BlueFlag Security

EU CYBER RESILIENCE ACT & DER SDLC · SOLUTION BRIEF · JULI 2026

Secure by Design — per Gesetz.
Der Nachweis entsteht in Ihrem SDLC.

Der Cyber Resilience Act verpflichtet Hersteller jedes Produkts mit digitalen Elementen zum Nachweis sicherer Entwicklung: Risikobewertungen, SBOMs, Zugriffskontrolle, Aktivitätsprotokollierung, Schwachstellenmanagement, 24-Stunden-Meldungen und zehn Jahre Dokumentation. Dieser Nachweis entsteht — oder geht verloren — im Software Development Lifecycle, in dem Entwickler, Contractors, Non-Human Identities und KI-Coding-Agenten die Produkte bauen, die der CRA reguliert.

LIVE HEUTE

In Kraft & in Vorbereitung

CRA in Kraft seit 10. Dez. 2024; Kapitel zu notifizierten Stellen gilt seit 11. Juni 2026

11. SEP. 2026

Meldepflichten starten

Art. 14 — in wenigen Wochen: 24 h Frühwarnung, 72 h Meldung über ENISAs Single Reporting Platform

11. DEZ. 2027

Volle Anwendung

Grundlegende Anforderungen, Konformitätsbewertung, technische Dokumentation und CE-Kennzeichnung

≥5 JAHRE

Support-Zeitraum

Schwachstellenmanagement über den erklärten Support-Zeitraum; Sicherheitsupdates zehn Jahre verfügbar

Verordnung (EU) 2024/2847 — veröffentlicht 20. Nov. 2024, in Kraft seit 10. Dez. 2024. Zeitplan gemäß den CRA-Implementierungsseiten der Europäischen Kommission; die ENISA Single Reporting Platform ist im Test und bis 11. Sep. 2026 operativ.

EXECUTIVE SUMMARY

Der CRA reguliert, wie Software entsteht — nicht nur, was ausgeliefert wird

Die Pflichten, die über Konformität entscheiden, sind **Entwicklungsprozess-Pflichten**: eine dokumentierte Risikobewertung als Design-Grundlage (Art. 13), grundlegende Anforderungen inklusive Schutz vor unbefugtem Zugriff und Protokollierung relevanter interner Aktivitäten (Anhang I Teil I), ein SBOM mit Komponenten-Due-Diligence (Anhang I Teil II, Art. 13(5)), Schwachstellenmanagement über einen erklärten Support-Zeitraum (Art. 13(8–9)), die Meldung ausgenutzter Schwachstellen und Vorfälle auf 24-h-/72-h-Uhren (Art. 14) und ein Anhang-VII-Paket technischer Dokumentation mit zehn Jahren Aufbewahrung (Art. 31).

Scanner, SBOM-Generatoren und Patching-Pipelines decken die **Artefakt-Ebene** ab. Was chronisch fehlt, ist die **Ebene der Entwicklungsevidenz**: wer — Mensch, Bot oder KI-Agent — jede Komponente geschrieben, freigegeben und ausgeliefert hat, ob der Zugriff auf Code- und Build-Systeme tatsächlich kontrolliert war und ob die Protokolle, die der CRA verlangt, für jedes Release existieren. BlueFlag Security ist das System of Record genau dafür: Software-Identität, Änderungs-Provenienz und SDLC-Governance-Evidenz.

DER BLINDE FLECK

DER TYPISCHE CRA-STACK — BEOBACHTET DAS ARTEFAKT

- SAST-/SCA-Scanning · SBOM-Generatoren
- Patching-Pipelines · Runtime & EDR · GRC

Notwendig für Anhang I und das Schwachstellenmanagement — aber nichts davon beweist, wer das Produkt gebaut hat, wer Zugriff hatte oder dass sichere Entwicklung tatsächlich stattgefunden hat.

→

DIE BLUEFLAG-FRAGE — KÖNNEN SIE SICHERE ENTWICKLUNG NACHWEISEN?

