Federal Office
for Information Security

Deutschland
Digital•Sicher•BSI•

# Vulnerability management with CSAF – why SBOM is not enough

Thomas Schmidt
Federal Office for Information Security (BSI)

# Who am I?

**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

# Vulnerability management

- Know the vulnerability
  - Details
  - Impact
  - Risks
  - Exploitability
  - …

- Know where the component is used

- Know how to remediate
  - What do I need to do?

Federal Office
for Information Security

# Vulnerability management

- Know the vulnerability
  - Details
  - Impact
  - Risks
  - Exploitability
  - …

CVE

- Know where the component is used

SBOM

- Know how to remediate
  - What do I need to do?

Security Advisory

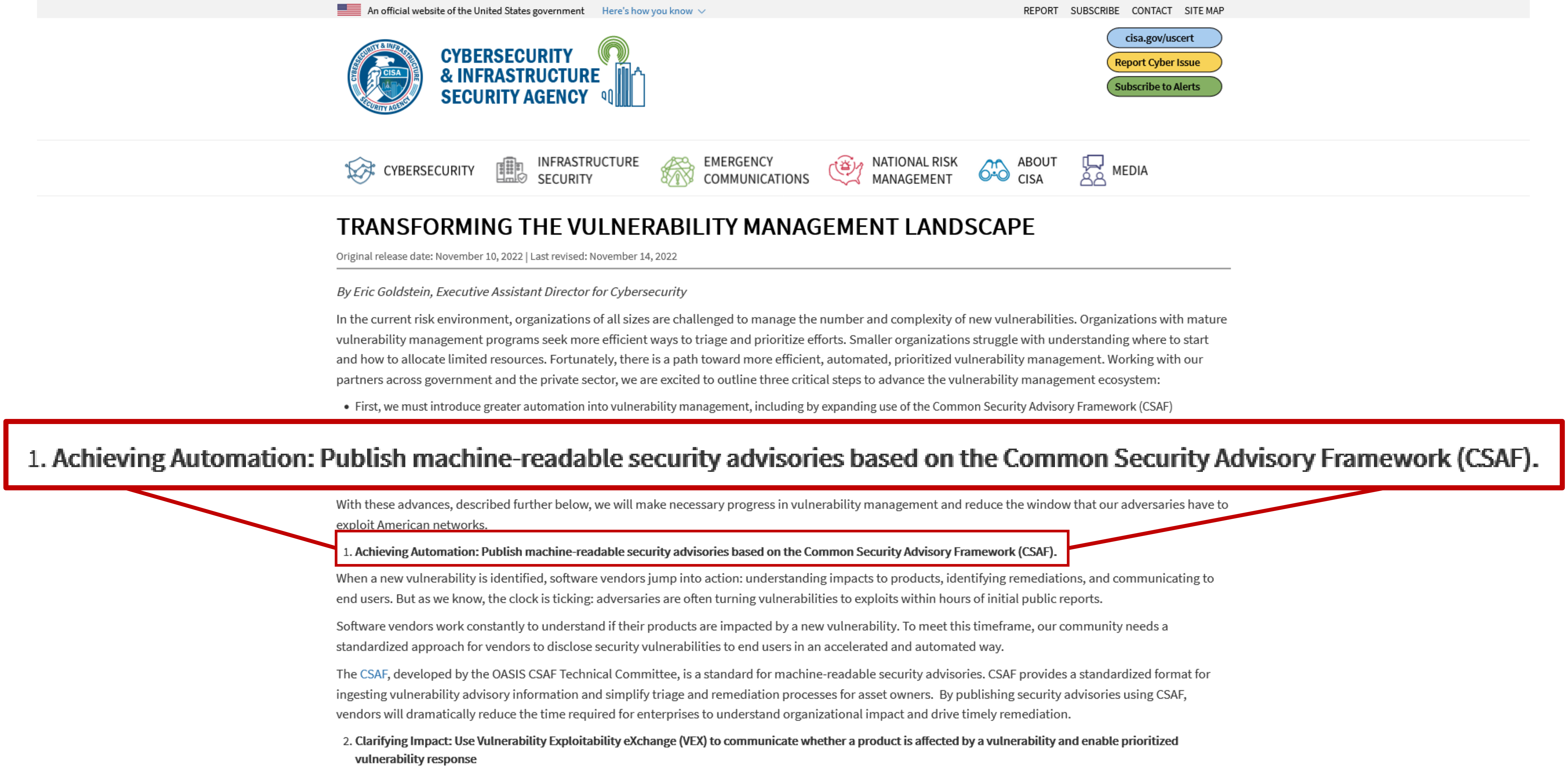
Just knowing the component is included is not enough...

# Just knowing the component is included is not enough...

... as you usually don’t have them in your asset database

# Just knowing the component is included is not enough...

...as it says nothing whether the vulnerability is exploitable in the product



# TRANSFORMING THE VULNERABILITY MANAGEMENT LANDSCAPE

Original release date: November 10, 2022 | Last revised: November 14, 2022

*By Eric Goldstein, Executive Assistant Director for Cybersecurity*

In the current risk environment, organizations of all sizes are challenged to manage the number and complexity of new vulnerabilities. Organizations with mature vulnerability management programs seek more efficient ways to triage and prioritize efforts. Smaller organizations struggle with understanding where to start and how to allocate limited resources. Fortunately, there is a path toward more efficient, automated, prioritized vulnerability management. Working with our partners across government and the private sector, we are excited to outline three critical steps to advance the vulnerability management ecosystem:

- First, we must introduce greater automation into vulnerability management, including by expanding use of the Common Security Advisory Framework (CSAF)

With these advances, described further below, we will make necessary progress in vulnerability management and reduce the window that our adversaries have to exploit American networks.

1. **Achieving Automation: Publish machine-readable security advisories based on the Common Security Advisory Framework (CSAF).**

When a new vulnerability is identified, software vendors jump into action: understanding impacts to products, identifying remediations, and communicating to end users. But as we know, the clock is ticking: adversaries are often turning vulnerabilities to exploits within hours of initial public reports.

Software vendors work constantly to understand if their products are impacted by a new vulnerability. To meet this timeframe, our community needs a standardized approach for vendors to disclose security vulnerabilities to end users in an accelerated and automated way.

The CSAF, developed by the OASIS CSAF Technical Committee, is a standard for machine-readable security advisories. CSAF provides a standardized format for ingesting vulnerability advisory information and simplify triage and remediation processes for asset owners.  By publishing security advisories using CSAF, vendors will dramatically reduce the time required for enterprises to understand organizational impact and drive timely remediation.

2. **Clarifying Impact: Use Vulnerability Exploitability eXchange (VEX) to communicate whether a product is affected by a vulnerability and enable prioritized vulnerability response**

1. **Achieving Automation: Publish machine-readable security advisories based on the Common Security Advisory Framework (CSAF).**

https://www.cisa.gov/blog/2022/11/10/transforming-vulnerability-management-landscape

# Security Advisories

- Details about the vulnerabilities (including a CVE)
- **Products that are affected**
- Remediation
- Scores
- General guidance

Federal Office
for Information Security

# CVE vs. Advisories

CVE

One vulnerability

**Focus: Talk about the same thing**

Advisory

One or multiple vulnerabilities

**Focus: Tell remediation**

# Security Advisories

- Details about the vulnerabilities (including a CVE)
- Products that are affected
- **Remediation**
- Scores
- General guidance

# Security Advisories

- Details about the vulnerabilities (including a CVE)
- Products that are affected
- **Remediation**
  - *Hotfix*
  - *Update*
  - *Upgrade*
  - *Mitigating countermeasures*
  - …

  Patch
- Scores
- General guidance

# For each new vulnerability, decide

Patch immediately

Patch next downtime

Accept risk

Federal Office
for Information Security

# How to decide?

# Risk-based approach

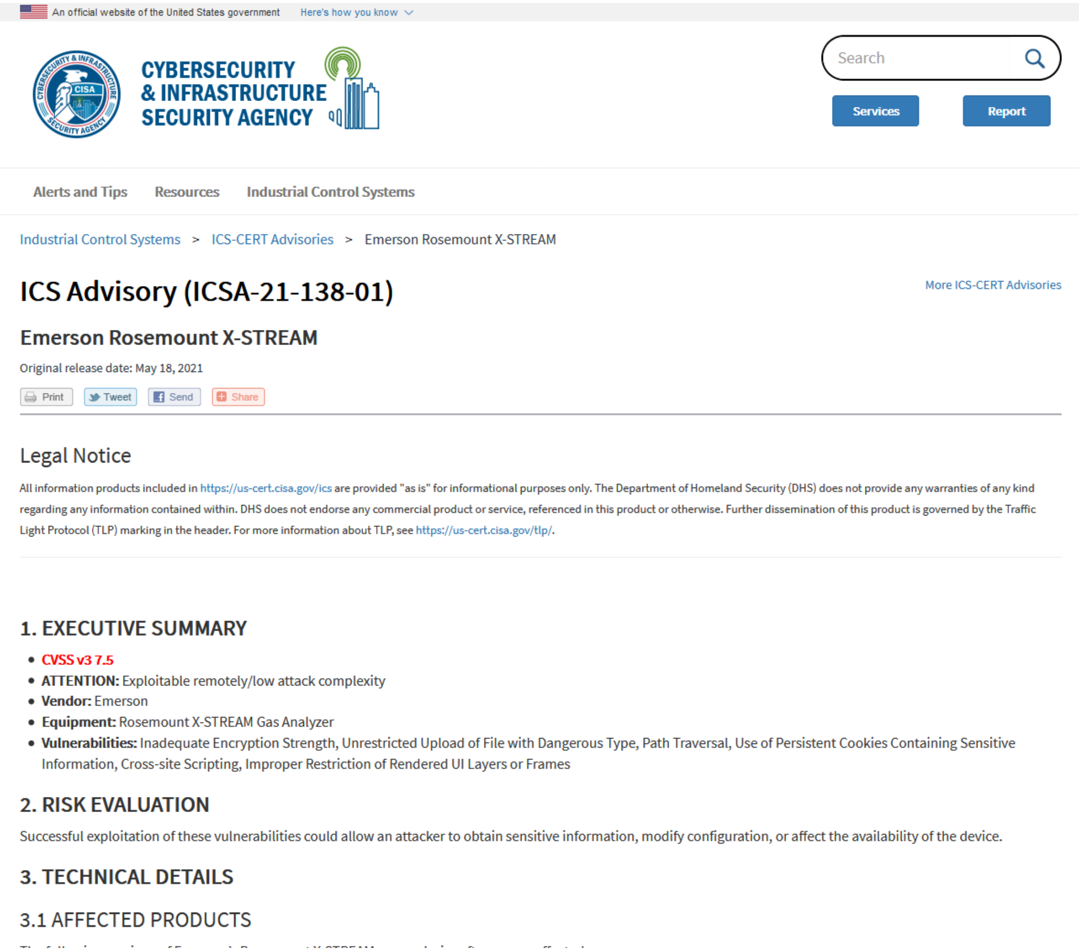
Risk and cost scales depend on:

- Vulnerability
- Safety impact
- Usage of the product
- Existing countermeasures in the infrastructure
- Likelihood of broken patches / incompatibilities
- Attacks in the wild

Where do I get the information?

# Security advisories!

# Some examples



An official website of the United States government
Here's how you know
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
Search
Services
Report
Alerts and Tips
Resources
Industrial Control Systems

Industrial Control Systems > ICS-CERT Advisories > Emerson Rosemount X-STREAM

## ICS Advisory (ICSA-21-138-01)

More ICS-CERT Advisories

### Emerson Rosemount X-STREAM

Original release date: May 18, 2021

### Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see https://us-cert.cisa.gov/tlp/.

