



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



Classification: Public



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
- Schwachstellenmanagement und –Behebung
- Meldewesen bei Schwachstellen 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:**

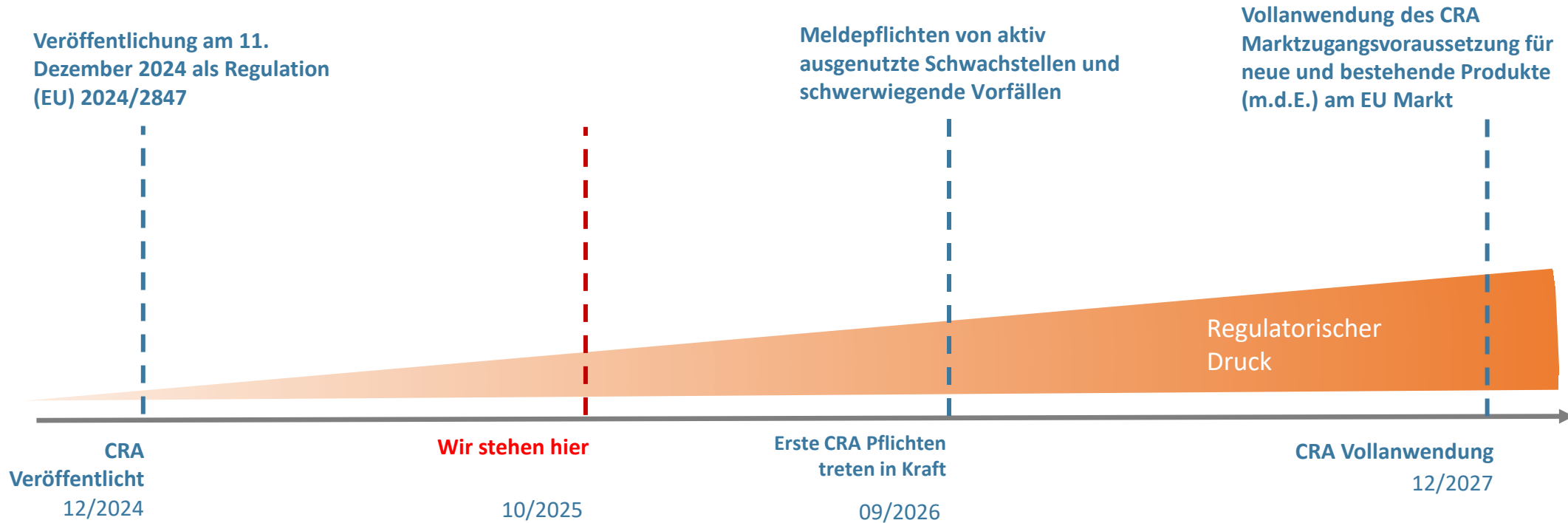
- **indirekt oder direkt mit anderen Systemen verbunden sind;**
- Daten **verarbeiten, speichern oder übertragen** können;
- einschließlich **aller für eine Funktion relevanten Fernbedienungsdienste (Cloud Service);**
- mit Gewinnerzielungsabsicht auf dem europäischen Markt platziert sind.

Ausnahmen:

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



Zeitleiste



EU CRA
Cyber Resilience Act

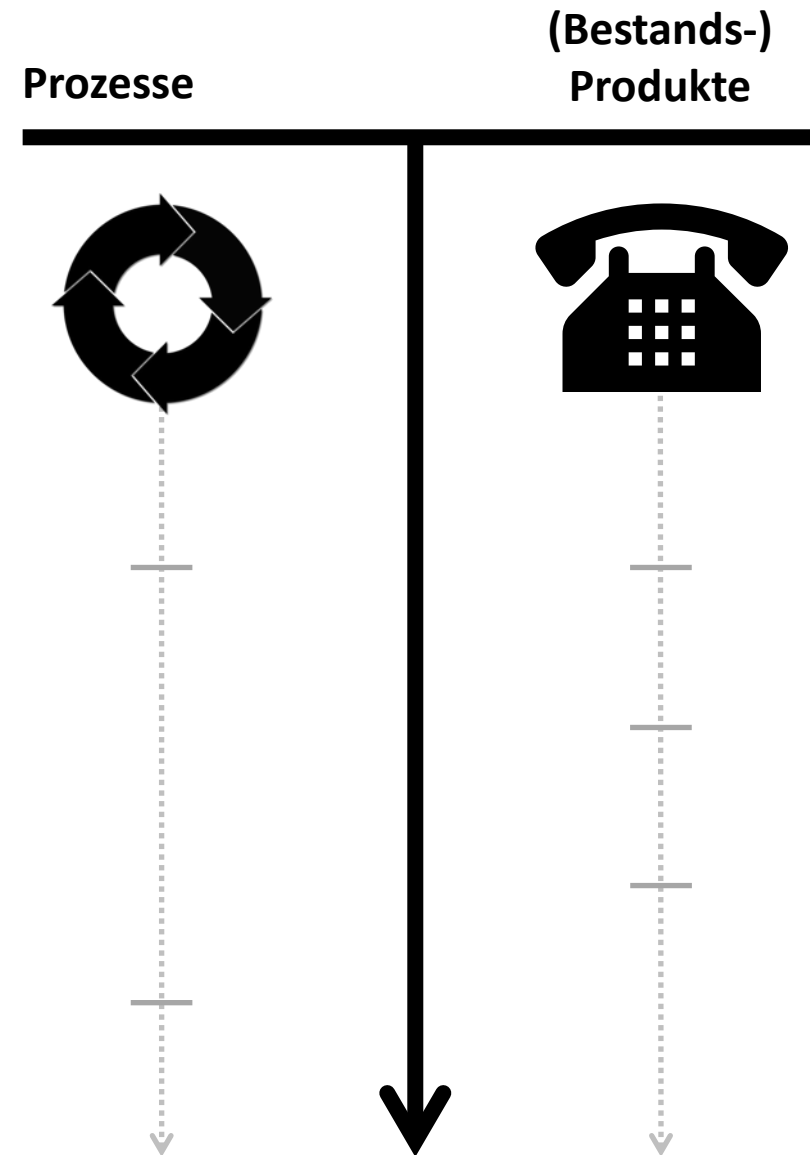


Setze den CRA um. So einfach wie möglich.



CRA: Einführung

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



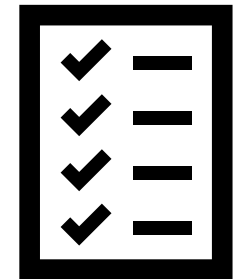
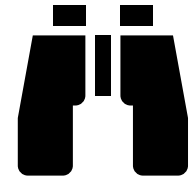
Stolperstein: Lieferanten

- 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



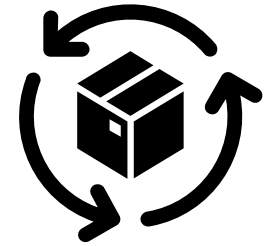
Ansätze: RASIC

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

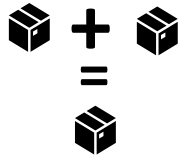
- Ungünstiger Produktlebenszyklus
 - Produktzyklus vs. CRA Timeline
- Produkte kann Anforderung nicht erfüllen
 - z.B. Updatefähigkeit
 - Per Design, (e)Fuse blown, etc.
- Produkte für einzelnen Kunden
 - Aufwändige Individuallentwicklung, bereits in Fertigung



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 Entwurf**
- 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



