Das CSAFversum

Und wie sie damit ihre Schwachstellen und Sicherheitspatches in den Griff bekommen

Bundesamt
für Sicherheit in der
Informationstechnik

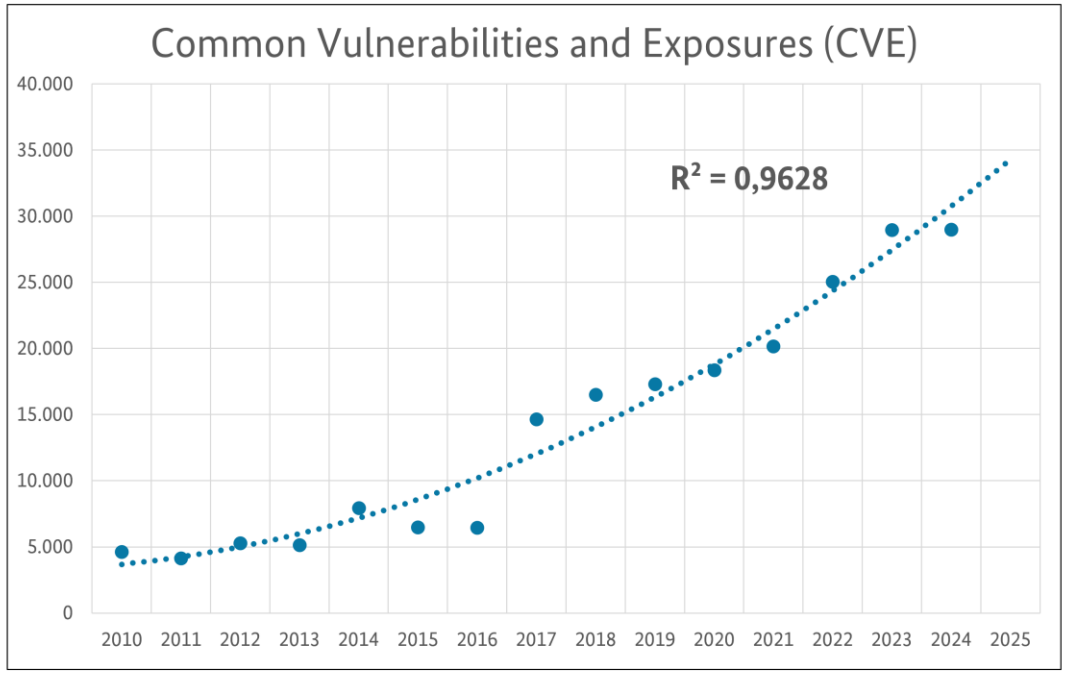
Wir haben eine Schwachstelle entdeckt!

Option A

Option B

Schwachstellenfund – na und?

Wie viele gemeldete Schwachstellen erwarten wir in den nächsten Jahren?



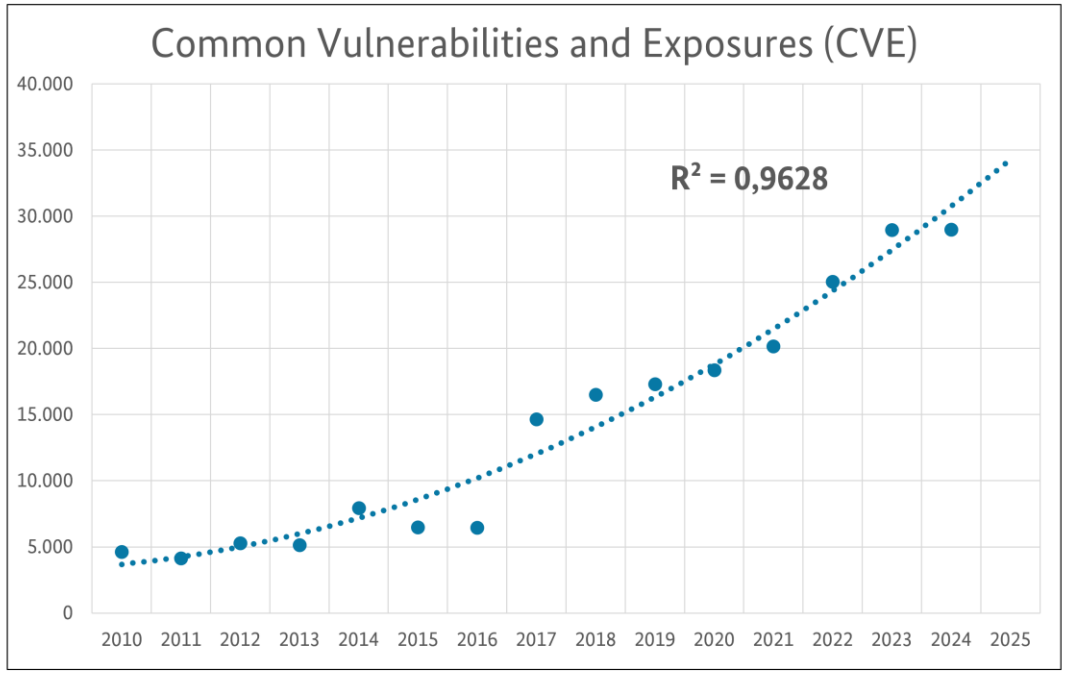
Jahr	Anzahl der CVE
2010	4.639
2011	4.150
2012	5.288
2013	5.142
2014	7.948
2015	6.494
2016	6.457
2017	14.645
2018	16.512
2019	17.308
2020	18.375
2021	20.161
2022	25.059
2023	28.961
2024	29.004

