CSAF

- the Magic Potion for Vulnerability Handling in Industrial Environments

Thomas Pröll and Tobias Limmer

SIEMENS

History of Industrial Environments

Air-gapped

Data exchange with IT

IoT / Cloud-based services

Holes in the perimeter

Long hardware lifetime

High availability

Limited know-how

Integrated security

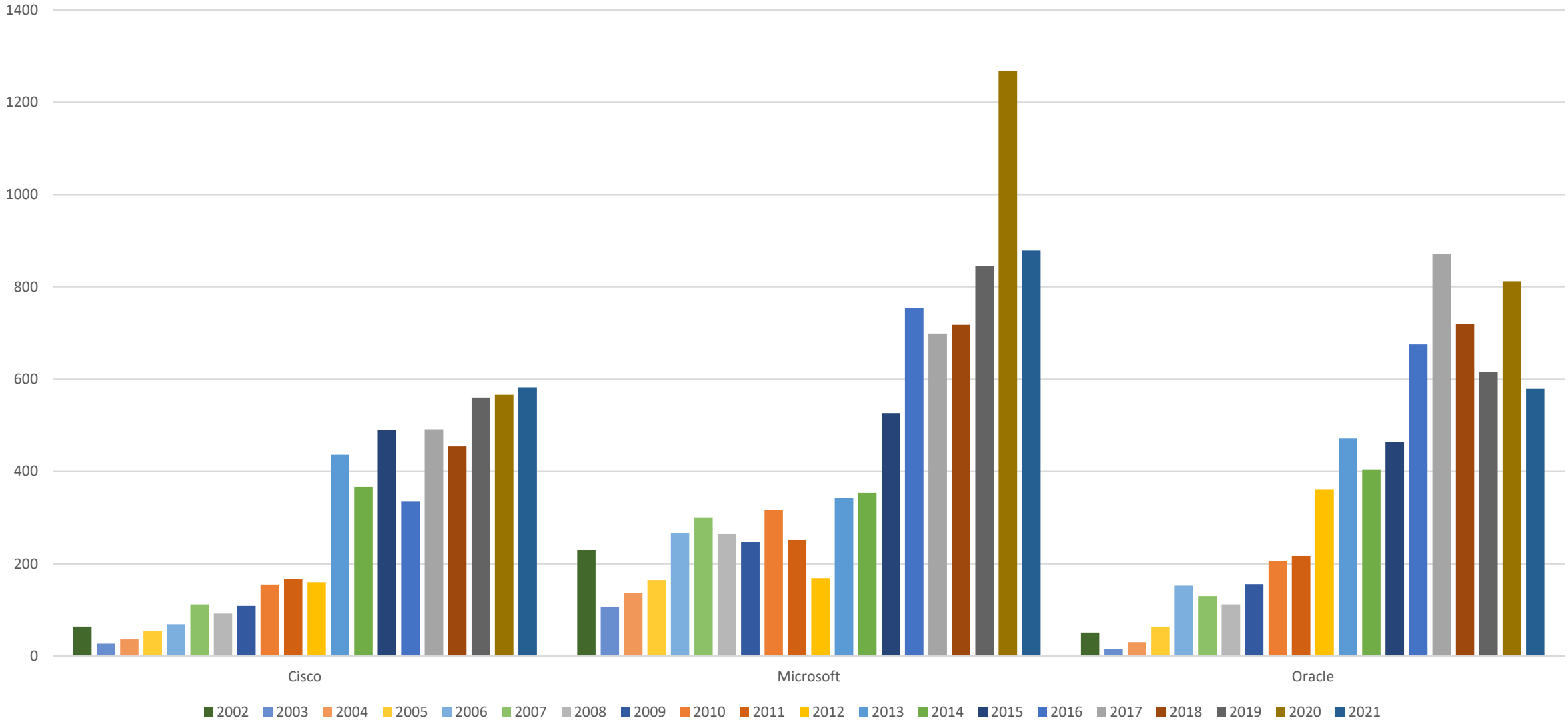
SIEMENS

OT with Manual Vulnerability Management

Time consuming – acceptable for only few vulns per year!

