OASIS OPEN

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

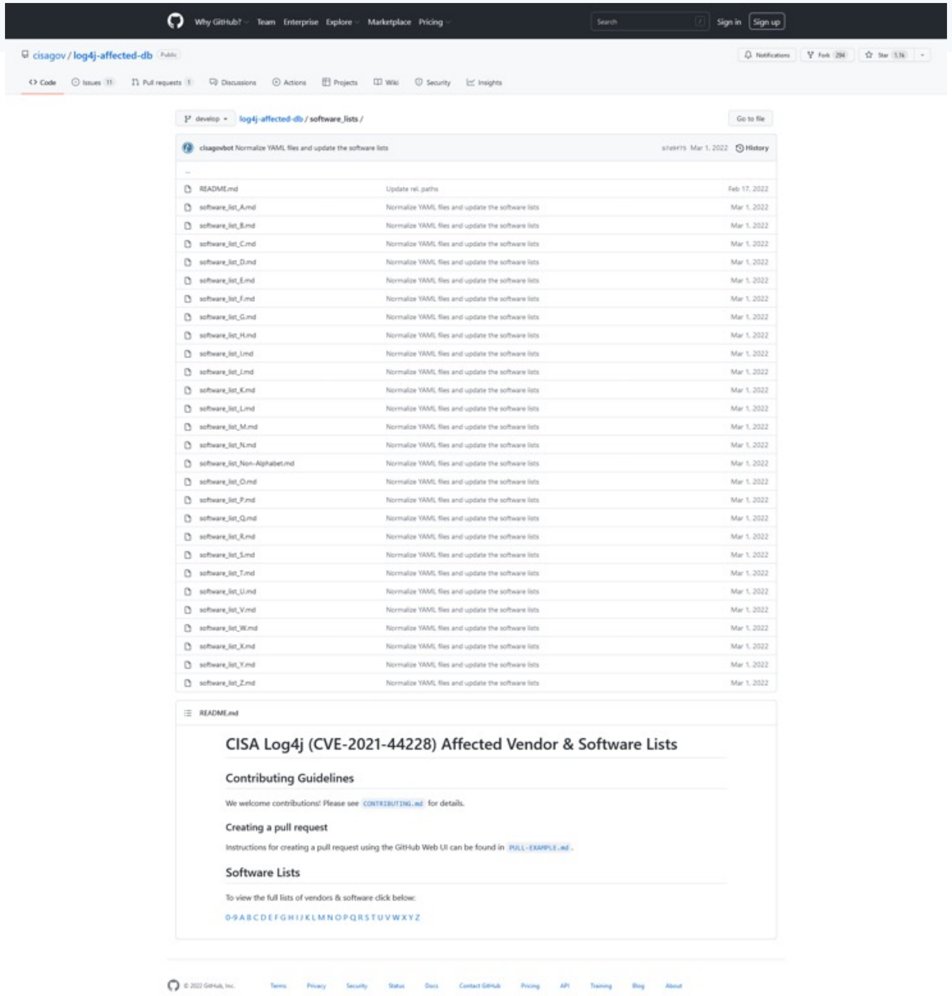
Thomas Schmidt, BSI

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



cisagov / log4j-affected-db Public

log4j-affected-db / software_lists /

cisagovbot Normalize YAML files and update the software lists Mar 1, 2022

..		
README.md	Update rel. paths	Feb 17, 2022
software_list_A.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_B.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_C.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_D.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_E.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_F.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_G.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_H.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_I.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_J.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_K.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_L.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_M.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_N.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_Non-Alphabet.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_O.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_P.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_Q.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_R.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_S.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_T.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_U.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_V.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_W.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_X.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_Y.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_Z.md	Normalize YAML 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

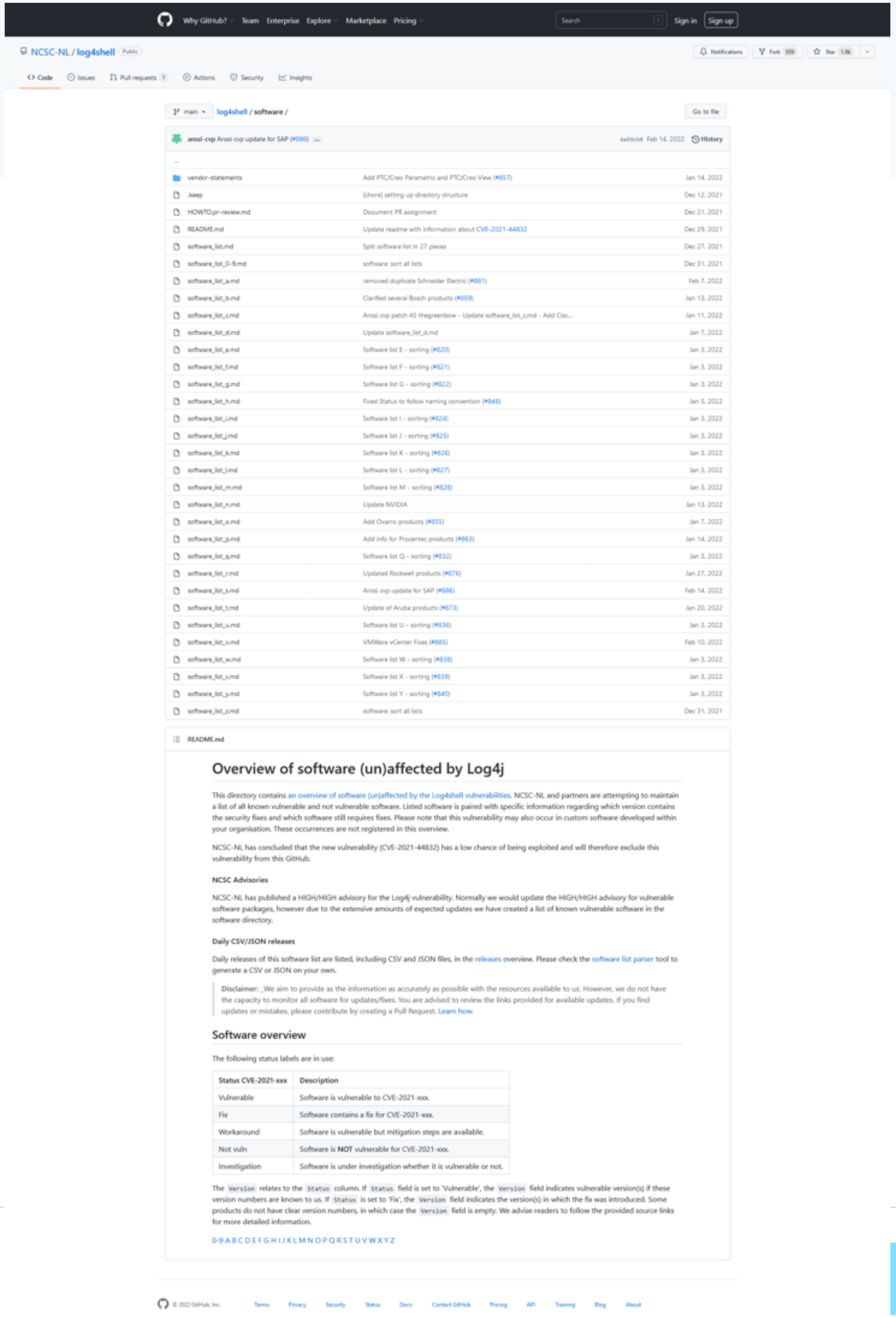
Instructions for creating a pull request using the GitHub Web UI can be found in `PULL-EXAMPLE.md`.

Software Lists

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

0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

© 2022 GitHub, Inc. Terms Privacy Security Status Docs Contact GitHub Pricing API Training Blog About



NCSC-NL / log4shell Public

log4shell / software /

anssi-cvp Anssi cvp update for SAP (#886) … Feb 14, 2022

..		
vendor-statements	Add PTC/Creo Parametric and PTC/Creo View (#857)	Jan 14, 2022
.keep	[chore] setting up directory structure	Dec 12, 2021
HOWTO.pr-review.md	Document PR assignment	Dec 21, 2021
README.md	Update readme with information about CVE-2021-44832	Dec 29, 2021
software_list.md	Split software list in 27 pieces	Dec 27, 2021
software_list_0-9.md	software: sort all lists	Dec 31, 2021
software_list_a.md	removed duplicate Schneider Electric (#881)	Feb 7, 2022
software_list_b.md	Clarified several Bosch products (#859)	Jan 13, 2022
software_list_c.md	Anssi cvp patch 45 thegreenbow - Update software_list_c.md - Add Cisc…	Jan 11, 2022
software_list_d.md	Update software_list_d.md	Jan 7, 2022
software_list_e.md	Software list E - sorting (#820)	Jan 3, 2022
software_list_f.md	Software list F - sorting (#821)	Jan 3, 2022
software_list_g.md	Software list G - sorting (#822)	Jan 3, 2022
software_list_h.md	Fixed Status to follow naming convention (#848)	Jan 5, 2022
software_list_i.md	Software list I - sorting (#824)	Jan 3, 2022
software_list_j.md	Software list J - sorting (#825)	Jan 3, 2022
software_list_k.md	Software list K - sorting (#826)	Jan 3, 2022
software_list_l.md	Software list L - sorting (#827)	Jan 3, 2022
software_list_m.md	Software list M - sorting (#828)	Jan 3, 2022
software_list_n.md	Update NVIDIA	Jan 13, 2022
software_list_o.md	Add Ovarro products (#855)	Jan 7, 2022
software_list_p.md	Add info for Procentec products (#863)	Jan 14, 2022
software_list_q.md	Software list Q - sorting (#832)	Jan 3, 2022
software_list_r.md	Updated Rockwell products (#876)	Jan 27, 2022
software_list_s.md	Anssi cvp update for SAP (#886)	Feb 14, 2022
software_list_t.md	Update of Aruba products (#873)	Jan 20, 2022
software_list_u.md	Software list U - sorting (#836)	Jan 3, 2022
software_list_v.md	VMWare vCenter Fixes (#885)	Feb 10, 2022
software_list_w.md	Software list W - sorting (#838)	Jan 3, 2022
software_list_x.md	Software list X - sorting (#839)	Jan 3, 2022
software_list_y.md	Software list Y - sorting (#840)	Jan 3, 2022
software_list_z.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/fixes. 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

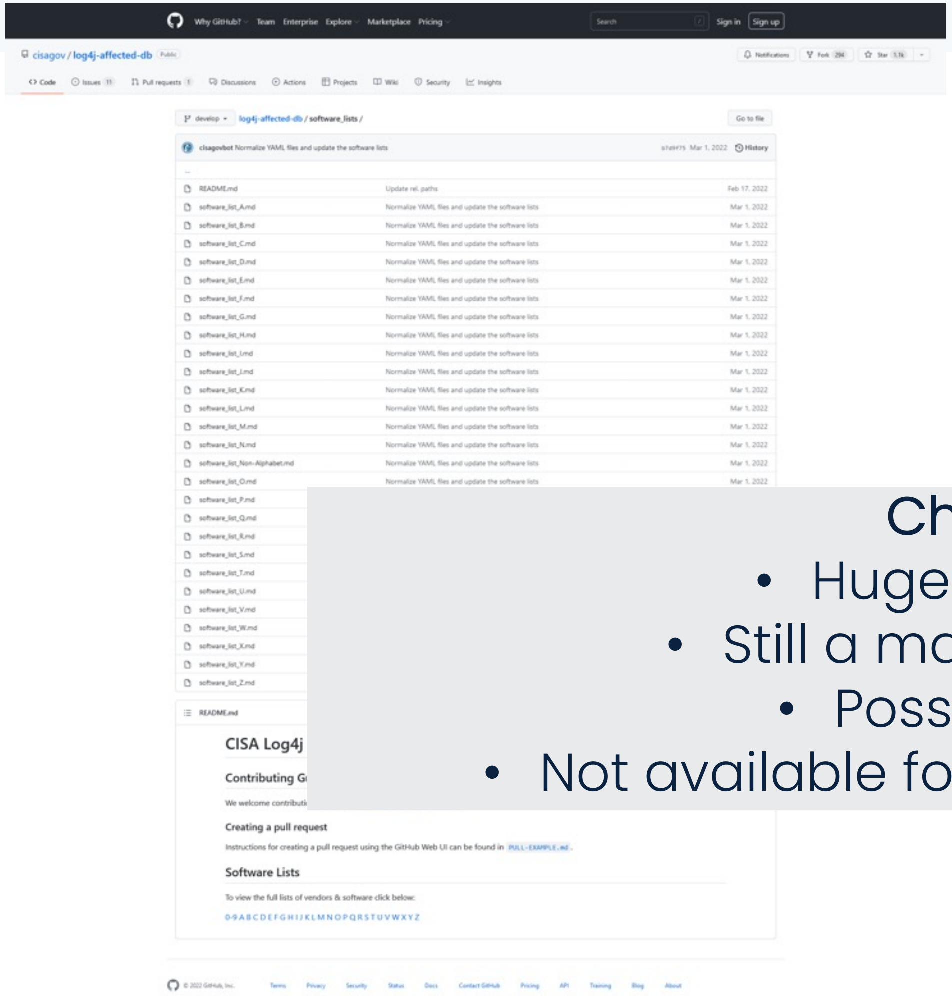
The following status labels are in use:

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.

0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

© 2022 GitHub, Inc. Terms Privacy Security Status Docs Contact GitHub Pricing API Training Blog About



cisagov / log4j-affected-db

log4j-affected-db / software_lists /

cisagovbot Normalize YAML files and update the software lists — Mar 1, 2022

..		
README.md	Update rel. paths	Feb 17, 2022
software_list_A.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_B.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_C.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_D.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_E.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_F.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_G.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_H.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_I.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_J.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_K.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_L.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_M.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_N.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_Non-Alphabet.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_O.md	Normalize YAML files and update the software lists	Mar 1, 2022
software_list_P.md		
software_list_Q.md		
software_list_R.md		
software_list_S.md		
software_list_T.md		
software_list_U.md		
software_list_V.md		
software_list_W.md		
software_list_X.md		
software_list_Y.md		
software_list_Z.md		

README.md

CISA Log4j

Contributing G

We welcome contributi

Creating a pull request

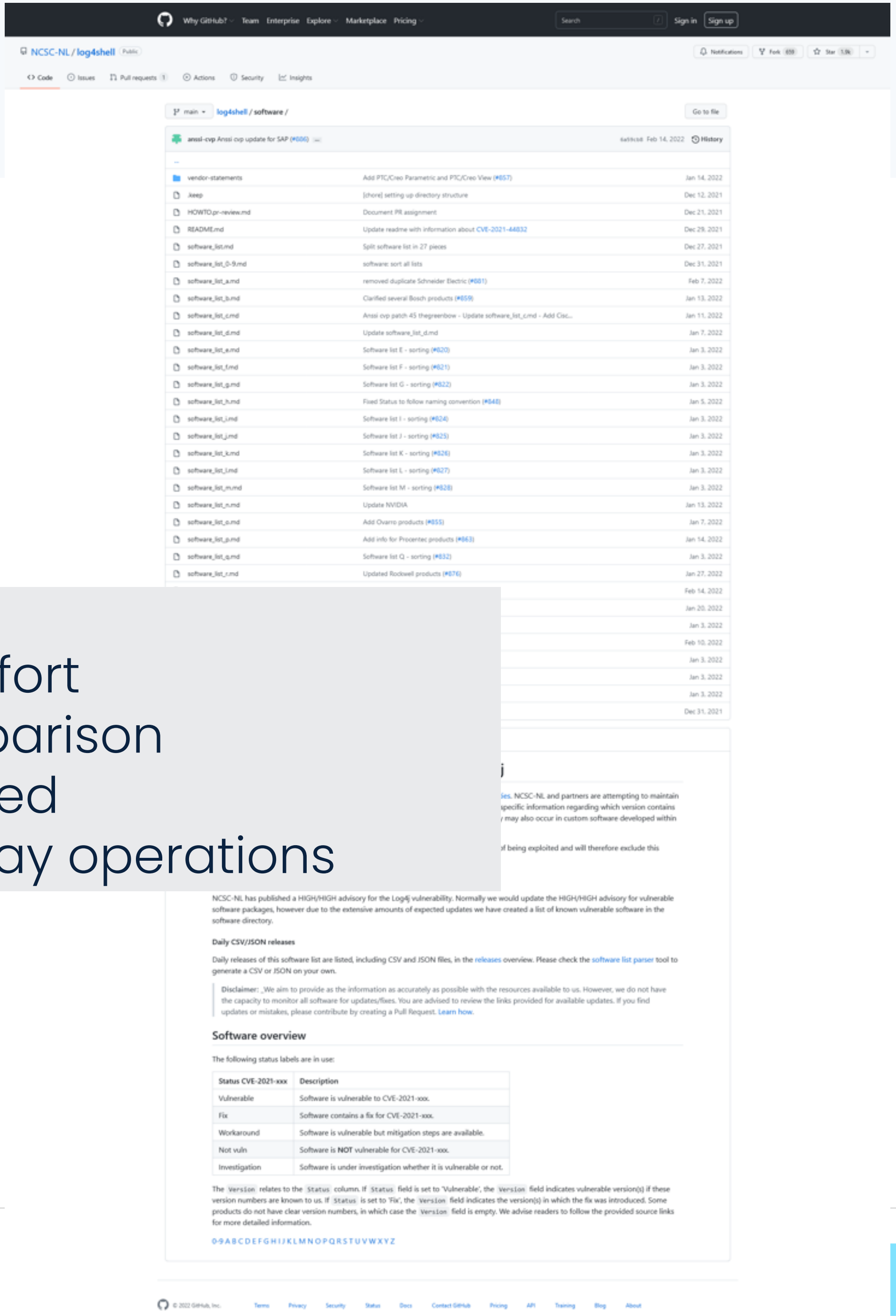
Instructions for creating a pull request using the GitHub Web UI can be found in `PULL-EXAMPLE.md`.

