Securing the Supply Chain Together – Through Automation of Advisories and Vulnerability Management

Jens Wiesner & Thomas Schmidt
Federal Office for Information Security (BSI)
Who are we?

Jens Wiesner

Team Lead ICS @BSI
(traveling presenter,
Saying important things to important people)

Responsible for Critical Infrastructure Protection
• Publishing Best Practices
• Assessing impact of vulnerabilities in CI
• Making the world a better place

Thomas Schmidt

Technical ICS Analyst @BSI
(usually not into standardization)

First day at work: analyze TRITON / TRISIS
Passion for
• ICS
• International Cooperation
• CVD
• Capacity building
Difference between Vulnerabilities and Advisories

**Vulnerability (CVE)**
- Can be discovered by anybody
  - Security researcher (hacker)
  - Vendor
  - User
- Usually for one product (although much more may be affected)
- Coordinated Vulnerability Disclosure Program should be established by the vendor, ([BSI Publication on Vulnerability Handling](https://bsi.bund.de/de/aktuelles/publikationen/handling-der-vulnerabilitaeten.html))
- Huge amount published each year in NVD > 28000 in 2021
- Use **RFC 9116** (security.txt)

**Advisory**
- Usually supplied by the vendor / maintainer of the software
- May cover multiple CVE
- Describes Patch and/or Mitigating countermeasures
- Takes some time to publish
- Often part of a support agreement

[Click here](https://opensourcesecurity.io/2021/03/30/itstime-to-fix-cve/)

Securing the Supply Chain Together – Through Automation of Advisories and Vulnerability Management | Jens Wiesner & Thomas Schmidt
Target audience should be interested in advisories

<table>
<thead>
<tr>
<th>How to</th>
<th>Producer of Vulnerability Reports</th>
<th>Advisories</th>
<th>Consumer of Vulnerability Reports</th>
<th>Advisories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write</td>
<td>o</td>
<td>++</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Generate</td>
<td>o</td>
<td>++</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Automate</td>
<td>o</td>
<td>++</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Upload / Publish</td>
<td>o</td>
<td>++</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Find / retrieve</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>++</td>
</tr>
<tr>
<td>Modify / Enrich</td>
<td>0</td>
<td>++</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Agenda

1. Presenting CSAF
2. 1st exercise analysis of a CSAF Document + writing own advisories (Secvisogram)
4. 2nd exercise Publish
5. 3rd exercise Retrieve CSAF Documents
6. 4th exercise Update existing CSAF Documents
7. 5th exercise CSAF Aggregator
8. Bonus exercise A: Push CSAF to ticket system or CSAF management system
9. Bonus exercise B: Compare a CSAF document with an SBOM or asset database
10. Bonus exercise C: Modify other CSAF Document
Key takeaways

• Securing the supply chain is necessary
• You can't secure the supply chain on your own - it works only together
• Automation is possible and reduces human workload
• CSAF is a step towards a more secure supply chain through automation
Workshop instructions
Basics
Why are Advisories important?

- Knowing the existence of a vulnerability is not enough
- Actions must be taken:
  - Assessing the risk
  - Assessing the cost

→ Relevant information is in the security advisory
Why is Vulnerability Management important?

• Prioritization:
  • Which vulnerability is patched first / most important?
  • How do I distribute my resources?
• Tracking:
  • Who is doing what?
  • How long does our process take?
  • What risk do I have?
• Scaling:
  • Multiple sources of information
  • Multiple vendors
  • Don’t forget anything.
But why do we need to automate things?
Asset Owners want to run their facility

Machines
Factory lines
Whole installations
Usually comprise of several different vendors
Asset Owners are confronted with a lot of things

- Regulatory requirements
- Availability, uptime, revenue
- Cyber-Security Patches, updates
So many sources of information – some examples

- Regulators
- Security researchers
- National CSIRTs
- Vendors
- ISACs
- ...