### 1. EXECUTIVE SUMMARY

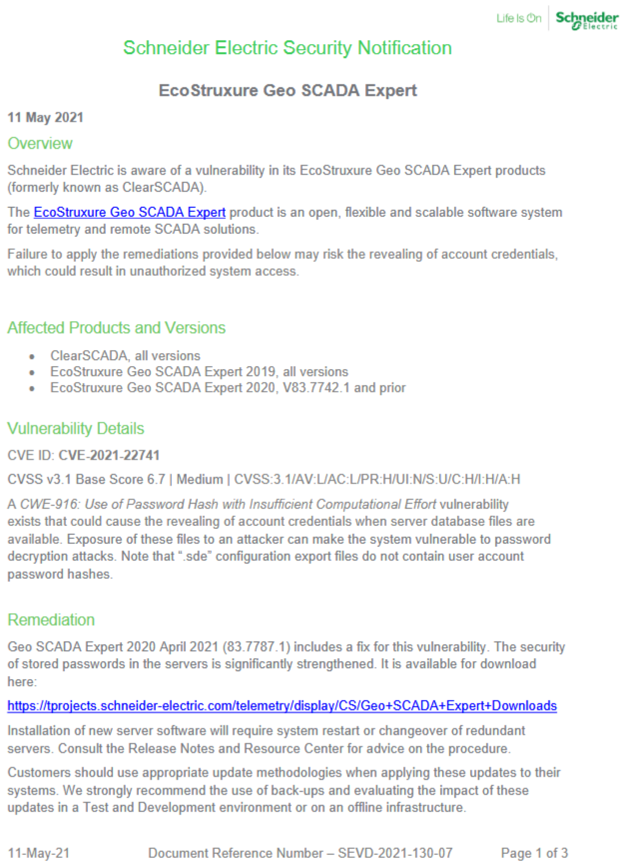
- CVSS v3 7.5
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Emerson
- **Equipment:** Rosemount X-STREAM Gas Analyzer
- **Vulnerabilities:** Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Type, Path Traversal, Use of Persistent Cookies Containing Sensitive Information, Cross-site Scripting, Improper Restriction of Rendered UI Layers or Frames

### 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



Life Is On Schneider Electric

## Schneider Electric Security Notification

### EcoStruxure Geo SCADA Expert

**11 May 2021**

### Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure Geo SCADA Expert products (formerly known as ClearSCADA).

The EcoStruxure Geo SCADA Expert product is an open, flexible and scalable software system for telemetry and remote SCADA solutions.

Failure to apply the remediations provided below may risk the revealing of account credentials, which could result in unauthorized system access.

### Affected Products and Versions

- ClearSCADA, all versions
- EcoStruxure Geo SCADA Expert 2019, all versions
- EcoStruxure Geo SCADA Expert 2020, V83.7742.1 and prior

### Vulnerability Details

CVE ID: **CVE-2021-22741**

CVSS v3.1 Base Score 6.7 | Medium | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

A *CWE-916: Use of Password Hash with Insufficient Computational Effort* vulnerability exists that could cause the revealing of account credentials when server database files are available. Exposure of these files to an attacker can make the system vulnerable to password decryption attacks. Note that ".sde" configuration export files do not contain user account password hashes.

### Remediation

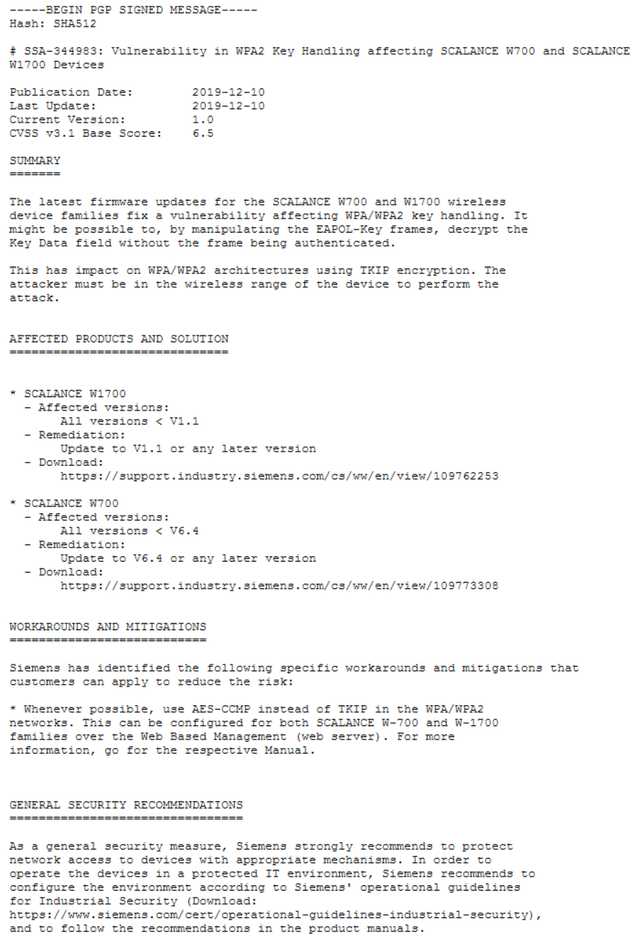
Geo SCADA Expert 2020 April 2021 (83.7787.1) includes a fix for this vulnerability. The security of stored passwords in the servers is significantly strengthened. It is available for download here:

https://tprojects.schneider-electric.com/telemetry/display/CS/Geo+SCADA+Expert+Downloads

Installation of new server software will require system restart or changeover of redundant servers. Consult the Release Notes and Resource Center for advice on the procedure.

Customers should use appropriate update methodologies when applying these updates to their systems. We strongly recommend the use of back-ups and evaluating the impact of these updates in a Test and Development environment or on an offline infrastructure.

11-May-21 Document Reference Number – SEVD-2021-130-07 Page 1 of 3



```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

# SSA-344983: Vulnerability in WPA2 Key Handling affecting SCALANCE W700 and SCALANCE
W1700 Devices

Publication Date:        2019-12-10
Last Update:             2019-12-10
Current Version:         1.0
CVSS v3.1 Base Score:    6.5

SUMMARY
=======

The latest firmware updates for the SCALANCE W700 and W1700 wireless
device families fix a vulnerability affecting WPA/WPA2 key handling. It
might be possible to, by manipulating the EAPOL-Key frames, decrypt the
Key Data field without the frame being authenticated.

This has impact on WPA/WPA2 architectures using TKIP encryption. The
attacker must be in the wireless range of the device to perform the
attack.


AFFECTED PRODUCTS AND SOLUTION
==============================


* SCALANCE W1700
  - Affected versions:
      All versions < V1.1
  - Remediation:
      Update to V1.1 or any later version
  - Download:
      https://support.industry.siemens.com/cs/ww/en/view/109762253

* SCALANCE W700
  - Affected versions:
      All versions < V6.4
  - Remediation:
      Update to V6.4 or any later version
  - Download:
      https://support.industry.siemens.com/cs/ww/en/view/109773308


WORKAROUNDS AND MITIGATIONS
===========================

Siemens has identified the following specific workarounds and mitigations that
customers can apply to reduce the risk:

* Whenever possible, use AES-CCMP instead of TKIP in the WPA/WPA2
networks. This can be configured for both SCALANCE W-700 and W-1700
families over the Web Based Management (web server). For more
information, go for the respective Manual.


GENERAL SECURITY RECOMMENDATIONS
================================

As a general security measure, Siemens strongly recommends to protect
network access to devices with appropriate mechanisms. In order to
operate the devices in a protected IT environment, Siemens recommends to
configure the environment according to Siemens' operational guidelines
for Industrial Security (Download:
https://www.siemens.com/cert/operational-guidelines-industrial-security),
and to follow the recommendations in the product manuals.
```

