# Problematik

ANGRIFF VIA OPENSSH

## Backdoor in XZ Utils gefährdet das Linux-Ökosystem

Zum Glück wurde die Backdoor entdeckt, bevor sie die breite Masse erreichen konnte. Angreifer hätten damit weltweit Millionen von Linux-Systemen infiltrieren können.

golem.de

## «Das ist der verrückteste Angriff»: Ein Programmierer entdeckt per Zufall eine gefährliche Hintertüre im Code – wohl von einem Geheimdienst

nzz.ch

## Aktenzeichen XZ ungelöst

In den vergangenen Tagen sind wir mit sehr viel Glück dem wohl größten Fias in der Geschichte des Internets gerade so entgangen. Wie konnte das passieren?

heise.de

ZDNet / Alerts

## XZ Utils-Vorfall: Open Source als Software Supply Chain-Falle

Ende März wurde in der XZ Utils Bibliothek, ein Kernbestandteil vieler Linux Distributionen, Schadcode entdeckt.

zdnet.de

Veröffentlicht am 03. März 2025

## Digitale Souveränität als Staatsaufgabe – Wie Abhängigkeiten unsere Demokratie gefährden

- Handelsblatt -

DIGITALE SOUVERÄNITÄT

## „Trump wird jede offene Flanke ausnutzen“

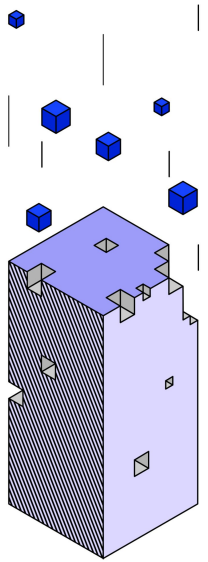
Deutschlands Verwaltungen sind von US-amerikanischen Tech-Anbietern abhängig. Es sei nur eine Frage der Zeit, bis die neue US-Regierung dies als Druckmittel nutzen wird, meint die

- Tagesspiegel Background -

# Problematik

“Die wachsende Komplexität moderner Softwarelieferketten und die Vielzahl digitaler Projekte in der öffentlichen Verwaltung machen nicht nachnutzbare und vollständig **manuelle Sicherheitsprüfungen zunehmend unpraktikabel** bis unmöglich.” (ZenDiS Strategiepapier SSDLC)

**Public Money Public Code** →
Bewertung von im Auftrag für die ÖV entwickelter Software

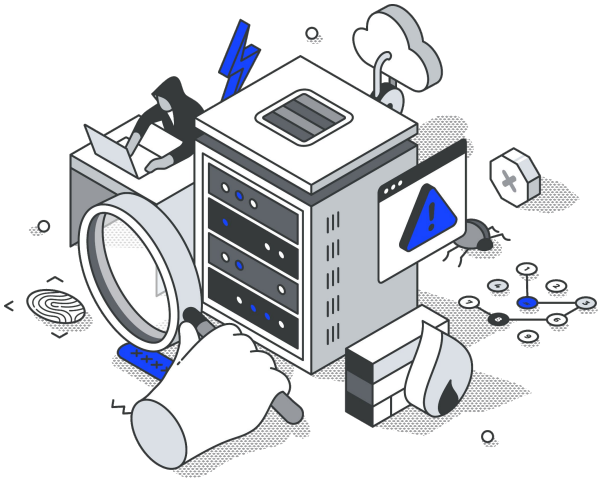


# Problematik

Was ist aus Ihrer Sicht der größte Nachteil, der gegen den Einsatz von OSS in Ihrer Organisation/ Ihrem Unternehmen spricht?

**→ 21 % der ÖV-Organisationen geben Sicherheitsaspekte als größten Vorbehalt an**

(Bitkom Open Source Monitor 2023)



# Was ist die Software-Supply-Chain?

> Eine Software-Lieferkette besteht aus den Komponenten, Bibliotheken, Tools und Prozessen, die zur Entwicklung, Erstellung und Veröffentlichung eines Software-Artefakts verwendet werden.