Securing the Supply Chain Together – Through Automation of Advisories and Vulnerability Management | Jens Wiesner & Thomas Schmidt
So many sources of information – so many channels and formats

- Security researchers
- National CSIRTs
- Vendors
- Regulators
- ISACs

Securing the Supply Chain Together – Through Automation of Advisories and Vulnerability Management | Jens Wiesner & Thomas Schmidt
What should an operator / asset owner do?
Patches and updates!
Manual process

Vendor
- Production of human-readable advisory
- Publication

Find
- Search websites for new / updated advisories
- Download

Prioritize
- Sift criticality of vulnerabilities

Evaluate
- Do you have affected products?
- Risk assessment
- Decision which actions should be taken

Severity of advisory
- low
- medium
- high
- critical
Securing the Supply Chain Together – Through Automation of Advisories and Vulnerability Management | Jens Wiesner & Thomas Schmidt
Analyze

Securing the Supply Chain Together – Through Automation of Advisories and Vulnerability Management | Jens Wiesner & Thomas Schmidt

ICS Advisory (ICSA-21-138-01)
Emerson Rosemount X-STREAM

Legal Notice

This product is intended for use only by qualified personnel. Emerson Process Management (hereinafter referred to as "Emerson") is committed to providing secure, reliable automation systems. However, users should be aware that there may be vulnerabilities in any software or system. Emerson recommends conducting a thorough risk assessment and following best practices to mitigate risks.

1. EXECUTIVE SUMMARY

- CWS.AI.0.01
- ATTENTION: Exploitable remotely/low attack complexity
- Vendor: Emerson
- Equipment: Rosemount X-STREAM Gas Analyzer
- Vulnerabilities: Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Types, Path Traversal, Use of Persistent Cookies Containing Sensitive Information, Cross-site Scripting, Improper Restriction of Redirection of User Controls

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to obtain sensitive information, modify configuration, or affect the availability of the device.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

4. VULNERABILITY DETAILS

CVE ID: CVE-2021-22741
CVE5.0: 'XIA-2021-0004'

5. REMEDIATION

- CWS.AI.0.02
- ATTENTION: Exploitable locally/medium attack complexity
- Vendor: Emerson
- Equipment: Rosemount X-STREAM Gas Analyzer
- Vulnerabilities: Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Types, Path Traversal, Use of Persistent Cookies Containing Sensitive Information, Cross-site Scripting, Improper Restriction of Redirection of User Controls

6. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to obtain sensitive information, modify configuration, or affect the availability of the device.

7. TECHNICAL DETAILS

7.1 AFFECTED PRODUCTS

8. VULNERABILITY DETAILS

CVE ID: CVE-2021-22741
CVE5.0: 'XIA-2021-0004'

9. REMEDIATION

- CWS.AI.0.02
- ATTENTION: Exploitable locally/medium attack complexity
- Vendor: Emerson
- Equipment: Rosemount X-STREAM Gas Analyzer
- Vulnerabilities: Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Types, Path Traversal, Use of Persistent Cookies Containing Sensitive Information, Cross-site Scripting, Improper Restriction of Redirection of User Controls

10. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to obtain sensitive information, modify configuration, or affect the availability of the device.

11. TECHNICAL DETAILS

11.1 AFFECTED PRODUCTS

12. VULNERABILITY DETAILS

CVE ID: CVE-2021-22741
CVE5.0: 'XIA-2021-0004'

13. REMEDIATION

- CWS.AI.0.02
- ATTENTION: Exploitable locally/medium attack complexity
- Vendor: Emerson
- Equipment: Rosemount X-STREAM Gas Analyzer
- Vulnerabilities: Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Types, Path Traversal, Use of Persistent Cookies Containing Sensitive Information, Cross-site Scripting, Improper Restriction of Redirection of User Controls

14. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to obtain sensitive information, modify configuration, or affect the availability of the device.

15. TECHNICAL DETAILS

15.1 AFFECTED PRODUCTS

16. VULNERABILITY DETAILS

CVE ID: CVE-2021-22741
CVE5.0: 'XIA-2021-0004'

17. REMEDIATION

- CWS.AI.0.02
- ATTENTION: Exploitable locally/medium attack complexity
- Vendor: Emerson
- Equipment: Rosemount X-STREAM Gas Analyzer
- Vulnerabilities: Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Types, Path Traversal, Use of Persistent Cookies Containing Sensitive Information, Cross-site Scripting, Improper Restriction of Redirection of User Controls

18. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to obtain sensitive information, modify configuration, or affect the availability of the device.

