



Setting the standard for open
collaboration

Using CSAF to Respond to Supply Chain Vulnerabilities at Large Scale



Welcome

Attendees may submit questions using the Zoom question panel.
Q&A with panelists will take place at the end of the program.

This presentation will be recorded and available to members after the event.

Speakers



Diane Morris, Cisco



Justin Murphy, CISA



Thomas Schmidt, BSI

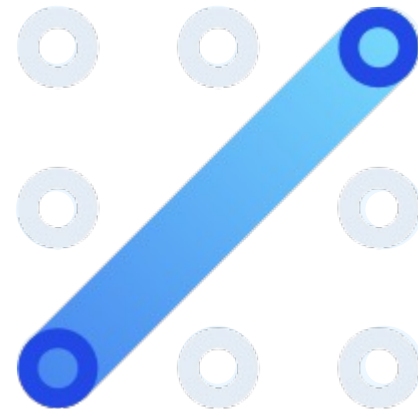


Omar Santos, Cisco

From *Transforming the Vulnerability Management Landscape* blog post, published Nov 14, 2022

“By publishing security advisories using CSAF, vendors will dramatically reduce the time required for enterprises to understand organizational impact and drive timely remediation.”

— *Eric Goldstein, Executive Assistant
Director of Cybersecurity, CISA*





<https://github.com/lunasec-io/lunasec/blob/998c69decc0894a214efa035854b48b1af18eb6e/docs/static/img/log4shell-logo.png>

develop • log4j-affected-db / software_lists / Go to file

chasevotel Normalize YAMLS files and update the software lists

1719119 Mar 1, 2022 History

...

README.md Update rel. paths Feb 17, 2022

software_list_A.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_B.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_C.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_D.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_E.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_F.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_G.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_H.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_I.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_J.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_K.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_L.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_M.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_N.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_Non-Alphabet.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_O.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_P.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_Q.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_R.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_S.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_T.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_U.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_V.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_W.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_X.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_Y.md Normalize YAMLS files and update the software lists Mar 1, 2022

software_list_Z.md Normalize YAMLS files and update the software lists Mar 1, 2022

README.md

CISA Log4j (CVE-2021-44228) Affected Vendor & Software Lists

Contributing Guidelines

We welcome contributions! Please see [CONTRIBUTING.md](#) for details.

Creating a pull request

Instructions for creating a pull request using the GitHub Web UI can be found in [PULL-EXAMPLE.md](#).

Software Lists

To view the full lists of vendors & software click below:

09ABCDEFGHIJKLMNPQRSTUVWXYZ

main • log4shell / software / Go to file

email-cop Annot cop update for SAP (P000)

latest Feb 14, 2022 History

...

vendor-statements Add PTC/Creo Parametric and PTC/Creo View (P037) Jan 14, 2022

Jeep [Shred] setting up directory structure Dec 12, 2021

HOWTOpr-review.md Document PR assignment Dec 21, 2021

README.md Update readme with information about CVE-2021-44832 Dec 29, 2021

software_list_A.md Split software list in 27 pieces Dec 27, 2021

software_list_B.md software sort all lists Dec 31, 2021

software_list_C.md removed duplicate Schneider Electric (P001) Feb 7, 2022

software_list_D.md Clarified several Bosch products (P009) Jan 13, 2022

software_list_E.md Annot cop patch 43 thegreenbox - Update software_list_C.md - Add Csc... Jan 11, 2022

software_list_F.md Update software_list_C.md Jan 7, 2022

software_list_G.md Software list E - sorting (P020) Jan 3, 2022

software_list_H.md Software list F - sorting (P021) Jan 3, 2022

software_list_I.md Software list G - sorting (P022) Jan 3, 2022

software_list_J.md Fixed Status to follow naming convention (P048) Jan 3, 2022

software_list_K.md Software list I - sorting (P024) Jan 3, 2022

software_list_L.md Software list J - sorting (P025) Jan 3, 2022

software_list_M.md Software list K - sorting (P026) Jan 3, 2022

software_list_N.md Software list L - sorting (P027) Jan 3, 2022

software_list_O.md Software list M - sorting (P028) Jan 3, 2022

software_list_P.md Update NVD&A Jan 13, 2022

software_list_Q.md Add Oerlem products (P030) Jan 7, 2022

software_list_R.md Add info for Procenter products (P063) Jan 14, 2022

software_list_S.md Software list Q - sorting (P032) Jan 3, 2022

software_list_T.md Updated Rockwell products (P076) Jan 27, 2022

software_list_U.md Annot cop update for SAP (P006) Feb 14, 2022

software_list_V.md Update of Aruba products (P078) Jan 25, 2022

software_list_W.md Software list U - sorting (P036) Jan 3, 2022

software_list_X.md VMware vCenter Files (P005) Feb 10, 2022

software_list_Y.md Software list W - sorting (P038) Jan 3, 2022

software_list_Z.md Software list X - sorting (P039) Jan 3, 2022

software_list_A.md Software list Y - sorting (P040) Jan 3, 2022

software_list_B.md software sort all lists Dec 31, 2021

README.md

Overview of software (un)affected by Log4j

This directory contains an overview of software (un)affected by the Log4shell vulnerabilities. NCSC-NL and partners are attempting to maintain a list of all known vulnerable and not vulnerable software. Listed software is paired with specific information regarding which version contains the security fixes and which software still requires fixes. Please note that this vulnerability may also occur in custom software developed within your organisation. These occurrences are not registered in this overview.

NCSC-NL has concluded that the new vulnerability (CVE-2021-44832) has a low chance of being exploited and will therefore exclude this vulnerability from this GitHub.

NCSC Advisories

NCSC-NL has published a HIGH/HIGH advisory for the Log4j vulnerability. Normally we would update the HIGH/HIGH advisory for vulnerable software packages, however due to the extensive amounts of expected updates we have created a list of known vulnerable software in the software directory.

Daily CSV/JSON releases

Daily releases of this software list are listed, including CSV and JSON files, in the [releases](#) overview. Please check the [software list parser](#) tool to generate a CSV or JSON on your own.

Disclaimer: We aim to provide as the information as accurately as possible with the resources available to us. However, we do not have the capacity to monitor all software for updates/files. You are advised to review the links provided for available updates. If you find updates or mistakes, please contribute by creating a Pull Request. [Learn how](#).

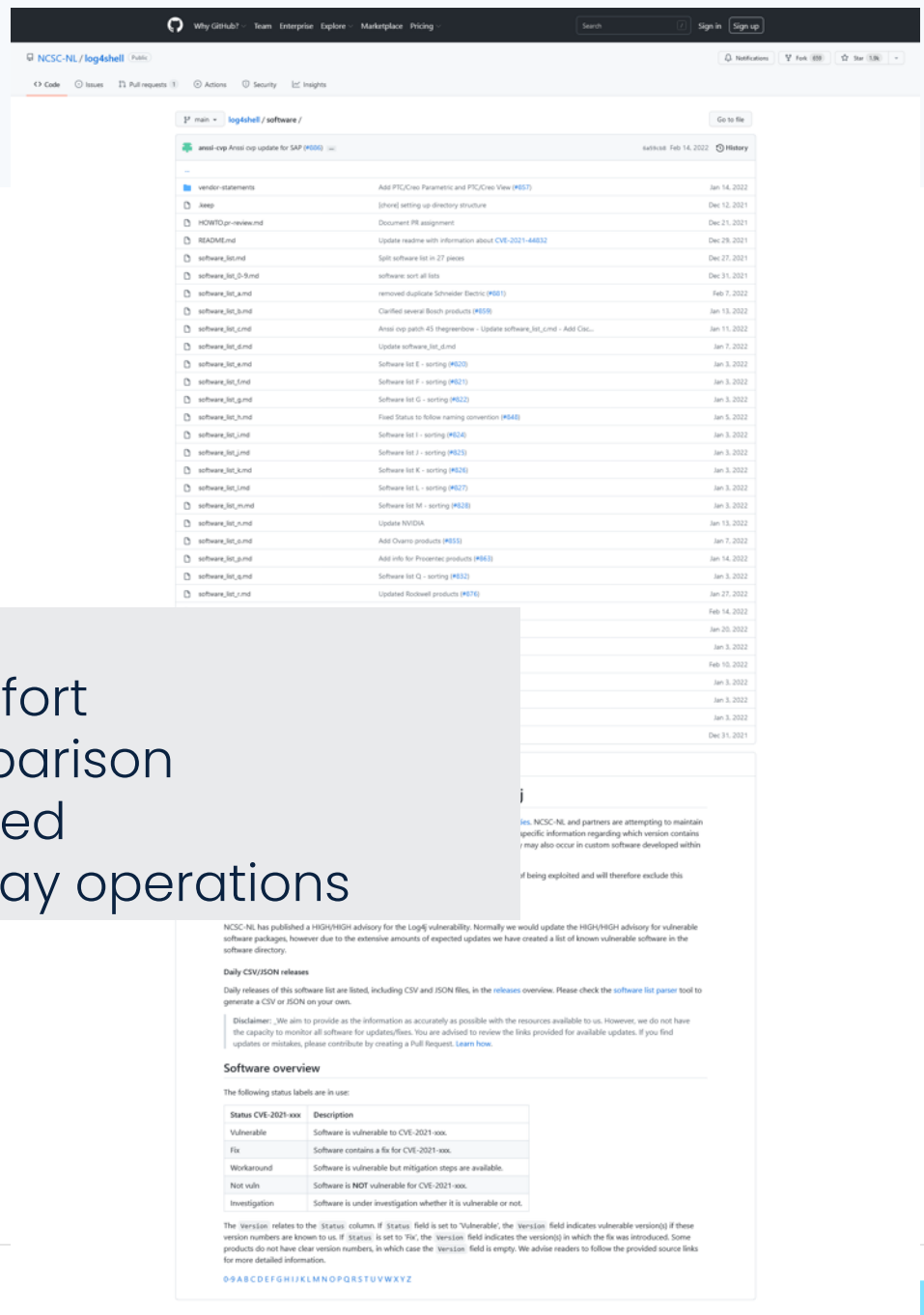
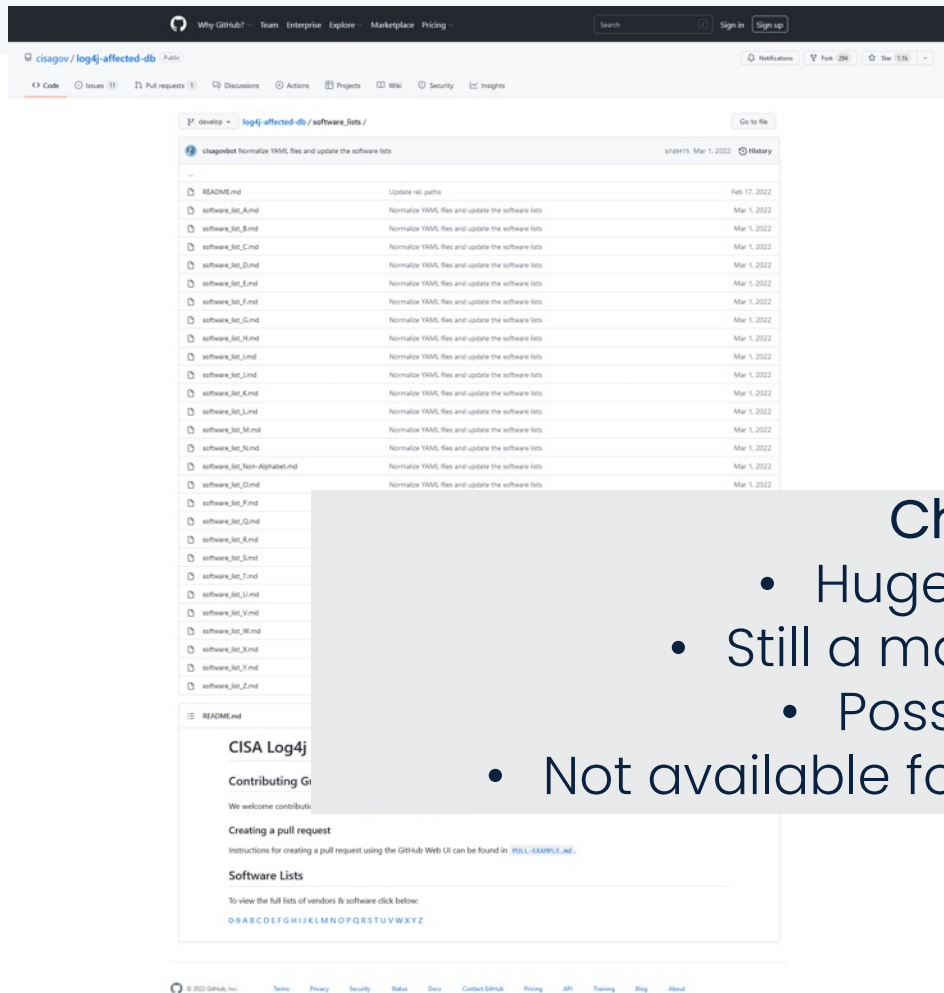
Software overview

