



IACS & CYBERSECURITY CONFERENCE



April 15th 2025 • Amersfoort • The Netherlands



Exploring the BSI ecosystem focusing on network monitoring and vulnerability management

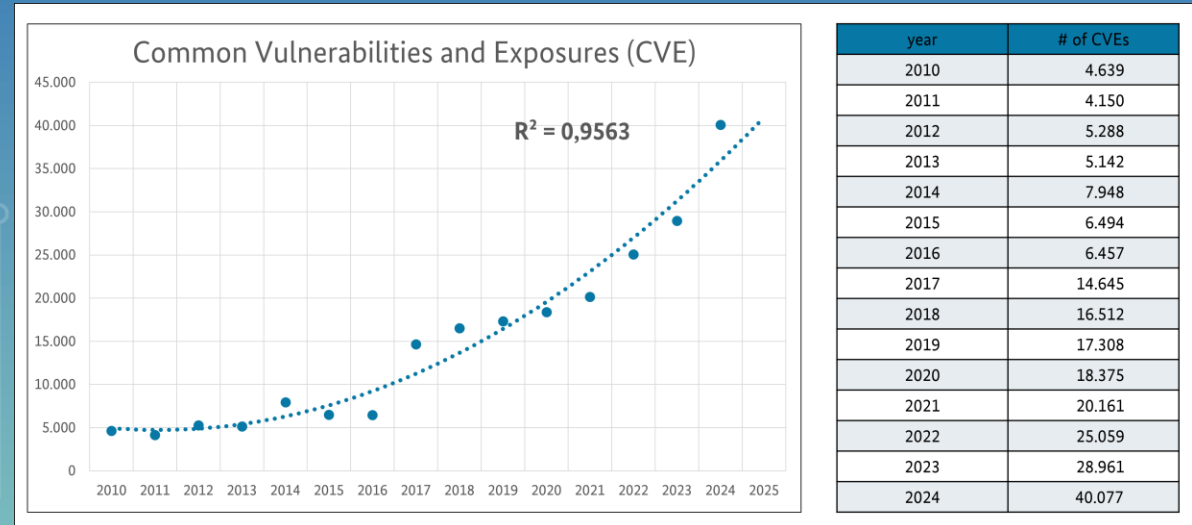


Do you have to deal with vulnerabilities? Have you heard of CSAF?



The number of vulnerabilities is constantly increasing

1. Trend: digital and fully-networked solutions (HW, SW, cloud solutions, remote access,...)
2. Enforced reporting: current and upcoming legal requirements (CRA, NIS 2, Machine Directive...)
3. Risk assessment and evaluation: manual efforts vs automation (information retrieval, assets, evaluation, assessment,...)





NIS 2 & Cyber Resilience Act

- NIS 2 and CRA demand the establishment of a vulnerability management system
 - NIS2 - Article 21
The measures [...] shall include at least the following: [...] vulnerability handling and disclosure [...]
 - CRA – Annex I Part II
Manufacturers of products with digital elements shall: [...] share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities



How do you retrieve relevant security information?

There's a plethora of channels, formats, and content

- Various sources (vendors, agencies,...)
- Different means of transmission (email, feed, webpage,...)
- Several formats (.pdf, .txt,...)
- Manual effort (content, asset inventory, infrastructure,...)
- Risk assessment (criticality, affected vs not affected,...)





CSAF – Common Security Advisory Framework

- **Machine readable** Format for Security Advisories (JSON)
- **Open Source** (OS) and OS Tools available
- **Standardized** Format and standardized dissemination of Information
- **Automatable** retrieval and comparison
- Information about **relevant security updates and measures**
- **CSAF 2.1** is to be at the ready
- Many (big) companies provide CSAF





