



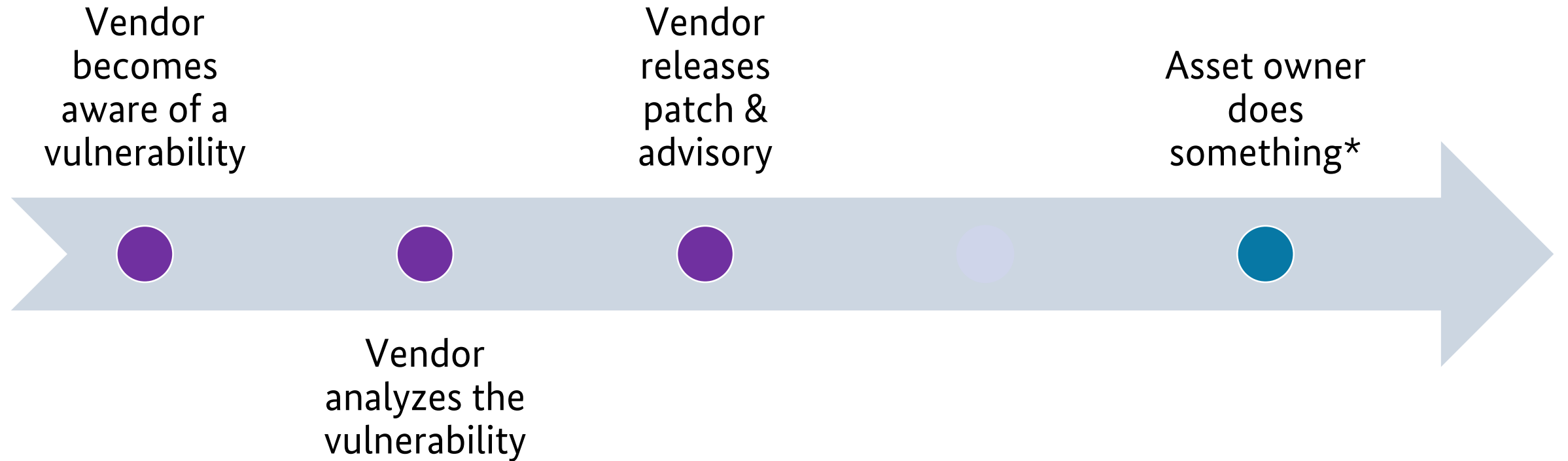
Federal Office  
for Information Security

Deutschland  
**Digital•Sicher•BSI•**

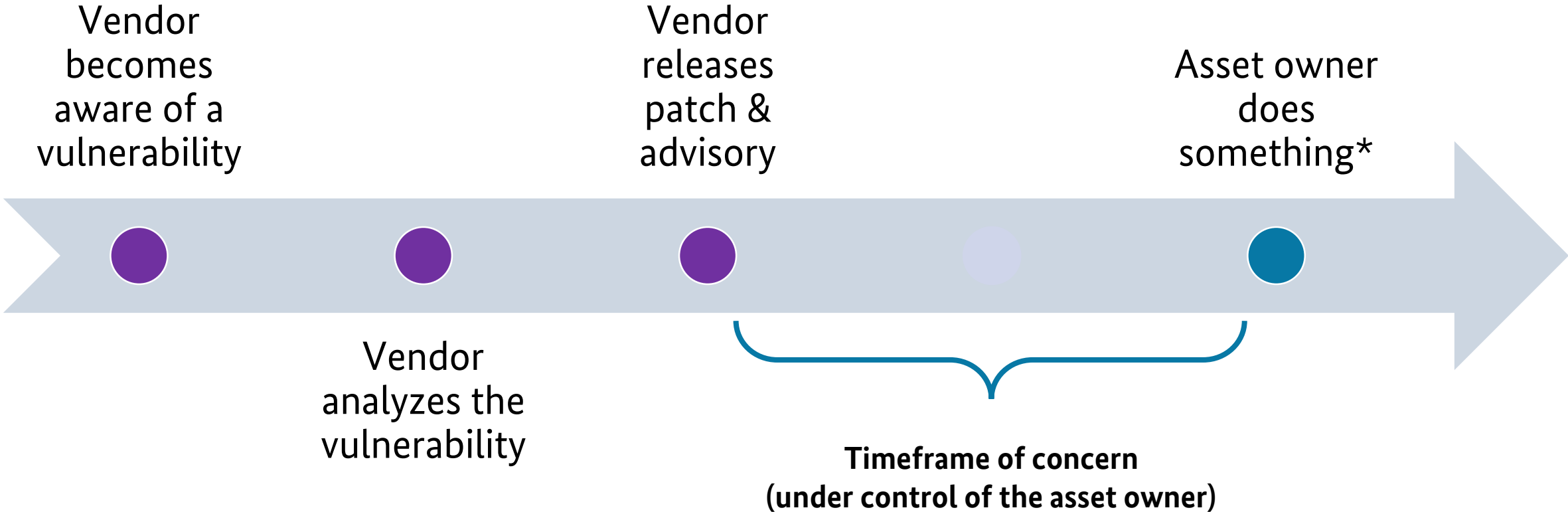
# Vulnerability Management 2.0: Automation as key to IT Security – also in Industrial Control and Automation Systems

Thomas Schmidt  
Federal Office for Information Security (BSI)

# Timeframe of concern



# Timeframe of concern



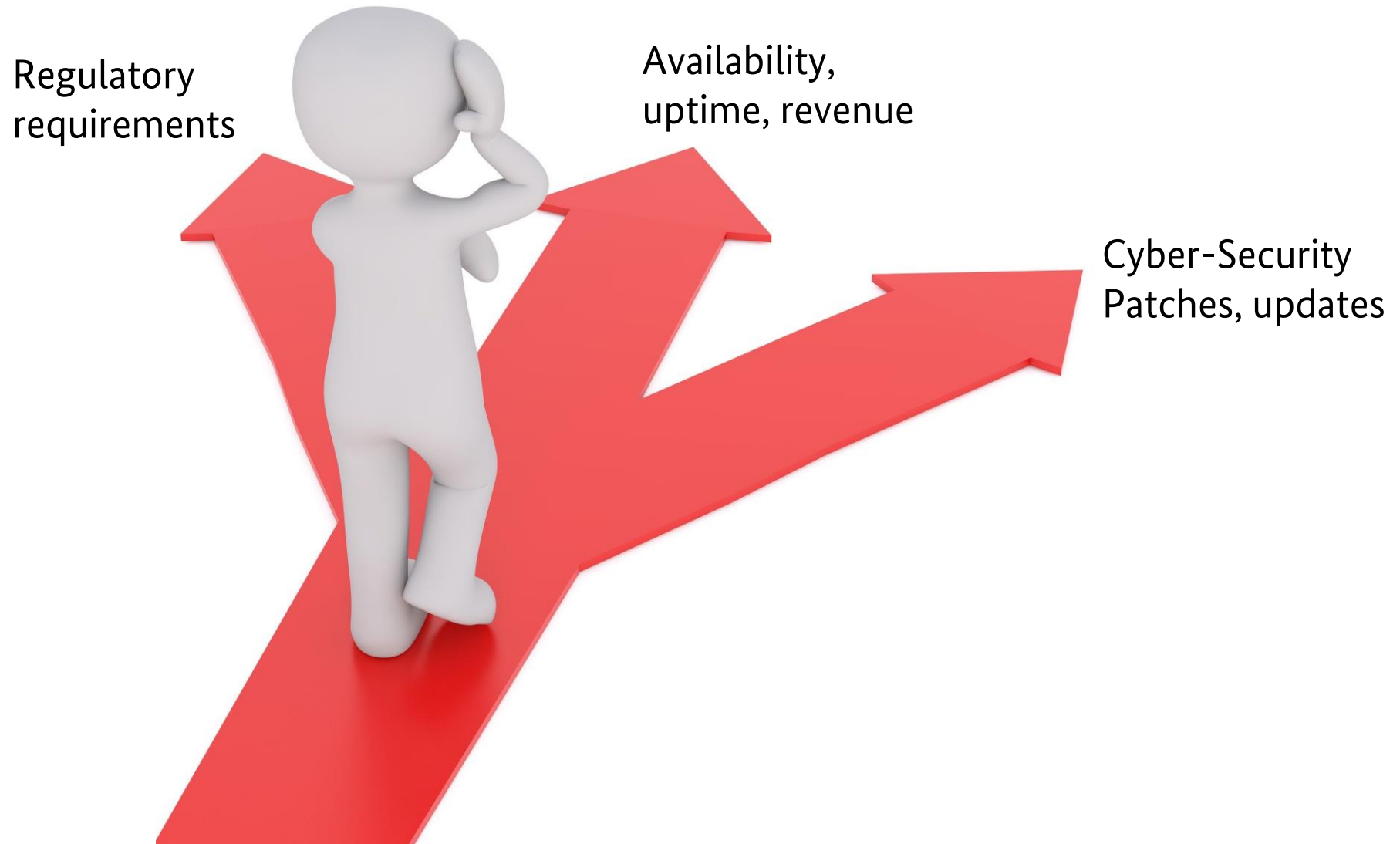
\* Patch, mitigate risk, or actively accept risk

# Asset Owners want to run their facility

Machines  
Factory lines  
Whole installations  
Usually comprise of several different vendors