Software Lists

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

0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

© 2022 GitHub, Inc. Terms Privacy Security Status Docs Contact GitHub Pricing API Training Blog About



NCSC-NL / log4shell

log4shell / software /

anssi-cvp Anssi cvp update for SAP (#886) … — Feb 14, 2022

..		
vendor-statements	Add PTC/Creo Parametric and PTC/Creo View (#857)	Jan 14, 2022
.keep	[chore] setting up directory structure	Dec 12, 2021
HOWTO.pr-review.md	Document PR assignment	Dec 21, 2021
README.md	Update readme with information about CVE-2021-44832	Dec 29, 2021
software_list.md	Split software list in 27 pieces	Dec 27, 2021
software_list_0-9.md	software: sort all lists	Dec 31, 2021
software_list_a.md	removed duplicate Schneider Electric (#881)	Feb 7, 2022
software_list_b.md	Clarified several Bosch products (#859)	Jan 13, 2022
software_list_c.md	Anssi cvp patch 45 thegreenbow - Update software_list_c.md - Add Cisc...	Jan 11, 2022
software_list_d.md	Update software_list_d.md	Jan 7, 2022
software_list_e.md	Software list E - sorting (#820)	Jan 3, 2022
software_list_f.md	Software list F - sorting (#821)	Jan 3, 2022
software_list_g.md	Software list G - sorting (#822)	Jan 3, 2022
software_list_h.md	Fixed Status to follow naming convention (#848)	Jan 5, 2022
software_list_i.md	Software list I - sorting (#824)	Jan 3, 2022
software_list_j.md	Software list J - sorting (#825)	Jan 3, 2022
software_list_k.md	Software list K - sorting (#826)	Jan 3, 2022
software_list_l.md	Software list L - sorting (#827)	Jan 3, 2022
software_list_m.md	Software list M - sorting (#828)	Jan 3, 2022
software_list_n.md	Update NVIDIA	Jan 13, 2022
software_list_o.md	Add Ovarro products (#855)	Jan 7, 2022
software_list_p.md	Add info for Procentec products (#863)	Jan 14, 2022
software_list_q.md	Software list Q - sorting (#832)	Jan 3, 2022
software_list_r.md	Updated Rockwell products (#876)	Jan 27, 2022
		Feb 14, 2022
		Jan 20, 2022
		Jan 3, 2022
		Feb 10, 2022
		Jan 3, 2022
		Jan 3, 2022
		Jan 3, 2022
		Dec 31, 2021

j

ies. NCSC-NL and partners are attempting to maintain
pecific information regarding which version contains
may also occur in custom software developed within

f being exploited and will therefore exclude this

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/fixes. 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.

0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

© 2022 GitHub, Inc. Terms Privacy Security Status Docs Contact GitHub Pricing API Training Blog About

Challenges:

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

Manual process

Manual Processes

1

Vendors

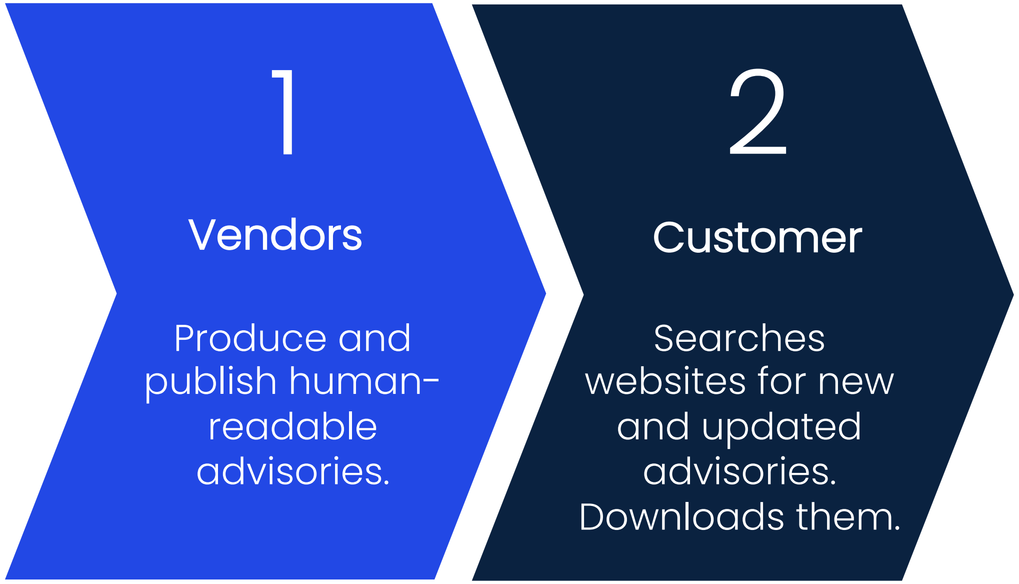
Produce and publish human-readable advisories.

Severity

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

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

Manual Processes



1

Vendors

Produce and publish human-readable advisories.

2

Customer

Searches websites for new and updated advisories. Downloads them.

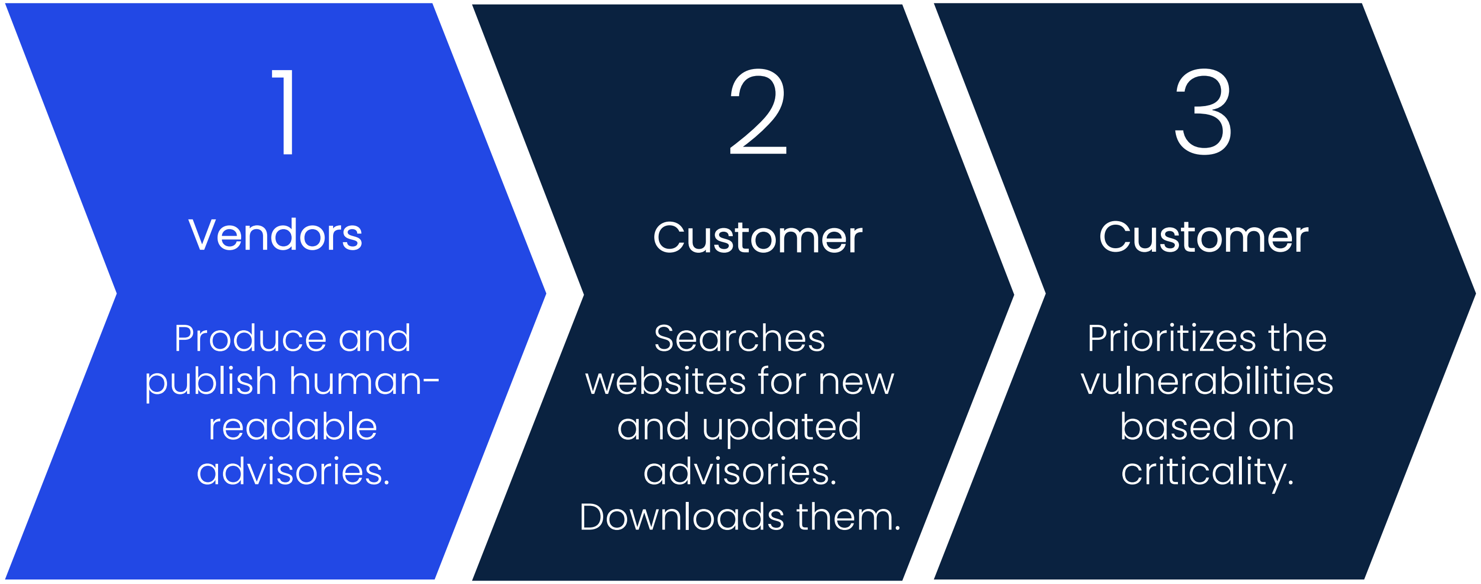
Severity

- 🟥 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



1

Vendors

Produce and publish human-readable advisories.

2

Customer

Searches websites for new and updated advisories. Downloads them.

3

Customer

Prioritizes the vulnerabilities based on criticality.

Severity

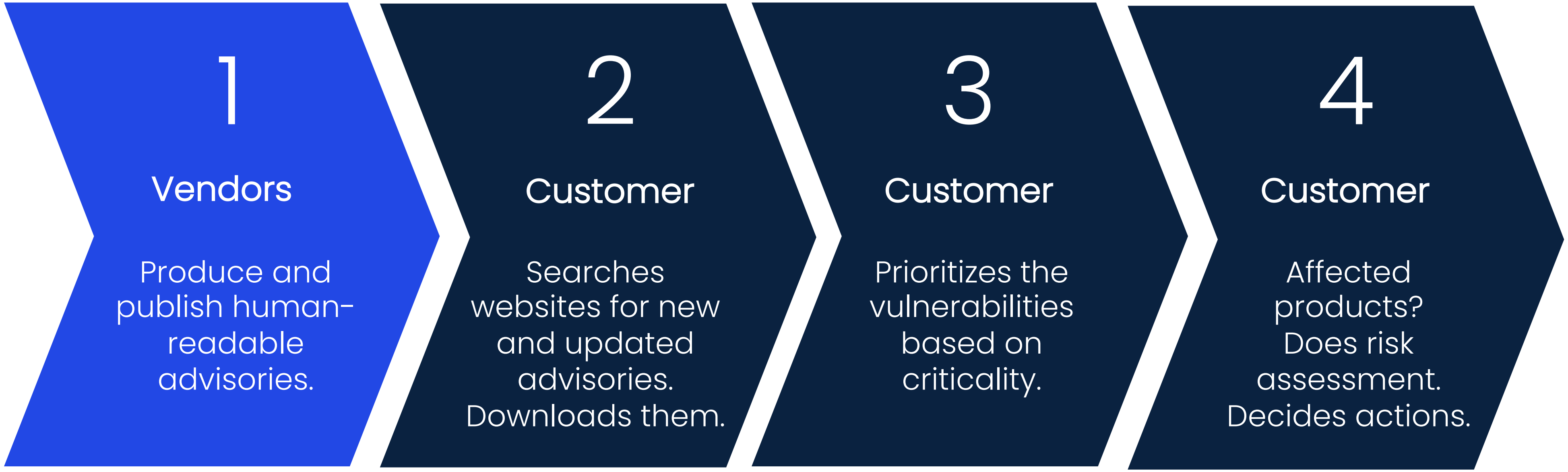
- 🟥 critical
- 🟧 high
- 🟨 medium
- 🟩 low

🟩 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



1

Vendors

Produce and publish human-readable advisories.

2

Customer

Searches websites for new and updated advisories. Downloads them.

3

Customer

Prioritizes the vulnerabilities based on criticality.

4

Customer

Affected products? Does risk assessment. Decides actions.

Severity

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

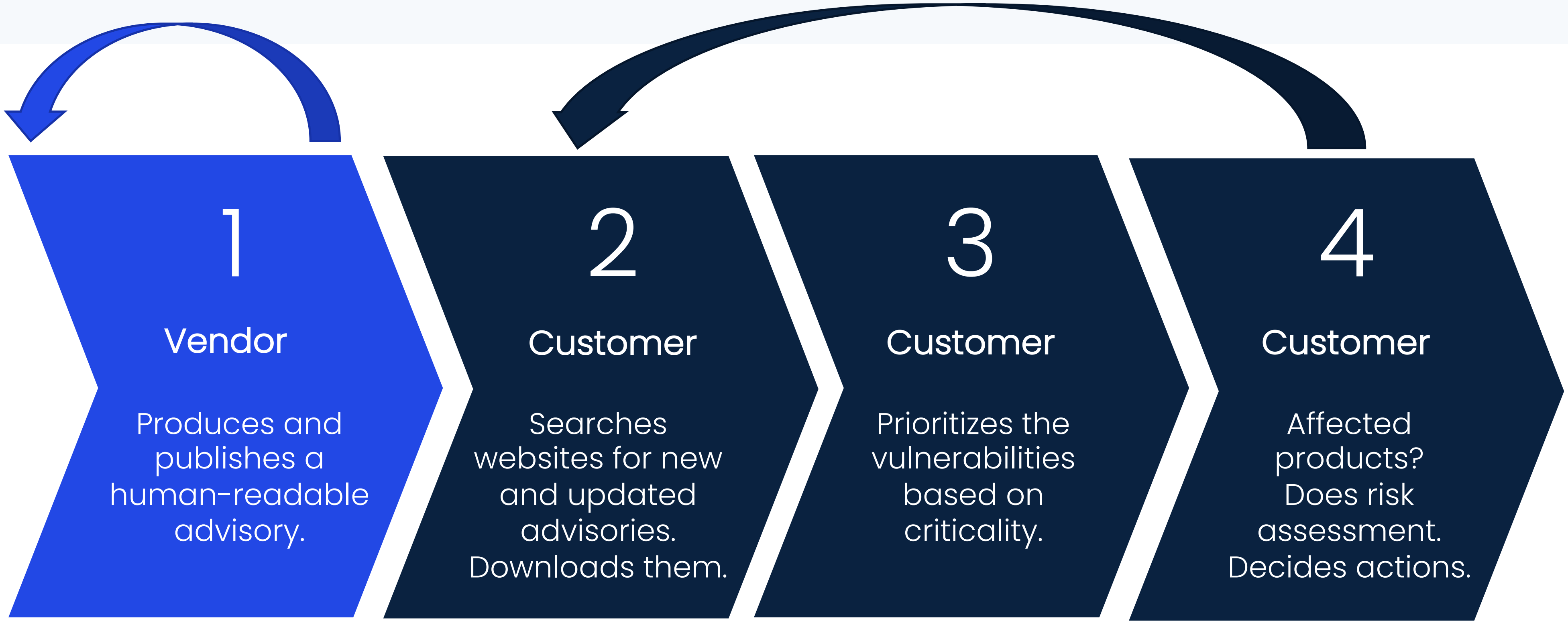
🟩 1	🟧 6	🟩 11
🟧 2	🟧 7	🟧 12
🟧 3	🟨 8	🟥 13
🟩 4	🟧 9	🟨 14
🟥 5	🟥 10	🟧 15

🟩 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



1

Vendor

Produces and publishes a human-readable advisory.

2

Customer

Searches websites for new and updated advisories. Downloads them.

3

Customer

Prioritizes the vulnerabilities based on criticality.

4

Customer

Affected products? Does risk assessment. Decides actions.

Severity	
🟥	critical
🟧	high
🟨	medium
🟩	low

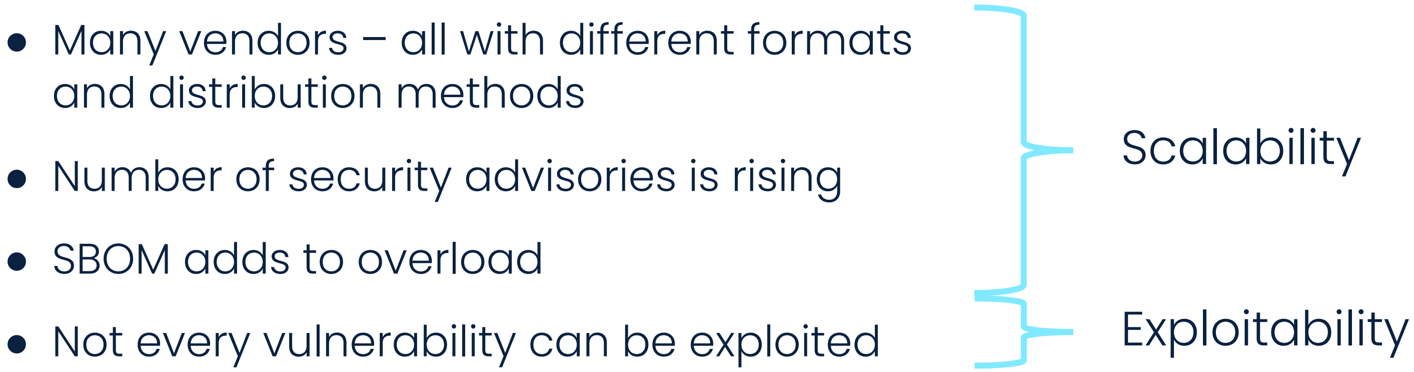
🟩 1	🟧 6	🟩 11
🟧 2	🟧 7	🟧 12
🟧 3	🟨 8	🟥 13
🟩 4	🟧 9	🟨 14
🟥 5	🟥 10	🟧 15

