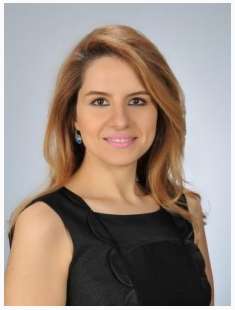
Demonstrator with CSAF-Matching

from the project ZenSIM4.0



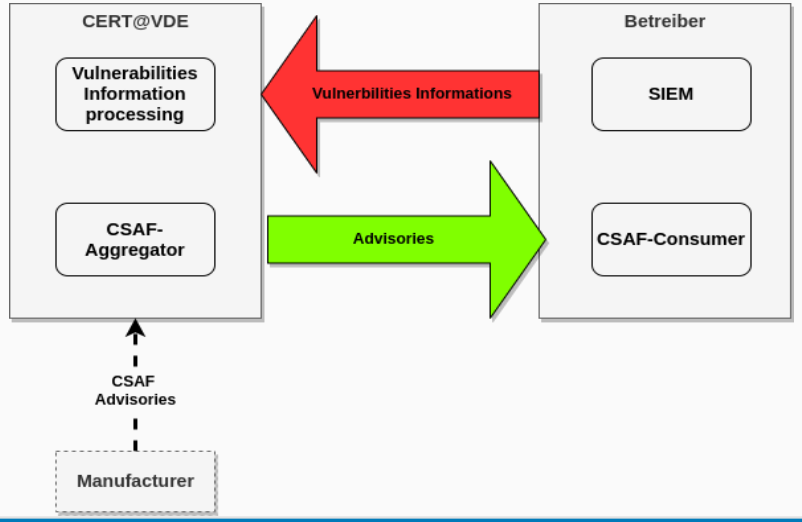
Dr. Salva Daneshgadeh Cakmakcı
DECOIT® GmbH & Co. KG
Fahrenheitstraße 9
D-28359 Bremen
https://www.decoit.de
daneshgadeh@decoit.de

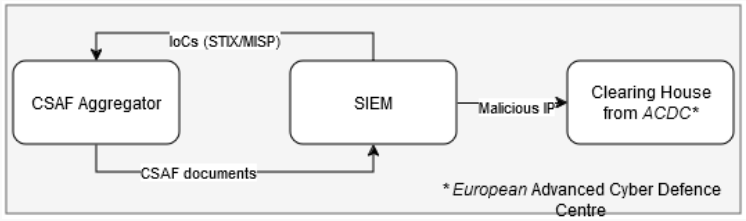
CSAF Community Days 2024

Table of Contents

Central Security Incident Management for SMEs in Industry 4.0 (ZenSIM4.0)

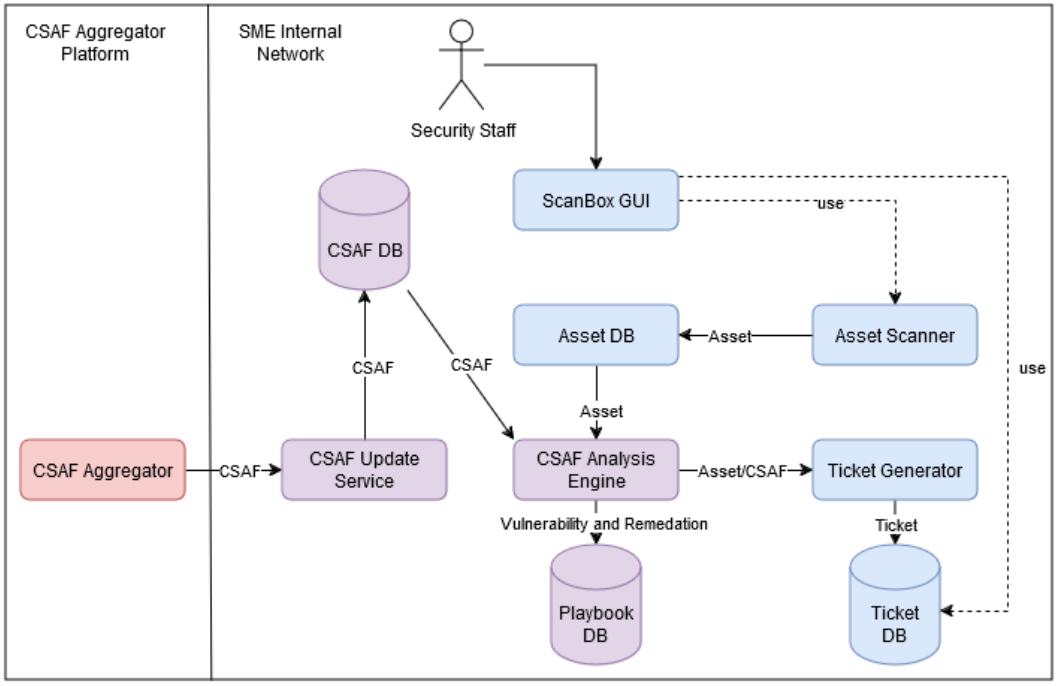
- BMBF project (September 2021 – November 2024)
- Website: https://zensim-project.de
- Partner: DECOIT®, Hochschule Bremen and CERT@VDE
- Overall budget: 1,57 Mio. €
- CSAF Consumer + ScanBox® (SIEM for Enterprises) → SIEM for ICS networks