A jack of all trades for automated vulnerability management

Document level
metadata

Product tree

Vulnerabilities

```
1 {
2   "document": {
3     "title": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability",
4     "category": "Cisco Security Advisory",
5     "csaf_version": "2.0",
6     "publisher": {
13    "tracking": {
14      "id": "cisco-sa-20180328-smi2",
15      "status": "final",
16      "version": "3.0.0",
17      "revision_history": [
54        "initial_release_date": "2018-03-28T16:00:00Z",
55        "current_release_date": "2018-04-17T15:08:41Z",
56        "generator": {
61      }
62    },
63    "notes": [
114   "references": [
115     {
116       "url": "https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2",
117       "summary": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability"
118     }
119   ],
120   },
121   "product_tree": {
122     "branches": [
2466   ],
2467   },
2468   "vulnerabilities": [
2469     {
2470       "title": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability",
2471       "ids": [
2472         "CVE-2018-0171",
2473         "cisco-sa-20180328-smi2"
2474       ],
2475       "notes": [
2476         "cisco-sa-20180328-smi2"
2477       ],
2478       "cve": "CVE-2018-0171",
2479       "product_status": {
2480         "known_affected": [
2750         ]
2751       },
2752       "scores": [
3023       ],
3024       "remediations": [
3025       ],
3026       "references": [
3027     ]
2468   ]
2469 }
2470 }
```

Let's VEXinate your vulnerability management

VEX (Vulnerability Exploitability eXchange) is a profile in CSAF

Possible statements about the status of a vulnerability in CSAF:

- Fixed
- Known affected (+ action statement)
- Known not affected (+ impact statement)
- Under investigation