Datenquelle: https://cve.mitre.org

Schwachstellenfund – na und?

Wie viele gemeldete Schwachstellen erwarten wir in den nächsten Jahren?

1. **Anzahl sicherheitsrelevanter Schwachstellen steigt**
2. **Gesetzliche Vorgaben** (BSIG, CRA, NIS 2, etc.)
3. **Schwachsellenmanagement vs manuelle Aufwände** (Abgleich mit den eigenen Systemen und der eigenen Infrastruktur, Bewertung von Kritikalität, Betroffenheit, etc.)



Jahr	Anzahl der CVE
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	29.004

Datenquelle: https://cve.mitre.org

Sicherheitsinformationen in Form von Security Advisories

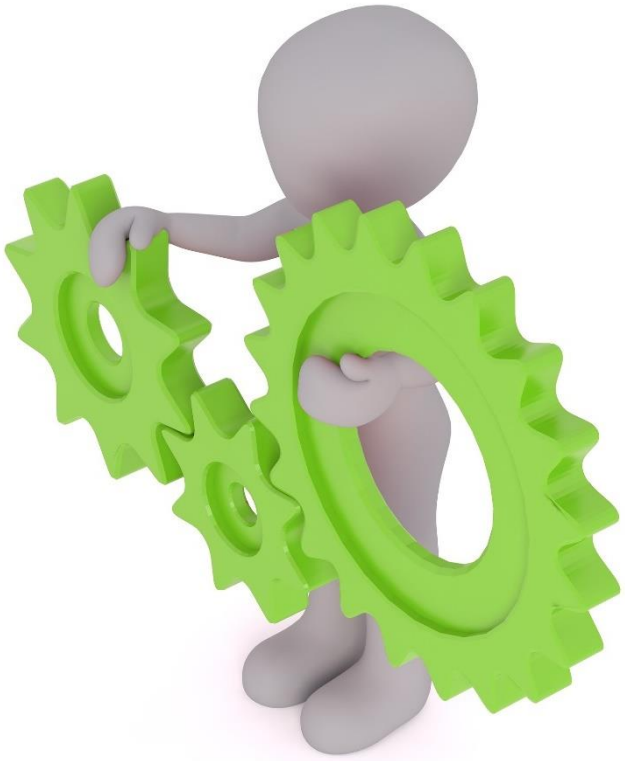
Woher bekomme ich meine Informationen?

- **Viele Quellen** (Hersteller, Behörde, etc.)
- **Unterschiedliche Übertragungswege** (Mail, Feed, Webseite, etc.)
- **Diverse Formate** (.pdf, .txt, etc.)

Was sollten Betreiber tun?

Patchen und updaten!