[4] übersetzt

# Die Softwarelieferkette nach “Supply Chain Levels for Software Artifacts (SLSA)”

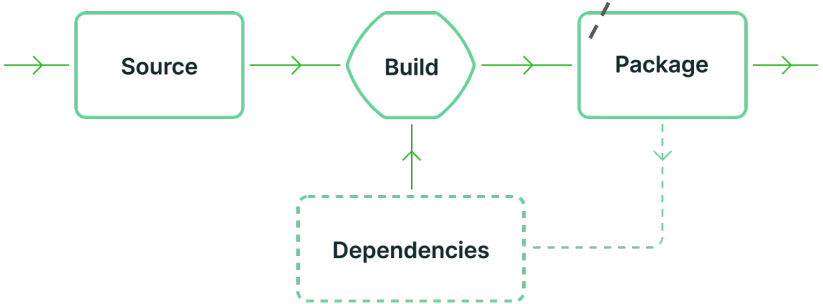
**Lieferant**

ein Unternehmen, das eine Software, Softwarekomponenten oder Softwarebibliotheken an ein anderes Unternehmen liefert.

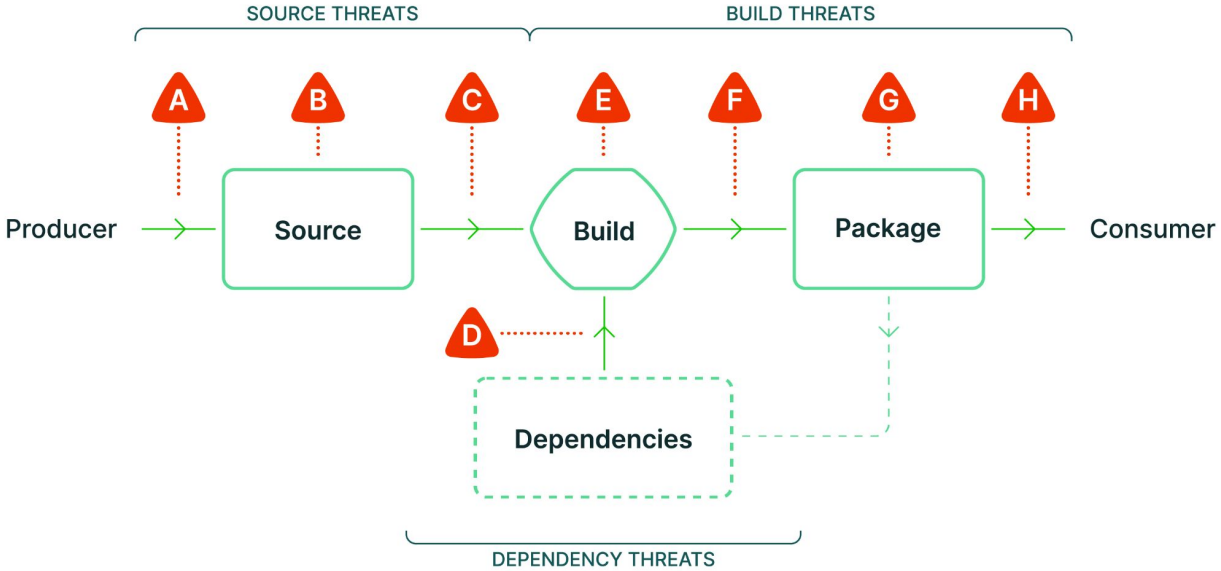
**Kunde**

das Unternehmen, das die vom Anbieter produzierte Software konsumiert.

Endkonsument oder selbst wieder Software-Lieferant



# Threat-Modell der Software-Entwicklung selbst




SOURCE THREATS

A Submit unauthorized change

B Compromise source repo

C Build from modified source

DEPENDENCY THREATS

D Use compromised dependency

BUILD THREATS

E Compromise build process

F Upload modified package

G Compromise package registry

H Use compromised package

# Software Supply Chain Attack Definition

„Ein Angriff auf die Lieferkette ist eine Art von Cyberangriff, bei dem nicht die Organisationen direkt angegriffen werden, sondern die **dazwischenliegenden Parteien**, wie z. B. Anbieter und deren Softwarecode.“

[1] übersetzt

„[...] Angreifer manipulieren das Endprodukt eines bestimmten Anbieters so, [...], dass es **von den Endnutzern über vertrauenswürdige Vertriebskanäle**, z. B. Download- oder Update-Sites, bezogen werden kann.“