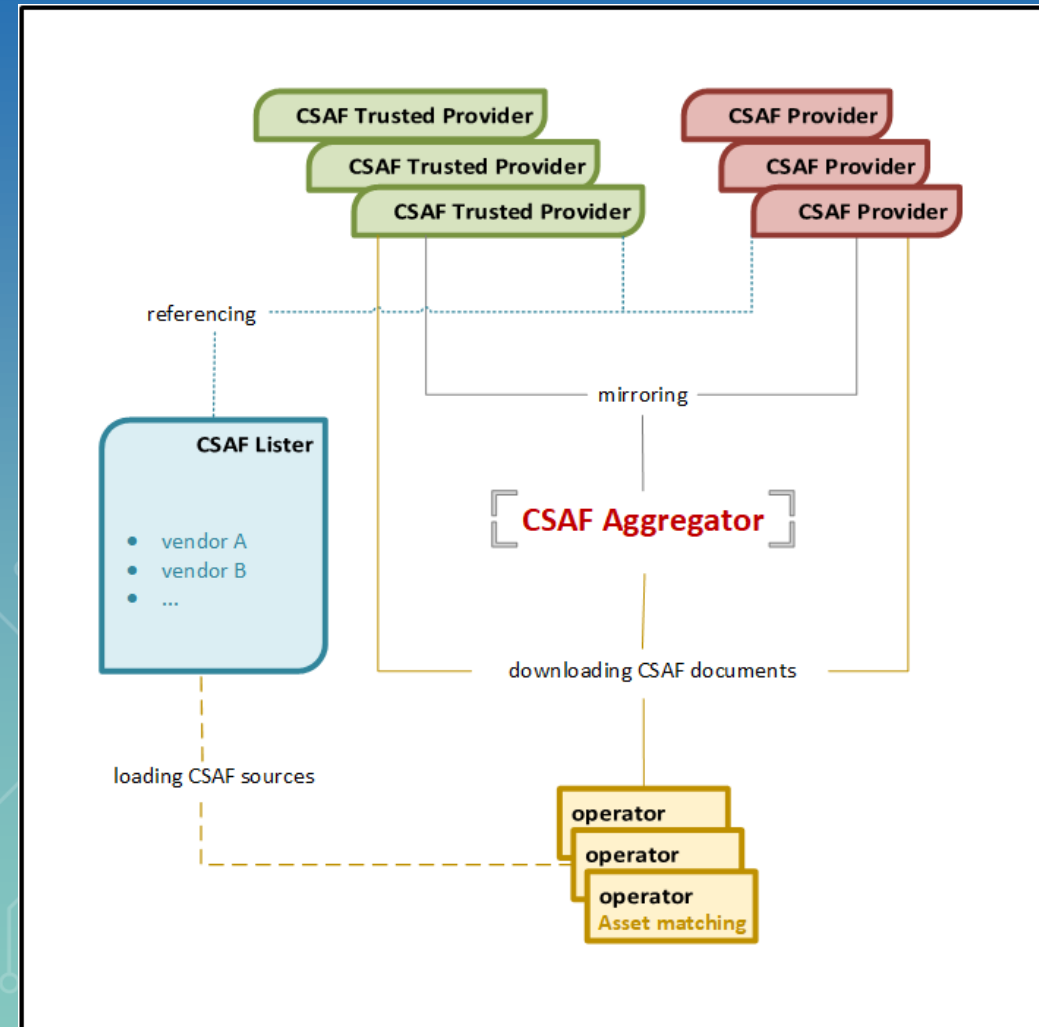


The BSI and CSAF: a passionate team

- Active participation and contribution in standardization
 - CSAF 2.0
 - CSAF 2.1
- Development and testing of OS tools and guidance material
 - Tools (Secvisogram, ISDuBA, CSAF trusted provider,...)
 - Technical guidance (e.g. TR-03191)
 - Publications
- Warning and security information service @BSI
 - Aggregation of Advisories from different sources/vendors (CSAF Aggregator @ BSI)
 - CSAF „yellow pages“ (CSAF Lister @ BSI)
- Hands-on workshops

CSAF in a nutshell

- Interaction between various OS tools
- Automatable retrieval and dissemination
- CSAF Aggregator @ BSI
- CSAF Lister @ BSI
- NCSC-NL as trusted provider





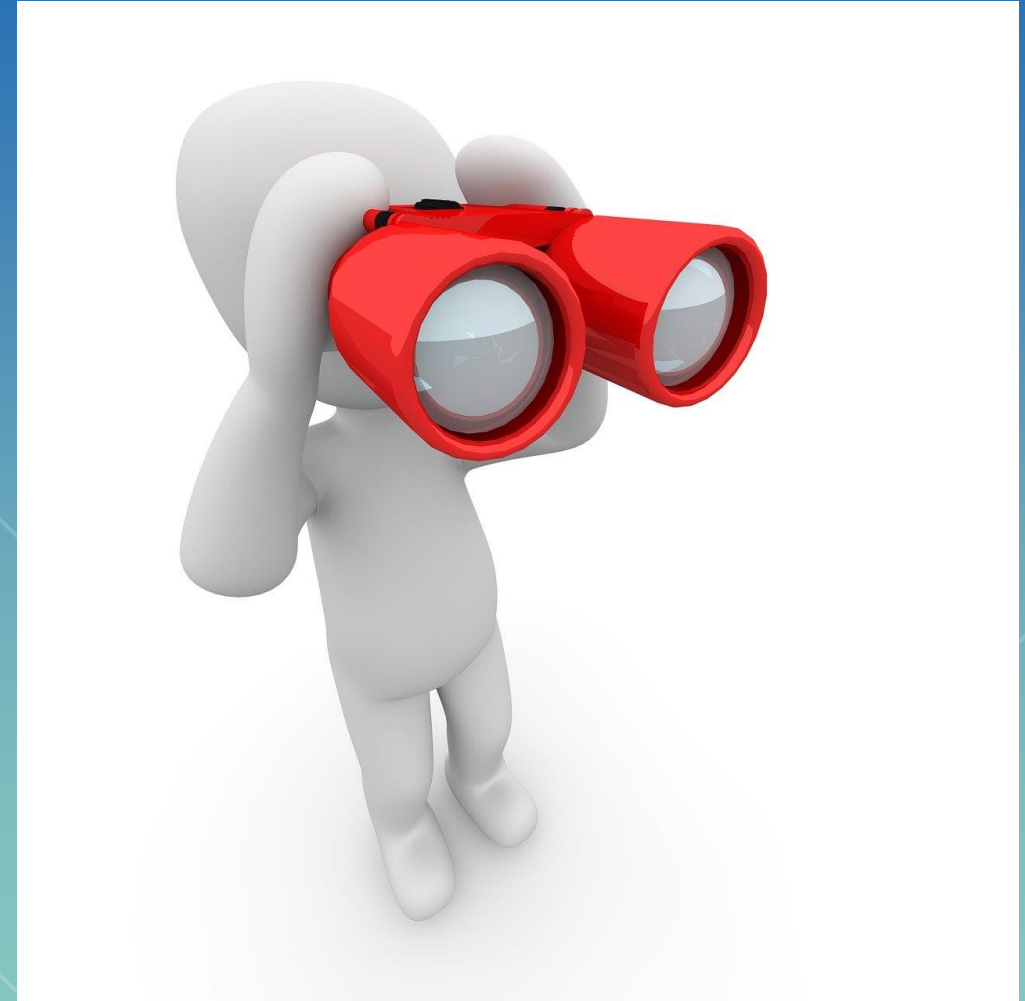
Who is issuing Advisories in CSAF?

