Sicherer Release: Signatur, Herkunft und Freigabe

PRUEFEN. BELEGEN. NACHHALTEN.

Arbeitsliste für Build-, Entwicklungs- und Deployment-Verantwortliche. Vertrauensanker und erwartete Herkunft vor der Artefaktprüfung festlegen; vorhandene Pipeline gezielt erweitern.

Pruefbereich / Team:

Datum:

- [ ] **01 / Quellrepository, Freigaberollen und Build-Workflow verbindlich zuordnen; Änderungen an Code und Pipeline vor Freigabe prüfen.**

  Nachweis: Geschützte Änderungspfade, Review-Nachweise und benannte Verantwortliche.

- [ ] **02 / Pipeline-Identitäten auf nötige Rechte begrenzen; kurzlebige Zugänge verwenden, wo unterstützt, und Geheimnisse aus nicht vertrauenswürdigen Builds heraushalten.**

  Nachweis: Effektive Berechtigungen und getrennte Verarbeitung externer Pull Requests.

- [ ] **03 / Build-Umgebung und Abhängigkeiten nachvollziehbar verwalten; Auflösung und Herkunft von Komponenten prüfen.**

  Nachweis: Build-Konfiguration, aufgelöste Versionen sowie dokumentierte Abhängigkeitsquellen.

- [ ] **04 / Komponentenübersicht beziehungsweise SBOM erzeugen und gegen relevante Schwachstellen bewerten; erreichbare betroffene Funktionen und Ausnahmen prüfen.**

  Nachweis: Release-bezogene Komponentenliste und nachverfolgte Bewertung der Funde.

- [ ] **05 / Ausgeliefertes Artefakt eindeutig über seinen kryptografischen Digest identifizieren; Integritätsinformationen aus vertrauenswürdiger Quelle beziehen.**

  Nachweis: Digest der tatsächlich geprüften und anschließend eingesetzten Bytes.

/ MAURISEC.DE

FIELD NOTES / CHECKLIST 11

- [ ] **06 / Signaturen beziehungsweise Attestierungen gegen festgelegte vertrauenswürdige Schlüssel oder Identitäten prüfen.**

  Nachweis: Verifizierungsprotokoll einschließlich des verwendeten Vertrauensankers.

- [ ] **07 / Provenance zusätzlich gegen erwarteten Builder, Quellstand und Build-Parameter prüfen; eine gültige Signatur allein reicht nicht als Freigabe.**

  Nachweis: Prüfregeln und negativer Test mit gültig signierter, aber unerwarteter Herkunft.

- [ ] **08 / Deployment an das geprüfte Artefakt binden und ungeprüften Austausch über veränderliche Tags verhindern.**

  Nachweis: Freigabenachweis, Deployment-Referenz und Übereinstimmung mit dem geprüften Digest.

- [ ] **09 / Release, Herkunftsnachweise und Prüfentscheidungen geschützt archivieren; Rücknahme und Reaktion auf spätere Schwachstellen vorbereiten.**

  Nachweis: Wiederauffindbarer Release-Satz und getesteter Eskalations-/Rücknahmeablauf.

GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

In einer isolierten Release-Prüfung ein nicht freigegebenes Testartefakt mit gültiger Signatur vorlegen; die Freigaberegel muss es dennoch zurückweisen.

GRENZEN UND VORAUSSETZUNGEN

Signaturen belegen unter definierten Vertrauensannahmen Integrität und Herkunft, nicht Fehlerfreiheit oder fachliche Freigabe. Eine SBOM ist keine automatische Vollständigkeitsgarantie. Provenance-Felder unterscheiden sich nach Format und Build-System. Ein dokumentierter SLSA-Level muss zur tatsächlich geprüften Plattform und Spezifikationsversion passen; hier wird kein Level verliehen.

PRIMAERQUELLEN / STAND 09.11.2026

NIST SP 800-218: Secure Software Development Framework
csrc.nist.gov

SLSA: Build - Verifying artifacts
slsa.dev

NIST SSDF - vollständige Veröffentlichung
doi.org