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

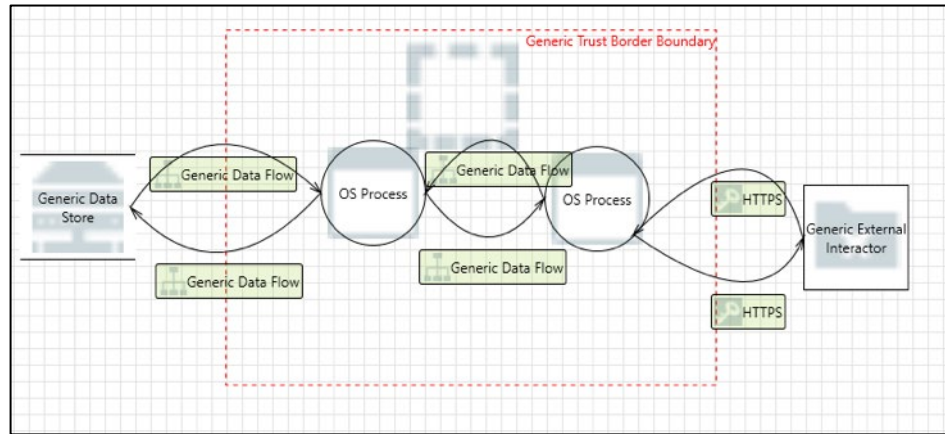
- „TLS hier, Secure Boot & Update da, fertig ist die Laube“
- Anforderungen basieren auf der Risikoanalyse
 - Ausmaß und Anwendbarkeit
- Risikoanalyse basiert auf dem Threat Model
- Beides fortlaufend Updaten



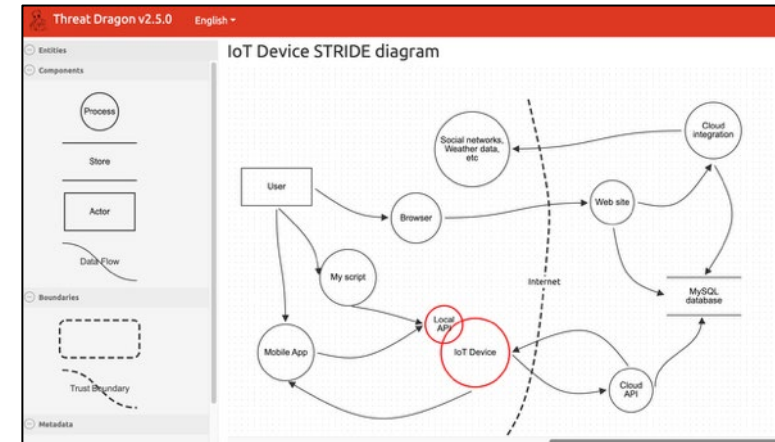
**Auf der Grundlage der
Bewertung der
Cybersicherheitsrisiken
gemäß Artikel 13 Absatz 2
müssen Produkte mit
digitalen Elementen, **soweit
zutreffen****



Risk Assessment: Tool Support



Microsoft Threat Modeling Tool



OWASP Threat Dragon

Element	Type	Data & Access Protection	Data & System Integrity	System Availability
IoT Device	Type: HARDWARE	🔗 pending	🔗 pending	🔗 pending
App Usage	Type: ANY	🔗 pending	🔗 pending	🔗 pending
Cloud to IoT Device HTTPS Channel	Type: ANY	🔗 pending	🔗 pending	🔗 pending
Web Usage	Type: ANY	🔗 pending	🔗 pending	🔗 pending
App	Type: SOFTWARE	🔗 pending	🔗 pending	🔗 pending
IoT Cloud	Type: SOFTWARE	🔗 pending	🔗 pending	🔗 pending
Web Interface	Type: SOFTWARE	🔗 pending	🔗 pending	🔗 pending
App to Cloud API	Type: ANY	🔗 pending	🔗 pending	🔗 pending

Graph

The graph shows an "Actor" connected to "App Usage" and "Web Usage". "App Usage" connects to "App", which then connects to "App to Cloud API". "Web Usage" connects to "Web Interface", which connects to "IoT Cloud" via "BiDir API". "IoT Cloud" connects to "Cloud to IoT Device HTTPS Channel", which then connects to "IoT Device". A dashed line labeled "Pressing Buttons" connects the "Actor" to the "IoT Device".

Comply



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

...

