Best Practices für die Umsetzung des EU Cyber Resilience Act

Von der Pflicht zur sicheren Praxis

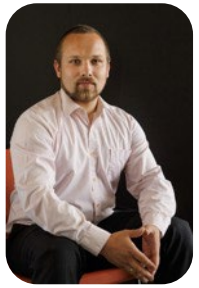
Alexander Aigner
Dr. Stephan Hutterer

CyberUp GmbH

CyberUp

OT | Security | Digitalization

Dr. Stephan Hutterer
CEO, Senior Consultant
Mail: sh@cyberup.at
Tel: +43 681 10877953



Alexander Aigner
CSO, Senior Consultant
Mail: aa@cyberup.at
Tel: +43 681 81582497

CRA Kompakt

Was: Security-Anforderungen für **alle Produkte mit digitalen Elementen**

Wo: EU Markt - nicht nur europäische Hersteller

Wie: Anforderungen an:

- Produkt (technische Eigenschaften)
- Prozess- und Dokumentation inkl. CE-Kennzeichnung
- Schachstellenmanagement und –Behebung
- Meldewesen bei Schachstellen und Vorfällen

Wann:

Für sämtliche Produkte “verkauft“ ab dem **11.12.2027**

Für sämtliche, auch bereits im Markt befindlichen, Produkte ab dem **11.09.2026**

Sanktionen: Bis zu **15 Mio. Euro oder 2.5% des Jahresumsatzes**

Produkte mit digitalen Elementen

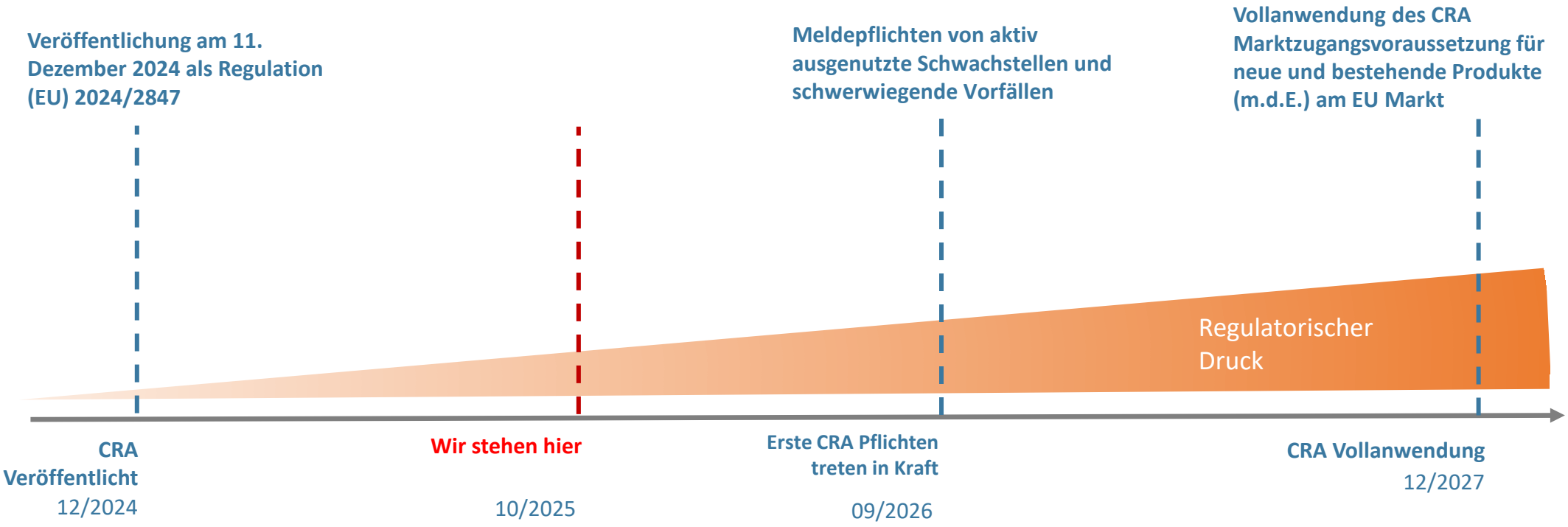
Hardware, Software oder **Kombinationen** davon die, **bestimmungsgemäß oder vernünftigerweise vorhersehbar:**