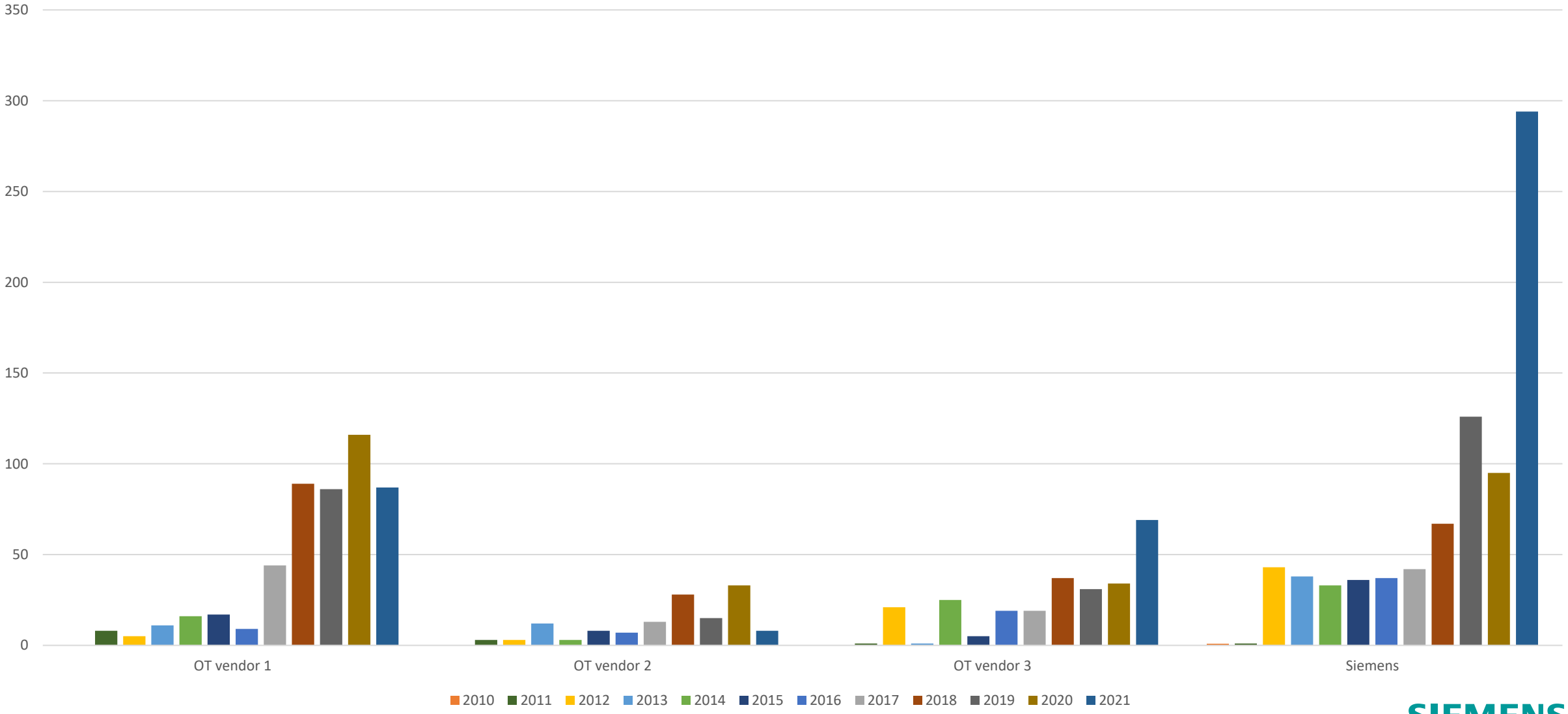
SIEMENS

Can we proceed like this?
How the vulnerabilities grow in IT



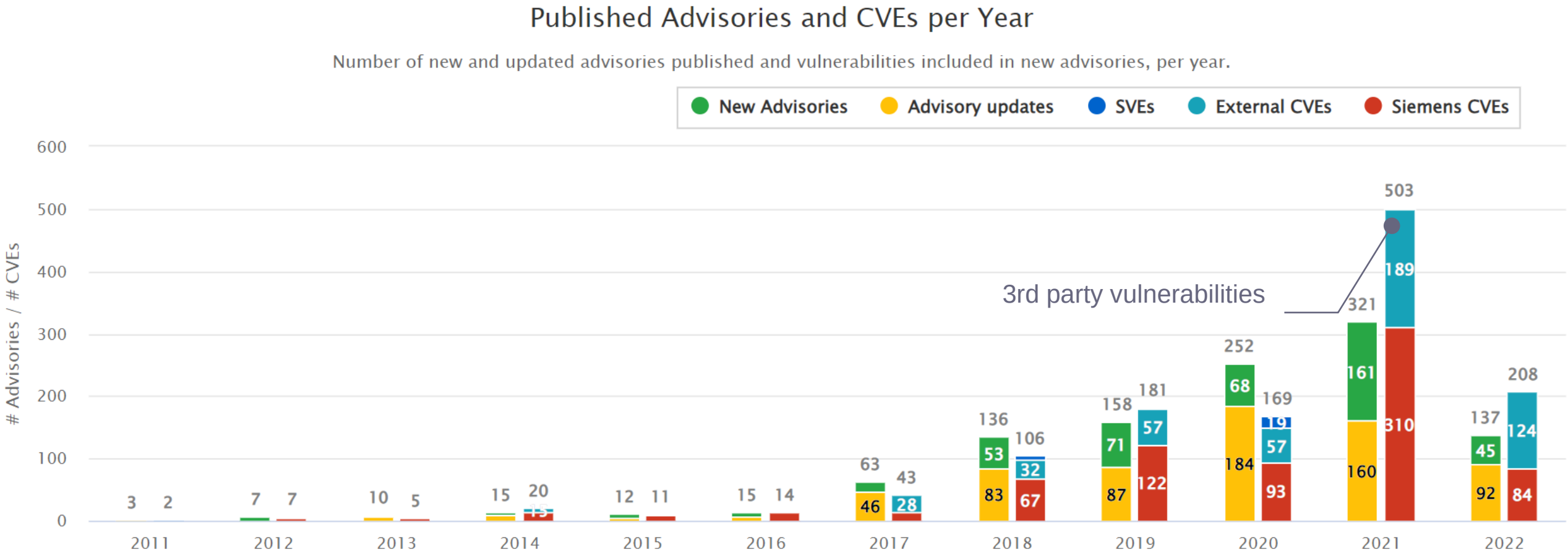
SIEMENS

Can we proceed like this?
How the vulnerabilities grow in OT



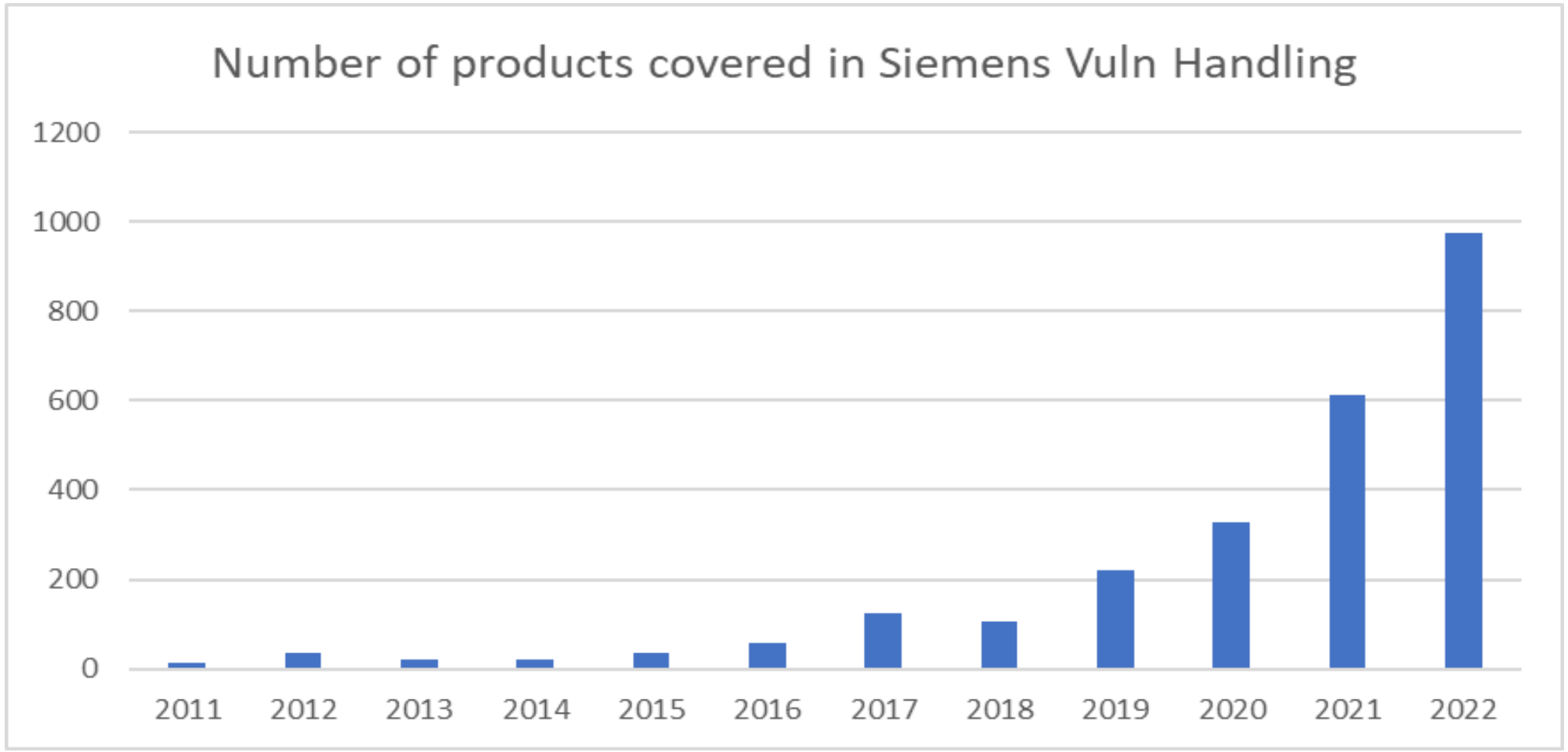
SIEMENS

