

# CRA: Die CI/CD-Pipeline liefert Evidenz nicht Konformität

26.09.2023 | carmasec GmbH & Co. KG



**Marek Ruschulte**  
Security Consultant

- + **Annahme: Standardklasse.** Wichtige/kritische Produkte: zusätzliche Anforderungen, heute außen vor
- + **Anhang I Teil I:** keine bekannten ausnutzbaren Schwachstellen, Secure by Default, Integritätsschutz
- + **Anhang I Teil II:** SBOM, regelmäßige Tests, zeitnahe Behebung, sichere Update-Verteilung
- + **Nachweis** landet in der technischen Dokumentation (Art. 31, Anhang VII)
- + **Alles andere** — Risikobewertung, Supportzusagen, Meldewege — ist Prozess, nicht Pipeline

# Was eine CRA Pipeline leistet – und was nicht

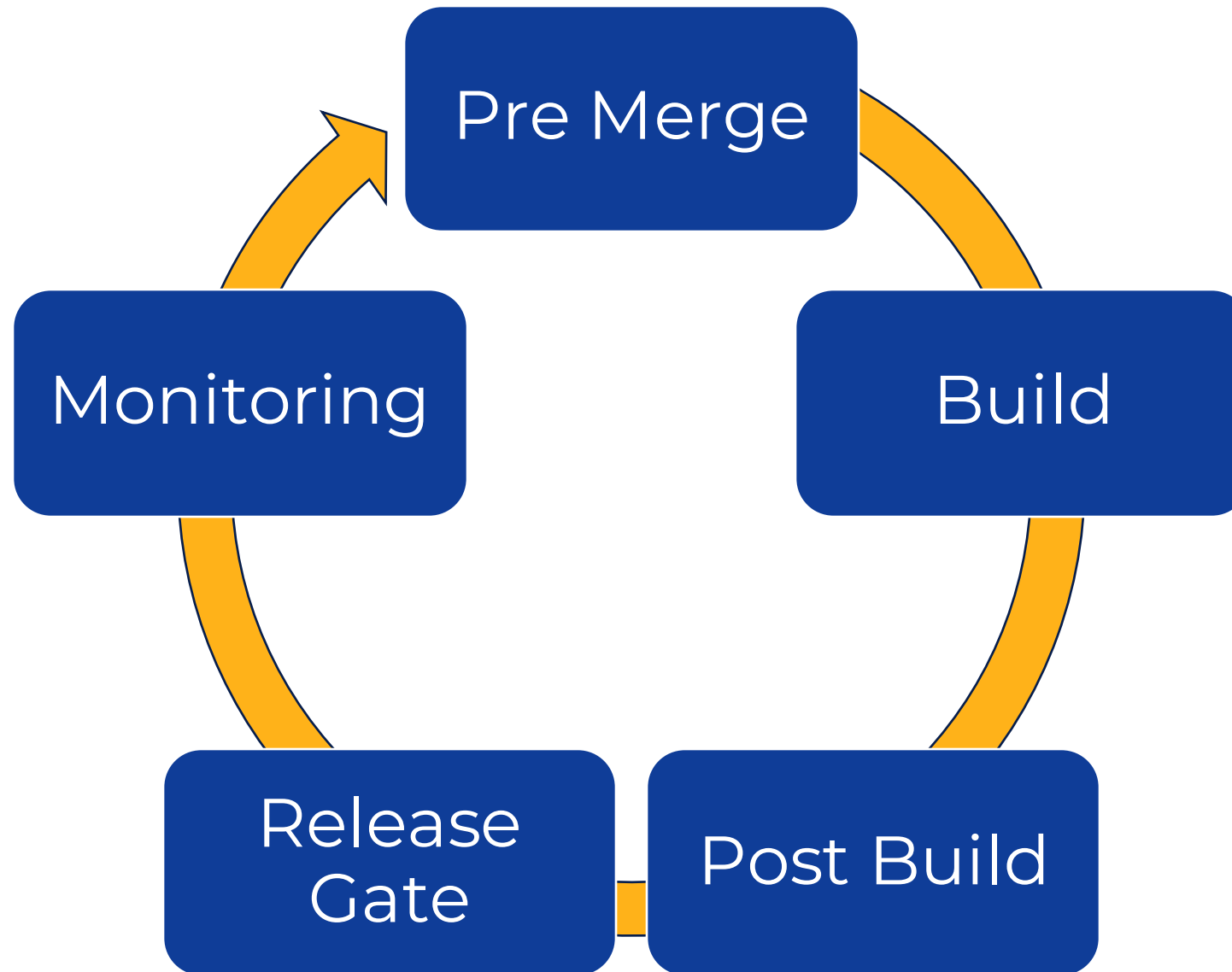
## Leistet

- Wiederholbarkeit
- Nachweisbarkeit
- Skalierung

## Leistet nicht

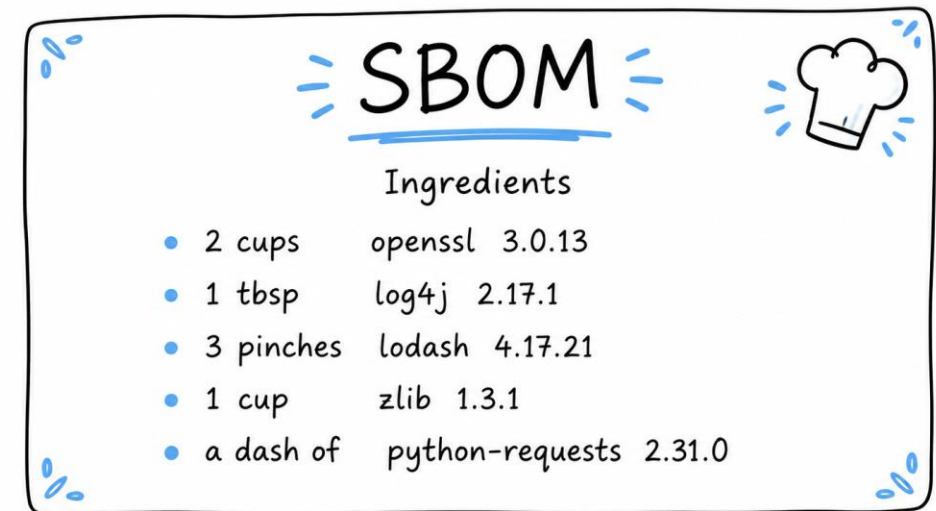
- Risikobewertung
- Prozesse
- Supportzeitraum
- Behördenkommunikation
- Perfekt Sicherheit

## Aufbau: welche Anforderungen liegen wo?



# SBOM: Inventar, nicht Anlage

- **Zweck:** vollständiges Komponenteninventar pro Build, maschinenlesbar, versioniert
- **CRA:** Teil der technischen Dokumentation, auf Verlangen vorzulegen
- **Mindestanspruch** sind Top-Level-Abhängigkeiten
- **Stolperstein:** SBOM aus dem Build statt aus dem fertigen Artefakt