🟩 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

Scalability

Exploitability

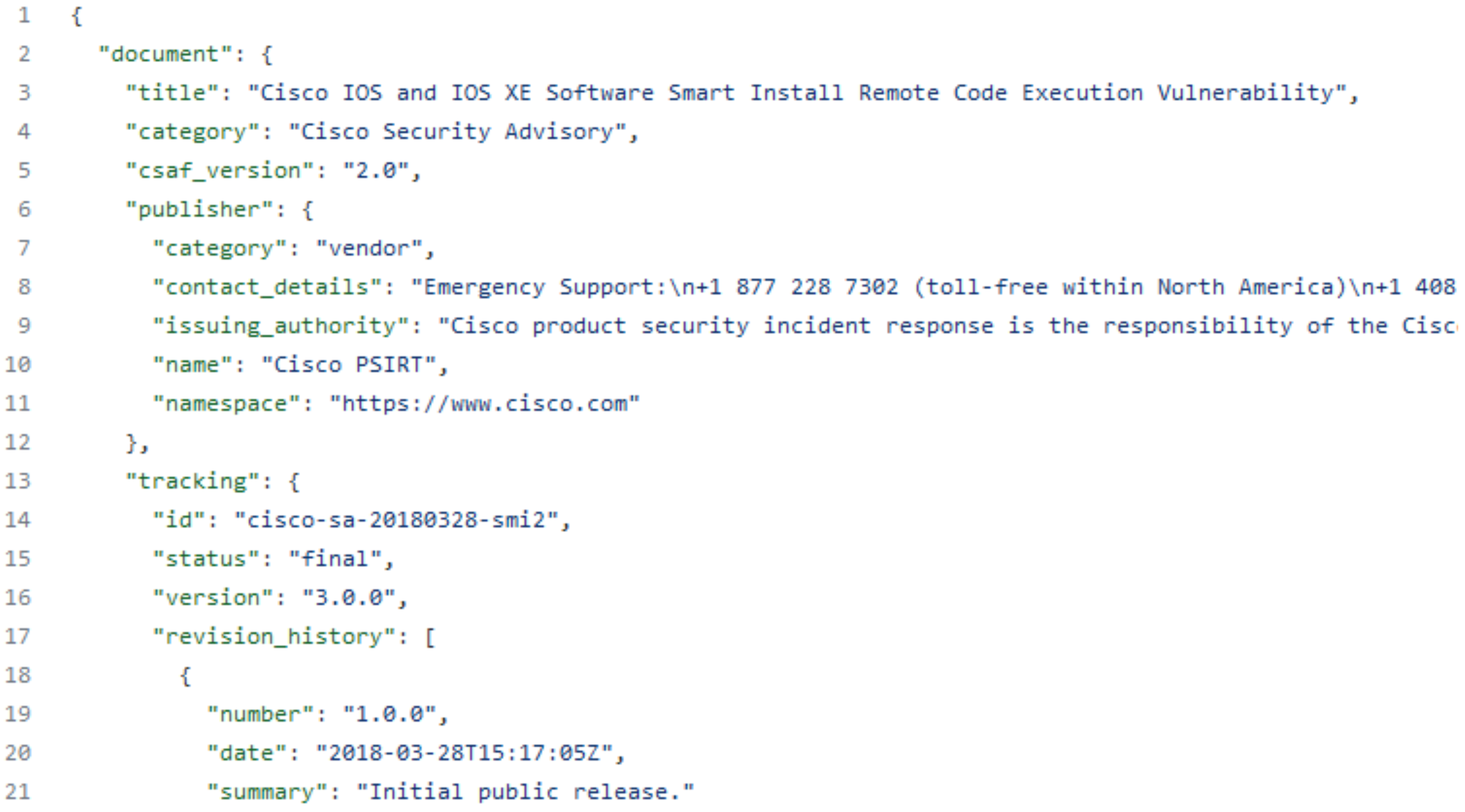
What is CSAF?

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

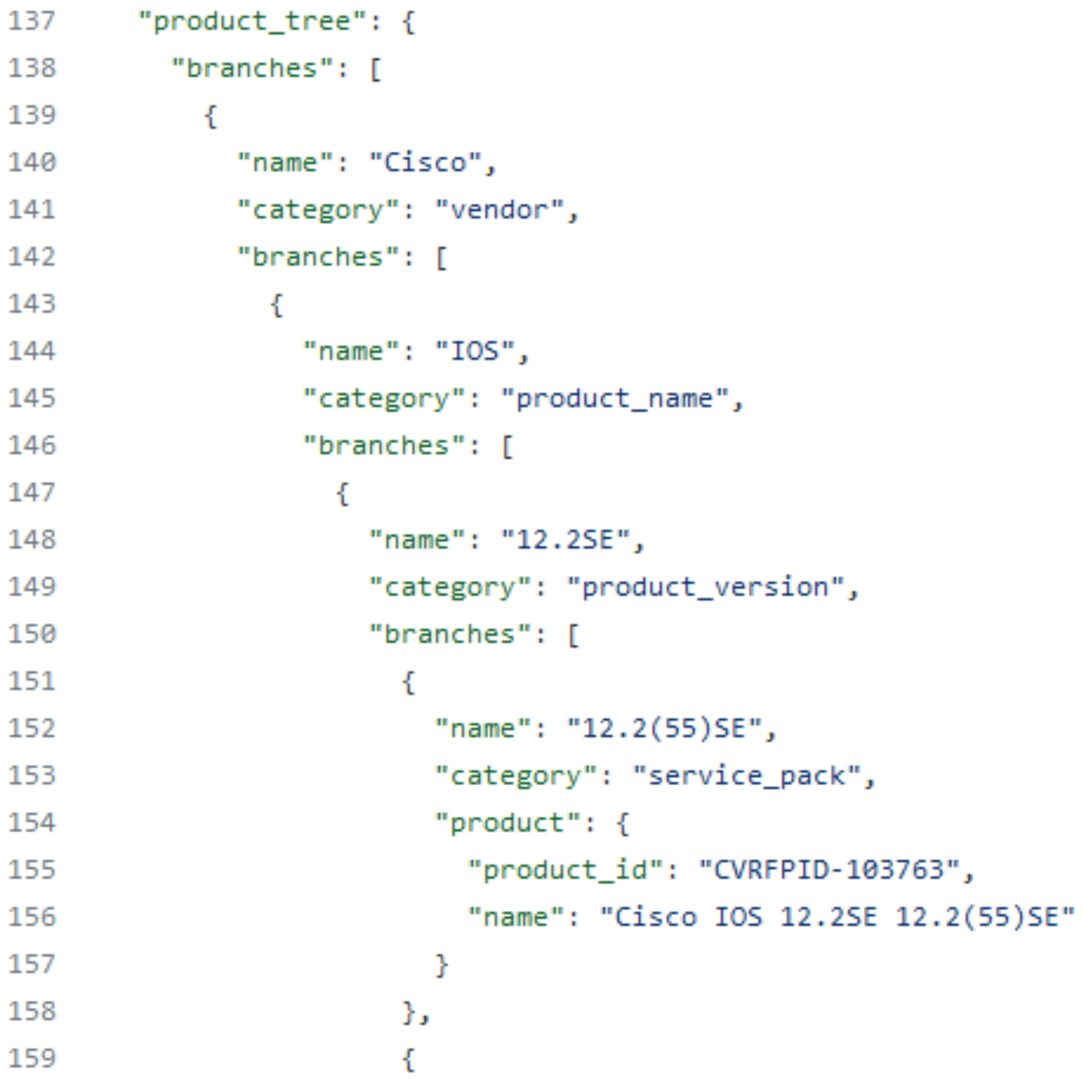
Document



```
{
  "document": {
    "title": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability",
    "category": "Cisco Security Advisory",
    "csaf_version": "2.0",
    "publisher": {
      "category": "vendor",
      "contact_details": "Emergency Support:\n+1 877 228 7302 (toll-free within North America)\n+1 408
      "issuing_authority": "Cisco product security incident response is the responsibility of the Cisc
      "name": "Cisco PSIRT",
      "namespace": "https://www.cisco.com"
    },
    "tracking": {
      "id": "cisco-sa-20180328-smi2",
      "status": "final",
      "version": "3.0.0",
      "revision_history": [
        {
          "number": "1.0.0",
          "date": "2018-03-28T15:17:05Z",
          "summary": "Initial public release."
```

Example: CSAF Document

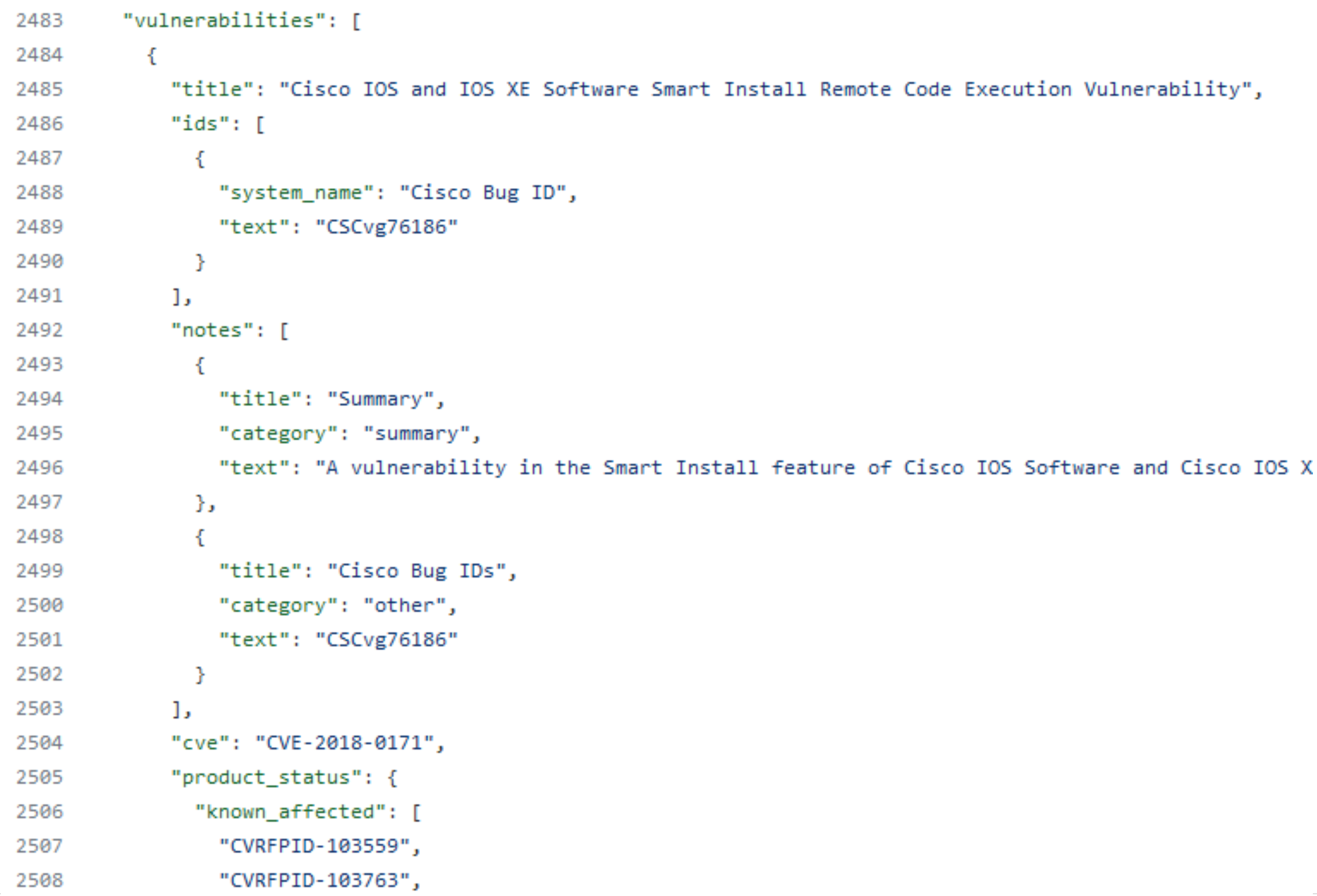
Product Tree



```
"product_tree": {
  "branches": [
    {
      "name": "Cisco",
      "category": "vendor",
      "branches": [
        {
          "name": "IOS",
          "category": "product_name",
          "branches": [
            {
              "name": "12.2SE",
              "category": "product_version",
              "branches": [
                {
                  "name": "12.2(55)SE",
                  "category": "service_pack",
                  "product": {
                    "product_id": "CVRFPID-103763",
                    "name": "Cisco IOS 12.2SE 12.2(55)SE"
                  }
                },
                {
```

Example: CSAF Document

Vulnerabilities



```
"vulnerabilities": [
  {
    "title": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability",
    "ids": [
      {
        "system_name": "Cisco Bug ID",
        "text": "CSCvg76186"
      }
    ],
    "notes": [
      {
        "title": "Summary",
        "category": "summary",
        "text": "A vulnerability in the Smart Install feature of Cisco IOS Software and Cisco IOS X
      },
      {
        "title": "Cisco Bug IDs",
        "category": "other",
        "text": "CSCvg76186"
      }
    ],
    "cve": "CVE-2018-0171",
    "product_status": {
      "known_affected": [
        "CVRFPID-103559",
        "CVRFPID-103763",
```

Process with CSAF

1

Vendor

Produces and publishes a **machine-readable** advisory.

Severity

🟥	critical
🟧	high
🟨	medium
🟩	low

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

Process with CSAF

1

Vendor

Produces and publishes a **machine-readable** advisory.

Severity

🟥 critical

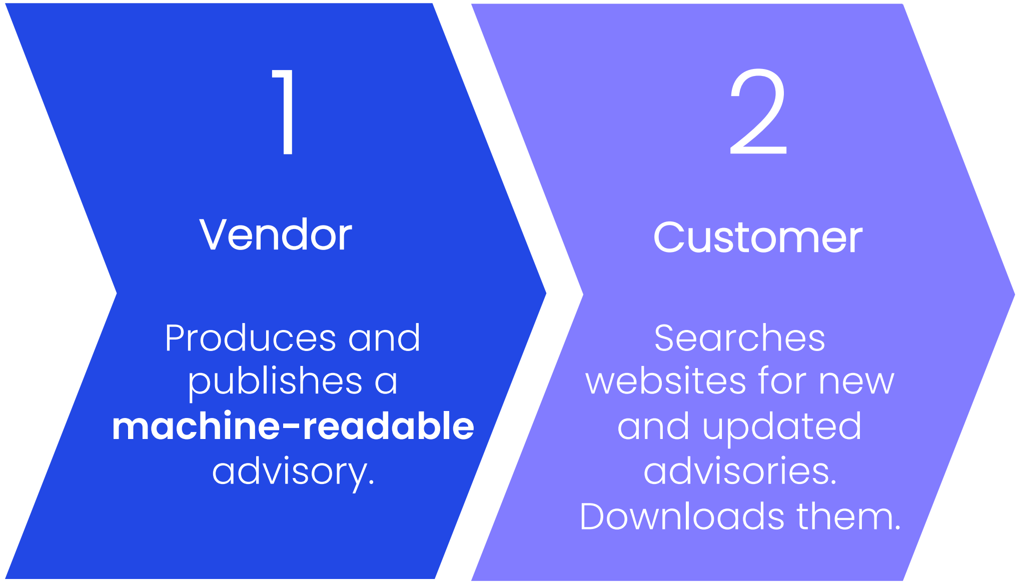
🟧 high

🟨 medium

🟩 low

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

Process with CSAF



1

Vendor

Produces and publishes a **machine-readable** advisory.

2

Customer

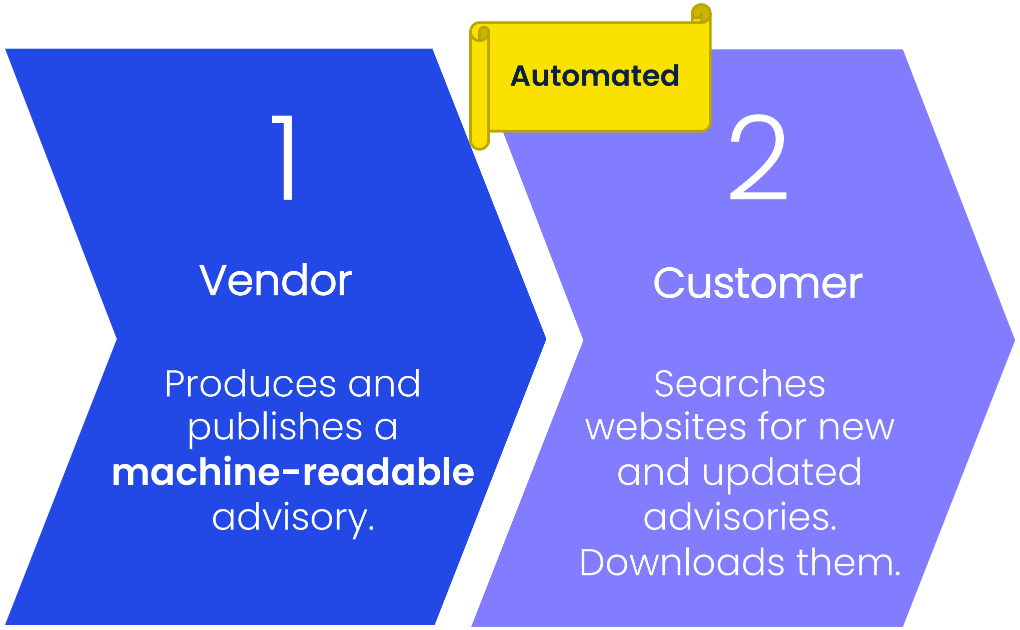
Searches websites for new and updated advisories. Downloads them.

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



Automated

1

Vendor

Produces and publishes a **machine-readable** advisory.

2

Customer

Searches websites for new and updated advisories. Downloads them.