Detailed look at Siemens



SIEMENS

Not just the vulnerabilties increase



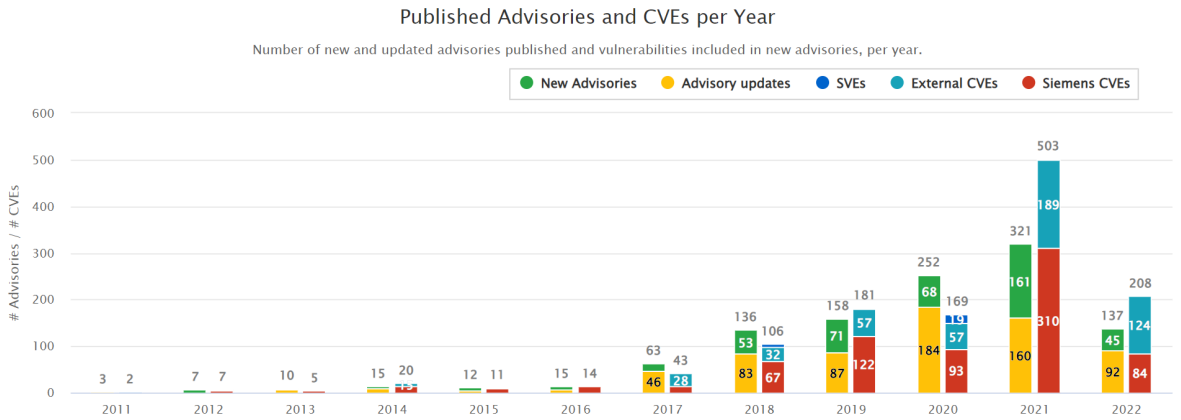
SIEMENS

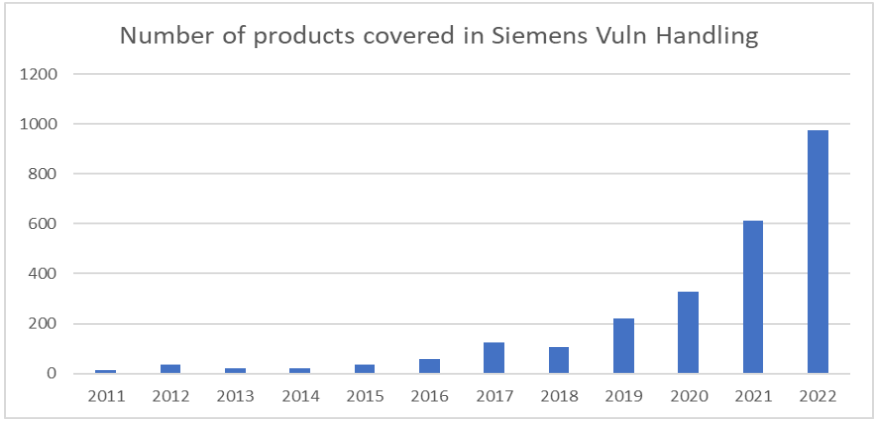
How fast is the problem growing?

Can this work in future?

Think for yourself:

- Is this exponential or linear growth?