[2] übersetzt

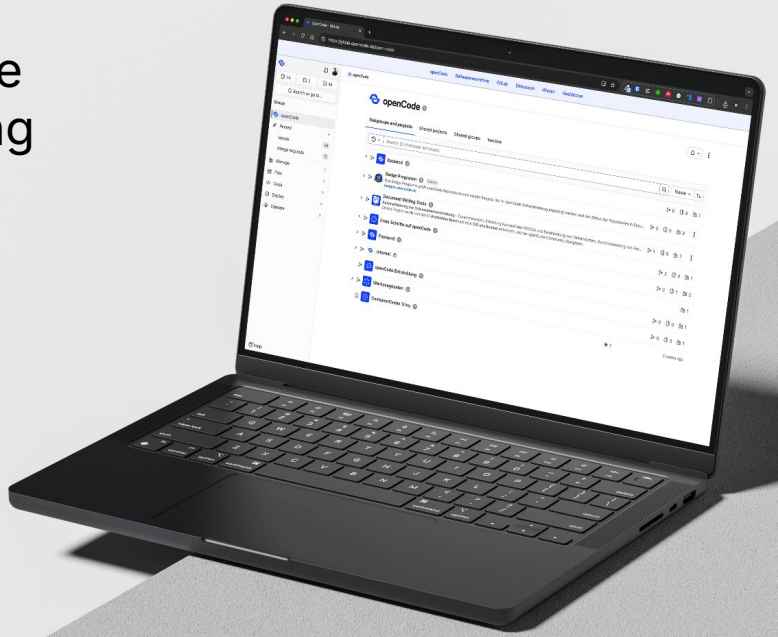
# Initiativen zur Absicherung von Software-Lieferketten aus der ÖV


# openCode

## Die Plattform für Digitale Souveränität & Open Source in der deutschen Verwaltung

openCode

Zentrum Digitale Souveränität




# Das Badge Programm

## Vertrauen in Open Source Software stärken

# Badge für aktive Wartung

## Stufe 1: Aktive Wartung

Das Projekt erfüllt die Mindestanforderungen für ein gewartetes Projekt. Es wird weiterentwickelt und auf Probleme wird schnell reagiert.

- Commits: Mindestens 5 Commits innerhalb der letzten 6 Monate
- Reaktionszeit auf Issues: Die durchschnittliche Reaktionszeit auf Issues, welche innerhalb der letzten 3 Monate entstanden sind, beträgt weniger als 7 Tage

## Level 2: Verlässliche Wartung

Das Projekt erfüllt die Anforderungen für ein zuverlässig gewartetes Projekt. Es werden regelmäßig neue Versionen veröffentlicht, auf Probleme wird schnell reagiert und es gibt eine aktive Community.

- Alle Kriterien des ersten Levels
- Releases: Mindestens 1 Veröffentlichung (Release oder Git-Tag) innerhalb der letzten 6 Monate.

## Level 3: Krisensichere Wartung

Das Projekt erfüllt die Anforderungen an ein krisensicher gewartetes Projekt. Es werden regelmäßig neue Versionen veröffentlicht, auf Probleme wird schnell reagiert und es gibt eine breite und aktive Community.

- Alle Kriterien der Levels 1 und 2
- Contributor Absence Factor: Mehrere Maintainer (Einzelpersonen) tragen aktiv zum Projekt bei. Das Projekt hat im Betrachtungszeitraum von 6 Monaten einen Contributor Absence Factor von mindestens 2.

# Nachnutzungs Badge

## Level 1: Bereit zur Nutzung

Das Projekt erfüllt die Anforderungen für eine spätere Verwendung. Pakete werden für die weitere Verwendung bereitgestellt.

- Pakete: In den letzten 6 Monaten wurde mindestens ein Paket veröffentlicht
- CI-Pipelines: In den letzten 6 Monaten gab es mindestens eine erfolgreiche CI-Pipeline

## Level 2: Aktiv genutzt

Das Projekt wird von mindestens einer Organisation produktiv genutzt.

- Nachnutzung: Mindestens eine Organisation nutzt das Projekt aktiv

## Level 3: Häufig aktiv genutzt

Das Projekt wird von mindestens 10 Organisationen produktiv genutzt.