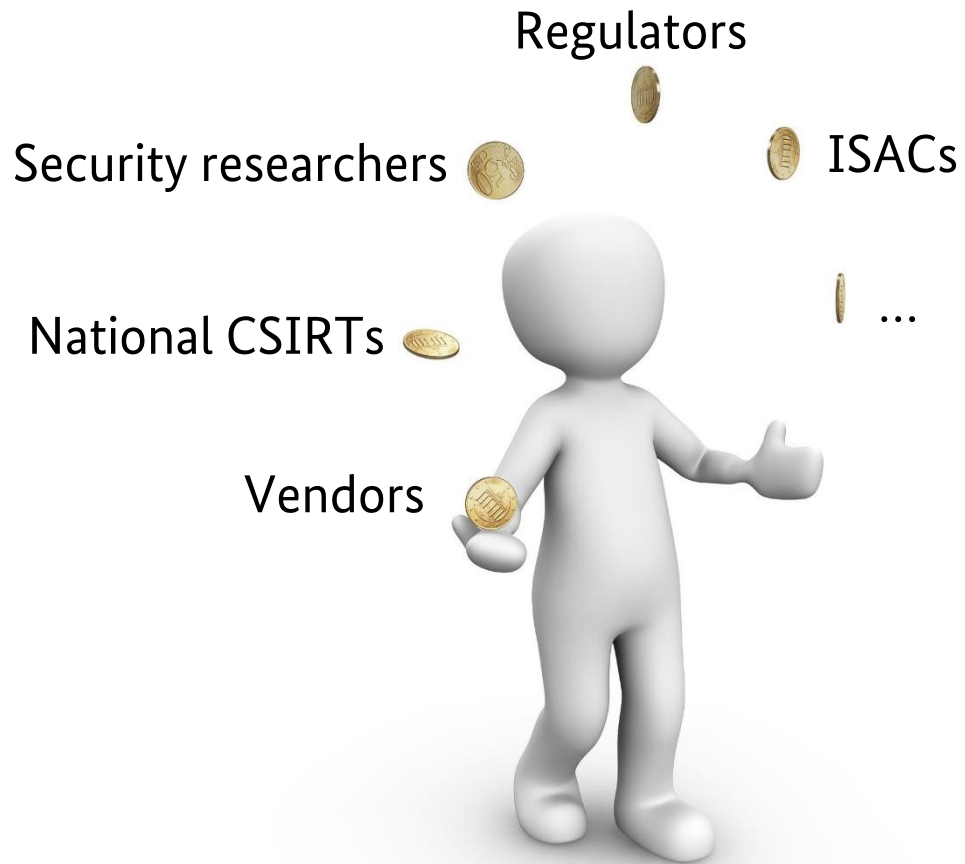
# Asset Owners are confronted with a lot of things



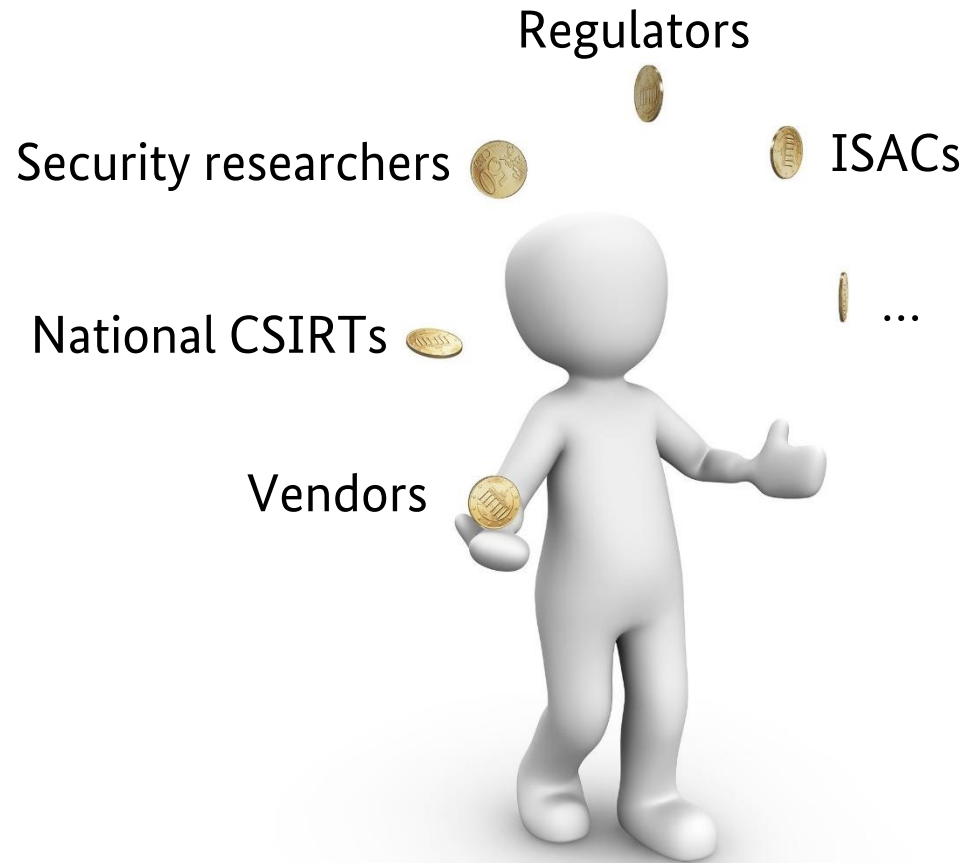
# So many vendors – some examples

ABB	Canbium	FEIG	Intel	Netgear	Samsung	TP-Link
Adobe	Networks	Festo	Joyent	Nokia	Schneider	Treck
Alcatel-Lucent	CareStream	F-Secure	Juniper	NVIDIA	Electric	Ubuntu
Apple	Caterpillar	Fujitsu	LANCOM	Oracle	Siemens	Veriv
Aruba Networks	Cisco Systems	G-Data	LG Electronics	Palo Alto	Sierra Wireless	Versiant
ASUS	Citrix	GE	Linksys	Philips	Sony	VMware
AVM	Debian	Google	Marvell	Electronics	Sophos	Wago
B. Brown	Dell	Green Hills	Semiconductor	Phoenix Contact	SUSE	Weidmüller
Barracuda	Devol	Harting	McAfee	Pilz	Swiss Control	Western Digital
Baxter	Digi	Hensoldt	MediaTek	QNAP	Systems	Wind River
Beckhoff	D-Link	HIMA	Microchip	Qualcomm	Symantec	Xerox
Belden	Eaton	Hitachi	Microsoft	Red Hat	Synology	Xiaomi
Belkin	Emerson	Honeywell	Mitsubishi	Ricoh	Technicolor	Xilinx
Bender	EMU	HP	Mozilla	Riverbed	Texas	Yokogawa
BlackBerry	Endress+Hauser	Huawei	NEC	Rockwell	Instruments	Zyxel
Brother	F5	IBM	NetApp	Automation	Toshiba	...

# So many sources of information – some examples

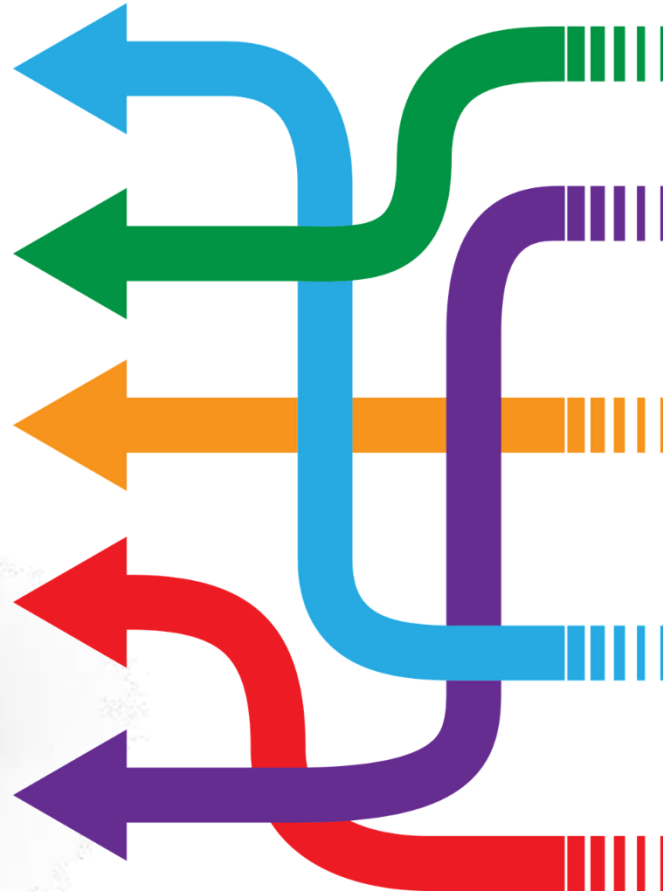


# So many sources of information – so many channels and formats



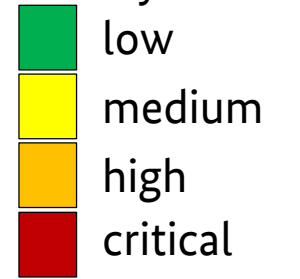


# What should an operator / asset owner do? Patches and updates!



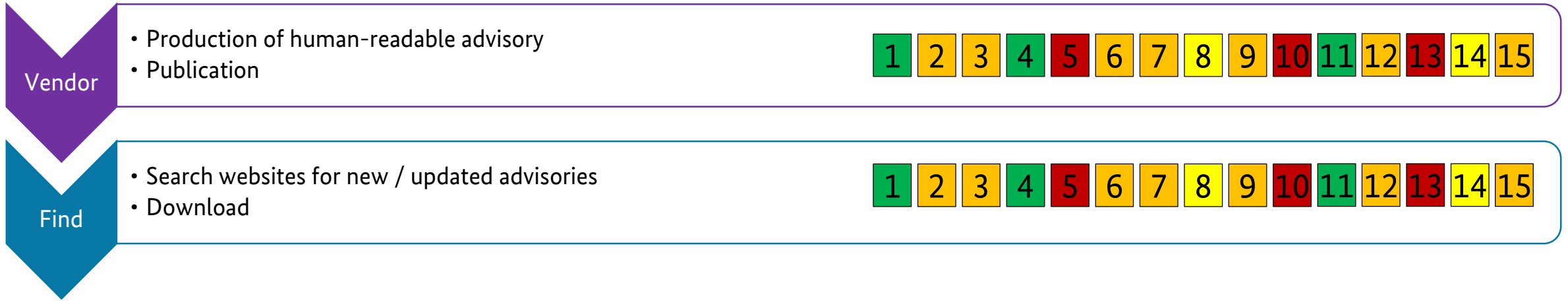
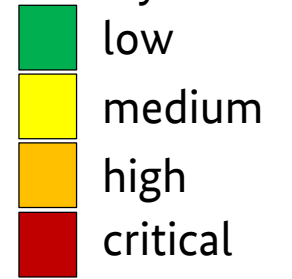
# Manual process