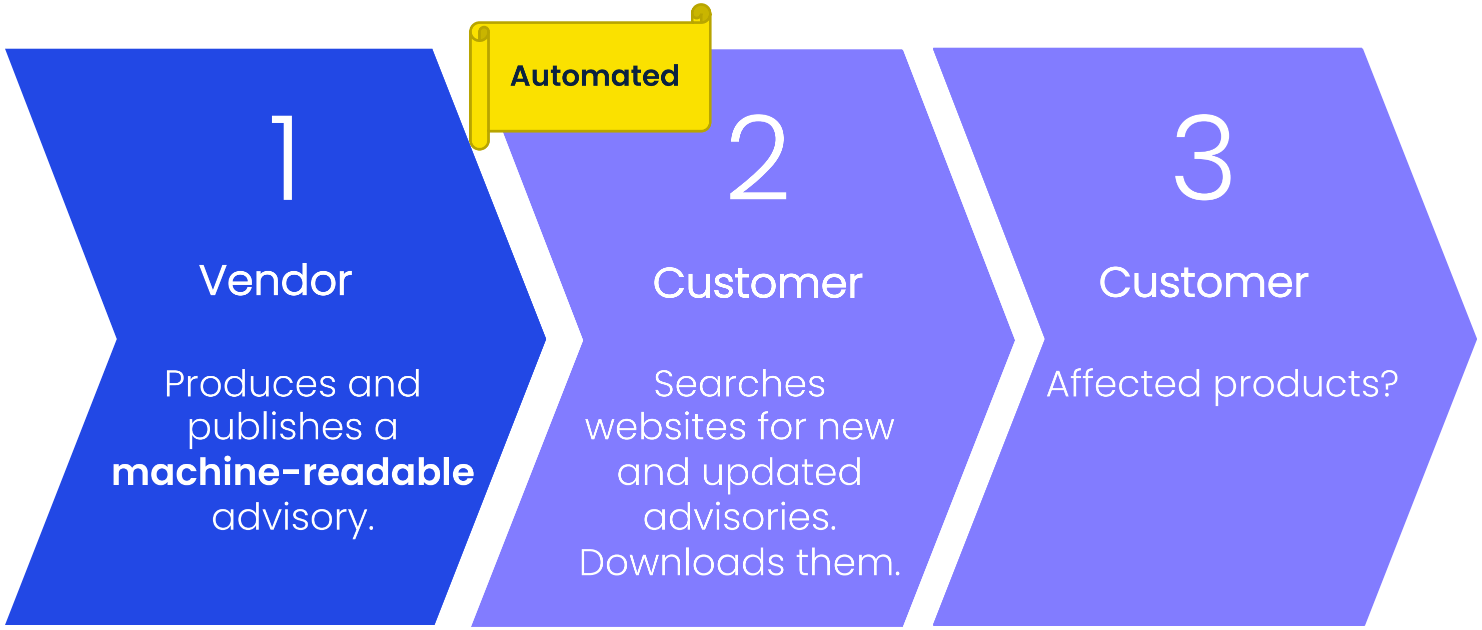
Severity

🟥	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



Automated

1

Vendor

Produces and publishes a **machine-readable** advisory.

2

Customer

Searches websites for new and updated advisories. Downloads them.

3

Customer

Affected products?

Severity

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

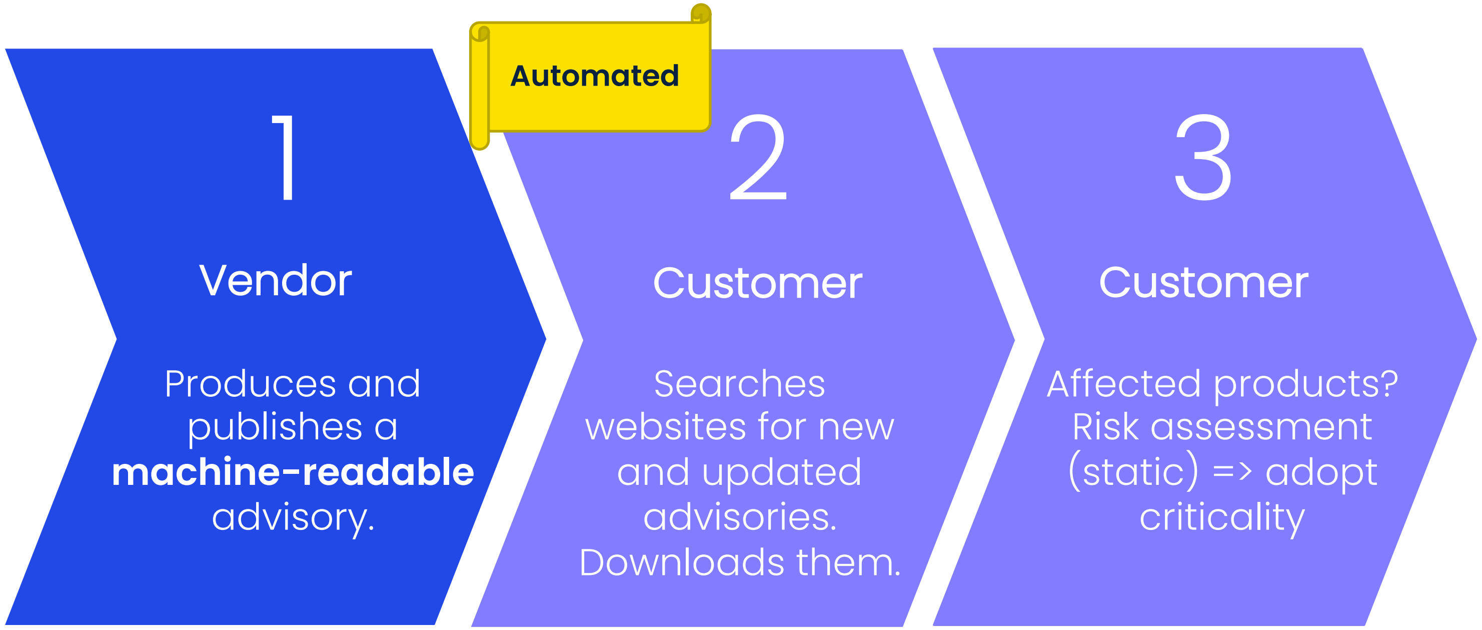
🟩 1	🟧 6	🟩 11
🟧 2	🟧 7	🟧 12
🟧 3	🟨 8	🟥 13
🟩 4	🟧 9	🟨 14
🟥 5	🟥 10	🟧 15

🟩 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

OASIS OPEN

Process with CSAF



1

Vendor

Produces and publishes a **machine-readable** advisory.

2

Customer

Searches websites for new and updated advisories. Downloads them.

3

Customer

Affected products? Risk assessment (static) => adopt criticality

Severity

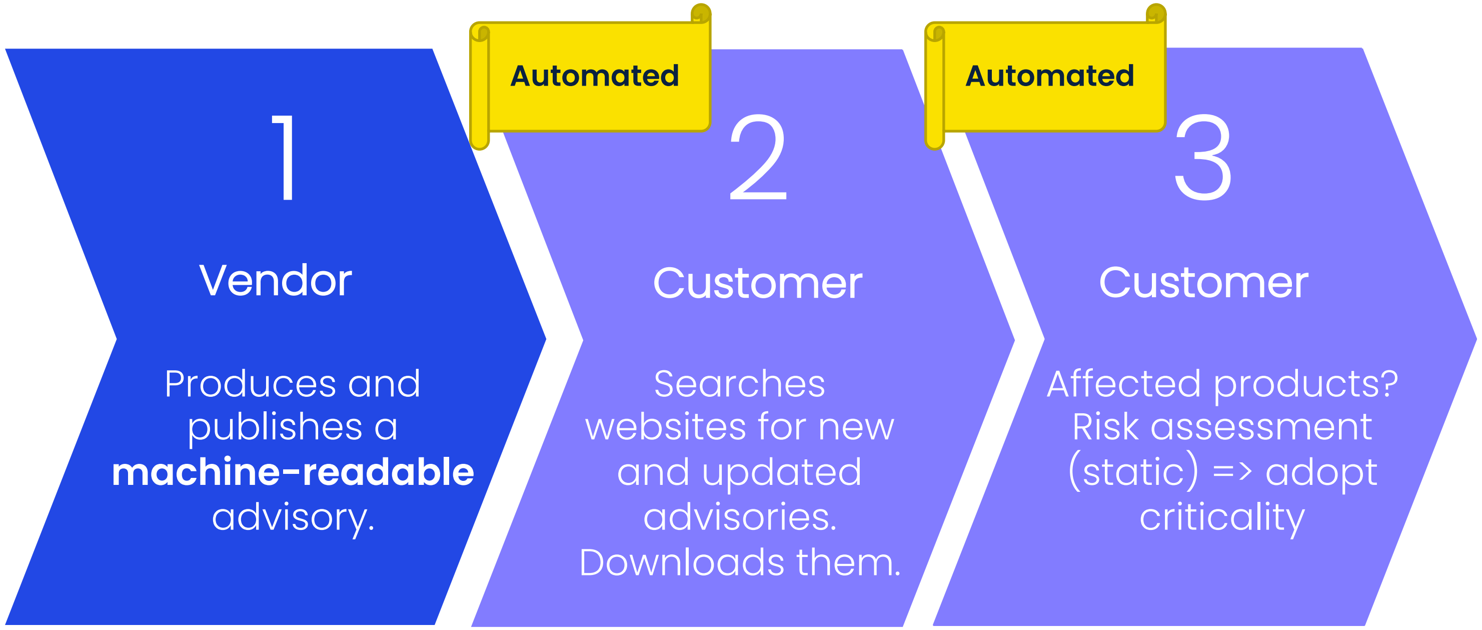
- 🟥 critical
- 🟧 high
- 🟨 medium
- 🟩 low

🟩 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

Process with CSAF



1

Vendor

Produces and publishes a **machine-readable** advisory.

2

Customer

Searches websites for new and updated advisories. Downloads them.

3

Customer

Affected products? Risk assessment (static) => adopt criticality

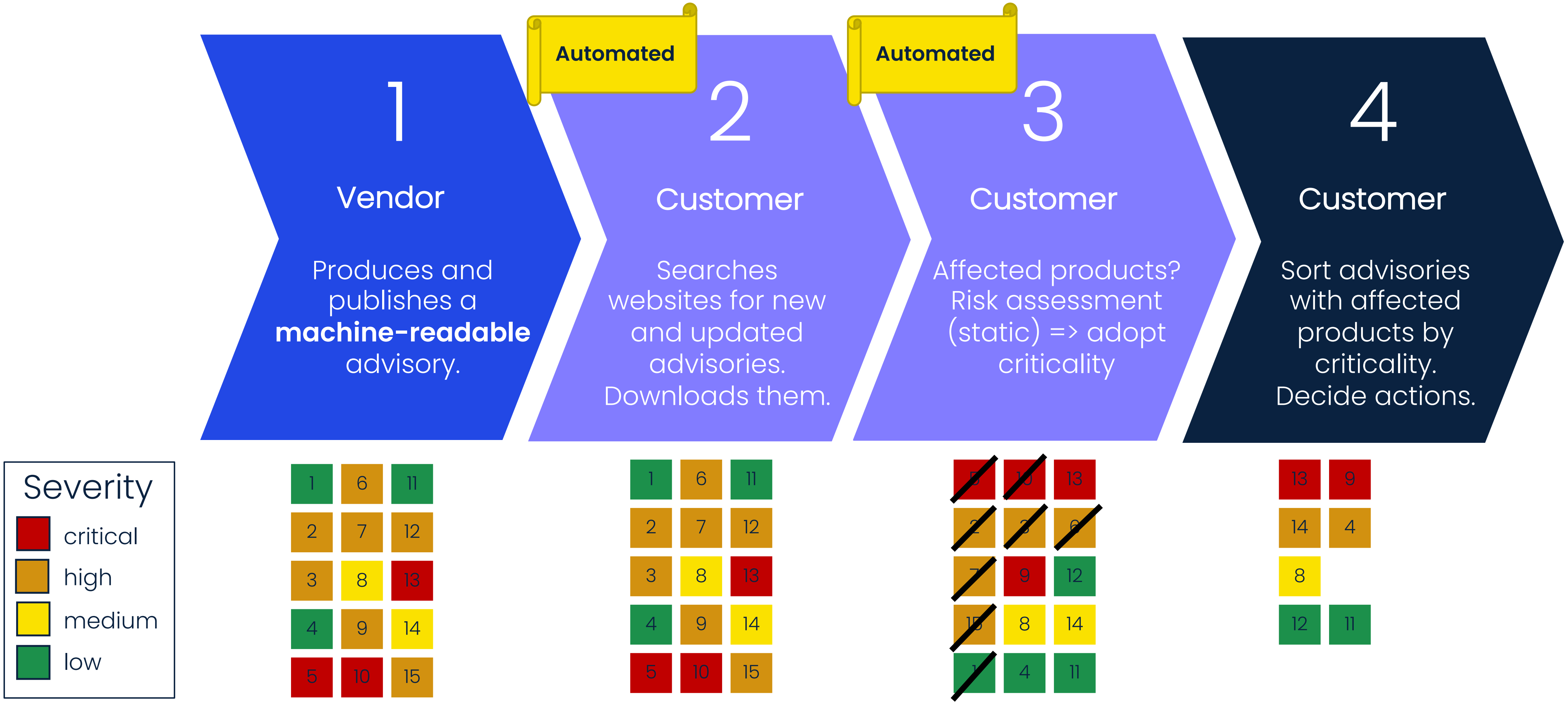
Severity	
🟥	critical
🟧	high
🟨	medium
🟩	low

🟩 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

Process with CSAF



Automated

Automated

1

Vendor

Produces and publishes a **machine-readable** advisory.

2

Customer

Searches websites for new and updated advisories. Downloads them.

3

Customer

Affected products? Risk assessment (static) => adopt criticality

4

Customer

Sort advisories with affected products by criticality. Decide actions.

Severity

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

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

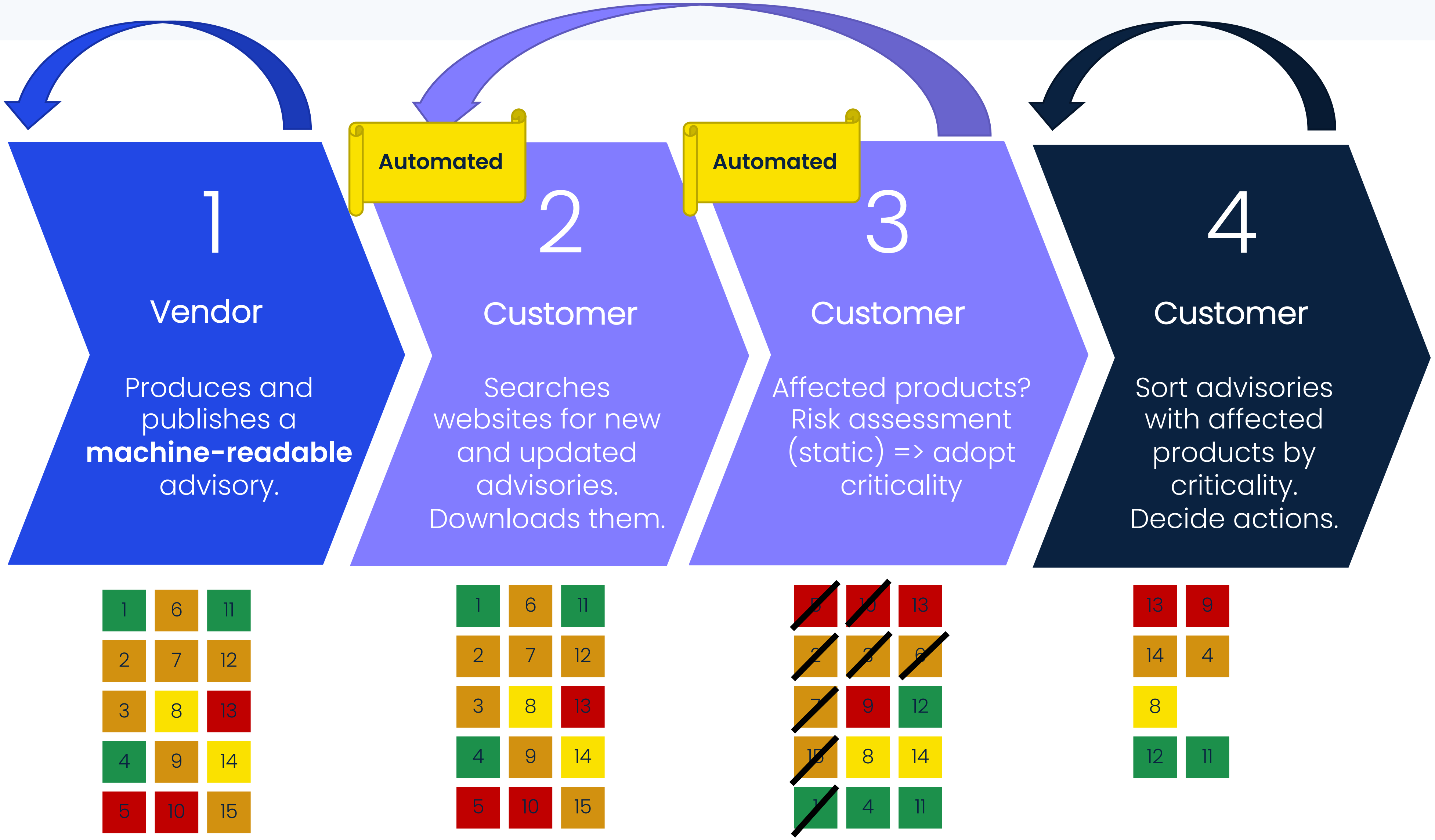
🟩 1	🟧 6	🟩 11
🟧 2	🟧 7	🟧 12
🟧 3	🟨 8	🟥 13
🟩 4	🟧 9	🟨 14
🟥 5	🟥 10	🟧 15

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

🟥 13	🟥 9
🟧 14	🟧 4
🟨 8	
🟩 12	🟩 11

OASIS OPEN

Process with CSAF



Automated

Automated

1

Vendor

Produces and publishes a **machine-readable** advisory.