Platform Architecture:
SIEM with CSAF Consumer Component

- CSAF Aggregator
- CSFA-Update-Service
- Asset Scanner
- CSAF-Analysis-Engine
- CSAF DB
- Asset DB
- Ticket DB
- Playbook DB



CSAF Aggregator & CSAF-Update-Service

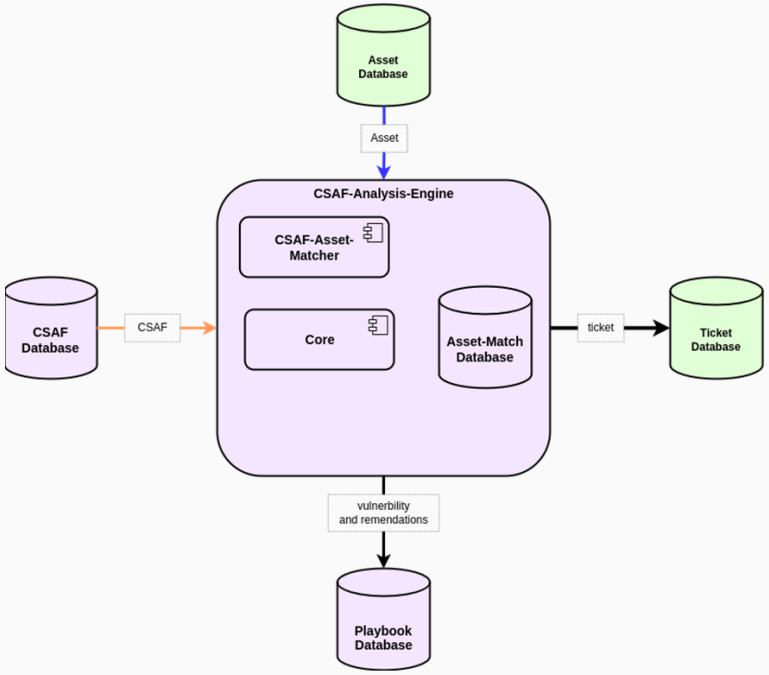
- In the project: CERT@DVE played a CSAF aggregator role.
- In this demonstrator: Siemens plays the CSAF aggregator role
- Csaf-Update-Service:
  - Receives CSAF documents from CSAF aggregator
  - Updates the local CSAF database (in ScanBox®) at regular intervals.