Severity of advisory



# Manual process

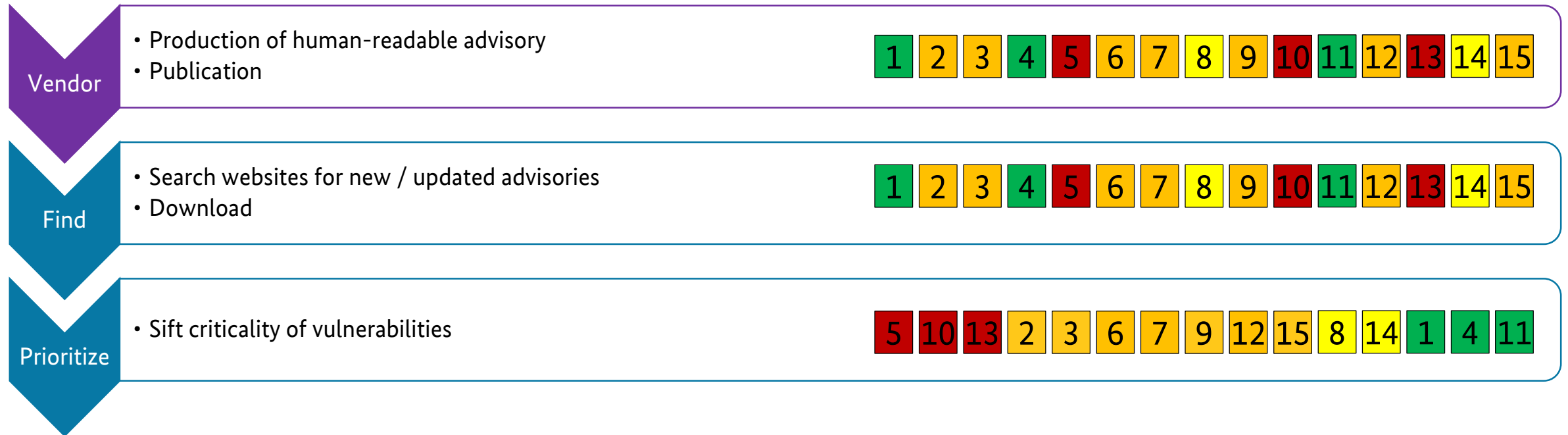
Severity of advisory



# Manual process

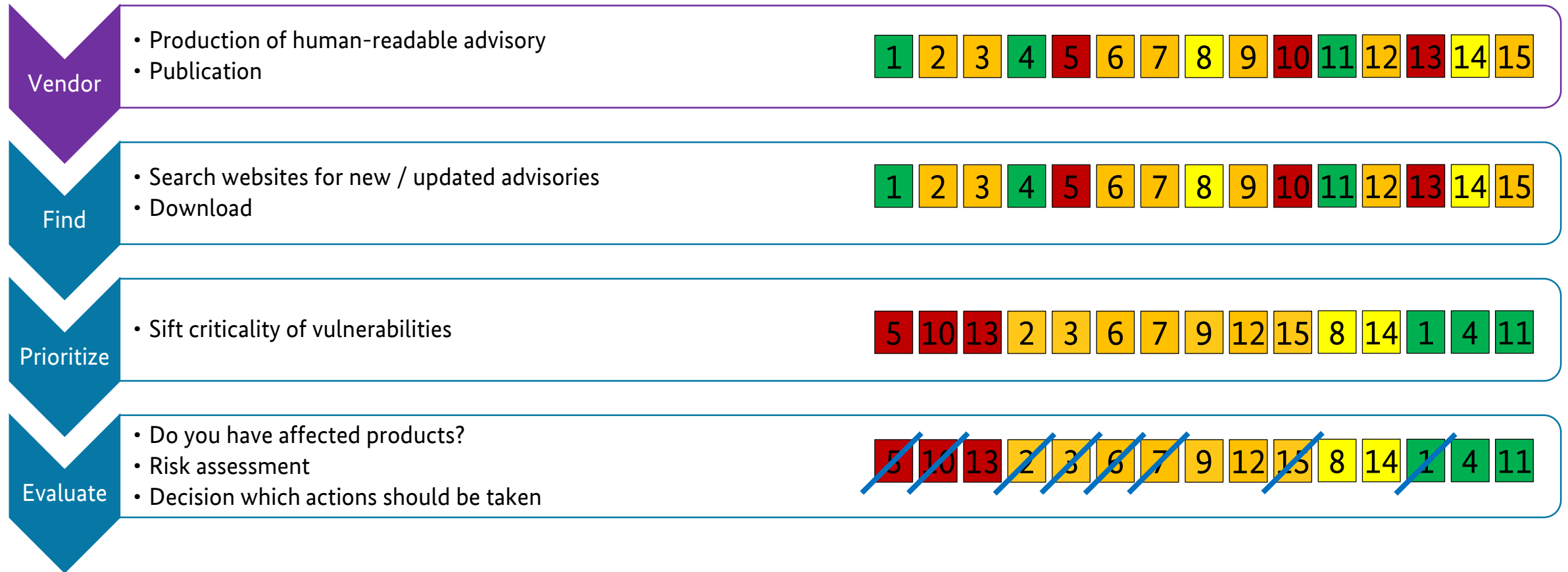
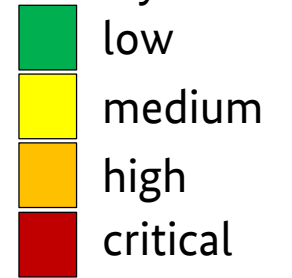
Severity of advisory

- low
- medium
- high
- critical



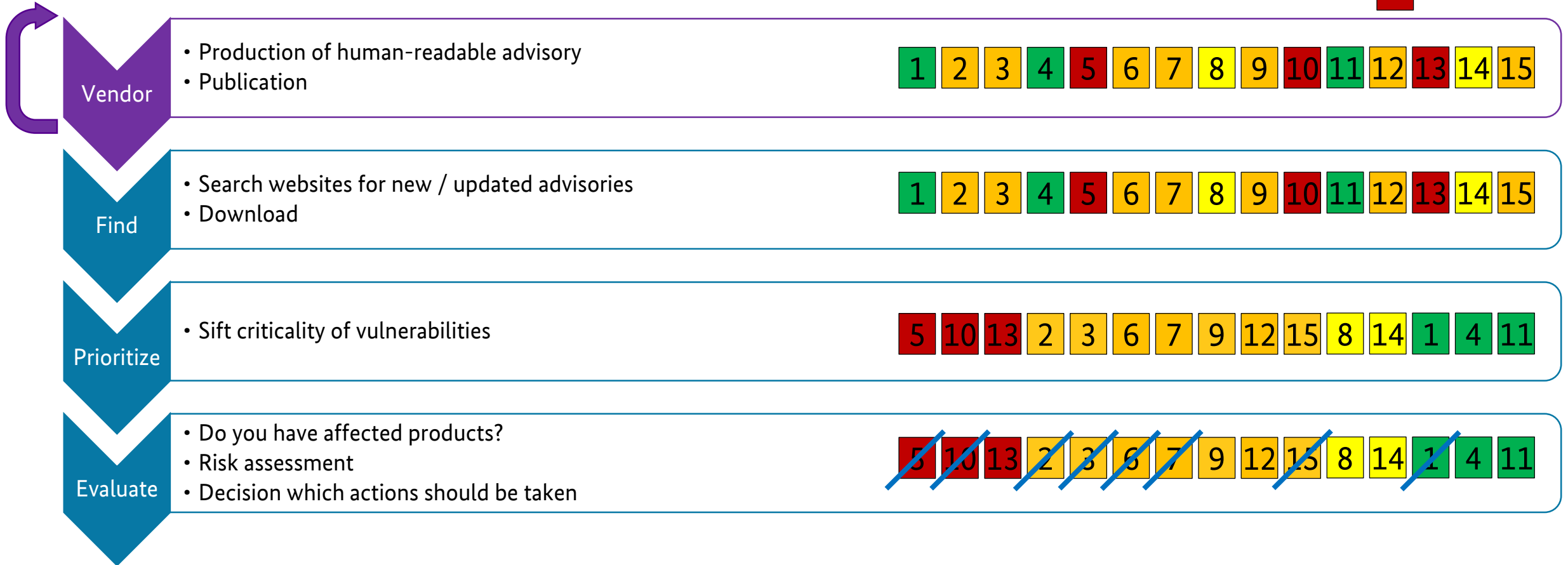
# Manual process

Severity of advisory



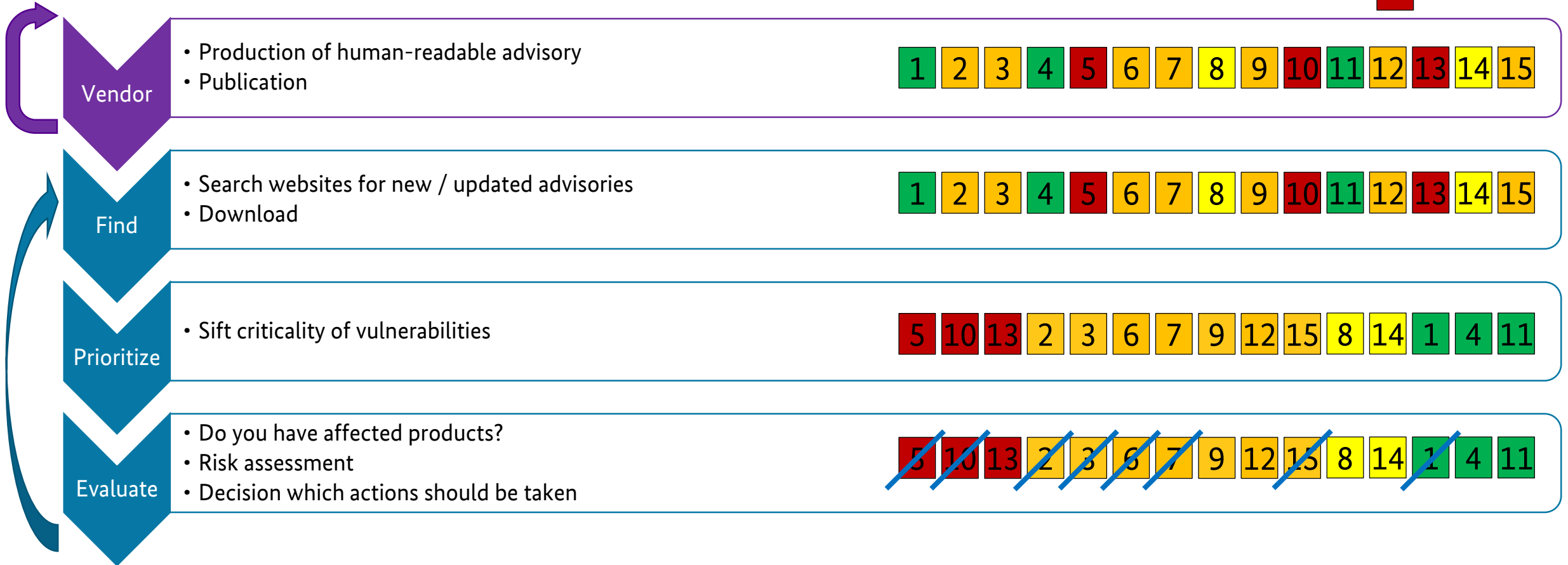
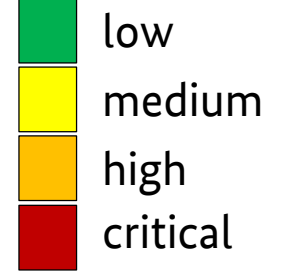
# Manual process

Severity of advisory



# Manual process

Severity of advisory








# Analyze

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)

### Emerson Rosemount X-STREAM

Original release date: May 18, 2021

Print Tweet Send Share

#### Legal Notice

All information products included in <https://us-cert.cisa.gov/ics> are provided "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the accuracy, reliability, or completeness of the information. 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 products or services, 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://www.dhs.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

## 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, all versions
- EcoStruxure Geo SCADA Expert, all versions

#### Vulnerability Details

CVE ID: CVE-2021-22741

CVSS v3.1 Base Score 6.7

A *CWE-916: Use of Passwords in URLs* vulnerability exists that could cause the disclosure of sensitive information over database files are available. Exposure of these sensitive information is vulnerable to password decryption attacks. Note that the sensitive information may 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://projects.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-344993: 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

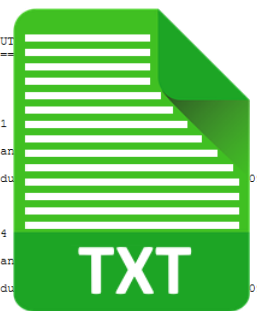
#### SUMMARY

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 SOLUTIONS

- \* SCALANCE W1700
  - Affected versions: All versions < V1.1
  - Remediation: Update to V1.1 or an earlier version
  - Download: <https://support.industry.siemens.com/cs/qa/qa-09762253>
- \* SCALANCE W700
  - Affected versions: All versions < V6.4
  - Remediation: Update to V6.4 or an earlier version
  - Download: <https://support.industry.siemens.com/cs/qa/qa-09773308>



#### WORKAROUNDS AND MITIGATIONS

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

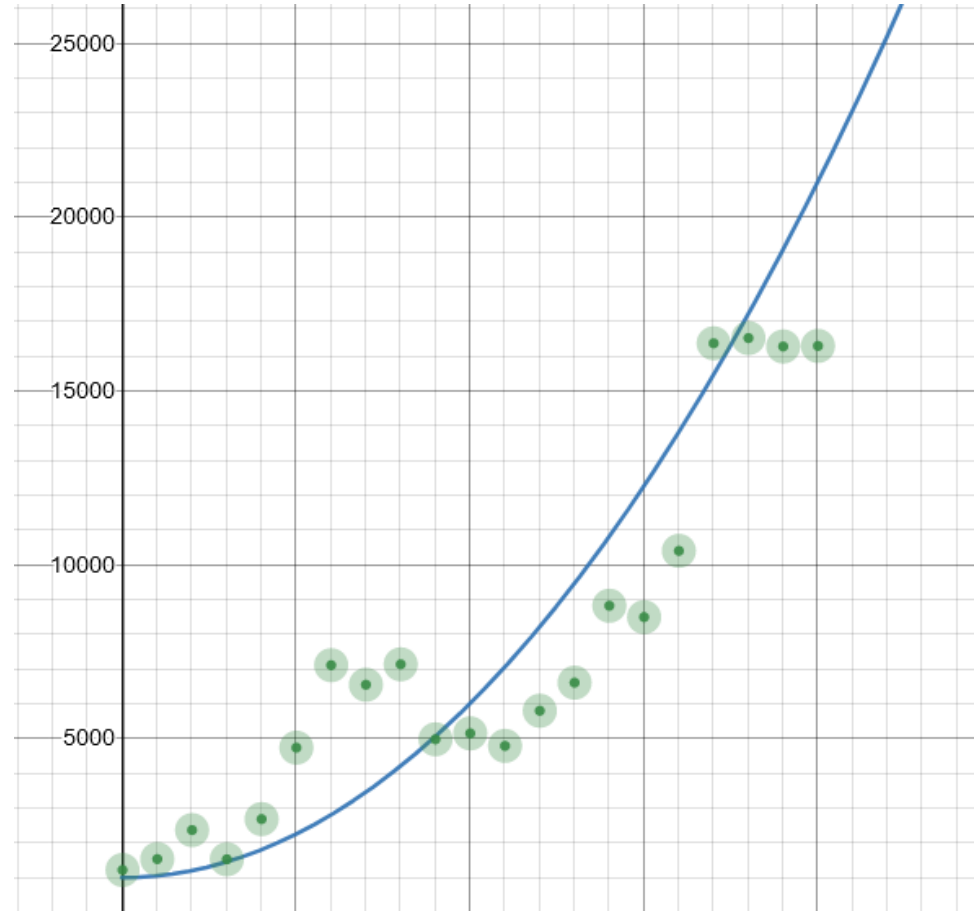
\* Whenever possible, use AES-CCMP instead of TKIP in the WPA/WPA2 networks. This can be configured for both SCALANCE W-700 and W-1700 families over the Web Based Management (web server). For more information, go for the respective Manual.

#### 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

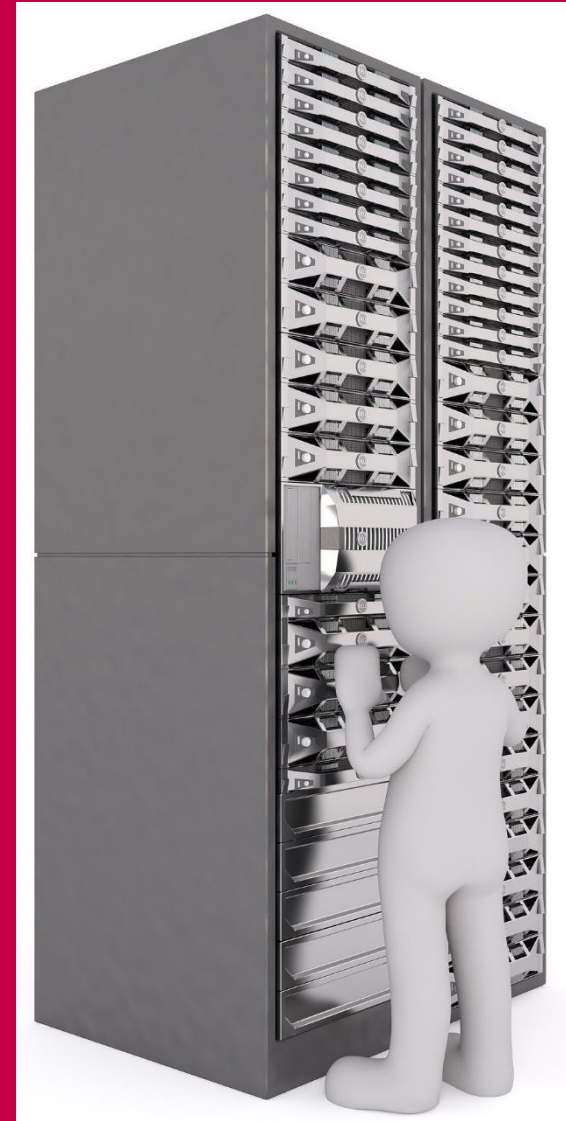


That doesn't scale!

# Possible solutions



Let's automate the process...



# Process with CSAF

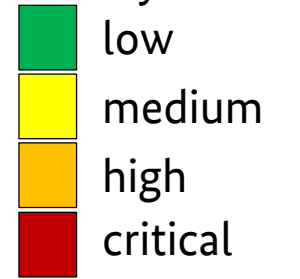
Severity of advisory

- low
- medium
- high
- critical



# Process with CSAF

Severity of advisory



Vendor

- Production of *machine-readable* advisory
- Publication



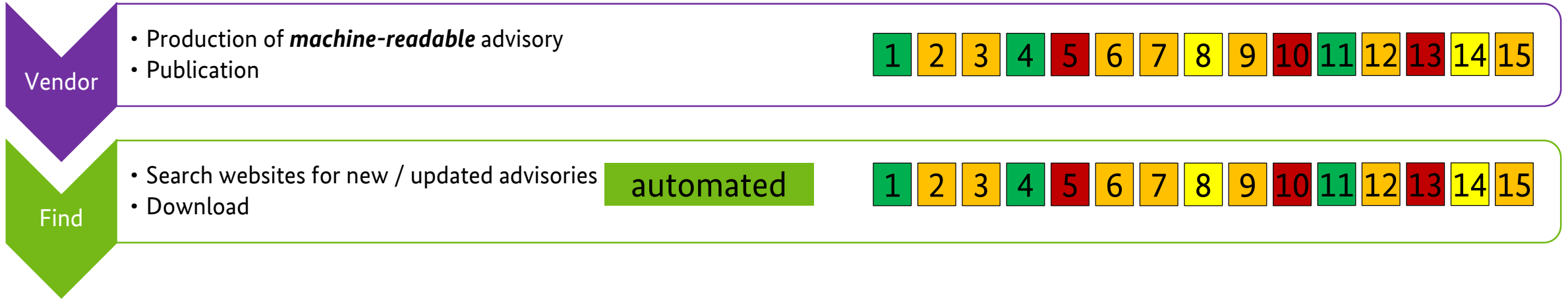
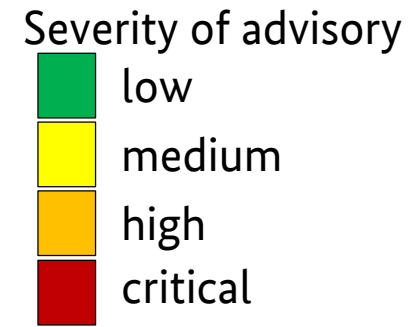


# Process with CSAF

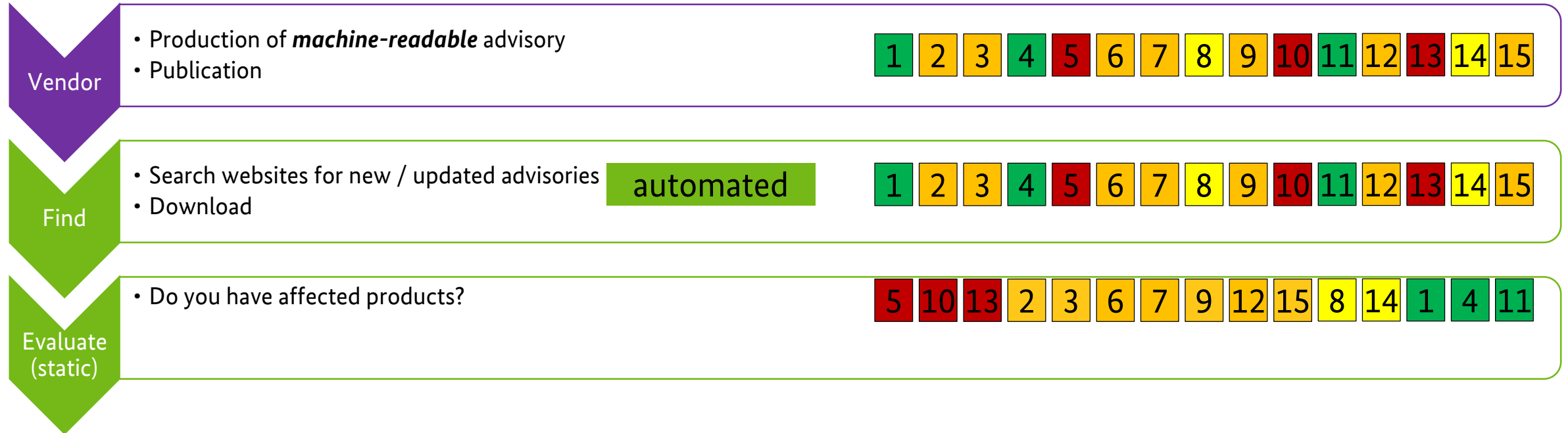
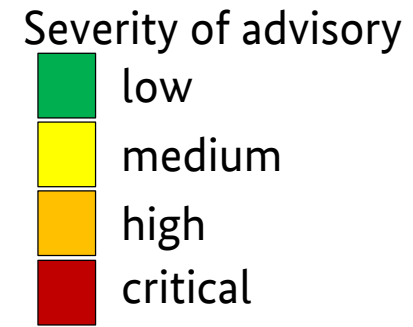
Severity of advisory



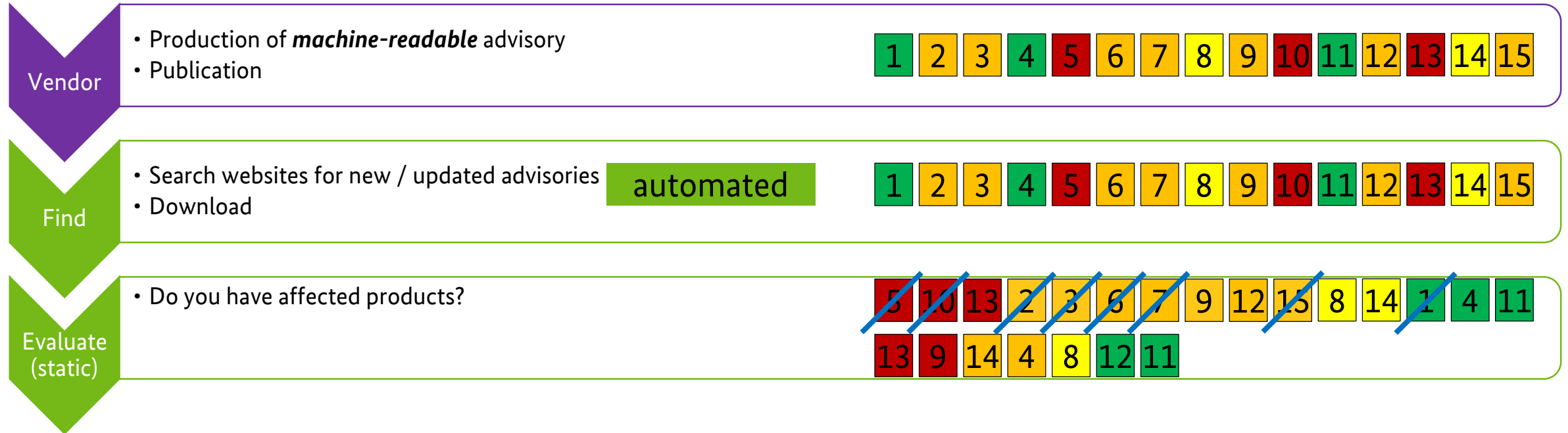
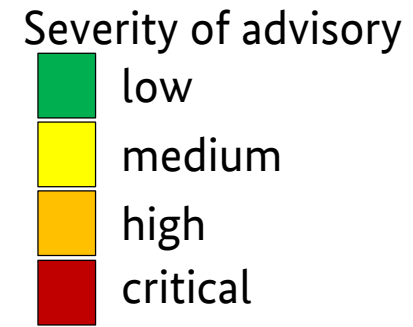
# Process with CSAF



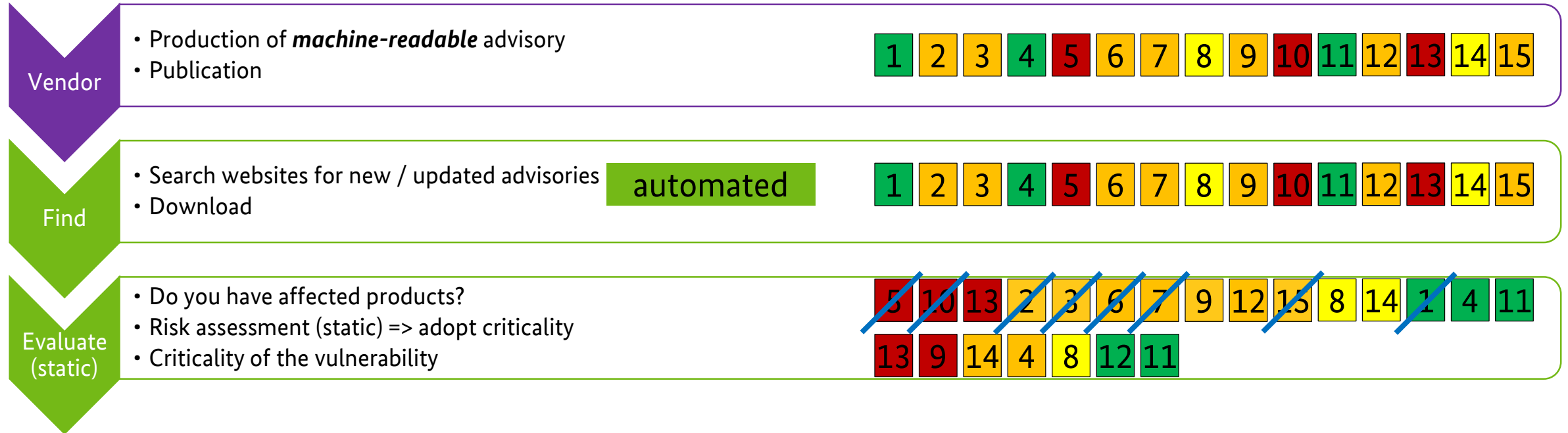
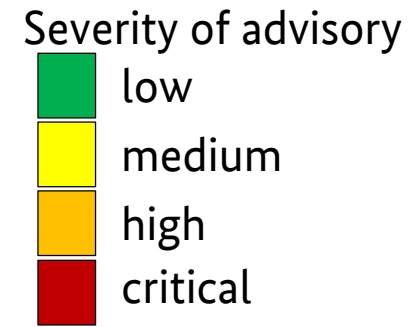
# Process with CSAF



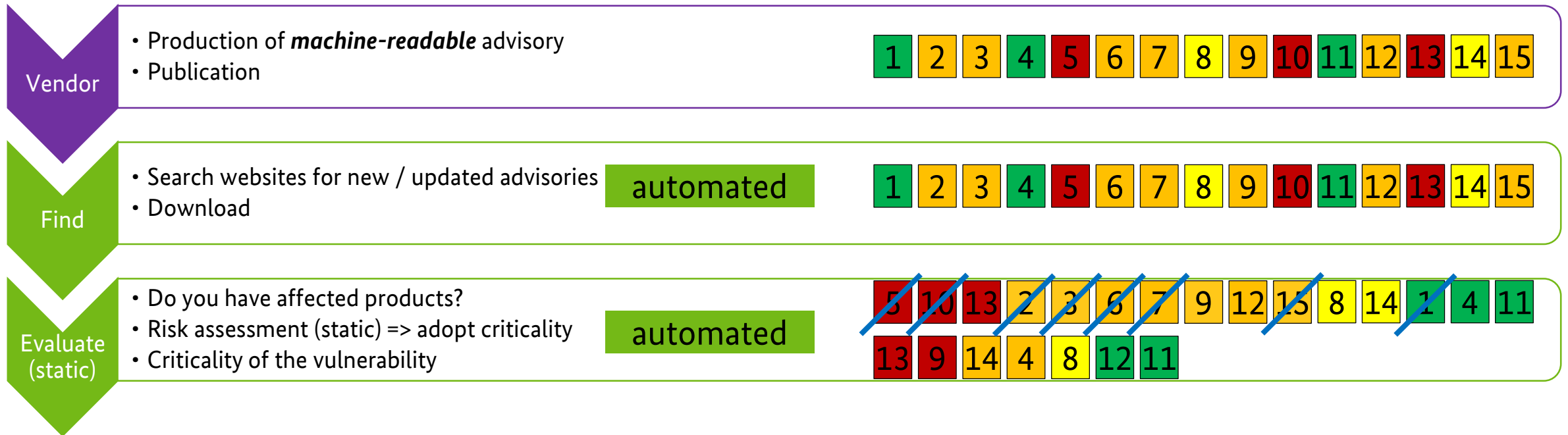
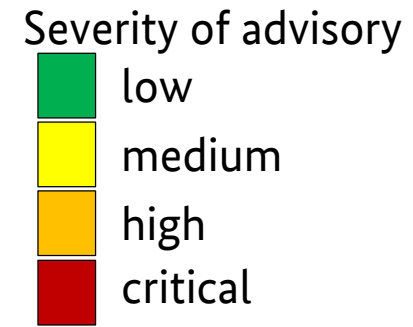
# Process with CSAF



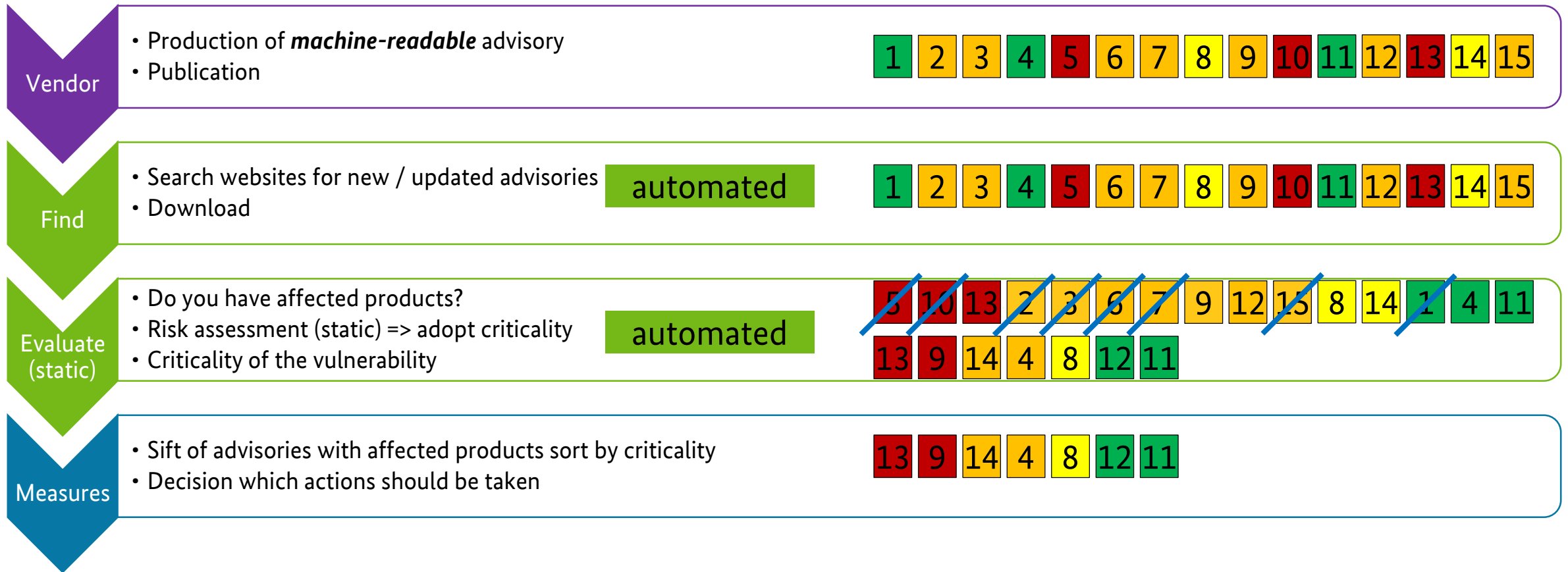
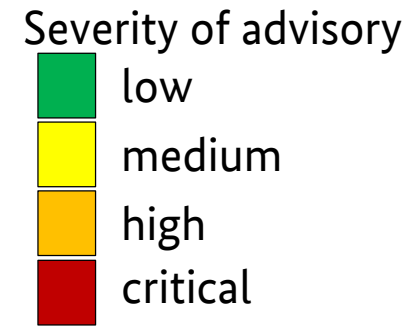
# Process with CSAF



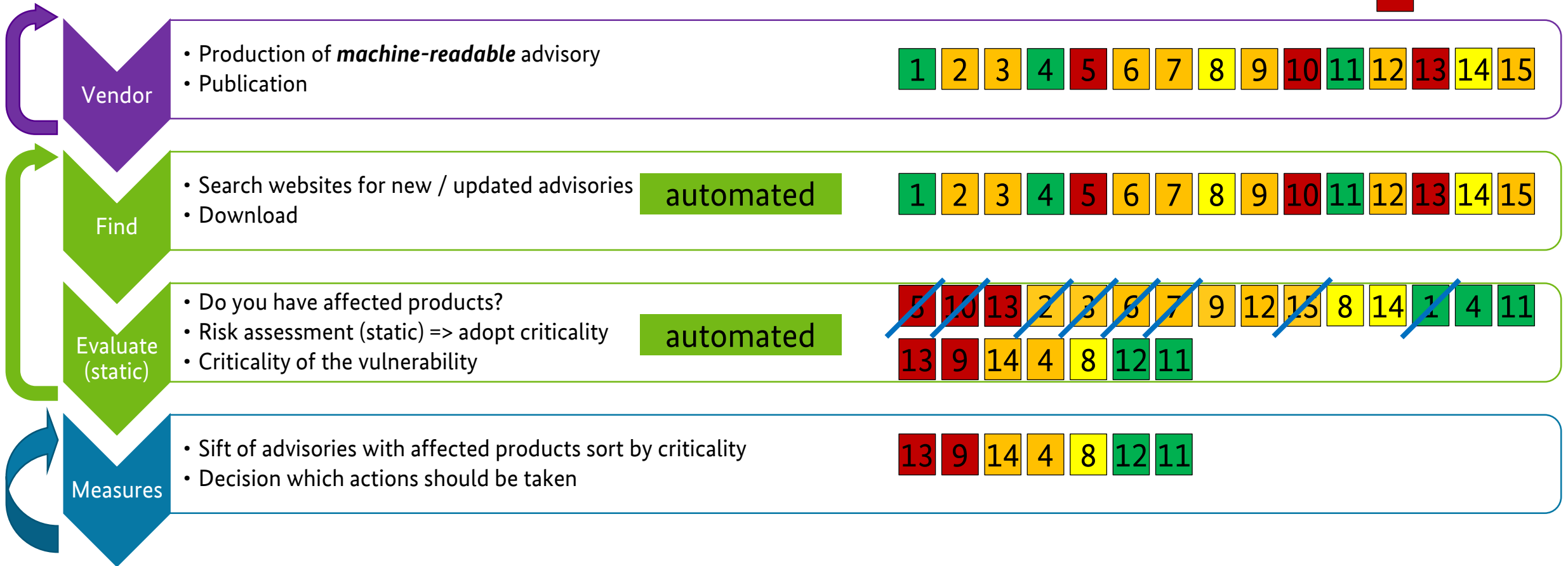
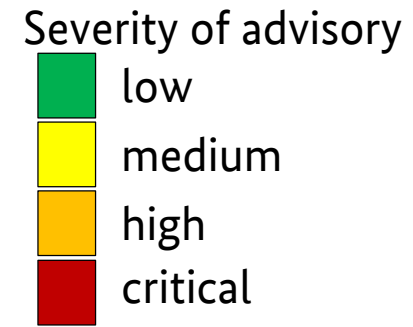
# Process with CSAF