The following status labels are in use:

Status CVE-2021-xxx	Description
Vulnerable	Software is vulnerable to CVE-2021-xxx.
Fix	Software contains a fix for CVE-2021-xxx.
Workaround	Software is vulnerable but mitigation steps are available.
Not vuln	Software is NOT vulnerable for CVE-2021-xxx.
Investigation	Software is under investigation whether it is vulnerable or not.

The `version` relates to the `status` column. If `status` field is set to 'Vulnerable', the `version` field indicates vulnerable version(s) (if these version numbers are known to us. If `status` is set to 'Fix', the `version` field indicates the version(s) in which the fix was introduced. Some products do not have clear version numbers, in which case the `version` field is empty. We advise readers to follow the provided source links for more detailed information.

09ABCDEFGHIJKLMNPQRSTUVWXYZ



- ## Challenges:
- Huge manual effort
 - Still a manual comparison
 - Possibly outdated
 - Not available for day-to-day operations

Manual process

Manual Processes

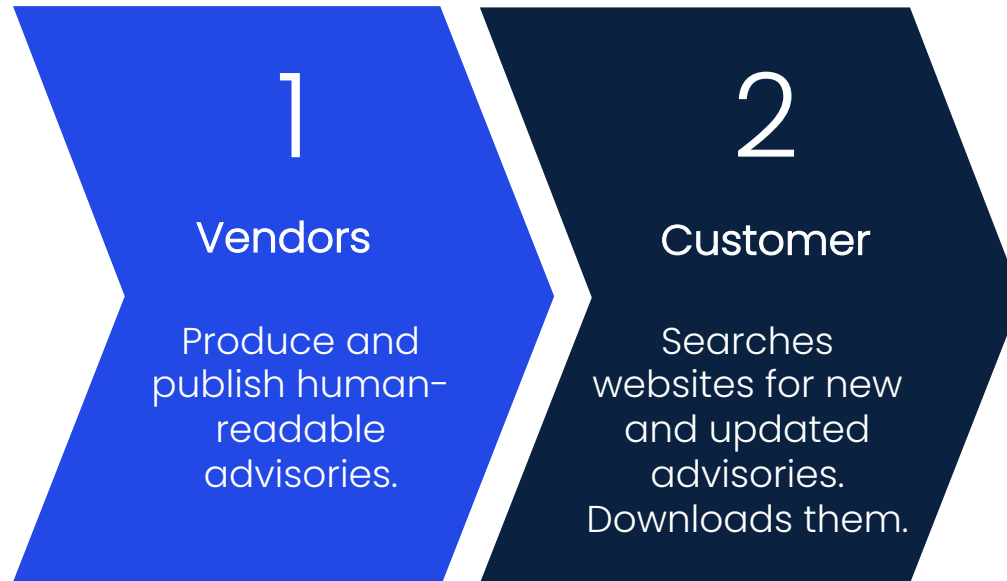


Severity

- critical
- high
- medium
- low

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

Manual Processes



Severity	
	critical
	high
	medium
	low

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

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

Manual Processes



Severity	
	critical
	high
	medium
	low

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

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

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

Manual Processes



Severity	
	critical
	high
	medium
	low

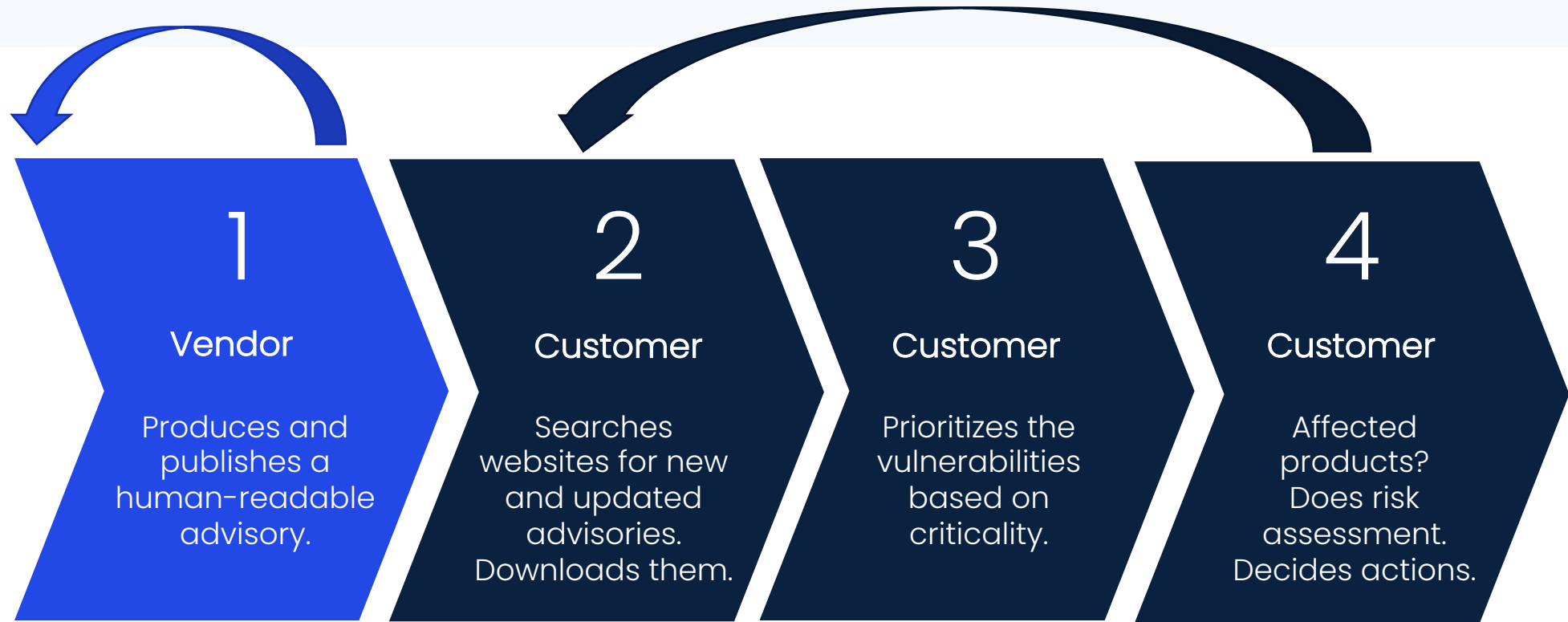
1	6	11
2	7	12
3	8	13
4	9	14
5	10	15

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

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

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

Manual Processes



Severity	
■	critical
■	high
■	medium
■	low

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

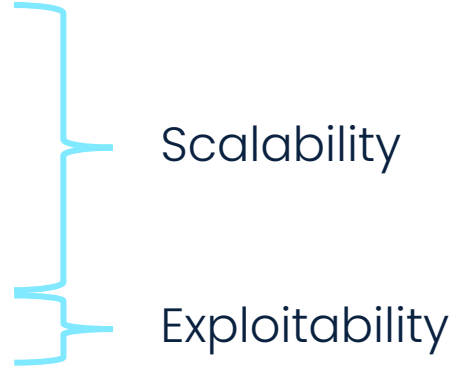
1	6	11
2	7	12
3	8	13
4	9	14
5	10	15

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

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

Problems to Solve

- Many vendors – all with different formats and distribution methods
- Number of security advisories is rising
- SBOM adds to overload
- Not every vulnerability can be exploited



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
- Successor of CSAF CVRF 1.2



Example: CSAF Document

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": {
7        "category": "vendor",
8        "contact_details": "Emergency Support:\n+1 877 228 7302 (toll-free within North America)\n+1 408
9        "issuing_authority": "Cisco product security incident response is the responsibility of the Cisco
10       "name": "Cisco PSIRT",
11       "namespace": "https://www.cisco.com"
12     },
13     "tracking": {
14       "id": "cisco-sa-20180328-smi2",
15       "status": "final",
16       "version": "3.0.0",
17       "revision_history": [
18         {
19           "number": "1.0.0",
20           "date": "2018-03-28T15:17:05Z",
21           "summary": "Initial public release."
```

Example: CSAF Document

Product Tree

```
137     "product_tree": {
138       "branches": [
139         {
140           "name": "Cisco",
141           "category": "vendor",
142           "branches": [
143             {
144               "name": "IOS",
145               "category": "product_name",
146               "branches": [
147                 {
148                   "name": "12.2SE",
149                   "category": "product_version",
150                   "branches": [
151                     {
152                       "name": "12.2(55)SE",
153                       "category": "service_pack",
154                       "product": {
155                         "product_id": "CVRFPID-103763",
156                         "name": "Cisco IOS 12.2SE 12.2(55)SE"
157                       }
158                     },
159                     {
```

Example: CSAF Document

Vulnerabilities