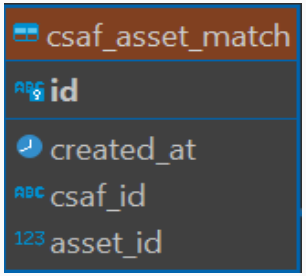
Asset Scanner

- Asset scanner is reachable by calling a REST API.
- Asset Scanner: Scans the network, stores asset's info in Asset Database
  - ```
    curl --insecure -X POST https://127.0.0.1:5000/scans -H "Content-Type: application/json" -H 'Authorization: Bearer <access_token>' -d '{"ip_range":"127.0.0.1","port_range":"80-100"}
    ```
  - ```
    curl --insecure -X POST https://127.0.0.1:5000/scans -H "Content-Type: application/json" -H 'Authorization: Bearer <access_token>' -d '{"ip_range":"192.168.178.0/24", "port_range":"100-120", "script":"s7-info"}'
    ```

CSAF-Analysis-Engine

- Asset matching is the main task of CSAF-Analysis-Engine



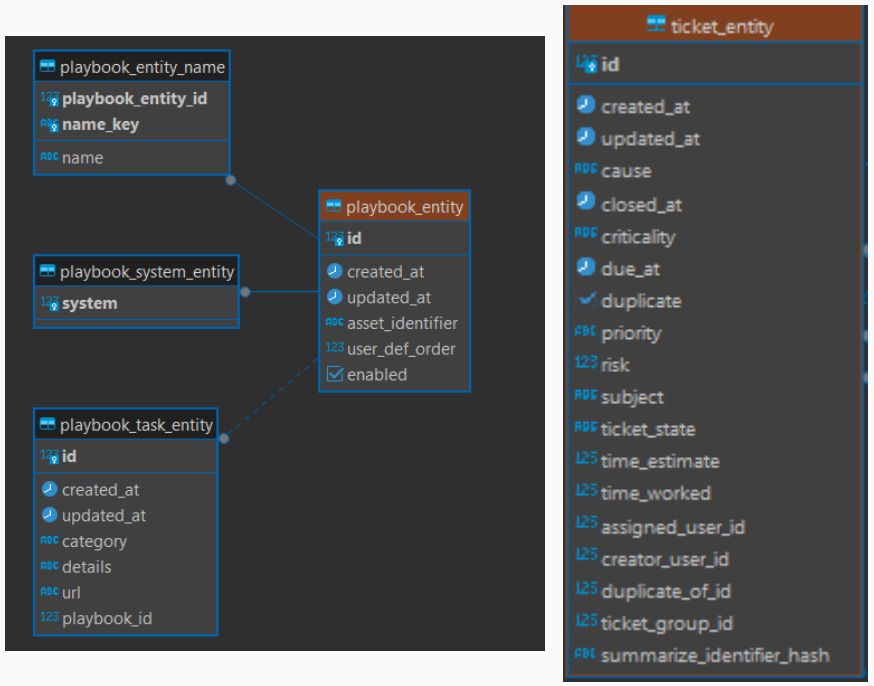


Asset Matcher

- For matching: The unique identification of an asset is crucial → lack of such globally defined identifier
- Namespace: manufacturer of the product
- Software Bill of Materials (SBOM): the name of the product + the manufacturer
- Matching OP1: Name of product + Version
  - Challenge: incompatibility between name of an asset retrieved from asset scanner and from CSAF documents
    - Pre-processing the name, such as converting all upper-case letters to lower-case letters
- Matching OP2: Common Platform Enumeration (CPE), package URL (purl), serial und model numbers, etc.

Playbook and Ticket Databases

- Playbook: assigned for an asset with known-vulnerabilities
- Includes tasks from „remediations“ field of the matched CSAF document
- Ticket: Consists of information about a vulnerable asset
  - Cause, criticality, risk, status, playbook, and etc.



Playbook Tasks from CSAF

- Remediation:
  - Mitigate
  - Vendor_fix
  - Workaround

Conclusion

- Ongoing and Future Enhancements:
  - Integrating IoT and ICS protocols into ScanBox®
  - Expanding capabilities of ScanBox® with asset vulnerability management
    - Utilizing CSAF documents
    - Utilizing known exploited vulnerabilities catalog (https://www.cisa.gov)
    - Integrating vulnerability scanning tools
  - Integrating standardized playbooks (in planning-phase)
- Tailored Solutions:
  - Offering customized projects to meet specific industry needs
- Collaboration Opportunities:
  - Open to shared industrial projects and partnerships
- Call to Action:
  - Partner with us to elevate your cybersecurity infrastructure

Thank you for the listening and open for questions

DECOIT GmbH & Co. KG
Fahrenheitstraße 9
D-28359 Bremen

https://www.decoit.de
info@decoit.de