19. TECHNICAL DETAILS

19.1 AFFECTED PRODUCTS

20. VULNERABILITY DETAILS

CVE ID: CVE-2021-22741
CVE5.0: 'XIA-2021-0004'

21. REMEDIATION

- CWS.AI.0.02
- ATTENTION: Exploitable locally/medium attack complexity
- Vendor: Emerson
- Equipment: Rosemount X-STREAM Gas Analyzer
- Vulnerabilities: Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Types, Path Traversal, Use of Persistent Cookies Containing Sensitive Information, Cross-site Scripting, Improper Restriction of Redirection of User Controls

The document discusses the Schneider Electric Security Notification, highlighting the risks associated with the EcoStruxure Geo SCADA Expert. It emphasizes the importance of timely updates and proper configuration to mitigate vulnerabilities. The advisory includes details on affected products, vulnerability details, and remediatory actions. The text is structured to provide clear guidance for system integrators and end-users, ensuring a secure and compliant operational environment.
Number of Advisories

\[ f(x) = 50x \]
\[ f(x) = x^3 \]
\[ f(x) = 2^x \]
Number of Advisories CVE

https://opensourcesecurity.io/2021/03/30/its-time-to-fix-cve/
That doesn’t scale!
Possible solutions
Let’s automate the process...
Process with CSAF

Vendor
- Production of *machine-readable* advisory
- Publication

Find
- Search websites for new / updated advisories
- Download

Evaluate (static)
- Do you have affected products?
- Risk assessment (static) => adopt criticality
- Criticality of the vulnerability

Measures
- Sift of advisories with affected products sort by criticality
- Decision which actions should be taken

Severity of advisory:
- low
- medium
- high
- critical

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
What is CSAF?

Common Security Advisory Framework
- Machine-readable format for security advisories (JSON)
- Standardized way of distribution security advisories
- Build with automation in mind
- Standardized tool set
- Guidance to actionable information
- Successor of CSAF CVRF 1.2

Ready to use!
Who is involved in the development of CSAF?

- AT&T
- Cisco
- Microsoft
- Red Hat
- Oracle
- Siemens
- BSI
- ...

See full list at: https://www.oasis-open.org/committees/membership.php?wg_abbrev=csaf

We need your support to make it work!
Benefits for asset owners

• Makes the impossible (stringent patch and update management) **possible** (at the moment often sporadic or dependent on personal availability/interests)

• **Reduce** human factor and individual work load
  • No more manual searching for advisories
  • Easier to determine affected devices
  • Delegable
  • See only relevant advisories

• **Scalable** across all participating vendors
• Enables basic risk assessment based on own environment
Two sides of the same coin – different maturity stages

Vendor

- Vendor (specific) internal tools and processes
- ... Continuously Security Advisory Release (CSAR)
- Unique Product IDs
- Content Management System
- Text editor / Writer
- Quality of advisories
- ... Supply Chain routinely included
- Input data for automatic asset management
- Existence of machine-readable format
- Existence of human-readable format

Asset owner

- Asset owner (specific) internal tools and processes
- ... Routinely patching
- Automatic processing of advisories
- (Semi-) Automated processing of advisories
- Manual processing of advisories

Requirements for tools and processes

- Security downtime accepted/ minimized/ mitigated
- Asset management system with unique Product IDs
- Asset management with smart search
- Web browser

Difficulty/maturity/automation capability

Vendor Asset owner

Two sides of the same coin – different maturity stages

Vendor Asset owner

Vendor Asset owner

Vendor Asset owner

Vendor Asset owner

Vendor Asset owner
Next step: reach stage 2 across parties

<table>
<thead>
<tr>
<th>Vendor (specific) internal tools and processes</th>
<th>Quality of advisories</th>
<th>Asset owner (specific) internal tools and processes</th>
<th>Requirements for tools and processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous Security Advisory Release (CSAR)</td>
<td></td>
<td>Routine patching</td>
<td>Security downtime accepted/ minimized/ mitigated</td>
</tr>
<tr>
<td>Unique Product IDs</td>
<td></td>
<td>Automatic processing of advisories</td>
<td>Asset management system with unique Product IDs</td>
</tr>
<tr>
<td>Content Management System</td>
<td>Existence of machine-readable format</td>
<td>(Semi-) Automated processing of advisories</td>
<td>Asset management with smart search</td>
</tr>
<tr>
<td>Text editor / Writer</td>
<td>Existence of human-readable format</td>
<td>Manual processing of advisories</td>
<td>Web browser</td>
</tr>
</tbody>
</table>