2

Customer

Searches websites for new and updated advisories. Downloads them.

3

Customer

Affected products? Risk assessment (static) => adopt criticality

4

Customer

Sort advisories with affected products by criticality. Decide actions.

Severity

🟥 critical

🟧 high

🟨 medium

🟩 low

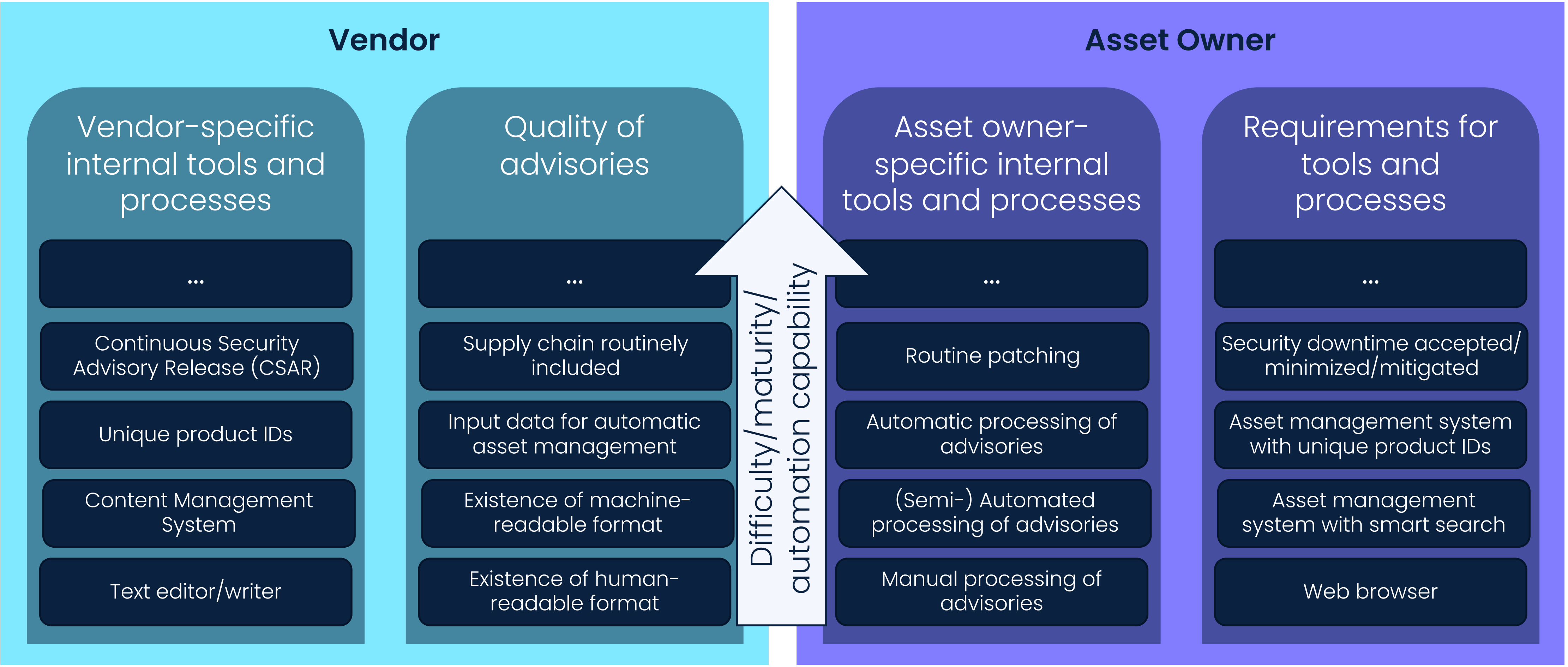
Benefits for Asset Owners

- 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

Requirements for Asset Owners

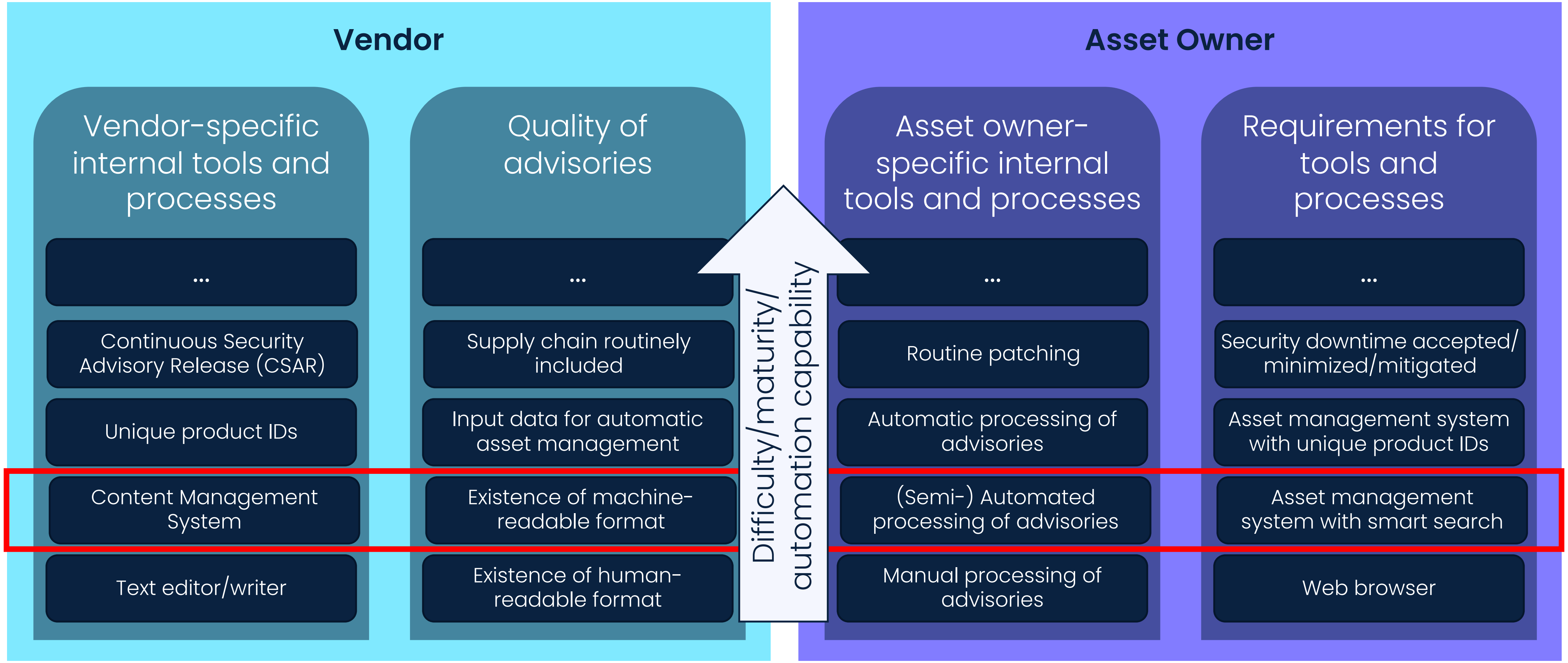
- Machine-readable asset inventory
- Request advisories in CSAF from vendors
- Connection between both to leverage full potential

Two Sides of the Same Coin – Different Maturity Stages



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		Routine patching	Security downtime accepted/ minimized/mitigated
Unique product IDs	Input data for automatic asset management	Difficulty/maturity/ automation capability	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 system with smart search
Text editor/writer	Existence of human-readable format		Manual processing of advisories	Web browser

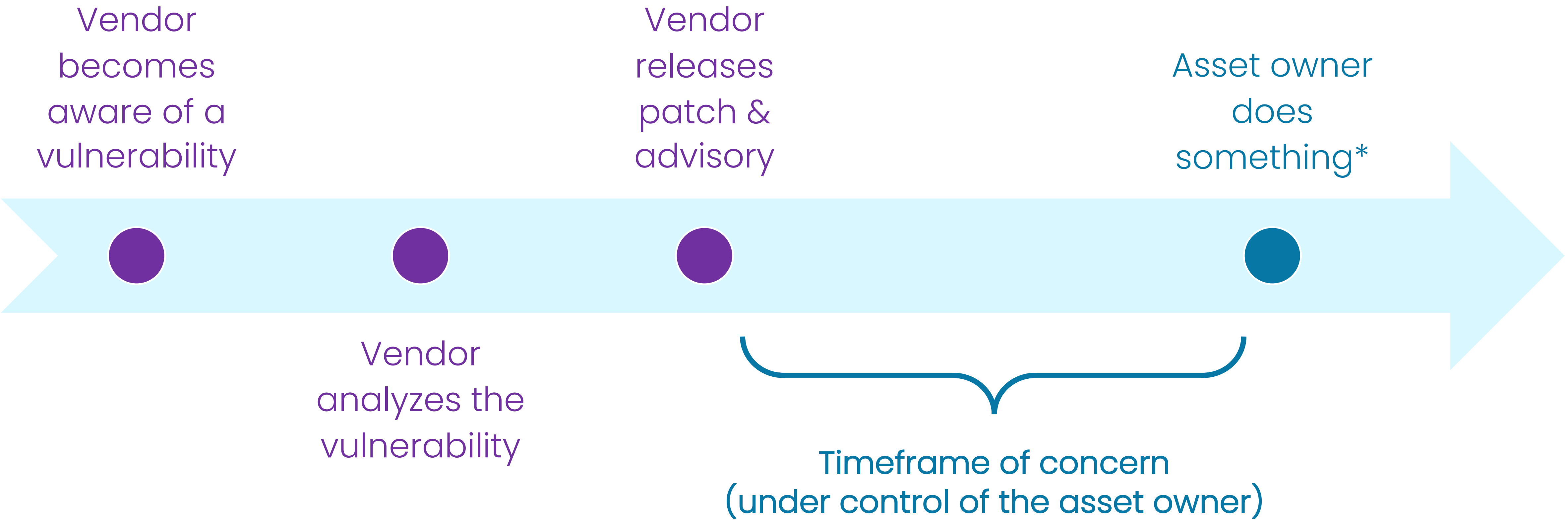
Next Step: Reach Stage 2 Across Parties



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	Routine 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 system with smart search
Text editor/writer	Existence of human-readable format	Manual processing of advisories	Web browser

Supply chain

Timeframe of concern



Vendor becomes aware of a vulnerability

Vendor analyzes the vulnerability

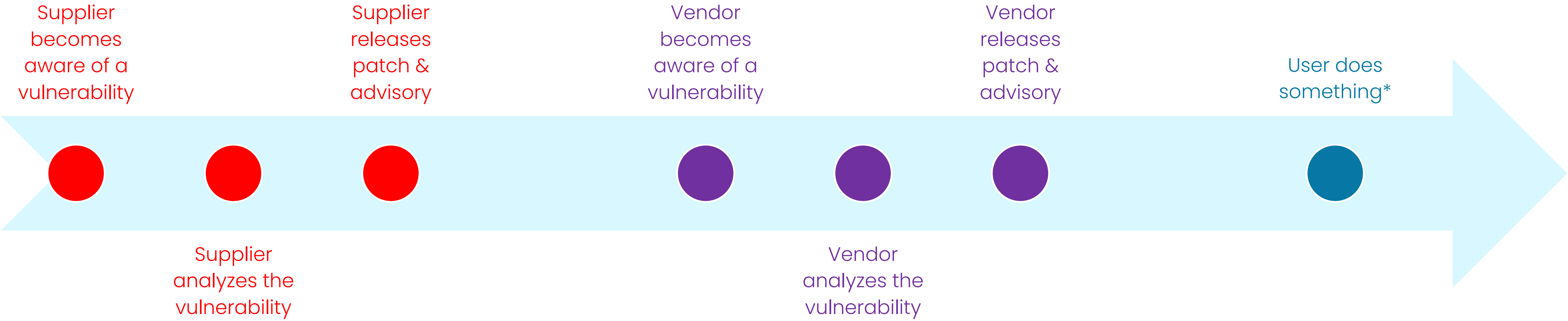
Vendor releases patch & advisory

Asset owner does something*

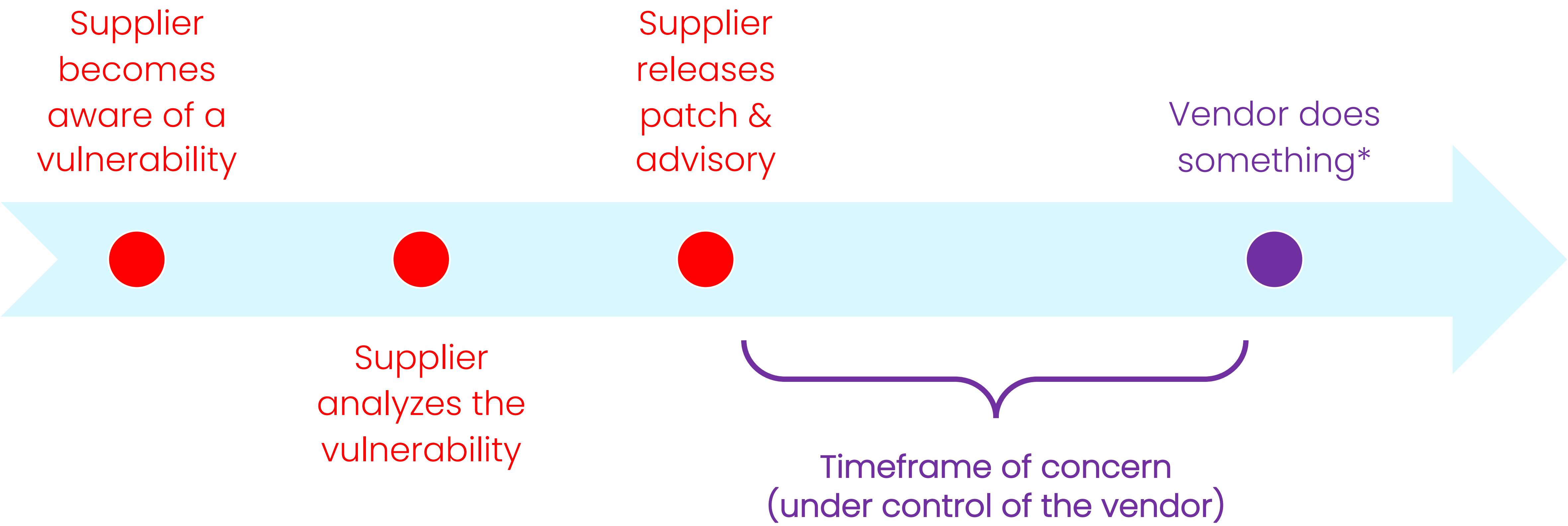
Timeframe of concern
(under control of the asset owner)

* Patch, mitigate risk, or actively accept risk

Supply chain


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

(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)

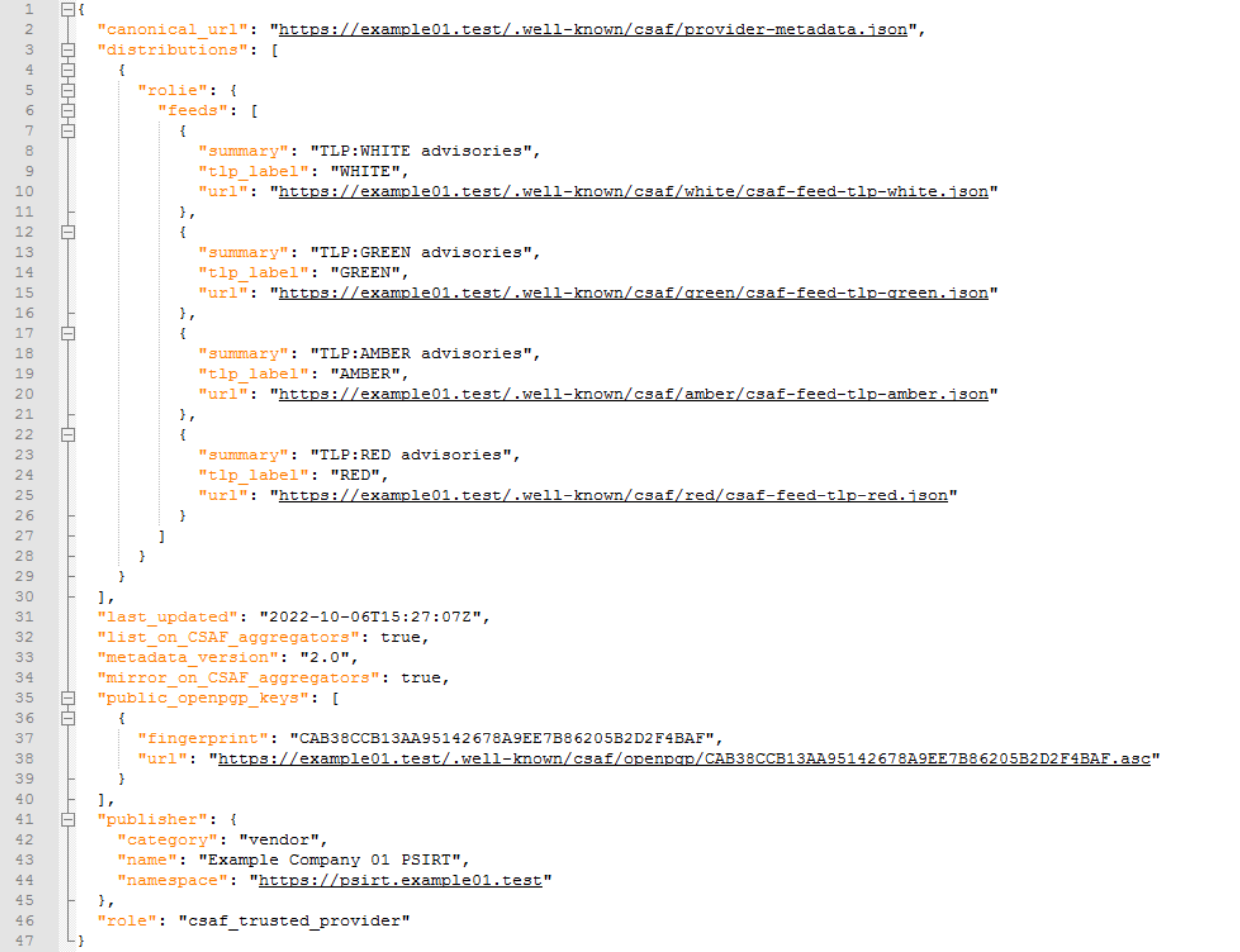
* Patch, mitigate risk, or actively accept risk

Distribution of CSAF

Where to find CSAF documents?

