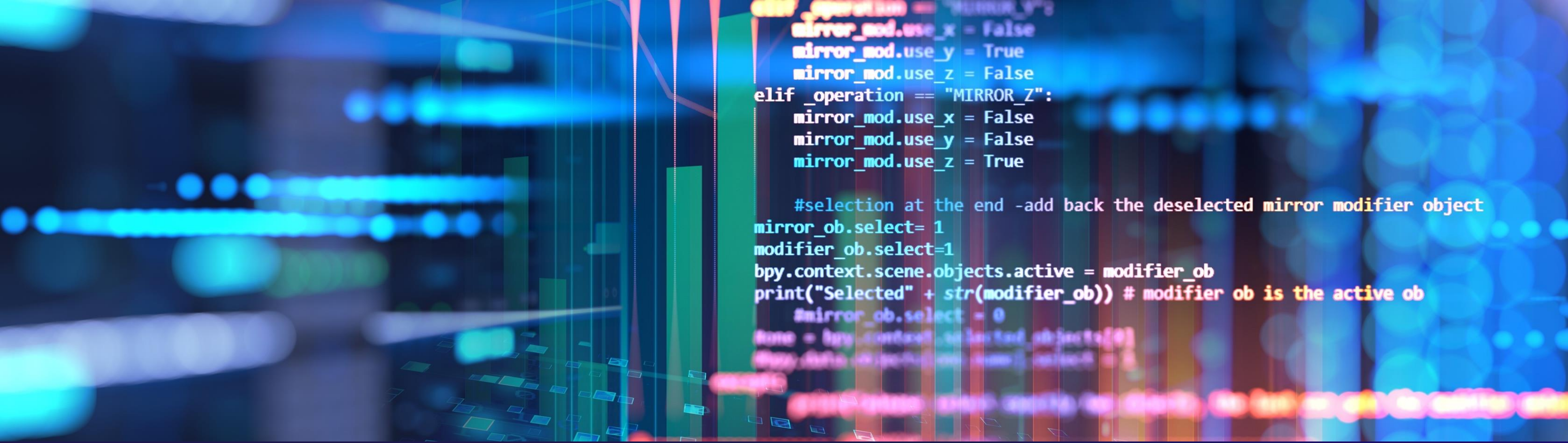


TLP:CLEAR

> CSAF Community Days

VEX-supported vulnerability management with SecObserve

Stefan Fleckenstein & Lukas Krug

Stackable

MAIBORNWOLFF

Who we are

Stefan Fleckenstein

- Executive IT and Cybersecurity Architect at MaibornWolff
- Background in software engineering and cybersecurity
- Passionate about vulnerability management and open source
- Founder and maintainer of SecObserve

Lukas Krug

- Platform Engineer at Stackable
- Background in software engineering and DevOps
- Likes working with Kubernetes and coding in Rust
- Interested in all things regarding supply chain security

TLP:CLEAR

Agenda

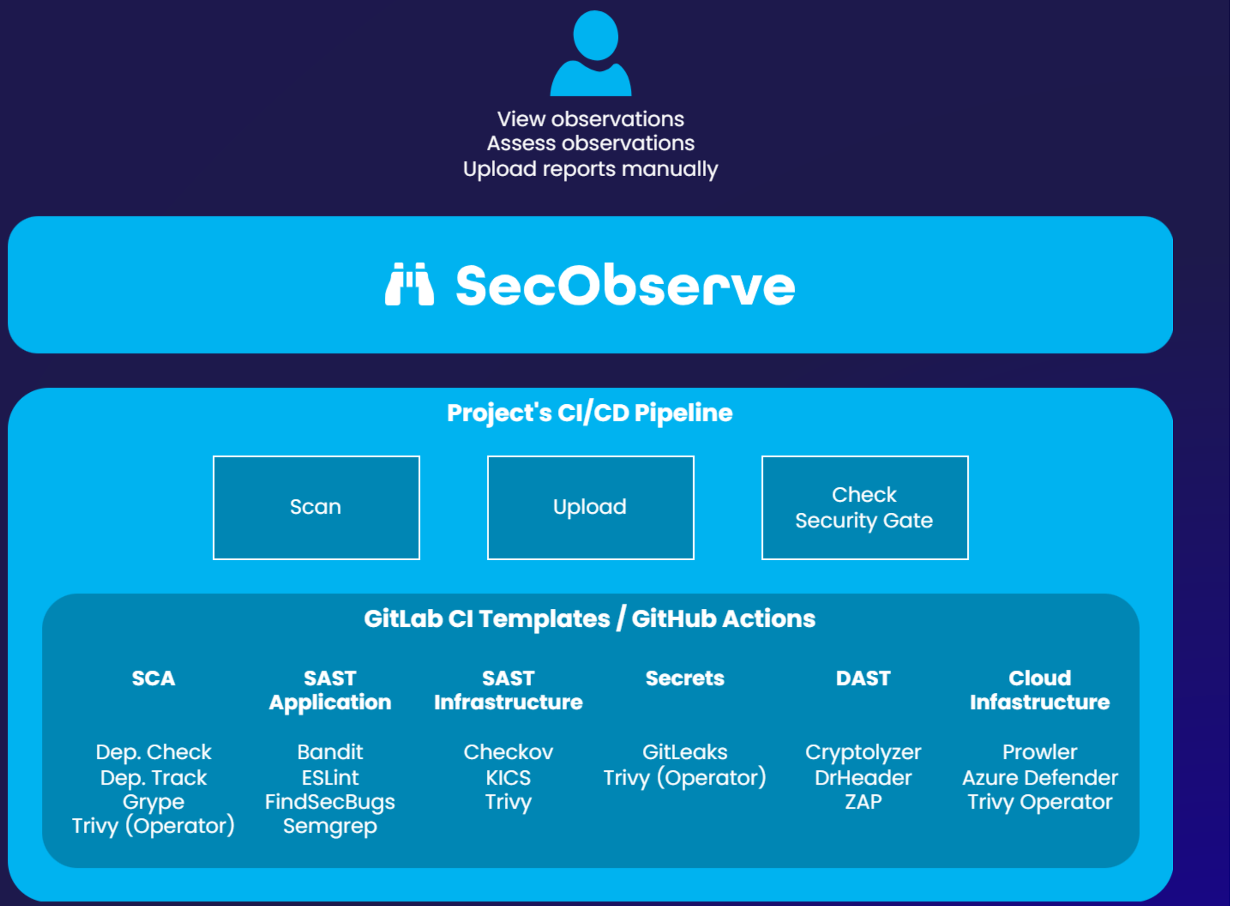
- Introduction to SecObserve
- Producing and consuming CSAF VEX documents