- In how many dimensions does it grow?
  - Number of vulns in OT code
  - Number of vulns in 3rd party code
  - Number of affected products
  - Number of vendors performing vulnerability handling

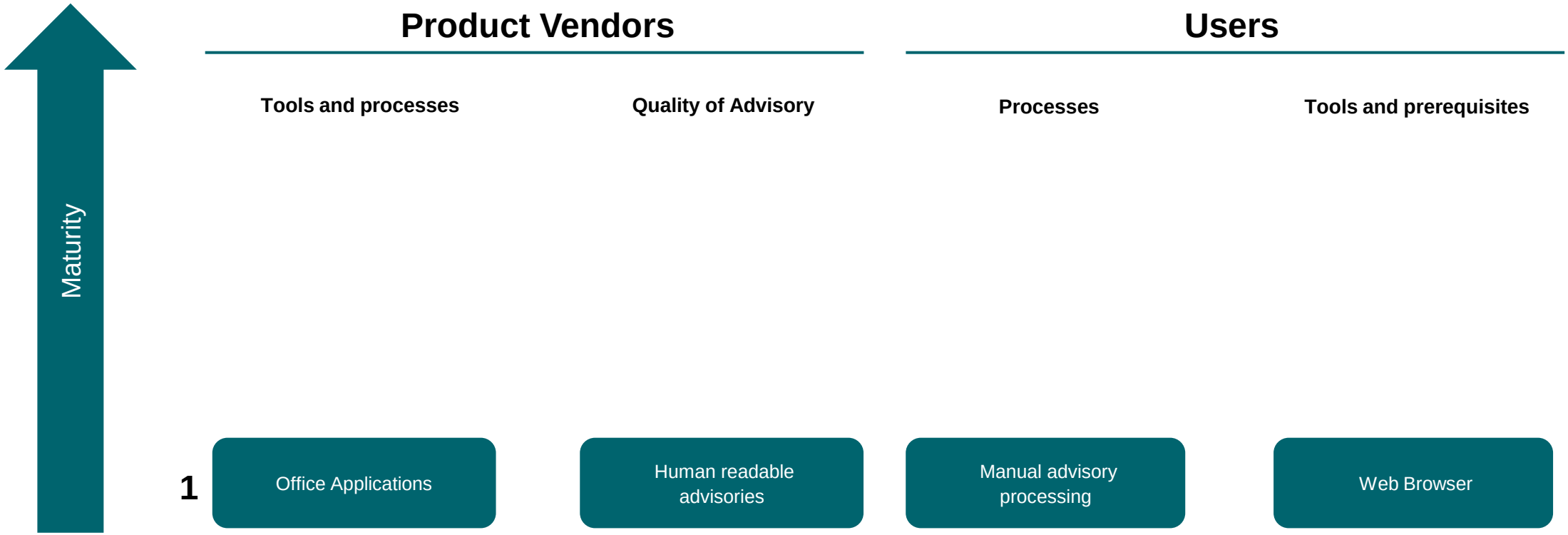




Manual handing of vulns and advisories does not scale.

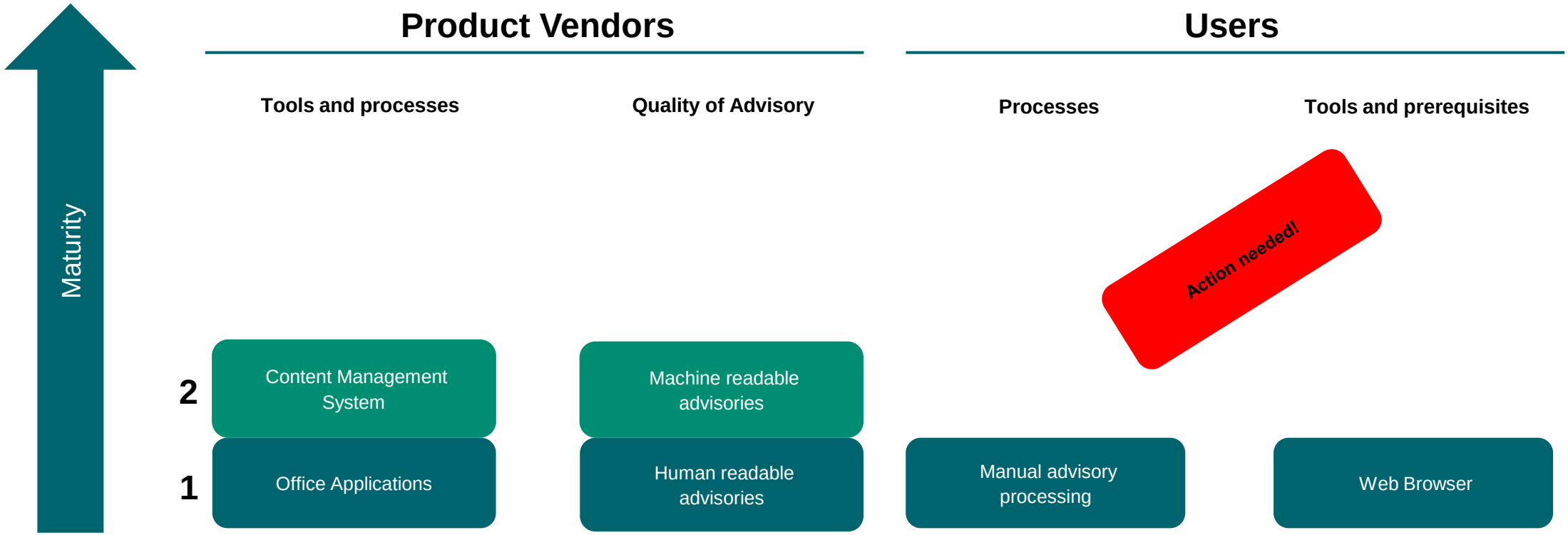
SIEMENS

Bridging Siemens-Customer Processes (e.g. Patch handling)