Mögliche Lösungen



CSAF – Common Security Advisory Framework

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

CSAF – Common Security Advisory Framework

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

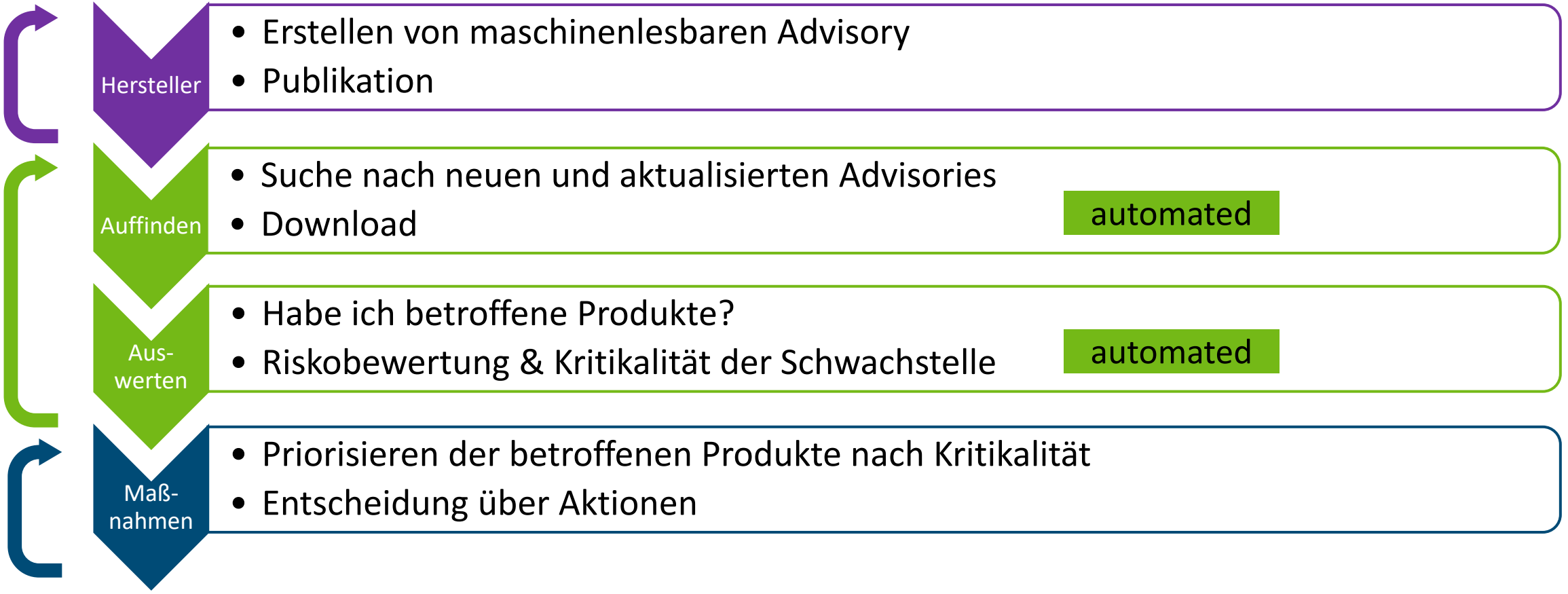
- **Maschinenlesbares, herstellerunabhängiges** Format für Security Advisories (JSON)
- **Open Source** (OS) und OS Tools verfügbar
- **Standardisiertes** Format und standardisierte Verteilung der Information
- **Automatisierbarer** Publikations-, Verteil- und Abrufmechanismus
- Benachrichtigungen über **verfügbare Sicherheitsupdates und Inhalte**

Welche Vorteile bietet die Nutzung von CSAF?

Automatisierbares Schwachstellenmanagement

- **Verarbeiten der Security-Advisories ist automatisierbar**
  - Weniger manueller Aufwand für das Bewerten, mehr Zeit für das Beheben der Schwachstellen
  - Vereinfachtes Risikomanagement
  - Betroffenheit einzelner Produkte direkt feststellbar (VEX ist Profil in CSAF)
- **Bessere Skalierbarkeit**
  - Steigende Anzahl von Security Advisories erzeugt aufgrund der Automatisierung keinen personellen Mehraufwand

Prozess mit CSAF



Welche Vorteile bietet die Nutzung von CSAF?