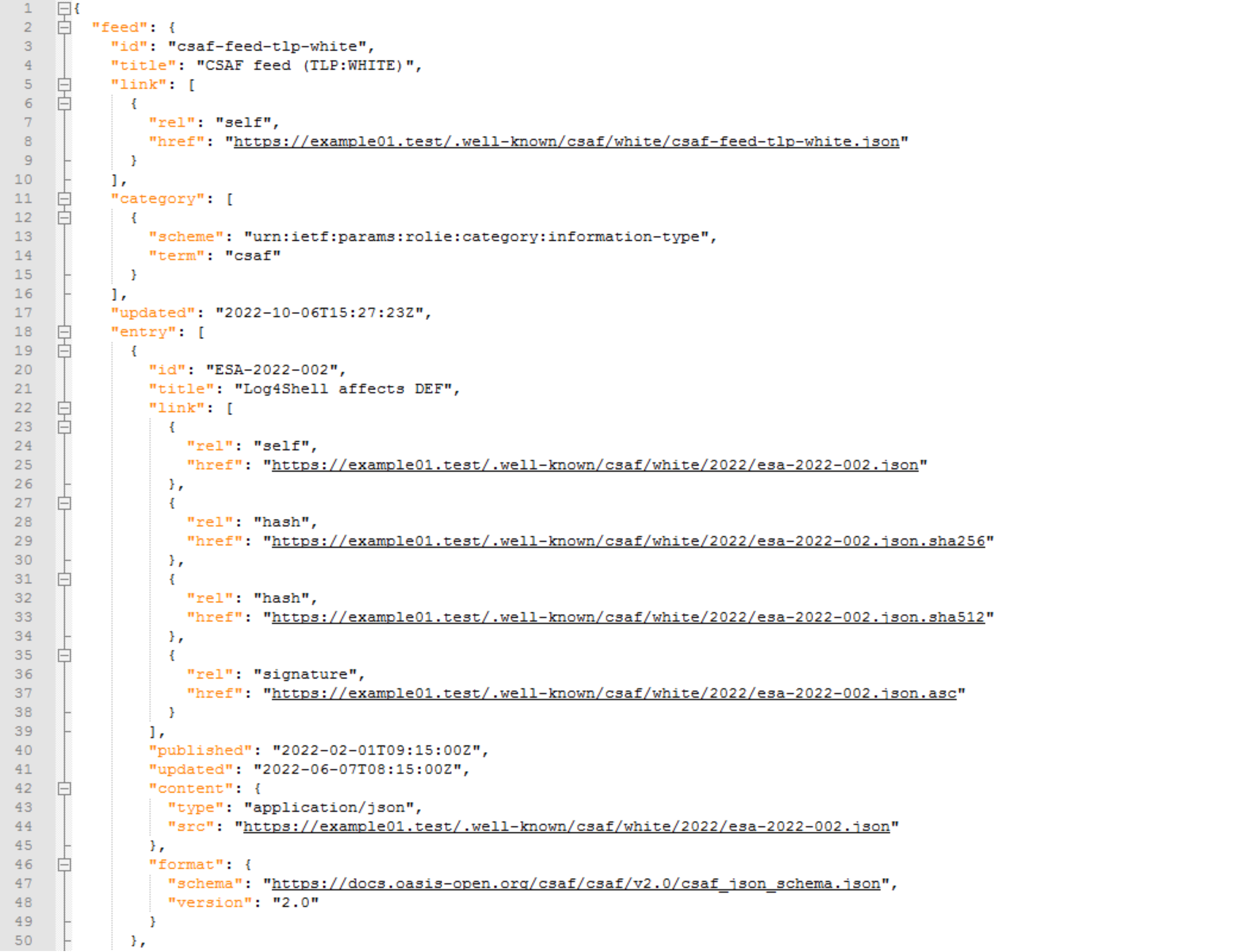
✓ Valid CSAF documents ✓ File name restrictions ✓ TLS enforced ✓ TLP:WHITE freely accessible	CSAF publisher
✓ Well-defined URL / security.txt / DNS => provider-metadata.json ✓ List of advisories and latest changes and Fixed folder structure ✓ or ROLIE feeds ✓ Restriction on >=TLP:AMBER ✓ All requirements 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



```
{
  "canonical_url": "https://example01.test/.well-known/csaf/provider-metadata.json",
  "distributions": [
    {
      "rolie": {
        "feeds": [
          {
            "summary": "TLP:WHITE advisories",
            "tlp_label": "WHITE",
            "url": "https://example01.test/.well-known/csaf/white/csaf-feed-tlp-white.json"
          },
          {
            "summary": "TLP:GREEN advisories",
            "tlp_label": "GREEN",
            "url": "https://example01.test/.well-known/csaf/green/csaf-feed-tlp-green.json"
          },
          {
            "summary": "TLP:AMBER advisories",
            "tlp_label": "AMBER",
            "url": "https://example01.test/.well-known/csaf/amber/csaf-feed-tlp-amber.json"
          },
          {
            "summary": "TLP:RED advisories",
            "tlp_label": "RED",
            "url": "https://example01.test/.well-known/csaf/red/csaf-feed-tlp-red.json"
          }
        ]
      }
    }
  ],
  "last_updated": "2022-10-06T15:27:07Z",
  "list_on_CSAF_aggregators": true,
  "metadata_version": "2.0",
  "mirror_on_CSAF_aggregators": true,
  "public_openpgp_keys": [
    {
      "fingerprint": "CAB38CCB13AA95142678A9EE7B86205B2D2F4BAF",
      "url": "https://example01.test/.well-known/csaf/openpgp/CAB38CCB13AA95142678A9EE7B86205B2D2F4BAF.asc"
    }
  ],
  "publisher": {
    "category": "vendor",
    "name": "Example Company 01 PSIRT",
    "namespace": "https://psirt.example01.test"
  },
  "role": "csaf_trusted_provider"
}
```

Example: ROLIE feed



```
{
  "feed": {
    "id": "csaf-feed-tlp-white",
    "title": "CSAF feed (TLP:WHITE)",
    "link": [
      {
        "rel": "self",
        "href": "https://example01.test/.well-known/csaf/white/csaf-feed-tlp-white.json"
      }
    ],
    "category": [
      {
        "scheme": "urn:ietf:params:rolie:category:information-type",
        "term": "csaf"
      }
    ],
    "updated": "2022-10-06T15:27:23Z",
    "entry": [
      {
        "id": "ESA-2022-002",
        "title": "Log4Shell affects DEF",
        "link": [
          {
            "rel": "self",
            "href": "https://example01.test/.well-known/csaf/white/2022/esa-2022-002.json"
          },
          {
            "rel": "hash",
            "href": "https://example01.test/.well-known/csaf/white/2022/esa-2022-002.json.sha256"
          },
          {
            "rel": "hash",
            "href": "https://example01.test/.well-known/csaf/white/2022/esa-2022-002.json.sha512"
          },
          {
            "rel": "signature",
            "href": "https://example01.test/.well-known/csaf/white/2022/esa-2022-002.json.asc"
          }
        ],
        "published": "2022-02-01T09:15:00Z",
        "updated": "2022-06-07T08:15:00Z",
        "content": {
          "type": "application/json",
          "src": "https://example01.test/.well-known/csaf/white/2022/esa-2022-002.json"
        },
        "format": {
          "schema": "https://docs.oasis-open.org/csaf/csaf/v2.0/csaf_json_schema.json",
          "version": "2.0"
        }
      },
```

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)

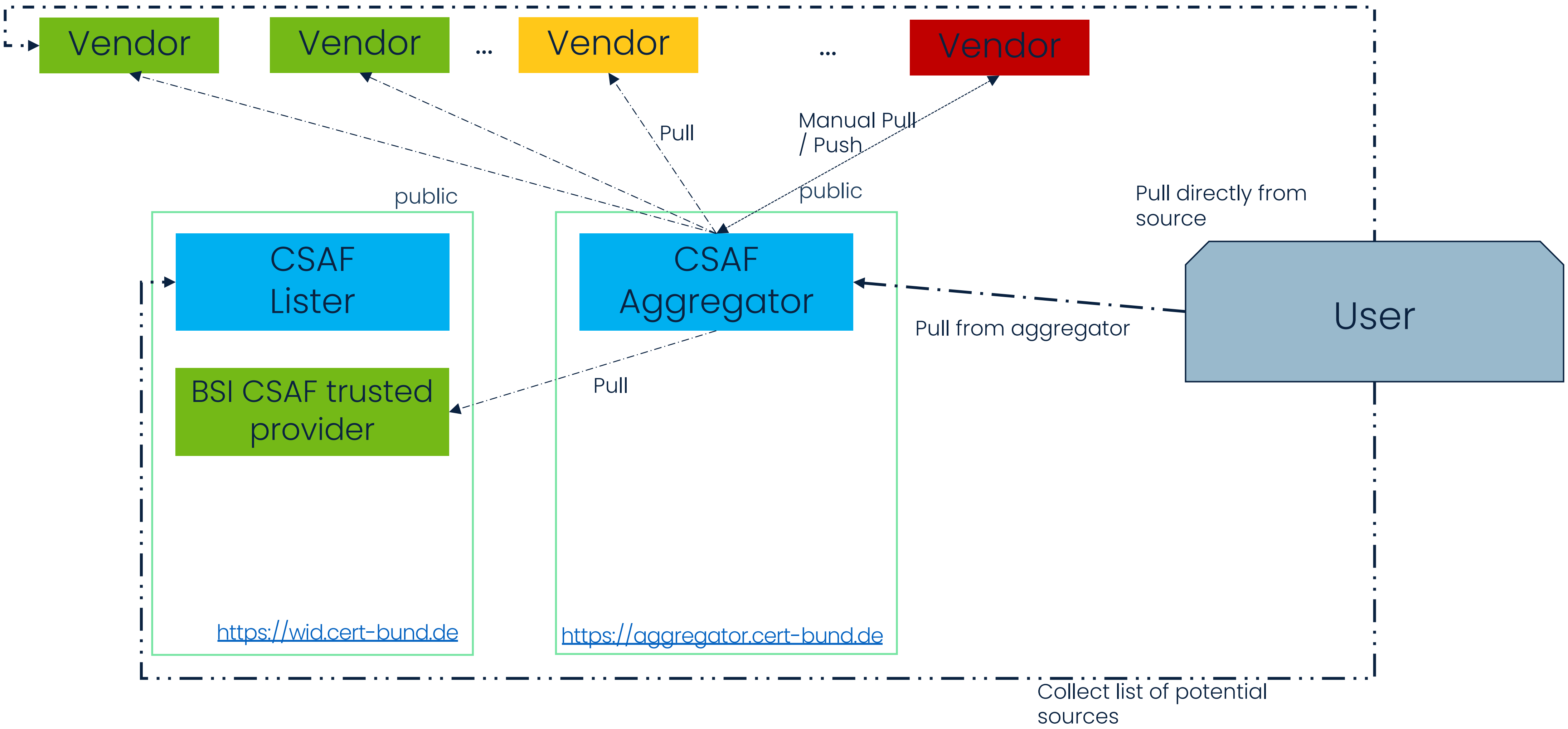
- First one available at https://wid.cert-bund.de

CSAF Aggregator

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

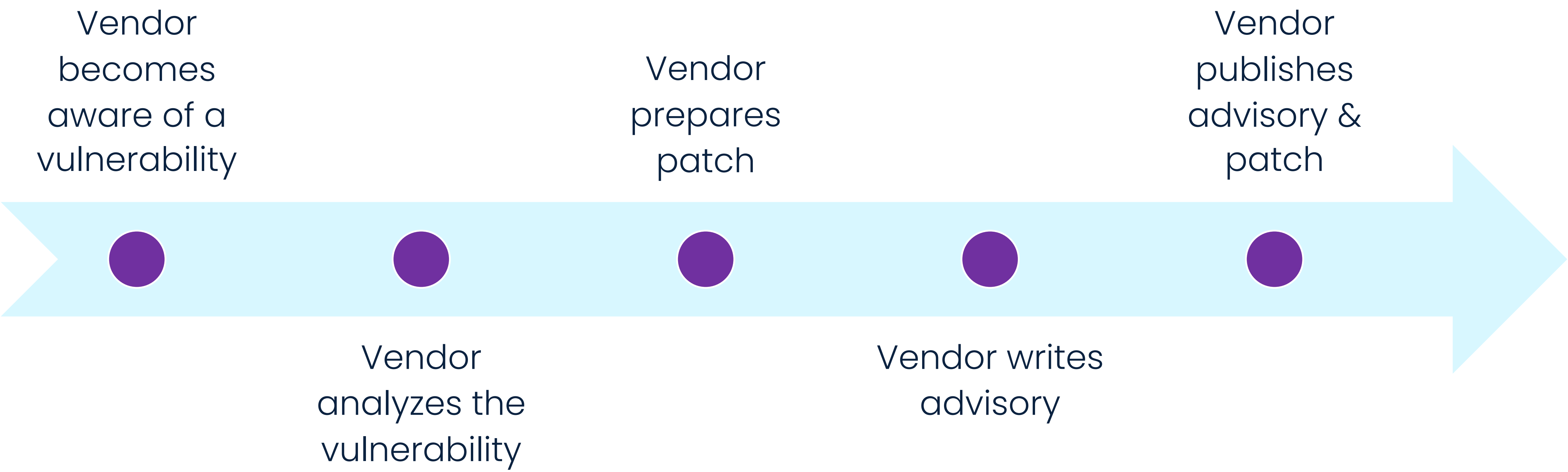
- First one available at https://aggregator.cert-bund.de

Ecosystem


Vendor
Vendor
...
Vendor
...
Vendor
Pull
Manual Pull / Push
public
public
Pull directly from source
CSAF Lister
CSAF Aggregator
User
Pull from aggregator
BSI CSAF trusted provider
Pull
https://wid.cert-bund.de
https://aggregator.cert-bund.de
Collect list of potential sources