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Our security address
Contact: <mailto:psirt@myproductsecurity.com>

Our PGP key
Encryption: <https://myproductsecurity.com/pgpkey.txt>

Our security acknowledgments page
Acknowledgments: <https://myproductsecurity.com/hall-of-fame.html>

Our security policy
Policy: <https://myproductsecurity.com/security-policy.html>

Canonical URI
Canonical: <https://myproductsecurity.com>

Expires: 2026-10-31T22:00:00Z

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.2

[signature]
-----END PGP SIGNATURE-----

Status: Informational
More info: [Errata exist](#) | [Datatracker](#) | [IPR](#) | [Info page](#)
Stream: Internet Engineering Task Force (IETF)
RFC: 9116
Category: Informational
Published: April 2022
ISSN: 2070-1721
Authors: E. Foudil, Y. Shafarovich, Nighswatch Cybersecurity

RFC 9116
A File Format to Aid in Security Vulnerability Disclosure

Abstract

When security vulnerabilities are discovered by researchers, proper reporting channels are often lacking. As a result, vulnerabilities may be left unreported. This document defines a machine-parsable format ("security.txt") to help organizations describe their vulnerability disclosure practices to make it easier for researchers to report vulnerabilities.

security.txt – RFC9116

MyProductSecurity GmbH

[Home](#) [Notifications](#) [Product Security Contact](#) [Documents](#)



The following table shows an overview on the considered products and their product lifecycle status.

Product Name	Lifecycle Status	Security End-of-Support
Product 1, Product Line X	Actively Supported	31.12.2025
Product 2, Product Line Y	Actively Supported	31.12.2031
Product 3, Product Line X	Discontinued	31.12.2024
Product 4, Product Line Y	Actively Supported	31.12.2027

PSIRT Contact

Quelle

Analyse

Umsetzung

Auslieferung

Entwicklung

Testen

Classification: Public



Vulnerabilities: Tool Support

The screenshot shows the 'Acme Portal' interface. At the top, it displays 'Acme Portal 6.4.2' with a 'NEW PUBLIC RELEASE' badge. On the right, there are five circular status indicators: 13 (red), 65 (orange), 27 (yellow), 10 (green), and 3 (blue). Below the header, there's a 'View Details' link. The main navigation bar includes 'Overview', 'Components (136)', 'Audit Vulnerabilities (16)', and 'Policy Violations (145)'. The 'Components' section is active, showing a table with columns: Component, Version, Group, Internal, License, Risk Score, and Vulnerabilities. The table lists 10 components, each with a version number, a group (all green triangles), an internal status (all empty), a license (various like GNU LGPL, ISC, MIT), a risk score (0 or 8), and a bar chart representing vulnerabilities. The 'agent-base' component has a risk score of 8 and a yellow bar, while others have a risk score of 0 and blue bars. At the bottom, it says 'Showing 1 to 10 of 1360 rows' with a '10 rows per page' dropdown and a pagination bar showing 1, 2, 3, 4, 5, and 136.

Component	Version	Group	Internal	License	Risk Score	Vulnerabilities
7zip	6.0.6	▲		GNU LGPL	0	0
abbrev	1.1.1	▲		ISC	0	0
accepts	1.3.4	▲		MIT	0	0
acorn	6.0.7	▲		MIT	8	0
acorn-dynamic-import	3.0.0	▲		MIT	0	0
agent-base	4.2.1	▲		MIT	0	0
ajv	6.8.1	▲		MIT	0	0
ajv-keywords	3.2.0	▲		MIT	0	0
alphanum-sort	1.0.2	▲		MIT	0	0
ansi-regex	1.0.1	▲		BSD-3-Clause OR MIT	0	0

Dependency Track

Security Pattern ARIANNA

Vulnerability Base Data
Manage coordinated disclosure policy and contact address
100.0%

[→ continue](#)

Actively exploited Vulnerabilities [+ Add Vulnerability](#)

Name	Discovery Time	24h Deadline	72h Deadline	14d Deadline	Status		
CVE-2025-KY21	2025-09-19 16h17	Status	Status	Status	Pending	Edit	Delete
CVE-2025-KY22	2025-09-19 16h17	Status	Status	Status	Pending	Edit	Delete
CVE-2025-KY23	2025-09-19 16h17	Status	Status	Status	Pending	Edit	Delete

Not Actively Exploited Vulnerabilities [+ Add Vulnerability](#)

Name	Discovery Time	Status		
CVE-2025-KY26	2025-09-17 16h17	Pending	Edit	Delete
CVE-2025-KY25	2025-09-17 16h17	Pending	Edit	Delete
CVE-2025-KY26	2025-09-17 16h17	Pending	Edit	Delete

Timeline Diagram:

- Discovery**
- Within 24 hours**
 - Early warning to CVEs and applicable CSIRT
- Within 72 hours**
 - Notification:
 - Product description
 - Nature of the exploit and its impact
 - Concrete steps to mitigate/mitigation measures
- Within 14 days after patch release**
 - Final report:
 - Detailed description
 - Impact/threat to the system
 - Number and ongoing mitigation measures

[+ timely notification of users](#)

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 Management 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

Classification: Public



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

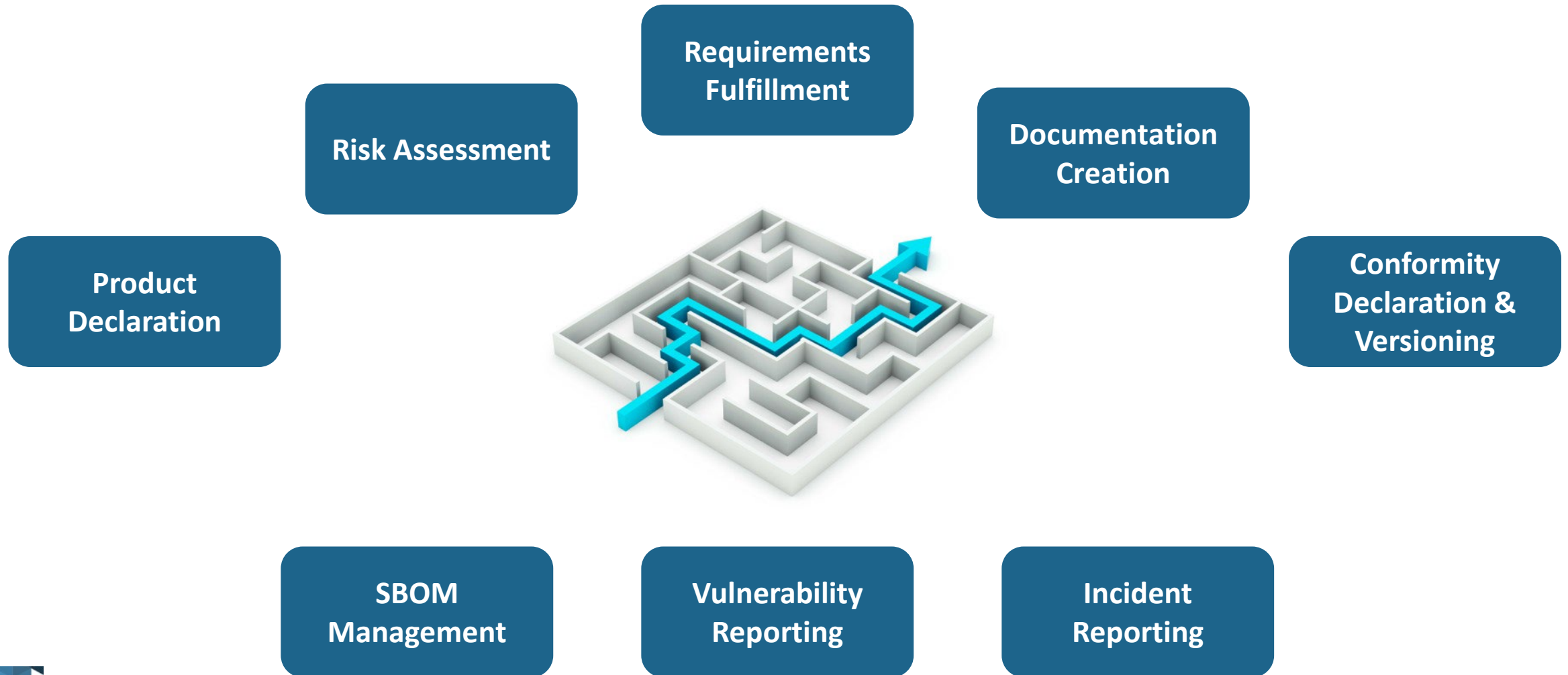
- <https://occtet.eu/resources/deliverables/cra-sme-requirements/>

Simplified Common Criteria for CRA

- <https://github.com/sCC4CRA/>



COMPLYD.IO: The Cyber Compliance Playbook





Let's cyber-up together!

Legen wir gemeinsam los:

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

