Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Thomas Schmidt (BSI)

Geheimrezept Automatisierung: Mehr Ressourcen für IT/OT-Sicherheit durch CSAF

Andreas Harner (CERT@VDE)

VDE CERT

Was ist CSAF?

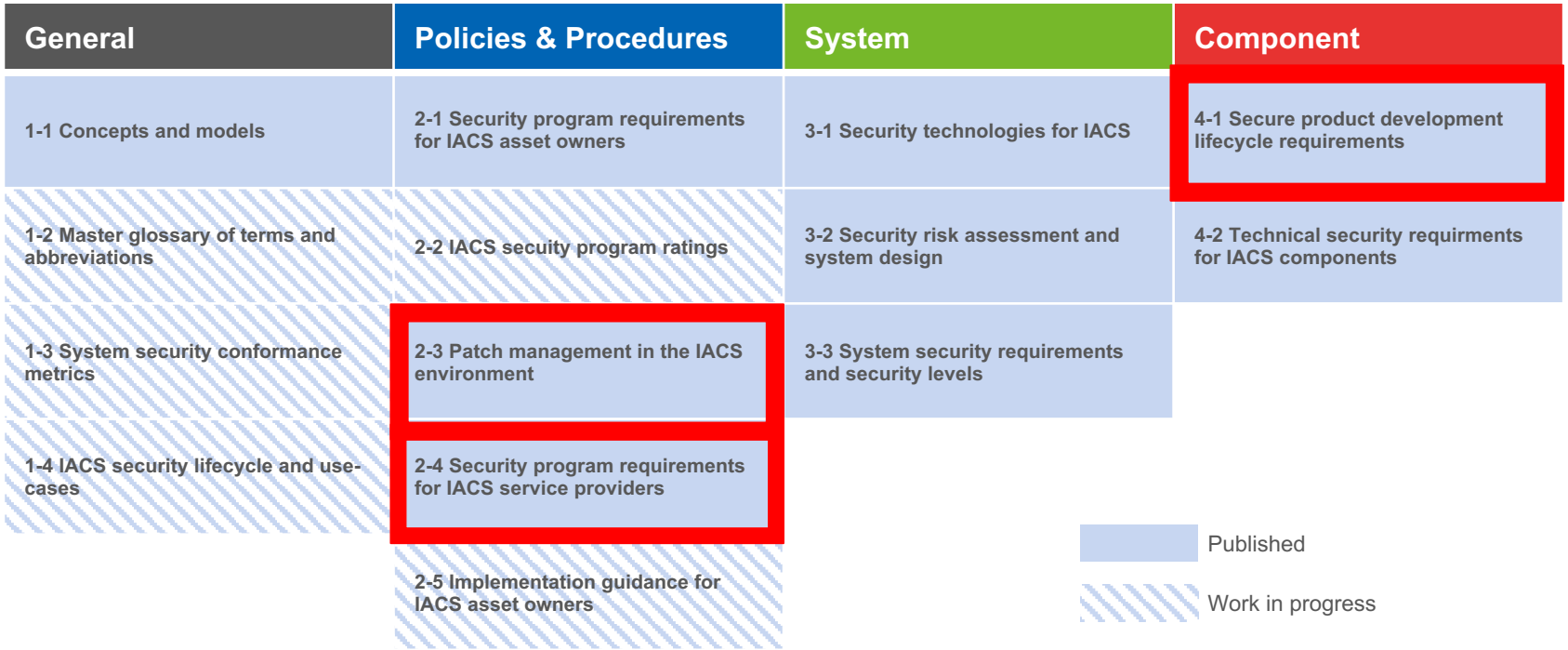
Carl Andrew Spaatz (**C**hief of **S**taff of the United States **A**ir **F**orce: 26.9.1947-29.4.1948

Was ist CSAF?

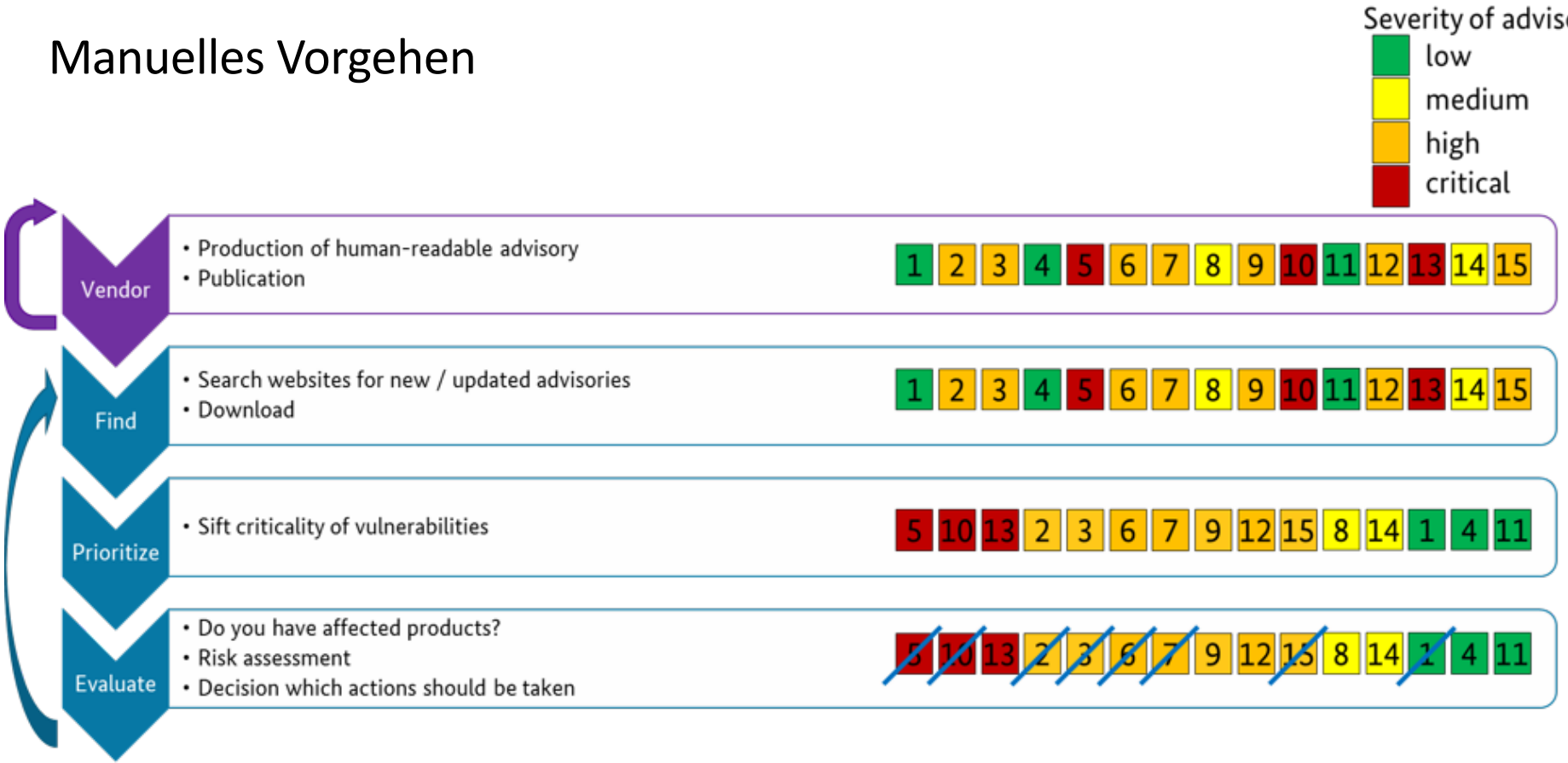
Common Security Advisory Framework

Wer hat davon schon gehört?
Wer verwendet es schon?

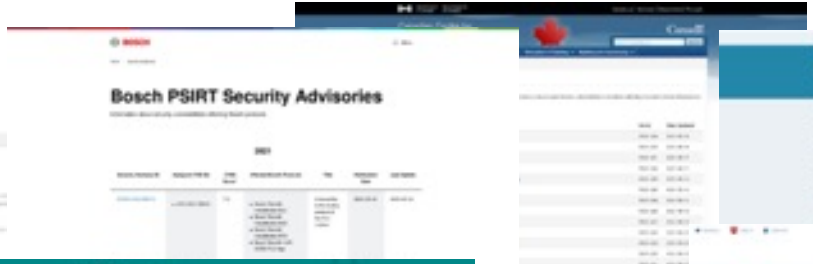
IEC 62443: Anforderungen zum Umgang mit Schwachstellen



Manuelles Vorgehen

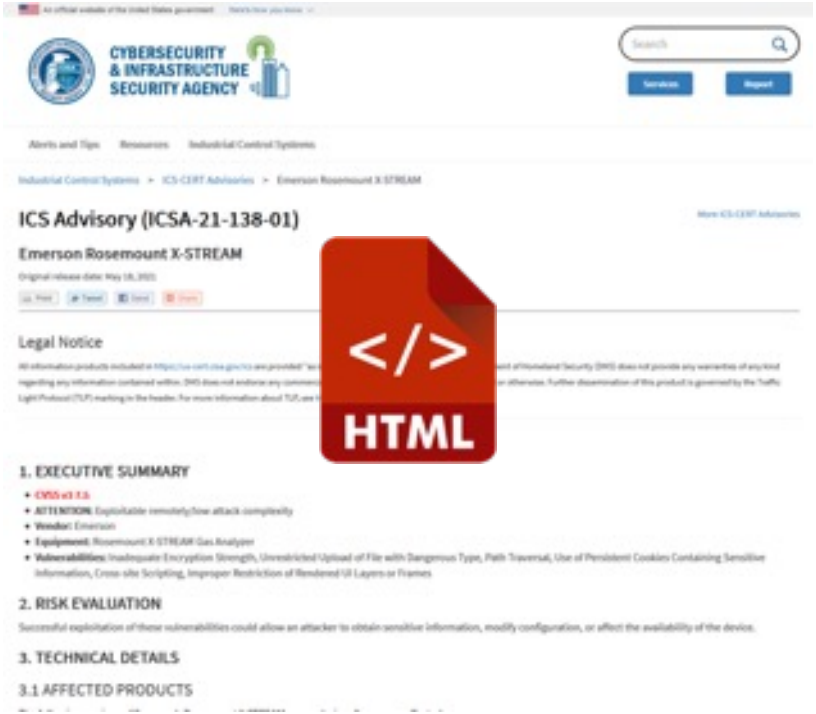


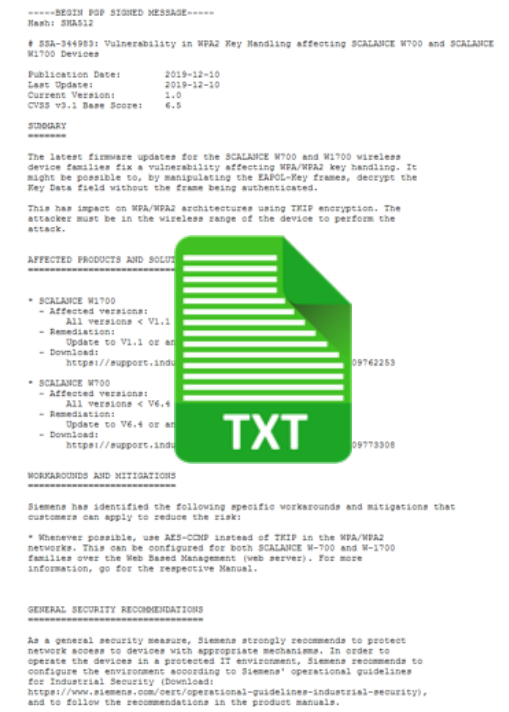
Finden



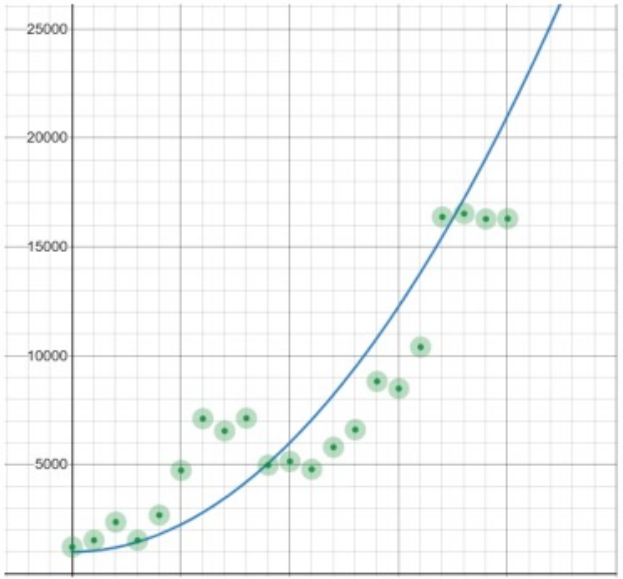
Bundesamt für Sicherheit in der Informationstechnik

Analysieren / Lesen

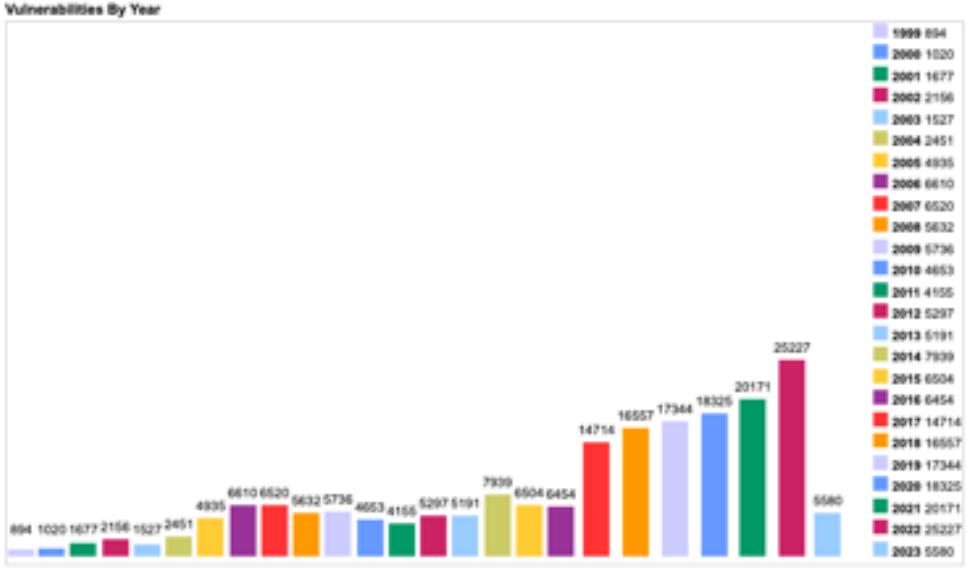




Die Anzahl von Schwachstellen steigt…

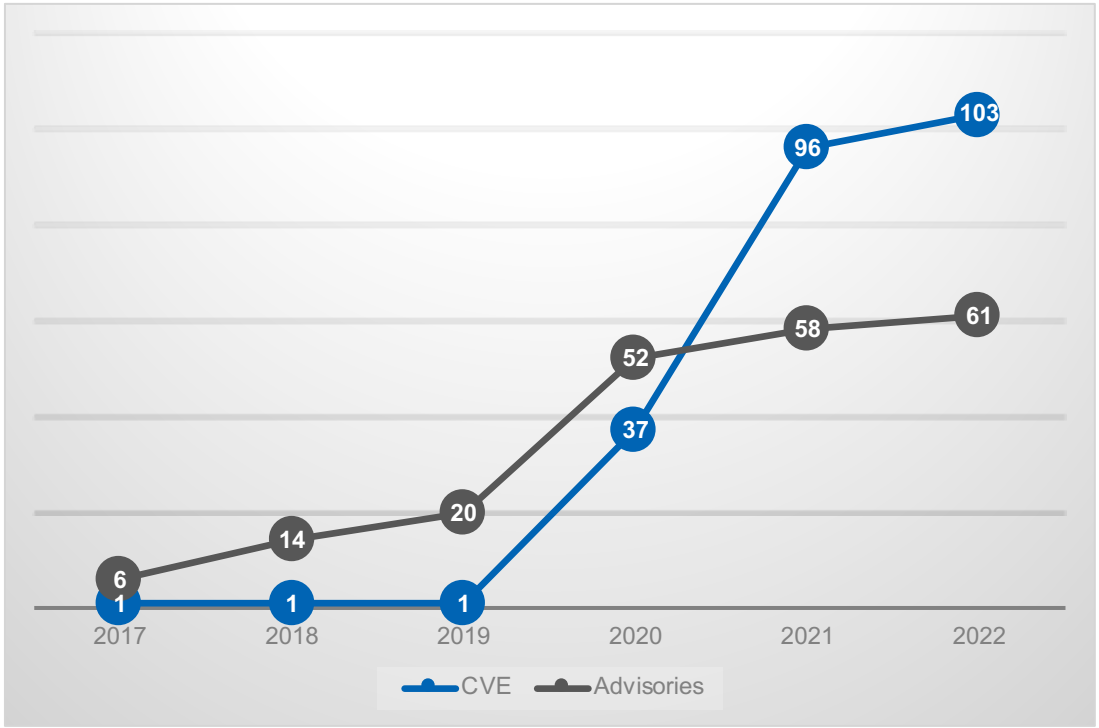


https://opensourcesecurity.io/2021/03/30/its-time-to-fix-cve/



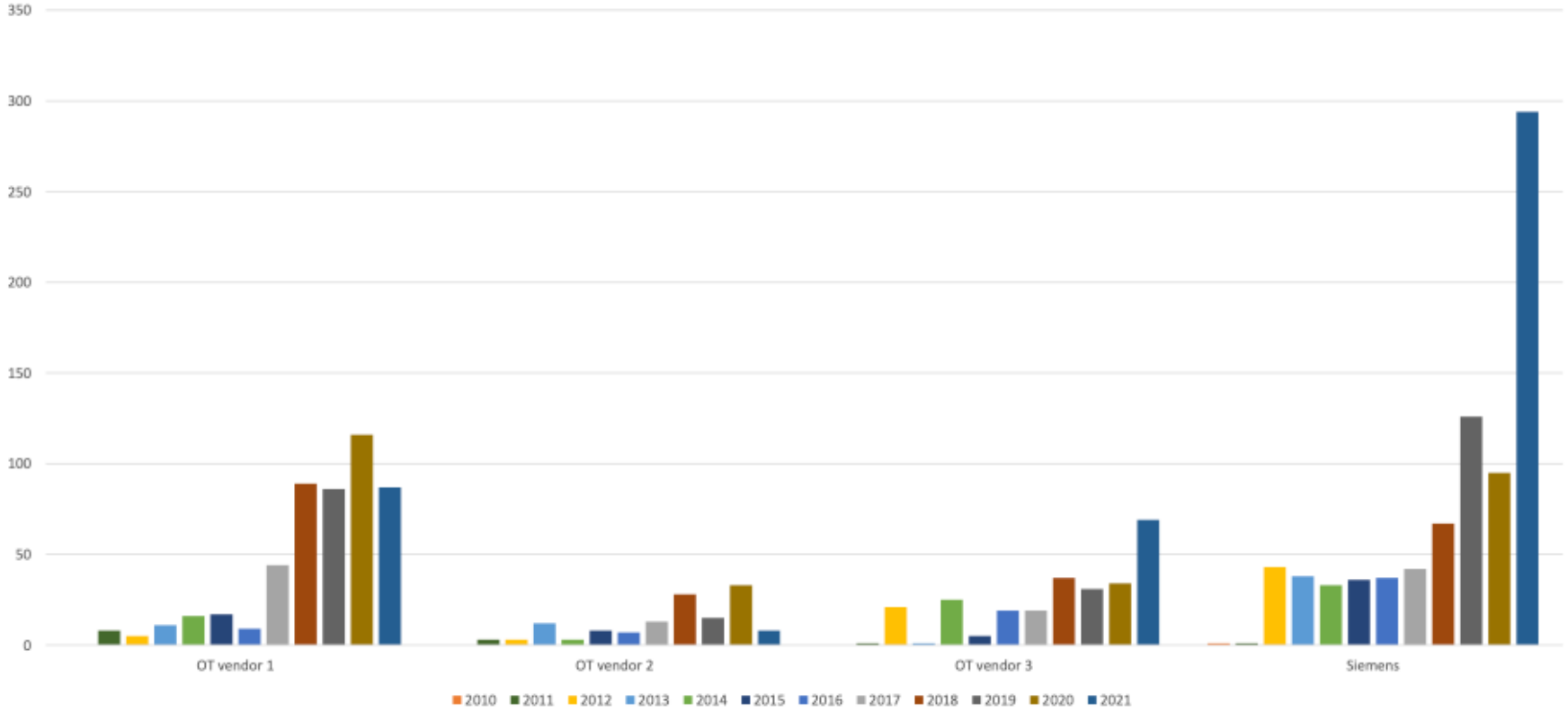
Source: https://www.cvedetails.com/browse-by-date.php

CERT@VDE: Die Anzahl von Schwachstellen und Advisories steigt



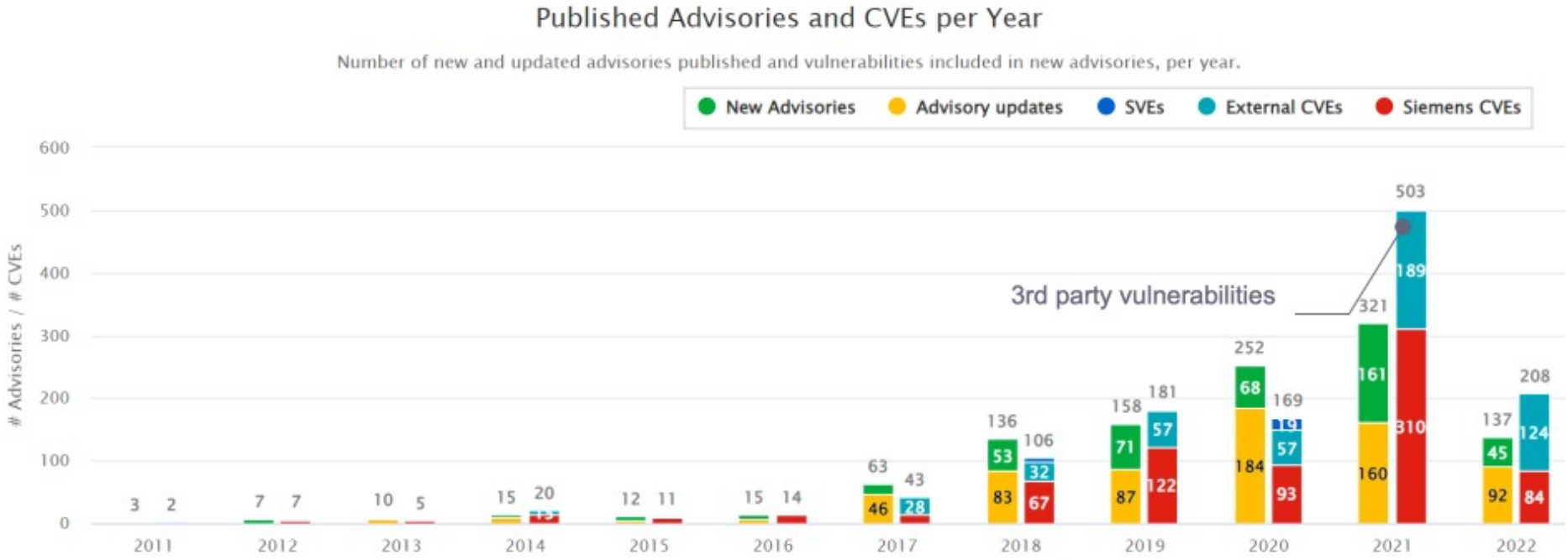
…dito: Siemens & andere Hersteller

(Quelle: Dr. Tom Pröll / Dr. Tobias Limmer, Siemens)



…detaillierter Blick auf Siemens

(Quelle: Dr. Tom Pröll / Dr. Tobias Limmer, Siemens)



Wie schnell wächst dieses Problem zukünftig?

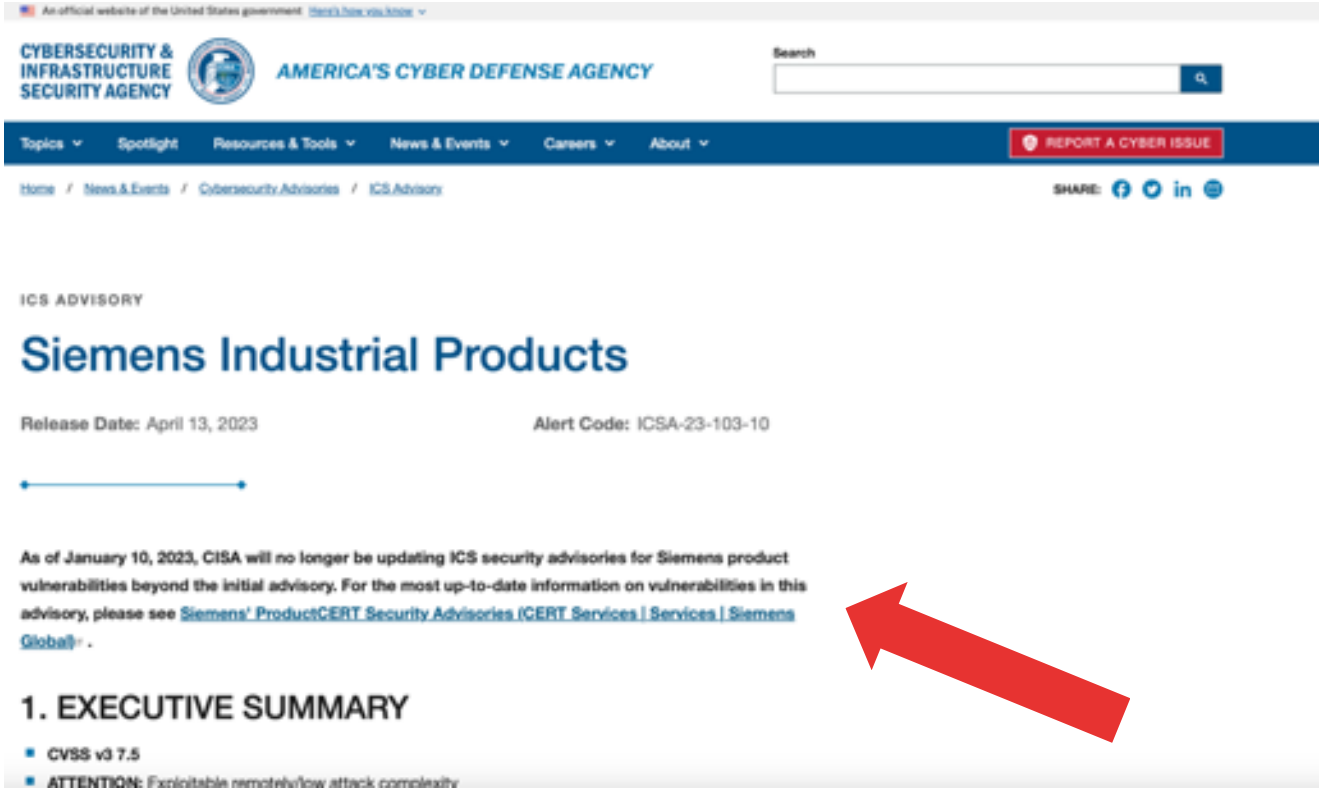
- Lineares oder exponentielles Wachstum?
- In welchen Dimensionen findet Wachstum statt:
  - Anzahl der Schwachstellen im OT-Code?
  - Anzahl der Schwachstellen in 3rd Party-Code?
  - Anzahl der betroffenen Produkte?
  - Anzahl der Hersteller und Zulieferer die Schwachstellen Handling machen?
- Was trägt Regulierung dazu bei?

Manuelles Schwachstellen-Handling:

„Das skaliert nicht!“

CISA: *„Das skaliert nicht….“*

(https://www.cisa.gov/news-events/ics-advisories/icsa-23-103-10)



An official website of the United States government Here's how you know

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About | REPORT A CYBER ISSUE

Home / News & Events / Cybersecurity Advisories / ICS Advisory

SHARE:

ICS ADVISORY

Siemens Industrial Products

Release Date: April 13, 2023

Alert Code: ICSA-23-103-10

As of January 10, 2023, CISA will no longer be updating ICS security advisories for Siemens product vulnerabilities beyond the initial advisory. For the most up-to-date information on vulnerabilities in this advisory, please see Siemens' ProductCERT Security Advisories (CERT Services | Services | Siemens Global) .

1. EXECUTIVE SUMMARY

- **CVSS v3 7.5**
- **ATTENTION:** Exploitable remotely/low attack complexity

Mögliche Lösungen

CSAF standardisiert Herstelleradvisories!

Für den Nutzer werden die Tools in Zukunft ohne Zusatzarbeit Informationen über relevante Patches und Updates anzeigen können

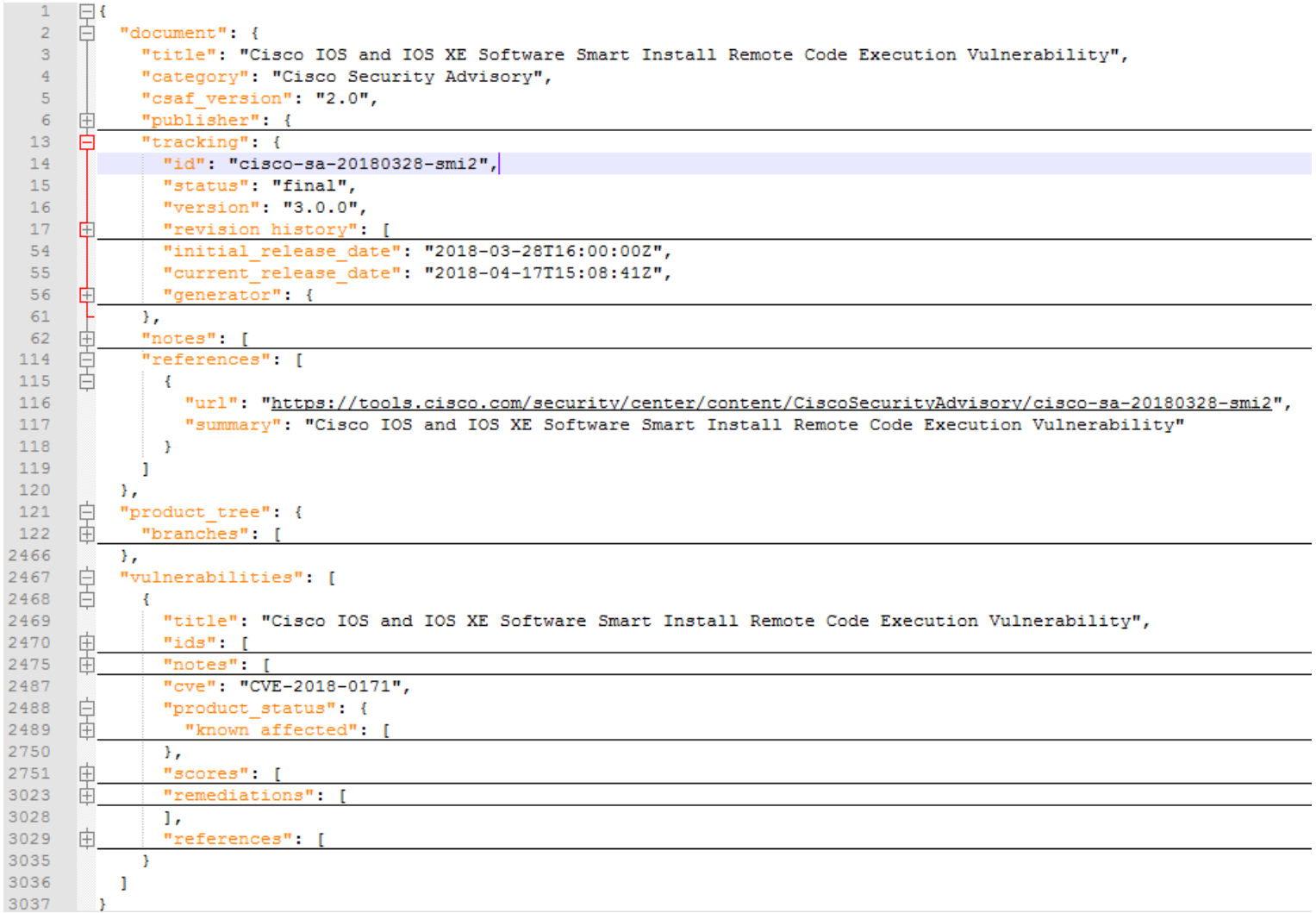
Was ist CSAF?

Common Security Advisory Framework

- Internationaler, kostenloser und offener Standard
- Maschinenlesbares Format für Security Advisories (JSON)
- Standardisierte Methode zur Verteilung von Security Advisories
- Ausgerichtet auf Automatisierung
- Standardisiertes Toolset
- Empfehlung für umsetzbarer
- Nachfolger von CSAF CVRF 1.2

Bereit zur Benutzung!

Beispiel CSAF Dokument



```
{
  "document": {
    "title": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability",
    "category": "Cisco Security Advisory",
    "csaf_version": "2.0",
    "publisher": {
    "tracking": {
      "id": "cisco-sa-20180328-smi2",
      "status": "final",
      "version": "3.0.0",
      "revision_history": [
      "initial_release_date": "2018-03-28T16:00:00Z",
      "current_release_date": "2018-04-17T15:08:41Z",
      "generator": {
    },
    "notes": [
    "references": [
      {
        "url": "https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2",
        "summary": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability"
      }
    ]
  },
  "product_tree": {
    "branches": [
  },
  "vulnerabilities": [
    {
      "title": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability",
      "ids": [
      "notes": [
      "cve": "CVE-2018-0171",
      "product_status": {
        "known_affected": [
      },
      "scores": [
      "remediations": [
      ],
      "references": [
    }
  ]
}
```

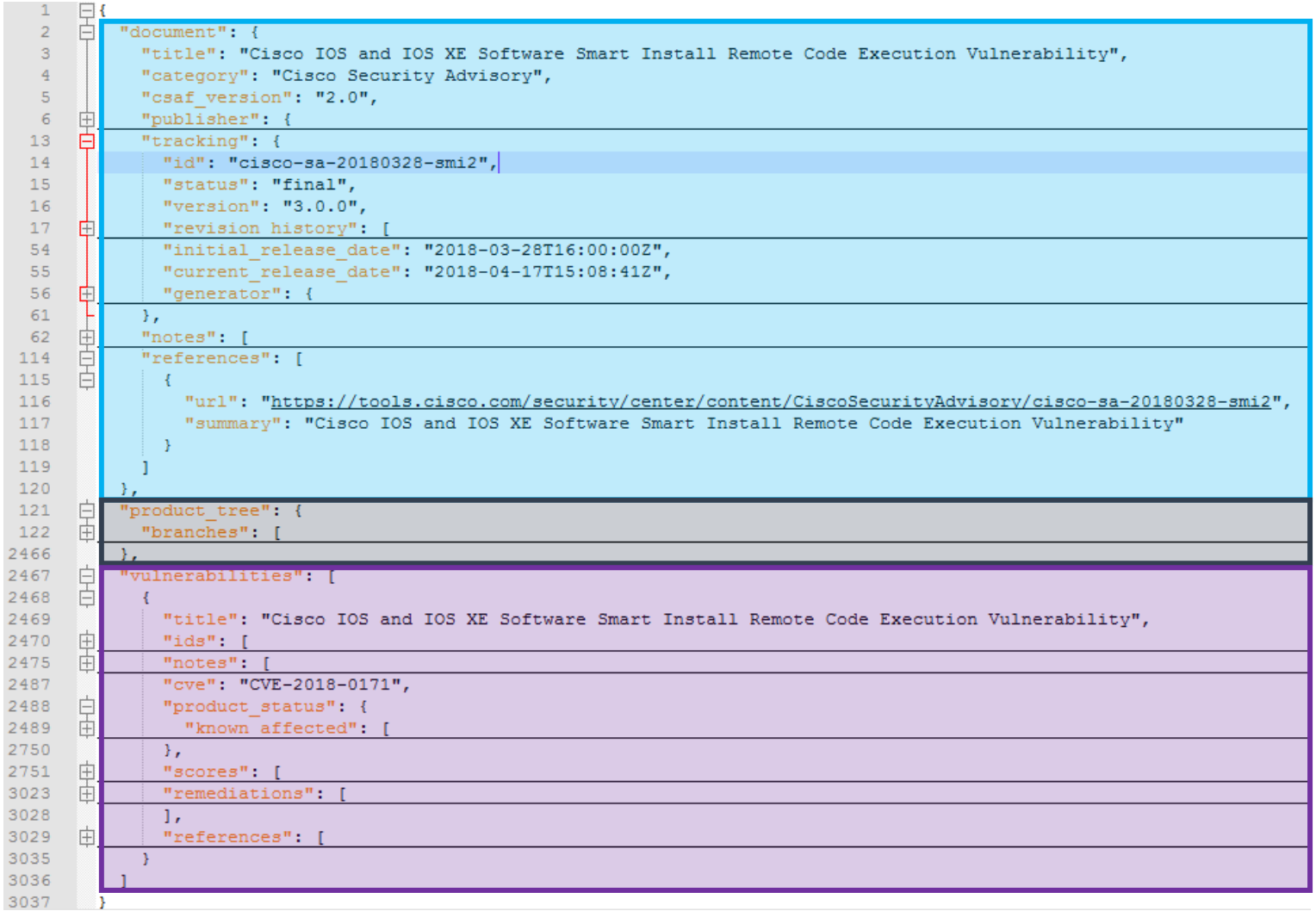
Bundesamt für Sicherheit in der Informationstechnik

Beispiel CSAF Dokument

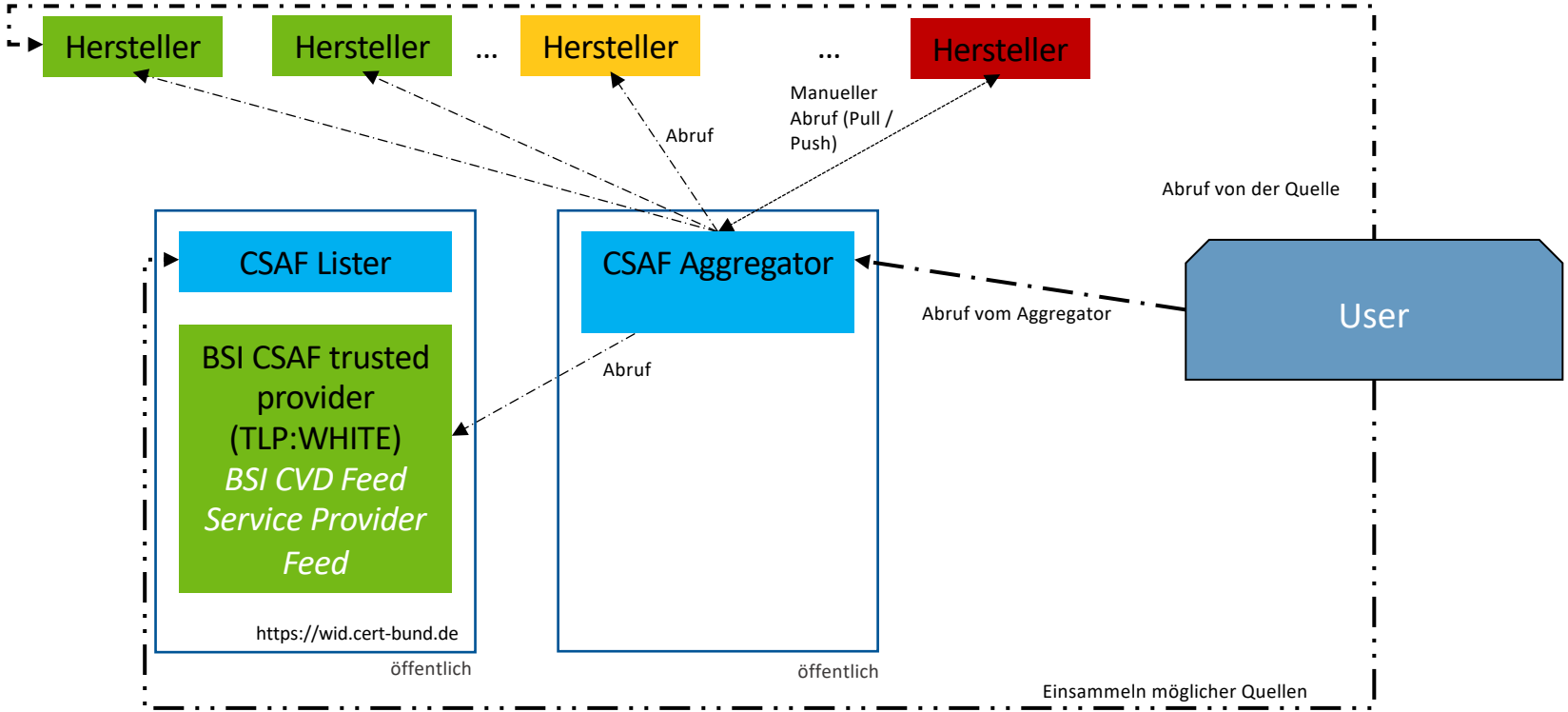
Metadaten auf Dokumentebene

Produktbaum

Schwachstellen

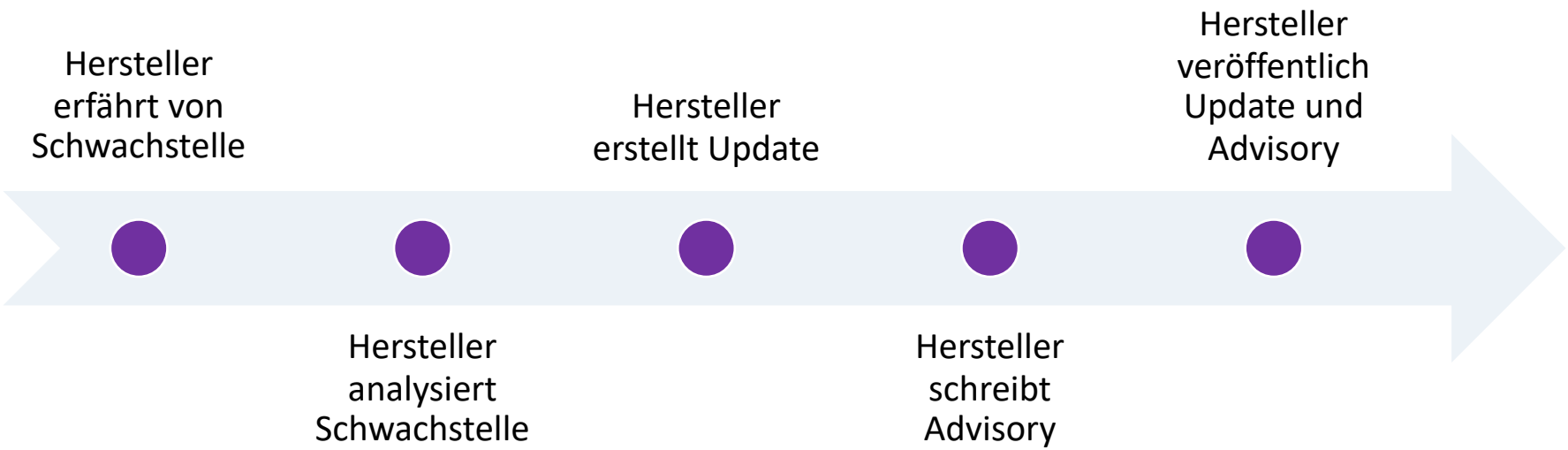


Bundesamt für Sicherheit in der Informationstechnik

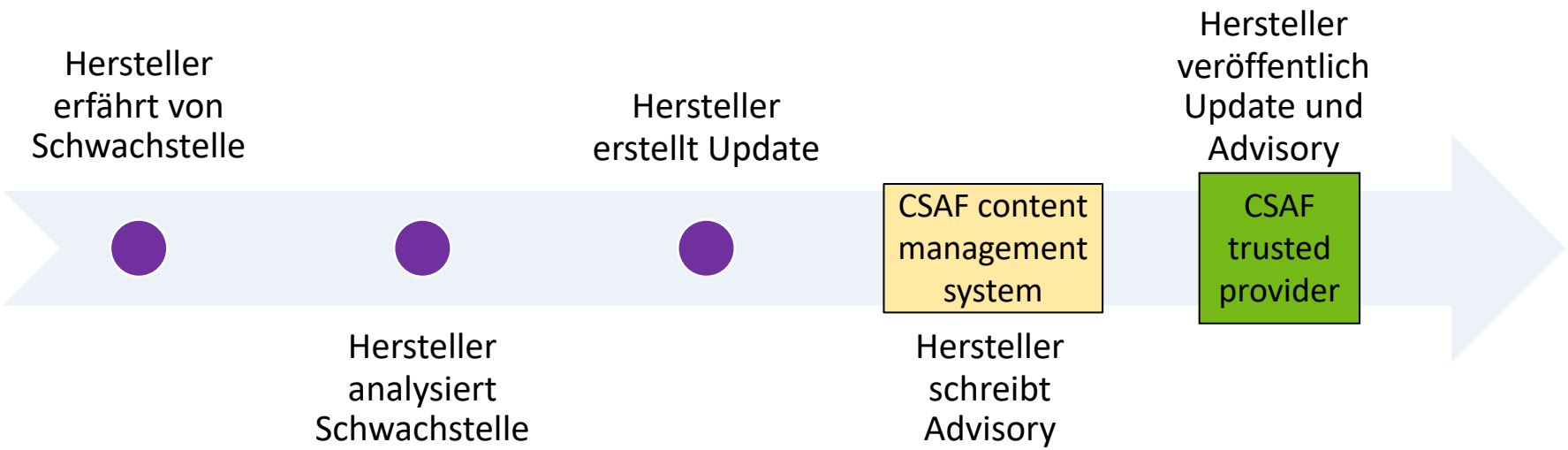

Hersteller
Hersteller
...
Hersteller
...
Hersteller
Abruf
Manueller Abruf (Pull / Push)
Abruf von der Quelle
CSAF Lister
CSAF Aggregator
User
Abruf vom Aggregator
BSI CSAF trusted provider (TLP:WHITE)
BSI CVD Feed
Service Provider Feed
Abruf
https://wid.cert-bund.de
öffentlich
öffentlich
Einsammeln möglicher Quellen

Sicht eines Herstellers

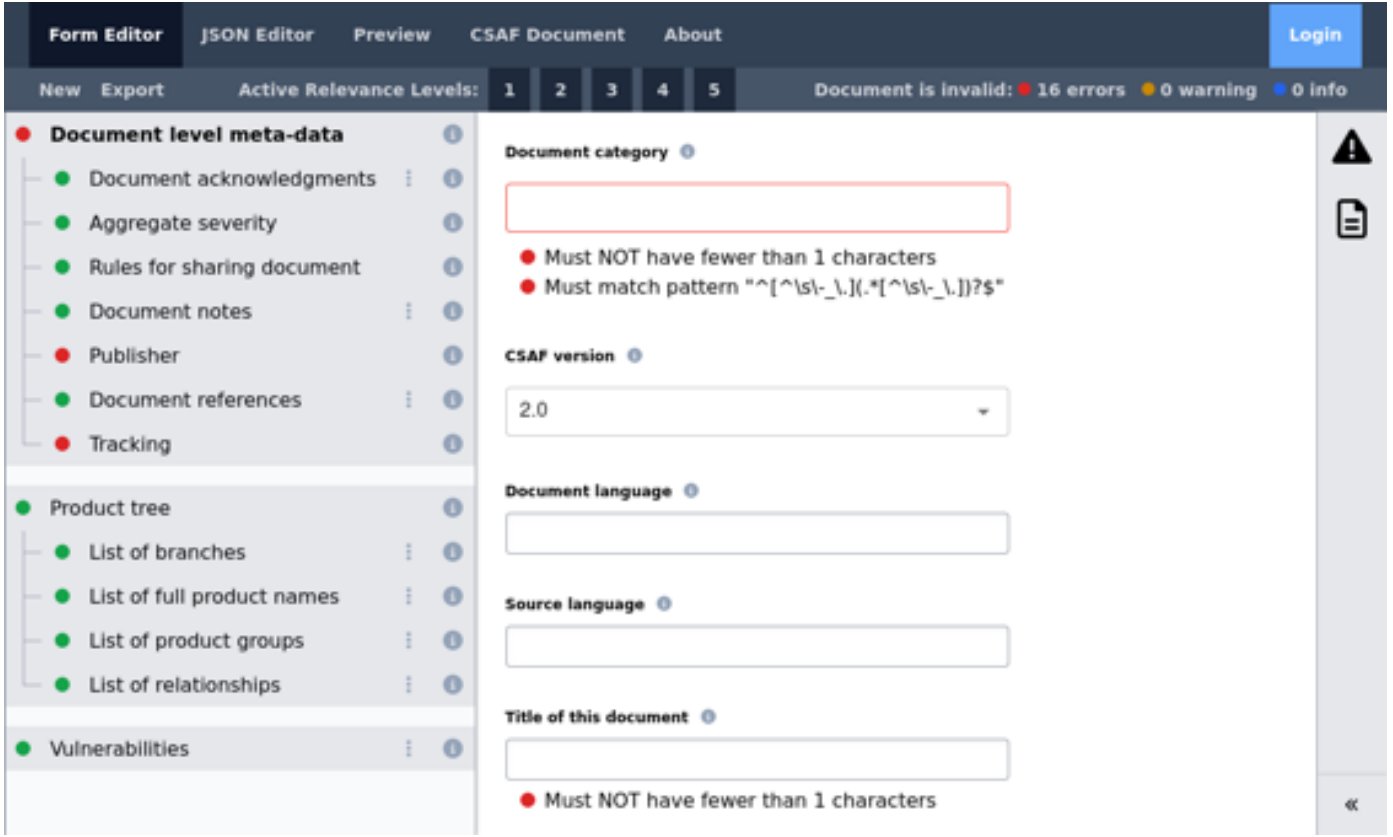
Hersteller


Hersteller erfährt von Schwachstelle
Hersteller analysiert Schwachstelle
Hersteller erstellt Update
Hersteller schreibt Advisory
Hersteller veröffentlich Update und Advisory

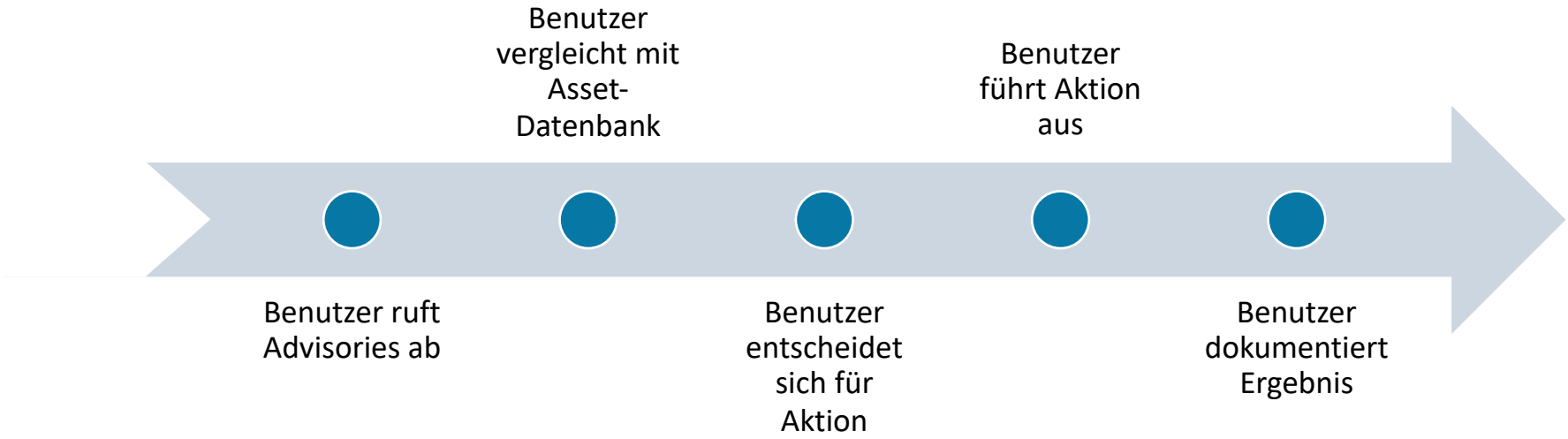
Hersteller


Hersteller erfährt von Schwachstelle
Hersteller analysiert Schwachstelle
Hersteller erstellt Update
Hersteller schreibt Advisory
CSAF content management system
Hersteller veröffentlich Update und Advisory
CSAF trusted provider

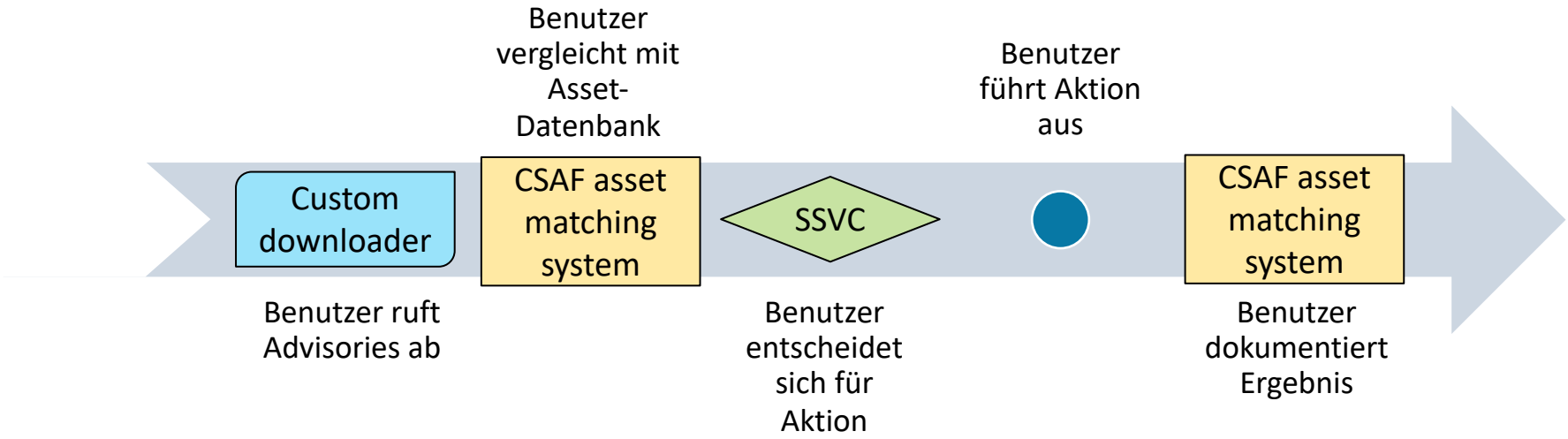
https://secvisogram.github.io



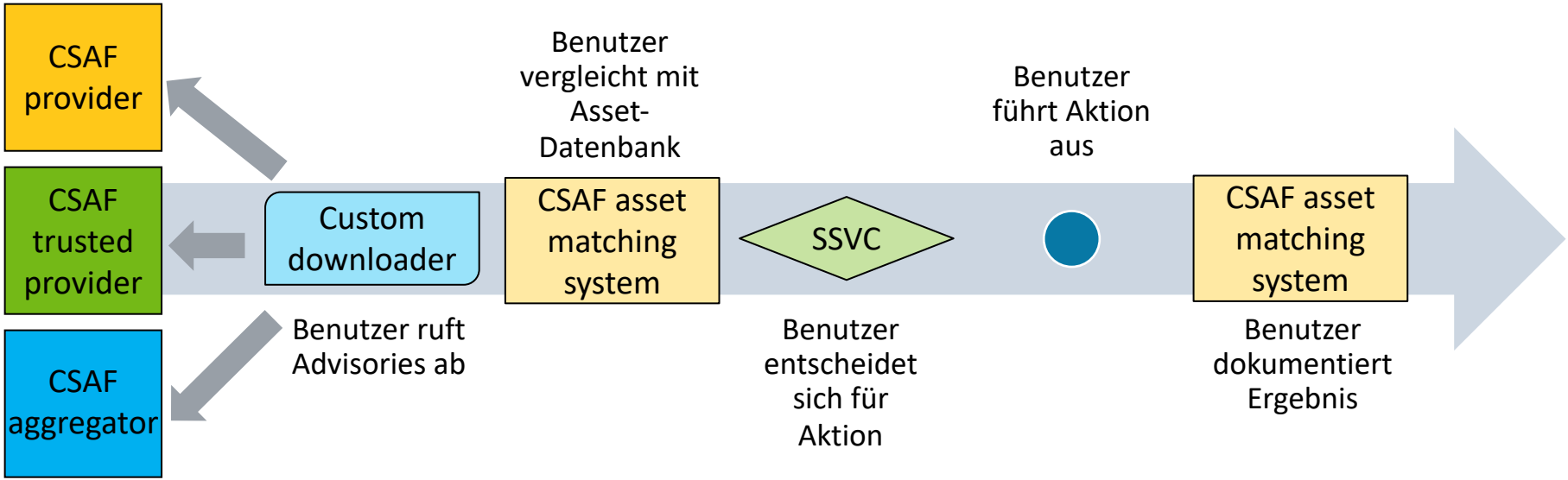
Benutzer


Benutzer vergleicht mit Asset-Datenbank
Benutzer führt Aktion aus
Benutzer ruft Advisories ab
Benutzer entscheidet sich für Aktion
Benutzer dokumentiert Ergebnis

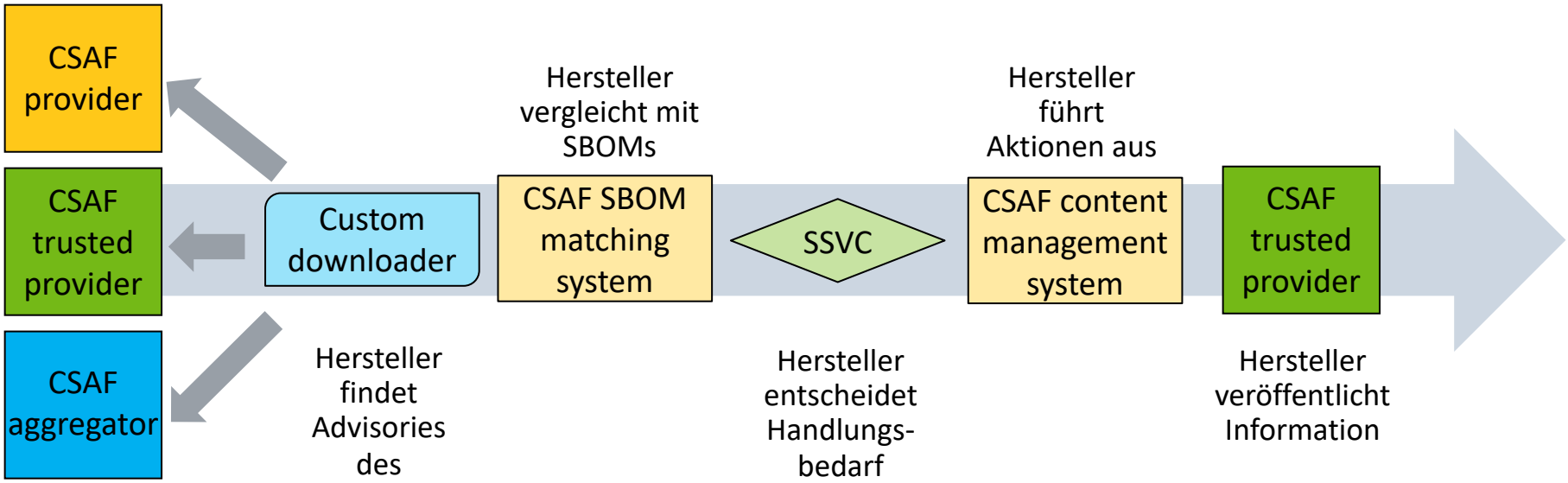
Benutzer


Benutzer vergleicht mit Asset-Datenbank
Benutzer führt Aktion aus
Custom downloader
CSAF asset matching system
SSVC
CSAF asset matching system
Benutzer ruft Advisories ab
Benutzer entscheidet sich für Aktion
Benutzer dokumentiert Ergebnis

Benutzer


CSAF provider
CSAF trusted provider
CSAF aggregator
Custom downloader
Benutzer ruft Advisories ab
Benutzer vergleicht mit Asset-Datenbank
CSAF asset matching system
SSVC
Benutzer entscheidet sich für Aktion
Benutzer führt Aktion aus
CSAF asset matching system
Benutzer dokumentiert Ergebnis

Lieferkette aus Sicht eines Herstellers



CSAF veröffentlichende Organisationen

Omicron

Festo

CERT@VDE:

CERT@VDE

CSAF aggregator

CSAF trusted provider

CSAF Consumer

CSAF trusted provider

CSAF trusted provider

CSAF trusted provider

CSAF trusted provider

PARTNER_1

PARTNER_2

PARTNER_3

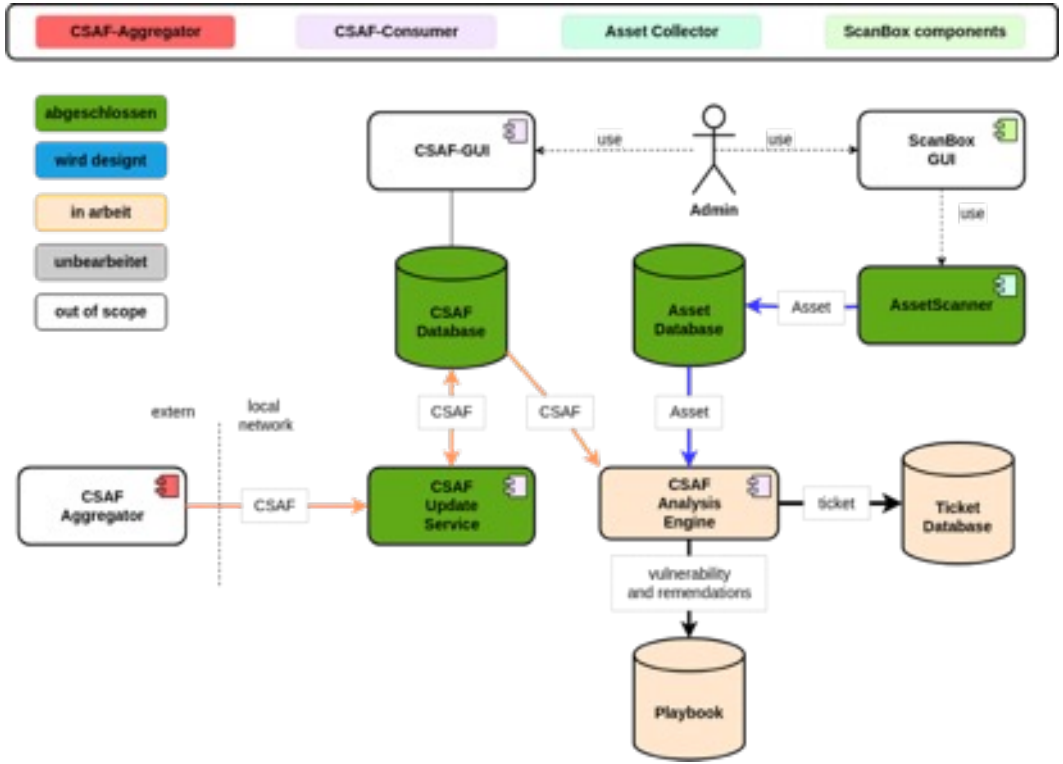
PARTNER_4

VDE CERT

VDE CERT

ZenSIM Industrie 4.0

GEFÖRDERT VOM
ZenSIM Industrie 4.0
Bundesministerium für Bildung und Forschung



Zusammenfassung & Aktionspunkte

- Die Zahl der entdeckten Schwachstellen steigt
  => auch die Zahl der Advisories
- Advisories werden für risikobasierte Entscheidungen benötigt
- Automatisierung ist möglich - also automatisieren Sie die langweiligen Aufgaben

- **Fordern Sie Ihre Zulieferer auf, CSAF 2.0 bereitzustellen**
- **Bereinigen und digitalisieren Sie Ihre Inventarlisten**
- **Fordern Sie CSAF in Ausschreibungen**
- **Verbreiten #oCSAF weiter**

Informationsmaterial unter https://csaf.io

OASIS TC: CSAF Webseite:	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf
CSAF GitHub:	https://github.com/oasis-tcs/csaf
CSAF 2.0 JSON Schema:	https://docs.oasis-open.org/csaf/csaf/v2.0/csaf_json_schema.json
CSAF 2.0 Text:	https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html
CSAF 2.0 Beispiele:	https://github.com/oasis-tcs/csaf/tree/master/csaf_2.0/examples
Secvisogram Quellcode:	https://github.com/secvisogram/secvisogram
Online-Editor:	https://secvisogram.github.io

Verfügbare Open Source Tools

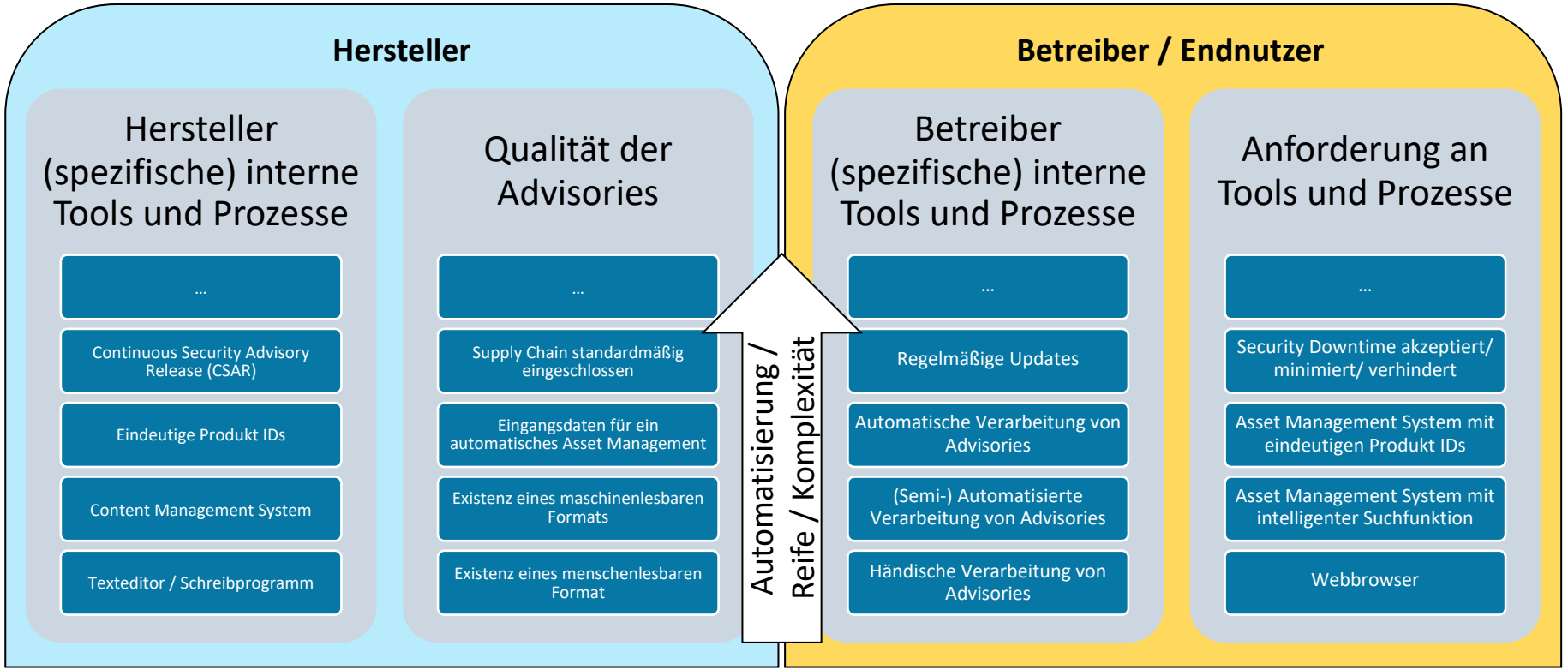
- CSAF producer: https://github.com/secvisogram/secvisogram OR https://github.com/mfd2007/yace
- CSAF content management system: https://github.com/secvisogram/secvisogram + https://github.com/secvisogram/csaf-cms-backend *(WIP)*
- CSAF trusted provider: https://github.com/csaf-poc/csaf_distribution
- CSAF aggregator: https://github.com/csaf-poc/csaf_distribution
- Provider checker: https://github.com/csaf-poc/csaf_distribution *(WIP)*
- CSAF management system: *open for commercial and Open Source tools*
- CSAF asset matching system: *open for commercial and Open Source tools*
- CSAF downloader: https://github.com/csaf-poc/csaf_distribution
- CSAF full validator: https://github.com/secvisogram/csaf-validator-service
- CSAF filename tester: https://pypi.org/project/paikalta/

Vielen Dank für Ihre Aufmerksamkeit!

Thomas Schmidt
Fachexperte
csaf@bsi.bund.de
+49 (0) 228 99 9582 6404
+49 (0) 228 99 10 9582 6404

Andreas Harner
Leiter CERT@VDE
Tel. +49 69 6308-392
andreas.harner@cert.vde.com

Zwei Seiten der gleichen Medaille – verschiedene Reifegrade



Nächster Schritt: Stufe 2 bei allen beteiligten Parteien