Tools

Vendor



Vendor becomes aware of a vulnerability

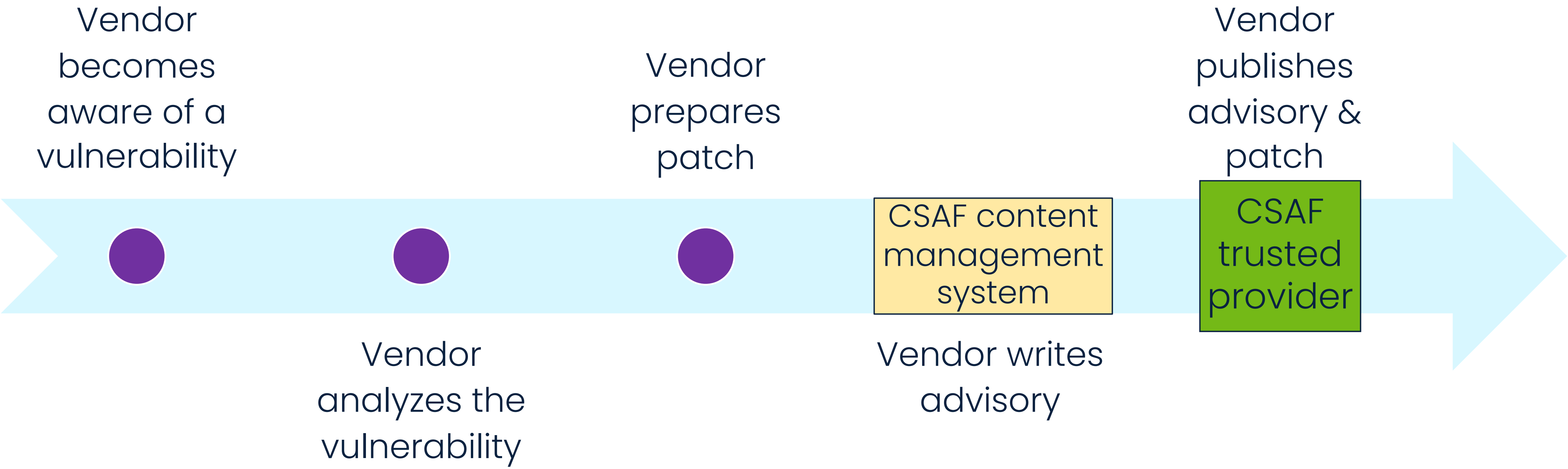
Vendor analyzes the vulnerability

Vendor prepares patch

Vendor writes advisory

Vendor publishes advisory & patch

Vendor



Vendor becomes aware of a vulnerability

Vendor analyzes the vulnerability

Vendor prepares patch

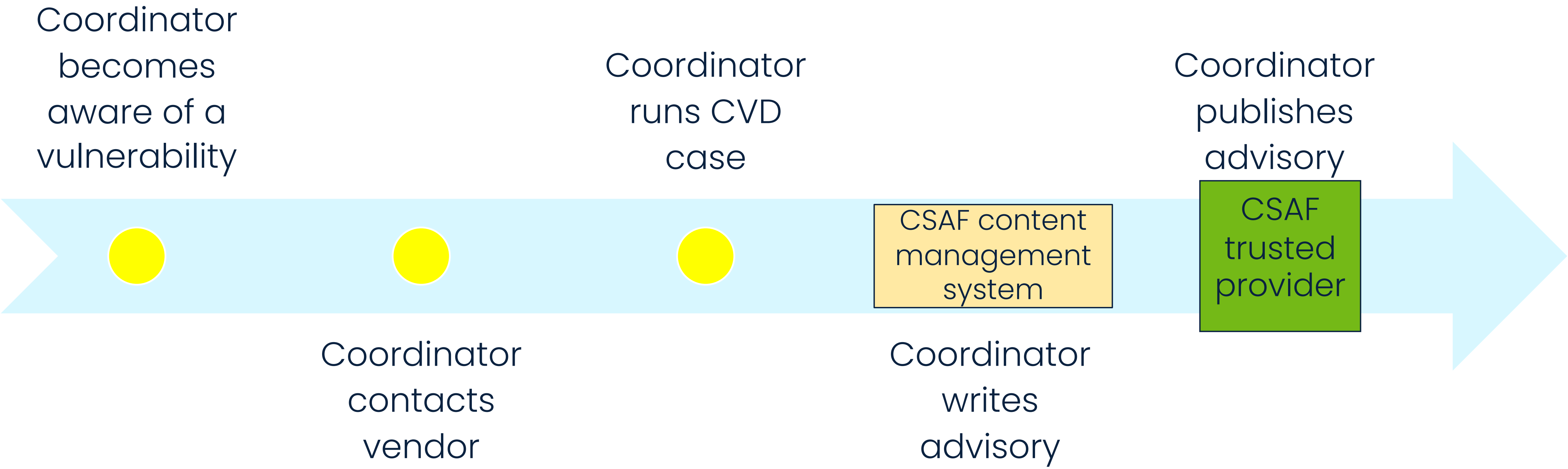
CSAF content management system

Vendor writes advisory

Vendor publishes advisory & patch

CSAF trusted provider

Coordinator (CVD)



Coordinator becomes aware of a vulnerability

Coordinator contacts vendor

Coordinator runs CVD case

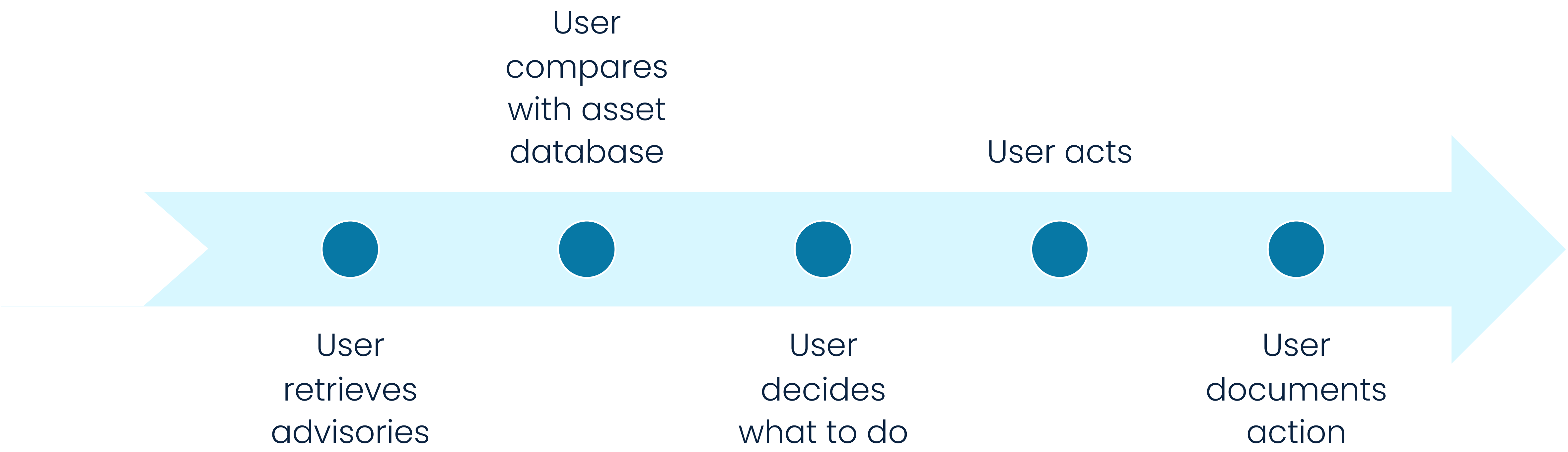
CSAF content management system

Coordinator writes advisory

Coordinator publishes advisory

CSAF trusted provider

User



User retrieves advisories

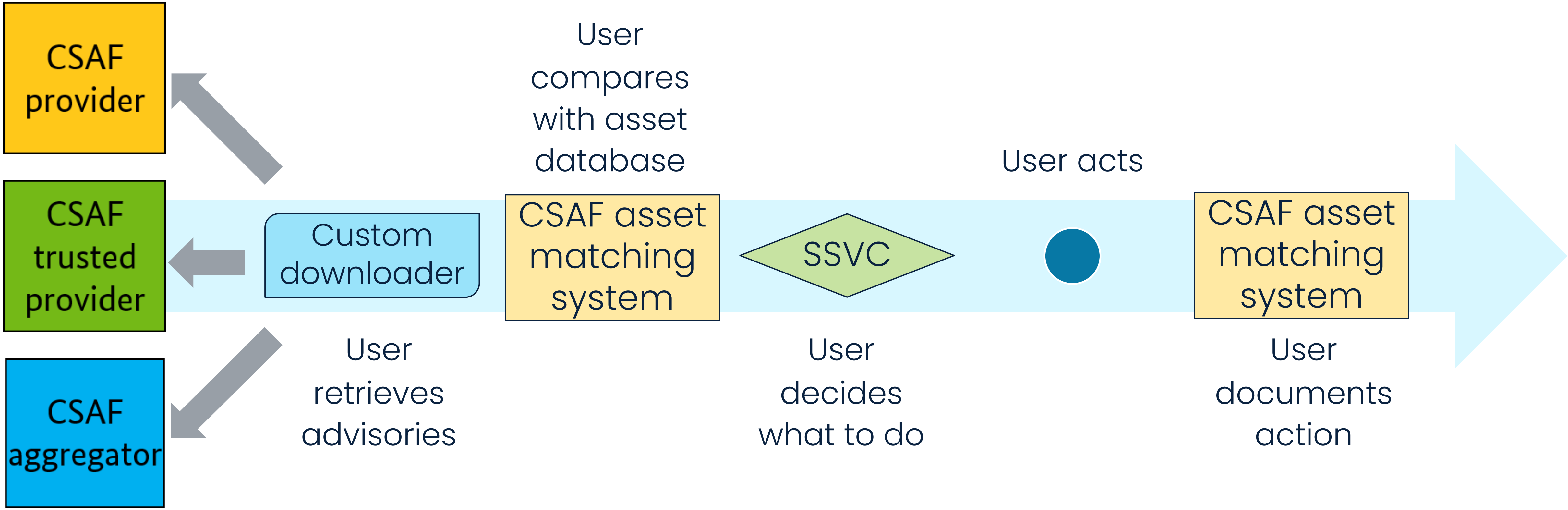
User compares with asset database

User decides what to do

User acts

User documents action

User



CSAF provider

CSAF trusted provider

CSAF aggregator

Custom downloader

User retrieves advisories

User compares with asset database

CSAF asset matching system

SSVC

User decides what to do

User acts

CSAF asset matching system

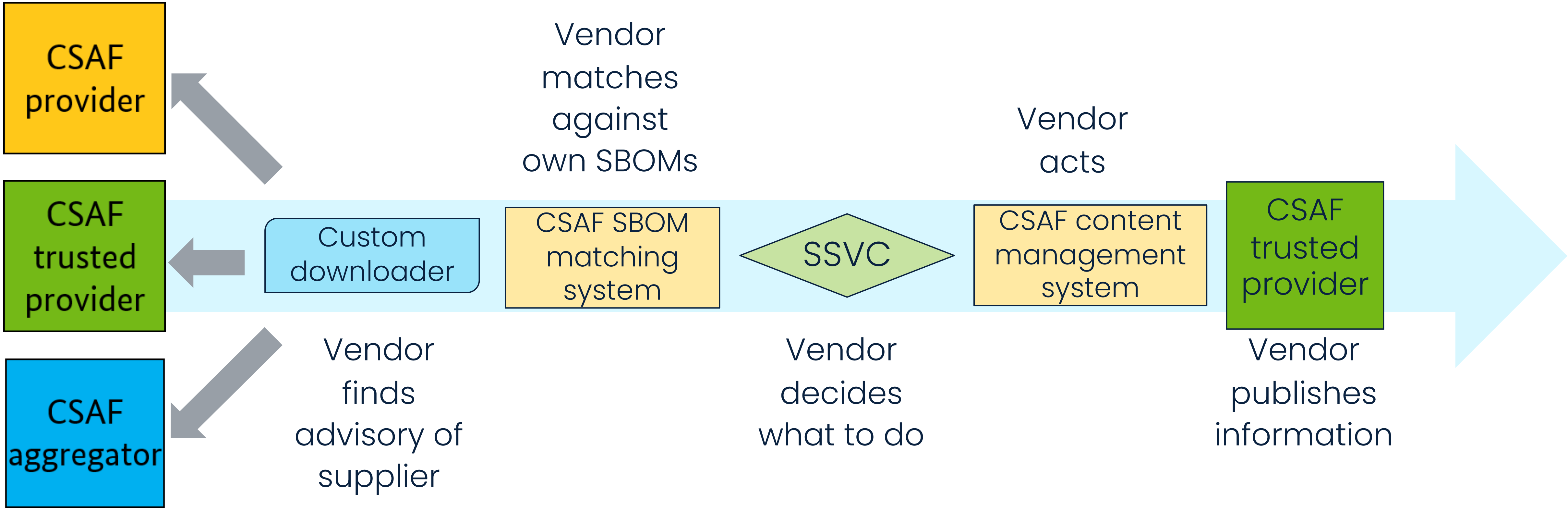
User documents action

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



CSAF provider

CSAF trusted provider

CSAF aggregator

Vendor finds advisory of supplier

Custom downloader

Vendor matches against own SBOMs

CSAF SBOM matching system

Vendor decides what to do

SSVC

Vendor acts

CSAF content management system

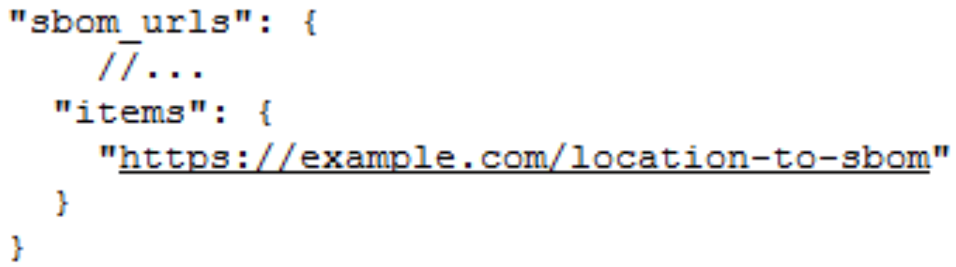
CSAF trusted provider

Vendor publishes information

How to link to an SBOM?

Product identification helpers:

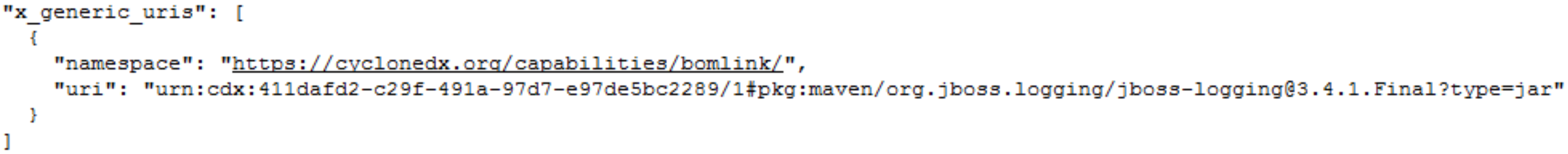
Retrievable SBOM



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

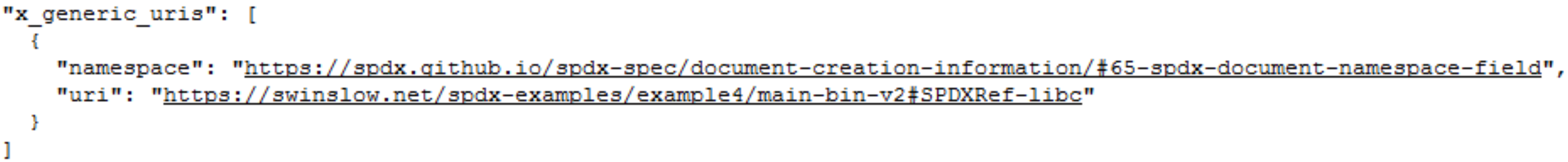
How to link to an SBOM component?

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"
  }
]
```

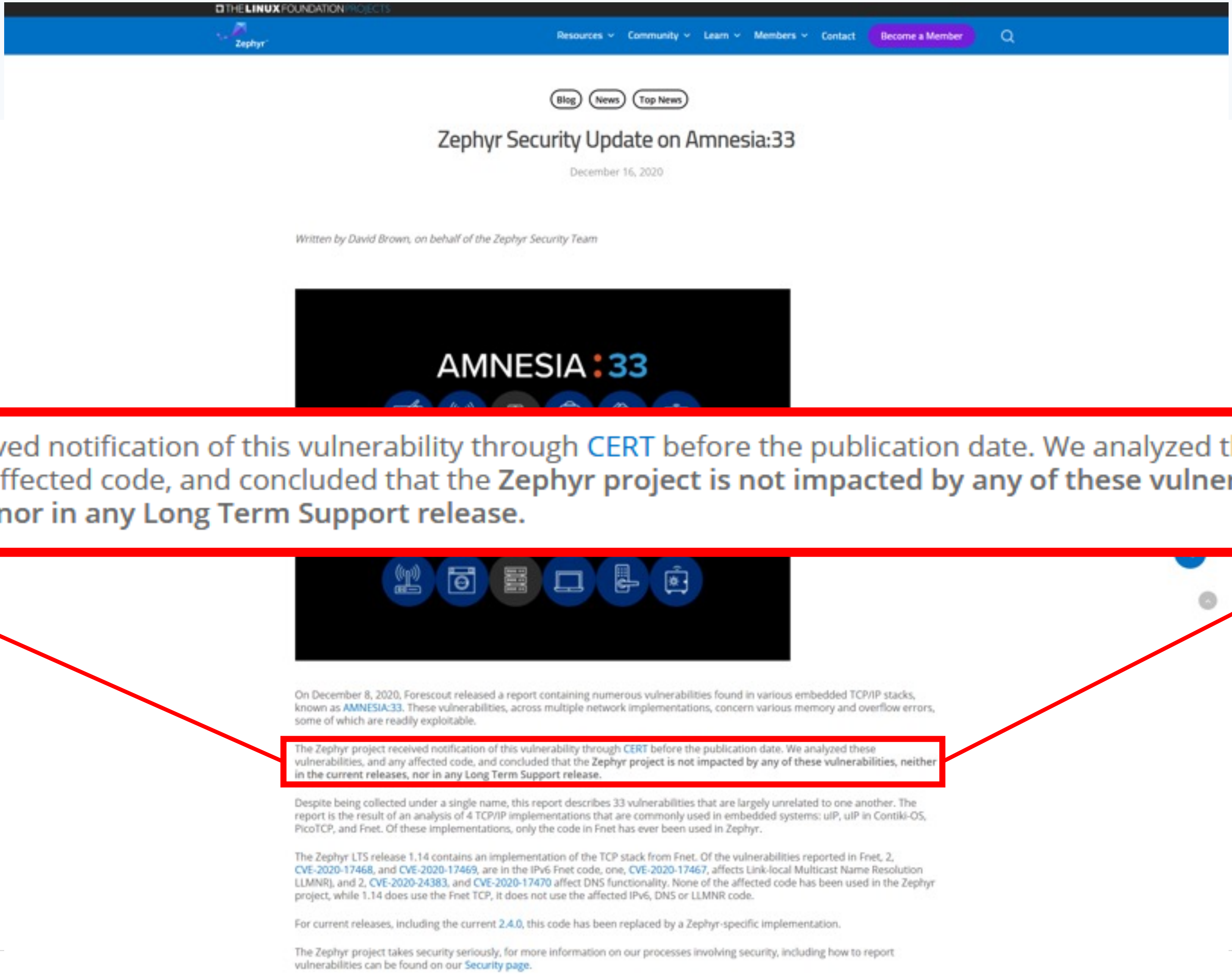
SPDX:



```
"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…

- **V**ulnerability **E**xploitability e**X**change (VEX)
- Communicate product status explicit
- Machine-readable to address scalability



Zephyr Security Update on Amnesia:33

December 16, 2020

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

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.**

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.

