Komponenten und SBOM abgleichen

Fiktive Fallwerte und begründete Auswertung

Der Hersteller einer Messstation vergleicht das Freigabepaket mit der SBOM. Die Lieferdatei für die Station und der für die Auswertung notwendige Fernprozess enthalten insgesamt neun direkte Bibliotheken. Die exportierte Liste enthält acht Einträge. Die fehlende Messdatenbibliothek ist laut Paketprotokoll im Fernprozess enthalten. Der Lieferant stellt eine korrigierte Datei bereit. Der Fernprozess muss mit genau dieser Fassung abgeglichen werden.

Prüfpunkt	Soll oder Vergleich	Beobachtung	Entscheidung
Direkte Abhängigkeiten	9 im Liefermanifest	8 in der SBOM	Dossier offen
Messdatenbibliothek	Eindeutige Version im Fernprozess	Im Paket enthalten	Eintrag und Nachweis ergänzen
Lieferantenkorrektur	Am Lieferprodukt bestätigt	Geänderter Export vorhanden	Versionsabgleich wiederholen

Erwartetes Arbeitsergebnis

Versionsbezogene Stückliste mit dokumentierter Korrektur und wiederholtem Paketvergleich.

Erwartete Komponenten aus den Lieferpaketen erfassen.

Version, Fundort und Rolle der Komponente mit dem SBOM-Eintrag vergleichen.

Abweichung mit Lieferantenänderung und erneutem Paketvergleich schließen.

Gegenprobe und nächste Entscheidung

Ergänzen Sie die neunte Position mit der Bibliotheksversion aus dem Testsystem. Die Anzahl stimmt, doch der Versionsabgleich hält die Position bis zur Bestätigung offen.

Komponenten und SBOM abgleichen

Nennen Sie zu Ihrer Beobachtung jeweils einen auffindbaren Beleg.

Vergleichen Sie Paketmanifest, maschinenlesbare SBOM und Version der tatsächlich ausgelieferten Komponente.

Prüfkennung, Rechtsträger und Stichtag

Bearbeitung und verantwortliche Stelle

Produkt, Auslieferung und Fundort des Builds

Komponente, Ebene und bestätigte Lieferfassung

SBOM-Ausgabe, Format und fehlende Positionen

Zuordnung zu Gerät, App oder erfasster Fernverarbeitung

Drittkomponentenhinweis, Meldung an Pflege und eigene Prüfung

Komponenten und SBOM abgleichen

Beziehen Sie Abhilfe und Nachtest auf den ursprünglichen Prüfauftrag.

Befund und zugehörige Belegreferenz

Korrektur, geänderter Export und Verantwortliche

Geprüfter Nachtest mit Datum, Beobachtung und Versionsbeleg

Bestätigter Gesamtumfang und zweiter Paketvergleich

Freigabe durch und am

Offener Auftrag und Termin