Cybersicherheit von Produkt und KI zuordnen

Fiktive Fallwerte und begründete Auswertung

Eine fiktive Firewall sichert relevante Kommunikation in einem Trinkwassersystem. Die Fachstelle hat die Firewall als wichtiges Produkt der Klasse II und das KI-System in der vorgesehenen Sicherheitsfunktion als Hochrisiko-System eingeordnet. Als Fallannahme ist die interne Kontrolle nach Anhang VI der KI-Verordnung einschlägig. Ein passender alternativer Zertifizierungsweg ist im Fall nicht verfügbar. Die interne Dokumentation belegt fünf Schutzanforderungen am aktuellen Stand. Zwei für das geforderte Sicherheitsniveau festgelegte Nachweise fehlen, darunter der Nachweis zur Integrität des freigegebenen Modellstands. Eine erforderliche CRA-Bewertung über den gewählten Weg ist noch nicht bestätigt. Das Ergebnis zur vereinbarten Genauigkeit ist dagegen dokumentiert.

Prüfpunkt	Soll oder Vergleich	Beobachtung	Entscheidung
Verfahren	CRA-Pfad für die Klasse II im Fall	Interne KI-Prüfung liegt vor	CRA-Bewertung noch bestätigen
Schutzwirkung	7 Anforderungen am Lieferstand	5 geprüft und belegt	2 Nachweise offen
KI-Anforderungen	Genauigkeit und Robustheit separat	Genauigkeitsprüfung dokumentiert	Weitere KI-Nachweise fortführen

Erwartetes Arbeitsergebnis

Abdeckungsentscheid mit eigenem CRA-Verfahrensstatus sowie weiter erforderlichen KI-Nachweisen.

Produktklasse, KI-Einstufung und geprüften Lieferstand bestätigen.

Verfahrensbeleg und inhaltliche Schutzwirkung getrennt erfassen.

Erklärung und fortzuführende KI-Nachweise abgleichen.

Gegenprobe und nächste Entscheidung

Ergänzen Sie einen passenden Bewertungsnachweis für die CRA-Route und lassen Sie die Modellintegrität ausdrücklich außerhalb des geprüften Erklärungsumfangs. Der Verfahrensbeleg liegt vor. Die Abdeckung des dafür erforderlichen Sicherheitsniveaus bleibt offen.

Cybersicherheit von Produkt und KI zuordnen

Nennen Sie zu Ihrer Beobachtung jeweils einen auffindbaren Beleg.

Ordnen Sie Produktstand, KI-Einstufung, Bewertungsweg, Anforderung, Wirkung und Erklärung derselben Prüfung zu.

Prüfkennung, Rechtsträger und Stichtag

Bearbeitung und verantwortliche Stelle

Verantwortliche Rechtsträger, Produkt- und Modellstand

CRA-Kategorie und eigenständige KI-Einstufung

Bewertungsweg einschließlich Art. 12 Abs. 3, falls einschlägig

Belegte Schutzwirkung und Prozesse zur Schwachstellenbehandlung

Abdeckung und Reichweite der unterschriebenen Erklärung

Cybersicherheit von Produkt und KI zuordnen

Beziehen Sie Abhilfe und Nachtest auf den ursprünglichen Prüfauftrag.

Befund und zugehörige Belegreferenz

Offene Cybersicherheits-, Genauigkeits- oder Robustheitsbelege

Geprüfter Nachtest mit Datum, Beobachtung und Versionsbeleg

Freigabeumfang und zusätzliche KI-Bewertung dokumentieren

Freigabe durch und am

Offener Auftrag und Termin