```
2483   "vulnerabilities": [  
2484     {  
2485       "title": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability",  
2486       "ids": [  
2487         {  
2488           "system_name": "Cisco Bug ID",  
2489           "text": "CSCvg76186"  
2490         }  
2491       ],  
2492       "notes": [  
2493         {  
2494           "title": "Summary",  
2495           "category": "summary",  
2496           "text": "A vulnerability in the Smart Install feature of Cisco IOS Software and Cisco IOS X  
2497         },  
2498         {  
2499           "title": "Cisco Bug IDs",  
2500           "category": "other",  
2501           "text": "CSCvg76186"  
2502         }  
2503       ],  
2504       "cve": "CVE-2018-0171",  
2505       "product_status": {  
2506         "known_affected": [  
2507           "CVRFPID-103559",  
2508           "CVRFPID-103763",
```

Process with CSAF



Severity	
	critical
	high
	medium
	low

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

Process with CSAF



Severity	
	critical
	high
	medium
	low

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

Process with CSAF

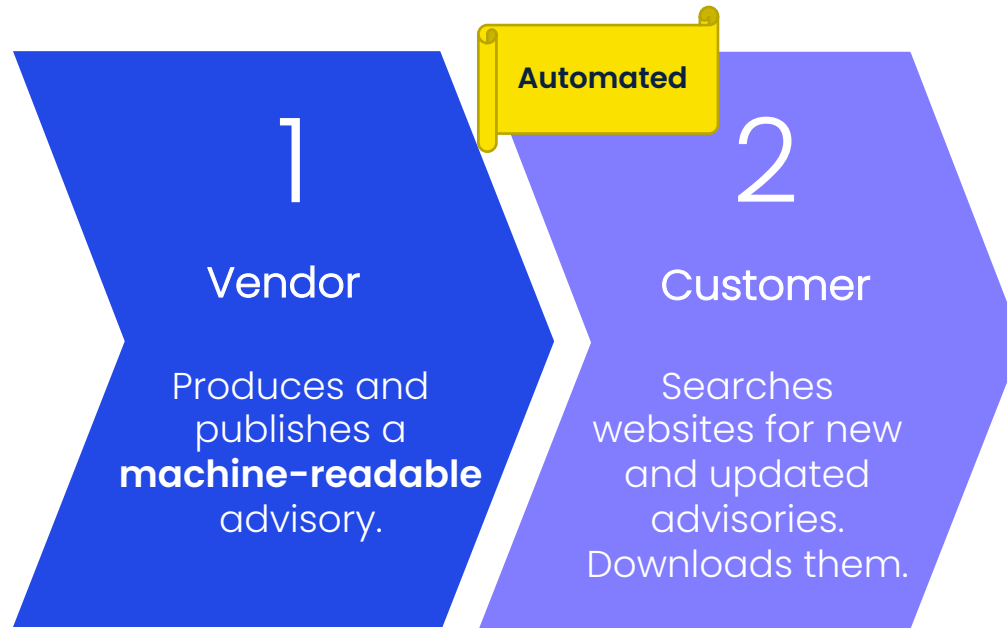


Severity	
	critical
	high
	medium
	low

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

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

Process with CSAF



Severity	
	critical
	high
	medium
	low

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

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

Process with CSAF



Severity	
	critical
	high
	medium
	low

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

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

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

Process with CSAF



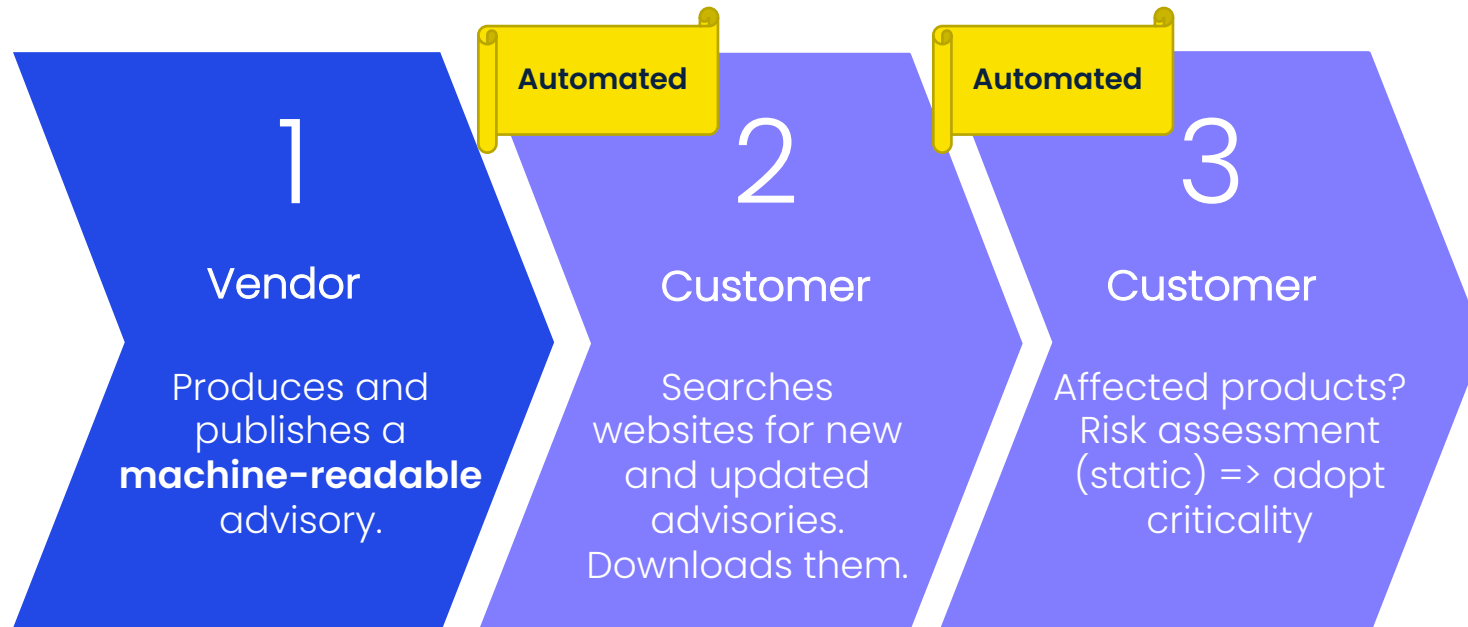
Severity	
	critical
	high
	medium
	low

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

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

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

Process with CSAF



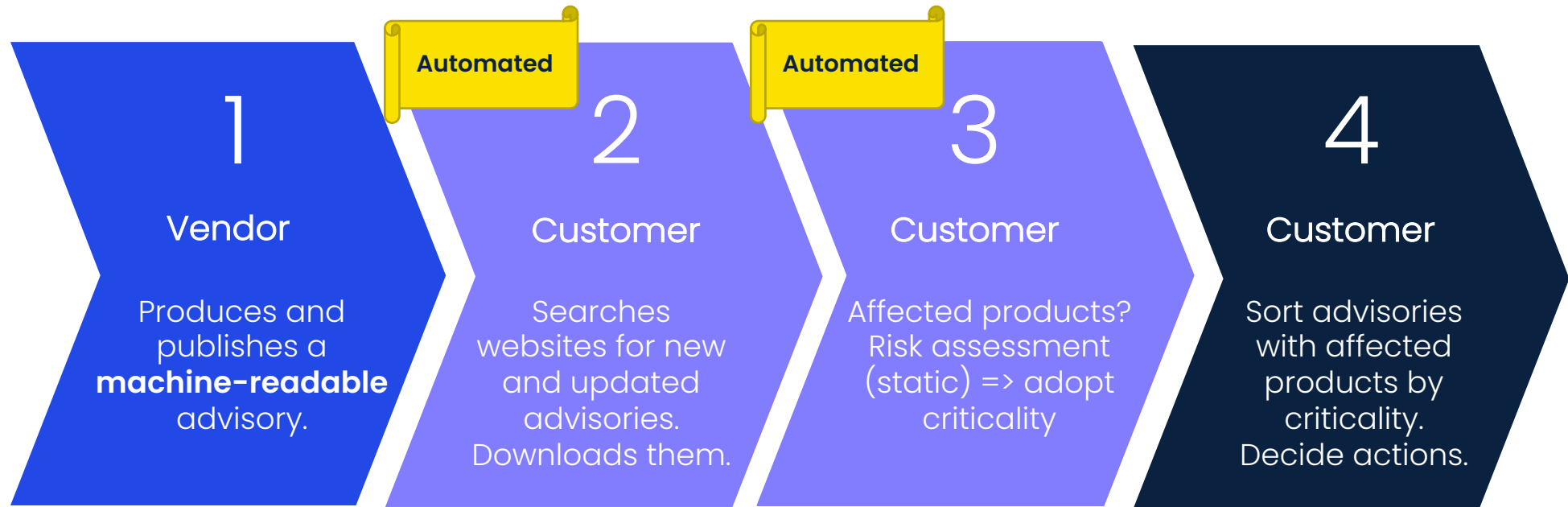
Severity	
	critical
	high
	medium
	low

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

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