Federal Office
for Information Security

# Manual process

Severity of advisory

🟩 low
🟨 medium
🟧 high
🟥 critical

Vendor

- Production of human-readable advisory
- Publication

🟩 1 🟧 2 🟧 3 🟩 4 🟥 5 🟧 6 🟧 7 🟨 8 🟧 9 🟥 10 🟩 11 🟧 12 🟥 13 🟨 14 🟧 15

# Manual process

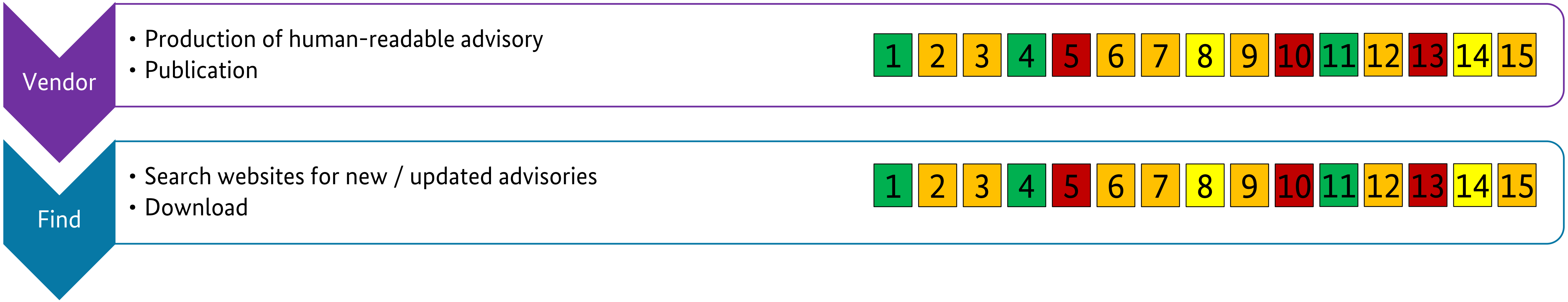
Severity of advisory

🟩 low

🟨 medium

🟧 high

🟥 critical



Vendor

- Production of human-readable advisory
- Publication

🟩1 🟧2 🟧3 🟩4 🟥5 🟧6 🟧7 🟨8 🟧9 🟥10 🟩11 🟧12 🟥13 🟨14 🟧15

Find

- Search websites for new / updated advisories
- Download

🟩1 🟧2 🟧3 🟩4 🟥5 🟧6 🟧7 🟨8 🟧9 🟥10 🟩11 🟧12 🟥13 🟨14 🟧15

# Manual process

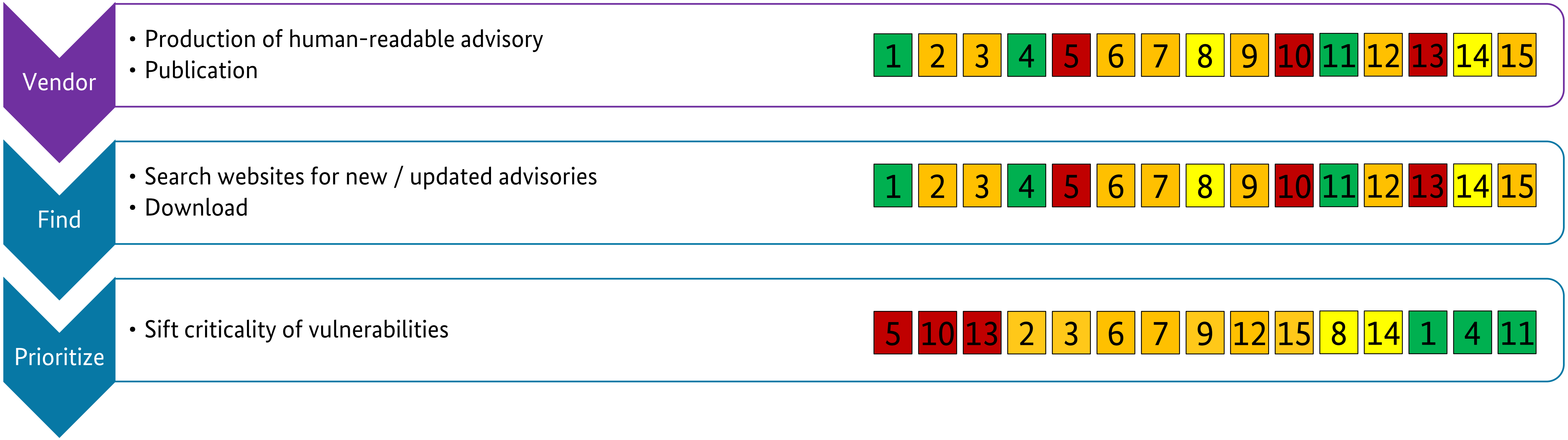
Severity of advisory

🟩 low

🟨 medium

🟧 high

🟥 critical



Vendor
- Production of human-readable advisory
- Publication

🟩1 🟧2 🟧3 🟩4 🟥5 🟧6 🟧7 🟨8 🟧9 🟥10 🟩11 🟧12 🟥13 🟨14 🟧15

Find
- Search websites for new / updated advisories
- Download

🟩1 🟧2 🟧3 🟩4 🟥5 🟧6 🟧7 🟨8 🟧9 🟥10 🟩11 🟧12 🟥13 🟨14 🟧15

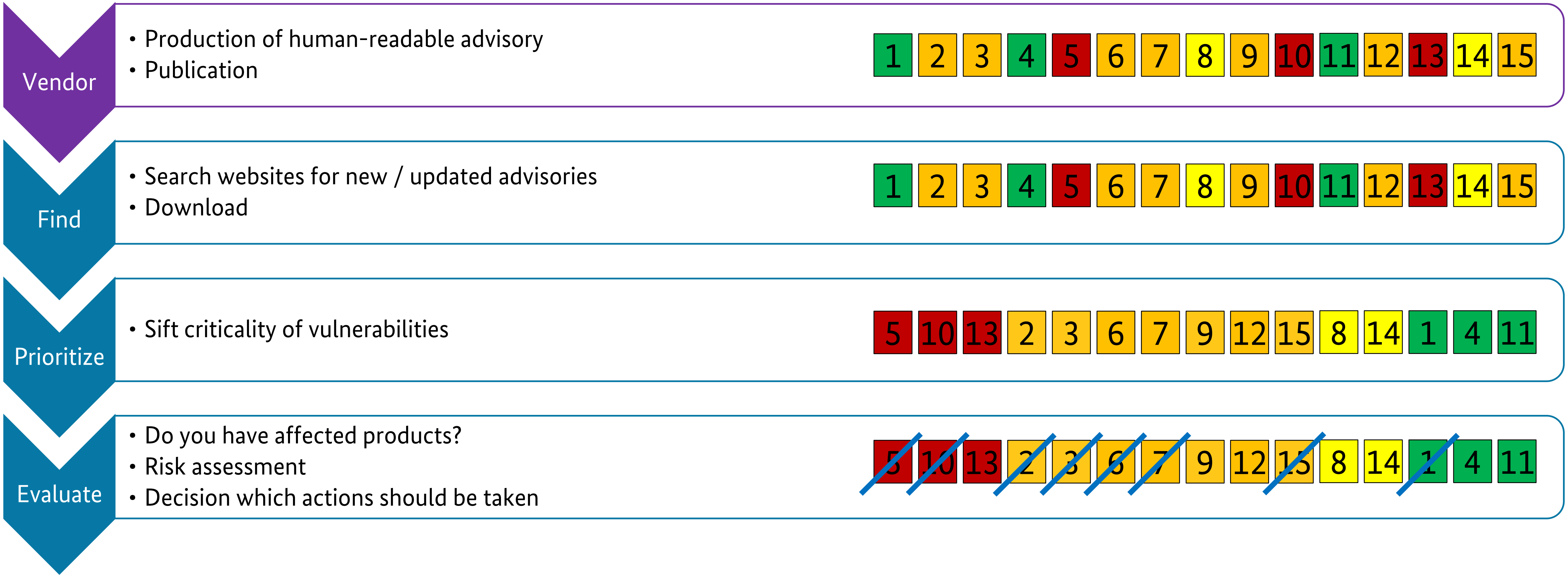
Prioritize
- Sift criticality of vulnerabilities

🟥5 🟥10 🟥13 🟧2 🟧3 🟧6 🟧7 🟧9 🟧12 🟧15 🟨8 🟨14 🟩1 🟩4 🟩11

# Manual process

Severity of advisory

🟩 low
🟨 medium
🟧 high
🟥 critical



Vendor
- Production of human-readable advisory
- Publication

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Find
- Search websites for new / updated advisories
- Download

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Prioritize
- Sift criticality of vulnerabilities

5 10 13 2 3 6 7 9 12 15 8 14 1 4 11

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

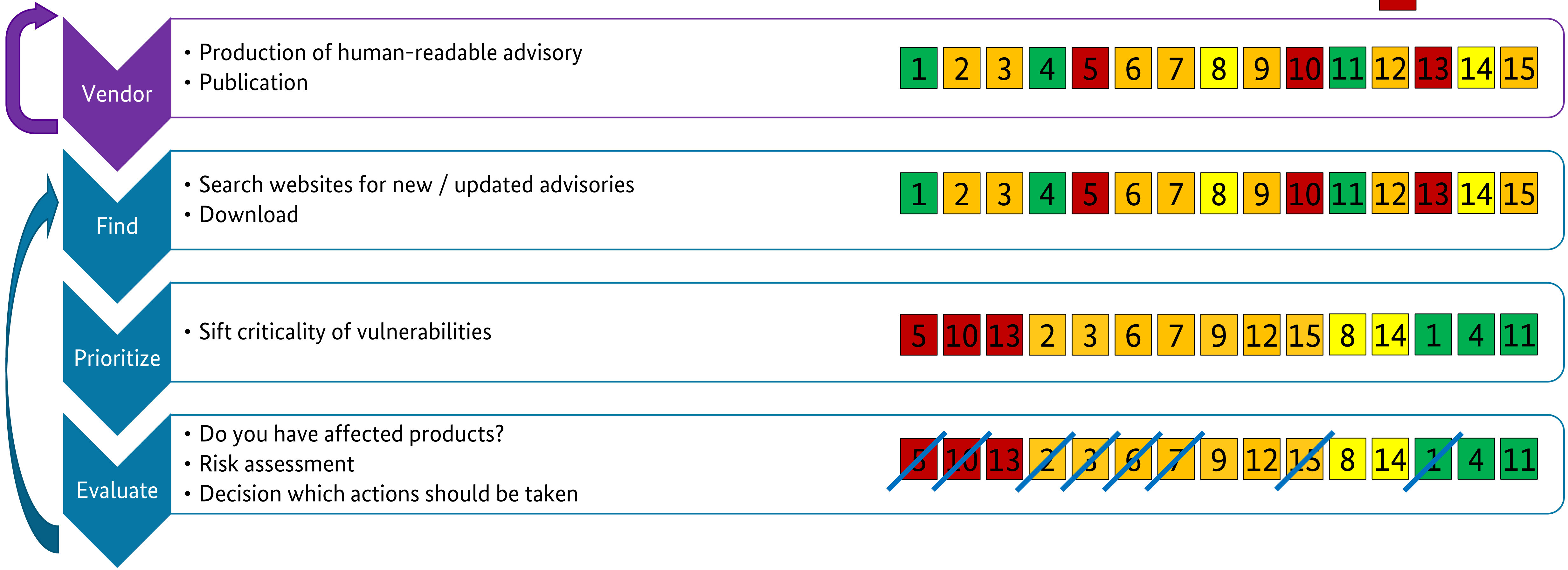
~~5~~ ~~10~~ 13 ~~2~~ ~~3~~ ~~6~~ ~~7~~ 9 12 ~~15~~ 8 14 ~~1~~ 4 11

Federal Office
for Information Security

# Manual process

Severity of advisory

- 🟩 low
- 🟨 medium
- 🟧 high
- 🟥 critical



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

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

**Find**
- Search websites for new / updated advisories
- Download

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

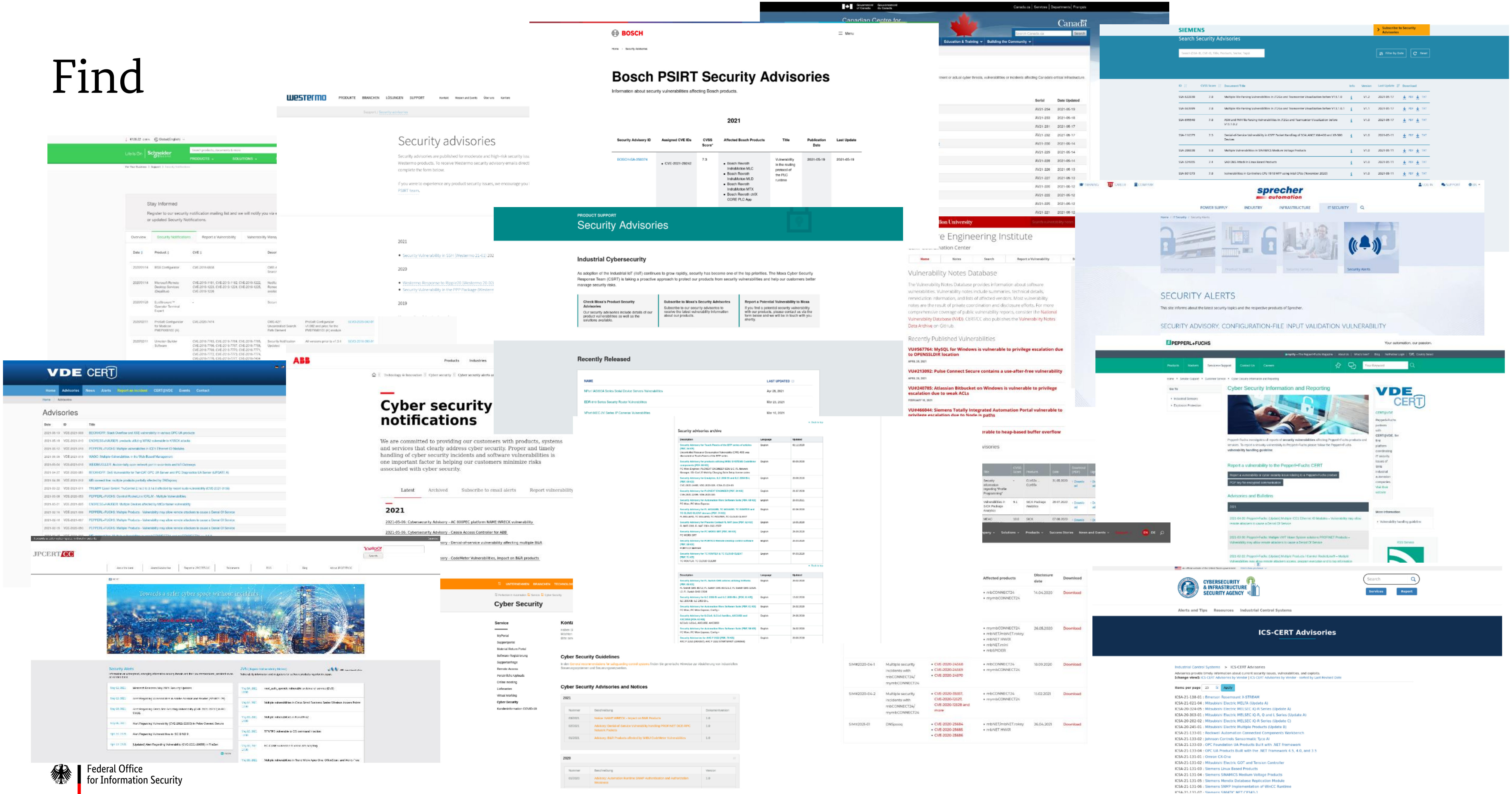
**Prioritize**
- Sift criticality of vulnerabilities