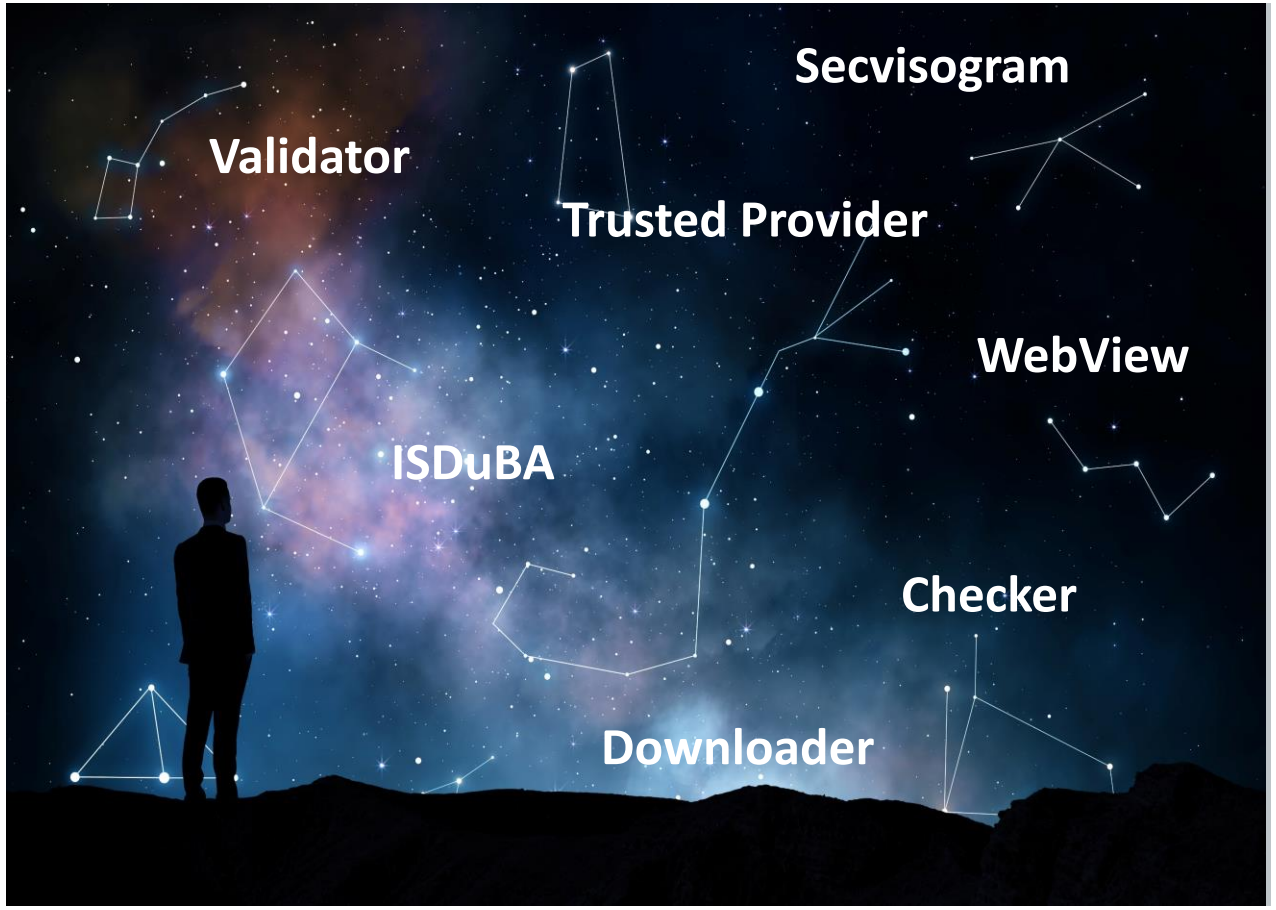
Automatisierbares Schwachstellenmanagement

- **Verarbeiten der Security-Advisories ist automatisierbar**
  - Weniger manueller Aufwand für das Bewerten, mehr Zeit für das Beheben der Schwachstellen
  - Vereinfachtes Risikomanagement
  - Betroffenheit einzelner Produkte direkt feststellbar (VEX ist Profil in CSAF)
- **Bessere Skalierbarkeit**
  - Steigende Anzahl von Security Advisories erzeugt aufgrund der Automatisierung keinen personellen Mehraufwand
- **Kostengünstig (CSAF und die entwickelten Tools sind Open Source)**
  - BSI stellt Open-Source-Werkzeuge zur Verfügung
- **Akzeptanz und Adaption steigt**
  - CSAF 2.0 ist ISO-Standard (ISO 20153), CSAF 2.1 steht in den Startlöchern
  - Neue Tools, Community entwickelt mit und weiter
  - Große Unternehmen wie Siemens, Microsoft oder Red Hat veröffentlichen bereits CSAF-Dokumente