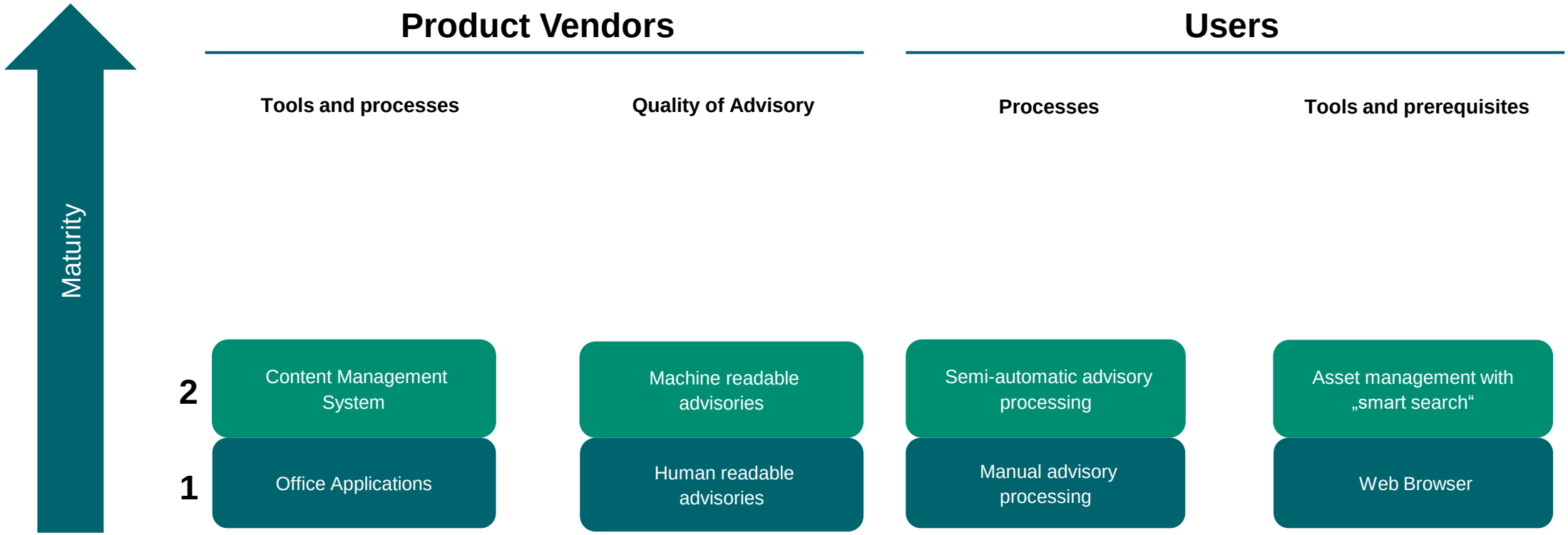
SIEMENS

Bridging Siemens-Customer Processes (e.g. Patch handling)
Current status



SIEMENS

Bridging Siemens-Customer Processes (e.g. Patch handling)



SIEMENS

OASIS Common Security Advisory Framework (CSAF) TC

Join This TC | TC Members Page | Send A Comment

Standardizing automated disclosure of cybersecurity vulnerability issues

Omar Santos, osantos@cisco.com, Chair

Table of Contents

- Announcements
- Overview
- Officers
- Subcommittees
- TC Liaisons
- TC Tools and Approved Publications
- Technical Work Produced by the Committee
- OASIS TC Open Repositories Sponsored by the Committee
- Expository Work Produced by the Committee

Related links

- Charter
- IPR Statement
- Membership
- Obligated Members
- Email Archives
- Comments Archive
- Ballots
- Documents
- Schedule

TC Participants

Representing these OASIS Foundationals and Sponsors:

- Accenture
- Cisco Systems
- Cryptsoft Pty Ltd.
- Cybeats
- Dell
- EclecticIQ
- Hitachi, Ltd.

Our Website for Advisories

Siemens Security Advisory by Siemens ProductCERT

SSA-392912: Multiple Denial Of Service Vulnerabilities in SCALANCE W1700 Devices

Publication Date: 2022-04-12
Last Update: 2022-04-12
Current Version: V1.0
CVSS v3.1 Base Score: 7.4

SUMMARY

Vulnerabilities have been identified in devices of the SCALANCE W-1700 (11ac) family that could allow an attacker to cause various denial of service conditions.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE W1788-1 M12 (6GK5788-1GY01-0AA0): All versions < V3.0.0	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1788-2 EEC M12 (6GK5788-2GY01-0TA0): All versions < V3.0.0	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1788-2 M12 (6GK5788-2GY01-0AA0): All versions < V3.0.0	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1788-2IA M12 (6GK5788-2HY01-0AA0): All versions < V3.0.0	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations

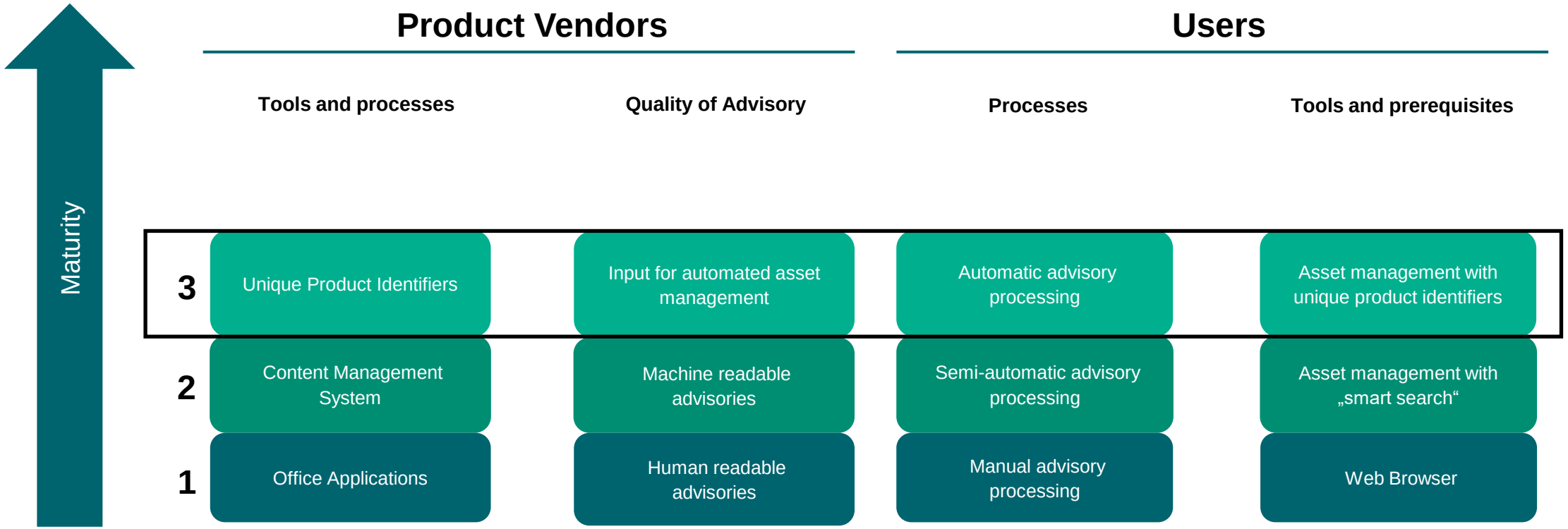
	Info	Version	Last Update	Download
	ⓘ	V1.0	2022-04-12	HTML CSAF PDF TXT
200 and S7-ants)	ⓘ	V1.0	2022-04-12	HTML CSAF PDF TXT
evices	ⓘ	V1.0	2022-04-12	HTML CSAF PDF TXT
	ⓘ	V1.0	2022-04-12	HTML CSAF PDF TXT
nterniche	ⓘ	V1.0	2022-04-12	HTML CSAF PDF TXT
	ⓘ	V1.0	2022-04-12	HTML CSAF PDF TXT

SIEMENS

CSAF – A quick glance into the format

SIEMENS

Introducing Unique Product Identifiers



SIEMENS

Identifying products – not a simple problem

Search Results (Refine Search)

Search Parameters:

- Keyword: s7-1500
- CPE Status: FINAL
- CPE Naming Format: 2.3

There are **259** matching records.
Displaying matches **1** through **20**.

Vendor	Product
cpe:2.3:a:siemens:simatic_s7-1500:-:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500
cpe:2.3:a:siemens:simatic_s7-1500:2.0:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500
cpe:2.3:a:siemens:simatic_s7-1500__software_controller:-:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500__software_controller
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:-:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500_software_controller
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:2.0:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500_software_controller
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:2.1:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500_software_controller
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:2.5:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500_software_controller
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:2.6:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500_software_controller
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:2.7:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500_software_controller
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:20.8:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500_software_controller
cpe:2.3:h:siemens:6es7510-1dj01-0ab0:-:*:*:*:*:*:*:* View CVEs	
siemens	6es7510-1dj01-0ab0
cpe:2.3:h:siemens:6es7510-1sj01-0ab0:-:*:*:*:*:*:*:* View CVEs	
siemens	6es7510-1sj01-0ab0
cpe:2.3:h:siemens:6es7511-1ak01-0ab0:-:*:*:*:*:*:*:* View CVEs	

-> CPE is not a solution for us

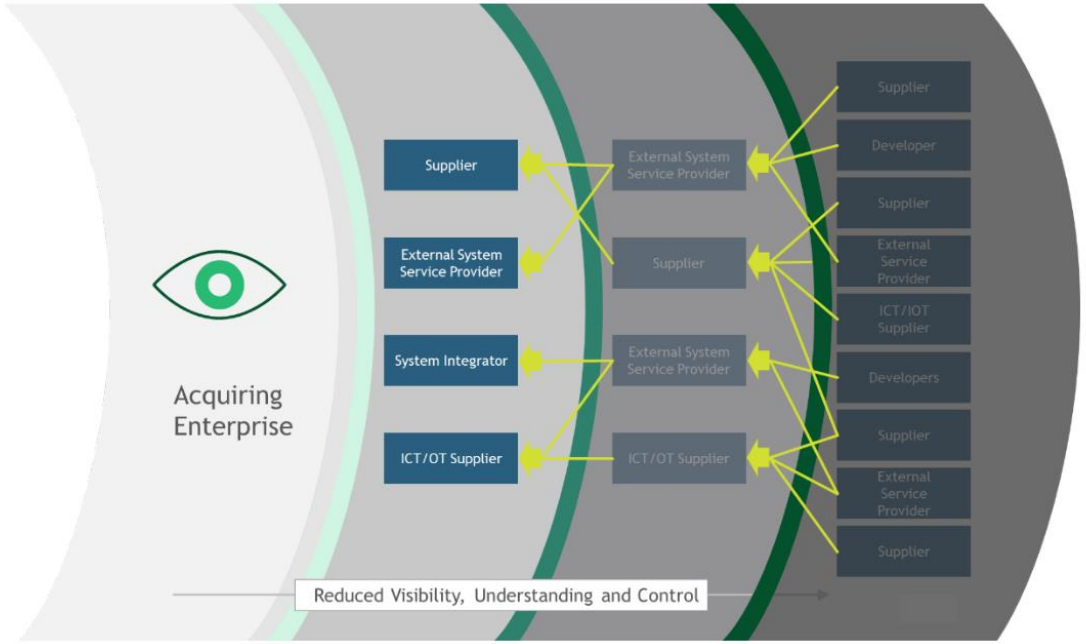
```
79   "product_tree": {
80     "branches": [
81       {
82         "name": "Siemens",
83         "category": "vendor",
84         "branches": [
85           {
86             "name": "SCALANCE W1788-1 M12",
87             "category": "product_name",
88             "branches": [
89               {
90                 "name": "< V3.0.0",
91                 "category": "product_version_range",
92                 "product": {
93                   "product_id": "1",
94                   "name": "SCALANCE W1788-1 M12",
95                   "product_identification_helper": {
96                     "model_numbers": [
97                       "6GK5788-1GY01-0AA0"
98                     ]
99                   }
100                }
```

-> our approach: use our own order numbers

SIEMENS

Bridging the gap to SBOM: VEX


```
{
  "document": {
    "title": "SSA-392912: Multiple Denial Of Service Vulnerabilities in SCALANCE W1700 Devices",
    "category": "Siemens Security Advisory",
    "csaf_version": "2.0",
    "publisher": {
      "name": "Siemens ProductCERT",
      "contact_details": "productcert@siemens.com",
      "category": "vendor",
      "namespace": "https://www.siemens.com"
    },
    "distribution": {
      "text": "Disclosure is not limited.",
      "tlp": {
        "label": "WHITE"
      }
    },
    "tracking": {
      "id": "SSA-392912",
      "status": "final",
      "version": "1",
      "revision_history": [
        {
          "number": "1",
          "legacy_version": "1.0",
          "date": "2022-04-12T00:00:00Z",
          "summary": "Publication Date"
        }
      ],
      "initial_release_date": "2022-04-12T00:00:00Z",
      "current_release_date": "2022-04-12T00:00:00Z",
      "generator": {
        "engine": {
```

CSAF: detailed information about a vulnerability

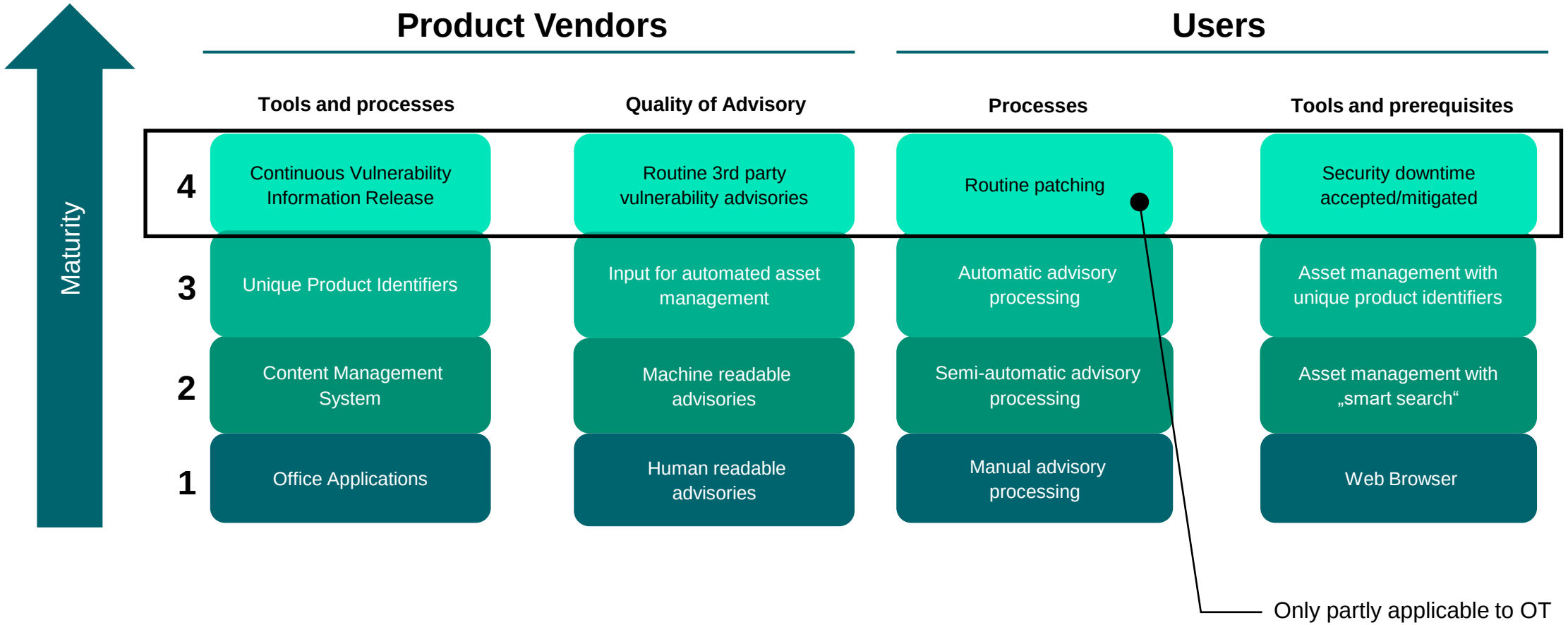
SBOM: deep visibility into supply chain

VEX: short vendor statement “affected” / “not affected” *)

*) CSAF offers a corresponding profile!

SIEMENS

Outlook



SIEMENS

Thanks for your attention!

SIEMENS