TLP:CLEAR

Introduction to SecObserve

TLP:CLEAR

INTRODUCTION TO SECOBSERVE



View observations
Assess observations
Upload reports manually

SecObserve

Project's CI/CD Pipeline

Scan | Upload | Check Security Gate

GitLab CI Templates / GitHub Actions

SCA	SAST Application	SAST Infrastructure	Secrets	DAST	Cloud Infastructure
Dep. Check	Bandit	Checkov	GitLeaks	Cryptolyzer	Prowler
Dep. Track	ESLint	KICS	Trivy (Operator)	DrHeader	Azure Defender
Grype	FindSecBugs	Trivy		ZAP	Trivy Operator
Trivy (Operator)	Semgrep				

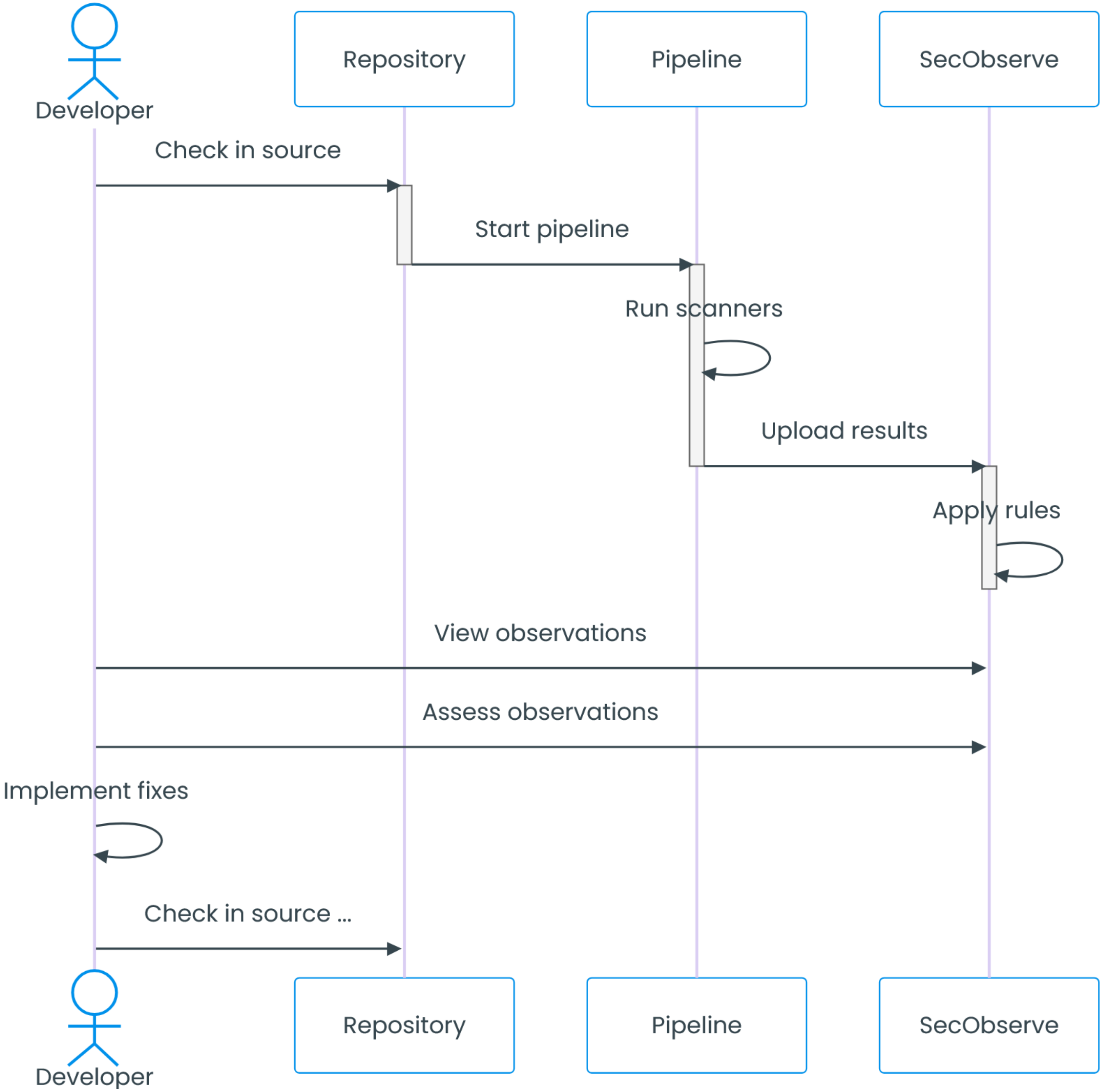
- SecObserve is an **open source vulnerability and license management** system for software development teams and cloud environments.
- It supports a **variety of open source vulnerability scanners** and integrates easily into CI/CD pipelines.
- Results about potential security flaws from various vulnerability scanning tools are made available for **assessment and reporting**.