Das CSAFversum expandiert

Werkzeuge für Hersteller

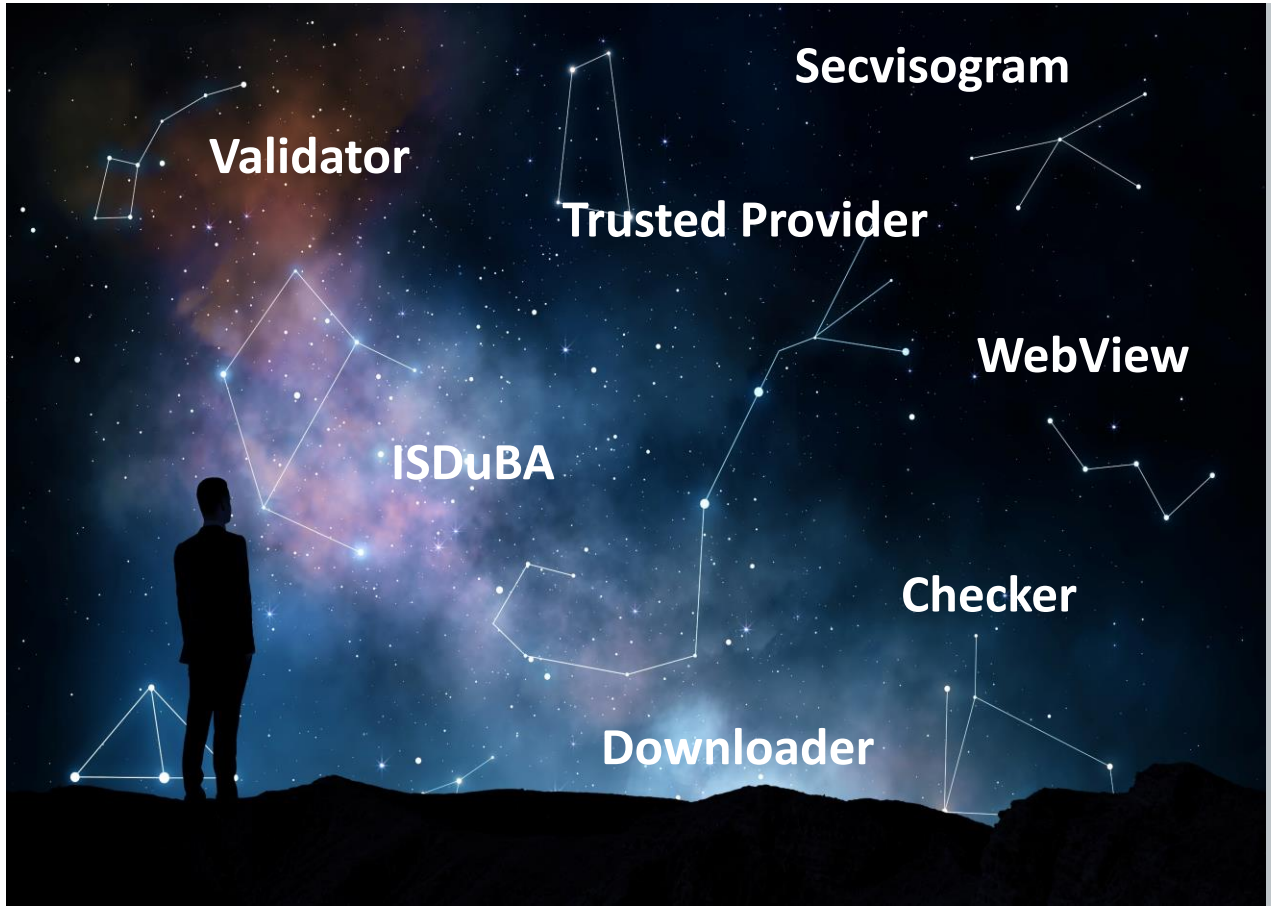
- Secvisogram & Sec-O-Simple
  - Erstellen von CSAF-Dokumenten
  - Einmal schreiben in alle Formate exportieren (json, pdf, html, ….)
- TrustedProvider
  - Werkzeug zum Erzeugen der Datenstrukturen für den Webserver, um CSAF-Daten bereitzustellen
- CSAF-Checker
  - Prüfen der Infrastruktur auf Konformität zum Standard



Das CSAFversum expandiert

Betreiber

- CSAF Downloader
  - Um CSAF Dokumente herunterzuladen
- ISDuBA
  - Zum Sammeln und Bewerten von Security-Advisories



Bundesamt
für Sicherheit in der
Informationstechnik

Beteiligen Sie sich am wachsenden CSAFversum

https://csaf.io/

CSAF TC GitHub: https://github.com/oasis-tcs/csaf

CSAF producer: https://github.com/secvisogram/secvisogram

CSAF full validator: https://github.com/secvisogram/csaf-validator-service

CSAF trusted provider: https://github.com/csaf-poc/csaf_distribution

CSAF aggregator: https://github.com/csaf-poc/csaf_distribution

Provider checker: https://github.com/csaf-poc/csaf_distribution

CSAF downloader: https://github.com/csaf-poc/csaf_distribution

CSAF webview: https://github.com/csaf-poc/csaf_webview

Download and evaluation of CSAF documents: https://github.com/ISDuBA/ISDuBA/

Jens Kluge

Jens.Kluge@bsi.bund.de
csaf@bsi.bund.de
+49 (0) 228 99 9582 5938
https://bsi.bund.de/csaf

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us: