TLP = CLEAR

OT Security in Sync:

A CSAF Template Powering ~~40~~ 45+ Vendors

Munich, December 13th, 2024

CERT@VDE
Web: https://certvde.com
Email: info@certvde.com

Jochen Becker
Information Security Manager

VDE CERT

Agenda

- Who?
  - CERT@VDE Partner
  - Tasks of CERT@VDE
- Why?
  - For the partners
  - For the consumers
  - For ourselves
- For what?
  - Number ranges
  - Variables and references
  - Documentation
  - The JSON Template

Who? CERT@VDE

- Founded in 2017 by 5 cooperation partners
- Coordinating PSIRT
- Standardizing work for small and medium-sized enterprises
- Under the umbrella of the non-profit VDE e.V.
- Memberships and collaboration in national and international working groups
- Continuous growth

CERT@VDE - a coordinating PSIRT for OT

KROHNE
PHOENIX CONTACT INSPIRING INNOVATIONS
VARTA
Miele
SMA SOLAR TECHNOLOGY
hilscher
BECKHOFF New Automation Technology
KUKA
WAGO
VEGA
baade M2M-Solutions
TRUMPF
PILZ THE SPIRIT OF SAFETY
CARLO GAVAZZI
Lenze
MURR ELEKTRONIK
auma Solutions for a world in motion
W&T www.WuT.de
E+H Endress+Hauser
ifm
PEPPERL+FUCHS
Helmholz COMPATIBLE WITH YOU
BUCHER automation
Weidmüller
FESTO
MB CONNECTLINE
swarco
CLAAS
K4 DIGITAL
adstec Industrial IT
BENDER
HARMAN A SAMSUNG COMPANY
GEA Engineering for a better world.
DURAG DURAG GROUP
FRAUSCHER
Dräger
YASKAWA
KEB
welotec a byte smarter
GROB
CODESYS
KEBA Automation by innovation.
HIMA SMART SAFETY.
EUCHNER More than safety.

- The global turnover generated by these partners was about 75 billion euros in 2022.
- A lot of Hidden champions: Some of the companies are world market leaders in specific sectros

Tasks of CERT@VDE

- Support with the drafting of advisories
  - Best practices and training
  - Assessment of vulnerabilities (especially CVSS and CWEs)
  - Coordination with supply chain, reporters etc.
  - Publication
- Networking and exchange
  - Among each other in workshops and working meetings
  - Representing the partners, for example at CERT-VERBUND, TI, FIRST etc.
- Provision of infrastructure
  - For processing (ticket system, file drops, toolbox,...)
  - For CSAF publication (trusted provider per partner, aggregator together)
- CVE Numbering Authority (CNA) for the partners

Funding project of the Federal Ministry of Education and Research: „ZenSim 4.0“

Centralized and simplified management of Incidents and vulnerabilities for SME

ZenSIM Industrie 4.0

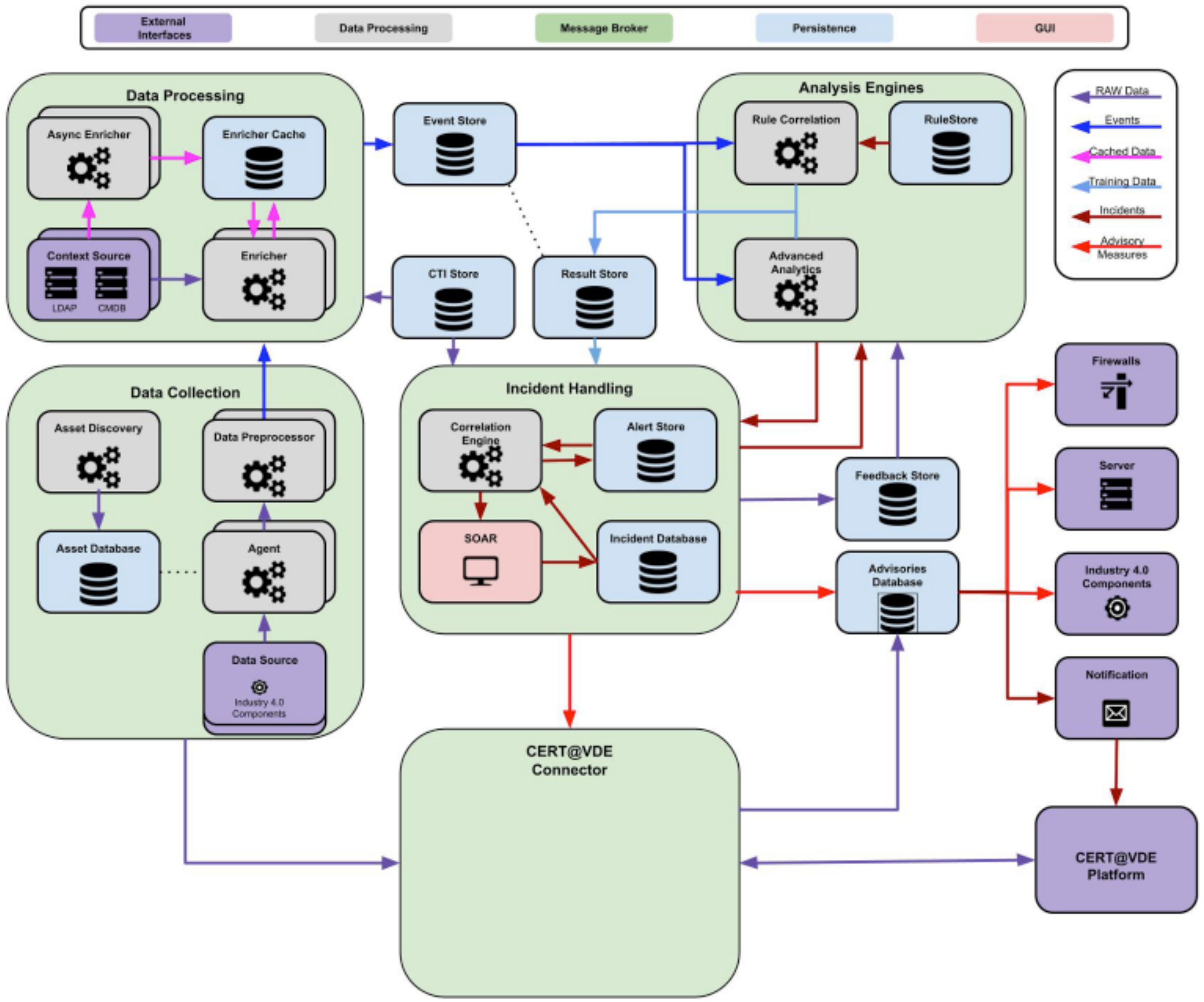


Abbildung 12: Teilbereich der Gesamtarchitektur mit Datenaufnahme, -aufbereitung und -analyse¶

PROJEKTINFORMATION

Verbundkoordinator

DECOIT GmbH, Bremen

Partner

- Hochschule Bremen
- VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V., Frankfurt am Main

Volumen

1,57 Mio. € (davon 81% Förderanteil durch BMBF)

Laufzeit

10/2021 - 09/2024

Bekanntmachung

KMU-innovativ

Bundesministerium
für Bildung
und Forschung

VDE CERT

Why? For the partners

- Handout to make it easier to get started
- Meet the minimum requirements of CSAF
- Check off the CSAF checklist
- Transfer CSAF experience from CERT@VDE to PSIRTS
- Combined with trainings and workshops for partners

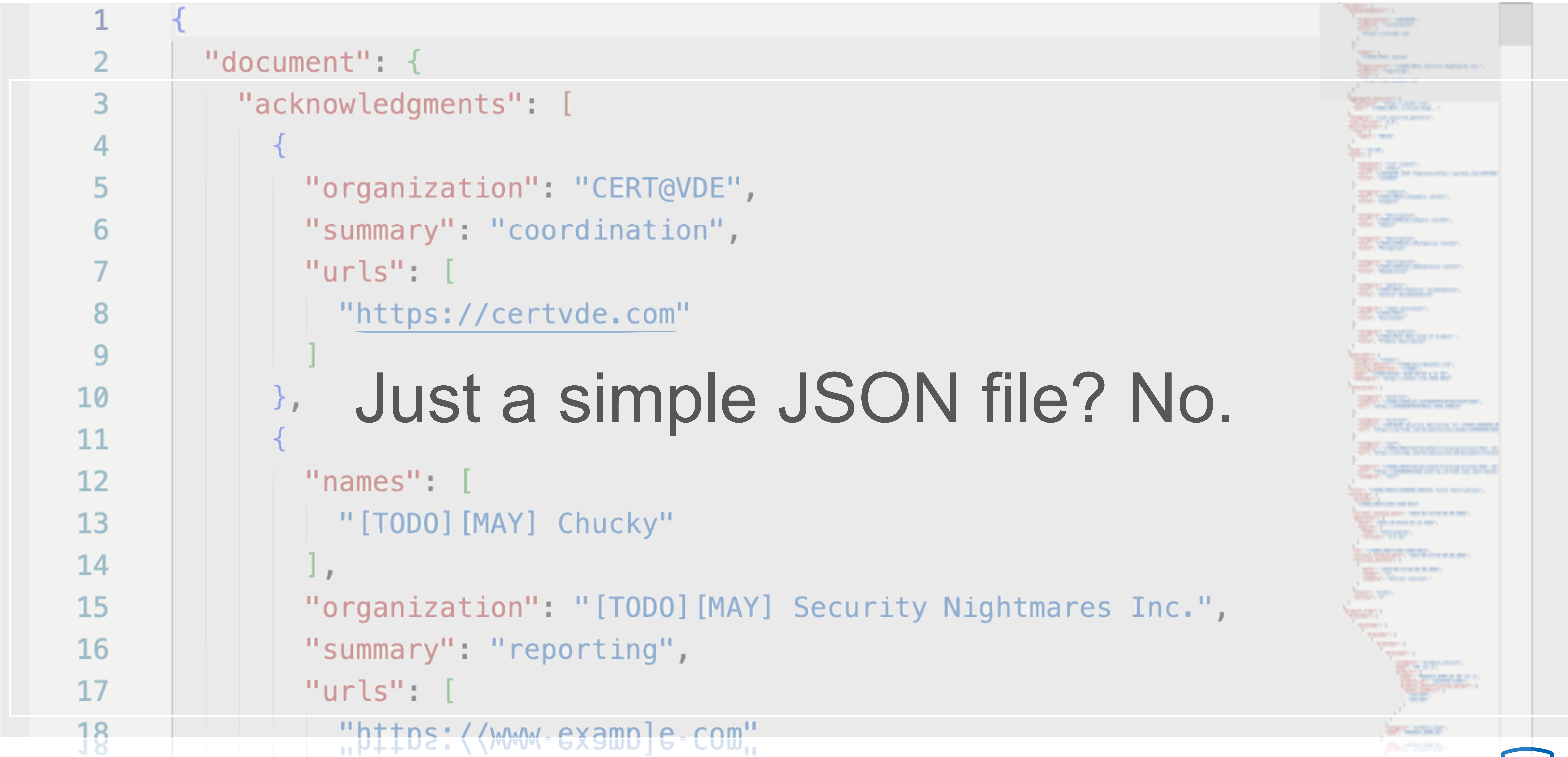
Why? For the consumers

- Standardized processing of CSAFs from CERT@VDE partners
  - For example
    - ...the product_identification_helper
    - ...the Remediations
    - ...the document notes
- High attention to machine processing, but still human-readable
  - the contents of our previous HTML advisories are available in the resulting document
  - the generation of HTML or Markdown documents from the CSAF must always be possible.

Why? For ourselves

- Simplification of processes through standards
- Basis also for the generation of HTML versions on certvde.com
- Automated check using CI/CD pipeline
- The manual, technical check has also been simplified (see number ranges)
- All partner requirements for an advisory seem to have been met so far
- Reduced training and support effort

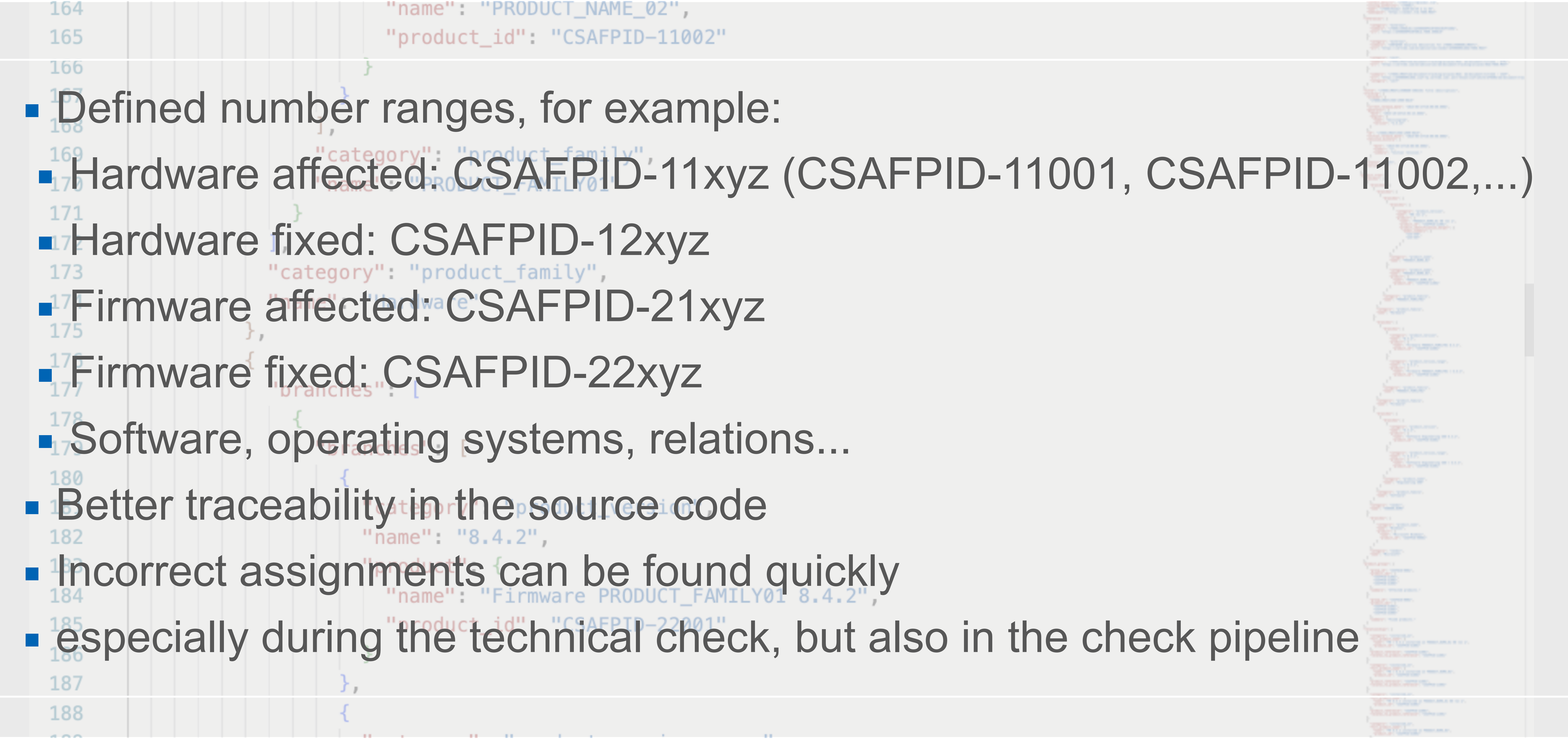
For what?



```
{
  "document": {
    "acknowledgments": [
      {
        "organization": "CERT@VDE",
        "summary": "coordination",
        "urls": [
          "https://certvde.com"
        ]
      },
      {
        "names": [
          "[TODO][MAY] Chucky"
        ],
        "organization": "[TODO][MAY] Security Nightmares Inc.",
        "summary": "reporting",
        "urls": [
          "https://www.example.com"
```

Just a simple JSON file? No.

Number ranges

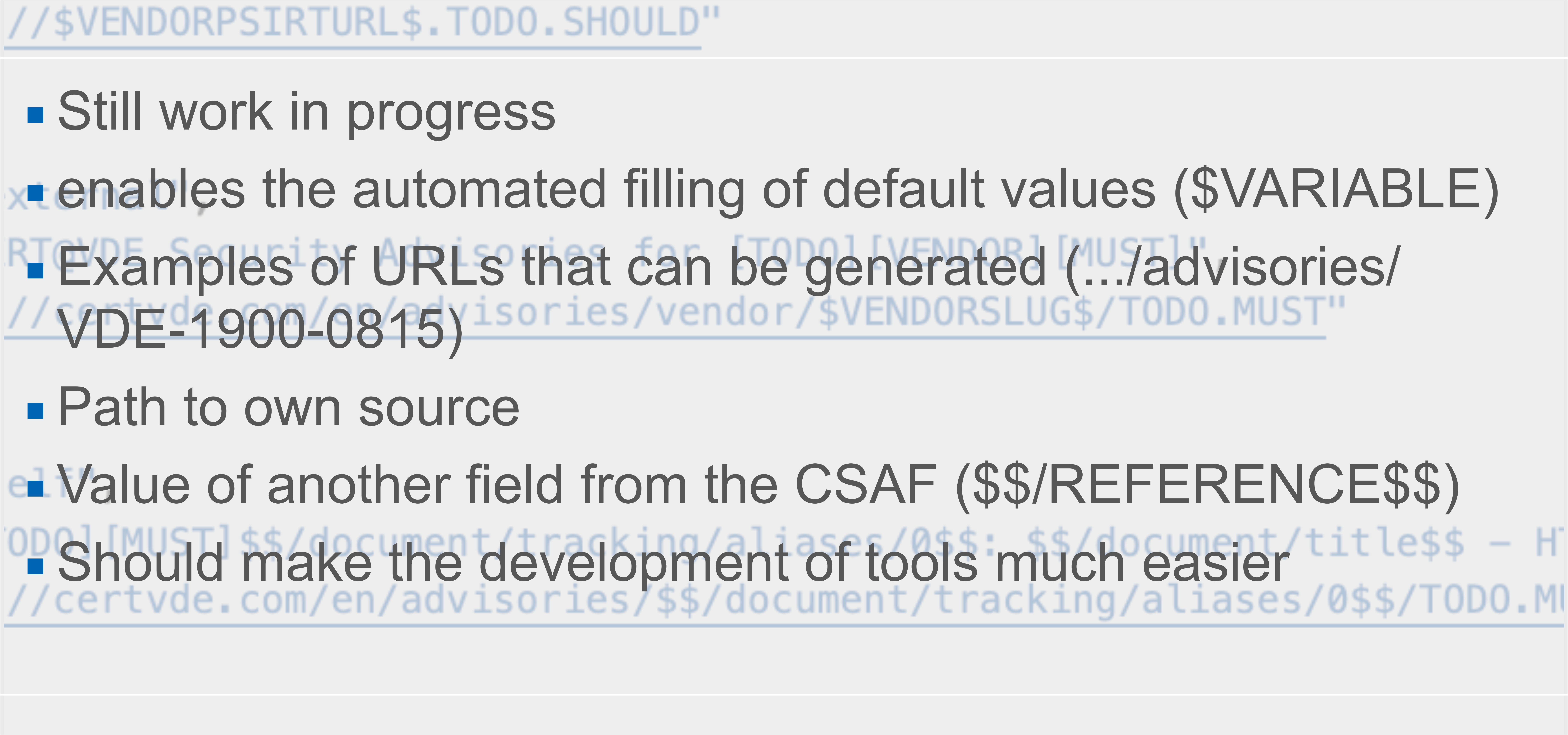


```
            "name": "PRODUCT_NAME_02",
            "product_id": "CSAFPID-11002"
          }
      },
      "category": "product_family",
      "name": "PRODUCT_FAMILY01"
    }
  ],
  "category": "product_family",
  "name": "Hardware"
},
{
  "branches": [
    {
      "branches": [
        {
          "category": "product_version",
          "name": "8.4.2",
          "product": {
            "name": "Firmware PRODUCT_FAMILY01 8.4.2",
            "product_id": "CSAFPID-22001"
          }
        },
        {
```

- Defined number ranges, for example:
  - Hardware affected: CSAFPID-11xyz (CSAFPID-11001, CSAFPID-11002,...)
  - Hardware fixed: CSAFPID-12xyz
  - Firmware affected: CSAFPID-21xyz
  - Firmware fixed: CSAFPID-22xyz
  - Software, operating systems, relations...
- Better traceability in the source code
- Incorrect assignments can be found quickly
- especially during the technical check, but also in the check pipeline

Variables

- Still work in progress
- enables the automated filling of default values ($VARIABLE)
- Examples of URLs that can be generated (.../advisories/VDE-1900-0815)
- Path to own source
- Value of another field from the CSAF ($$/REFERENCE$$)
- Should make the development of tools much easier



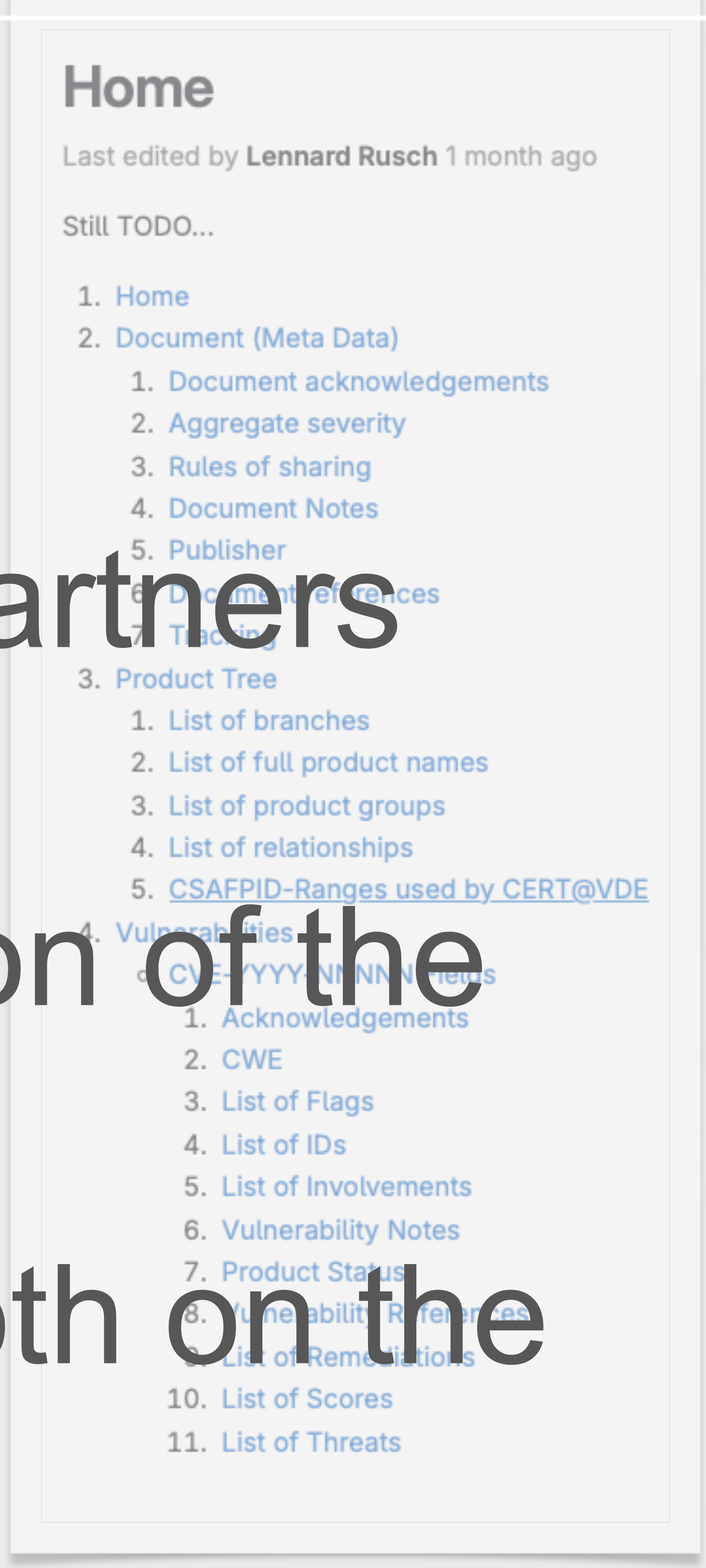
```
//$VENDORPSIRTURL$.TODO.SHOULD"

xternal",
RTCVDE Security Advisories for [TODO][VENDOR][MUST]",
//certvde.com/en/advisories/vendor/$VENDORSLUG$/TODO.MUST"

el",
ODO][MUST] $$/document/tracking/aliases/0$$: $$/document/title$$ – H
//certvde.com/en/advisories/$$/document/tracking/aliases/0$$/TODO.MU
```

Documentation

- Always about one release behind, of course ;)
- Deals preferentially with the topics for which our partners have made requests
- Despite “expandability” already noticeable reduction of the support volume
- Collaboration on issues, forks, merge requests, both on the project and on the documentation/wiki



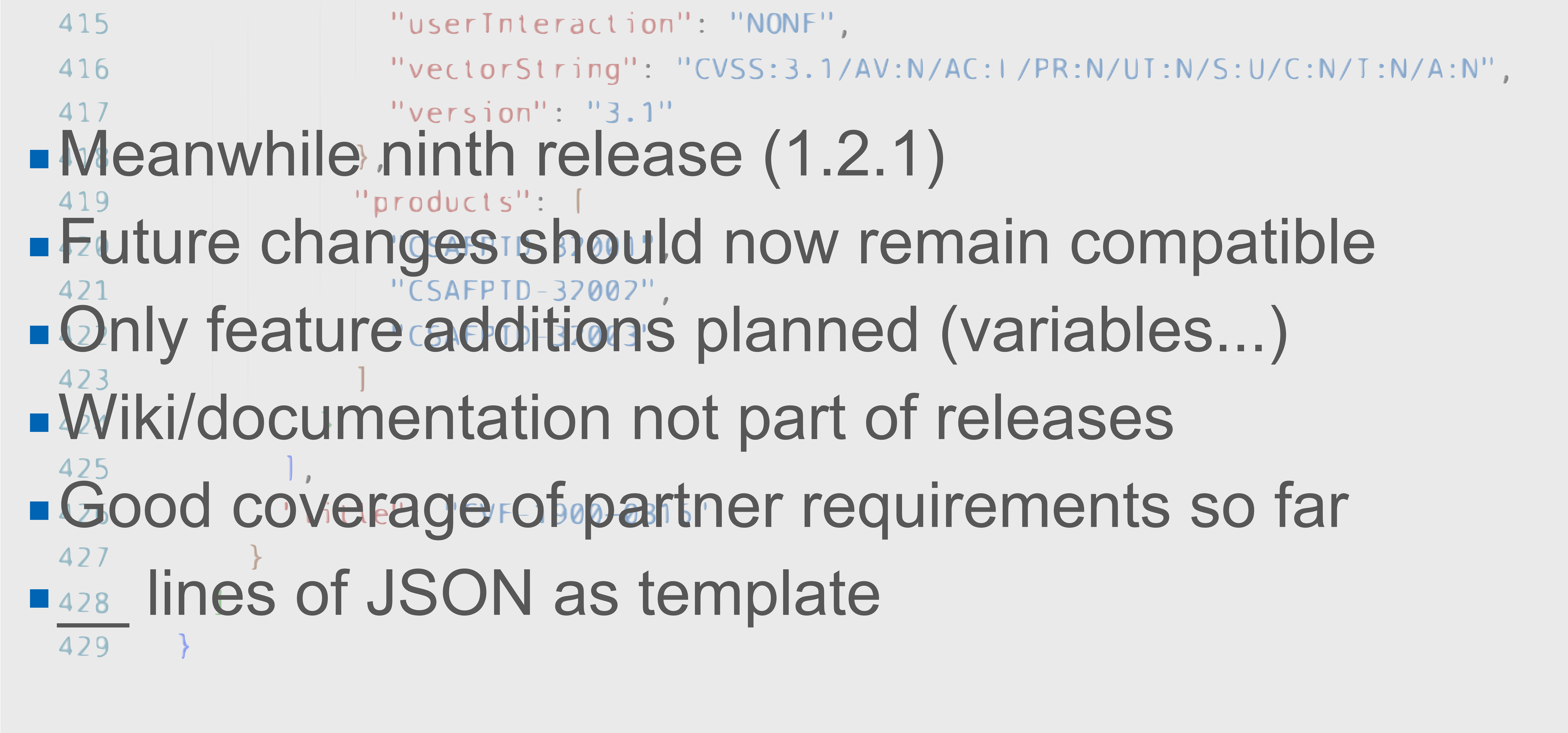
Home

Last edited by **Lennard Rusch** 1 month ago

Still TODO...

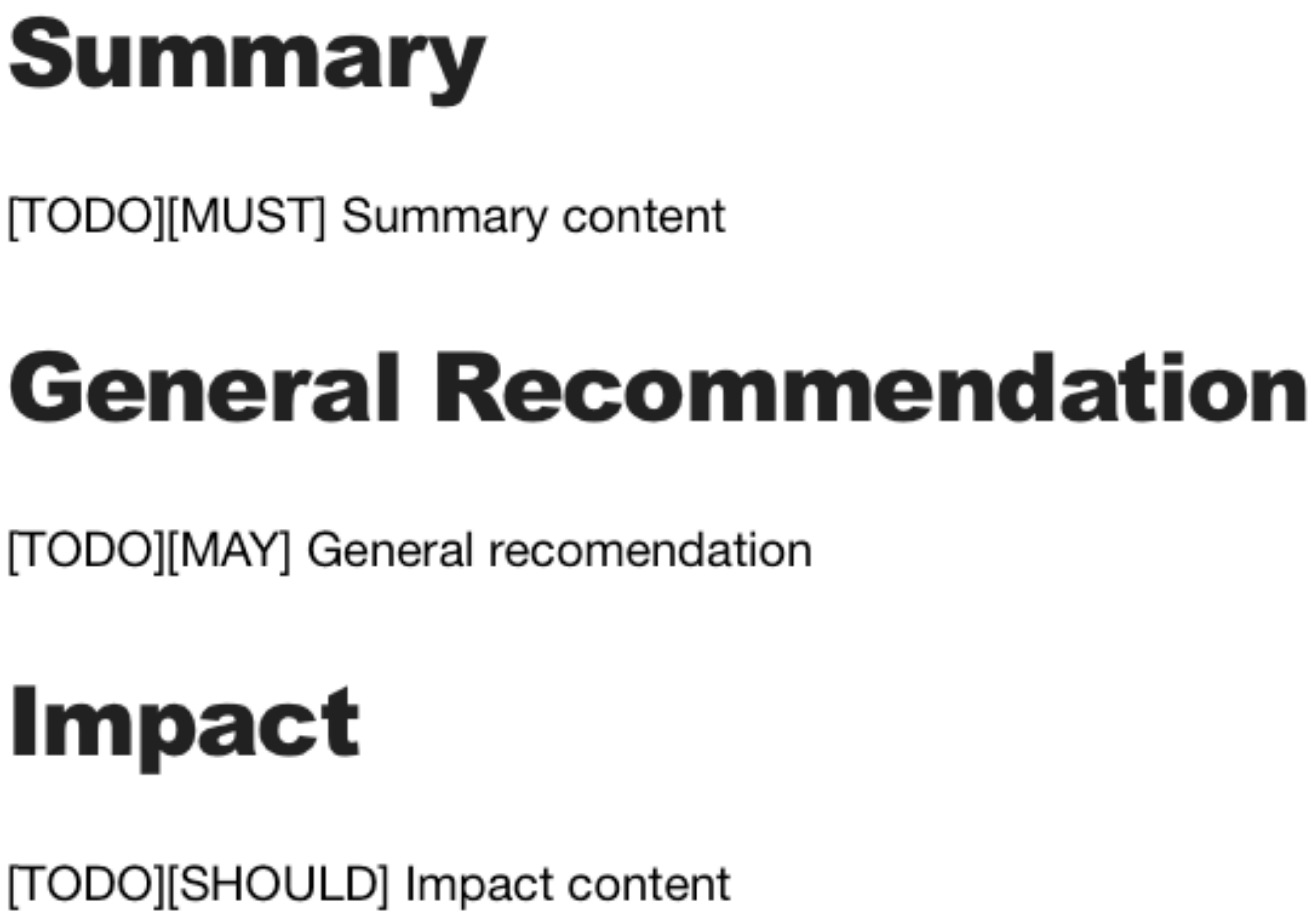
1. Home
2. Document (Meta Data)
   1. Document acknowledgements
   2. Aggregate severity
   3. Rules of sharing
   4. Document Notes
   5. Publisher
   6. Document References
   7. Tracking
3. Product Tree
   1. List of branches
   2. List of full product names
   3. List of product groups
   4. List of relationships
   5. CSAFPID-Ranges used by CERT@VDE
4. Vulnerabilities
   - CVE-YYYY-NNNNN Fields
     1. Acknowledgements
     2. CWE
     3. List of Flags
     4. List of IDs
     5. List of Involvements
     6. Vulnerability Notes
     7. Product Status
     8. Vulnerability References
     9. List of Remediations
     10. List of Scores
     11. List of Threats

JSON File



```
                "userInteraction": "NONE",
                "vectorString": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N",
                "version": "3.1"
              },
              "products": [
                "CSAFPID-32001",
                "CSAFPID-32002",
                "CSAFPID-32003"
              ]
            }
          ],
          "title": "CVE-1900-0315"
        }
      ]
    }
```

- Meanwhile ninth release (1.2.1)
- Future changes should now remain compatible
- Only feature additions planned (variables...)
- Wiki/documentation not part of releases
- Good coverage of partner requirements so far
- ____ lines of JSON as template



Summary

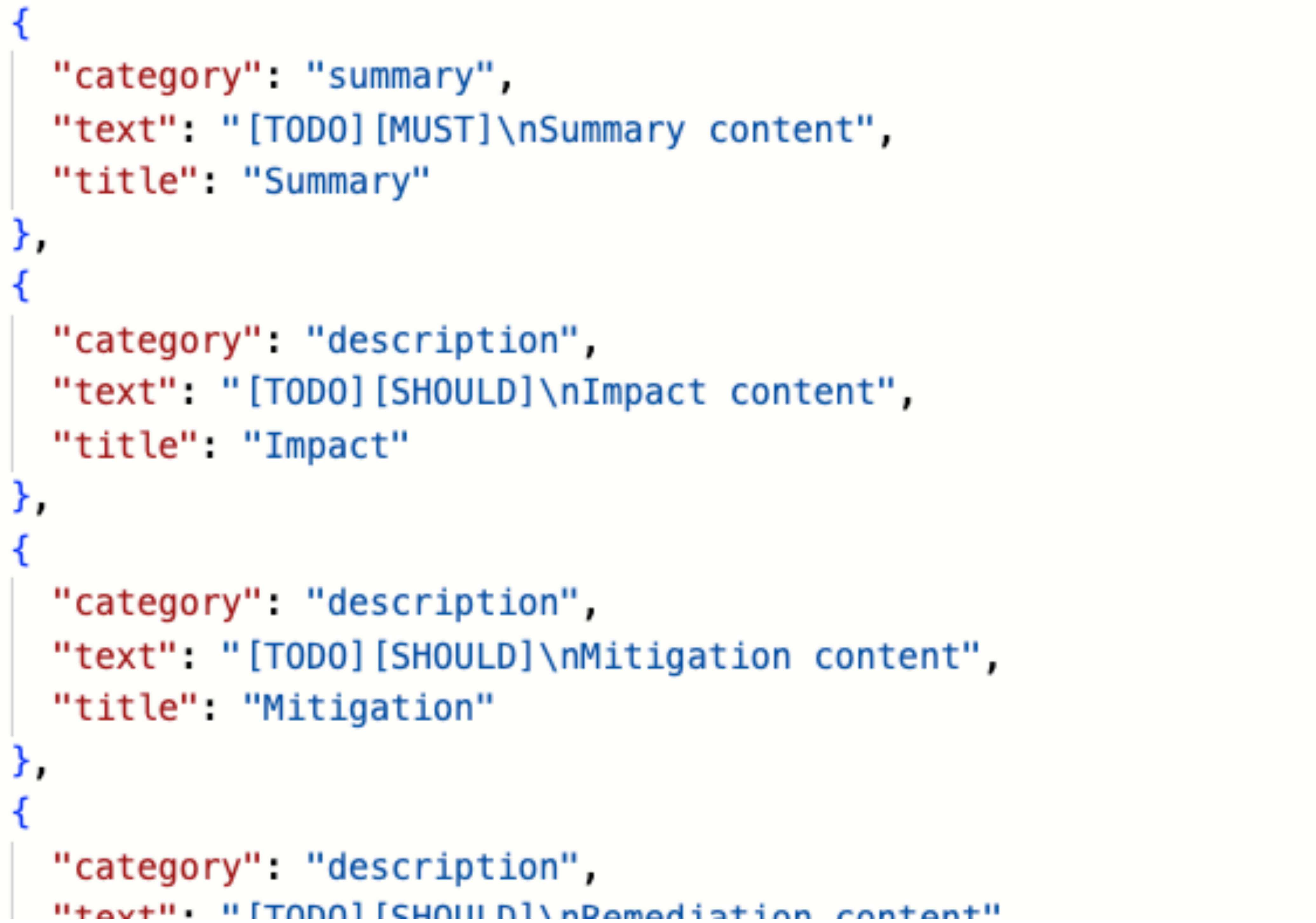
[TODO][MUST] Summary content

General Recommendation

[TODO][MAY] General recomendation

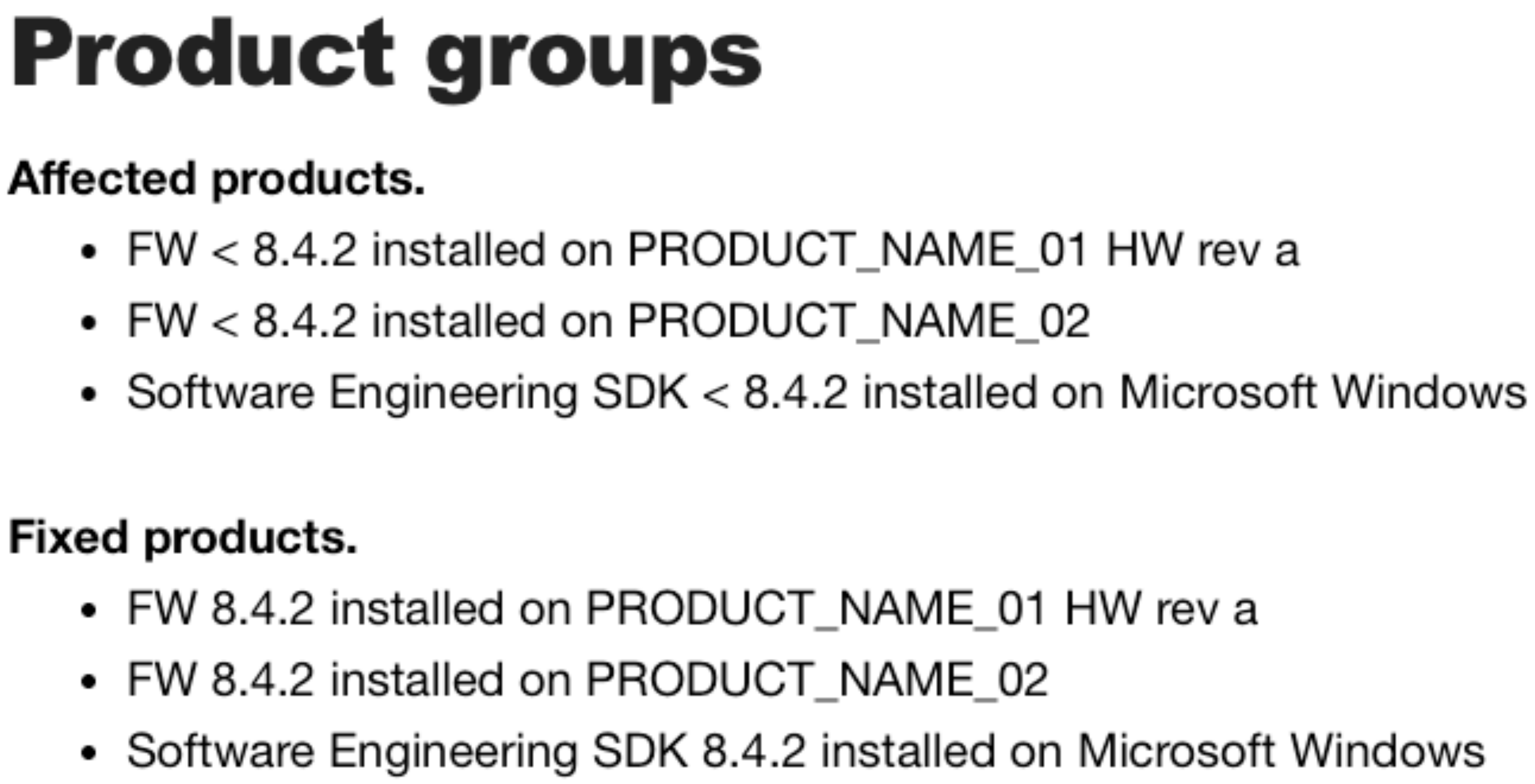
Impact

[TODO][SHOULD] Impact content



```
{
  "category": "summary",
  "text": "[TODO][MUST]\nSummary content",
  "title": "Summary"
},
{
  "category": "description",
  "text": "[TODO][SHOULD]\nImpact content",
  "title": "Impact"
},
{
  "category": "description",
  "text": "[TODO][SHOULD]\nMitigation content",
  "title": "Mitigation"
},
{
  "category": "description",
  "text": "[TODO][SHOULD]\nRemediation content"
```

Terms according to rfc2119



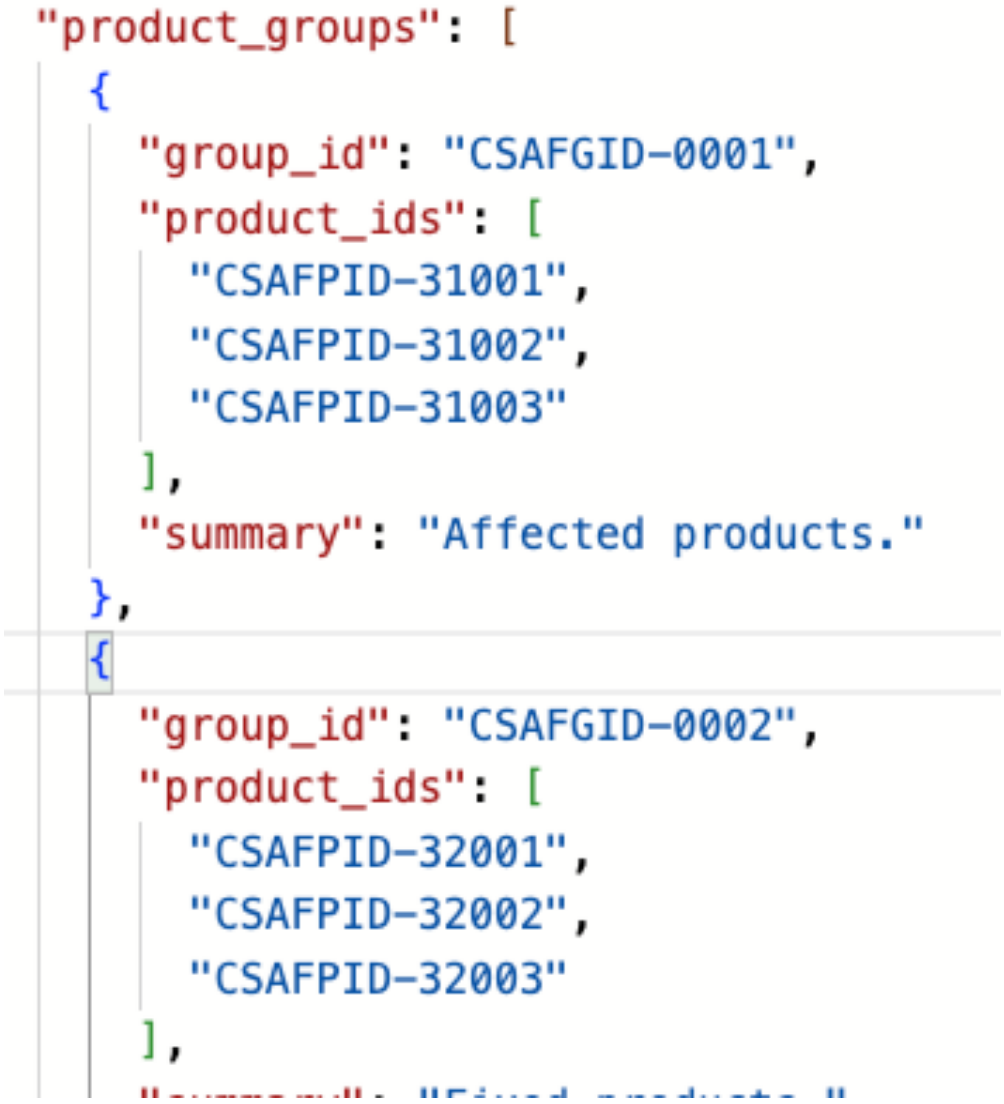
Product groups

Affected products.

- FW < 8.4.2 installed on PRODUCT_NAME_01 HW rev a
- FW < 8.4.2 installed on PRODUCT_NAME_02
- Software Engineering SDK < 8.4.2 installed on Microsoft Windows

Fixed products.

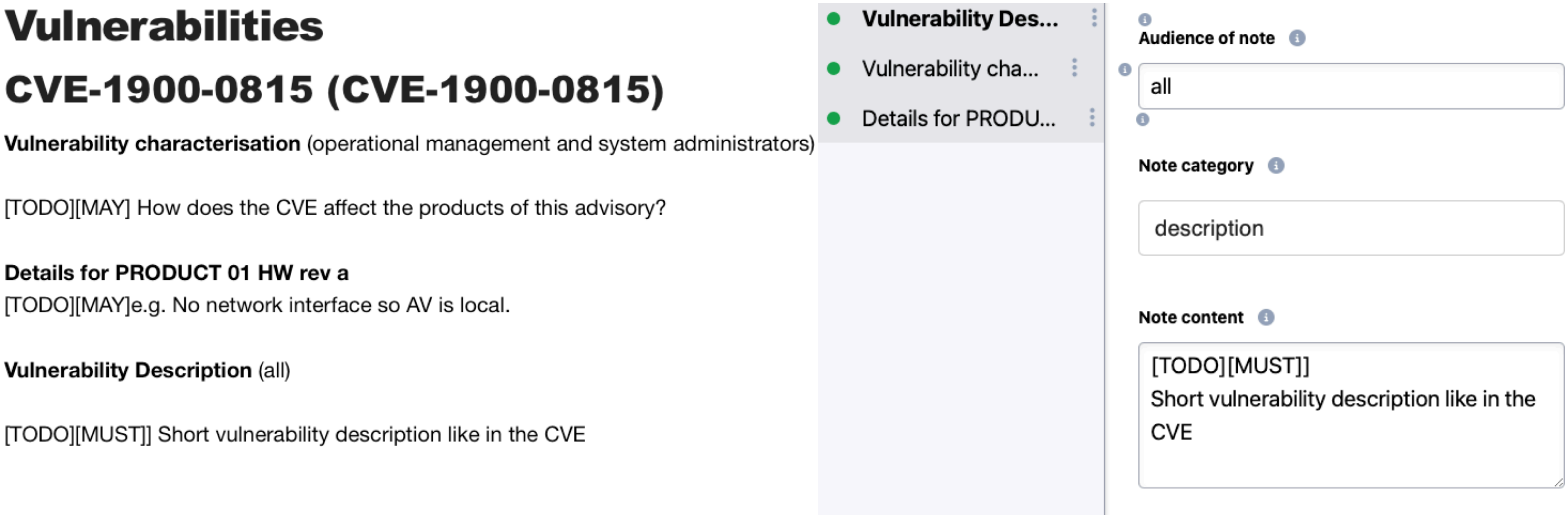
- FW 8.4.2 installed on PRODUCT_NAME_01 HW rev a
- FW 8.4.2 installed on PRODUCT_NAME_02
- Software Engineering SDK 8.4.2 installed on Microsoft Windows



```
"product_groups": [
  {
    "group_id": "CSAFGID-0001",
    "product_ids": [
      "CSAFPID-31001",
      "CSAFPID-31002",
      "CSAFPID-31003"
    ],
    "summary": "Affected products."
  },
  {
    "group_id": "CSAFGID-0002",
    "product_ids": [
      "CSAFPID-32001",
      "CSAFPID-32002",
      "CSAFPID-32003"
    ],
    "summary": "Fixed products."
```

