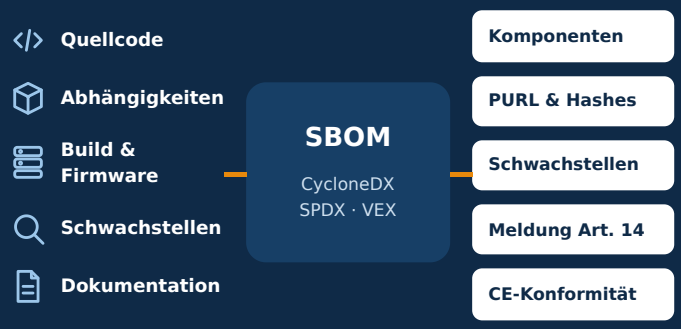
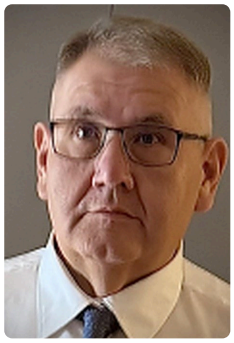
CRA: SBOM & HERSTELLERPFLICHTEN

Software-Stücklisten, die Prüfungen bestehen

SBOM, Schwachstellenmanagement und Meldepflichten nach dem Cyber Resilience Act (VO (EU) 2024/2847).

Von der Komponente bis zur Meldung an ENISA und CSIRT





Heinrich Markus Schulte
IT-Auditor · Sachverständiger

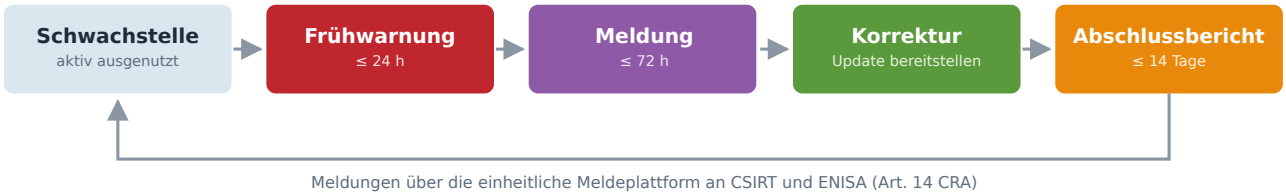
SBOM als Pflicht und Werkzeug

6 Module · 14 Lektionen · 63 Fragen

Nach CRA und BSI TR-03183-2. Praxisnah.

Komponenten kennen. Schwachstellen behandeln. Fristgerecht melden.

Meldekette bei aktiv ausgenutzten Schwachstellen



Meldungen über die einheitliche Meldeplattform an CSIRT und ENISA (Art. 14 CRA)

Meldepflicht gilt
Art. 14 CRA verpflichtet Hersteller seit dem 11. September 2026 zur Meldung.

SBOM gefordert
Anhang I verlangt eine Software-Stückliste mindestens der obersten Abhängigkeiten.

Volle Geltung 2027
Ab dem 11. Dezember 2027 gelten alle übrigen Herstellerpflichten.

6	14	63	~100 min	75 %	DE + EN
Module	Lektionen	Quizfragen	Lernzeit	Bestehen	Sprachen

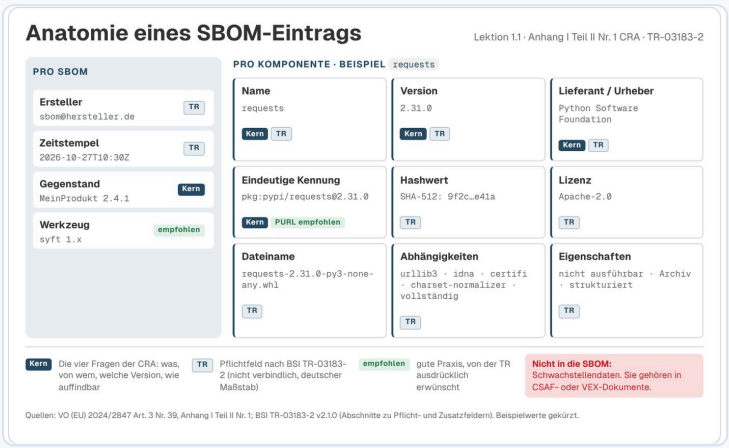
Testzugang oder Demo anfragen

Schulungsseite öffnen

12 Monate Zugang einschließlich Updates · Deutsch und Englisch · DSGVO-freundlich, ohne Werbe-Tracker

Eine SBOM ist kein Export-Knopf.