Name	URL
BSI	https://wid.cert-bund.de/.well-known/csaf/
NCSC.nl*	https://vulnerabilities.ncsc.nl/csaf
CISA	https://github.com/cisagov/CSAF
cert@vde (35 companies)	https://certvde.com/de/more/csaf/
Microsoft, Redhat, Dell, Oracle, ...	Go to https://vendor-domain/.well-known/security.txt and look there
Siemens, Schneider Electric	

* By 01.04.2025 318518 CSAF Documents available

Who is consuming CSAF?

- Please don't do it manually
- Tools are still sparse / don't support CSAF
 - BSI is working on integration in DependencyTrack & netbox
- Please ask your supplier for providing CSAF





Key takeaways & actions

- Number of vulnerabilities discovered is rising
=> also the number of advisories
- Advisories are needed for risk-based decisions
- Automation is possible – so automate the boring stuff
- Request your vendors to provide CSAF
- Provide CSAF documents to your customers to ease their pain
- **Spread the word! #oCSAF #advisory**



Now to something completely different

that could solve a lot of issues:
Network Monitoring with Malcolm



Malcolm – A short introduction

- Developed by Idaho National Laboratory (INL)
- Only Open source tools
- Focus on ICS/OT network protocols
- Passive network Monitoring
- Quite Mature (BSI working with Malcolm since 2019)

Streamlined deployment:

Docker cluster, isolated modules & automation scripts

Secure communications:

Encrypted server, sensor & client communication

Permissive license:

Widely used open source tools

Malcolm

Powerfull traffic analysis:

Kibana, Moloch & Arkime

Easy to use:

Full PCAPS & Zeek logs

Expanding controll systems visibility:

Aim to provide parsers for ICS common protocols

Dutch Authority for Digital
Infrastructure
Ministry of Economic Affairs

National Cyber Security Centre
Ministry of Justice and Security

IACS Coalition



Under the hood – The usual suspects

- Zeek protocol dissectors
- Suricata IDS rulesets
- Arkime Network session monitoring
- Netbox Active asset inventory
- OpenSearch Stack Streamlined Data aggregation regardless of source



