org-metaeffekt/metaeffekt-universe
- https://tinyurl.com/y32uutzb
- https://www.metaeffekt.com/security/cvss/calculator
- https://openchainproject.org/webinar/2024/03/22/webinar-universal-cvss-calculator
- Example Dashboards:
  - https://metaeffekt.com/security/dashboards/openssl-1.1.1o-dashboard.html
  - https://metaeffekt.com/security/dashboards/openssl-3.0.6-dashboard.html
  - https://metaeffekt.com/security/dashboards/keycloak-25.0.4-dashboard.html
  - https://metaeffekt.com/security/dashboards/keycloak-24.0.5-dashboard.html