5 10 13 2 3 6 7 9 12 15 8 14 1 4 11

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

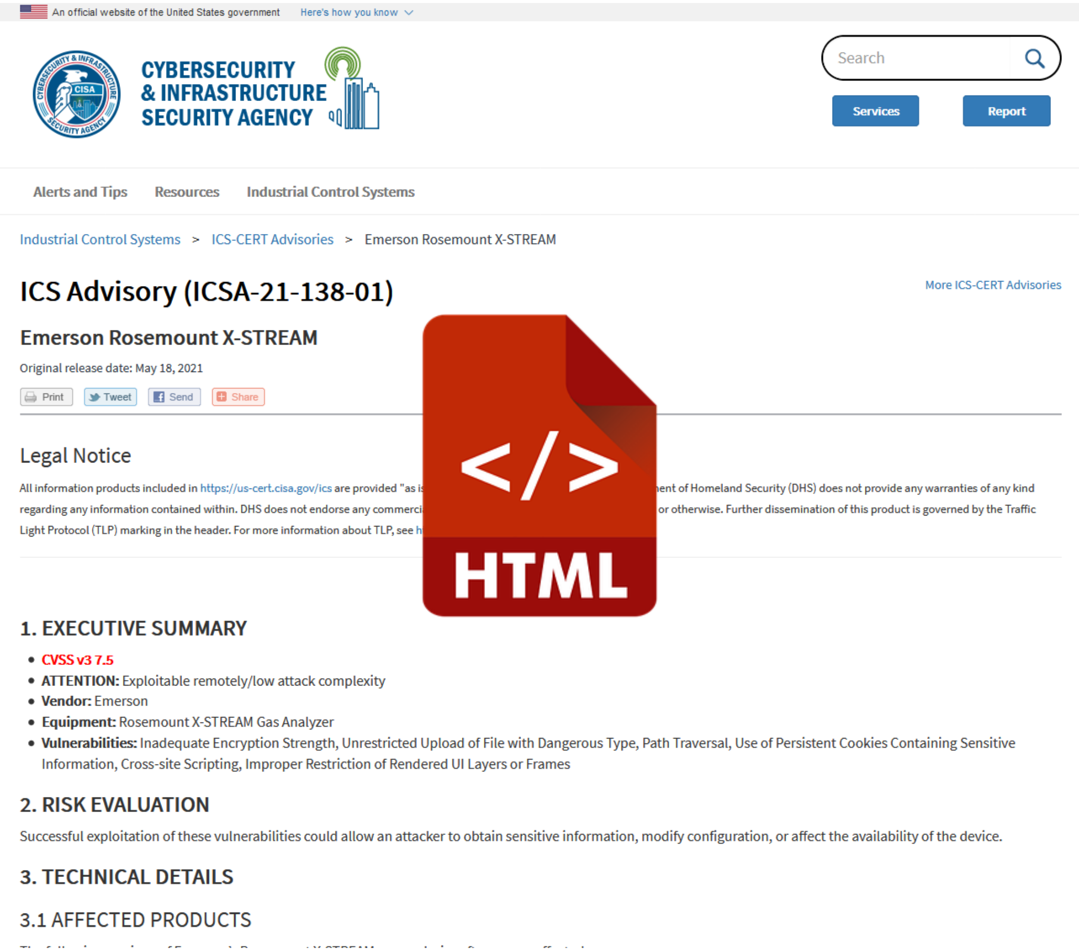
~~5~~ ~~10~~ 13 ~~2~~ ~~3~~ ~~6~~ ~~7~~ 9 12 ~~15~~ 8 14 ~~1~~ 4 11

# Find


Bosch PSIRT Security Advisories
Security advisories
Security Advisories
Industrial Cybersecurity
Recently Released
Canadian Centre for
Canada
SIEMENS
Search Security Advisories
Vulnerability Notes Database
Recently Published Vulnerabilities
Software Engineering Institute
sprecher automation
SECURITY ALERTS
SECURITY ADVISORY, CONFIGURATION-FILE INPUT VALIDATION VULNERABILITY
PEPPERL+FUCHS
Cyber Security Information and Reporting
VDE CERT
Advisories
ABB
Cyber security notifications
2021
JPCERT CC
Towards a safer cyber space without incidents
Schneider Electric
Stay Informed
westermo
Cyber Security
Cyber Security Guidelines
Cyber Security Advisories and Notices
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
ICS-CERT Advisories

Federal Office
for Information Security

# Analyze



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

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Industrial Control Systems > ICS-CERT Advisories > Emerson Rosemount X-STREAM

## ICS Advisory (ICSA-21-138-01)

More ICS-CERT Advisories

### Emerson Rosemount X-STREAM

Original release date: May 18, 2021

### Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as i ent of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commerci or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see h

### 1. EXECUTIVE SUMMARY

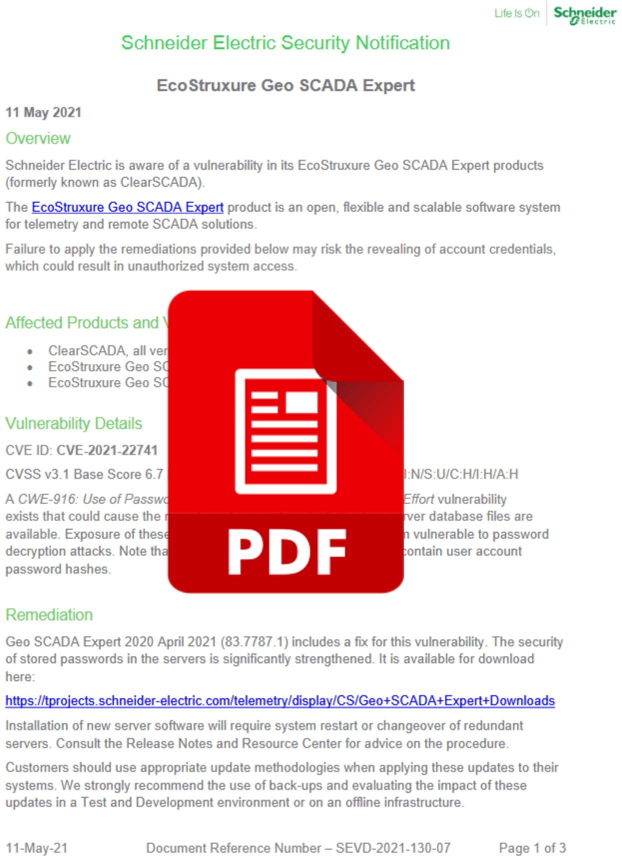
- CVSS v3 7.5
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Emerson
- **Equipment:** Rosemount X-STREAM Gas Analyzer
- **Vulnerabilities:** Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Type, Path Traversal, Use of Persistent Cookies Containing Sensitive Information, Cross-site Scripting, Improper Restriction of Rendered UI Layers or Frames

### 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



## Schneider Electric Security Notification

### EcoStruxure Geo SCADA Expert

**11 May 2021**

### Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure Geo SCADA Expert products (formerly known as ClearSCADA).

The EcoStruxure Geo SCADA Expert product is an open, flexible and scalable software system for telemetry and remote SCADA solutions.

Failure to apply the remediations provided below may risk the revealing of account credentials, which could result in unauthorized system access.

### Affected Products and V

- ClearSCADA, all ver
- EcoStruxure Geo SC
- EcoStruxure Geo SC

### Vulnerability Details

CVE ID: **CVE-2021-22741**

CVSS v3.1 Base Score 6.7 I:N/S:U/C:H/I:H/A:H

A *CWE-916: Use of Passwo* *Effort* vulnerability exists that could cause the r ver database files are available. Exposure of these n vulnerable to password decryption attacks. Note tha contain user account password hashes.

### Remediation

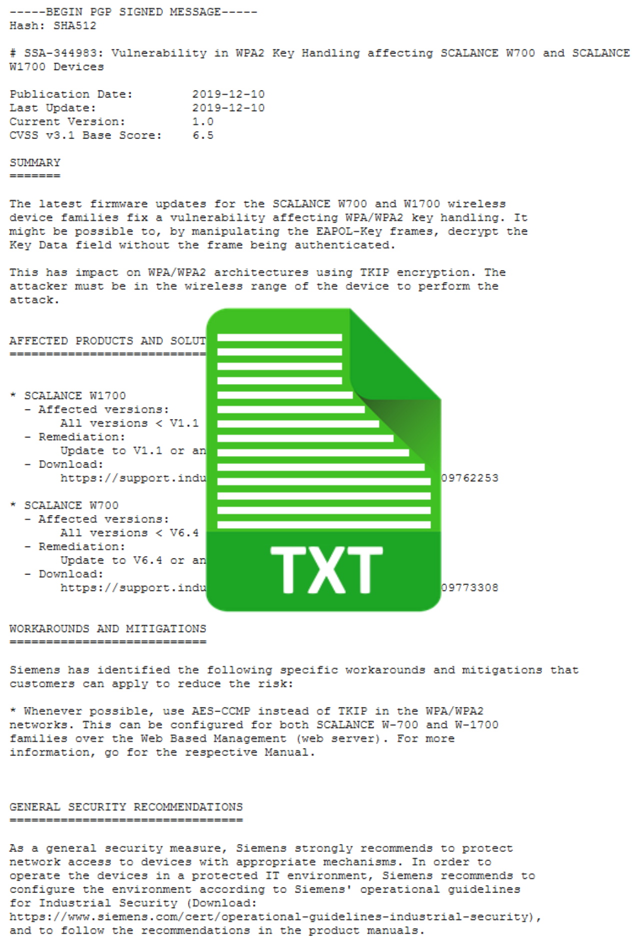
Geo SCADA Expert 2020 April 2021 (83.7787.1) includes a fix for this vulnerability. The security of stored passwords in the servers is significantly strengthened. It is available for download here:

https://tprojects.schneider-electric.com/telemetry/display/CS/Geo+SCADA+Expert+Downloads

Installation of new server software will require system restart or changeover of redundant servers. Consult the Release Notes and Resource Center for advice on the procedure.

Customers should use appropriate update methodologies when applying these updates to their systems. We strongly recommend the use of back-ups and evaluating the impact of these updates in a Test and Development environment or on an offline infrastructure.