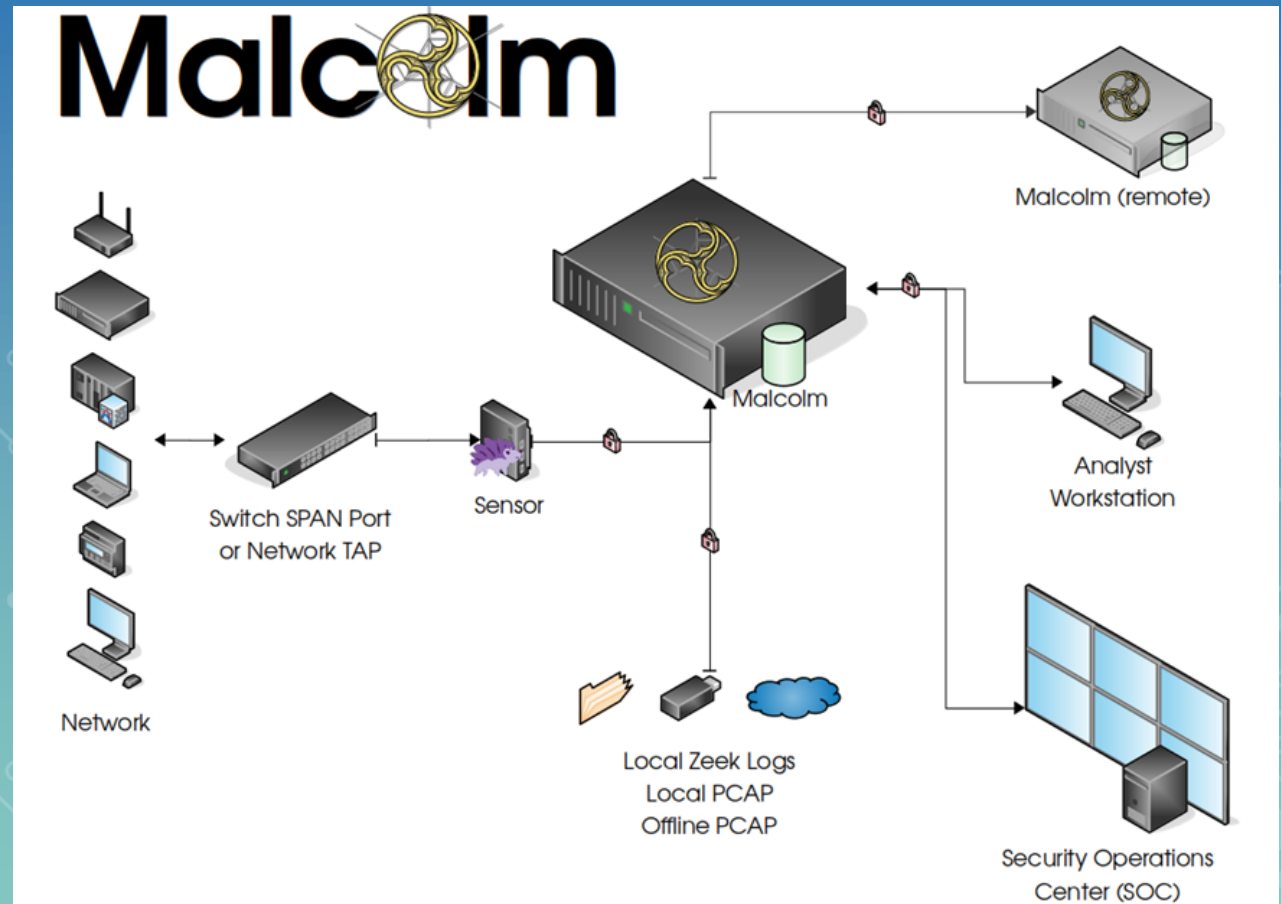
Malcolm

<https://github.com/cisagov/Malcolm>



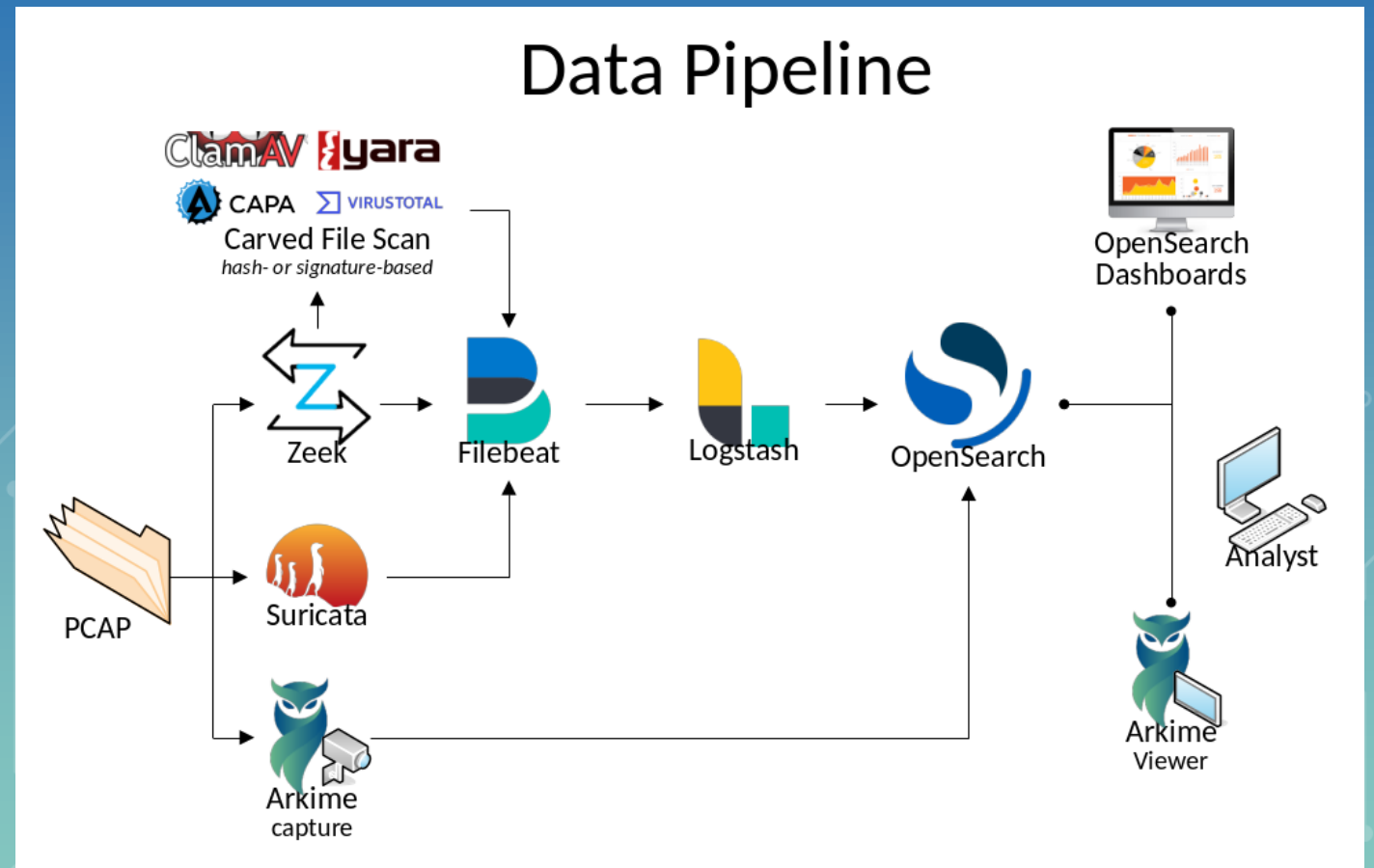
Deployment – Aimed at your needs

- **Deploy as you need it**
 - Full stack analysis: Malcolm (server)
 - Only data capturing: Hedgehog (sensor)
- **Scalable**
 - Forward Data from n Hedgehogs to Malcolm
 - Or from n Malcolms from to Malcolm
- **Remote Accessible**
 - Web UIs for SOCs and Analysts
 - User Management out of the Box
- **Live and offline Data injection**
 - Simultaneous Live and PCAP based data injections



Data Pipeline - Perfected Harmonie

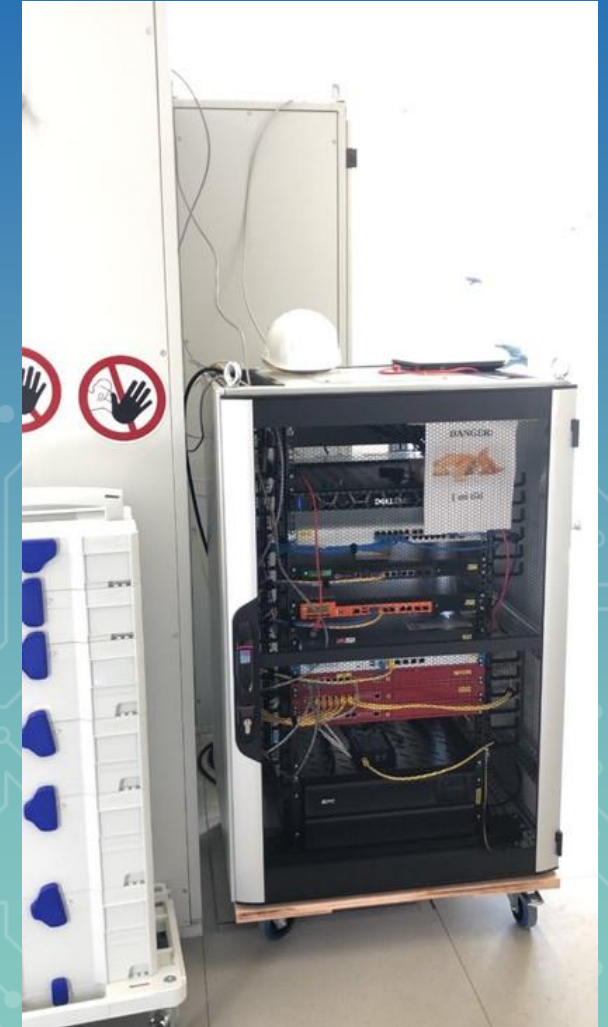
- Beats and Logstash harmonizing every input
- Integrated File carvers and scanners
- OpenSearch as base of truth for all Web-Interfaces
 - Kibana
 - Classic Log and alert inspection
 - Arkime (Viewer)
 - Session and communication analyses
 - Netbox
 - Your (automated) Asset Database