As far as possible: build groups

Two members minimum!



Vulnerabilities

CVE-1900-0815 (CVE-1900-0815)

Vulnerability characterisation (operational management and system administrators)

[TODO][MAY] How does the CVE affect the products of this advisory?

Details for PRODUCT 01 HW rev a

[TODO][MAY]e.g. No network interface so AV is local.

Vulnerability Description (all)

[TODO][MUST]] Short vulnerability description like in the CVE

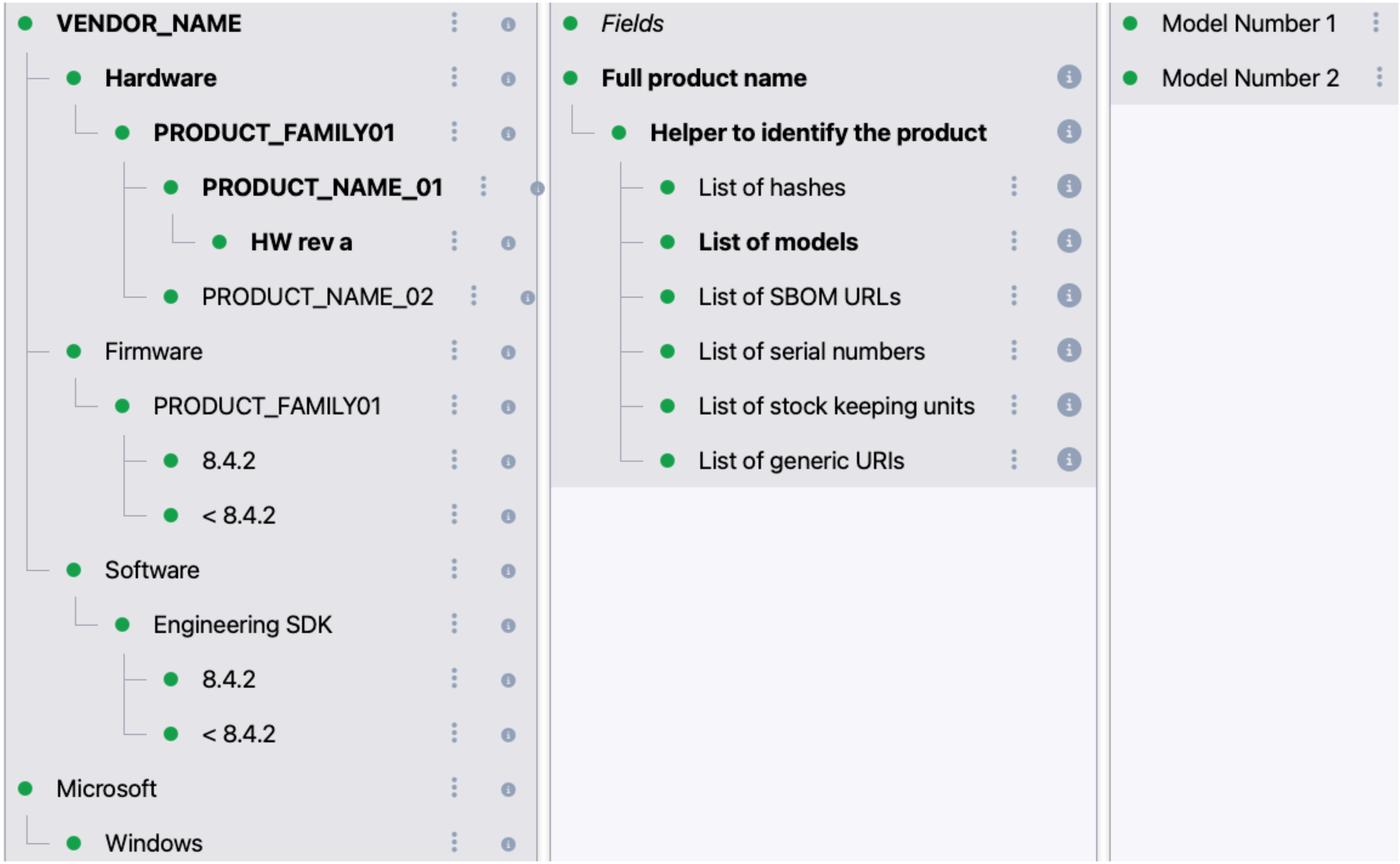
Audience of note: all

Note category: description

Note content: [TODO][MUST]] Short vulnerability description like in the CVE

CVEs next steps: Variables

Already in testing. Simplifies import of cve.org

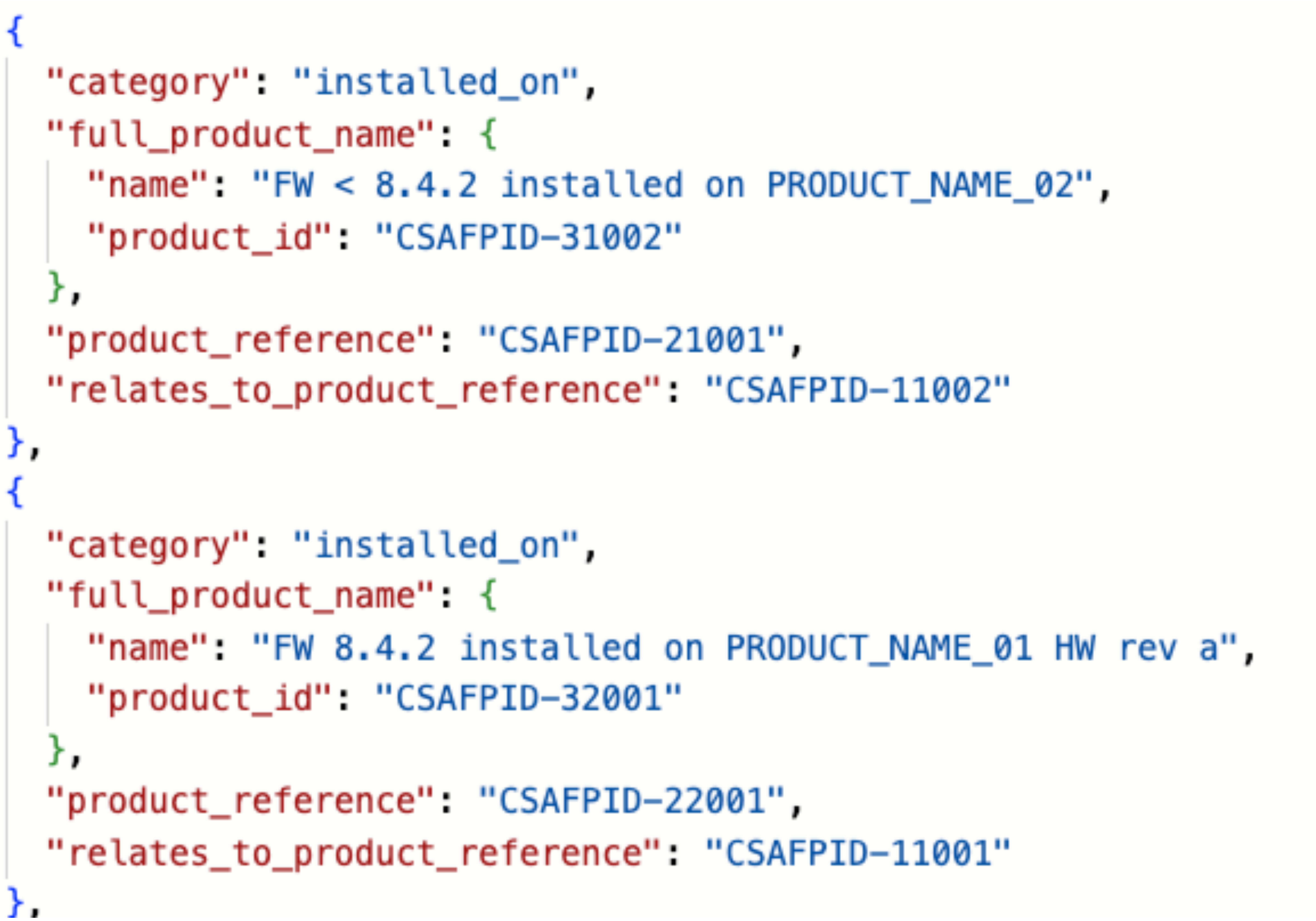


- **VENDOR_NAME**
  - **Hardware**
    - **PRODUCT_FAMILY01**
      - **PRODUCT_NAME_01**
        - **HW rev a**
      - PRODUCT_NAME_02
  - Firmware
    - PRODUCT_FAMILY01
      - 8.4.2
      - < 8.4.2
  - Software
    - Engineering SDK
      - 8.4.2
      - < 8.4.2
- Microsoft
  - Windows

- *Fields*
- **Full product name**
  - **Helper to identify the product**
    - List of hashes
    - **List of models**
    - List of SBOM URLs
    - List of serial numbers
    - List of stock keeping units
    - List of generic URIs

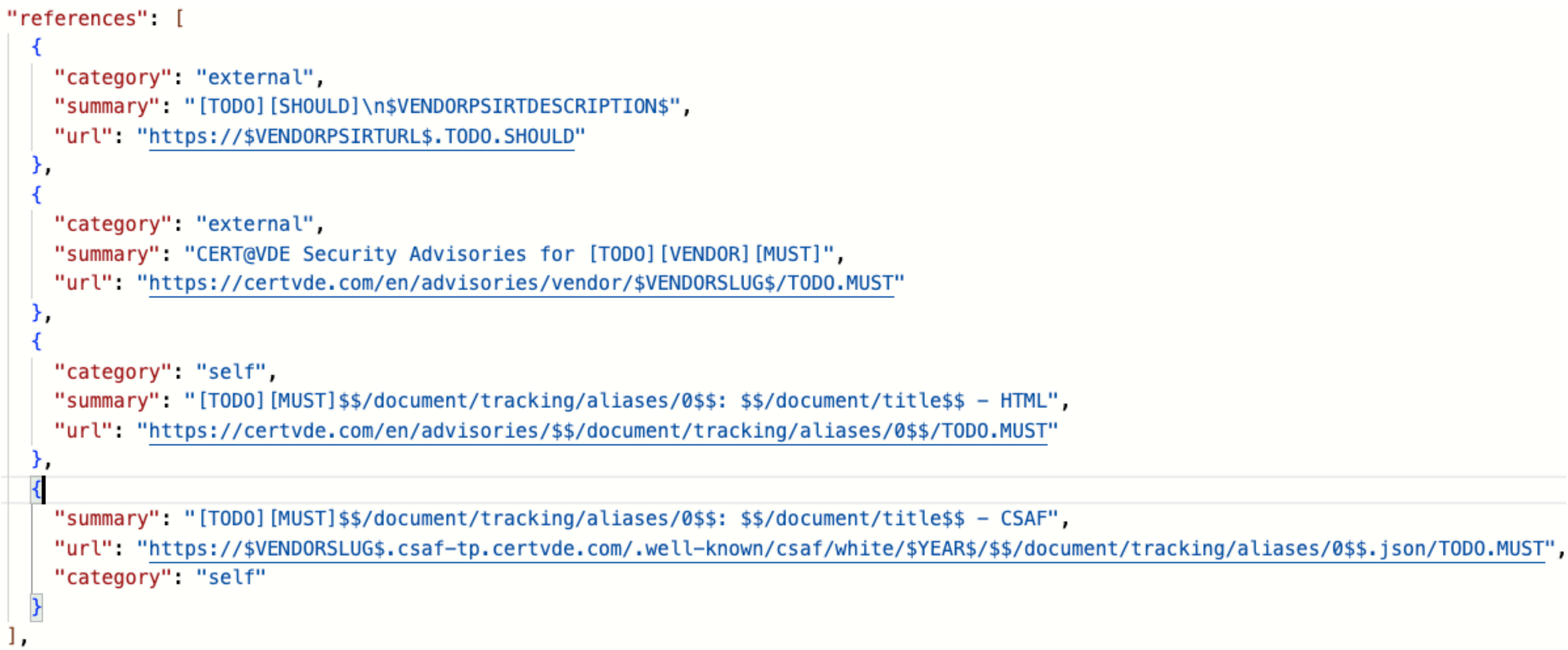
- Model Number 1
- Model Number 2

Product Tree: Represents typical ICS/OT trees
Separation of Hard- and Software



```
{
  "category": "installed_on",
  "full_product_name": {
    "name": "FW < 8.4.2 installed on PRODUCT_NAME_02",
    "product_id": "CSAFPID-31002"
  },
  "product_reference": "CSAFPID-21001",