Warum Software-Stücklisten Prozess, Werkzeug und Nachweis zugleich sind



Anatomie eines SBOM-Eintrags: Name, Version, Lieferant, PURL, Hash und Abhängigkeiten.

Der Cyber Resilience Act macht Cybersicherheit zur Voraussetzung für die CE-Kennzeichnung von Produkten mit digitalen Elementen. Hersteller müssen Schwachstellen über den gesamten Unterstützungszeitraum behandeln, aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle melden und eine Software-Stückliste führen.

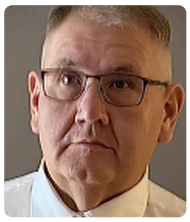
Die Schulung erklärt, was eine gute SBOM ausmacht: Komponenten, PURL und Hashwerte, die Formate CycloneDX, SPDX und VEX, die Tiefe nach BSI TR-03183-2 sowie Erstellung und Pflege in der Build-Pipeline. Werkzeuge wie cdxgen, Syft, Grype und Dependency-Track werden eingeordnet – herstellerneutral.

Darauf aufbauend geht es um die Meldekette nach Art. 14, weitere Herstellerpflichten, die Einstufung von Produkten und die Konformitätswege bis zur CE-Kennzeichnung.

RECHTSRAHMEN & BEZÜGE

VO (EU) 2024/2847 · **Art. 13, 14 CRA** · **Anhang I CRA** · **Art. 32 CRA** · **BSI TR-03183-2** · **CycloneDX · SPDX**

Der CRA kennt keine persönliche Schulungspflicht; die Bescheinigung belegt die Schulung, nicht die Produktkonformität. Grundlage ist ein AGPL-3.0-Kurs aus open-isms, bearbeitet und erweitert.



PRÜFERBLICK

Heinrich Markus Schulte

IT-Auditor · Sachverständiger
CISA · CISM · CIPP/E · CEH · T.I.S.P.

> *Die SBOM wird im Audit nicht gelesen, sondern geprüft: Ist sie vollständig, aktuell und mit dem Schwachstellenprozess verbunden?*

SBOM-GRUNDLAGEN

Komponenten, Lieferanten, PURL, Hashwerte, Abhängigkeitstiefe nach BSI TR-03183-2.

FORMATE & VEX

CycloneDX oder SPDX, VEX-Aussagen getrennt pflegen, maschinenlesbar austauschen.

PIPELINE & PFLEGE

eine SBOM pro Version, signieren, ablegen, Schwachstellen laufend abgleichen.

PFLICHTEN & KONFORMITÄT

Meldung nach Art. 14, Unterstützungszeitraum, Klassen, Konformitätswege, CE.

Fragen, die Aufsicht und Prüfer stellen

- Gibt es zu jeder ausgelieferten Version eine SBOM?
- Wie schnell erkennen Sie, ob eine neue Schwachstelle Ihre Produkte betrifft?
- Wer meldet eine aktiv ausgenutzte Schwachstelle binnen 24 Stunden?
- Welcher Konformitätsweg gilt für Ihr Produkt?

Inventarisieren · Prüfen · Bewerten · Beheben · Melden · Belegen

CRA: SBOM & HERSTELLERPFLICHTEN

Ablauf, Nutzen und Pakete

Sechs Module – von der Komponente bis zur CE-Kennzeichnung



Von der Schwachstelle zur Meldung: Fristen und Inhalte nach Art. 14 CRA.

Was Sie lernen

1. **Grundlagen der SBOM**
   Zweck, Mindestinhalte, Anhang I CRA
2. **Komponenten, PURL, Hashwerte**
   eindeutige Identifikation und Tiefe
3. **Formate**
   CycloneDX, SPDX, VEX im Vergleich
4. **Erstellung & Pflege**
   Pipeline, Werkzeuge, Signatur, Archiv
5. **Meldekette nach Art. 14**
   24 h, 72 h, Abschlussbericht
6. **Herstellerpflichten & Konformität**
   Klassen, Verfahren, CE-Kennzeichnung

FÜR WEN **Produktmanagement · Entwicklung · Product Security · PSIRT · Qualitäts- und Risikomanagement bei Herstellern**

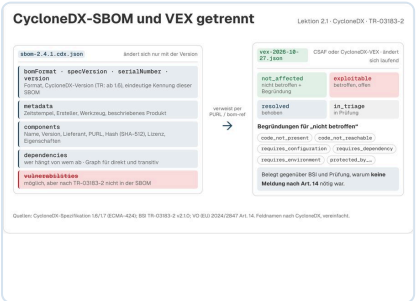
IHR MEHRWERT

Aktuell
Meldepflichten seit 11. September 2026 berücksichtigt.