https://github.com/MaibornWolff/SecObserve

TLP:CLEAR

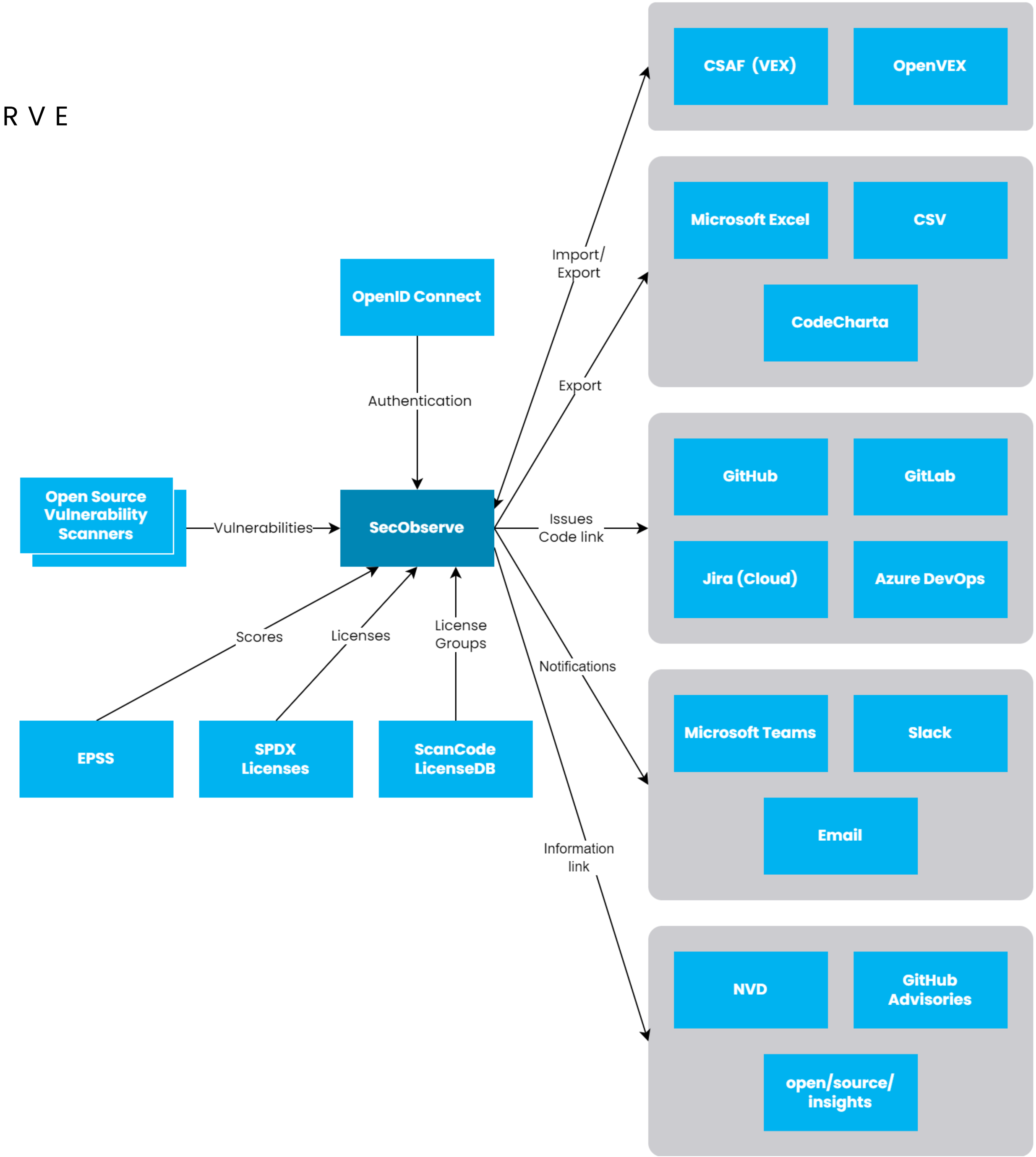
Process

TLP:CLEAR



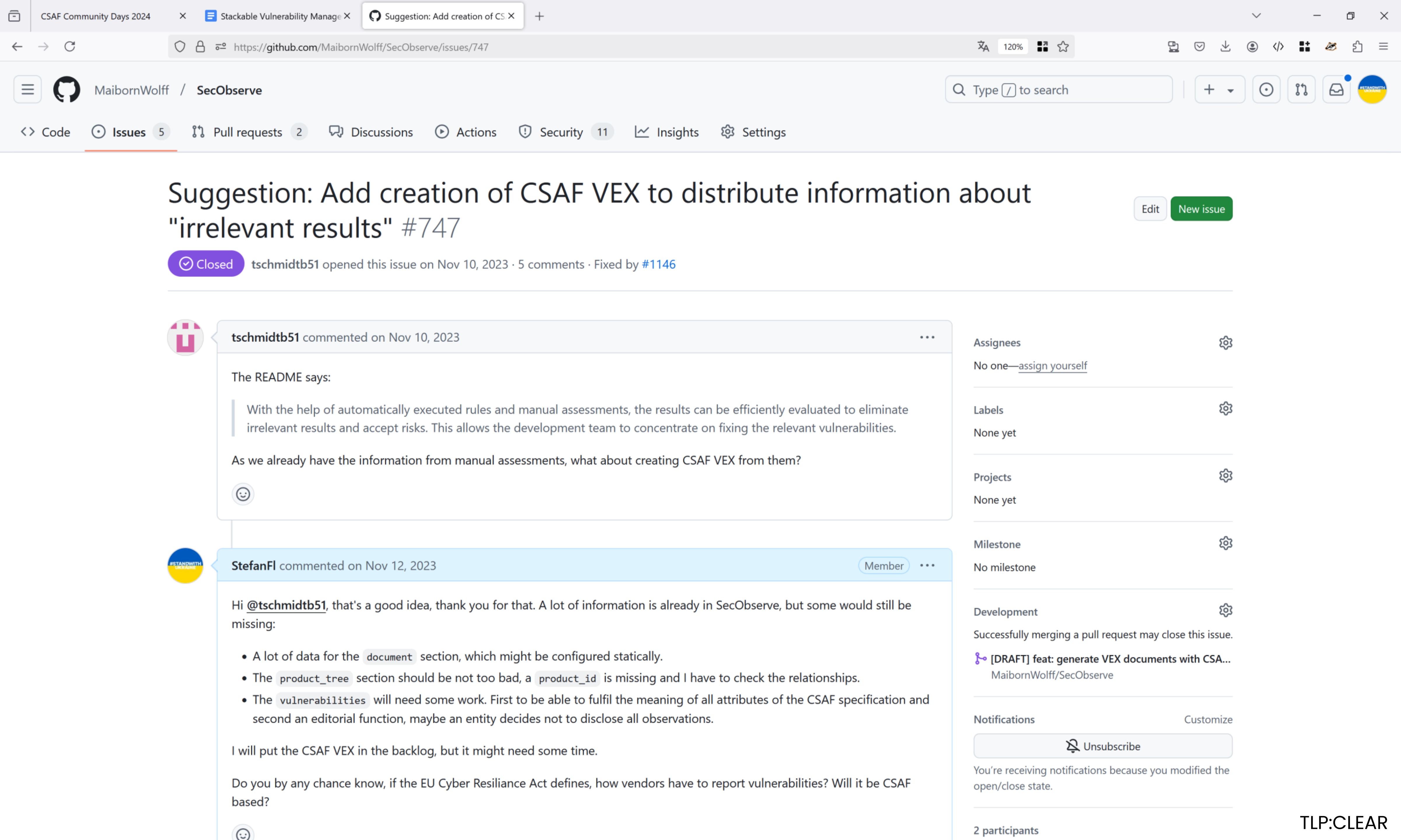
https://github.com/MaibornWolff/SecObserve

Integrations



https://github.com/MaibornWolff/SecObserve

TLP:CLEAR


CSAF Community Days 2024
Stackable Vulnerability Manage
Suggestion: Add creation of CS
https://github.com/MaibornWolff/SecObserve/issues/747
120%
MaibornWolff / SecObserve
Type / to search
Code
Issues 5
Pull requests 2
Discussions
Actions
Security 11
Insights
Settings
Edit
New issue

Suggestion: Add creation of CSAF VEX to distribute information about "irrelevant results" #747

Closed tschmidtb51 opened this issue on Nov 10, 2023 · 5 comments · Fixed by #1146

tschmidtb51 commented on Nov 10, 2023

The README says:

> With the help of automatically executed rules and manual assessments, the results can be efficiently evaluated to eliminate irrelevant results and accept risks. This allows the development team to concentrate on fixing the relevant vulnerabilities.

As we already have the information from manual assessments, what about creating CSAF VEX from them?