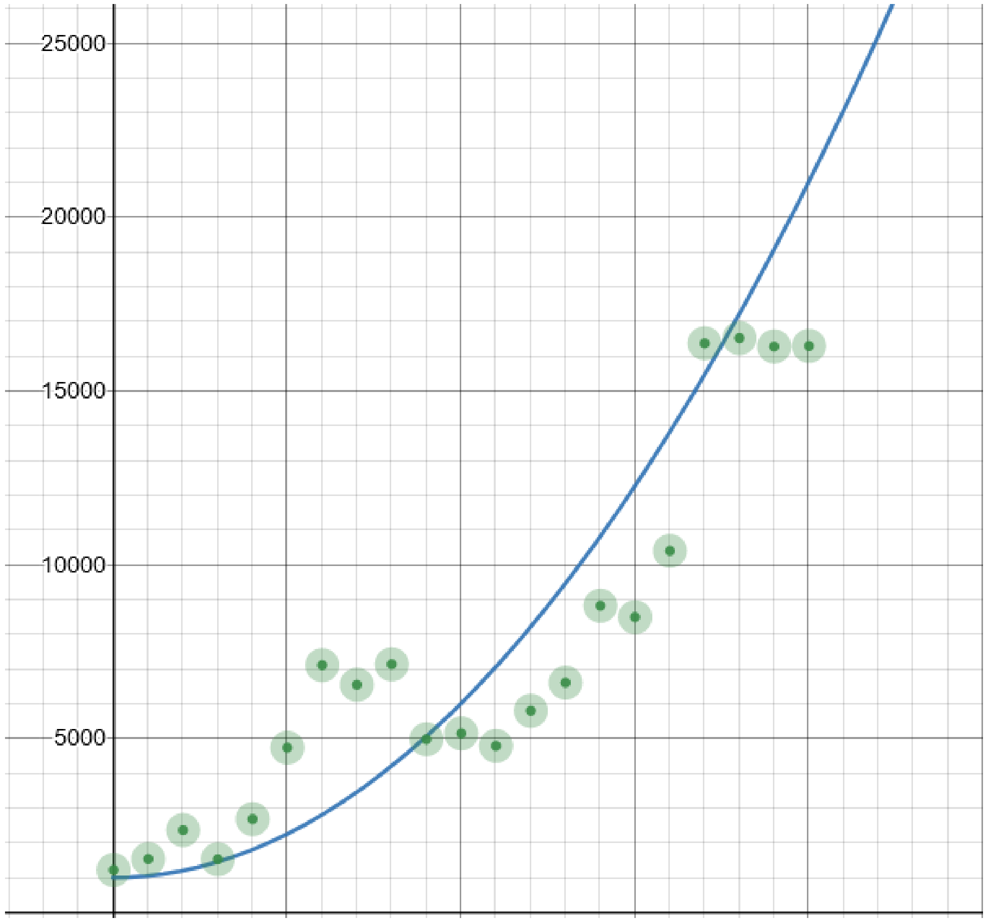
11-May-21 Document Reference Number – SEVD-2021-130-07 Page 1 of 3



```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

# SSA-344983: Vulnerability in WPA2 Key Handling affecting SCALANCE W700 and SCALANCE
W1700 Devices

Publication Date:        2019-12-10
Last Update:             2019-12-10
Current Version:         1.0
CVSS v3.1 Base Score:    6.5

SUMMARY
=======

The latest firmware updates for the SCALANCE W700 and W1700 wireless
device families fix a vulnerability affecting WPA/WPA2 key handling. It
might be possible to, by manipulating the EAPOL-Key frames, decrypt the
Key Data field without the frame being authenticated.

This has impact on WPA/WPA2 architectures using TKIP encryption. The
attacker must be in the wireless range of the device to perform the
attack.


AFFECTED PRODUCTS AND SOLUT
=============================


* SCALANCE W1700
  - Affected versions:
      All versions < V1.1
  - Remediation:
      Update to V1.1 or an
  - Download:
      https://support.indu                                 09762253

* SCALANCE W700
  - Affected versions:
      All versions < V6.4
  - Remediation:
      Update to V6.4 or an
  - Download:
      https://support.indu                                 09773308

WORKAROUNDS AND MITIGATIONS
===========================

Siemens has identified the following specific workarounds and mitigations that
customers can apply to reduce the risk:

* Whenever possible, use AES-CCMP instead of TKIP in the WPA/WPA2
networks. This can be configured for both SCALANCE W-700 and W-1700
families over the Web Based Management (web server). For more
information, go for the respective Manual.



GENERAL SECURITY RECOMMENDATIONS
================================

As a general security measure, Siemens strongly recommends to protect
network access to devices with appropriate mechanisms. In order to
operate the devices in a protected IT environment, Siemens recommends to
configure the environment according to Siemens' operational guidelines
for Industrial Security (Download:
https://www.siemens.com/cert/operational-guidelines-industrial-security),
and to follow the recommendations in the product manuals.
```

# Number of Advisories

# Number of ~~Advisories~~ CVE



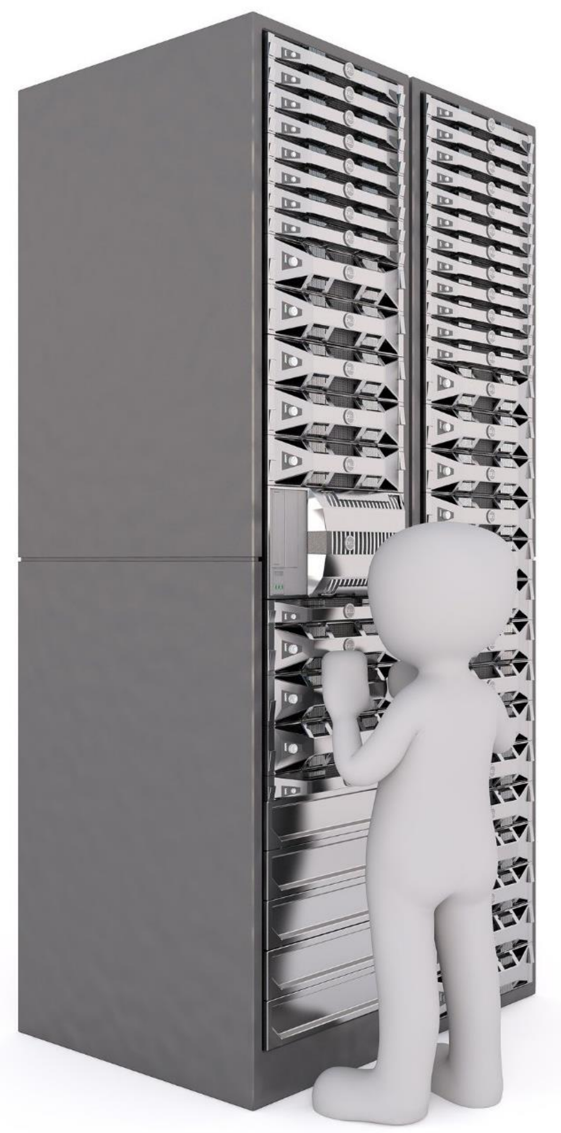
Federal Office
for Information Security

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

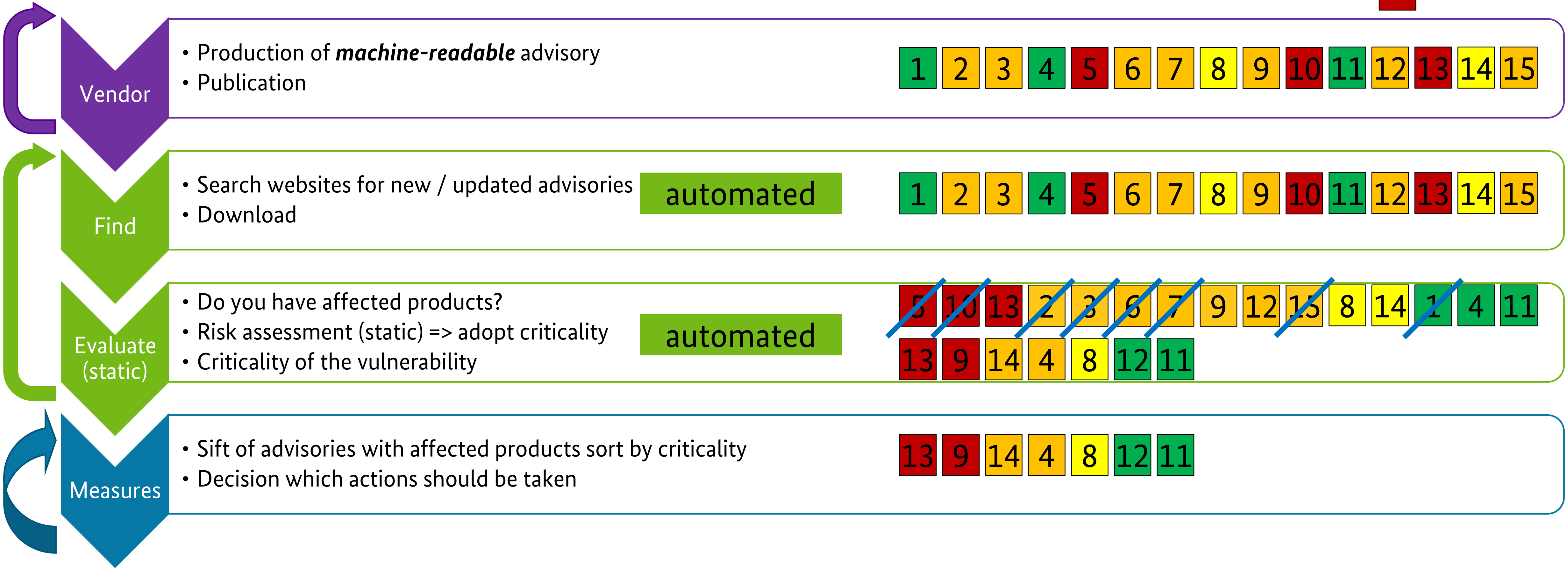
Severity of advisory

🟩 low

🟨 medium

🟧 high

🟥 critical



Vendor

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

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Find

- Search websites for new / updated advisories
- Download

automated

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Evaluate (static)

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

automated

~~5~~ ~~10~~ 13 ~~2~~ ~~3~~ ~~6~~ ~~7~~ 9 12 ~~15~~ 8 14 ~~1~~ 4 11

13 9 14 4 8 12 11

Measures

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

13 9 14 4 8 12 11

Federal Office
for Information Security

# What is CSAF?

**Common Security Advisory Framework**

- International, open and free standard
- 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

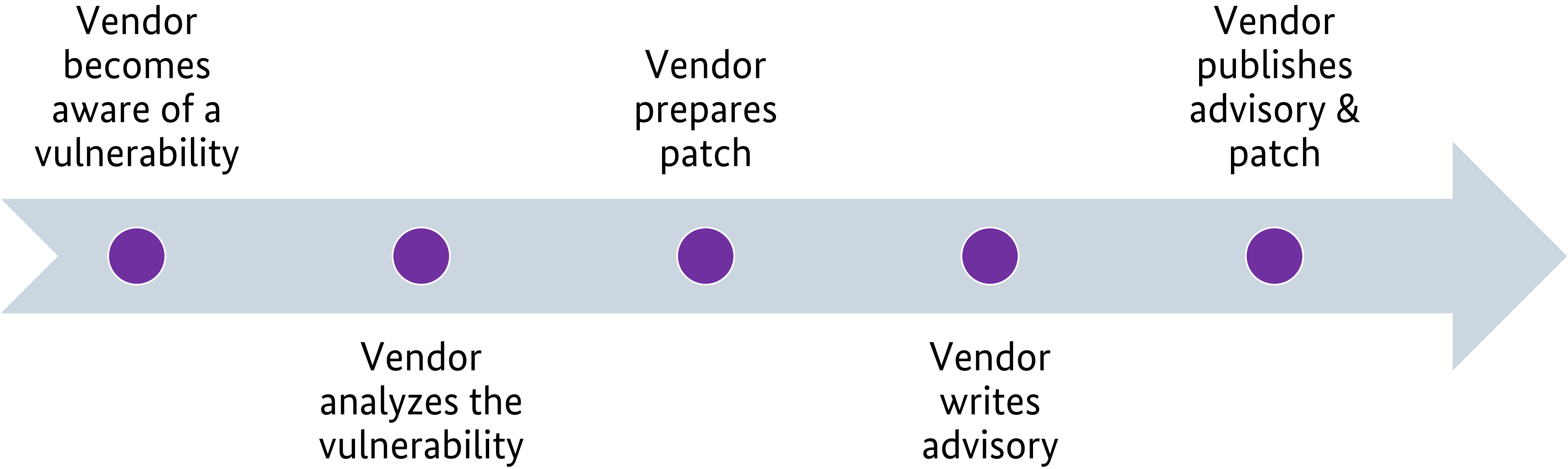
Ready to use!