**Difficulty/ maturity / automation capability**

- **Vendor:** 
  - Difficulty
  - Maturity
  - Automation capability

- **Asset owner:** 
  - Routine patching
  - Automatic processing of advisories
  - (Semi-) Automated processing of advisories
  - Manual processing of advisories
Requirements for asset owners

- Machine-readable asset inventory
- Request Advisories in CSAF from vendors
- Connection between both of them to leverage the full potential
How does that help in the supply chain?
Timeframe of concern

Vendor becomes aware of a vulnerability
Vendor analyzes the vulnerability
Vendor releases patch & advisory
Asset owner does something*

Timeframe of concern
(under control of the asset owner)

* Patch, mitigate risk, or actively accept risk
Supply chain

Supplier becomes aware of a vulnerability

Supplier releases patch & advisory

Vendor becomes aware of a vulnerability

Vendor releases patch & advisory

User does something*

* Patch, mitigate risk, or actively accept risk
(Almost) Every vendor is a user

- Supplier becomes aware of a vulnerability
- Supplier analyzes the vulnerability
- Supplier releases patch & advisory
- Vendor does something*

Timeframe of concern (under control of the vendor)

* Patch, mitigate risk, or actively accept risk
PART II
Where to find basic information?

https://csaf.io


CSAF GitHub:  https://github.com/oasis-tcs/csaf

CSAF 2.0 JSON Schema:  https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/json_schema/csaf_json_schema.json

CSAF 2.0 Prose:  https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/prose/csaf-v2-editor-draft.md

CSAF 2.0 Examples:  https://github.com/oasis-tcs/csaf/tree/master/csaf_2.0/examples

Secvisogram sources:  https://github.com/secvisogram/secvisogram

Running Demo:  https://secvisogram.github.io
Exercise 1

Write an advisory in CSAF
Example CSAF Document

---

```
"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-ssa-20180328-sm12",
      "status": "final",
      "version": "3.0.0",
      "revision_history": [
        {
          "initial_release_date": "2018-03-28T16:00:00Z",
          "current_release_date": "2018-04-17T15:05:41Z",
          "generator": {
            "product_tree": {
              "branches": [

              ]
            }
          }
        }
      ]
    },
    "notes": {
      "references": [
        {
          "url": "https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-ssa-20180328-sm12",
          "summary": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability"
        }
      ]
    },
    "vulnerabilities": [
      {
        "title": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability",
        "ids": {
          "cve": "CVE-2018-0171",
          "product_status": {
            "known_affected": [
              {
                "scores": {
                  "remediations": {
                    "references": [

                    ]
                  }
                }
              }
            ]
          }
        }
      }
    ]
  }
}
```
Example CSAF Document

Document level metadata

Product tree

Vulnerabilities
Break
One problem solved: unified format specified
Exercise 2

Publish a CSAF document
“When security risks in web services are discovered by independent security researchers who understand the severity of the risk, they often lack the channels to disclose them properly. As a result, security issues may be left unreported. security.txt defines a standard to help organizations define the process for security researchers to disclose security vulnerabilities securely.”

Place a file security.txt on your website under the .well-known directory
Example [https://www.bsi.bund.de/.well-known/security.txt](https://www.bsi.bund.de/.well-known/security.txt)

```plaintext
Contact: mailto:certbund@bsi.bund.de
Contact: https://www.bsi.bund.de/Security-Contact
Encryption: https://www.bsi.bund.de/Security-Contact
Preferred-Languages: de, en
Canonical: https://bsi.bund.de/.well-known/security.txt
Hiring: https://www.bsi.bund.de/Jobs
```

Further info at
- [https://securitytxt.org](https://securitytxt.org)

Not valid according to RFC 9116 !!!
Where to find CSAF documents?