StefanFl commented on Nov 12, 2023 Member

Hi @tschmidtb51, that's a good idea, thank you for that. A lot of information is already in SecObserve, but some would still be missing:

- A lot of data for the `document` section, which might be configured statically.
- The `product_tree` section should be not too bad, a `product_id` is missing and I have to check the relationships.
- The `vulnerabilities` will need some work. First to be able to fulfil the meaning of all attributes of the CSAF specification and second an editorial function, maybe an entity decides not to disclose all observations.

I will put the CSAF VEX in the backlog, but it might need some time.

Do you by any chance know, if the EU Cyber Resiliance Act defines, how vendors have to report vulnerabilities? Will it be CSAF based?

Assignees
No one—assign yourself

Labels
None yet

Projects
None yet

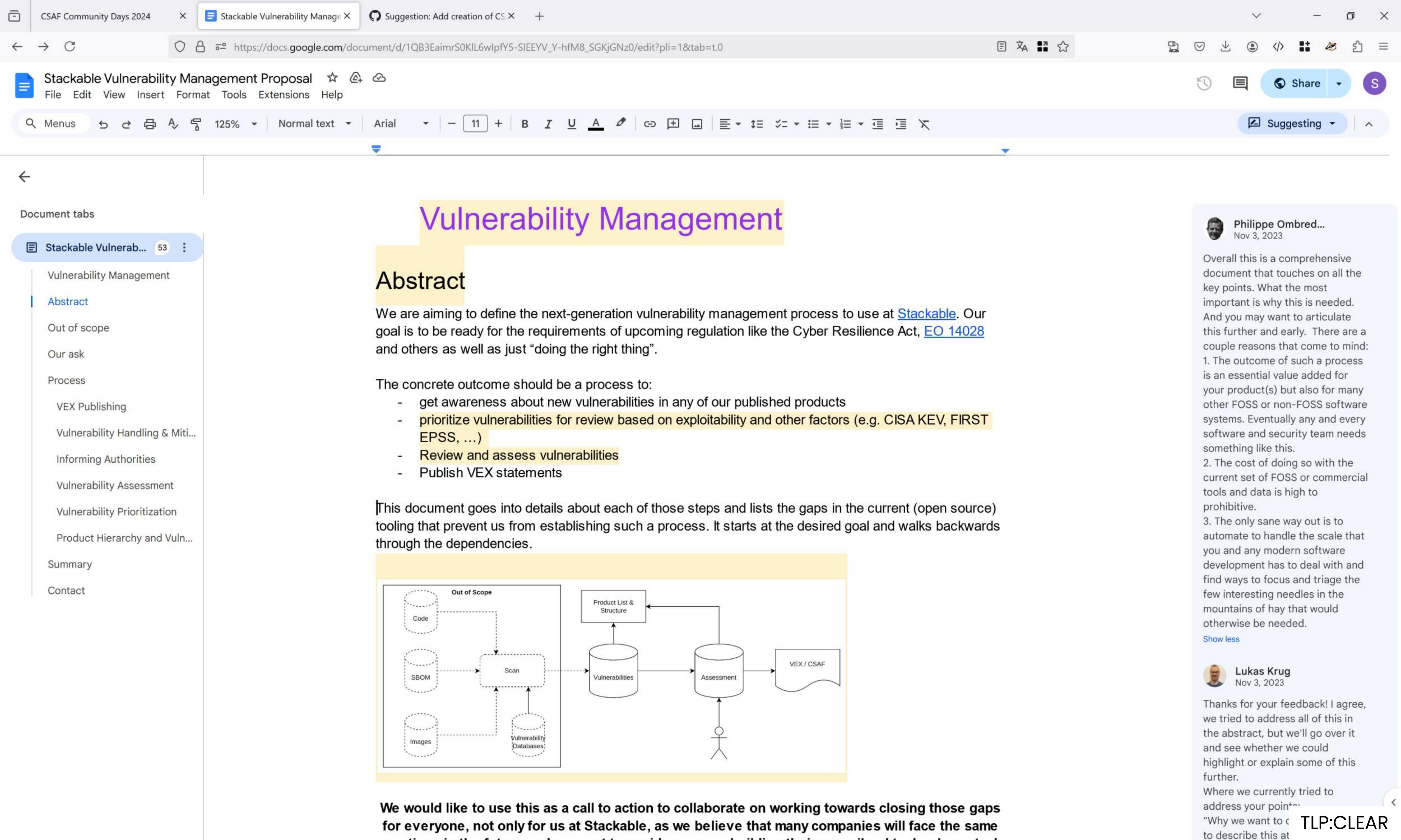
Milestone
No milestone

Development
Successfully merging a pull request may close this issue.
[DRAFT] feat: generate VEX documents with CSA...
MaibornWolff/SecObserve

Notifications Customize
Unsubscribe
You're receiving notifications because you modified the open/close state.

2 participants

TLP:CLEAR


CSAF Community Days 2024
Stackable Vulnerability Manage
Suggestion: Add creation of CS
https://docs.google.com/document/d/1QB3EaimrS0KlL6wIpfY5-SIEEYV_Y-hfM8_SGKjGNz0/edit?pli=1&tab=t.0
Stackable Vulnerability Management Proposal
File
Edit
View
Insert
Format
Tools
Extensions
Help
Share
S
Menus
125%
Normal text
Arial
11
Suggesting
Document tabs
Stackable Vulnerab...
53
Vulnerability Management
Abstract
Out of scope
Our ask
Process
VEX Publishing
Vulnerability Handling & Miti...
Informing Authorities
Vulnerability Assessment
Vulnerability Prioritization
Product Hierarchy and Vuln...
Summary
Contact

Vulnerability Management

Abstract

We are aiming to define the next-generation vulnerability management process to use at Stackable. Our goal is to be ready for the requirements of upcoming regulation like the Cyber Resilience Act, EO 14028 and others as well as just “doing the right thing”.

The concrete outcome should be a process to:

- get awareness about new vulnerabilities in any of our published products
- prioritize vulnerabilities for review based on exploitability and other factors (e.g. CISA KEV, FIRST EPSS, …)
- Review and assess vulnerabilities
- Publish VEX statements

This document goes into details about each of those steps and lists the gaps in the current (open source) tooling that prevent us from establishing such a process. It starts at the desired goal and walks backwards through the dependencies.

We would like to use this as a call to action to collaborate on working towards closing those gaps for everyone, not only for us at Stackable, as we believe that many companies will face the same

Philippe Ombred...
Nov 3, 2023

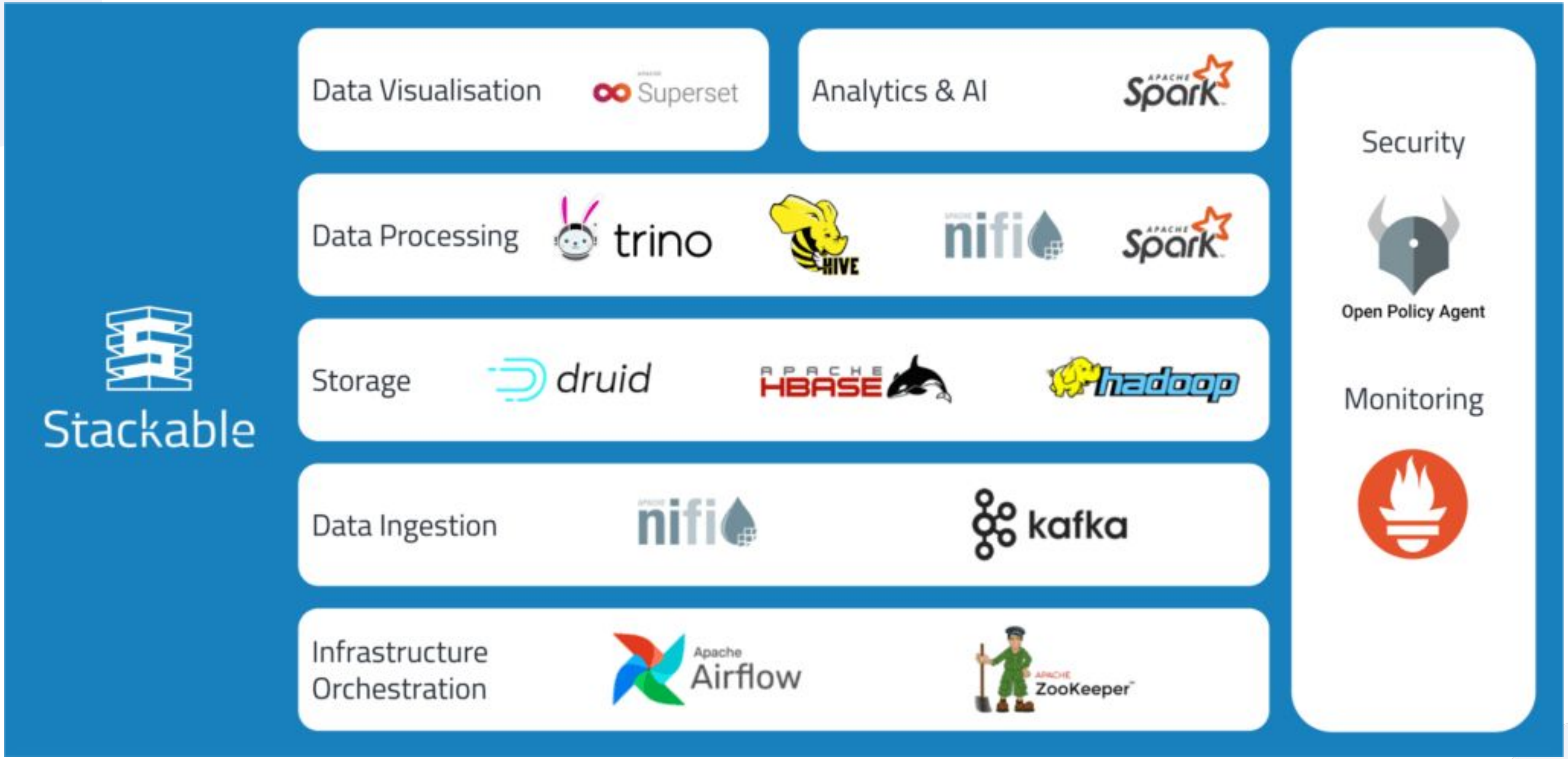
Overall this is a comprehensive document that touches on all the key points. What the most important is why this is needed. And you may want to articulate this further and early. There are a couple reasons that come to mind:
1. The outcome of such a process is an essential value added for your product(s) but also for many other FOSS or non-FOSS software systems. Eventually any and every software and security team needs something like this.
2. The cost of doing so with the current set of FOSS or commercial tools and data is high to prohibitive.
3. The only sane way out is to automate to handle the scale that you and any modern software development has to deal with and find ways to focus and triage the few interesting needles in the mountains of hay that would otherwise be needed.

Show less

Lukas Krug
Nov 3, 2023

Thanks for your feedback! I agree, we tried to address all of this in the abstract, but we'll go over it and see whether we could highlight or explain some of this further.
Where we currently tried to address your poin
"Why we want to c
to describe this at

Producing and consuming CSAF VEX documents



Data Visualisation

Analytics & AI

Data Processing

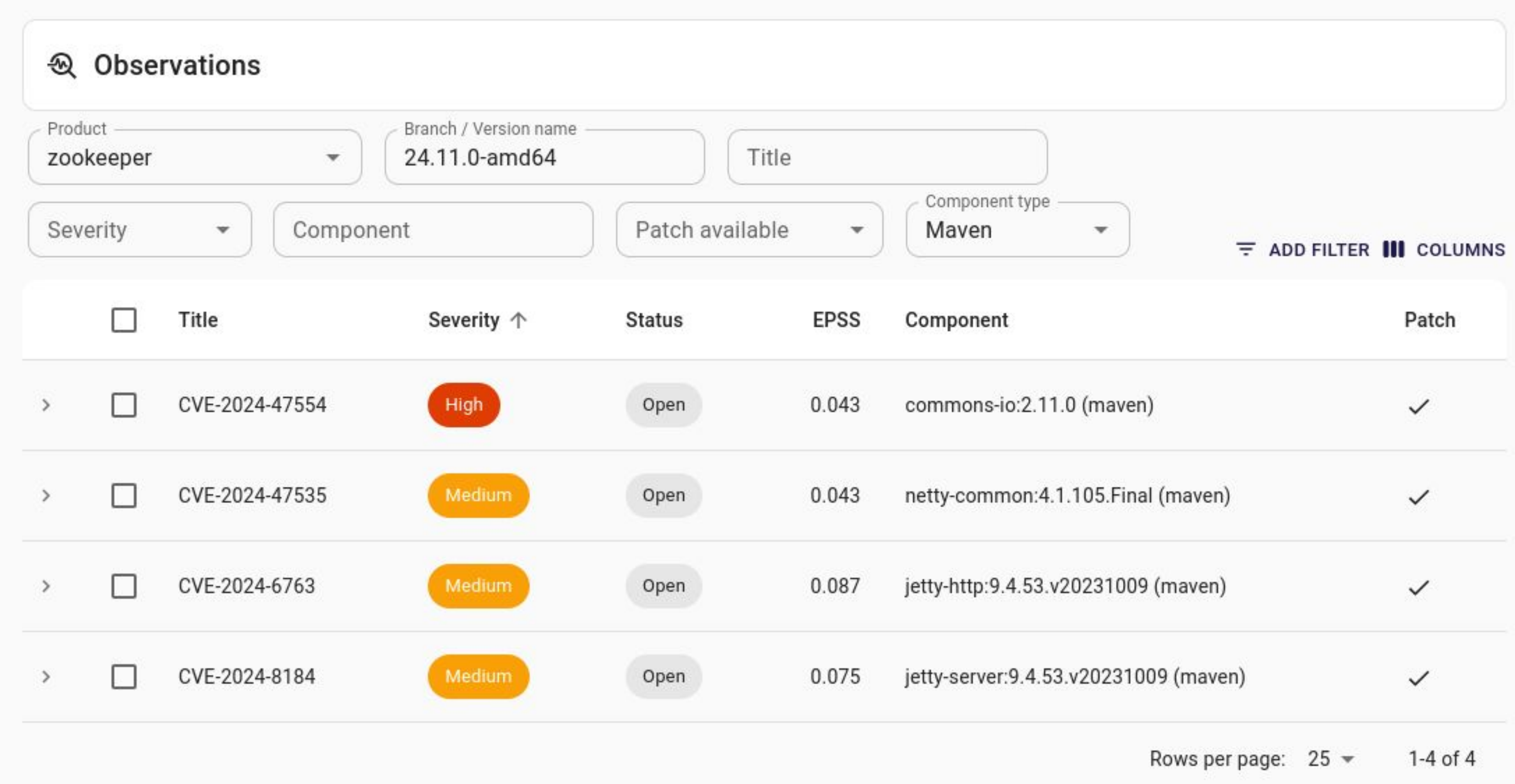
Storage

Data Ingestion

Infrastructure Orchestration

Security

Monitoring



Observations

Product: zookeeper

Branch / Version name: 24.11.0-amd64

Title

Severity

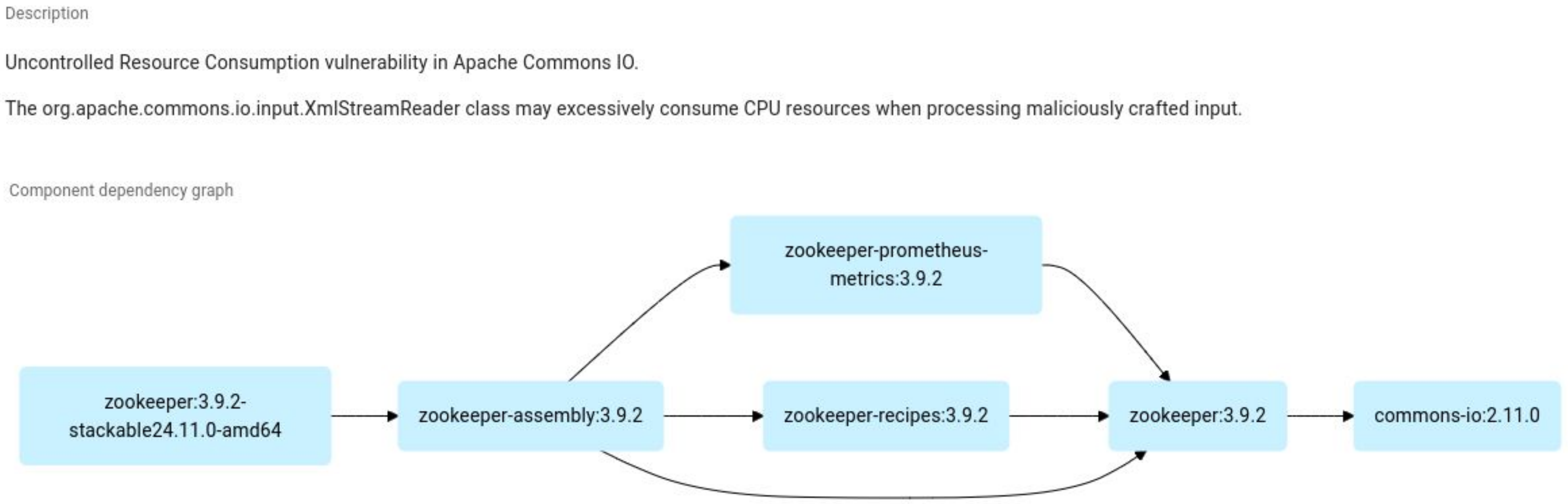
Component

Patch available

Component type: Maven

	□	Title	Severity ↑	Status	EPSS	Component	Patch
›	□	CVE-2024-47554	High	Open	0.043	commons-io:2.11.0 (maven)	✓
›	□	CVE-2024-47535	Medium	Open	0.043	netty-common:4.1.105.Final (maven)	✓
›	□	CVE-2024-6763	Medium	Open	0.087	jetty-http:9.4.53.v20231009 (maven)	✓
›	□	CVE-2024-8184	Medium	Open	0.075	jetty-server:9.4.53.v20231009 (maven)	✓

Rows per page: 25 1-4 of 4



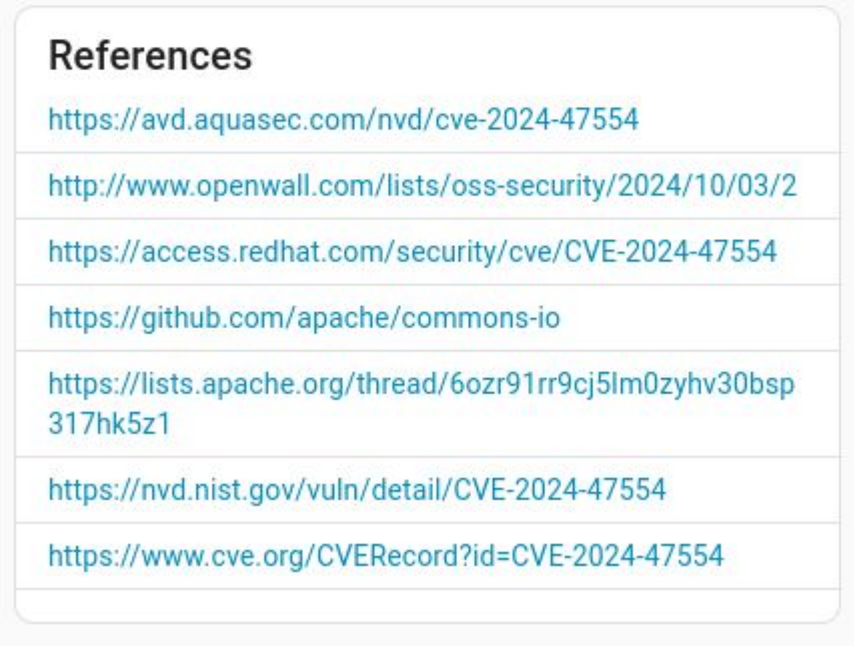
Description

Uncontrolled Resource Consumption vulnerability in Apache Commons IO.

The org.apache.commons.io.input.XmlStreamReader class may excessively consume CPU resources when processing maliciously crafted input.