# Process with CSAF



# Process with CSAF





# 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

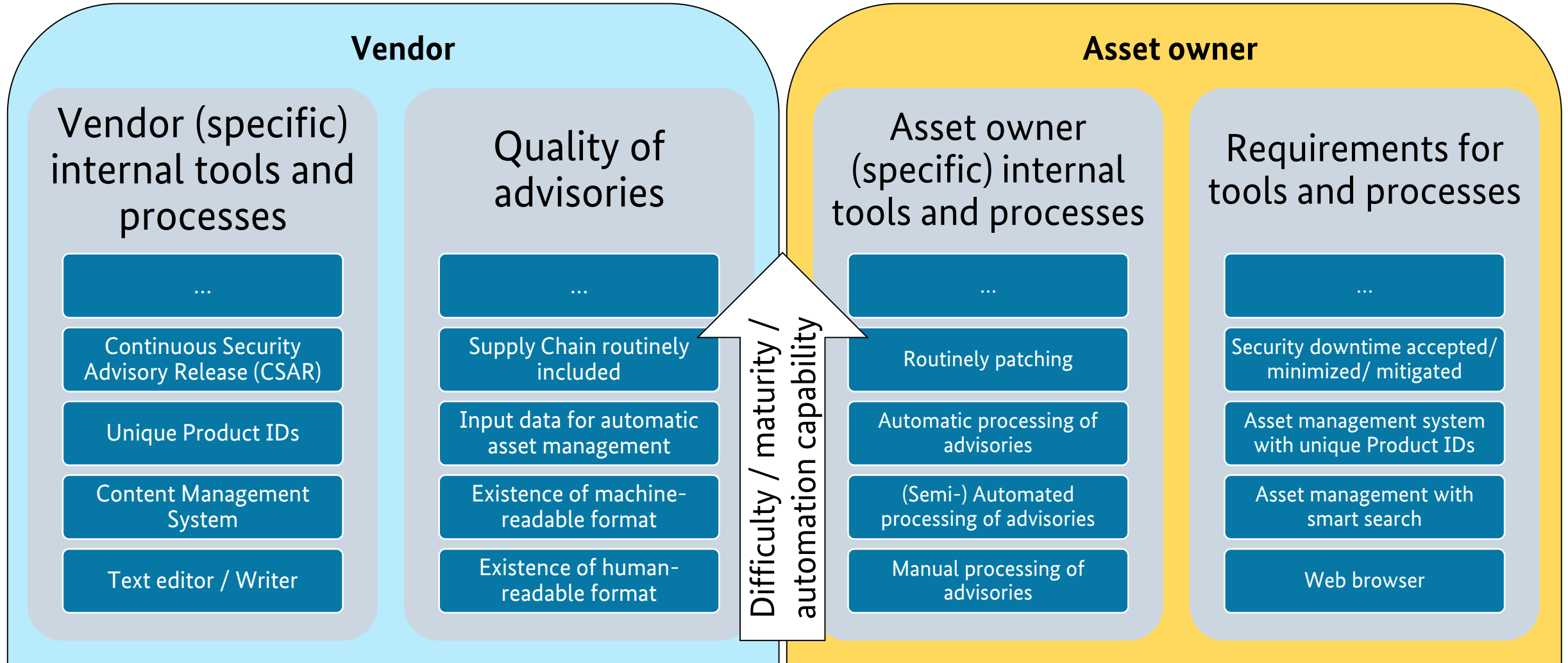


# Requirements for asset owners

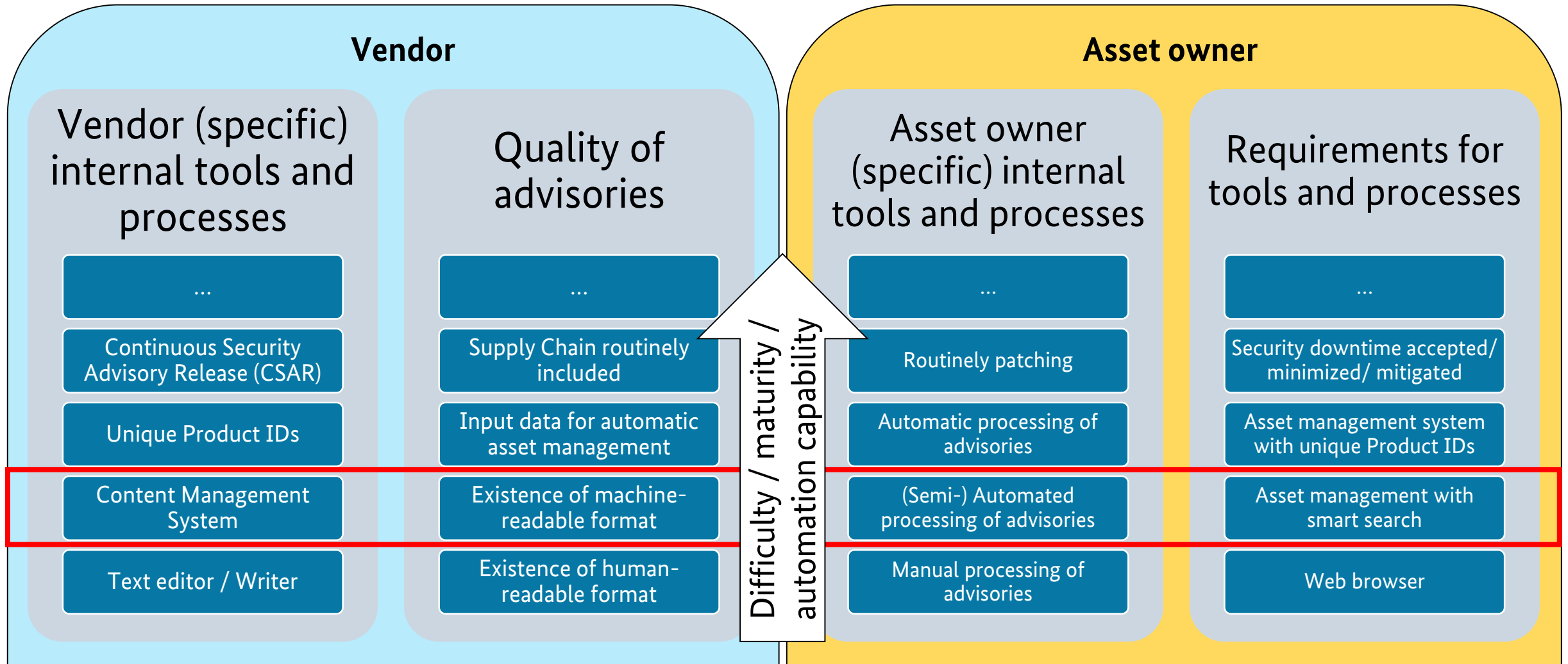
- Machine-readable asset inventory
- Request Advisories in CSAF from vendors
- Connection between both of them to leverage the full potential



# Two sides of the same coin – different maturity stages



# Next step: reach stage 2 across parties



# 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?

- Arista
- Cisco
- Dell
- Red Hat
- Oracle
- Siemens
- BSI
- ...



See full list at: [https://www.oasis-open.org/committees/membership.php?wg\\_abbrev=csaf](https://www.oasis-open.org/committees/membership.php?wg_abbrev=csaf)

# We need your support to make it work!

# Example CSAF Document

```
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    "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  "vulnerabilities": [
2468    {
2469      "title": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability",
2470      "ids": [
2475      "notes": [
2487      "cve": "CVE-2018-0171",
2488      "product_status": {
2489        "known_affected": [
2750      },
2751      "scores": [
3023      "remediations": [
3028      ],
3029      "references": [
3035      ]
3036    ]
3037  }
```