- **indirekt oder direkt mit anderen Systemen verbunden sind;**
- Daten **verarbeiten, speichern oder übertragen** können;
- einschließlich **aller für eine Funktion relevanten Fernbedienungsdienste (Cloud Service);**
- mit Gewinnerziehlungsabsicht auf dem europäischen Markt platziert sind.

Ausnahmen:

- Produkt ist bereits stärker oder gleichwertig reguliert (UNECE R155, EU MDR, …)
    - Keine Sektorausnamen Automotive / MedTech / etc.
- Reine SaaS Bereitstellung
- Reine Bereitstellung als Ersatzteil
- Sonderbehandlung OSS

Zeitleiste

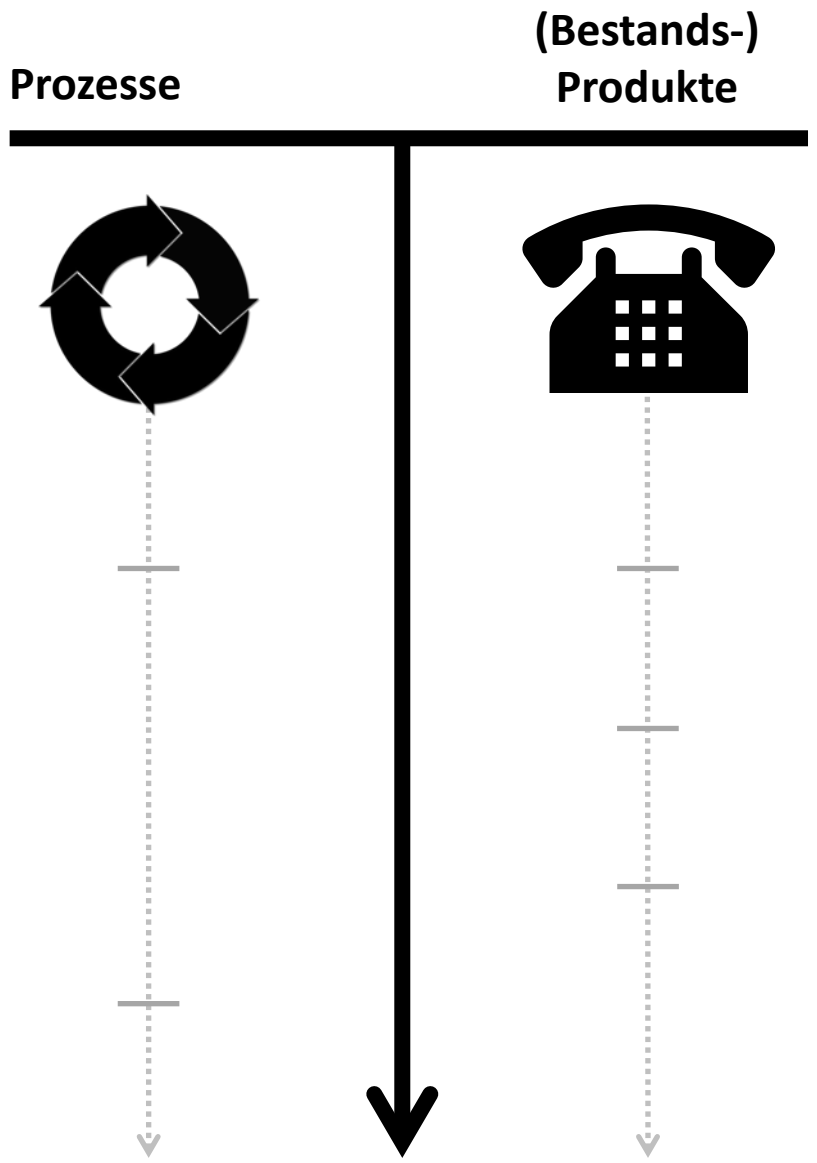


EU CRA
Cyber Resilience Act

Setze den CRA um. So einfach wie möglich.

CRA: Einführung

- **Bestandsaufnahme**
  - Prozesse
  - **Lieferanten**
  - **(Bestands!-)Produkte**
- Umsetzungsfahrplan
  - Prozess, neue Produkte
  - **(Bestands!-)Produkte**
- Umsetzung
  - etc.



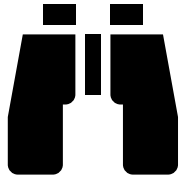
Stolperstein: Lieferanten

- Lieferant von Hardware liefert teils auch …
  - Betriebssystem
  - Firmware
  - Binär-Blobs
  - etc.

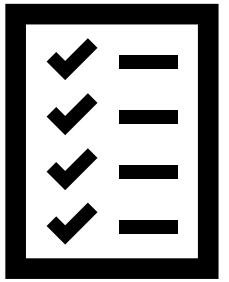
- Zugekaufte Softwarekomponenten
  - Abseits von Paketverwaltung etc.
  - Händisch verwaltet
  - Teils nicht über Einkaufsprozesse erfasst

Ansätze: Lieferanten

- Jedweden Beschaffungsweg erfassen
  1. In die Abteilungen gehen, Altbestand aufnehmen
  2. Technische Lösungen, Automatisierung



- Lieferanten frühzeitig in Umsetzung miteinbeziehen
  1. Austausch- und Ablauf bei Schwachstellen
  2. Zusammenarbeit bei Ereignis definieren (RASIC)
  3. Ereignis Testen, Effektivität sicherstellen



Ansätze: RASIC

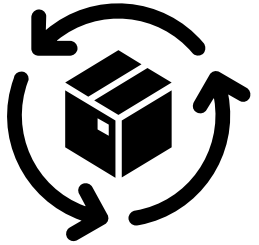
The Scope of this Agreement covers the following Workproducts and the corresponding Activities with respect to the Product defined on the Overview sheet

CSIA for [PRODUCT] between [MANUFACTURER] and [SUPPLIER]	**M** Manufacturer **S** Supplier	**R** Responsible (works on the work product) **A** Accountable (approves the work product) **S** Supports (supports the responsible to work on the work product) **I** Informed (this person is kept up to date on progress) **C** Consulted (counsels the people who work on the work product, delivers information)	**I** Initial **U** Updated **F** Final

WP-ID	Work Product or Activity	Responsibility					Interchange Agreement	Manufacturer Notes	Supplier Notes	Timeline			
		R	A	S	I	C				M1	M2	M3	M4
CSIA-01	Cybersecurity interface agreement	M/S	M				Full as Deliverable			F			
CSIA-02	Software Bill of Materials (SBOM)	S	S		M		Short as Deliverable and Full at Locaction			I	U	U	F
CSIA-03	Cryptographic Bill of Materials (CBOM)	S	S	M	M		Full as Deliverable				I	F	

Stolperstein: Bestandsprodukte

- Ungünstiger Produktlebenszyklus
  - Produktzyklus vs. CRA Timeline



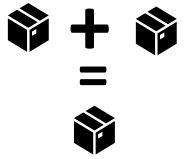
- Produkte kann Anforderung nicht erfüllen
  - z.B. Updatefähigkeit
  - Per Design, (e)Fuse blown, etc.

- Produkte für einzelnen Kunden
  - Aufwändige Individuallentwicklung, bereits in Fertigung

Extra-Stolperstein: Was ist ein Produkt

… oder „Welche Produkte habe ich überhaupt?“

- Gesamtanlagen als Produkt
  - zusätzlich Produkte: Nur angeboten im Kontext Gesamtanlage



- Entwicklungs-/Parametriert-/Servicetools
  - Teils in weiterer Vertriebskette, nicht direkte beim Endkunden

Ansätze: Bestandsprodukte

- Frühzeitig Abkündigen (wenn möglich)

- Anforderung ist nicht zutreffend
  - Behebung von Schwachstellen durch Hardwaretausch
  - Nicht-Aktualisierbarkeit ist Security-Feature

- “Jedes einzelne Produkt kann nur einmal auf dem Unionsmarkt in Verkehr gebracht werden“

Risikobasierter Entwurf

Produktdesign und Entwicklung

Entwurfsgrundlagen

- **Risikobasierter, sicherer Entwuf**
- Datenintegrität / –vertraulichkeit
- Zugriffskontrolle
- Angriffsflächenreduktion, sicherer Standardzustand
- Datenminimierung
- Sichere Datenlöschung und -Wiederherstellung
- Keine bekannten, ausnutzbaren Schwachstellen

Readiness & Resilience

- Protokollierung / Auditfähigkeit
- SBOMs
- Begrenzung/Reduzierung der Auswirkungen von Vorfällen
- Eindämmung & Begrenzung von Vorfällen
- Verfügbarkeit wesentlicher Funktionen

Wartung & Support

Schwachstellen- & Vorfallsmanagement

- Offenlegungsprozess; für ausgenutzte Schwachstellen und schwerwiegende Vorfälle
- CSIRT/PSIRT
- Sicherheitsupdates
- Sicherheitstests und –bewertungen

Öffentlich / Nutzerdokumentation

Benutzerdokumentation

- Vorgesehener Verwendungszweck
- Vorgesehen Einsatzumgebung und Eigenschaften
- Vorhersehbarer Missbrauch
- Sicherheitsrelevante Handhabung (Härtungsmaßnahmen, Außerbetriebnahme, Installation von Updates usw.)
- Supportzeitraum

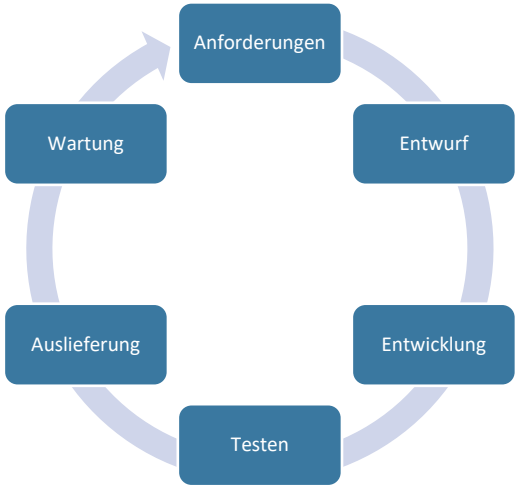
CE

Dokumentation zur Konformität

Technische- & Prozessdokumentation

- Risikobewertung / Modell
- Produktbeschreibung, Verwendungszweck und Umgebung
- Informationen zum Produktdesign (Architektur, Abhängigkeiten usw.)
- Selbstdeklaration oder Prüfbericht zur Konformität
- Supportzeitraum