In the field Project MIDSE 🐱 ['mi:tʃə] (kitty)

- “Mobile Intrusion Detection System in Evaluation”
- Comparison of commercial NIDS and MALCOLM
 - Full packet capture in the OT network Level 1-3
 - Deep packet inspection of OT protocols
 - Network hygiene
 - Hands-On together with the operators





Mission Report - Where we went

5x	critical water sector, drinking water supply industry (2x network + 4x drinking water production)
4x	critical water sector, wastewater disposal industry (2x sewer + 2x wastewater treatment)
3x	critical energy sector, electricity industry (distribution networks)
1x	critical infrastructure, waste management sector (thermal treatment)
1x	critical transport & traffic sector, traffic control system
1x	critical infrastructure, health sector, patient monitoring
1x	building control system for pneumatic tube
2x	chemical industry, laboratory environments
1x	building control system with intruder alarm system / fire alarm system / access control / lighting / polder control / elevators / video / escape route control / media system / air conditioning / smoke extraction /...



Findings: Start with the basics

- Look what's going on: examine & monitor the network
- Understand the network and who's talking
- Network Hygiene, clean it up!
- Separation of networks (cloud and zero trust have to wait)
- IDS and SIEM/SOC are a good goal but not the first step



The day to day with Malcolm

Pro:

- + Easy application
- + Meaningful analyses
- + High level of detail

Operational gain of knowledge:

- Network hygiene is always worse than described by the operator
- There are always „low-hanging-fruits“
- An (old) Excel file is not a Asset Database
- „PCAP or it did not happen“ – data is everything

Con:

- (Still) missing parsers
- User with technical knowledge is expected



Malcolm as a PoC what is possible with CSAF

- **Goal: prioritization of patches and updates + filter necessity**
- **No strict naming convention**
(no unique product identifier exist, CPE no solution)
- **(Semi)automatically matching asset database with vendor's advisories**
 - BSI will publish lookup tables (string sysiphos) to ease the pain
- **Name of product in advisory <-> common names of the product (+spelling errors)**
 - Additional function classes (string atlas) for enhanced matching
 - Contribution system to community



Our Work – Improvement of Malcolm

- Preliminary Device Detection and Device Characterization (DDDC)
- Malcolm-Netbox Plugin for assisted device management
- Nmap scripts for OT device friendly information queries
- Network protocol Parsers for EU plants
 - HART-IP
 - IEC60870-5-104
 - IEC61850
 - GOOSE
 - SV
 - MMS



DINA-community – join the endeavor

DINA-community

Overview **Repositories** 5 Projects Packages People

Find a repository... Type Lang

- ot-parsers** (Public)
a collection of OT and ICS protocol parsers for Zeek
Zeek BSD-3-Clause 1 4 1 1 Updated 6 hours ago
- ot-assetdatabase** (Public)
Apache-2.0 0 0 0 0 Updated 2 weeks ago
- DDDC-Netbox-plugin** (Public)
The DDDC plugin for NetBox
Python Apache-2.0 0 1 0 0 Updated on Dec 21, 2023
- ot-nmap-scripts** (Public)
a collection of NMAP NSE scrips for OT protocols
Lua 0 1 0 0 Updated on Dec 21, 2023

DINA-community

Overview **Repositories** 5 Projects Packages People

README .md

About the project

The aim of the Detection and Identification of Network Assets (DINA) project is to improve the information of the active devices and their connections in industrial networks.