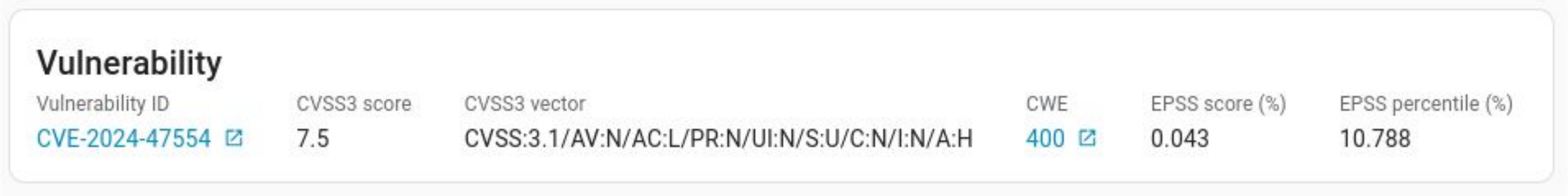
Component dependency graph

TLP:CLEAR



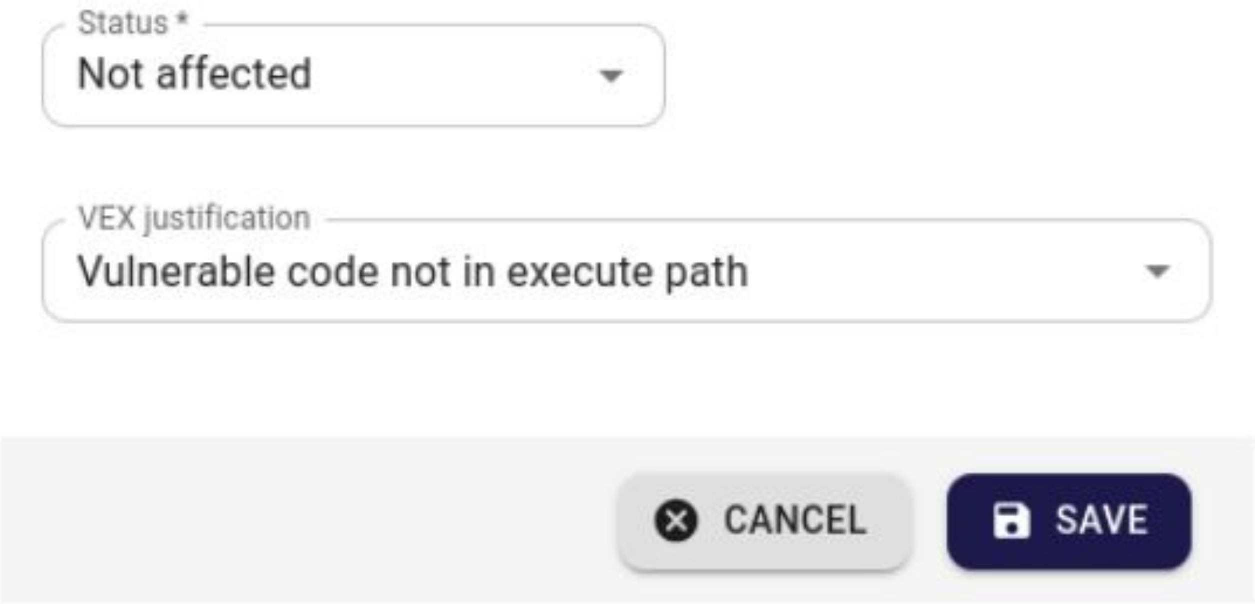
References

- https://avd.aquasec.com/nvd/cve-2024-47554
- http://www.openwall.com/lists/oss-security/2024/10/03/2
- https://access.redhat.com/security/cve/CVE-2024-47554
- https://github.com/apache/commons-io
- https://lists.apache.org/thread/6ozr91rr9cj5lm0zyhv30bsp317hk5z1
- https://nvd.nist.gov/vuln/detail/CVE-2024-47554
- https://www.cve.org/CVERecord?id=CVE-2024-47554



Vulnerability

Vulnerability ID	CVSS3 score	CVSS3 vector	CWE	EPSS score (%)	EPSS percentile (%)
CVE-2024-47554	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	400	0.043	10.788