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

Process with CSAF



Severity	
	critical
	high
	medium
	low

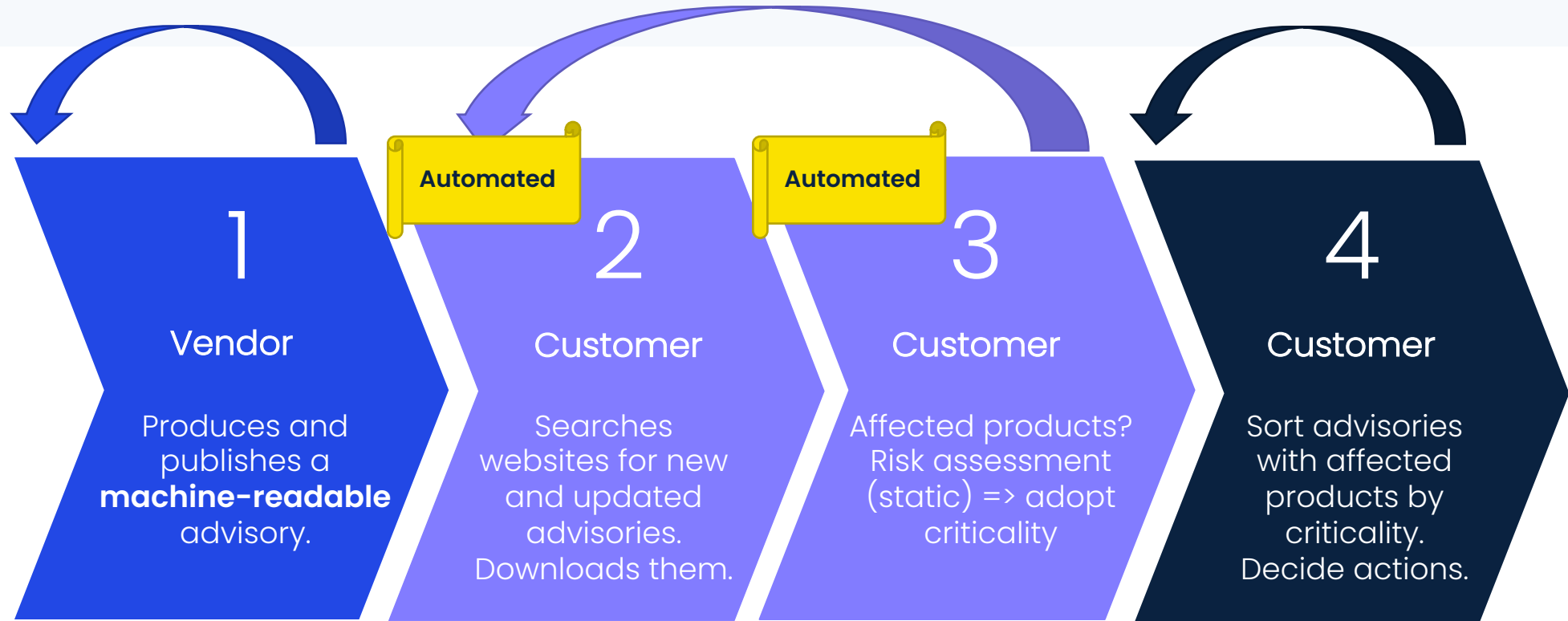
1	6	11
2	7	12
3	8	13
4	9	14
5	10	15

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

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

13	9
14	4
8	
12	11

Process with CSAF



Severity

■	critical
■	high
■	medium
■	low

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

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

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

13	9
14	4
8	
12	11



Benefits for Asset Owners

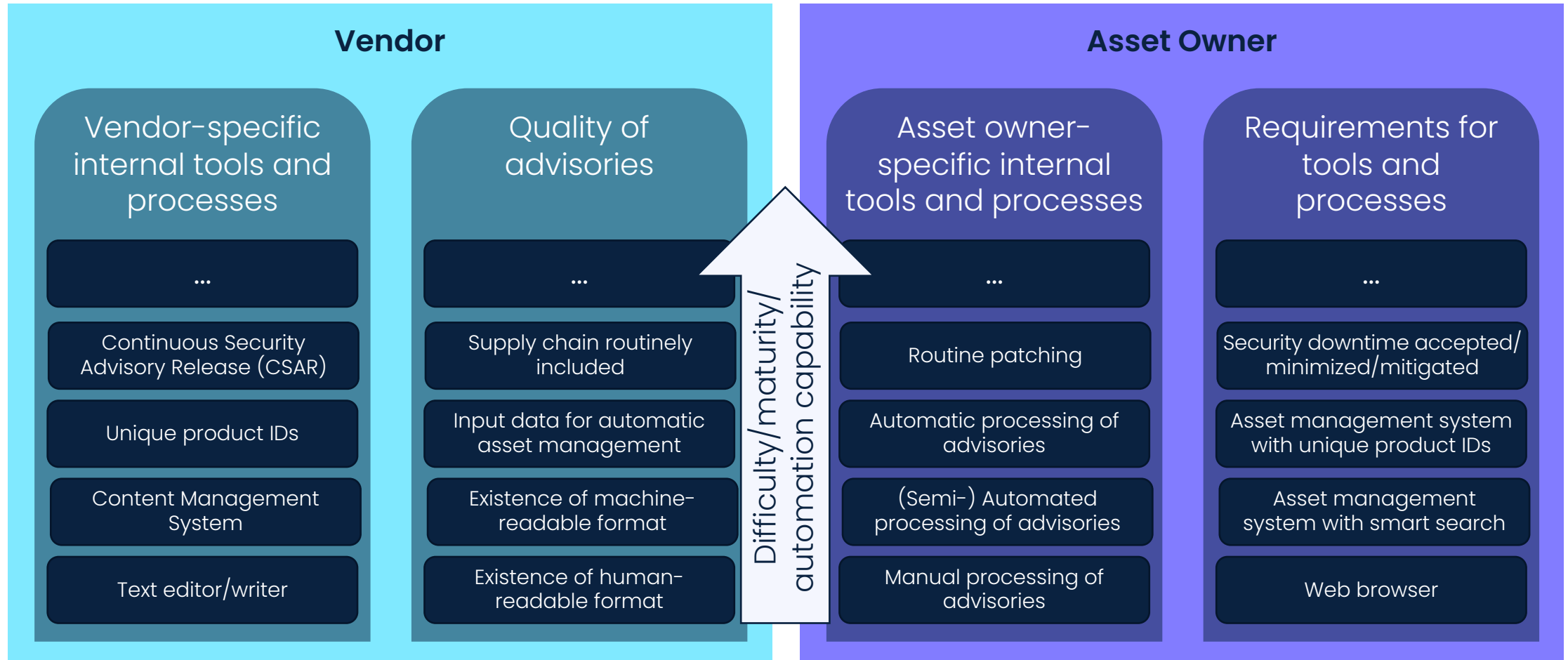
- Makes the impossible – stringent patch and update management, which currently is often sporadic or dependent on personal availability or interests – **possible**.
- **Reduces** human factor and individual workload
 - No more manual searching for advisories
 - Easier to determine affected devices
 - Delegable
 - See only relevant advisories
- **Scalable** across all participating vendors
- Enables basic risk assessment based on own environment

A person with short dark hair, wearing a dark blue sweater, is seated at a desk in a workshop or lab. They are focused on a task, using a yellow multimeter and several red and black wires. A computer monitor and a desk lamp are visible in the background. The scene is brightly lit, suggesting a window nearby.

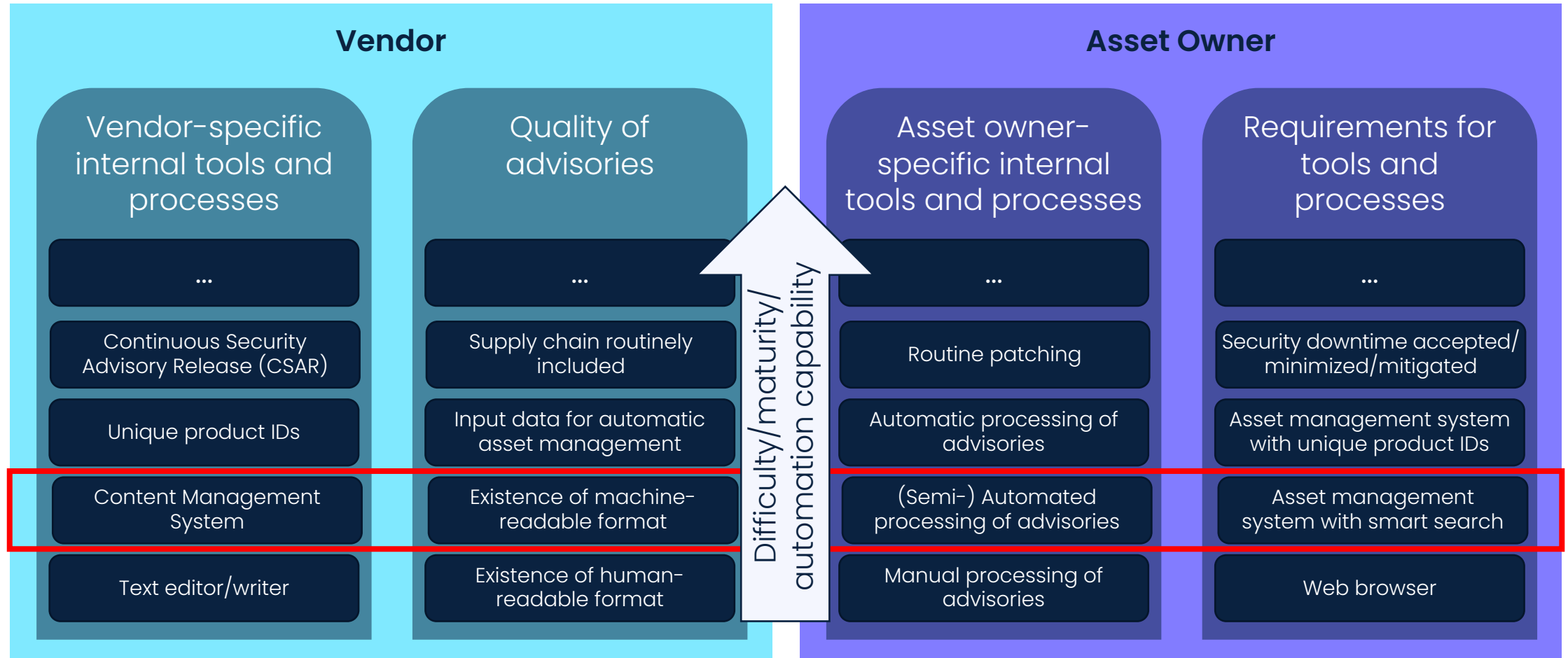
Requirements for Asset Owners

- Machine-readable asset inventory
- Request advisories in CSAF from vendors
- Connection between both to leverage full potential

Two Sides of the Same Coin – Different Maturity Stages

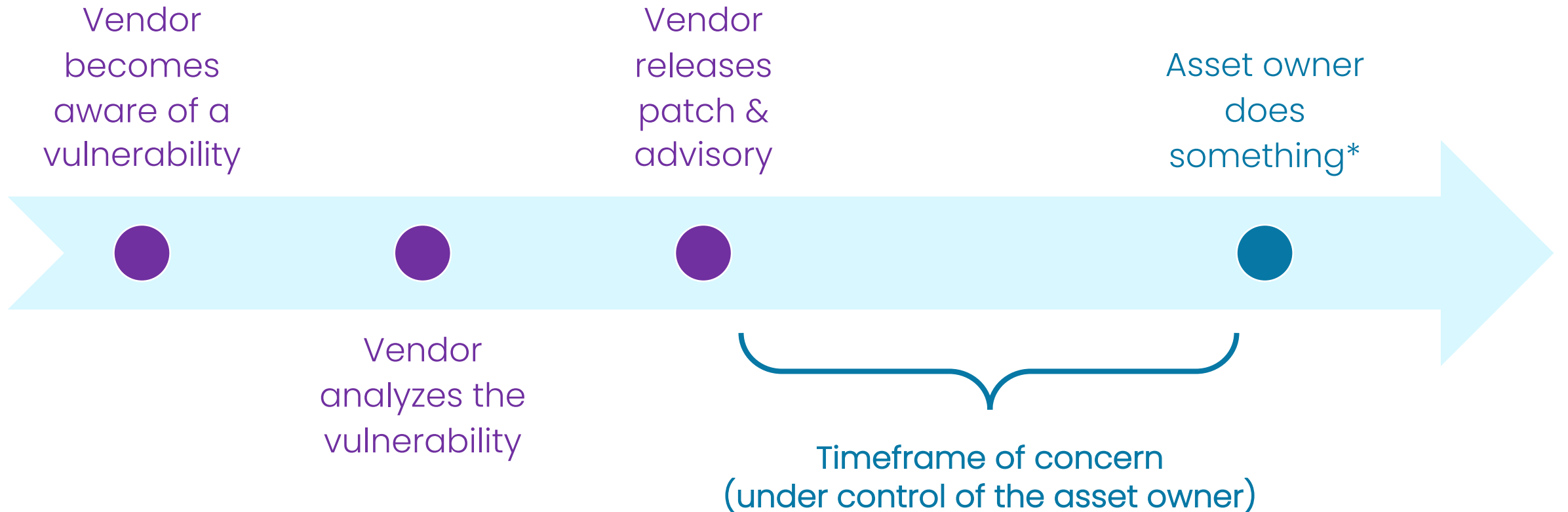


Next Step: Reach Stage 2 Across Parties



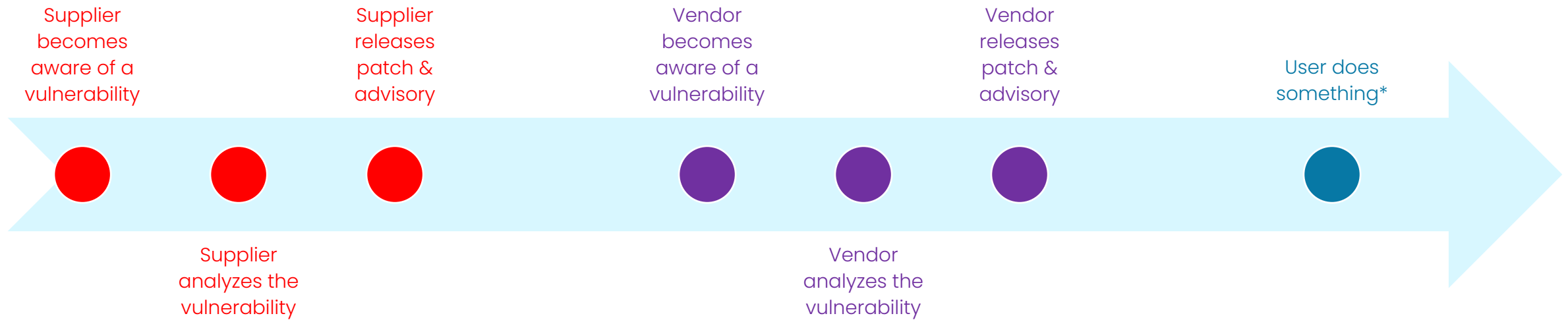
Supply chain

Timeframe of concern

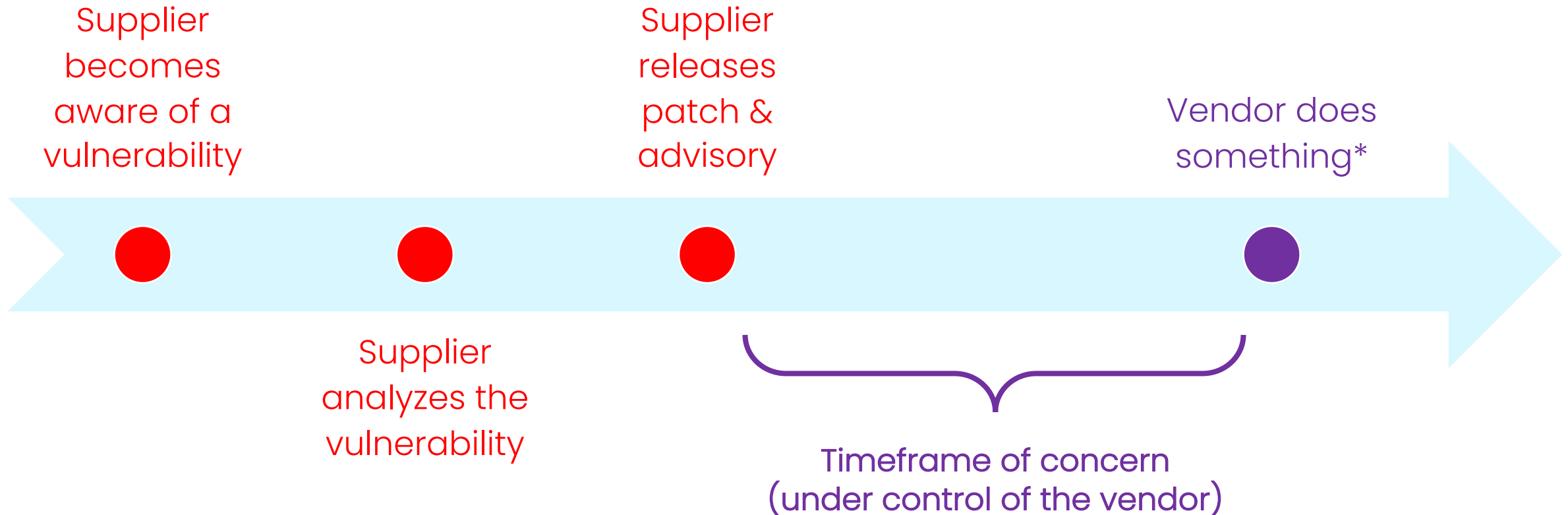


* Patch, mitigate risk, or actively accept risk

Supply chain



(Almost) Every vendor is a user



* Patch, mitigate risk, or actively accept risk

Distribution of CSAF

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 >=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

Example: provider- metadata.json

```
1 {
2   "canonical_url": "https://example01.test/.well-known/csaf/provider-metadata.json",
3   "distributions": [
4     {
5       "rolie": {
6         "feeds": [
7           {
8             "summary": "TLP:WHITE advisories",
9             "tlp_label": "WHITE",
10            "url": "https://example01.test/.well-known/csaf/white/csaf-feed-tlp-white.json"
11          },
12          {
13            "summary": "TLP:GREEN advisories",
14            "tlp_label": "GREEN",
15            "url": "https://example01.test/.well-known/csaf/green/csaf-feed-tlp-green.json"
16          },
17          {
18            "summary": "TLP:AMBER advisories",
19            "tlp_label": "AMBER",
20            "url": "https://example01.test/.well-known/csaf/amber/csaf-feed-tlp-amber.json"
21          },
22          {
23            "summary": "TLP:RED advisories",
24            "tlp_label": "RED",
25            "url": "https://example01.test/.well-known/csaf/red/csaf-feed-tlp-red.json"
26          }
27        ]
28      }
29    ]
30  },
31  "last_updated": "2022-10-06T15:27:07Z",
32  "list_on_CSAF_aggregators": true,
33  "metadata_version": "2.0",
34  "mirror_on_CSAF_aggregators": true,
35  "public_openpgp_keys": [
36    {
37      "fingerprint": "CAB38CCB13AA95142678A9EE7B86205B2D2F4BAF",
38      "url": "https://example01.test/.well-known/csaf/openpgp/CAB38CCB13AA95142678A9EE7B86205B2D2F4BAF.asc"
39    }
40  ],
41  "publisher": {
42    "category": "vendor",
43    "name": "Example Company 01 PSIRT",
44    "namespace": "https://psirt.example01.test"
45  },
46  "role": "csaf_trusted_provider"
47 }
```

Example: ROLIE feed