Central points to achieve this goal are

- Connection to [Malcolm](#),
- Cooperation with INL/CISA,
- feedback from operators and
- further development by the community.

In order to make this easier, software is published under licenses such as Apache 2.0 or BSD.

In terms of content, the following focal points arise, which are stored in the respective repositories:

- [Source of Truth](#)
- [Interface for different information sources](#)
- [Passive network analysis](#)
- [Active requests](#)

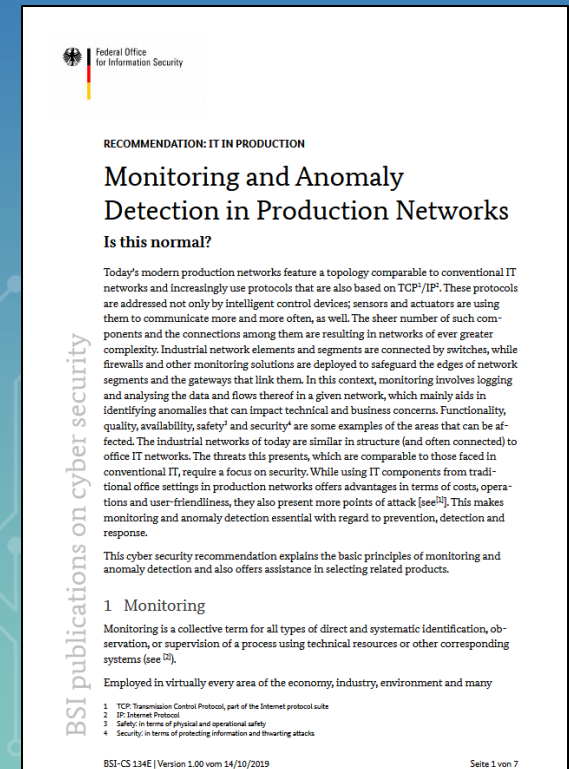
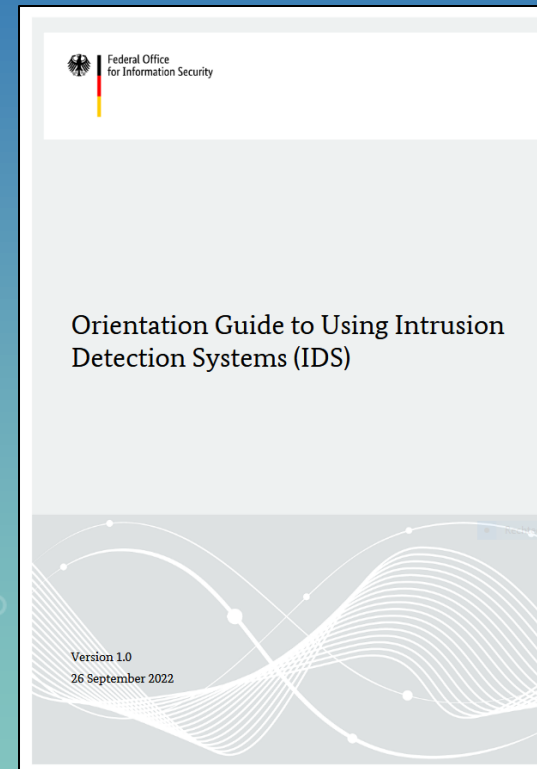
Source of Truth

The asset management tool [Netbox](#) serves as a user interface for capturing assets. The "[Device Detection and Device Characterization](#)" plugin is provided to enable the import of asset information from other sources (currently operator lists, Malcolm and experimental ML-...



Reading time – Our Papers

- Orientation Guide to Using Intrusion Detection Systems
- Monitoring and Anomaly Detection in Production Networks (BSI-CS 134)
 - revision planned:
 - Guideline for the creation of an individual catalogue of requirements
 - Carrying out several proofs of concepts



<https://www.bsi.bund.de/iacs>



Thank you for your attention!

Jens Cordt

Jens.cordt@bsi.bund.de

Federal Office for Information Security (BSI)

Godesberger Allee 87, 53175 Bonn

Germany

www.bsi.bund.de/iacs