<table>
<thead>
<tr>
<th>Valid CSAF documents</th>
<th>File name restrictions</th>
<th>TLS enforced</th>
<th>TLP:WHITE freely accessible</th>
</tr>
</thead>
</table>

- Well-defined URL / security.txt / DNS => provider-metadata.json
- List of advisories and latest changes and Fixed folder structure
- or ROLIE feeds
- Restriction on >=TLP:AMBER
- All requirements from CSAF publisher

<table>
<thead>
<tr>
<th>Sign own advisories</th>
<th>Hash advisories</th>
<th>Published PGP keys for integrity checks</th>
<th>All requirements from CSAF provider</th>
</tr>
</thead>
</table>

https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/prose/csaf-v2-editor-draft.md#7-distributing-csaf-documents
Example: provider-metadata.json
Example: ROLIE feed
Eco System of Advisories

![Diagram showing the relationship between Multiplier, Vendor, and User with PUSH and PULL arrows.]

Securing the Supply Chain Together – Through Automation of Advisories and Vulnerability Management | Jens Wiesner & Thomas Schmidt
Vendors’ Perspective
Vendor

1. Vendor becomes aware of a vulnerability
2. Vendor analyzes the vulnerability
3. Vendor prepares patch
4. Vendor writes advisory
5. Vendor publishes advisory & patch
Vendor becomes aware of a vulnerability

Vendor analyzes the vulnerability

Vendor prepares patch

Vendor writes advisory

CSAF content management system

Vendor publishes advisory & patch

CSAF trusted provider
Exercise 3

Retrieve a CSAF document
Retrieving order

1. **Finding provider-metadata.json**
   1. Check Well-known URL (requirement 9 in section 7.1)
   2. Check security.txt (requirement 8 in section 7.1)
   3. Check DNS path (requirement 10 in section 7.1)
   4. Select one or more provider-metadata.json to use

2. **Retrieving CSAF documents**
   1. Parse provider-metadata.json: ROLIE-based (requirements 15 to 17 in section 7.1, preferred) or directory-based distribution (requirements 11 to 14 in section 7.1) to locate CSAF documents
   2. For CSAF trusted providers: retrieved hash and signature files (requirements 18 to 19 in section 7.1); check before further processing
   3. Test CSAF document against schema
   4. Execute mandatory tests
How to know the main domain?

**CSAF Lister**
- Like telephone directory
- Lists known CSAF providers
- JSON structure
Exercise 4

Update a CSAF document
Everything perfect?
Obviously not! Still many sources of information
One more step needed to make it easy ... Saradi to the rescue!
Scalable and resilient advisory distribution infrastructure (Saradi)

CSAF aggregator

• Trusted party
• Collects advisories from issuers
• Provides them
• API optional
• One-stop-shop
• Multiple around the world (National CERTs)
Demo: CSAF Aggregator
Users’ Perspective
User retrieves advisories
User compares with asset database
User decides what to do
User acts
User documents action
User

User retrieves advisories

User compares with asset database

User decides what to do

User acts

User documents action

Custom downloader
User

CSAF provider

CSAF trusted provider

CSAF aggregator

User retrieves advisories

Custom downloader

User compares with asset database

User decides what to do

User acts

User acts

User documents action

Securing the Supply Chain Together – Through Automation of Advisories and Vulnerability Management | Jens Wiesner & Thomas Schmidt
User

User retrieves advisories

CSAF trusted provider

User compares with asset database

CSAF asset matching system

User decides what to do

User acts

User documents action

Custom downloader

CSAF provider

CSAF aggregator
User

CSAF provider

CSAF trusted provider

CSAF aggregator

User retrieves advisories

Custom downloader

User prioritizes advisories

CSAF management system

User decides what to do

User acts

User documents action
Bonus Exercise A

Push CSAF to ticket system or CSAF management system
Supply chain: vendors’ view
Supply chain

Vendor finds advisory of supplier

Vendor matches with own SBOMs

Vendor publishes information

Vendor acts

Vendor decides what to do

CSAF aggregator

CSAF provider

CSAF trusted provider

Custom downloader

CSAF SBOM matching system

SSVC

CSAF content management system

CSAF trusted provider

Securing the Supply Chain Together – Through Automation of Advisories and Vulnerability Management | Jens Wiesner & Thomas Schmidt
Bonus Exercise B

Compare a CSAF document against an SBOM or asset database
Exercise Compare a CSAF document against an SBOM or asset database

- Do it yourself later
- No software available at the moment
- Please tell us if you changed that

- Principles for matching
  - Input: match(product_tree, asset_database) or match(product_tree, sbom_database)
  - Output: for each product_id in product_tree: list of tuples (matched_asset_id, probability)
Multiplier