# Requirements for asset owners

- Machine-readable asset inventory
- Request Advisories in CSAF from vendors
- Connection between both of them to leverage the full potential

# Vendors’ Perspective

# Vendor


Vendor becomes aware of a vulnerability

Vendor analyzes the vulnerability

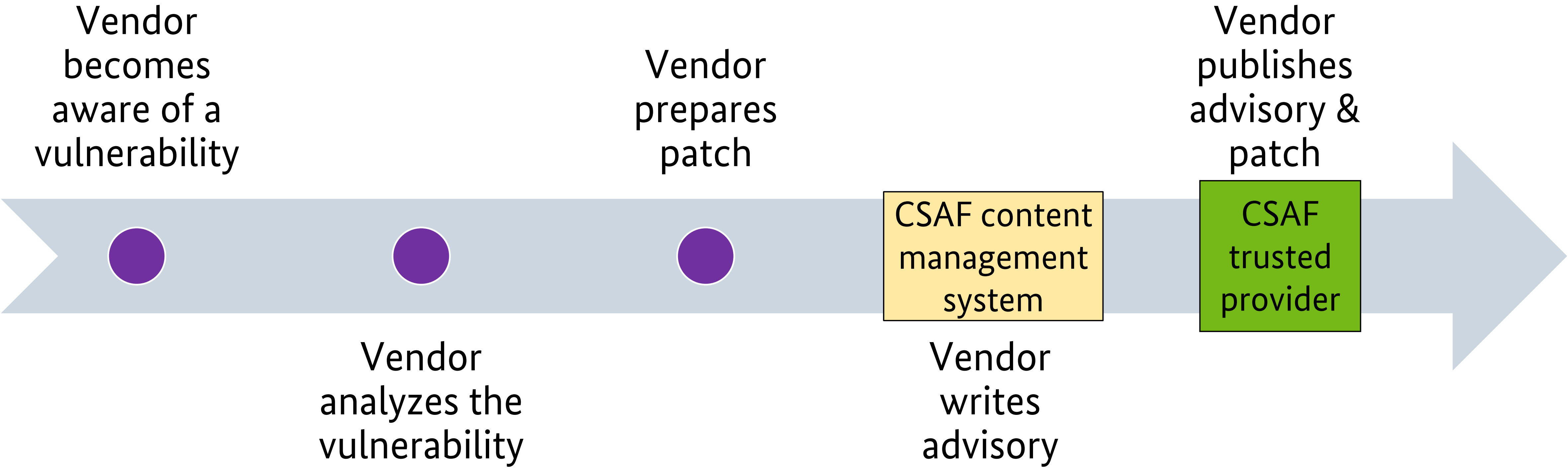
Vendor prepares patch

Vendor writes advisory

Vendor publishes advisory & patch

Federal Office
for Information Security

# Vendor



Vendor becomes aware of a vulnerability

Vendor analyzes the vulnerability

Vendor prepares patch

Vendor writes advisory

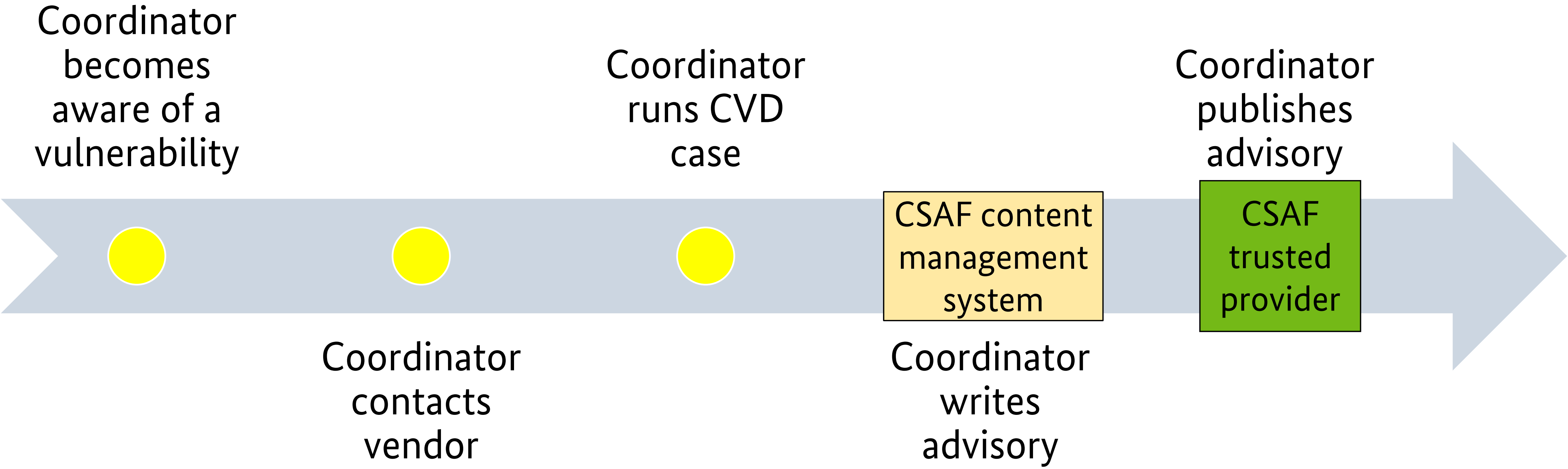
CSAF content management system

Vendor publishes advisory & patch

CSAF trusted provider

Federal Office for Information Security

# Coordinator (CVD)



Coordinator becomes aware of a vulnerability

Coordinator contacts vendor

Coordinator runs CVD case

CSAF content management system

Coordinator writes advisory

Coordinator publishes advisory

CSAF trusted provider

Federal Office
for Information Security

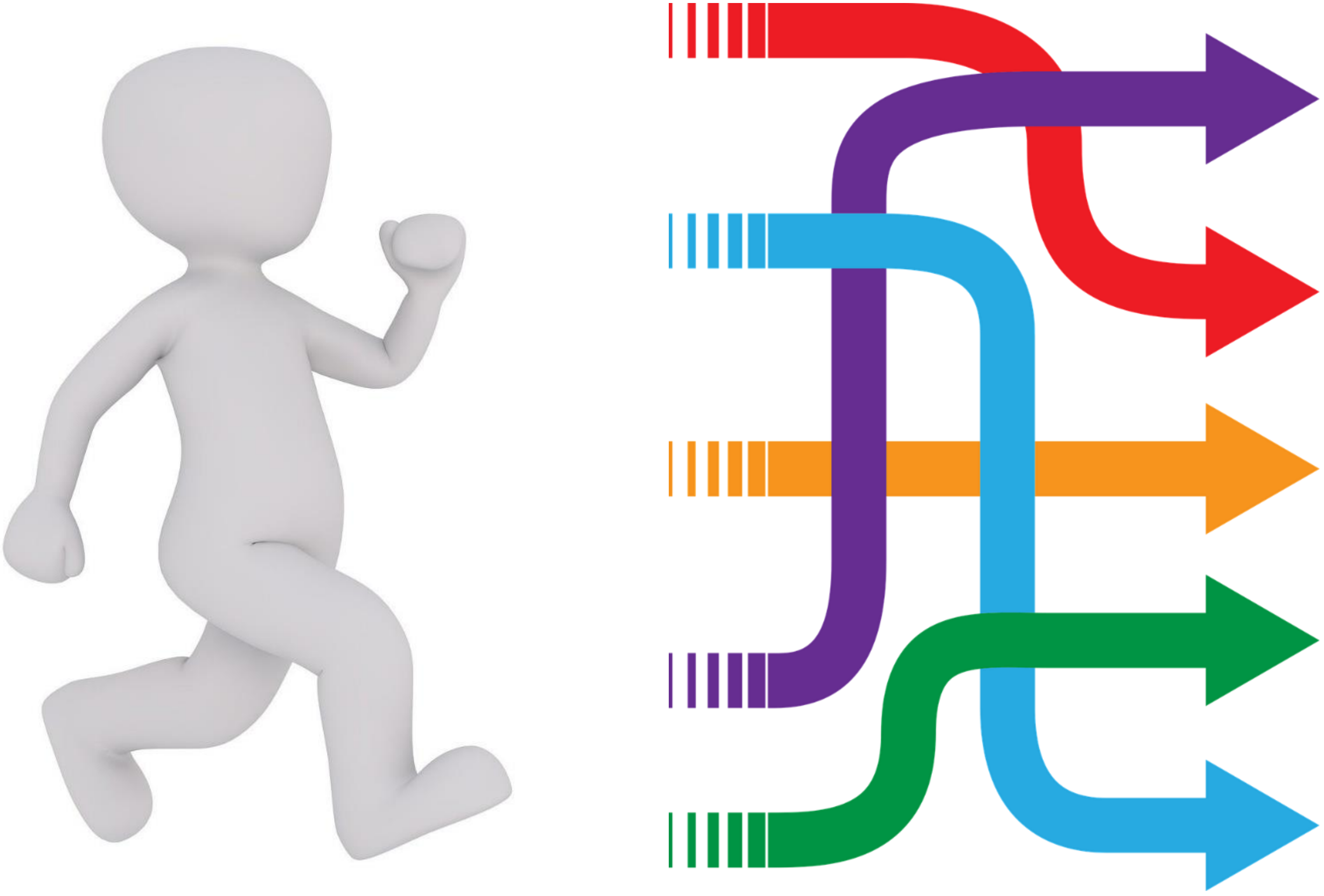
# Distribution

# Where to find CSAF documents?

| | |
|---|---|
| ✓ Valid CSAF documents<br>✓ File name restrictions<br>✓ TLS enforced<br>✓ TLP:WHITE freely accessible | CSAF publisher |
| ✓ Well-defined URL / security.txt / DNS => provider-metadata.json<br>✓ List of advisories and latest changes and Fixed folder structure<br>✓ or ROLIE feeds<br>✓ Restriction on >=TLP:AMBER<br>✓ All requirements from CSAF publisher | CSAF provider |
| ✓ Sign own advisories<br>✓ Hash advisories<br>✓ Published OpenPGP keys for integrity checks<br>✓ All requirements from CSAF provider | CSAF trusted provider |

https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html#7-distributing-csaf-documents

# Everything perfect?



CSAF publisher

CSAF provider

CSAF trusted provider

Federal Office
for Information Security

# Obviously not! Still many sources of information

| | | | | | |
|---|---|---|---|---|---|
| CSAF publisher | CSAF publisher | CSAF publisher | CSAF provider | CSAF publisher | CSAF provider |
| CSAF publisher | CSAF publisher | CSAF trusted provider | CSAF publisher | CSAF provider | CSAF publisher |
| CSAF publisher | CSAF trusted provider | CSAF provider | CSAF provider | CSAF provider | CSAF trusted provider |
| CSAF trusted provider | CSAF trusted provider | CSAF trusted provider | CSAF provider | CSAF publisher | CSAF publisher |
| CSAF publisher | CSAF publisher | CSAF publisher | CSAF publisher | CSAF trusted provider | CSAF provider |
| CSAF trusted provider | CSAF provider | CSAF publisher | CSAF publisher | CSAF publisher | CSAF provider |
| CSAF trusted provider | CSAF trusted provider | CSAF trusted provider | CSAF trusted provider | CSAF provider | CSAF trusted provider |