- **Wer — Mensch, Bot oder KI-Agent — hat diese Komponente geschrieben und freigegeben?**
- **War der Zugriff auf Code- und Build-Systeme kontrolliert?**
- **Existieren die Anhang-I-Aktivitätsprotokolle — für jedes Release?**
- **Können Sie eine ausgenutzte CVE in Minuten bis zu Commit und Owner zurückverfolgen?**

WARUM JETZT

Vier Gründe, warum der SDLC über CRA-Compliance entscheidet

FRIST

Meldung in Wochen

Art. 14 gilt ab 11. Sep. 2026: 24 h Frühwarnung, 72 h vollständige Meldung, Abschlussbericht binnen 14 Tagen (Schwachstellen) bzw. eines Monats (Vorfälle).

GELTUNGSBEREICH

Jedes digitale Produkt

Hardware und Software mit direkter oder indirekter Datenverbindung — die CE-Kennzeichnung zertifiziert jetzt CRA-Konformität als Marktzugang.

EVIDENZ

Ein Dokumentationsregime

Risikobewertung, SBOM, Aktivitätsprotokolle und das Anhang-VII-Paket — zehn Jahre aufbewahrt, Behörden auf Verlangen vorgelegt.

SANKTIONEN

Echte Konsequenzen

Bußgelder bis 15 Mio. € oder 2,5 % des weltweiten Umsatzes bei Verstößen gegen grundlegende Anforderungen oder die Pflichten der Artikel 13–14.

DAS FRAMEWORK

Eine Plattform, drei Rollen in Ihrem CRA-Programm

ROLLE	HERAUSFORDERUNG	BLUEFLAG-SECURITY-MEHRWERT
1 · Sichere Entwicklung nachweisen	Anhang I verlangt Zugriffskontrolle und Protokollierung relevanter interner Aktivitäten; Konformität setzt sichere Prozesse voraus — nicht nur gescannte Artefakte.	Der **Activity Intelligence Graph** attribuiert jeden Commit, jedes Review, jeden Build und jedes Deployment einem Menschen, einer NHI oder einem KI-Agenten; Least Privilege wird kontinuierlich über SCM, CI/CD und Registries durchgesetzt — Anhang I 3.1.4 (Zugriffskontrolle) und 3.1.12 (Protokollierung) operationalisiert und exportierbar.
2 · Die Lieferkette beherrschen	Das SBOM listet Komponenten; die Due Diligence (Art. 13(5)) verlangt zu wissen und zu steuern, wie jede einzelne ins Produkt gelangt ist.	Das **SI-BOM (Software Identity BOM)** verknüpft jede Abhängigkeit mit der Identität, die sie eingebracht hat — mit Approval-Trails für Komponentenänderungen und Upstream-Notification-Support, wenn der Fehler einer Komponente gefunden wird (Art. 13(6)) — im Zusammenspiel mit CycloneDX-/SPDX-Generatoren für volle Tiefe.
3 · Reagieren & melden — auf der Uhr	Die 24-h-/72-h-Uhren starten mit der Kenntnisnahme; manuelle Rekonstruktion über Git, CI und Ticketing sprengt das Zeitfenster.	**Schwachstelle-zu-Commit-zu-Owner-Trace in Minuten**: forensische Lineage des betroffenen Releases, der einbringenden Änderung und der verantwortlichen Identität — als Faktenbasis für die Meldungen an die Single Reporting Platform und den Abschlussbericht (Art. 14).

Positionierungsdisziplin: BlueFlag scannt nicht nach CVEs, deployt keine Patches, reicht keine ENISA-Meldungen ein und trifft keine Konformitätsentscheidungen. Es operationalisiert die Entwicklungsprozess-Kontrollen, die der CRA prüft — und bewahrt die Evidenz.