SSDLC

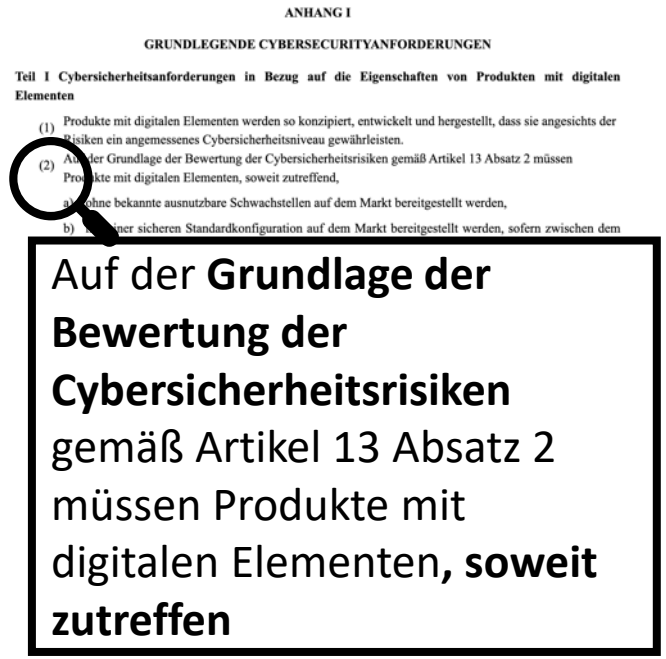


Risk Assessment

Nicht mit der Anforderungsdefinition beginnen

- „TLS hier, Secure Boot & Update da, fertig ist die Laube“

- Anforderungen basieren auf der Risikoanalyse
  - Ausmaß und Anwendbarkeit
- Risikoanalyse basiert auf dem Threat Model
- Beides fortlaufend Updaten



ANHANG I

GRUNDLEGENDE CYBERSECURITYANFORDERUNGEN

Teil I Cybersicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen

(1) Produkte mit digitalen Elementen werden so konzipiert, entwickelt und hergestellt, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten.

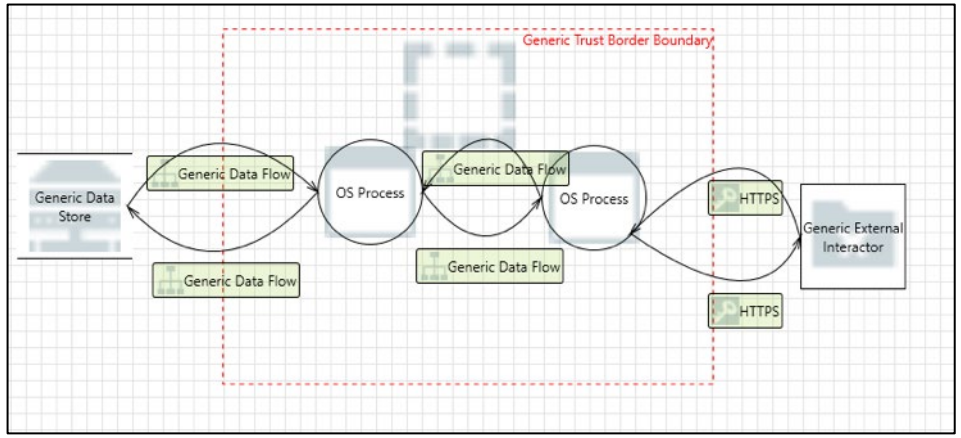
(2) Auf der Grundlage der Bewertung der Cybersicherheitsrisiken gemäß Artikel 13 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend,

a) ohne bekannte ausnutzbare Schwachstellen auf dem Markt bereitgestellt werden,

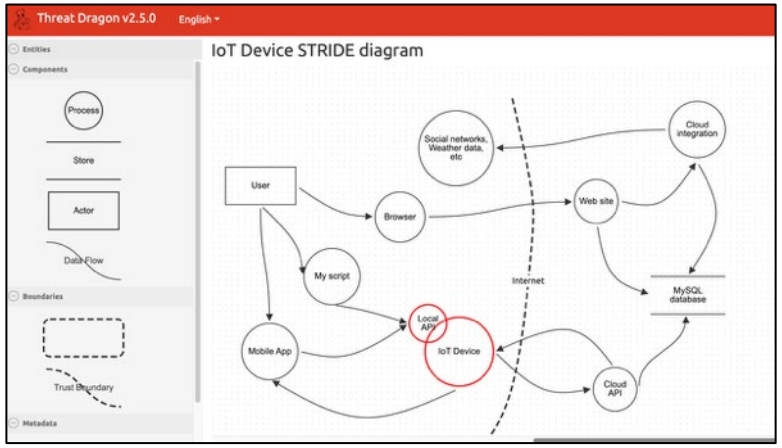
b) [illegible]ner sicheren Standardkonfiguration auf dem Markt bereitgestellt werden, sofern zwischen dem