- **Zweck:** eigener Code früh prüfen, Fremdcode dauerhaft beobachten
- **CRA:** „keine bekannten ausnutzbaren Schwachstellen" gilt zum Inverkehrbringen
- Danach läuft die Pflicht weiter — Monitoring ist kein Build-Schritt
- **Stolperstein:** Befundflut ohne dokumentierte Bewertung und Ausnahmeentscheidung

- **Zweck:** belegen, *was* gebaut wurde, *woraus* und *wo*
- **CRA:** Schutz vor unbefugter Veränderung; sichere Verteilung von Updates
- **Stolperstein:** Signatur wird erzeugt, aber nirgends im Deployment verifiziert
- **Build-Umgebung** ist Teil des Produkts — auch wenn sie nicht ausgeliefert wird



# Evidenz überlebt die Pipeline nicht

- Runner sind flüchtig, Logs rotieren, Registries werden aufgeräumt
- Technische Dokumentation: **10 Jahre** ab Inverkehrbringen, bei längerem Supportzeitraum länger
- Supportzeitraum im Normalfall **5 Jahre**, bei langlebigen Produkten deutlich mehr
- Konsequenz: Evidenz aus der Pipeline *herausschreiben* — unveränderlich, versioniert, auffindbar
- Was in acht Jahren niemand findet, hat es nie gegeben

”  
Die Pipeline liefert Evidenz. Konformität  
erklärt ihr.  
“

# Lust auf Kontakt?



## Marek Ruschulte

[marek.ruschulte@carmasec.com](mailto:marek.ruschulte@carmasec.com)

carmasec GmbH & Co. KG