ARTIKEL FÜR ARTIKEL

Wo BlueFlag die Pflicht trägt

Sechs Pflichten, bei denen der CRA genau das verlangt, was eine identity-first SDLC-Kontrollebene liefert — abgeleitet aus der vollständigen Control-Mapping-Analyse.

1 Zugriffskontrolle · Anhang I 3.1.4

- Identitätsinventar über SCM / CI/CD / Cloud
- Least Privilege & JIT, Bereinigung veralteter Credentials
- Erkennung anomaler Zugriffe & Eskalationen

COMPLIANCE-WERT

„Schutz vor unbefugtem Zugriff" — kontinuierlich durchgesetzt, auf Verlangen belegt.

2 Protokollierung & Monitoring · Anhang I 3.1.12

- Audit-Trails für Commits, Merges, Pipeline-Läufe
- Toolchain-Observability über SCM & Registries
- SIEM-Streaming für Aufbewahrung & Korrelation

COMPLIANCE-WERT

Der Anhang-I-Nachweis relevanter interner Aktivität existiert — standardmäßig, für jedes Release.

3 SBOM & Due Diligence · 3.2.1 · Art. 13(5–6)

- SI-BOM: jede Komponente mit ihrem Einbringer verknüpft
- Approval-Trails für Dependency-Änderungen
- Upstream-Notification-Support bei Komponentenfehlern

COMPLIANCE-WERT

Das SBOM erhält einen verantwortlichen Owner für jede Komponente.

4 Schwachstellenmanagement · Art. 13(8–9)

- Schwachstelle-zu-Commit-zu-Owner-Tracing
- Remediation-Workflow via Jira / ITSM mit SLAs
- Support-Zeitraum-Tracking pro Produkt

COMPLIANCE-WERT

„Unverzüglich" wird messbar — mit benannten Ownern und Zeitstempeln.

5 Meldebereitschaft · Art. 14

- Forensische Korrelation des Angriffspfads
- Release-Lineage des betroffenen Builds
- Attribution ausgenutzter CVEs in Minuten

COMPLIANCE-WERT

Die 24-h-/72-h-Uhren starten mit Fakten — nicht mit Archäologie.

6 Technische Dokumentation · Art. 31 / Anhang VII

- Identity-Graphen, Logs und SI-BOM exportiert
- Approval- & Ausnahme-Register pro Release
- Aufbewahrungsfertige Pakete für den Zehn-Jahres-Horizont

COMPLIANCE-WERT

Das Dossier entsteht aus Aufzeichnungen — nicht aus Erinnerung.

VOLLSTÄNDIGE PROVENIENZ ÜBER DEN PRODUKTLEBENSZYKLUS

Produkt & Releases › **Repos & Pipelines** › **Identitäten & Agenten** › **SBOM & Approvals** › **Evidenz-Paket**

EHRLICHER SCOPE · ALLEIN NICHT AUSREICHEND

WO DER CRA WEITERE EBENEN BRAUCHT

- Schwachstellenerkennung — SAST / DAST / Fuzzing
- SBOM-Generierung in voller Tiefe — CycloneDX / SPDX
- Verschlüsselung, Härtung & Resilienz — Anhang I 3.1.5–3.1.9
- Patch-Deployment & Zehn-Jahres-Release-Archive
- Runtime-Detection — EDR / IDS; Konformitätsbewertung & CE-Kennzeichnung

→

DAS INTEGRATIONSMUSTER — SDLC SYSTEM OF RECORD

- **SAST / SCA** — Findings mit einbringender Identität und Release-Gate verknüpft
- **SBOM-Generator + SI-BOM** — ein Dokument: Komponenten plus Owner
- **Secrets-Manager** — BlueFlag markiert Exposures; Vault hält die Schlüssel
- **SIEM / SOAR** — Akteur- & Release-Lineage für die Art.-14-Response ausgetauscht
- **Jira / ITSM** — Remediation-Evidenz mit SLA-Zeitstempeln

DAS OPERATING MODEL

Meldebereit in Wochen. Konformitätsbereit bis Dezember 2027.