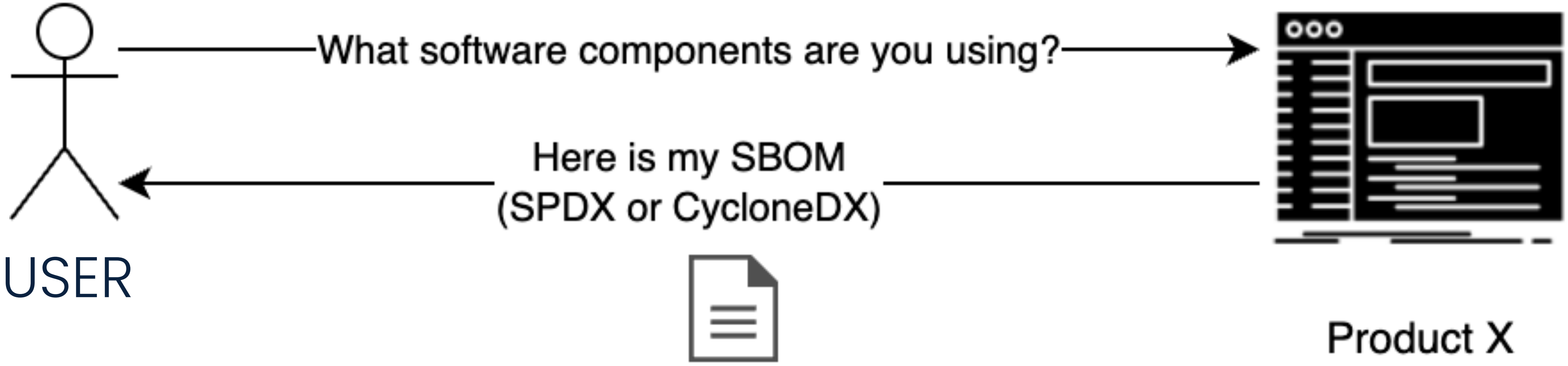
]

VEX is a Profile in CSAF

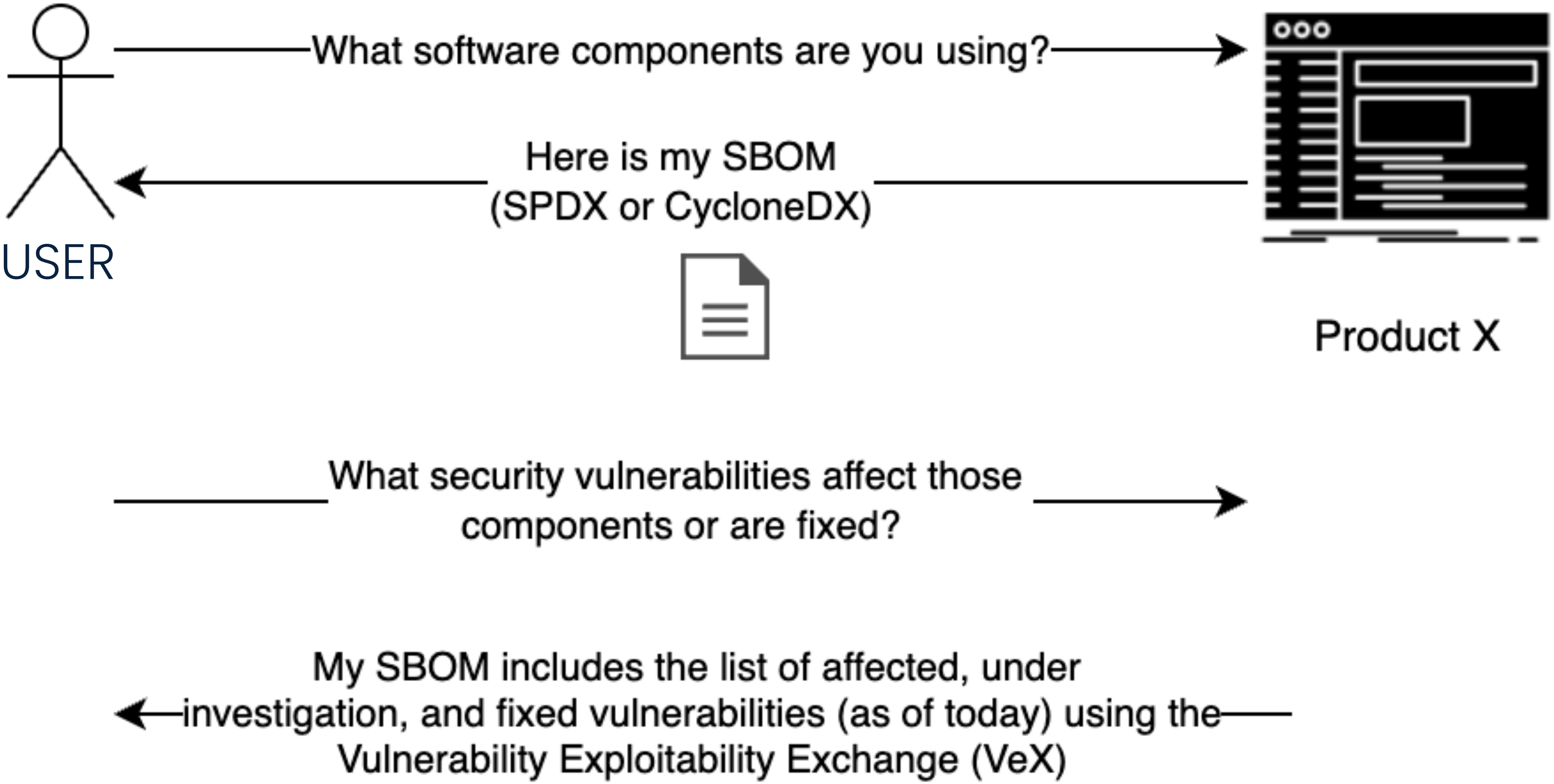
The Vulnerability Exploitability eXchange (VEX) allows a software supplier or other parties to assert the status of specific vulnerabilities in a particular product..

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?

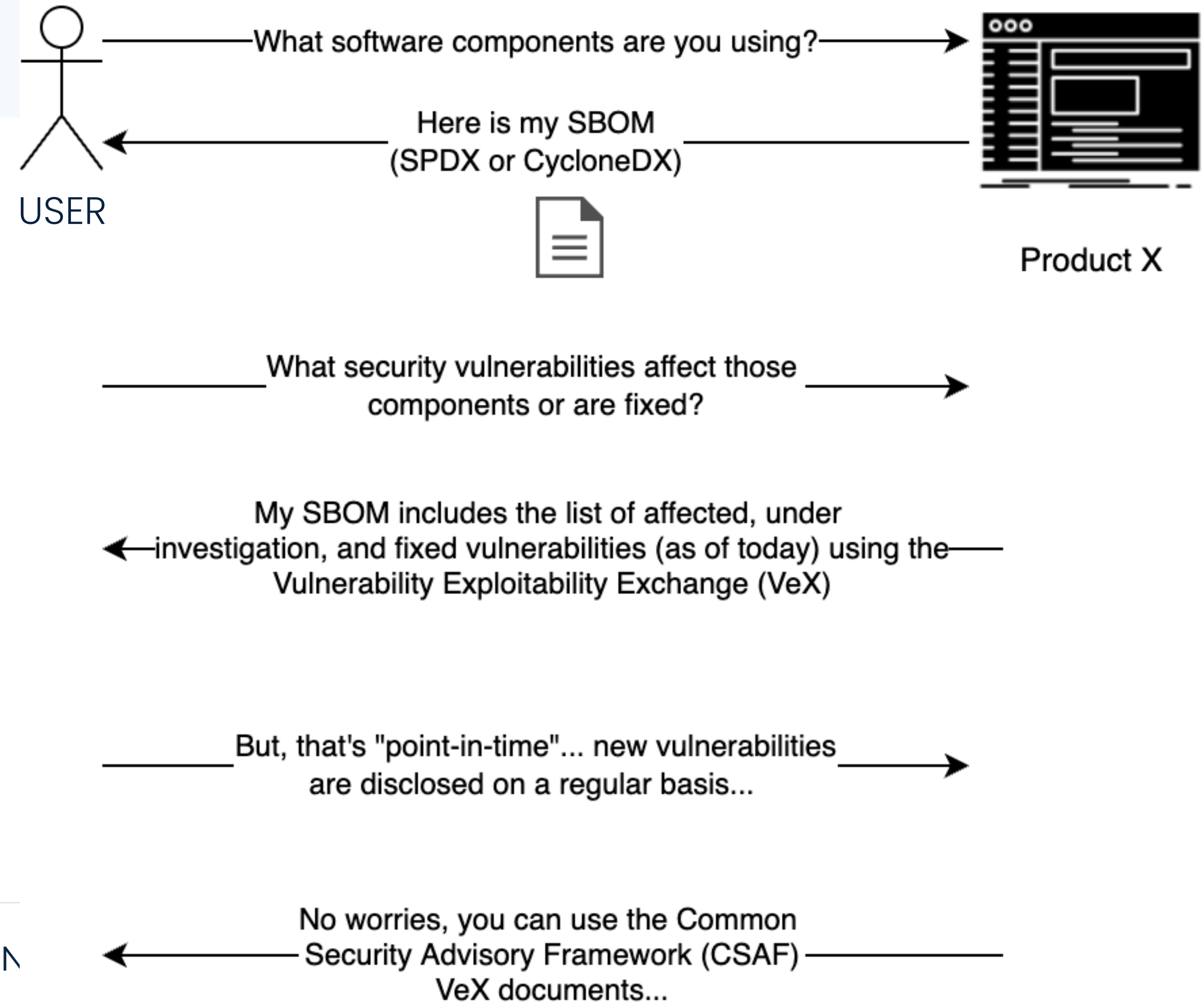


What software components are you using?

Here is my SBOM
(SPDX or CycloneDX)

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)



USER

Product X

What software components are you using?

Here is my SBOM (SPDX or CycloneDX)

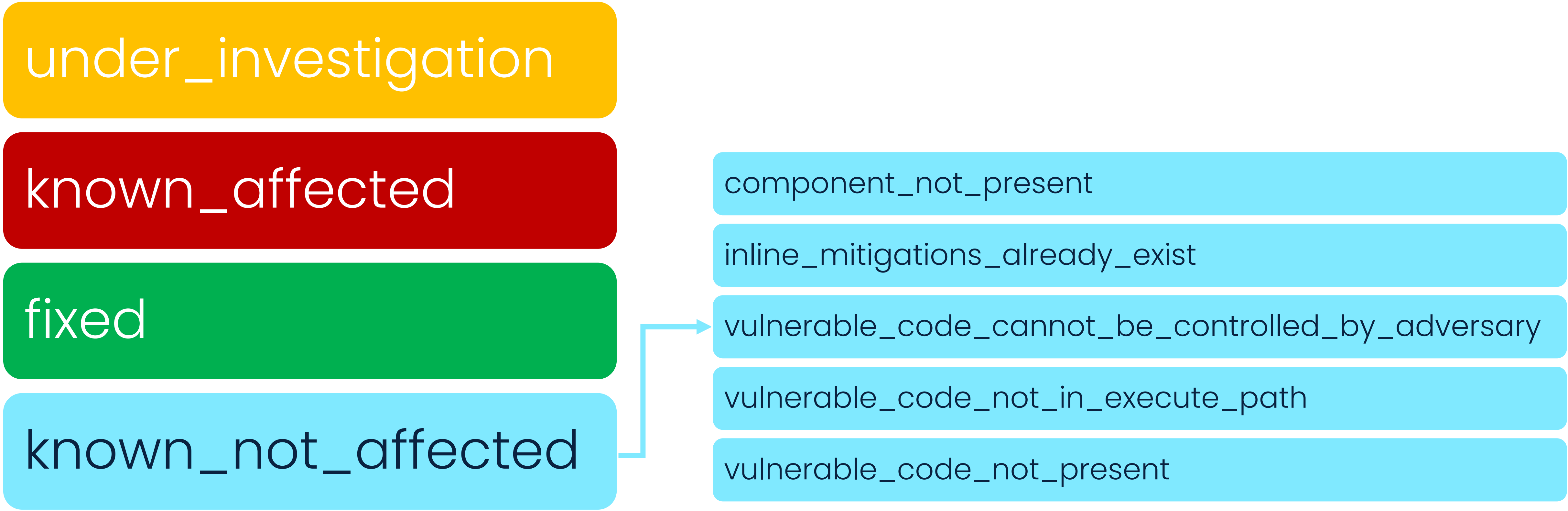
What security vulnerabilities affect those components or are fixed?

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

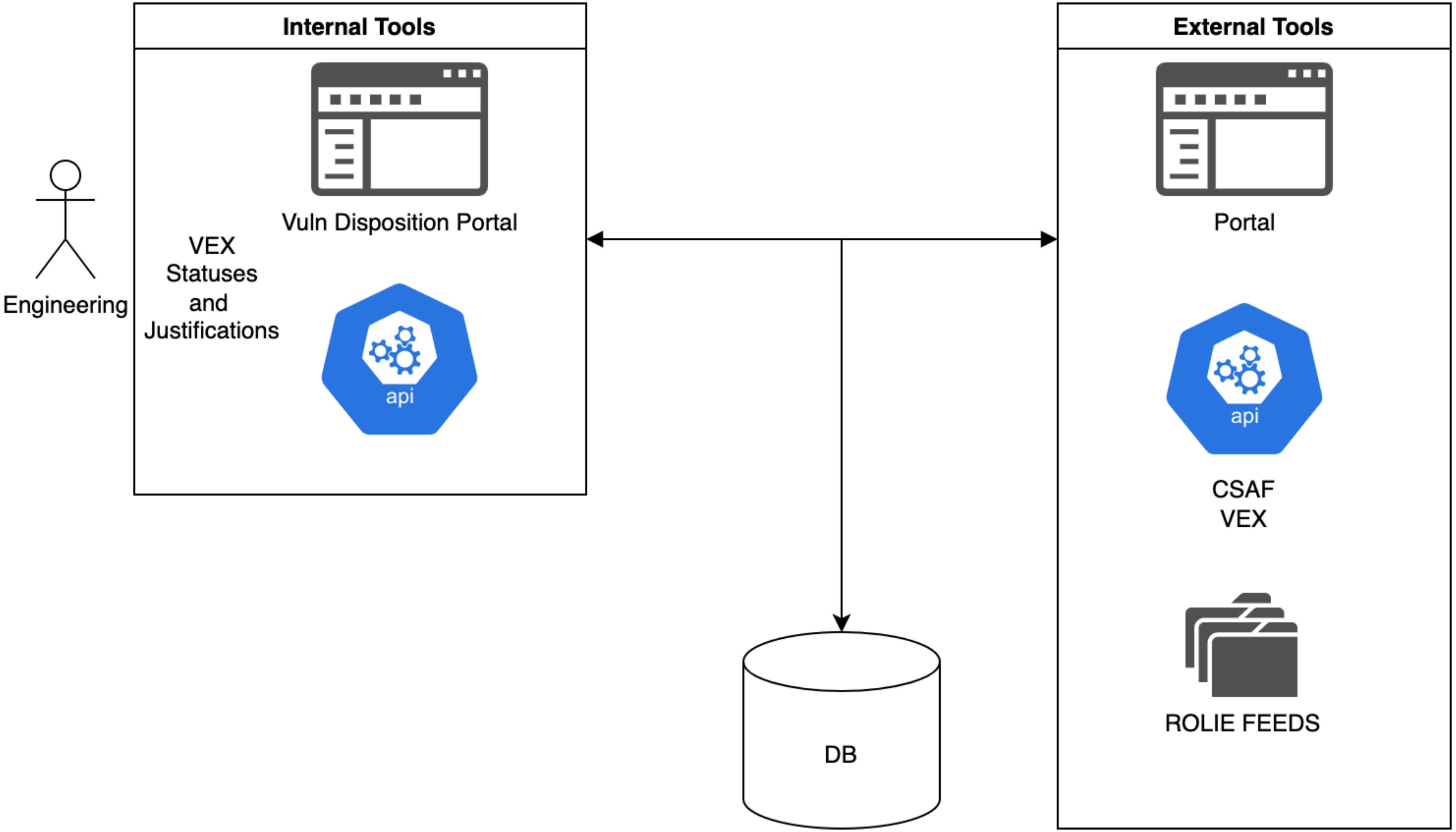
VEX Justifications: https://www.cisa.gov/sites/default/files/publications/VEX_Status_Justification_Jun22.pdf

You Don’t Need an SBOM to VEX

CSAF

OASIS OPEN

Example of "Dynamic Automated" Advisories



- ✓ Scan Reports
- ✓ Rumors
- ✓ Compliance
- ✓ Product Certification

CSAF in operations

Organizations publishing CSAF

CISCO

TIBCO™

SIEMENS

Federal Office
for Information Security

ORACLE

Life Is On | Schneider Electric

Red Hat

Hitachi Energy

ARISTA

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

OASIS OPEN