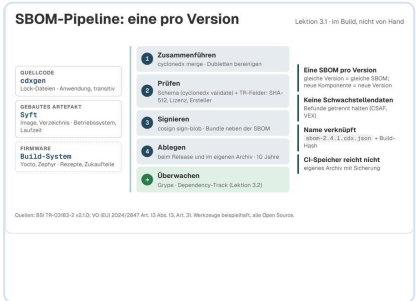
Werkzeugneutral
cdxgen, Syft, Grype, Dependency-Track eingeordnet.

Kompakt
Rund 100 Minuten für das gesamte Team.

Zweisprachig
Deutsch und Englisch für internationale Teams.



CycloneDX-SBOM und VEX



SBOM-Pipeline pro Version



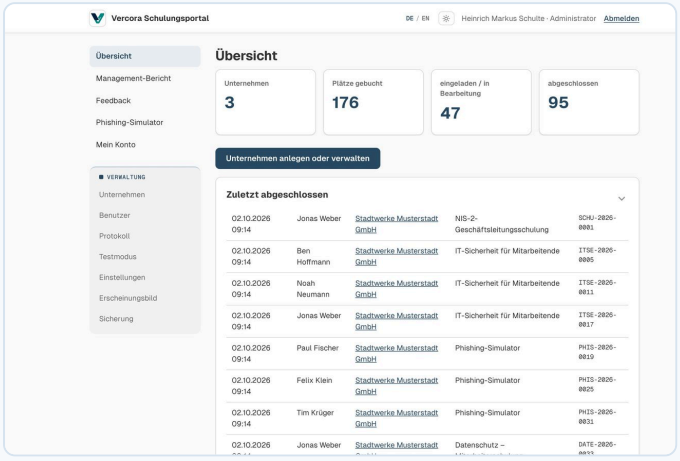
Vom Produkt zur CE-Kennzeichnung

PAKET & BUCHUNG Add-on zum Abo oder als Einzelplatz mit 12 Monaten Zugang · ideal für ganze Produkt- und Entwicklungsteams.

So läuft es ab

Vom Teamzugang bis zur nachweisbaren SBOM-Kompetenz

Im Vercora Schulungsportal inklusive



- **Teilnehmerverwaltung:** Plätze buchen, Personen anlegen, persönliche Einladungslinks ohne Passwort
- **Fortschritt & Management-Bericht:** Teilnahme, Abschlüsse und fällige Auffrischungen als PDF für die Leitung
- **Nummerierte Bescheinigung:** PDF mit Online-Echtheitsprüfung, Protokoll und eigenem Nummernkreis
- **Wiederholungsintervall:** je Schulung 6, 12, 24 oder 36 Monate – das Portal zeigt, wann nachgeschult wird
- **Ihr Erscheinungsbild:** auf Wunsch mit Ihrem Logo und Ihrer Farbe – auch auf Bescheinigung und Bericht
- **Sicher & datensparsam:** Anmeldung mit zweitem Faktor, Hash-Ketten-Protokoll, keine Werbe-Tracker

Der Schulungsprozess im Überblick

1 Buchen
Einzelplätze oder Team als Add-on

2 Lernen
sechs Module mit Lernkontrollen

3 Anwenden
SBOM-Pipeline und Meldekette

4 Nachweisen
Bescheinigung je Person

5 Auffrischen
Auffrischung bei Rechtsänderungen

Was Sie erhalten

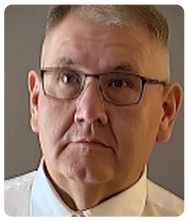
Sechs Module
14 Lektionen von der SBOM bis zur Konformität

Werkzeugeinordnung
cdxgen, Syft, Grype und Dependency-Track

Fristen & Meldewege
Art. 14 CRA als Ablaufgrafik

Prüfbarer Abschluss
nummerierte, online verifizierbare Bescheinigung

PRÜFERBLICK



Heinrich Markus Schulte

IT-Auditor · Sachverständiger
CISA · CISM · CIPP/E · CEH · T.I.S.P.

> *Wer seine Komponenten kennt, kann in Stunden statt Wochen sagen, ob er betroffen ist.*

Demo oder Testzugang anfragen

itschulte.de/schulungen.html

Sachverständigenbüro Schulte
Grünberger Weg 9 · 40627 Düsseldorf · +49 211 93375777 · sachverstaendiger@itschulte.de