  "relates_to_product_reference": "CSAFPID-11002"
},
{
  "category": "installed_on",
  "full_product_name": {
    "name": "FW 8.4.2 installed on PRODUCT_NAME_01 HW rev a",
    "product_id": "CSAFPID-32001"
  },
  "product_reference": "CSAFPID-22001",
  "relates_to_product_reference": "CSAFPID-11001"
},
```

Relations, to link Hardware with Firmware



```
"references": [
  {
    "category": "external",
    "summary": "[TODO][SHOULD]\n$VENDORPSIRTDESCRIPTION$",
    "url": "https://$VENDORPSIRTURL$.TODO.SHOULD"
  },
  {
    "category": "external",
    "summary": "CERT@VDE Security Advisories for [TODO][VENDOR][MUST]",
    "url": "https://certvde.com/en/advisories/vendor/$VENDORSLUG$/TODO.MUST"
  },
  {
    "category": "self",
    "summary": "[TODO][MUST]$$/document/tracking/aliases/0$$: $$/document/title$$ - HTML",
    "url": "https://certvde.com/en/advisories/$$/document/tracking/aliases/0$$/TODO.MUST"
  },
  {
    "summary": "[TODO][MUST]$$/document/tracking/aliases/0$$: $$/document/title$$ - CSAF",
    "url": "https://$VENDORSLUG$.csaf-tp.certvde.com/.well-known/csaf/white/$YEAR$/$$/document/tracking/aliases/0$$.json/TODO.MUST",
    "category": "self"
  }
],
```

$Variable$ versus $$Reference$$

In addition

- Training for our partners
- Development and exchange of tools and best practices
  - Idea of a lightweight editor
  - Test pipeline for quality control based on Gitlab CICD
  - More to come
- Maintaining the repository and documentation
- https://github.com/CERTVDE/CSAF-Template
- Documentation and wiki to come, currently only partner-internal (work in progress)