- Alle Kriterien des Level 2
- Nachnutzung: Mindestens 10 Organisationen nutzen das Projekt aktiv



# Open-Source-Lizenz Badge

# Badge für Sicherheit

## Level 1: Basis Sicherheit

- Reaktionszeit auf Issues: Die durchschnittliche Reaktionszeit auf Issues, welche innerhalb der letzten 3 Monate entstanden sind, beträgt weniger als 7 Tage.
- Geschützte Branches: Der default Branch ist als `protected` konfiguriert und es sind keine Force-Pushes auf den default Branch erlaubt.
- Sicherheitsrichtlinie: Prüft, ob eine Datei `SECURITY.md` im Stammverzeichnis des Default-Branches existiert

## Level 2: Erweiterte Sicherheit

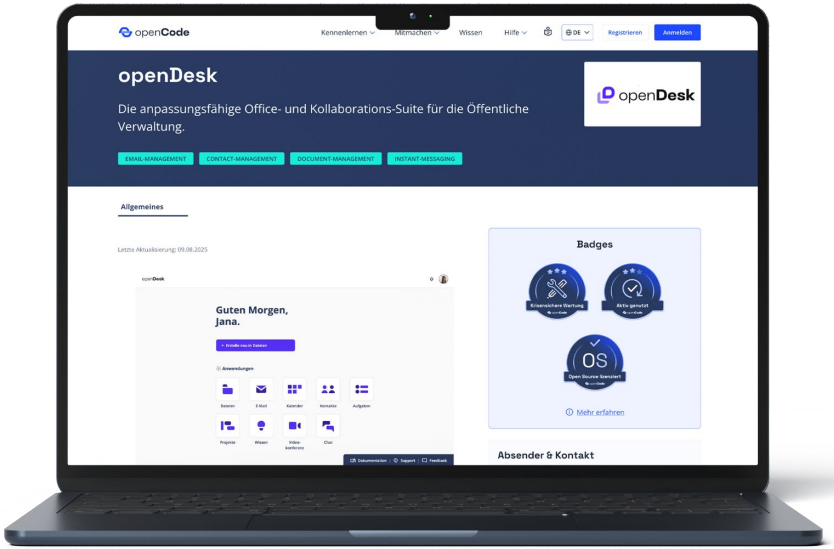
- Alle Kriterien aus Level 1
- Code Review: Prüft, ob mind. 75% der Merge Requeste in den letzten 6 Monaten durch einen Maintainer geprüft wurden.
- Signierte Tags: Prüft, ob mind. 80% der Tags der letzten 6 Monate signiert wurden

## Level 3: Umfassende Sicherheit

- Alle Kriterien der Level 1 und 2
- Letzte Releases ohne bekannte kritische Schwachstellen: TBD
- Schwachstellenmanagement - Behebungszeit von CVEs: TBD