Auf der **Grundlage der Bewertung der Cybersicherheitsrisiken** gemäß Artikel 13 Absatz 2 müssen Produkte mit digitalen Elementen**, soweit zutreffen**

Risk Assessment: Tool Support



Microsoft Threat Modeling Tool



OWASP Threat Dragon

Complyd

Stolperstein: Vulnerabilities

„Mein Produkt darf keine Komponenten / SW-Bibliotheken mit Schwachstellen mehr enthalten?“

- **Vulnerability**
  - Davon gibt es viele
  - Bewertung durchführen
- **Known Exploitable** Vulnerability
  - Auf meinem Produkt (!) ausnutzbar
  - Müssen behoben werden
- **Actively exploited** Vulnerability
  - Lösen Meldepflichten aus
  - 24h/72h nach Kenntnis, 14 Tage nach Verfügbarkeit Korrektur

Vulnerabilities: Ablauf

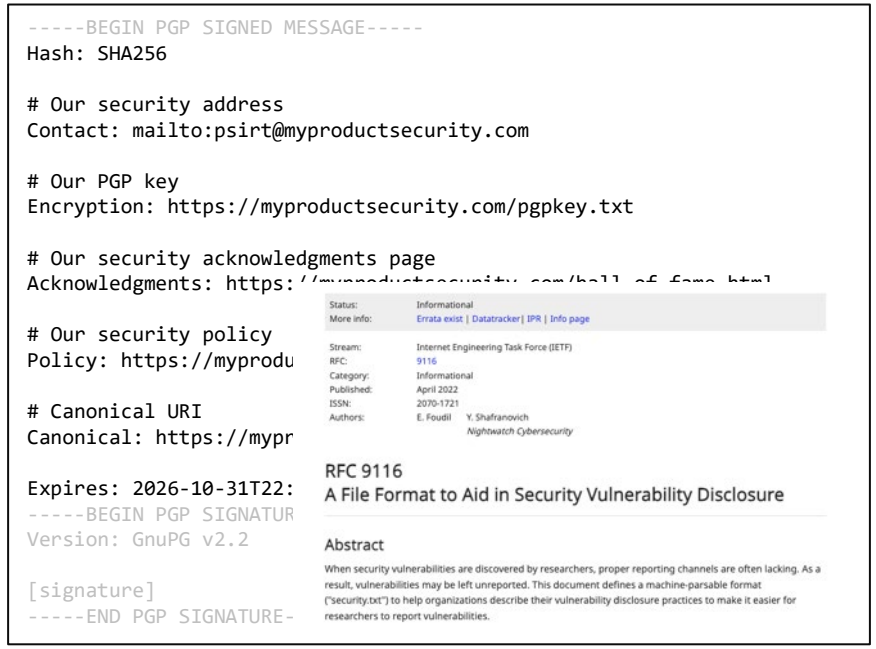
Externe Meldung **über CSIRT**

Externe Meldung an **Hersteller**

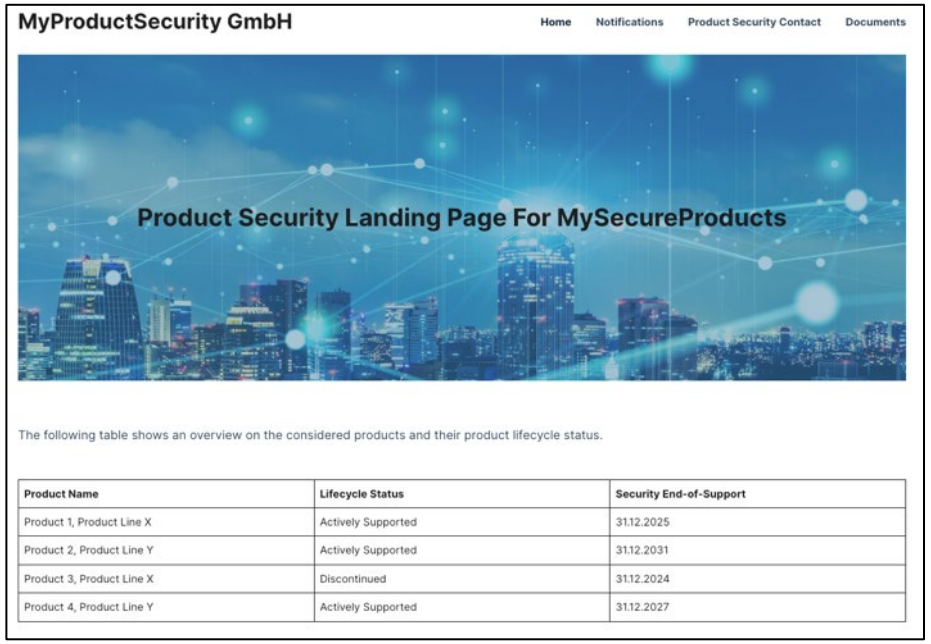
Fund via **Monitoring**, etc.

Vorfall

...