◉

Wochen 0–8 — Meldebereit bis 11. Sep.

Identitäts- und Toolchain-Discovery; forensische Lineage live; Intake–Triage–Eskalations-Workflow mit Ihrem Single-Reporting-Platform-Prozess verdrahtet.

⚙

Q4 2026 — Den Bestand governen

Organisationsweiter Rollout, Least Privilege und Bereinigung veralteter Konten über SCM / CI/CD, Policy-Definition und Developer-Onboarding.

▣

H1 2027 — Lieferkette & Schwachstellen

SI-BOM plus SBOM-Tooling, SAST-/SCA-Integration, Vulnerability-Triage-Workflow mit SLAs, Support-Zeiträume pro Produkt erklärt.

✓

H2 2027 — Konformität bis 11. Dez.

Internes Audit, Anhang-VII-Paket aus BlueFlag-Outputs assembliert, Einbindung notifizierter Stellen wo erforderlich, CE-Kennzeichnung.

WARUM JEDER STAKEHOLDER PROFITIERT

CISO / Product Security	Anhang I operationalisiert: Zugriffskontrolle, Least Privilege, Aktivitätsprotokollierung und Anomalie-Erkennung über die Pipelines, die jedes CE-gekennzeichnete Produkt bauen — mit dem forensischen Art.-14-Trail bereit vor dem 11. September.
GRC / Compliance	Die technische Dokumentation nach Anhang VII entsteht aus Live-Aufzeichnungen — Risikobewertungs-Inputs, SI-BOM, Logs, Approvals — über den Zehn-Jahres-Horizont aufbewahrt und Marktüberwachungsbehörden auf Verlangen vorgelegt.
Produkt / R&D-Leitung	Support-Zeiträume, Komponenten-Ownership und Update-Evidenz pro Produktlinie getrackt — die Datenbasis für Bewertungs-, Roadmap- und End-of-Support-Entscheidungen.
Legal / Regulatory	Saubere Rollentrennung: BlueFlag liefert den attribuierbaren technischen Nachweis; die Rechtsabteilung verantwortet Produktklassifizierung (Anhänge III/IV), den Konformitätsweg und die EU-Konformitätserklärung.
Engineering / Platform	Kontrollen leben im bestehenden Path-to-Merge — kein paralleler Compliance-Workflow; KI-Agenten und Automatisierung liefern weiter, mit einem benannten Owner hinter jeder Komponente und jeder Änderung.

EXECUTIVE MESSAGE

„Der CRA macht sichere Entwicklung zur Marktzugangsvoraussetzung. BlueFlag ist das System of Record, das sie nachweist — wer das Produkt gebaut hat, wer Zugriff hatte und dass die Kontrollen gehalten haben — Release für Release, über den Zehn-Jahres-Horizont.“

BlueFlag Security · EU Cyber Resilience Act & der SDLC

Seien Sie meldebereit — vor dem 11. September.

In unter 30 Minuten live — kein Agent, keine Code-Änderungen

blueflagsecurity.com

Informatives Solution Brief — keine Rechtsberatung. Referenzen: Verordnung (EU) 2024/2847 (Cyber Resilience Act), veröffentlicht im ABl. L am 20. Nov. 2024, in Kraft seit 10. Dez. 2024; Zeitplan und Meldemechanik gemäß den CRA-Seiten der Europäischen Kommission und der ENISA-Guidance zur Single Reporting Platform (notifizierte Stellen seit 11. Juni 2026; Art.-14-Meldungen ab 11. Sep. 2026; volle Anwendung 11. Dez. 2027; Abschlussberichte binnen 14 Tagen bzw. eines Monats). Produktklassifizierung (Anhänge III/IV), Konformitätsbewertung, CE-Kennzeichnung und Behördenmeldungen bleiben Kundenverantwortung. BlueFlag-Fähigkeitsaussagen entsprechen der öffentlichen Produktdokumentation.