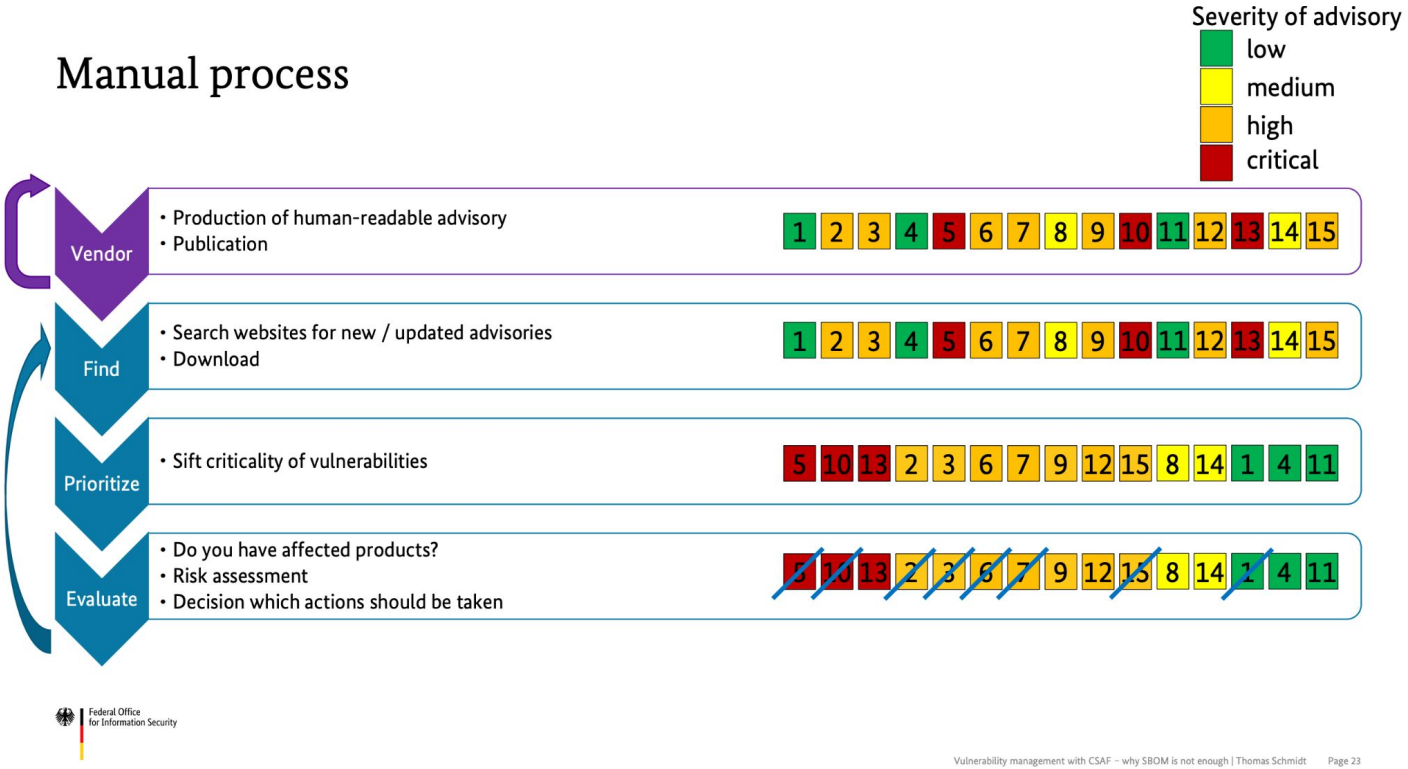


# Darstellung im Softwareverzeichnis




**Vertrauen & Verlässlichkeit**
bei der Beschaffung von
Open-Source-Software

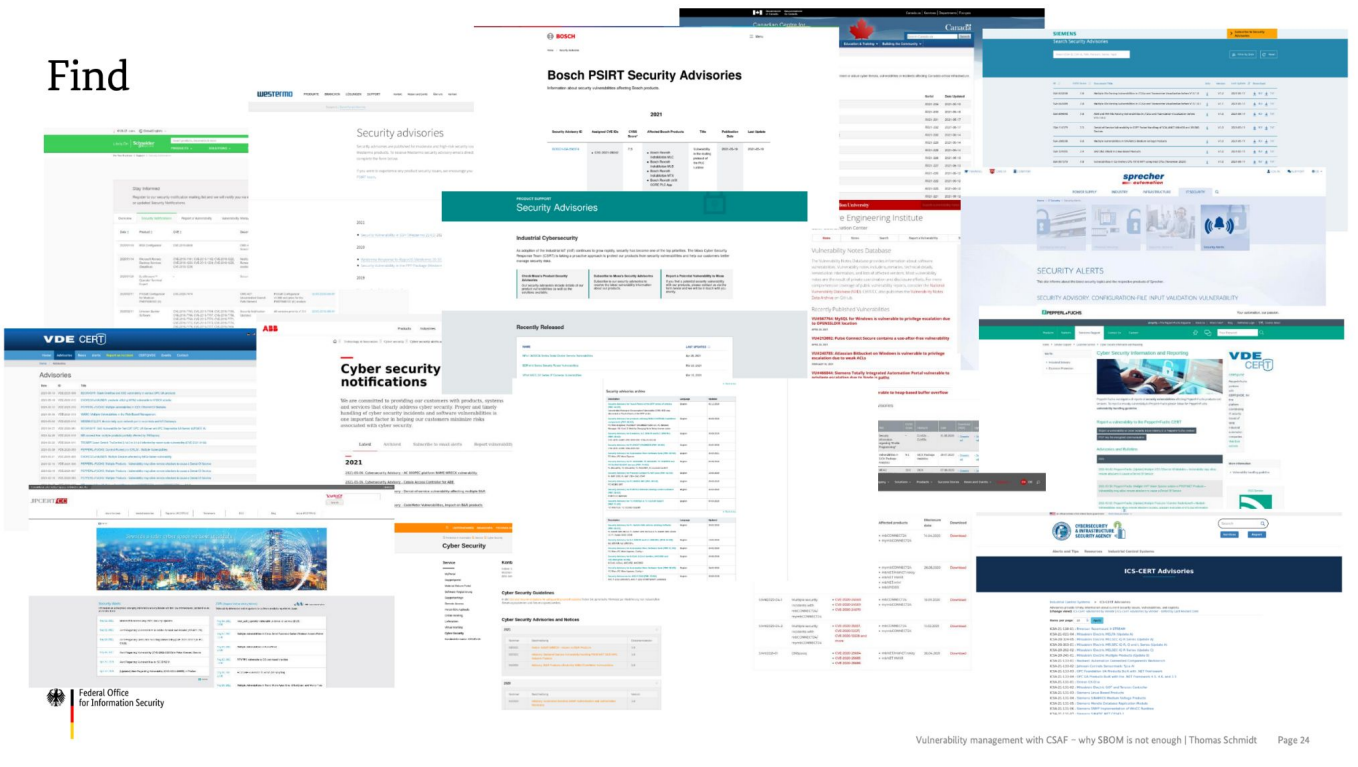
# CSAF & VEX






Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt (BSI) | Abgerufen am 12.08.25 | owasp.org/www-chapter-frankfurt/assets/slides/58_OWASP_Frankfurt_Stammtisch_1.pdf

# CSAF & VEX



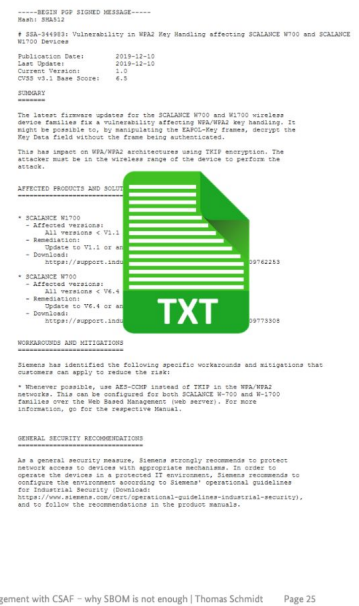



Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt (BSI) | Abgerufen am 12.08.25 | owasp.org/www-chapter-frankfurt/assets/slides/58_OWASP_Frankfurt_Stammtisch_1.pdf