security.txt – RFC9116



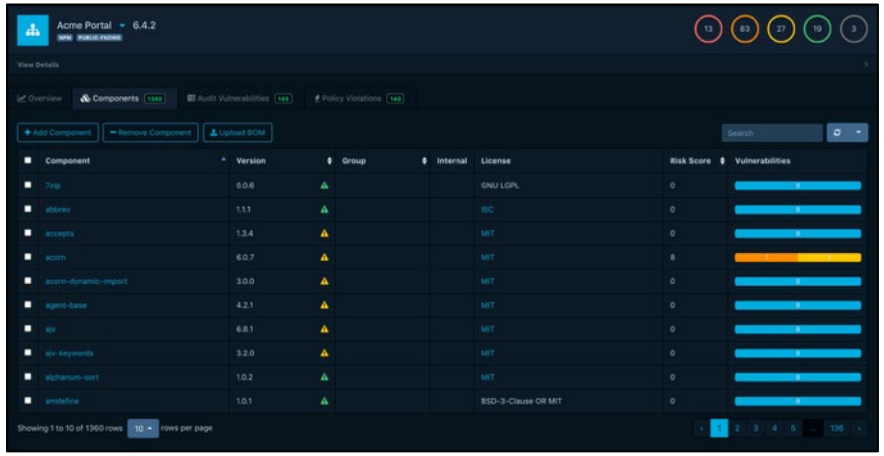
PSIRT Contact

Quelle

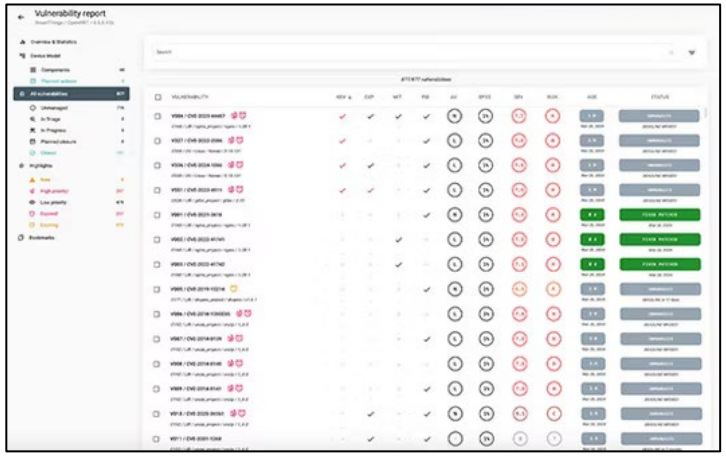
Analyse

Umsetzung

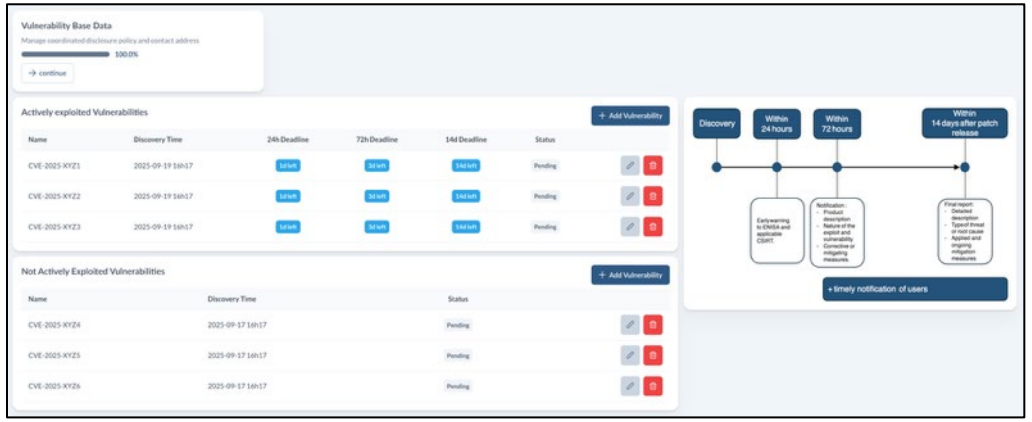
Vulnerabilities: Tool Support



Dependency Track



Security Pattern ARIANNA



Complyd

SBOM: Software Bill of Materials

- Strukturierte Liste aller Komponenten, Bibliotheken und Abhängigkeiten, die in einer Software enthalten sind
- Mehrere Ebenen möglich - Abhängigkeiten von Abhängigkeiten
- CRA fordert “**zumindest die obersten Abhängigkeiten**” d.h. eine Ebene
- Gängige Formate:
    - SPDX
    - CycloneDX
    - CSAF

SBOM: Erstellung

- Manuell
- Quellcode-Scanner
- IDE / Paket Mangement Plugins
  - Automatische Erzeugung bei Entwicklung
- CI/CD Pipeline Integration
  - Überwachung von Repositories, automatische Erzeugung