# One more step needed to make it easy …
# Saradi to the rescue!

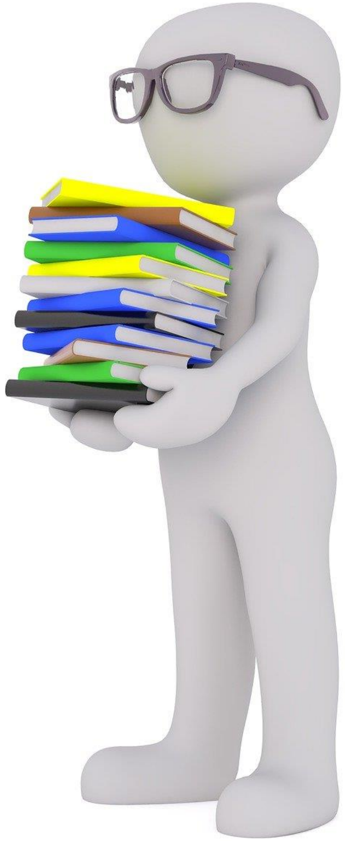
CSAF aggregator

Federal Office
for Information Security

# Scalable and resilient advisory distribution infrastructure (Saradi)

## CSAF aggregator

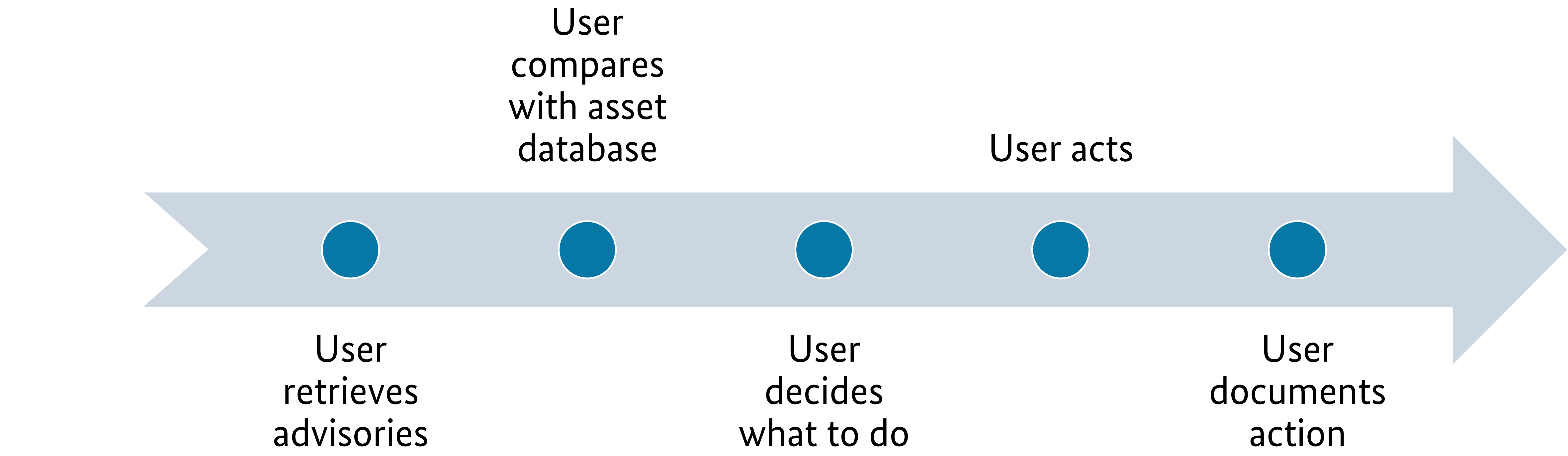
- Trusted party
- Collects advisories from issuers
- Provides them
- API optional
- One-stop-shop
- Multiple around the world (National CERTs)



Federal Office
for Information Security

# Users’ Perspective

# User



User retrieves advisories

User compares with asset database

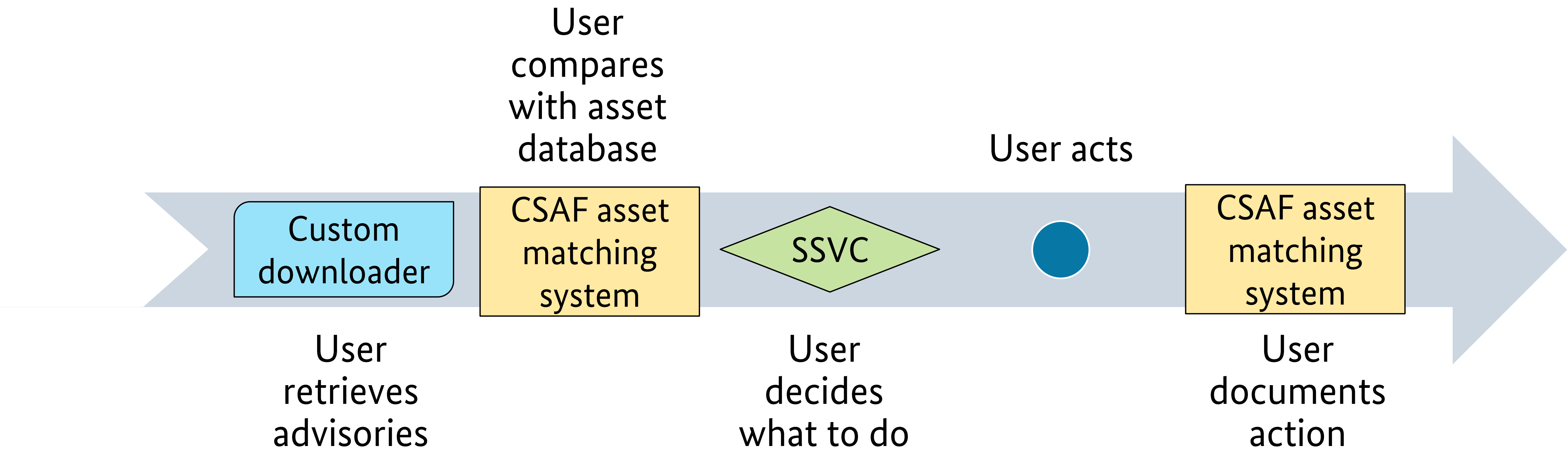
User decides what to do

User acts

User documents action

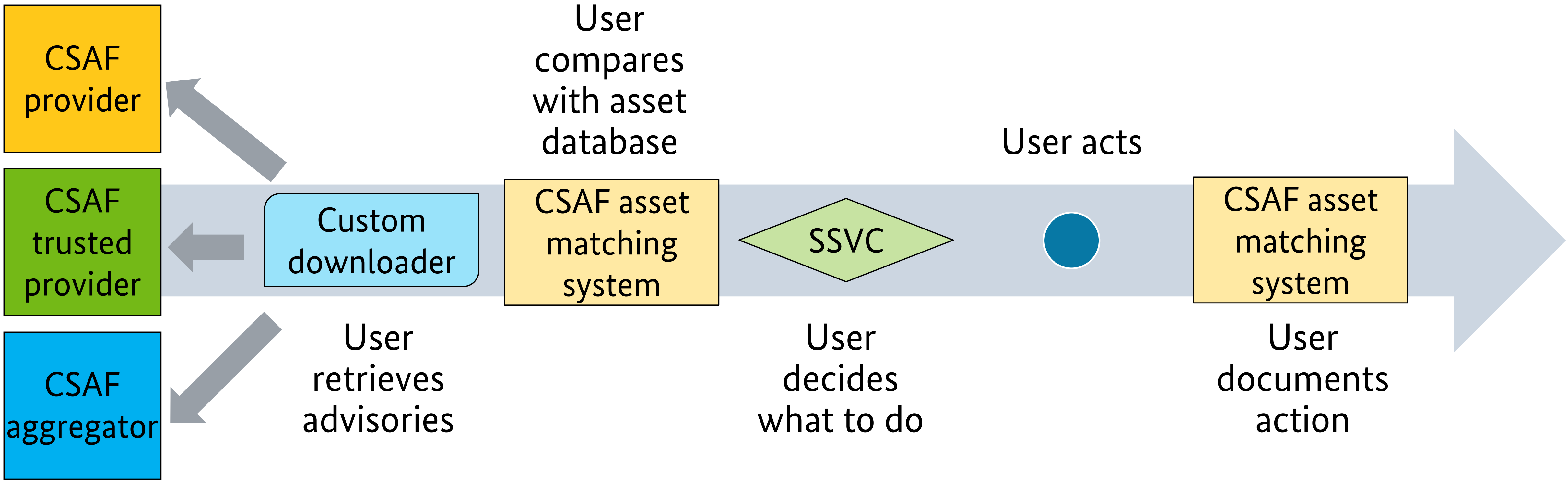
Federal Office
for Information Security

# User


User compares with asset database
User acts
Custom downloader
CSAF asset matching system
SSVC
CSAF asset matching system
User retrieves advisories
User decides what to do
User documents action

Federal Office for Information Security

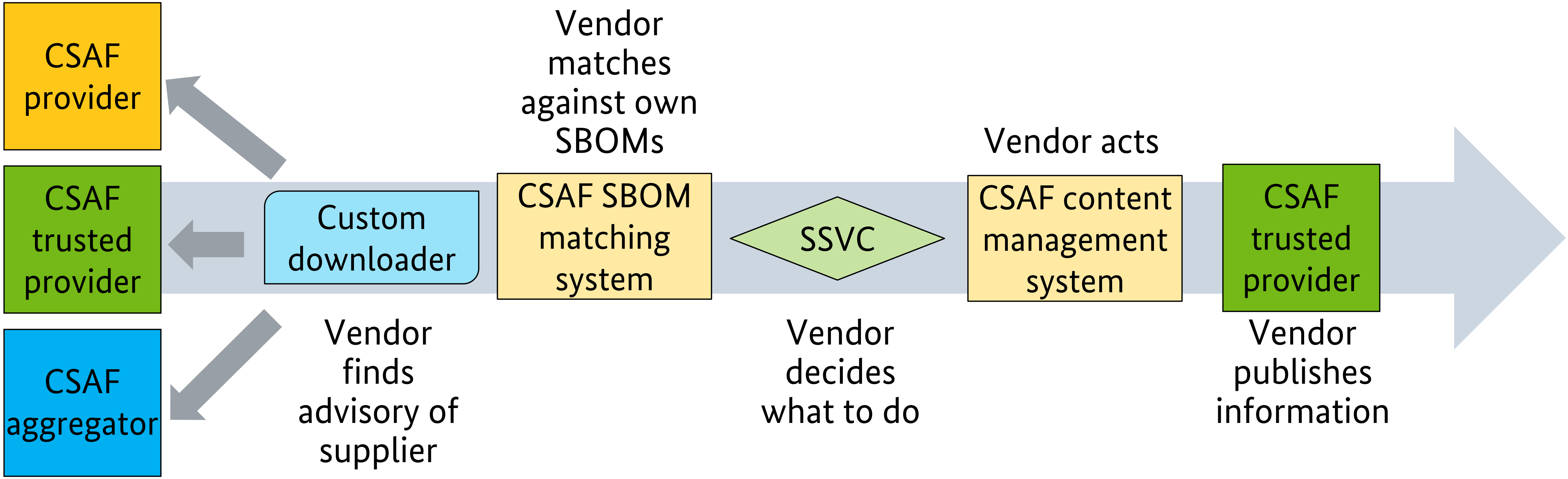
# User



Federal Office for Information Security

# Supply chain: vendors’ view

# Supply chain



CSAF provider

CSAF trusted provider

CSAF aggregator

Custom downloader

Vendor finds advisory of supplier

Vendor matches against own SBOMs

CSAF SBOM matching system

SSVC

Vendor decides what to do

Vendor acts

CSAF content management system

CSAF trusted provider

Vendor publishes information

Federal Office
for Information Security

# Tools developed by the community

- CSAF producer: https://github.com/secvisogram/secvisogram
- 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

- **Your tools?**

Federal Office
for Information Security

# What about VEX?

# VEX

- **V**ulnerability **E**xploitability e**X**change
- Communicate product status explicit
  - Not affected
  - Affected
  - Fixed
  - Under investigation
- Machine-readable to address scalability

# VEX and CSAF

- VEX is a profile in CSAF
- Specific, mandatory fields
- Uses same infrastructure and systems
- VEX is parallel to SBOM (not necessarily in the SBOM)

