TROOPERS

Troopers Roundtable Supply Chain Security

How to strengthen Supply Chain Security — Practical Exchange and Roadmap

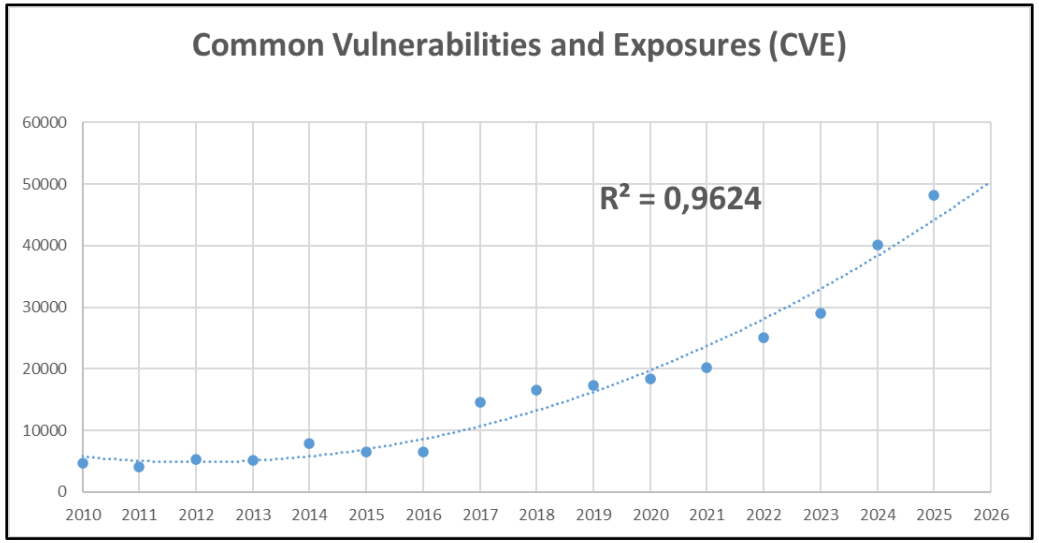
Agenda – Roundtable Supply Chain Security

1. Presentation
    1. Cyber Resilience Act (Michael Schuster)
    2. SBOM (Florian v. Samson)
    3. Vulnerability Management (Dr. Dina Truxius)
    4. Live Demo (Stefan Fleckenstein)
2. Q&A
3. Open Discussion

The number of vulnerabilities is constantly increasing

How can we handle 130+ vulnerabilities/day?

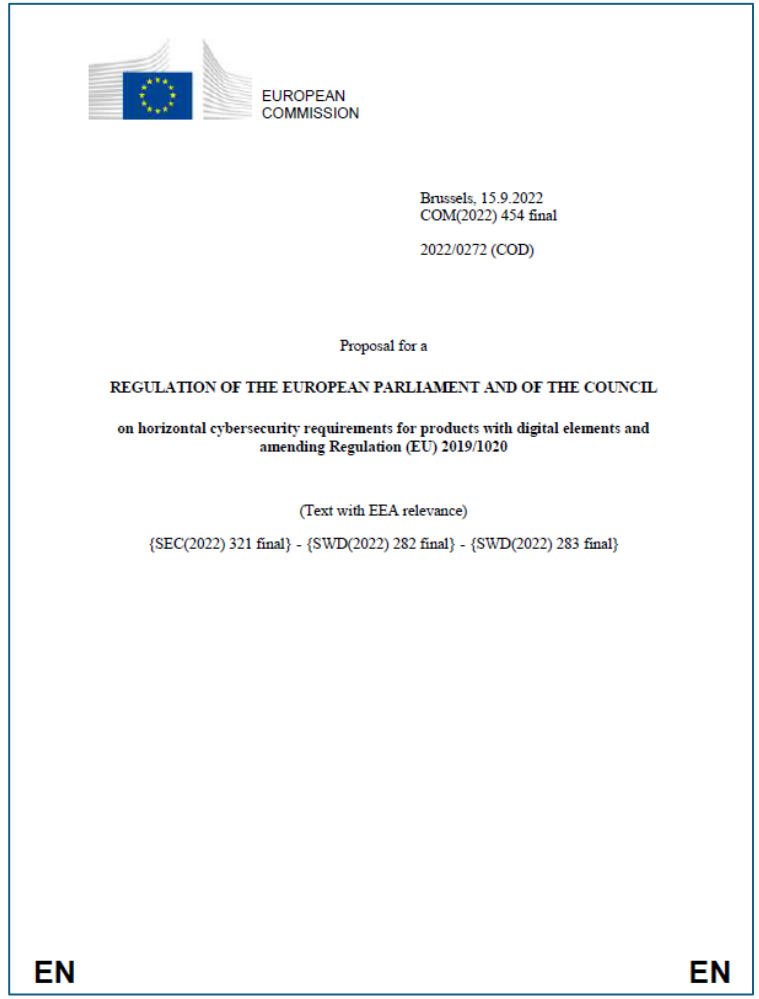
1. **Trend: digital and fully-networked solutions** (HW, SW, cloud solutions, remote access,…)
2. **Enforced reporting: current and upcoming legal requirements** (CRA, NIS 2,...)
3. **Risk assessment and evaluation: manual efforts vs automation** (information retrieval, assets, evaluation, assessment,...)