(Governmental) CERTs
Multiplier

Vendor

Multiplier receives advisories

Multiplier writes ("enriches") advisory

Multiplier decides what to do

Multiplier publishes advisory
Re-Use of existing information
Bonus Exercise C

Modify a CSAF document programmatically
CSAF modifier

The program:
• satisfies the "CSAF post-processor" conformance profile.
• adds, deletes or modifies at least one property, array, object or value of a property or item of an array.
• does not emit any objects, properties, or values which, according to section 9, are intended to be produced only by CSAF translators.
• satisfies the normative requirements given below.

The resulting modified document:
• does not have the same /document/tracking/id as the original document. The modified document can use a completely new /document/tracking/id or compute one by appending the original /document/tracking/id as a suffix after an ID from the naming scheme of the issuer of the modified version. It SHOULD not use the original /document/tracking/id as a prefix.
• includes a reference to the original advisory as first element of the array /document/references[].
Tools and more information
Open Source tools in development

**Secvisogram**
- Generating CSAF documents based on a form
- Experts mode available

**Validator**
- Check whether given CSAF document is valid
- Provides additional remarks how to improve usability

**Domain checker**
- Tests whether given domain is (known to) distribute CSAF documents
- Checks which requirements are fulfilled
Tools developed by the community

- CSAF producer: [https://github.com/secvisogram/secvisogram](https://github.com/secvisogram/secvisogram)
- CSAF trusted provider: [https://github.com/csaf-poc/csaf_distribution](https://github.com/csaf-poc/csaf_distribution) (WIP)
- CSAF aggregator: [https://github.com/csaf-poc/csaf_distribution](https://github.com/csaf-poc/csaf_distribution) (WIP)
- Provider checker: [https://github.com/csaf-poc/csaf_distribution](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 modifier: *custom implementation*
- CSAF downloader: [https://github.com/csaf-poc/csaf_distribution](https://github.com/csaf-poc/csaf_distribution) (WIP)
- CSAF full validator: [https://github.com/secvisogram/csaf-validator-lib](https://github.com/secvisogram/csaf-validator-lib) (WIP)

- **Your tools?**
Structure of CSAF 2.0 Specification

- Introduction & Design Considerations
- Schema elements
- Profiles
- Additional Conventions
- Tests
  - Mandatory
  - Optional
  - Informative
- Distributing CSAF documents
- Safety, Security, and Data Protection Considerations
- Conformance
Specification of conformance targets – document level

https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/prose/csaf-v2-editor-draft.md#9-conformance
Specification of conformance targets – document level

https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/prose/csaf-v2-editor-draft.md#9-conformance
Where to find more information?

https://csaf.io


CSAF GitHub: https://github.com/oasis-tcs/csaf

CSAF 2.0 JSON Schema: https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/json_schema/csaf_json_schema.json

CSAF 2.0 Prose: https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/prose/csaf-v2-editor-draft.md

CSAF 2.0 Examples: https://github.com/oasis-tcs/csaf/tree/master/csaf_2.0/examples

Secvisogram sources: https://github.com/secvisogram/secvisogram

Running Demo: https://secvisogram.github.io

Securing the Supply Chain Together – Through Automation of Advisories and Vulnerability Management | Jens Wiesner & Thomas Schmidt
Open questions for CSAF 2.x & CSAF 3.0

- More automation
- API definition
- Distribution of advisories across aggregators
- Additional metrics like SSVC

- Solving the problem of unique product identifiers
- Improving integration of SBOM
Conclusions
BSI continues its efforts

For success active support of many parties is required

• Adopt CSAF for own advisories
• Marketing
• Additional support tools
• Strong endorsement of CSAF towards
  • Vendors
  • Operators

What is your contribution?
Key takeaways & actions

- Securing the supply chain is necessary
- You can't secure the supply chain on your own - it works only together
- Automation is possible and reduces human workload
- CSAF is a step towards a more secure supply chain through automation

- Request your vendors to provide CSAF 2.0
- Provide CSAF documents to your customers to ease their pain
- Clean up your asset inventory / Setup SBOMs
- Spread the word! #oCSAF #advisory

- Don’t miss the presentation on VEX! (Thursday 11:20-11:55)