# Example CSAF Document

Document level  
metadata

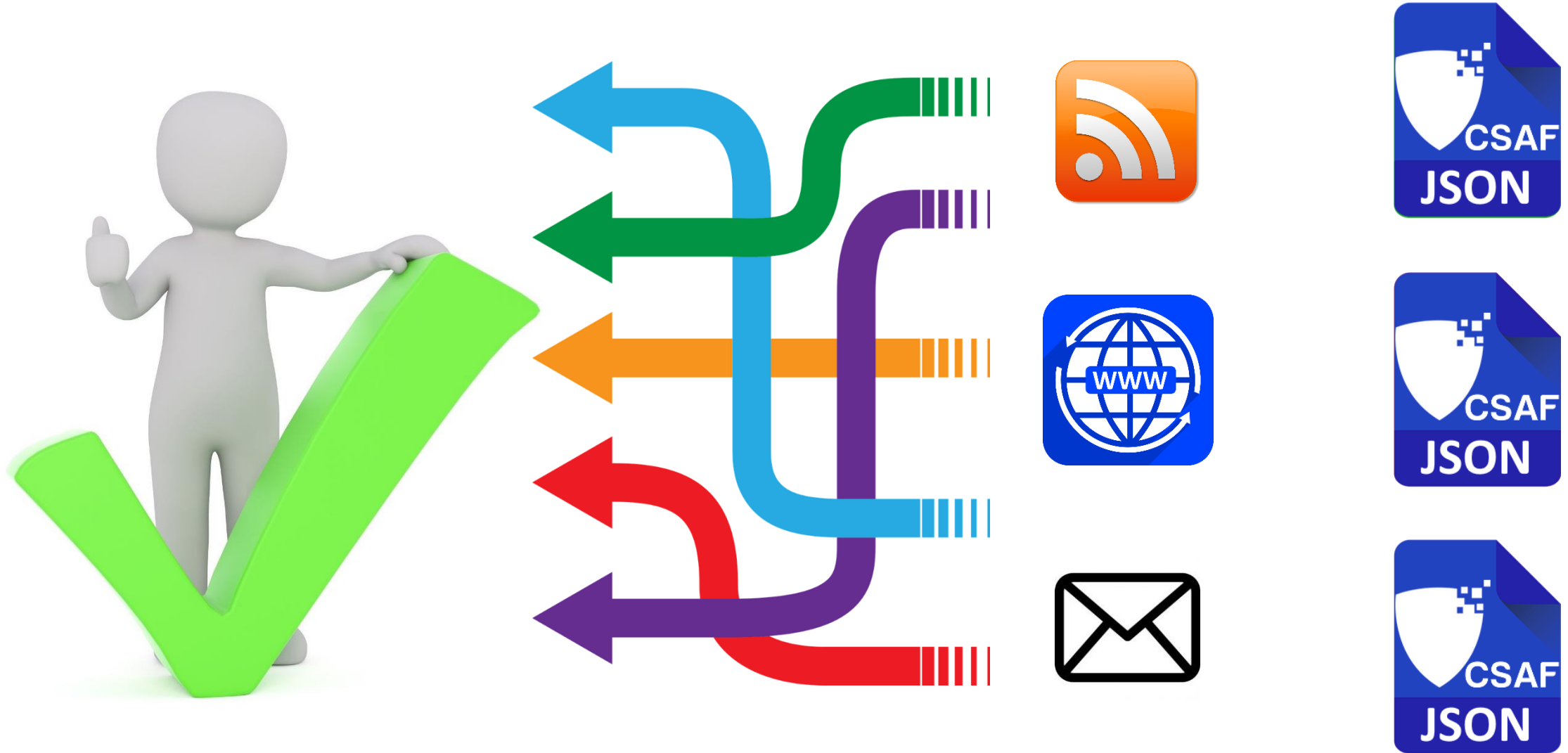
Product tree

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     "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  "vulnerabilities": [
2468    {
2469      "title": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability",
2470      "ids": [
2475      "notes": [
2487      "cve": "CVE-2018-0171",
2488      "product_status": {
2489        "known_affected": [
2750      ],
2751      "scores": [
3023      "remediations": [
3028      ],
3029      "references": [
3035      ]
3036    ]
3037  }
```



# One problem solved: unified format specified



# Where to find CSAF documents?

- ✓ Valid CSAF documents

- ✓ File name restrictions

- ✓ TLS enforced

- ✓ TLP:WHITE freely accessible

CSAF publisher

- ✓ Well-defined URL / security.txt / DNS => provider-metadata.json

- ✓ List of advisories and latest changes and Fixed folder structure

- ✓ or ROLIE feeds

- ✓ Restriction on  $\geq$ TLP:AMBER

- ✓ All requirements from CSAF publisher

CSAF provider

- ✓ Sign own advisories

- ✓ Hash advisories

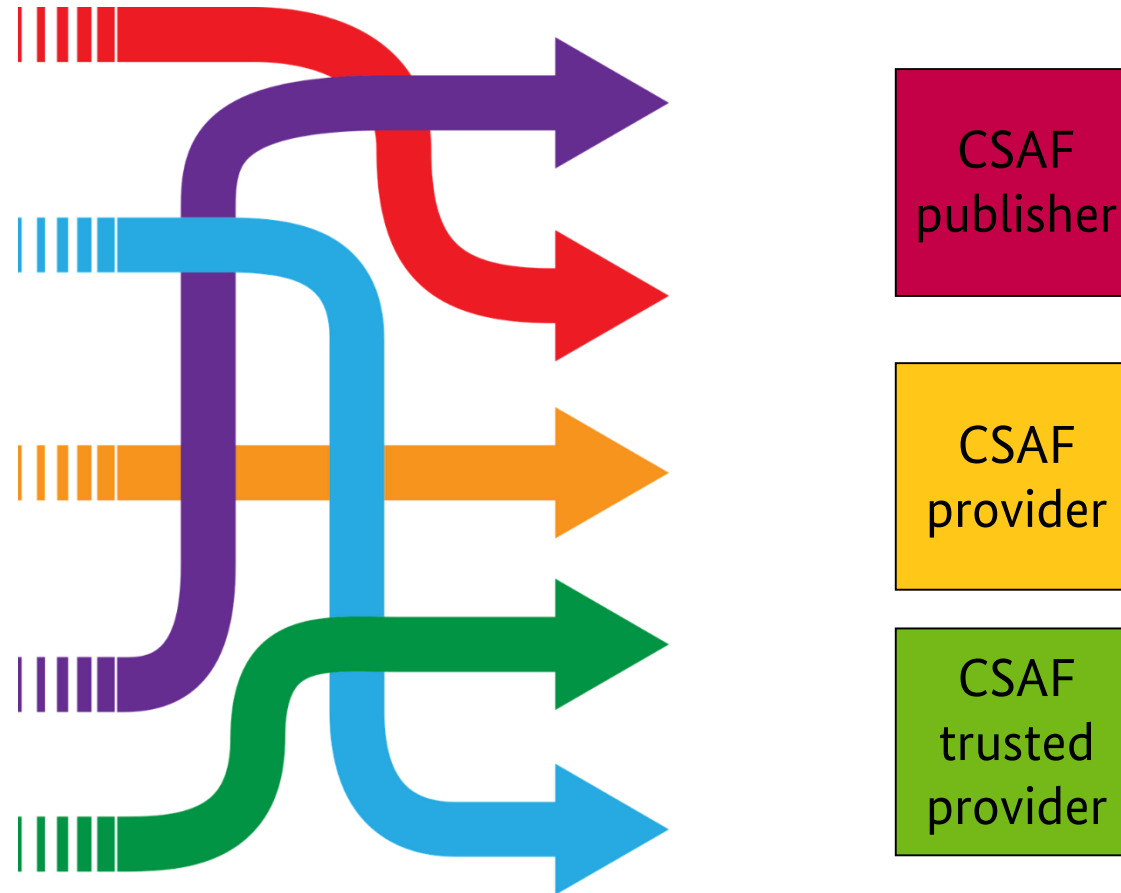
- ✓ Published OpenPGP keys for integrity checks

- ✓ All requirements from CSAF provider

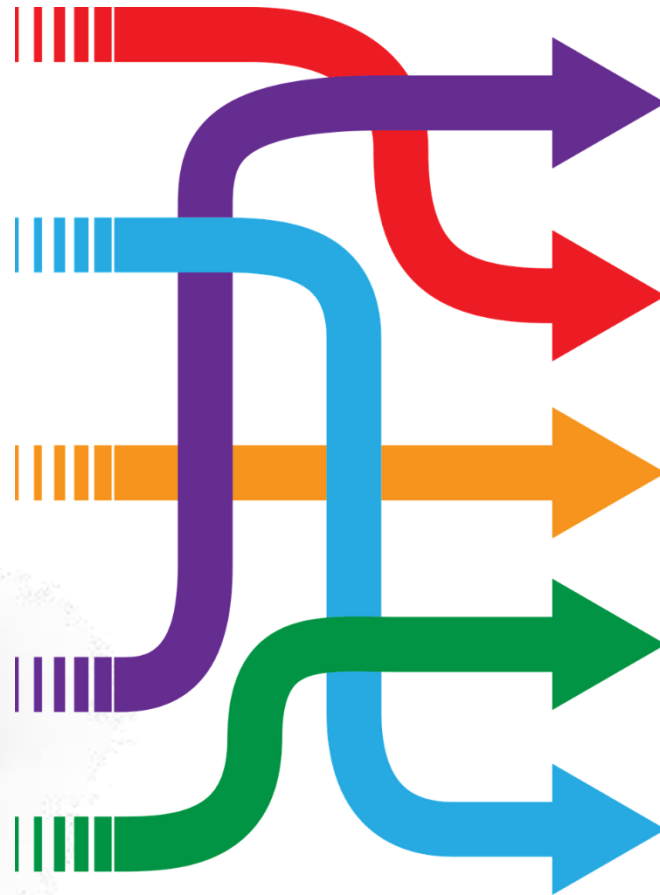
CSAF trusted  
provider

[https://github.com/oasis-tcs/csaf/blob/master/csaf\\_2.0/prose/csaf-v2-editor-draft.md#7-distributing-csaf-documents](https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/prose/csaf-v2-editor-draft.md#7-distributing-csaf-documents)

# Everything perfect?



# 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!

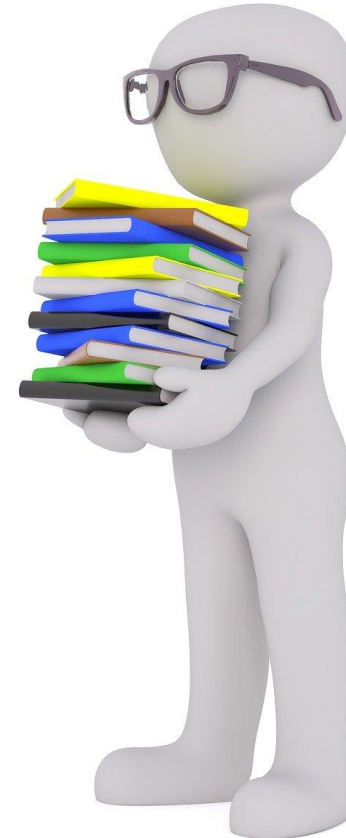


CSAF aggregator

# 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)

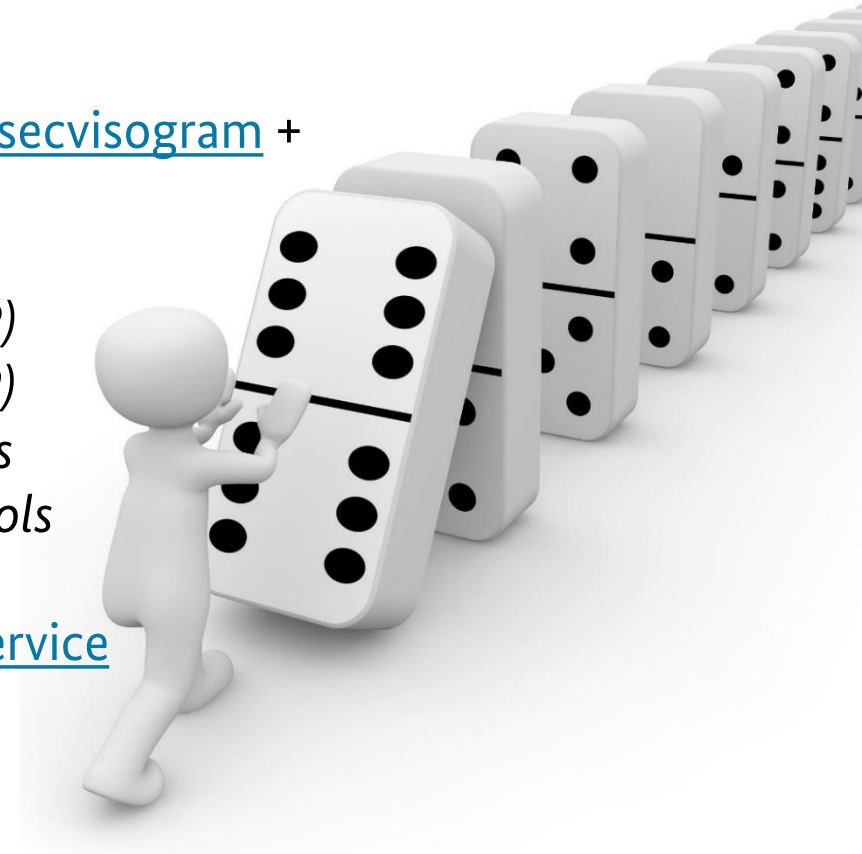


# Related topics

- Asset management: needed for matching on asset owner side
- SBOM: identify easier which components to find advisories for
- VEX: tell customers that the product is not affected
- Security.txt (RFC 9116): tell researchers how to contact you
- CACAO: playbooks for automated actions

# 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](https://github.com/csaf-poc/csaf_distribution)
- 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 downloader: [https://github.com/csaf-poc/csaf\\_distribution](https://github.com/csaf-poc/csaf_distribution)
- CSAF full validator: <https://github.com/secvisogram/csaf-validator-service>





# Secvisogram

Form Editor | JSON Editor | Preview | CSAF Document

v1.14.0 License: MIT Secvisogram

### ▼ Common Security Advisory Framework

#### ▼ Document level meta-data

Add 'Document acknowledgments'

Add 'Aggregate severity'

**Document category**

Must NOT have fewer than 1 characters  
Must match pattern `"^[^s\-\.\.](.*[^s\-\.\.])?$"`

**CSAF version**

2.0

Add 'Rules for sharing document'

Add 'Document language'

Add 'Document notes'

New (minimal fields)

New (all fields)

Open

Save

Expand all

Collapse all

#### Validation Status

**16**

[Hide errors](#)

**Validation Errors:**

- `/document/category:` must NOT have fewer than 1 characters
- `/document/category:` must match pattern `"^[^s\-\.\.](.*[^s\-\.\.])?$"`
- `/document/publisher/category:` must be equal to one of the allowed values
- `/document/publisher/name:` must NOT have fewer than 1 characters

# Conclusions

# Where to find more information?

<https://csaf.io>

OASIS TC: CSAF website: [https://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=csaf](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](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](https://github.com/oasis-tcs/csaf/tree/master/csaf_2.0/examples)

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

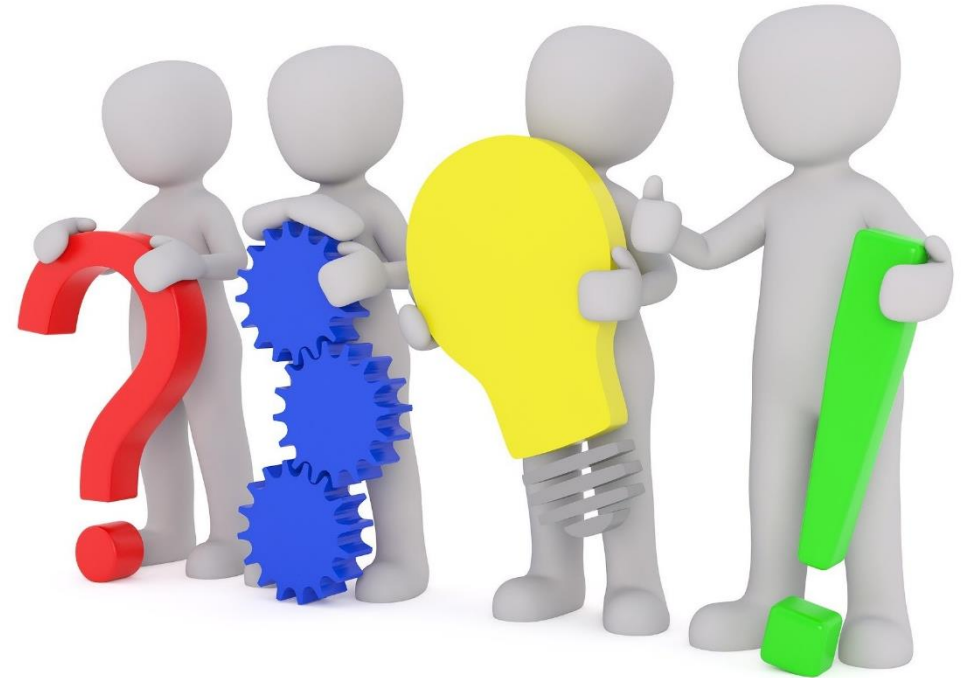
Running Demo: <https://secvisogram.github.io>

# Summary & Action Items

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



# 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
- Clean up your asset inventory
- Provide CSAF documents to your customers to ease their pain
- **Spread the word! #oCSAF #advisory**



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

[csaf@bsi.bund.de](mailto: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](http://www.bsi.bund.de/dok/en_csaf)