```
1 {
2   "feed": {
3     "id": "csaf-feed-tlp-white",
4     "title": "CSAF feed (TLP:WHITE)",
5     "link": [
6       {
7         "rel": "self",
8         "href": "https://example01.test/.well-known/csaf/white/csaf-feed-tlp-white.json"
9       }
10    ],
11    "category": [
12      {
13        "scheme": "urn:ietf:params:rolie:category:information-type",
14        "term": "csaf"
15      }
16    ],
17    "updated": "2022-10-06T15:27:23Z",
18    "entry": [
19      {
20        "id": "ESA-2022-002",
21        "title": "Log4Shell affects DEF",
22        "link": [
23          {
24            "rel": "self",
25            "href": "https://example01.test/.well-known/csaf/white/2022/esa-2022-002.json"
26          },
27          {
28            "rel": "hash",
29            "href": "https://example01.test/.well-known/csaf/white/2022/esa-2022-002.json.sha256"
30          },
31          {
32            "rel": "hash",
33            "href": "https://example01.test/.well-known/csaf/white/2022/esa-2022-002.json.sha512"
34          },
35          {
36            "rel": "signature",
37            "href": "https://example01.test/.well-known/csaf/white/2022/esa-2022-002.json.asc"
38          }
39        ],
40        "published": "2022-02-01T09:15:00Z",
41        "updated": "2022-06-07T08:15:00Z",
42        "content": {
43          "type": "application/json",
44          "src": "https://example01.test/.well-known/csaf/white/2022/esa-2022-002.json"
45        },
46        "format": {
47          "schema": "https://docs.oasis-open.org/csaf/csaf/v2.0/csaf_json_schema.json",
48          "version": "2.0"
49        }
50      }
51    ]
52  },
53 }
```

Scalable and resilient advisory distribution infrastructure (Saradi)

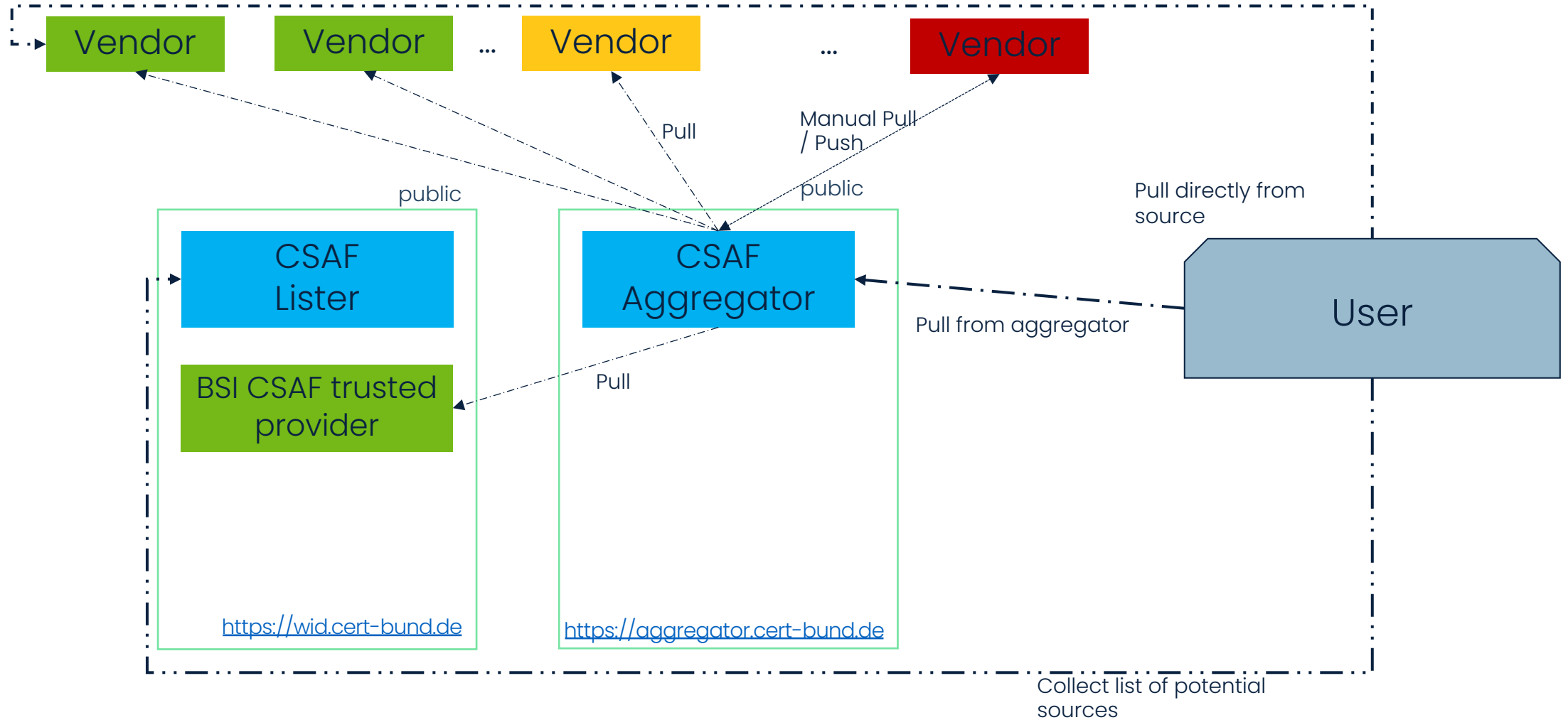
CSAF Lister

- Trusted party
- “yellow pages”
- List of CSAF providers and CSAF trusted providers
- Multiple around the world (National CERTs)
- First one available at <https://wid.cert-bund.de>

CSAF Aggregator

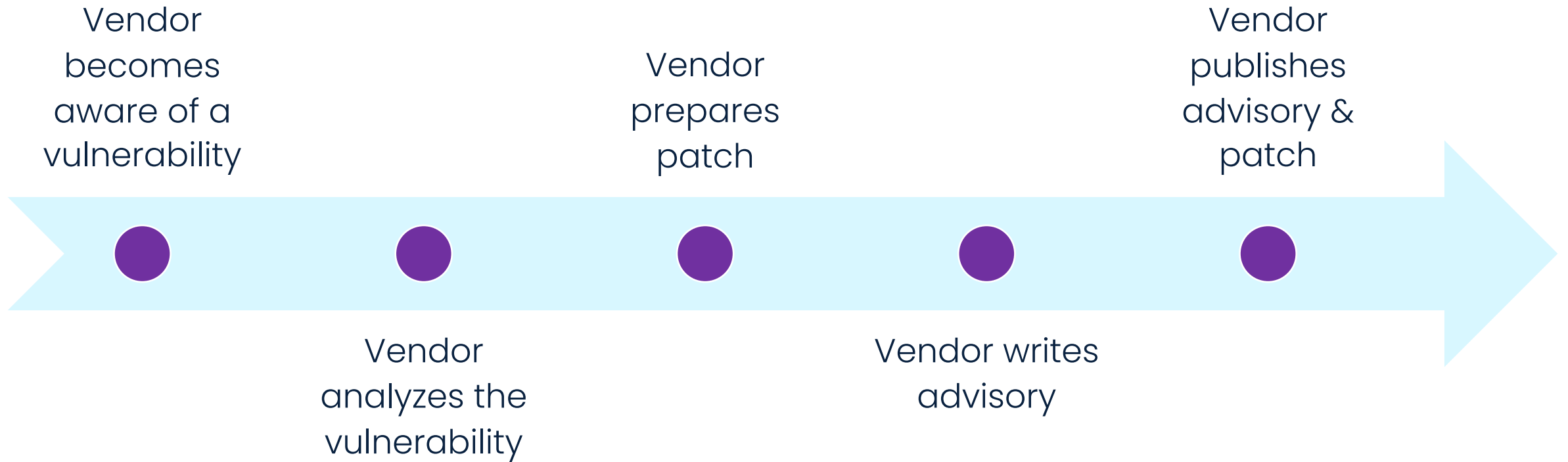
- Trusted party
- Collects advisories from issuers
- Provides them for automation
- One-stop-shop
- Multiple around the world (National CERTs)
- First one available at <https://aggregator.cert-bund.de>

Ecosystem

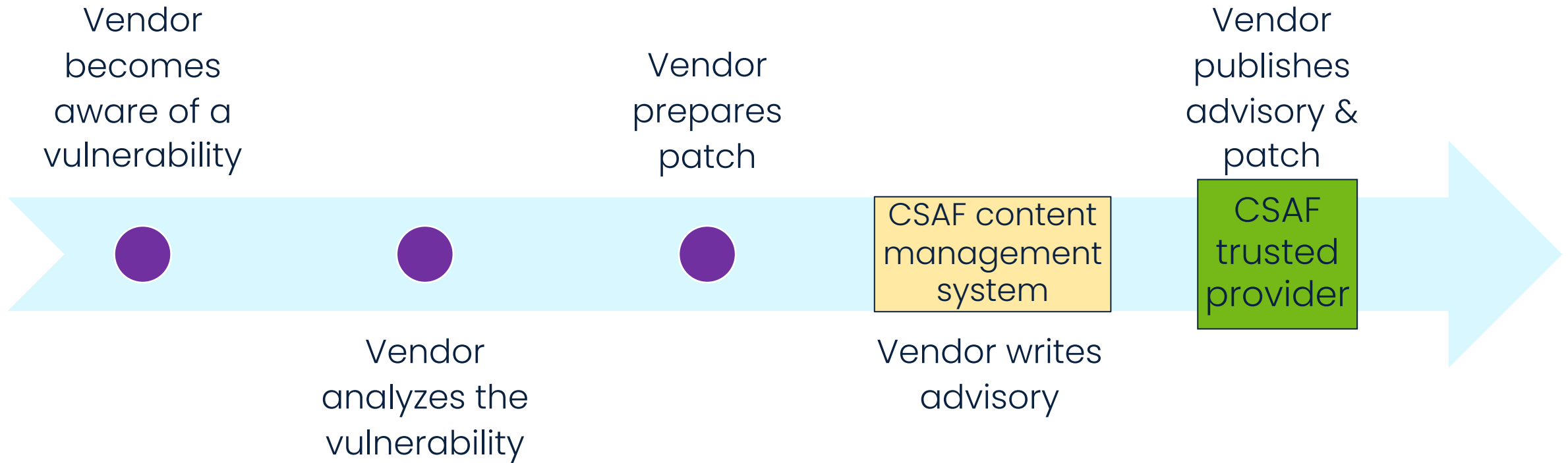


Tools

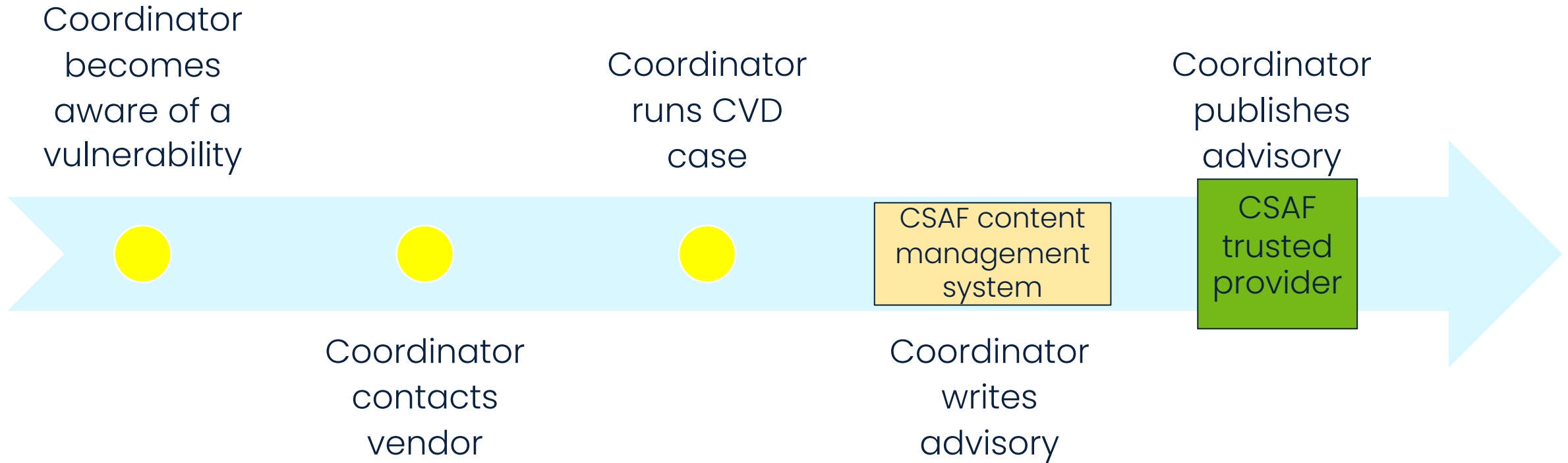
Vendor



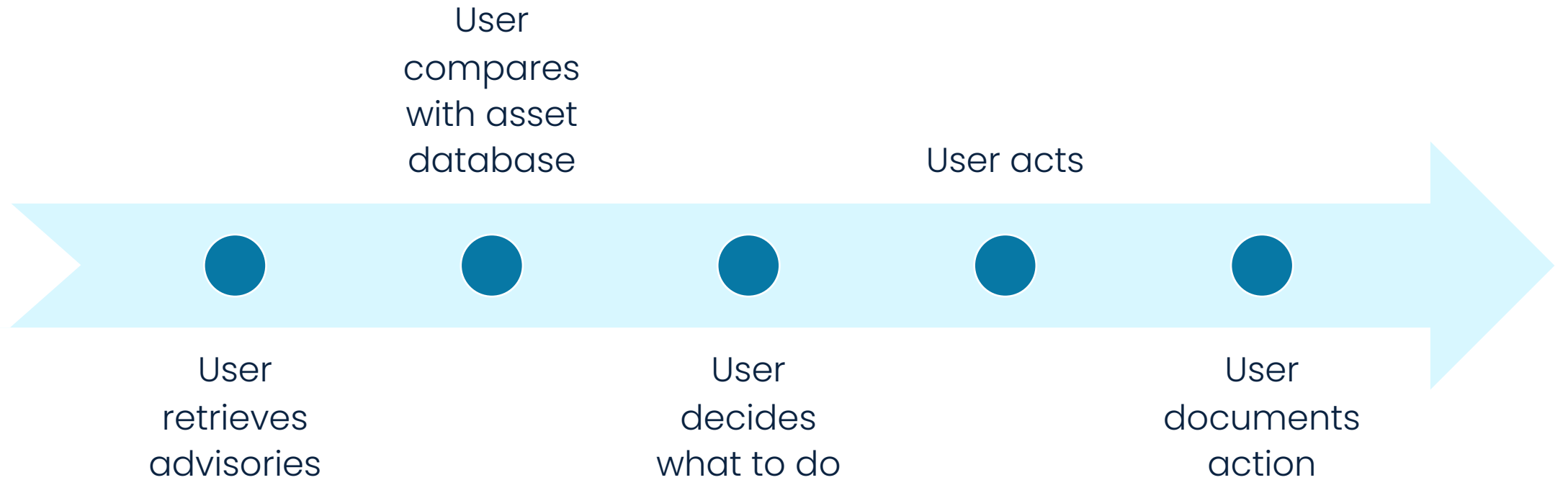
Vendor



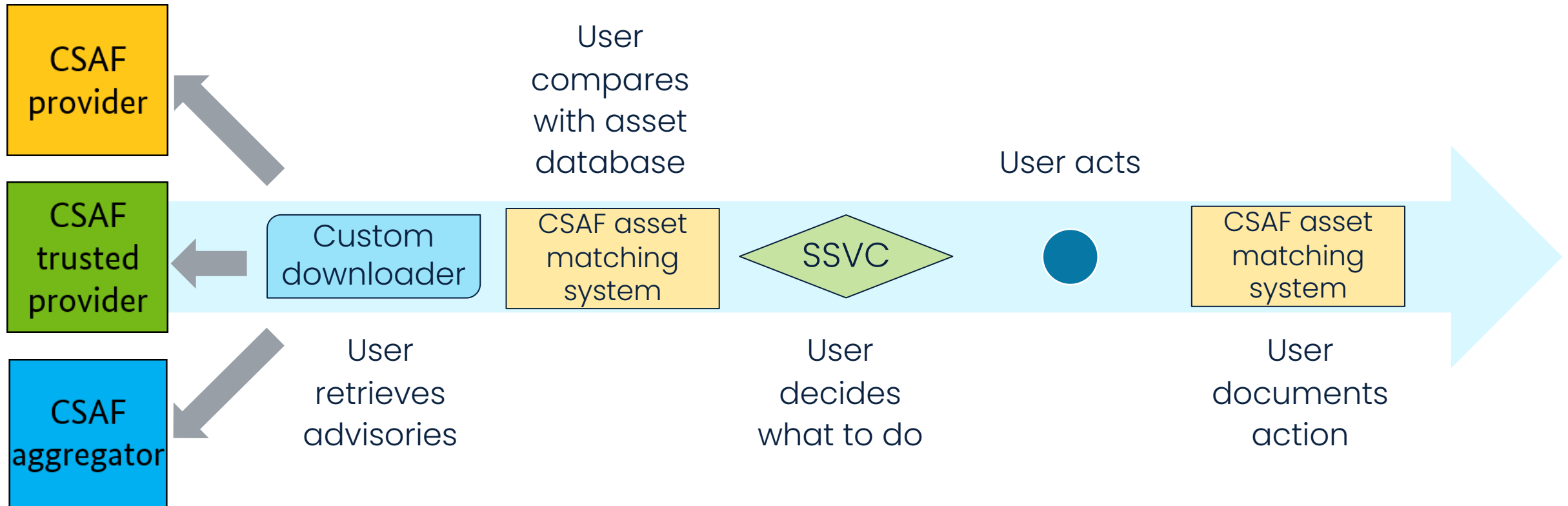
Coordinator (CVD)



User



User



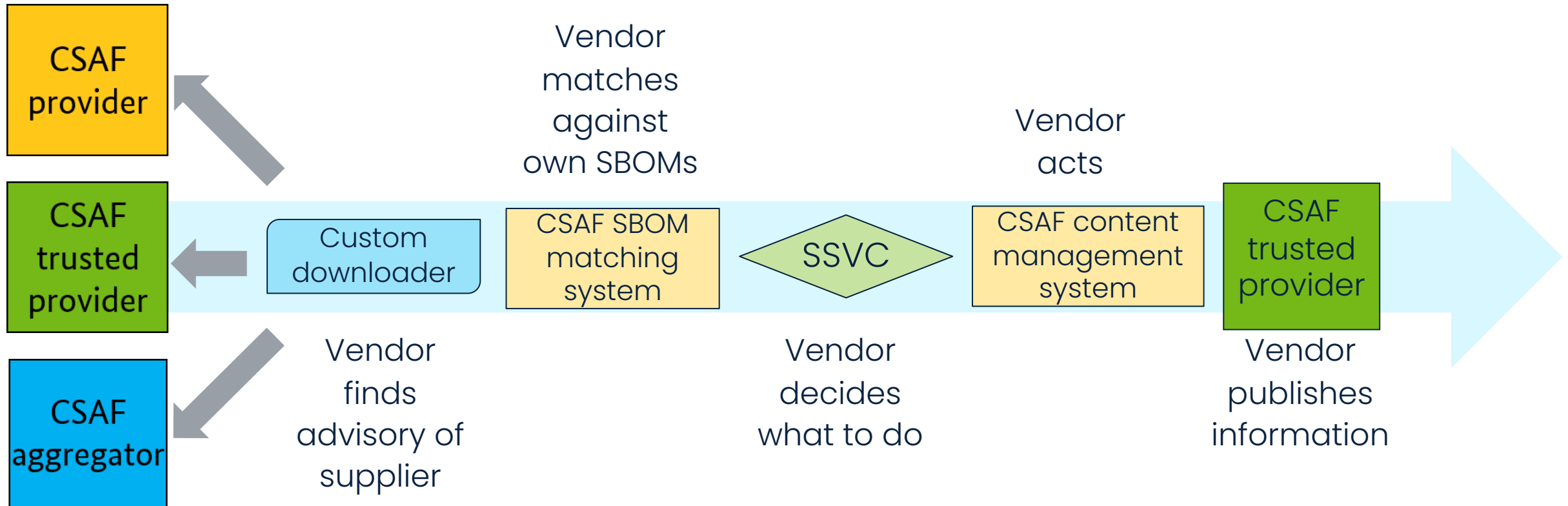
Tools developed by the community

- 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?**



SBOM and VEX

Supply chain



How to link to an SBOM?

Product identification helpers:

Retrievable SBOM