- Binary Decomposition
  - Versuch (!) der Erkennung aus bestehenden Anwendungen

Je früher im Produktentstehungsprozessdest o besser!

NICHT bzw. **nur für Legacy** empfohlen

Leitfäden

BSI TR-03183

- General Requirements, SBOM, Vuln. Reports
- https://www.bsi.bund.de/dok/TR-03183-en

Occtet - CRA SME requirements and self-assessment checklists

- https://occtet.eu/resources/deliverables/cra-sme-requirements/

Simplified Common Criteria for CRA

- https://github.com/sCC4CRA/

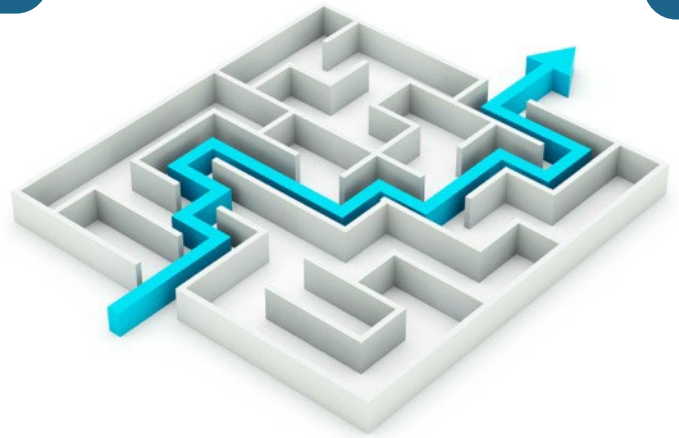
COMPLYD.IO: The Cyber Comliance Playbook

Requirements Fulfillment

Risk Assessment

Documentation Creation

Product Declaration



Conformity Declaration & Versioning

SBOM Management

Vulnerability Reporting

Incident Reporting

Let‘s cyber-up together!

Legen wir gemeinsam los:

Web: cyberup.at
Mail: sh@cyberup.at