# CSAF in Operation

# Organizations publishing CSAF

TIBCO™

Federal Office
for Information Security

CISCO

SIEMENS

ORACLE

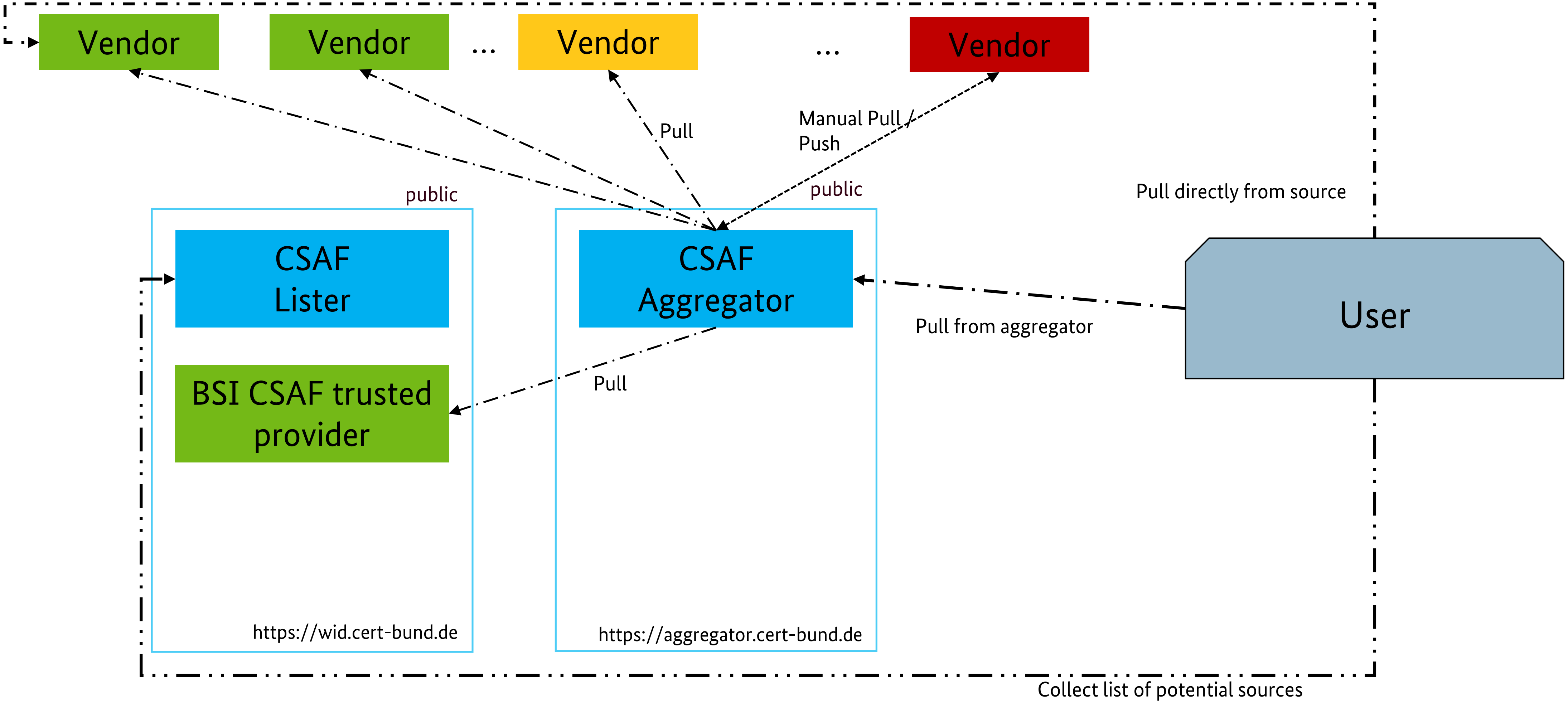
Red Hat

Life Is On | Schneider Electric

Hitachi Energy

ARISTA

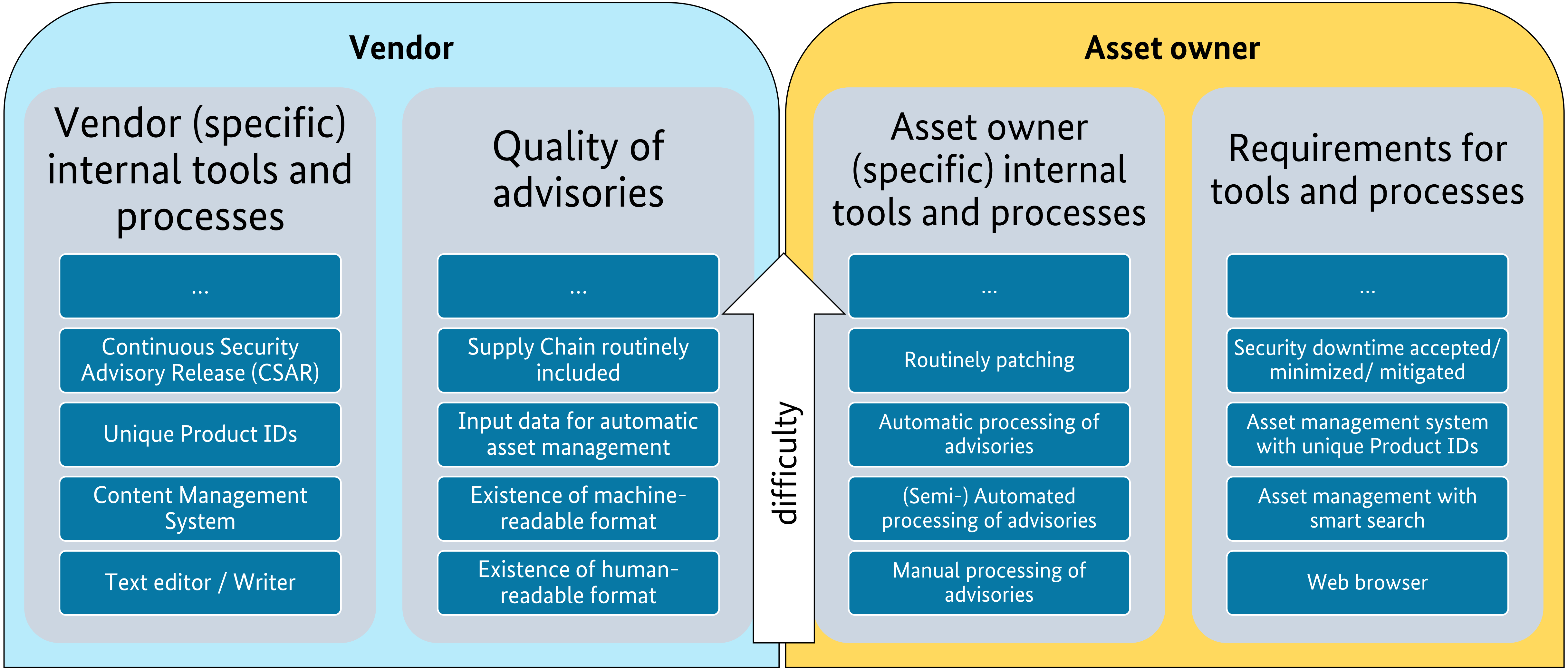
# Ecosystem



Federal Office
for Information Security

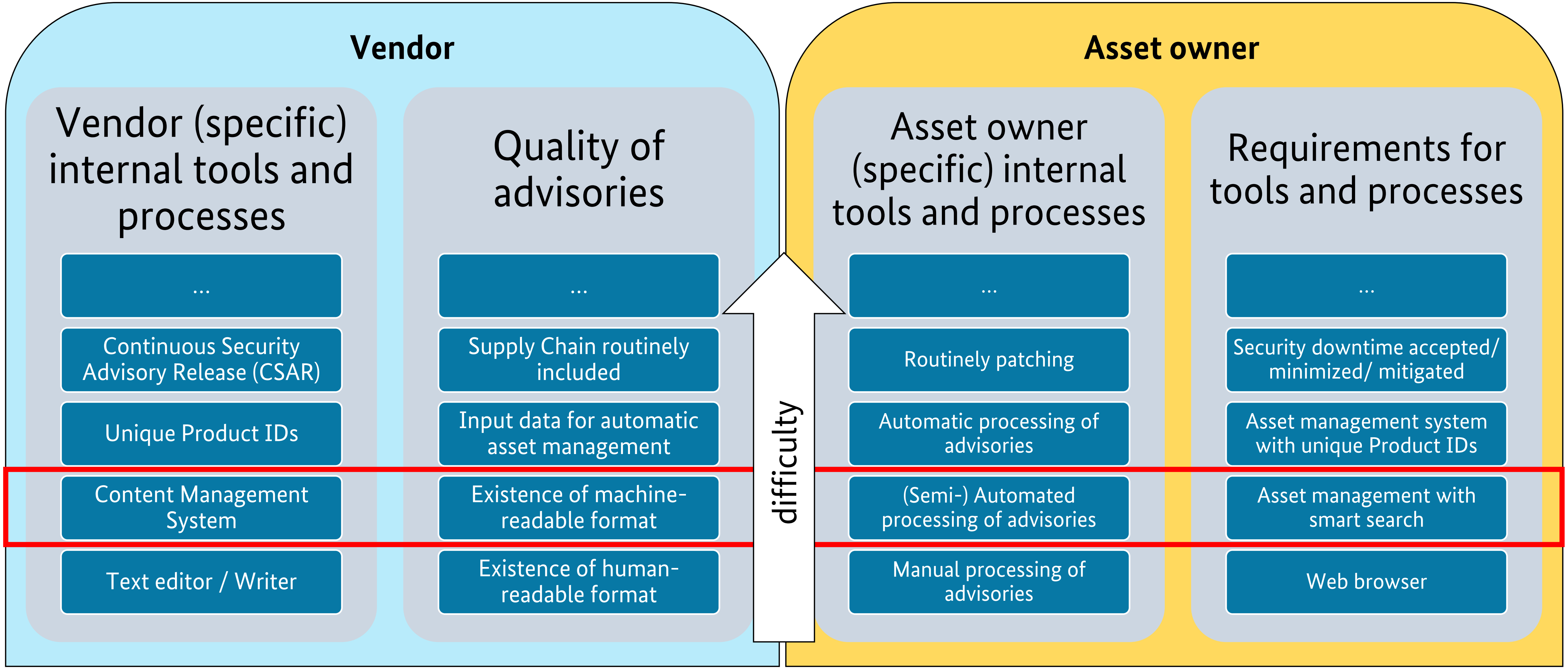
# Conclusions

# Two sides of the same coin – different maturity stages



| Vendor | | Asset owner | |
|---|---|---|---|
| Vendor (specific) internal tools and processes | Quality of advisories | Asset owner (specific) internal tools and processes | Requirements for tools and processes |
| … | … | … | … |
| Continuous Security Advisory Release (CSAR) | Supply Chain routinely included | Routinely patching | Security downtime accepted/ minimized/ mitigated |
| Unique Product IDs | Input data for automatic asset management | Automatic processing of advisories | Asset management system with unique Product IDs |
| Content Management System | Existence of machine-readable format | (Semi-) Automated processing of advisories | Asset management with smart search |
| Text editor / Writer | Existence of human-readable format | Manual processing of advisories | Web browser |

# Next step: reach stage 2 across parties



| Vendor | | Asset owner | |
|---|---|---|---|
| Vendor (specific) internal tools and processes | Quality of advisories | Asset owner (specific) internal tools and processes | Requirements for tools and processes |
| … | … | … | … |
| Continuous Security Advisory Release (CSAR) | Supply Chain routinely included | Routinely patching | Security downtime accepted/ minimized/ mitigated |
| Unique Product IDs | Input data for automatic asset management | Automatic processing of advisories | Asset management system with unique Product IDs |
| Content Management System | Existence of machine-readable format | (Semi-) Automated processing of advisories | Asset management with smart search |
| Text editor / Writer | Existence of human-readable format | Manual processing of advisories | Web browser |

# Key takeaways & actions

- Number of vulnerabilities discovered is rising
  => number of advisories as well
- Advisories are needed for risk-based decisions
- Automation is possible – so automate the boring stuff

- Request your vendors to provide CSAF 2.0
- Provide CSAF documents to your customers to ease their pain
- Send out VEX as CSAF to use the same tools
- **Spread the word! #oCSAF #advisory**

Federal Office
for Information Security

# Where to find more information?
# https://csaf.io

| | |
|---|---|
| OASIS TC: CSAF website: | 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 Prose: | https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html |
| 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 |

Mr. Thomas Schmidt
Subject Matter Expert
Industrial Automation and Control Systems

csaf@bsi.bund.de
Tel. +49 (0) 228 9582 6404
Fax +49 (0) 228 10 9582 6404
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de/dok/en_csaf

Prävention Detektion Reaktion BSI