```
"sbom_urls": {  
  //...  
  "items": {  
    "https://example.com/location-to-sbom"  
  }  
}
```

How to link to an SBOM component?

CycloneDX:

```
"x_generic_uris": [  
  {  
    "namespace": "https://cyclonedx.org/capabilities/bomlink/",  
    "uri": "urn:cdx:411dafd2-c29f-491a-97d7-e97de5bc2289/1#pkg:maven/org.jboss.logging/jboss-logging@3.4.1.Final?type=jar"  
  }  
]
```

SPDX:

```
"x_generic_uris": [  
  {  
    "namespace": "https://spdx.github.io/spdx-spec/document-creation-information/#65-spdx-document-namespace-field",  
    "uri": "https://swinslow.net/spdx-examples/example4/main-bin-v2#SPDXRef-libc"  
  }  
]
```


Not every vulnerability is exploitable...

- Vulnerability Exploitability eXchange (VEX)
- Communicate product status explicit
- Machine-readable to address scalability

THE LINUX FOUNDATION PROJECTS

Zephyr


Resources Community Learn Members Contact Become a Member

Blog News Top News

Zephyr Security Update on Amnesia:33

December 16, 2020

Written by David Brown, on behalf of the Zephyr Security Team



On December 8, 2020, Forescout released a report containing numerous vulnerabilities found in various embedded TCP/IP stacks, known as **AMNESIA:33**. These vulnerabilities, across multiple network implementations, concern various memory and overflow errors, some of which are readily exploitable.

The Zephyr project received notification of this vulnerability through **CERT** before the publication date. We analyzed these vulnerabilities, and any affected code, and concluded that the Zephyr project is not impacted by any of these vulnerabilities, neither in the current releases, nor in any Long Term Support release.

Despite being collected under a single name, this report describes 33 vulnerabilities that are largely unrelated to one another. The report is the result of an analysis of 4 TCP/IP implementations that are commonly used in embedded systems: uIP, uIP in Contiki-OS, PicoTCP, and Fnet. Of these implementations, only the code in Fnet has ever been used in Zephyr.

The Zephyr LTS release 1.14 contains an implementation of the TCP stack from Fnet. Of the vulnerabilities reported in Fnet, 2, **CVE-2020-17468**, and **CVE-2020-17469**, are in the IPv6 Fnet code, one, **CVE-2020-17467**, affects Link-local Multicast Name Resolution (LLMNR), and 2, **CVE-2020-24383**, and **CVE-2020-17470** affect DNS functionality. None of the affected code has been used in the Zephyr project, while 1.14 does use the Fnet TCP, it does not use the affected IPv6, DNS or LLMNR code.

For current releases, including the current **2.4.0**, this code has been replaced by a Zephyr-specific implementation.

The Zephyr project takes security seriously, for more information on our processes involving security, including how to report vulnerabilities can be found on our [Security page](#).

The Zephyr project received notification of this vulnerability through **CERT** before the publication date. We analyzed these vulnerabilities, and any affected code, and concluded that the Zephyr project is not impacted by any of these vulnerabilities, neither in the current releases, nor in any Long Term Support release.

VEX is a Profile in CSAF

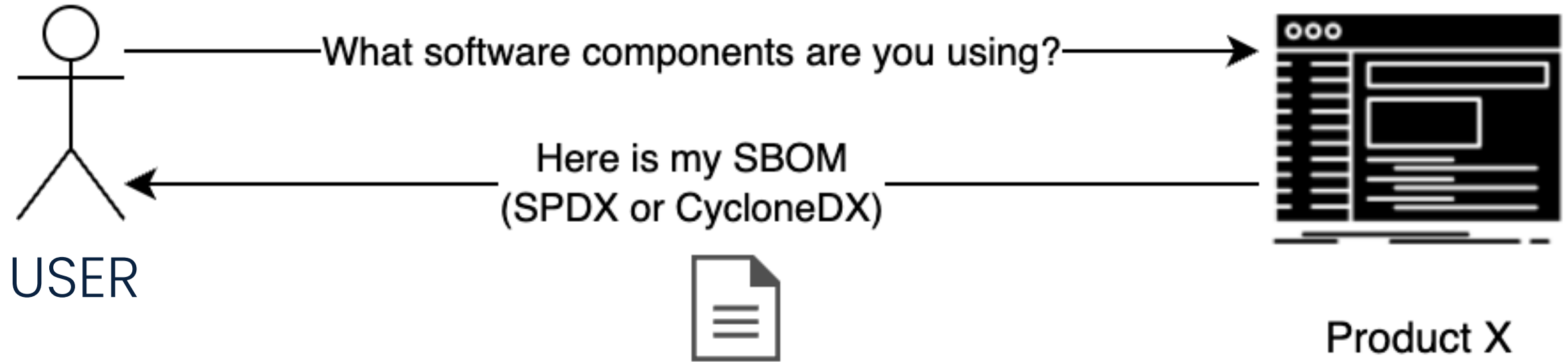
The Vulnerability Exploitability eXchange (VEX) allows a software supplier or other parties to assert the status of specific vulnerabilities in a particular product..

References:

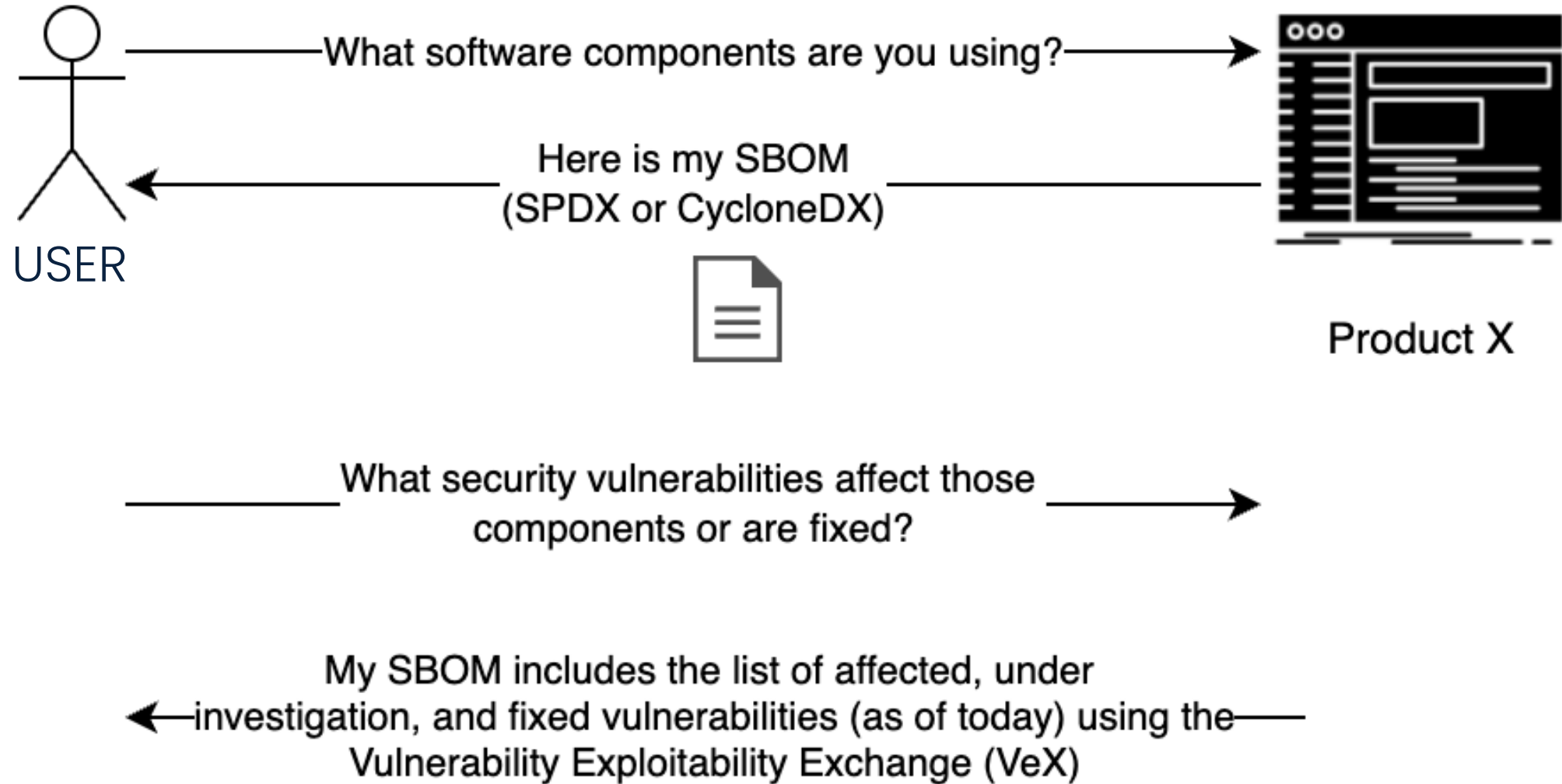
CISA's VEX Use Cases: https://www.cisa.gov/sites/default/files/publications/VEX_Use_Cases_Aprill2022.pdf

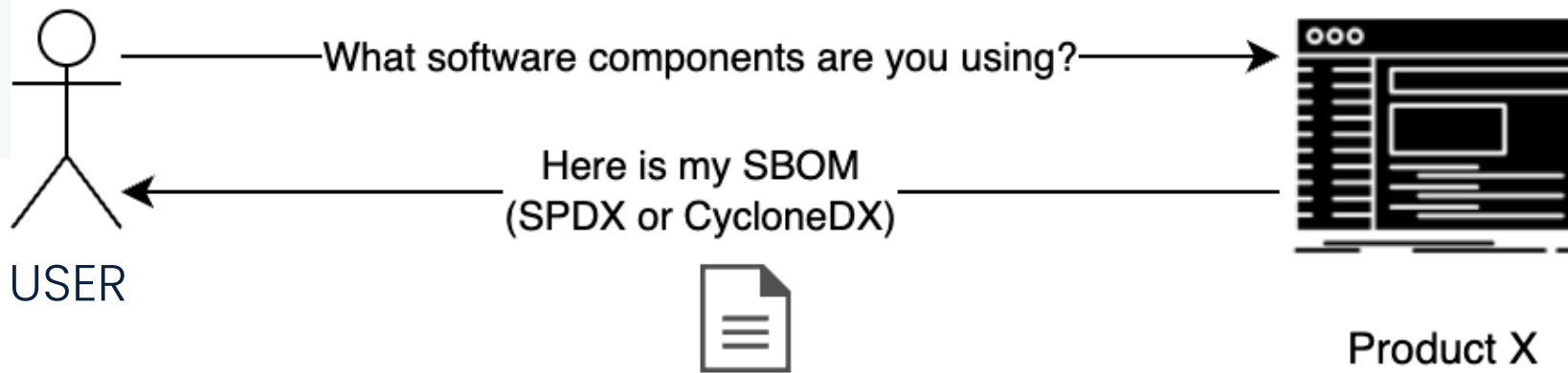
CISA's VEX Justifications: https://www.cisa.gov/sites/default/files/publications/VEX_Status_Justification_Jun22.pdf

How does this work?



How does this work?





What security vulnerabilities affect those components or are fixed?

My SBOM includes the list of affected, under investigation, and fixed vulnerabilities (as of today) using the Vulnerability Exploitability Exchange (VeX)

But, that's "point-in-time"... new vulnerabilities are disclosed on a regular basis...

No worries, you can use the Common Security Advisory Framework (CSAF) VeX documents...

VEX Statuses and Justifications

under_investigation

known_affected

fixed

known_not_affected

component_not_present

inline_mitigations_already_exist

vulnerable_code_cannot_be_controlled_by_adversary

vulnerable_code_not_in_execute_path

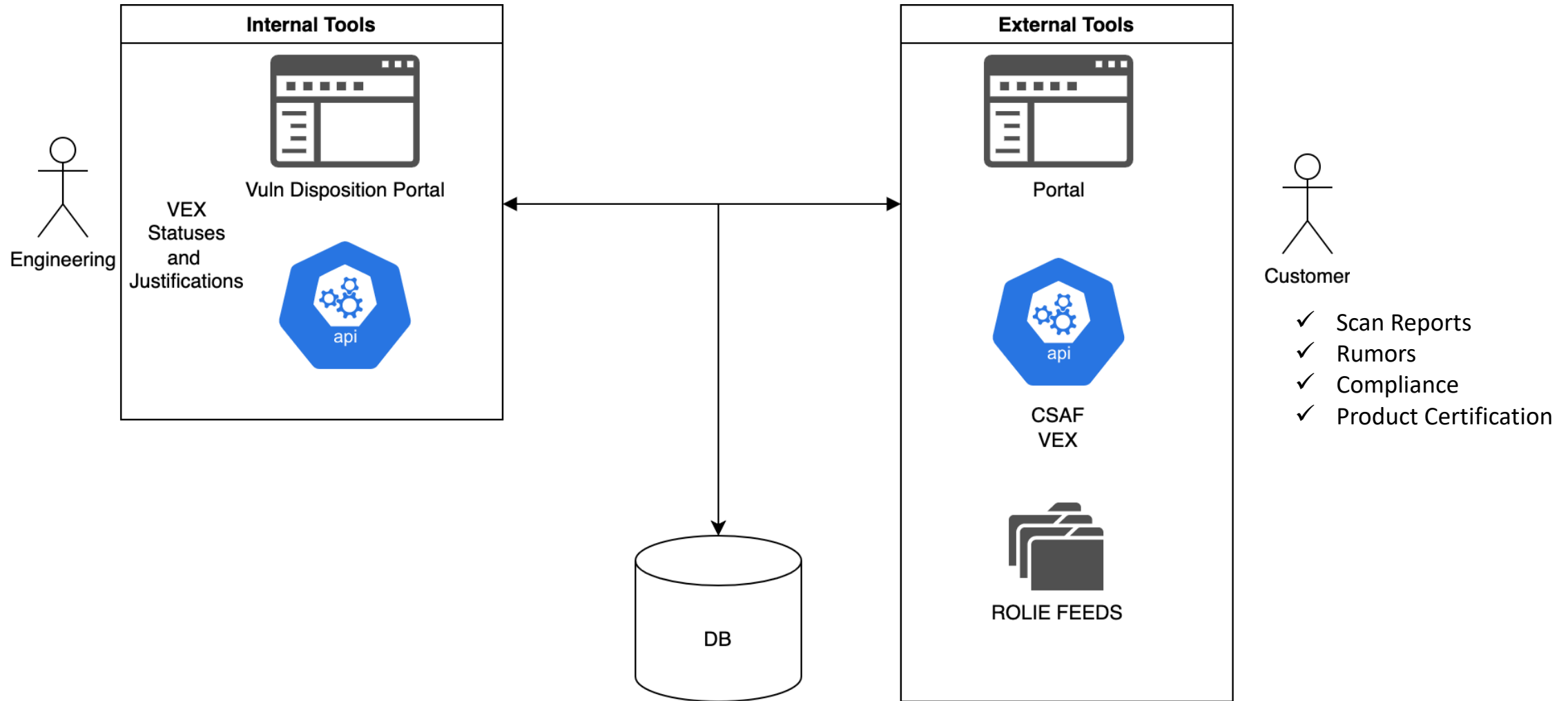
vulnerable_code_not_present

VEX Justifications: https://www.cisa.gov/sites/default/files/publications/VEX_Status_Justification_Jun22.pdf

You Don't Need an SBOM to VEX



Example of "Dynamic Automated" Advisories



CSAF in operations

Organizations publishing CSAF



Federal Office
for Information Security



Life Is On



Red Hat



Summary

Summary and Action items

- 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
- Spread the word! #oCSAF #advisory