Year	# of CVEs
2010	4,639
2011	4,150
2012	5,288
2013	5,142
2014	7,948
2015	6,494
2016	6,457
2017	14,645
2018	16,512
2019	17,308
2020	18,375
2021	20,161
2022	25,059
2023	28,961
2024	40,077
2025	48,244

Cyber Resilience Act (CRA)

- CRA regulates the **market access** in form of **horizontal European cybersecurity requiremens** for a broad range of **digital products and services**
- CRA as part of the New Legislative Framework **extends** the legislation from **safety** to **security**
- Includes requirements for products across the **whole life cycle**



EUROPEAN
COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

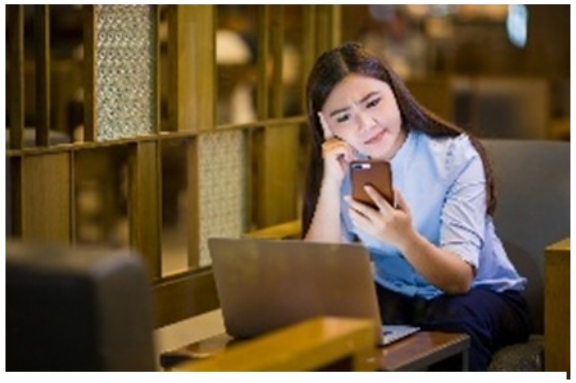
(Text with EEA relevance)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

EN EN

TROOPERS

Products with Digital Elements





What does the CRA demand?

Security requirements relating to the properties of products with digital elements

- **Security-by-design, Security-by-default**
- protection from unauthorised access; protection of confidentiality and integrety of data
- designed, developed and produced to limit attack surfaces […]

Vulnerability handling

- **SBOM** at the very least of the top-level dependencies of the product;
- Address and **remediate vulnerabilities without delay**, including by providing security updates
- Public disclose of information about fixed vulnerabilities, information allowing users to identify the product […]

Minimum information for the user

- Contact information where cybersecurity vulnerabilities of the product can be reported and received
- Identification of product, **intended use**
- Possibility to asses conformity information and if made available SBOM […]

Obligations of manufacturers during the product‘s lifecycle

Assessment of the risks associated with a product

1. **Product-related** essential requirements (Annex I, Section 1)
2. **Vulnerabilty handling** essential requirements (Annex I, Section 2)
3. **Technical documentation, including information and instructions** for use (Annex V + II)

Conformity assessment, CE marking, EU Declaration of Conformity (Annex V + VIII)

Continued compliance with **vulnerability handling** essential requirements throughout the products‘ life time (Annex I, Section 2))

Reporting obligations (Article 14)
1. **Activly Exploited vulnerabilities**
2. **Severe Incidents** having an impact on the security of the product

Reporting obligations to continue

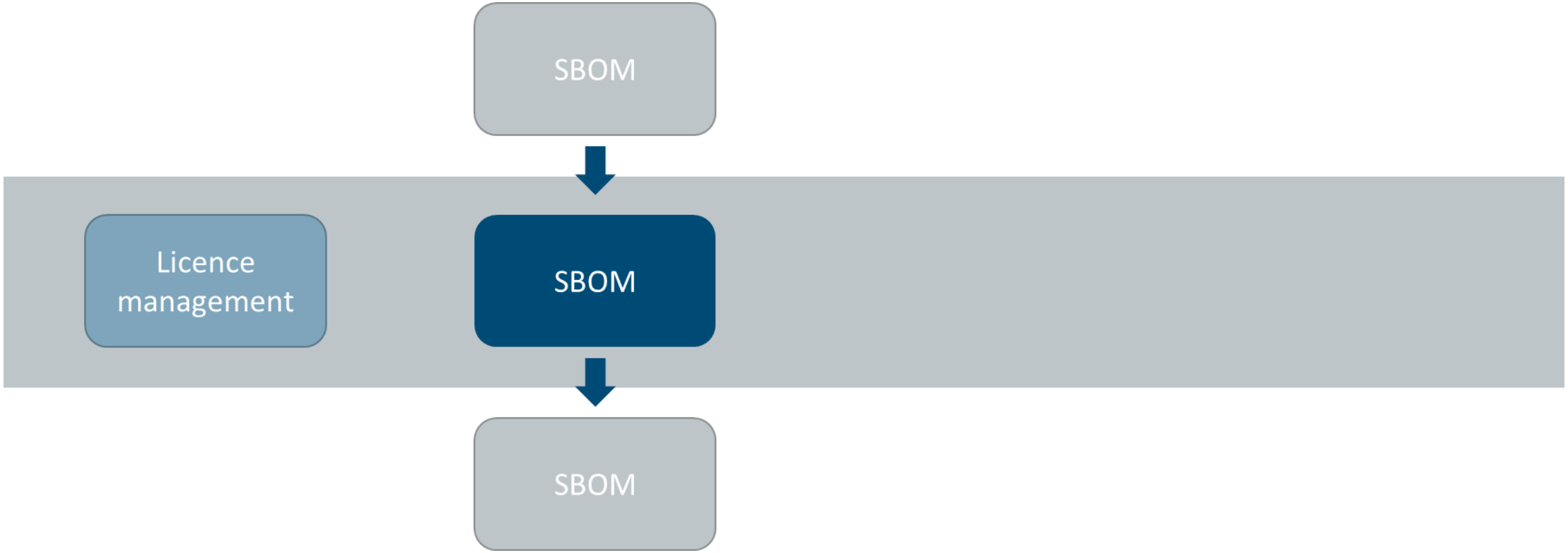
Why is SBOM becoming more relevant?

- Executive Order 14028
  - SBOM required for software procured by the US government
- Cyber Resilience Act (CRA) of the EU:
  - applies to (almost) all “products with digital elements”
  - extends the requirements of the CE Mark from safety to security
  - applicable from presumably 2027
  - Requirements:
    - secure by design, secure by default,
    - vulnerability management,
    - security updates throughout product‘s lifetime, …
    - SBOM

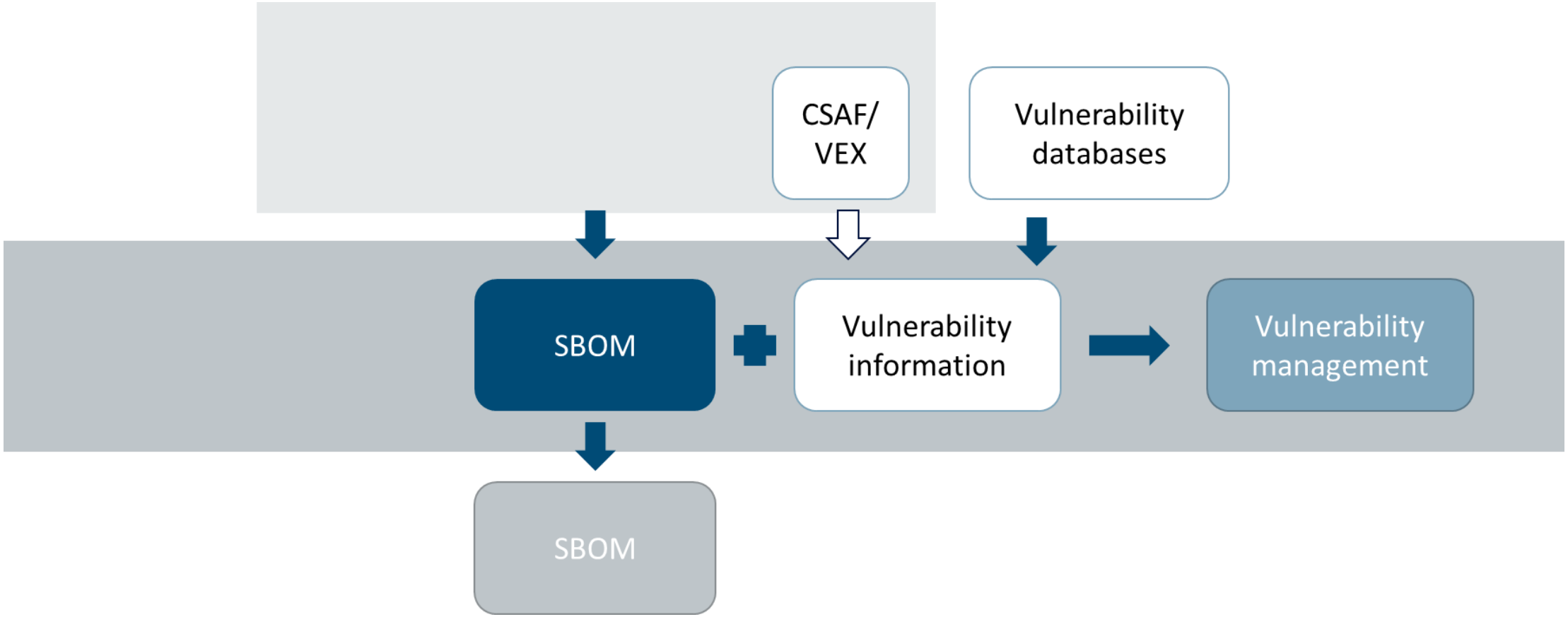
SBOM as part of CRA requirements

- Creating an SBOM *in a commonly used and machine-readable format* to identify and document vulnerabilities is required
  - *covering at least the top-level dependencies of the products*
- The Commission can specify the format and elements of an SBOM
- SBOM must be provided to market surveillance upon reasoned request to verify conformity with the essential requirements
  - SBOM has to be maintained and used internally for vulnerability management
  - SBOM does not have to be published

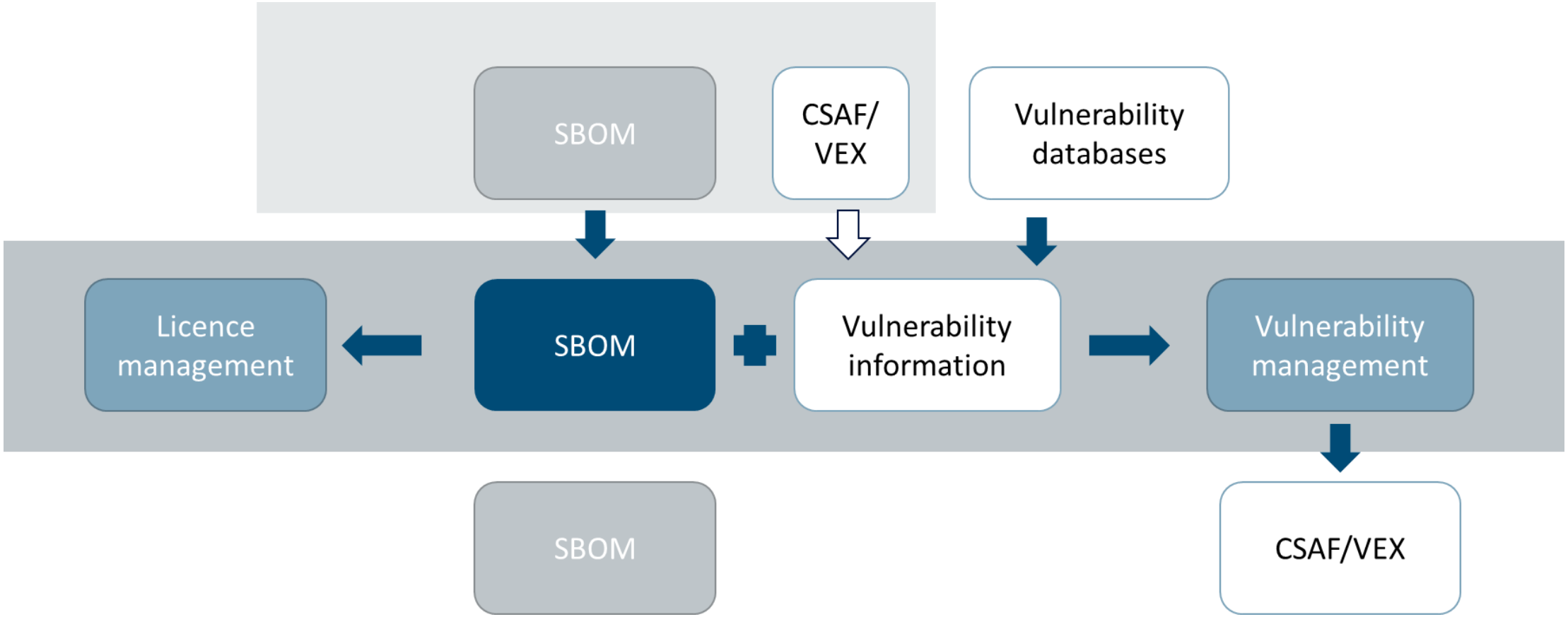
How to get more out of an SBOM?



How to get more out of an SBOM?



How to get more out of an SBOM?



Fostering a useful and well working SBOM ecosystem

BSI TR-03183-2 fills the gap between high-level requirements (e.g. aforementioned by the EU, CISA's SBOM minimum elements) and the base specifications (CycloneDX and SPDX).

- Specifies field values more concisely.
- Demands more information, e.g.
  - Delivery item SBOM
  - Etc.
- Unfortunately this makes generating TR-compliant SBOMs at other points than the build process hard.
- https://www.bsi.bund.de/dok/TR-03183

SBOMs in national IT-procurement (EVB-IT)

- The EVB-IT contract templates published in spring 2026 offer a checkbox for delivering an SBOM with every software update.

- Side notes:
  - More security related requirements and options are becoming implemented for the next EVB-IT release.
  - E.g. vulnerability information needed by institutions which must comply with the NIS2 regulation.

Security Advisory - typical information

1 Release Info

- Published date
- Last updated

2 Publisher / Source

- Publisher
- Source / advisory link

3 Affected Products

- Product + version ranges
- Affected platforms

4 Vulnerability Details

- CVE / ID (if present)
- Short description

5 Risk / Severity

- CVSS (if present)
- Severity level

6 Impact / Affected Status

- CIA impacts
- Affected status

7 Mitigations / Workarounds

- Workarounds
- Mitigations

8 Fix Information

- Fixed in version(s)
- Patch availability

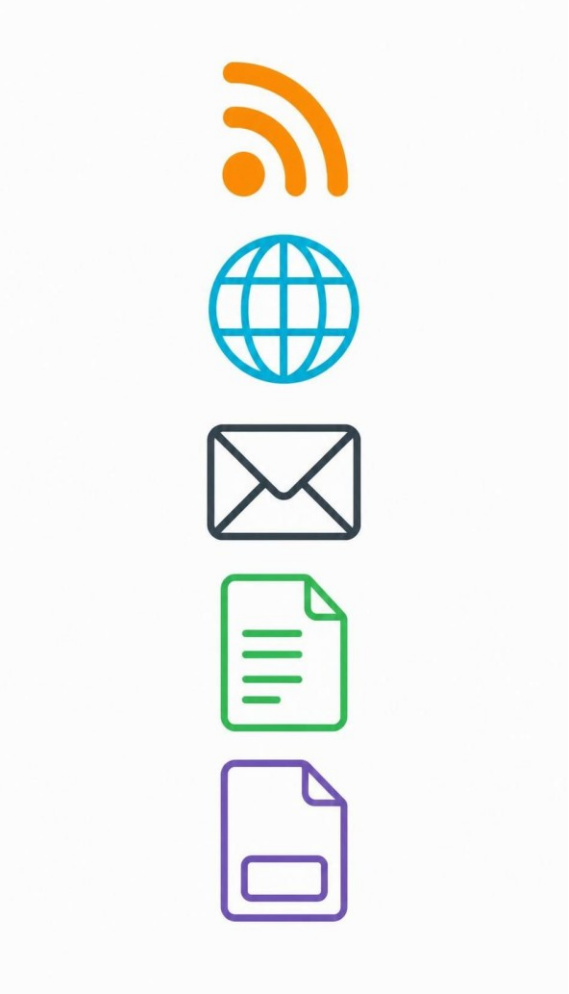
9 Credits / Coordination

- Reported by / credits
- Coordination

A plethora of channels, formats, and content

How do you retrieve relevant security information?

- **Various sources** (vendors, agencies,...)
- **Different means of transmission** (email, feed, webpage,...)
- **Several formats** (.pdf, .txt,...)
- **Manual effort** (content, asset inventory, infrastructure,…)
- **Risk assessment** (criticality, affected vs not affected,...)



→ Need for Standardization and Automation!

CSAF – Common Security Advisory Framework

CSAF 2.0: 2022 internat. Standard OASIS Foundation, 2025 ISO/IEC 20153:2025

- **Machine readable** format for Security Advisories (JSON)
- **Open Source** (OS) and OS Tools available
- **Standardized** format and standardized dissemination of information
- **Automatable** retrieval und comparison, **scalability**
- Information about **relevant security updates and measures**
- Different profiles, e.g. **VEX** and **simplified risk management**
- Many (big) **companies provide CSAF**
- **CSAF 2.1** is to be at the ready

Let‘s VEXinate your vulnerability management

VEX (Vulnerability Exploitability eXchange) is a profile in CSAF

A vulnerability is discovered… Are you infected… uhm, sorry affected?

4 Status in VEX:

- /vulnerabilities[]/product_status/**fixed**
- /vulnerabilities[]/product_status/**known_affected (+ action statement)**
- /vulnerabilities[]/product_status/**known_not_affected (+ impact statement)**
- vulnerabilities[]/product_status/**under_investigation**

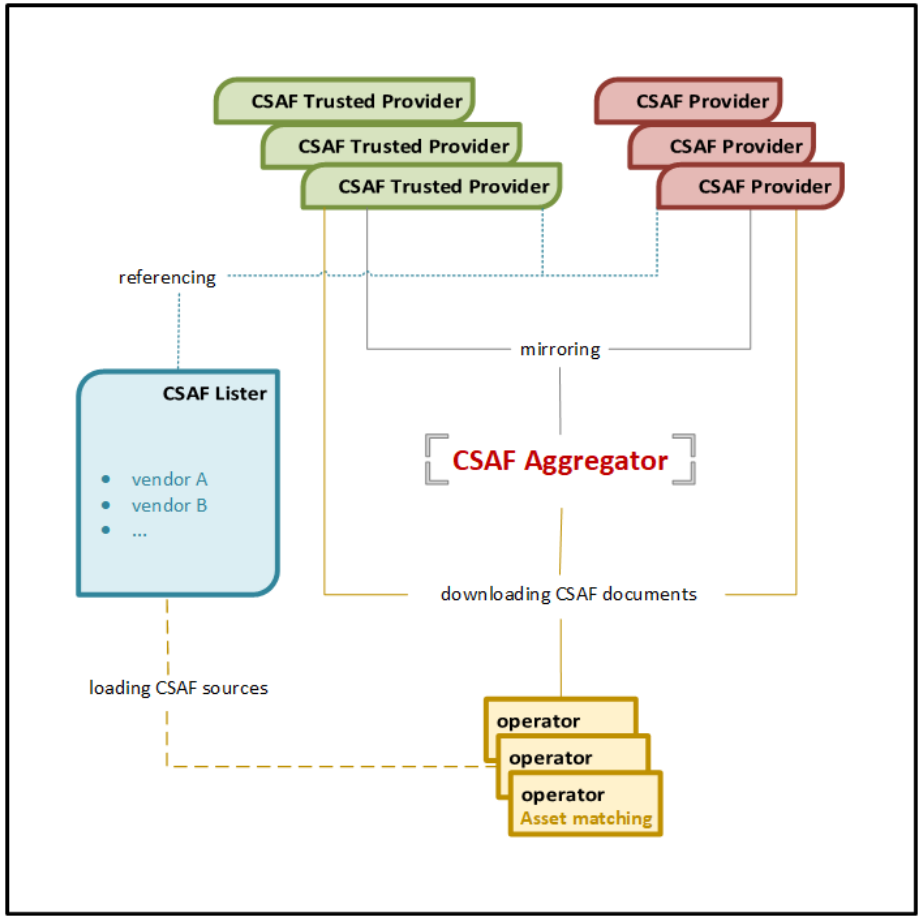
The CSAFversum in a nutshell

How different tools build up a functional ecosystem

- **Interaction** between various (OS) tools
- Do you care for your **Asset Management?**
- Do you have a standardized contact **(security.txt)**?
- Can you **provide** CSAF documents?
- Do you know the CSAF **Aggregator** & CSAF Lister @ BSI?
- Are you aware of the **CSAF Technical Guideline** BSI TR-03191?
- Do you need **compliance** with CRA (vulnerability management)?

https://www.bsi.bund.de/dok/en_csaf

https://www.csaf.io/



TROOPERS

Thank you for your attention!

We hope you enjoyed our little presentation, which will be followed by:

1. A short demonstration.
2. A Q&A round, focussing on the presentation and demonstration.
3. A open discussion on the presented and related topics.