CSAF (Common Security Advisory Framework)

ein Standard, der das Schwachstellenmanagement revolutioniert

Bundesamt
für Sicherheit in der
Informationstechnik

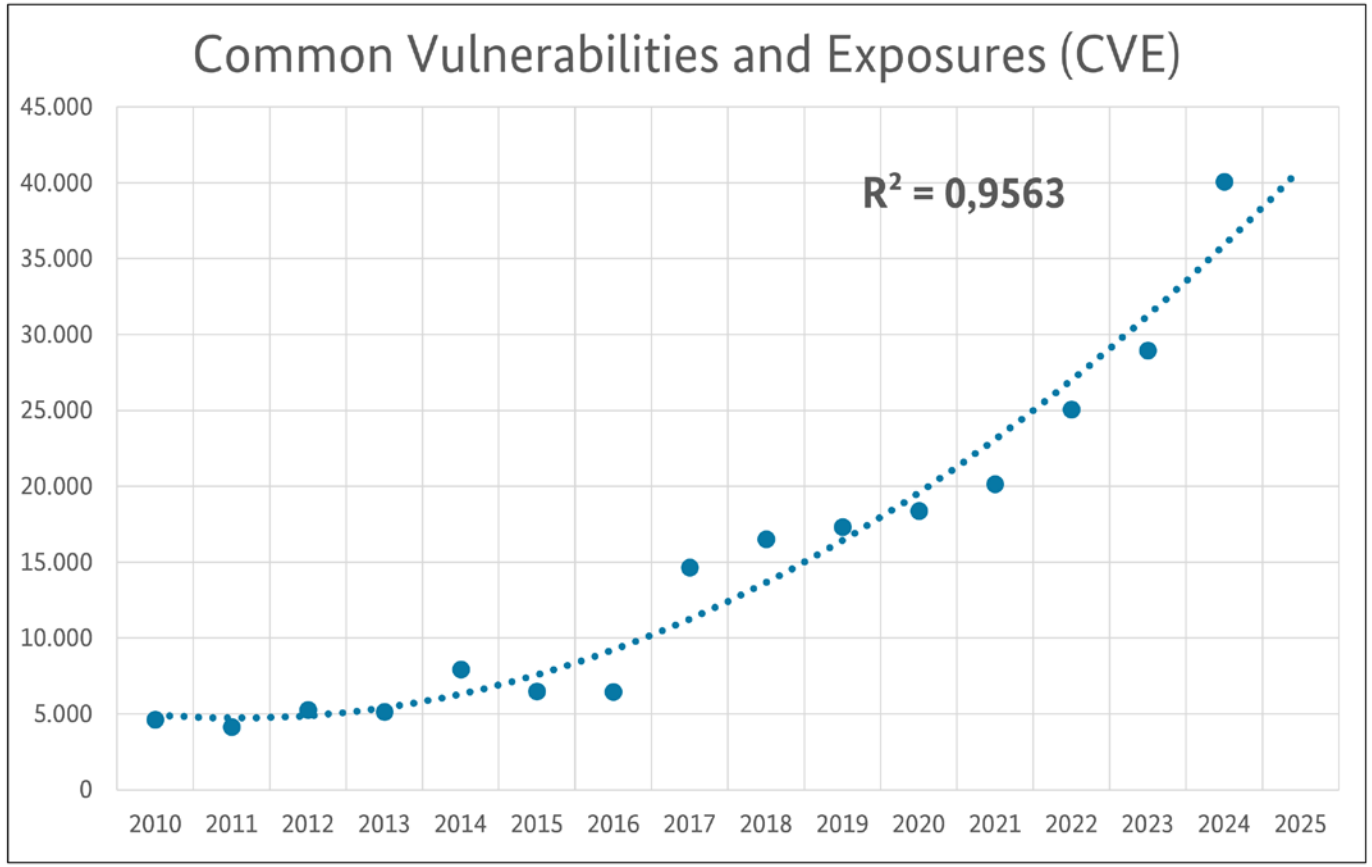
Schwachstelle? Patch me if you can!

Option A


Option B

2024: Mehr als 100 Schwachstellen pro Tag

Wie viele gemeldete Schwachstellen erwarten wir in den nächsten Jahren?



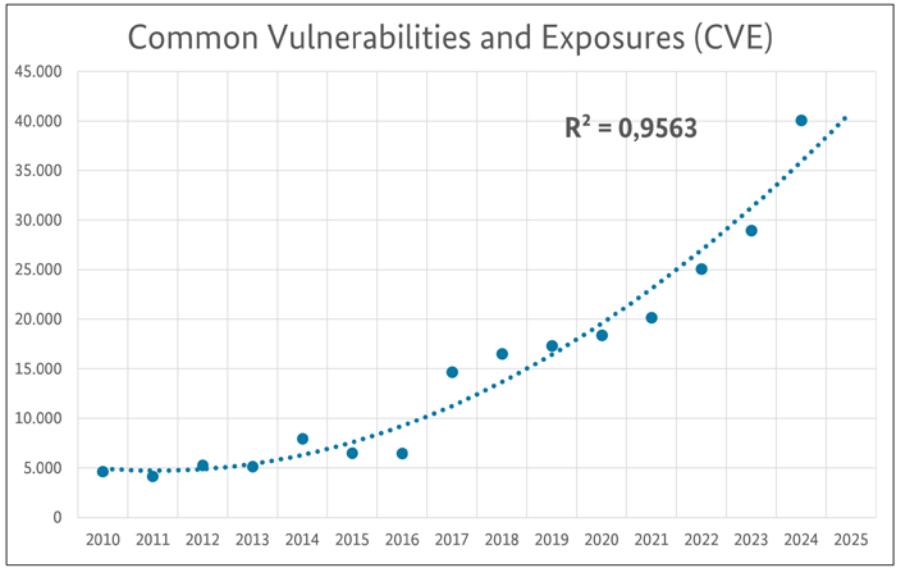
Jahr	Anzahl der CVE
2010	4.639
2011	4.150
2012	5.288
2013	5.142
2014	7.948
2015	6.494
2016	6.457
2017	14.645
2018	16.512
2019	17.308
2020	18.375
2021	20.161
2022	25.059
2023	28.961
2024	40.077

Datenquelle: https://cve.mitre.org

2024: Mehr als 100 Schwachstellen pro Tag

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	40.077

Was brauchen wir (noch)?

Wir brauchen CVEn und Advisories

CVE

Eine Schwachstelle
mit eindeutiger Nummer

Ziel:
über dasselbe reden

Advisory

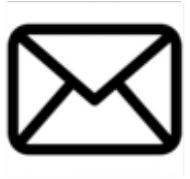
Umgang mit einer oder
mehrerer Schwachstellen

Ziel:
Beseitigung oder Gegenmaßnahmen beschreiben

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.)



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.)
- **Manueller Abgleich** mit den eigenen Systemen und der eigenen Infrastruktur
- **Manuelle Bewertung** (Kritikalität, Betroffenheit, etc.)

§-Reiten leicht gemacht: Der CRA in Daten und Fakten

11.12.2024

Der CRA tritt in Kraft

11.06.2026

Konformitätsbewertungs-stellen können die Erfüllung der Anforderungen an den CRA bewerten

11.09.2026

Meldepflicht für Schwachstellen und Sicherheitsvorfälle

11.12.2027

Alle CRA-Anforderungen sind bei neuen Produkten eingehalten

CSAF – Common Security Advisory Framework

CSAF 2.0 seit 11.2022 internationaler Standard der OASIS, seit 02.2025 ISO-Standard

- **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

CSAF – Common Security Advisory Framework

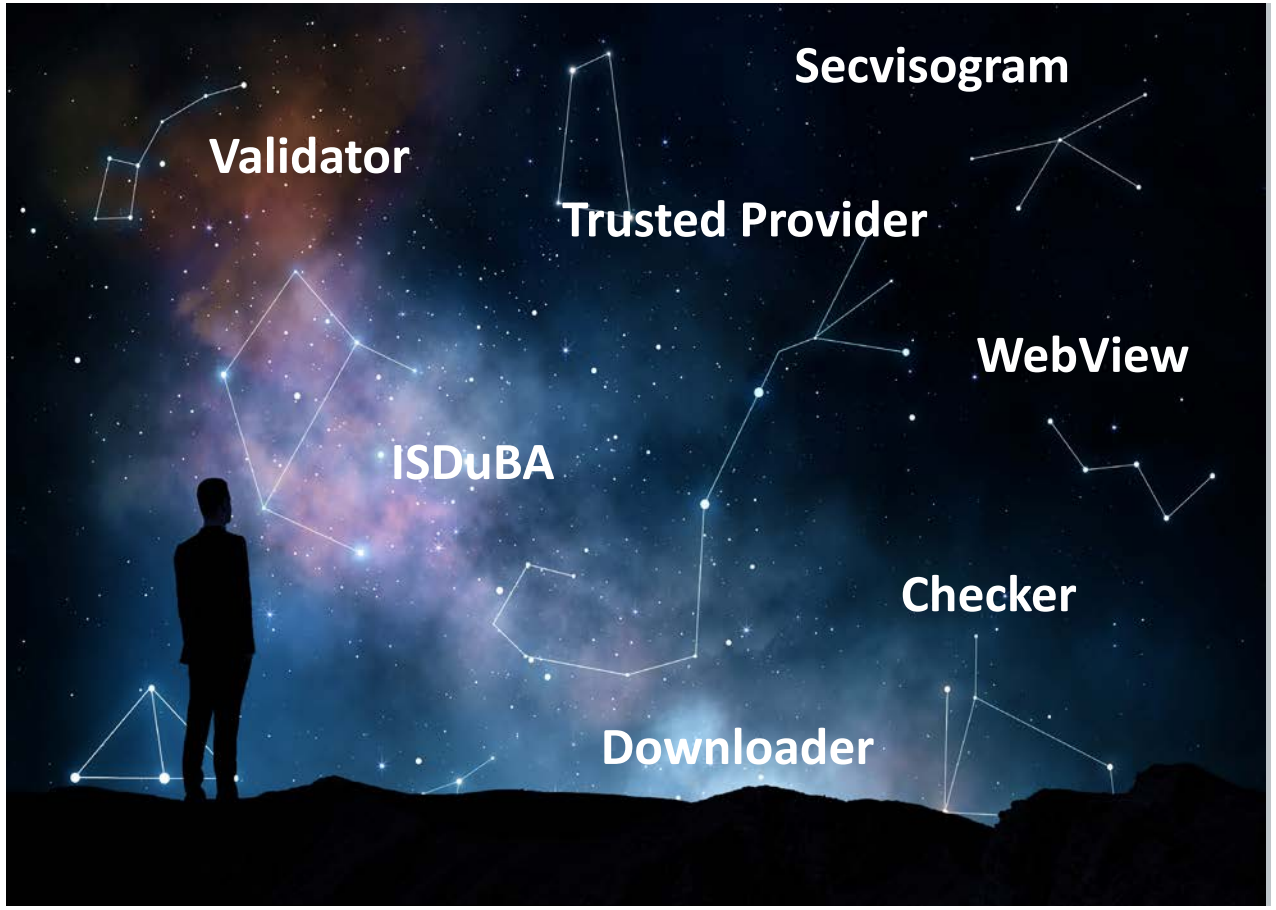
CSAF 2.0 seit 11.2022 internationaler Standard der OASIS, seit 02.2025 ISO-Standard

- **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
- Abgleich mit **Asset Management** und **SBOMs** möglich
- Benachrichtigungen über **verfügbare Sicherheitsupdates und Inhalte**

Das CSAFversum expandiert

CSAF fordern und fördern

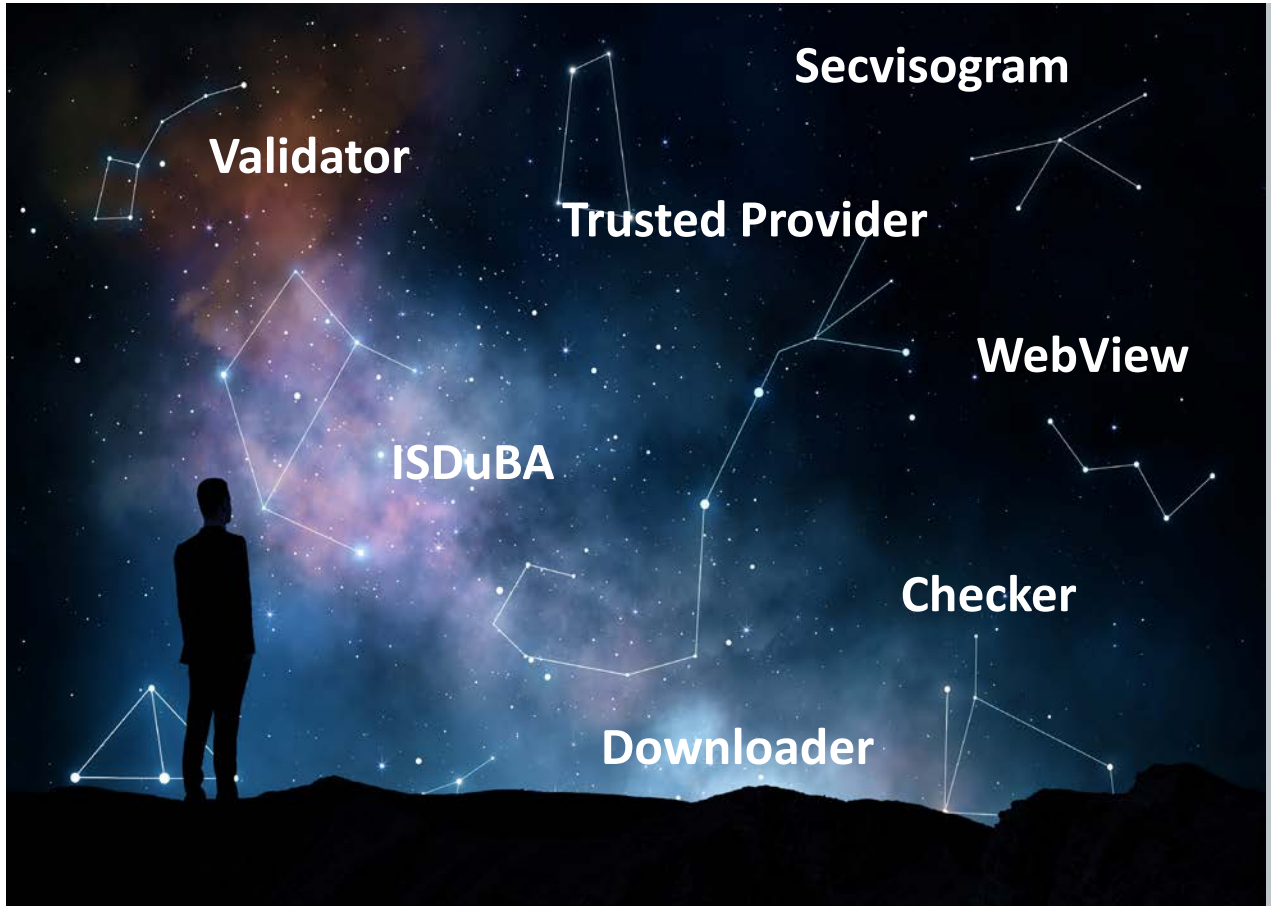
- **CSAF wird genutzt und eingefordert**
- **Open Source Tools** werden weiterentwickelt
- **Synergien** zwischen einzelnen Tools



Das CSAFversum expandiert

CSAF fordern und fördern

- **CSAF wird genutzt und eingefordert**
- **Open Source Tools** werden weiterentwickelt
- **Synergien** zwischen einzelnen Tools
- **CSAF 2.1 Standard** in den Startlöchern
- **Awareness** durch Vorträge, Workshops und Publikationen rund um das Thema 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

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 OS)**
  - 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

Die Rolle des BSI

Das CSAFversum expandiert durch viele ineinandergreifende Tätigkeiten

- **Aktive Mitarbeit in der Standardisierung**
- **Erstellung & Erprobung von - sowie Initiativen zu Tools, um Einstieg zu erleichtern**
  - Secvisogram
  - ISDuBA
  - Sec-o-simple
  - TR-03191

Die Rolle des BSI

Das CSAFversum expandiert durch viele ineinandergreifende Tätigkeiten

- Aktive Mitarbeit in der Standardisierung
- Erstellung & Erprobung von - sowie Initiativen zu Tools, um Einstieg zu erleichtern
  - Secvisogram
  - **ISDuBA**
  - Sec-o-simple
  - TR-03191
- **Bereitstellen von Advisories des Warn- und Informationsdienst mittels CSAF**
  - Aggregation von Advisories von Herstellern (CSAF Aggregator des BSI)
  - Pflege der „Gelben Seiten“ für CSAF (CSAF Lister des BSI)
- **Workshops mit Herstellern & Anwendern (Nov. 2025)**

https://www.bsi.bund.de/csaf

csaf@bsi.bund.de

CSAF TO GO

Diese Punkte verdienen Be**ACHT**ung

1. CSAF ist OpenSource, Toolsammlung, Community
2. Standardisiertes, maschinenverarbeitbares Format (JSON)
3. Automatisierbarer Abruf und Verteilung
4. Skalierbarkeit, weniger manueller Aufwand (delegierbar)

CSAF TO GO

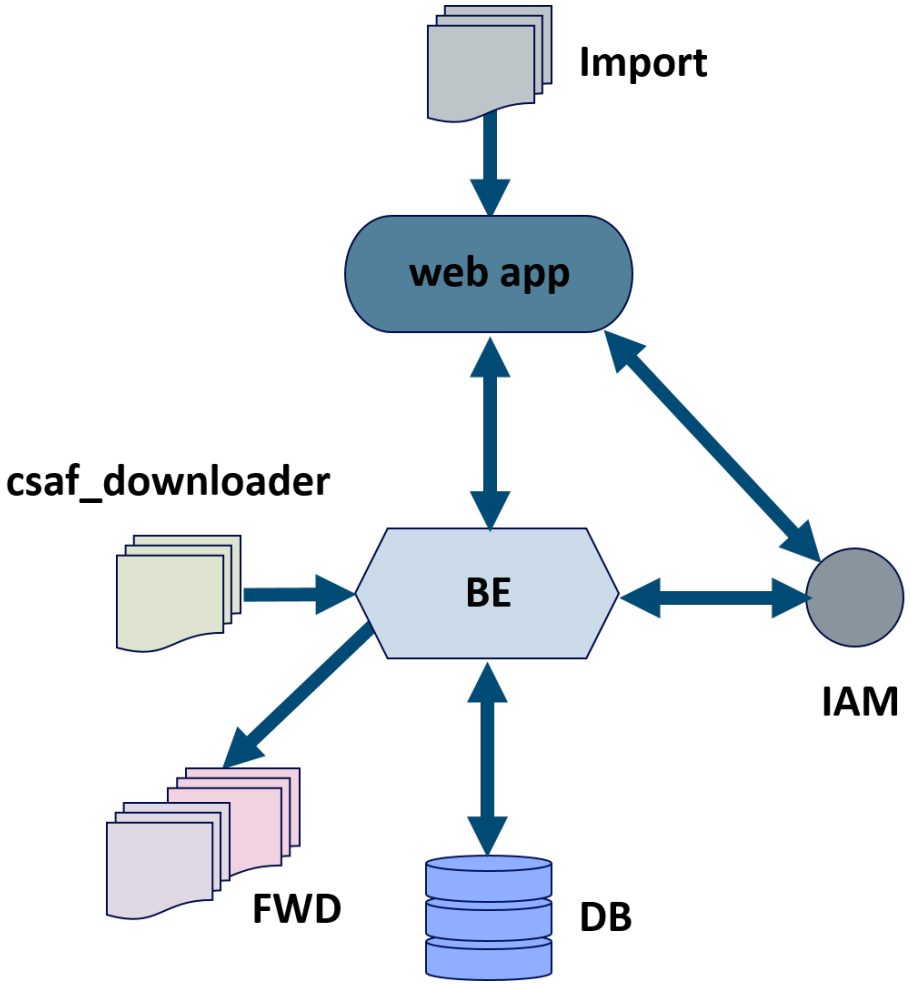
Diese Punkte verdienen Be**ACHT**ung

1. CSAF ist OpenSource, Toolsammlung, Community
2. Standardisiertes, maschinenverarbeitbares Format (JSON)
3. Automatisierbarer Abruf und Verteilung
4. Skalierbarkeit, weniger manueller Aufwand (delegierbar)
5. Betroffenheit einzelner Produkte direkt feststellbar (VEX ist Profil in CSAF)
6. Nur relevante Advisories werden geladen
7. CSAF 2.1 in den Startlöchern
8. Vereinfachtes Risikomanagement

Projekt 621: ISDuBA

Internes **S**ystem zum **D**ownload **u**nd zur **B**ewertung von **A**dvisories

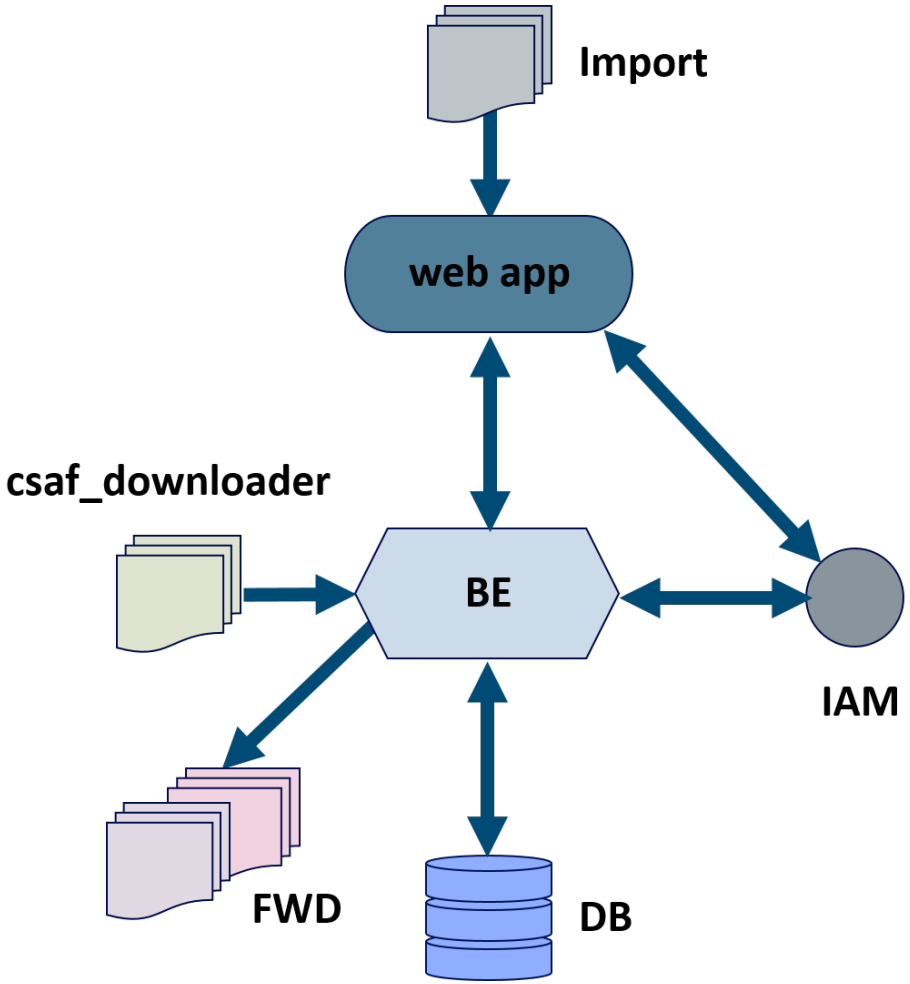
- Backend: Go
- Datenbank: PostgreSQL
- IAM: keycloak
- Web App Frontend: svelte-flowbite



Projekt 621: ISDuBA

Internes **S**ystem zum **D**ownload **u**nd zur **B**ewertung von **A**dvisories

- Backend: Go
- Datenbank: PostgreSQL
- IAM: keycloak
- Web App Frontend: svelte-flowbite
- csaf_distribution: Advisory-Download
- csaf_webview: Dokumentenanzeige
- Docker-Container



Demo ISDuBA

Bild: © AdobeStock/ The Little Hut

Dr. Dina Truxius

Fachexpertin

dina.truxius@bsi.bund.de

csaf@bsi.bund.de

+49 (0) 228 99 9582 6147

+49 (0) 15120968958

https://bsi.bund.de/csaf

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us:

Links und weiterführende Informationen

- **CSAF webpage:** https://csaf.io
- **CSAF producer:** https://github.com/secvisogram/secvisogram
- **CSAF producer:** https://github.com/sec-o-simple/
- **CSAF download and evaluation:** https://github.com/ISDuBA/ISDuBA
- **CSAF trusted provider, checker, aggregator and downloader:** https://github.com/gocsaf/csaf
- **BSI TR-03191:** https://www.bsi.bund.de/dok/TR-03191
- **OASIS TC:** https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf
- **CSAF GitHub:** https://github.com/oasis-tcs/csaf
- **Noch mehr CSAF Tools:** https://oasis-open.github.io/csaf-documentation/tools