# CSAF & VEX

## Analyze



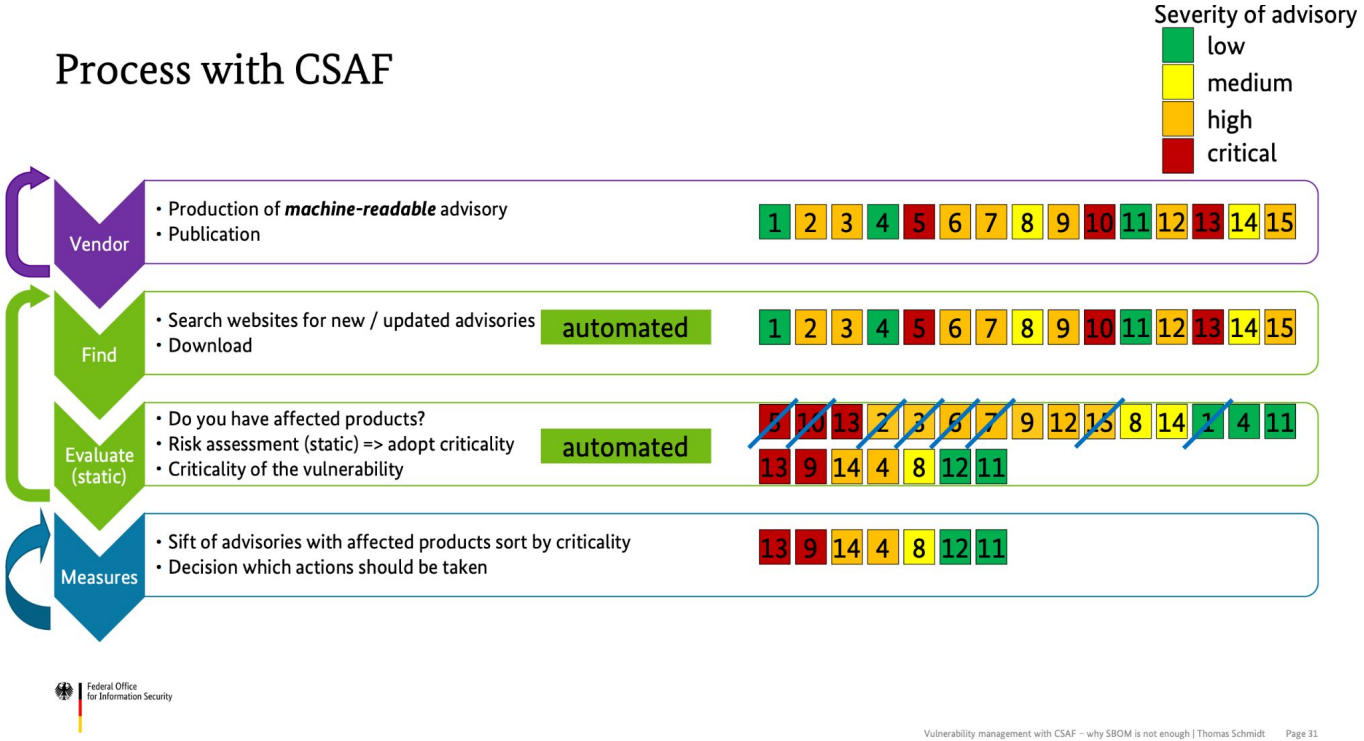







Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt (BSI) | Abgerufen am 12.08.25 | owasp.org/www-chapter-frankfurt/assets/slides/58_OWASP_Frankfurt_Stammtisch_1.pdf

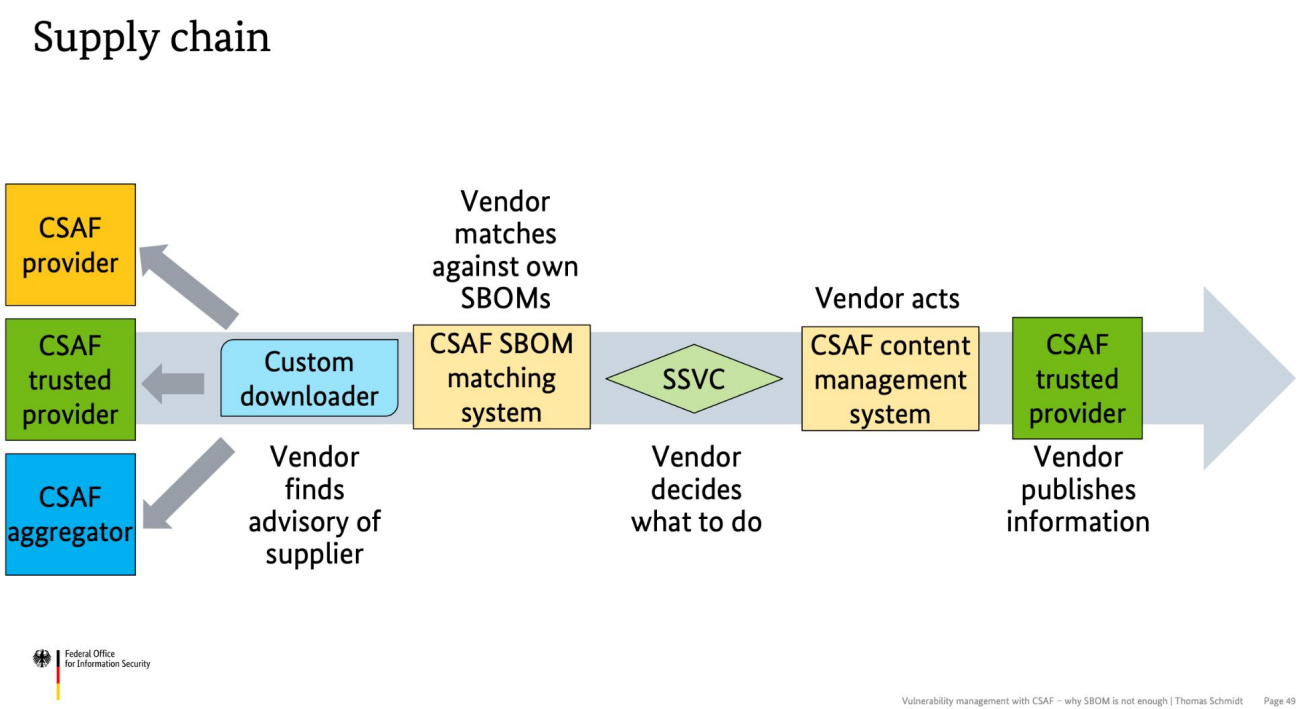
# CSAF & VEX






Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt (BSI) | Abgerufen am 12.08.25 | owasp.org/www-chapter-frankfurt/assets/slides/58_OWASP_Frankfurt_Stammtisch_1.pdf

# CSAF & VEX






Vulnerability management with CSAF – why SBOM is not enough | Thomas Schmidt (BSI) | Abgerufen am 12.08.25 | owasp.org/www-chapter-frankfurt/assets/slides/58_OWASP_Frankfurt_Stammtisch_1.pdf

# CSAF & VEX

Das **Common Security Advisory Framework (CSAF)** ist ein standardisiertes und quelloffenes Framework zur Kommunikation und automatisierbaren Verteilung von maschinenverarbeitbaren Schwachstellen- und Mitigationsinformationen, so genannten Security Advisories

**Vulnerability Exploitability eXchange (VEX, CASF Profil)** ist ein standardisiertes Format, das verwendet wird, um Informationen über die Ausnutzbarkeit von Schwachstellen in Softwareprodukten zu übermitteln und auszutauschen.

Bundesamt für Sicherheit in der Informationstechnik

L3montree [Lemontree]
Cybersecurity

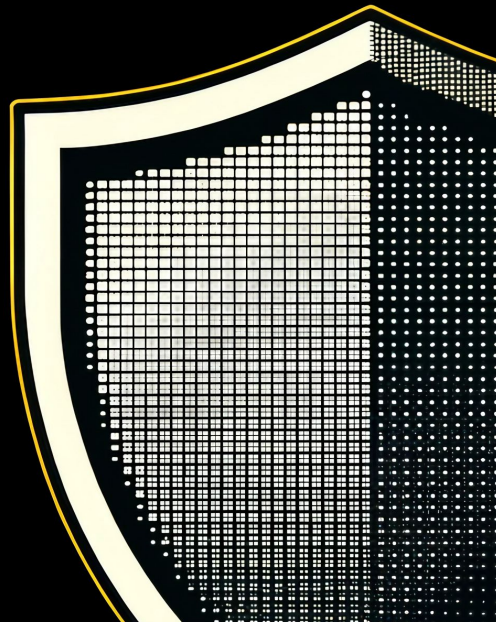
# Securing your Software & Cloud-Native Environment


Email: info@l3montree.com

Telefon: +49 (0)228 92998568
+49 177 7438521

Adresse: Markt 3
53111 Bonn


**LinkedIn L3montree**



# Quellen

[1] GeeksforGeeks. (2023). *Evolution of Software Development | History, Phases and Future Trends*. [online] Available at: https://www.geeksforgeeks.org/evolution-of-software-development-history-phases-and-future-trends/.

[2] Intelligence, G.T. (2020). Cybersecurity: Timeline. [online] Verdict. Available at: https://www.verdict.co.uk/cybersecurity-timeline

[3] Bundesamt für Sicherheit in der Informationstechnik. (n.d.). Die Lage der IT-Sicherheit in Deutschland. [online] Available at: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html.

[4] "For Good Measure Counting Broken Links: A Quant's View of Software Supply Chain Security" (PDF). USENIX ;login. Retrieved 2022-07-04.

[5] Wintergerst, R. and Berlin, B.-P. (2023). Wirtschaftsschutz 2023. [online] Available at: https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf.

[6] owasp.org. (n.d.). OWASP DevSecOps Guideline | OWASP Foundation. [online] Available at: https://owasp.org/www-project-devsecops-guideline/.

[7] Supply-chain levels for software artifacts. (n.d.-b). SLSA. https://slsa.dev/

[8] Supply chain compromise, Technique T1195 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/techniques/T1195/

[9] Bedrohungen der Softwarelieferkette. (n.d.). Google Cloud. https://cloud.google.com/software-supply-chain-security/docs/attack-vectors

[10] Sonatype Inc. (n.d.). 2020 Software Supply Chain Report | Download. https://www.sonatype.com/resources/white-paper-state-of-the-software-supply-chain-2020

[11] www.threatmodelingmanifesto.org. (n.d.). Threat Modeling Manifesto. [online] Available at: https://www.threatmodelingmanifesto.org/.

[12] ReversingLabs: The state of Software Supply Chain Security 2024