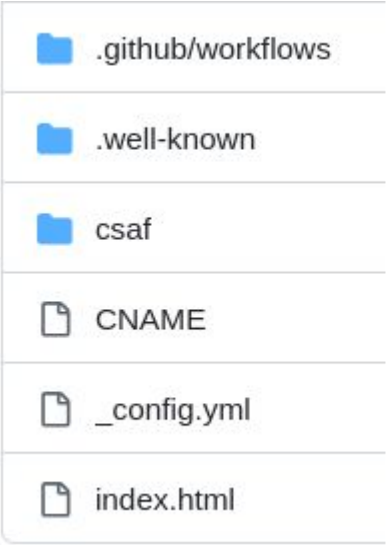
Status *
Not affected

VEX justification
Vulnerable code not in execute path

CSAF publishing workflow

Checkout Git repo

CSAF publishing workflow



.github/workflows

.well-known

csaf

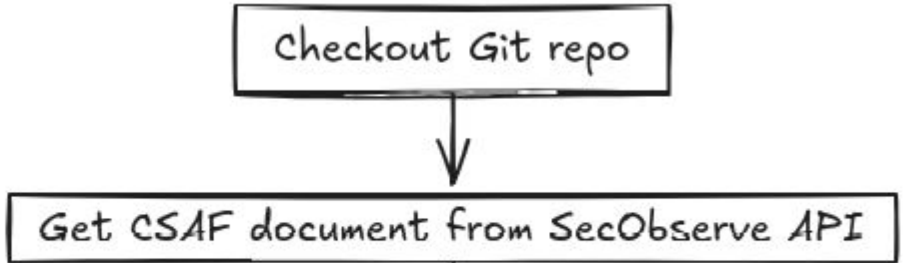
CNAME

_config.yml

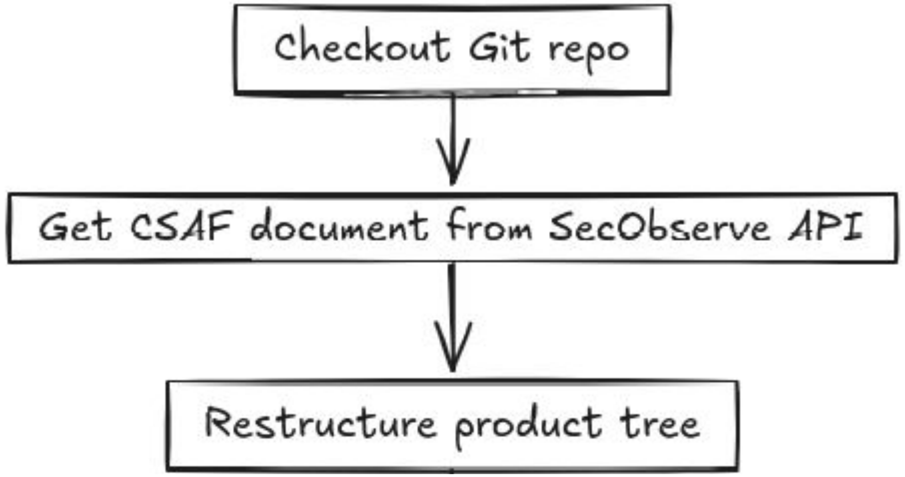
index.html

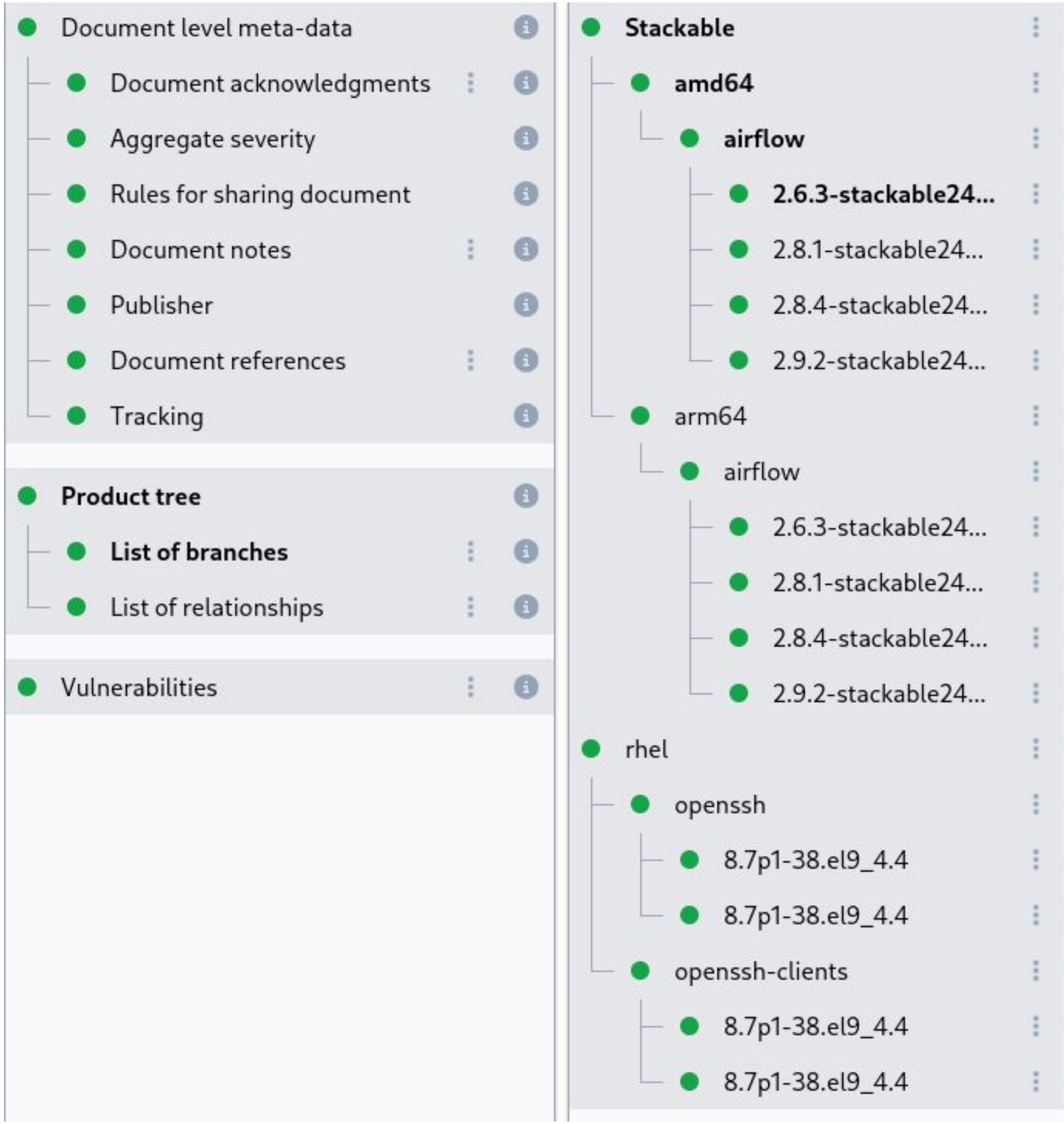
TLP:CLEAR

CSAF publishing workflow



CSAF publishing workflow



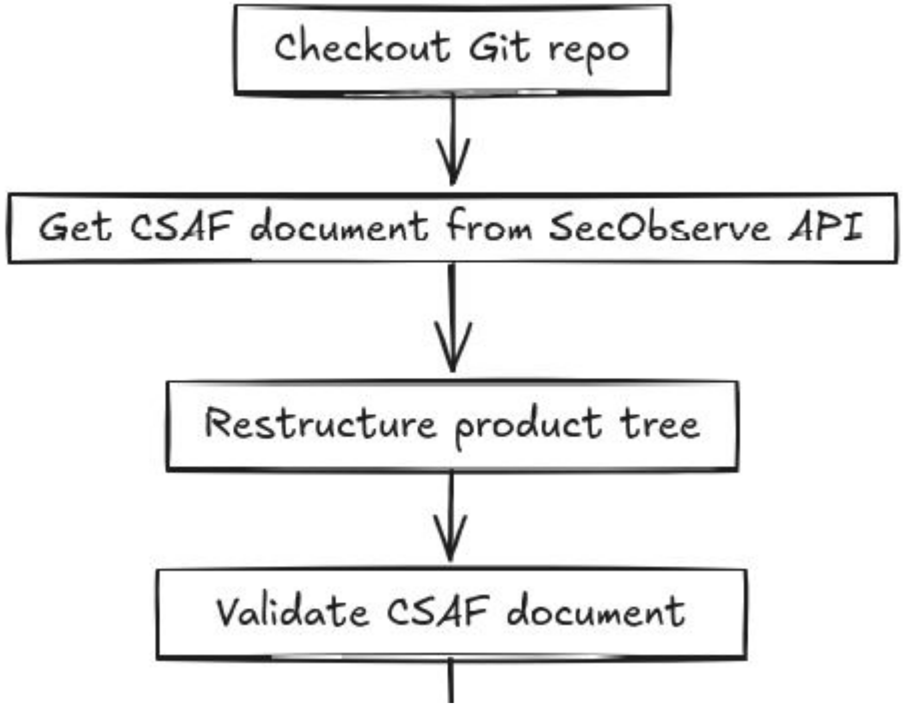


- Document level meta-data
  - Document acknowledgments
  - Aggregate severity
  - Rules for sharing document
  - Document notes
  - Publisher
  - Document references
  - Tracking
- **Product tree**
  - **List of branches**
  - List of relationships
- Vulnerabilities

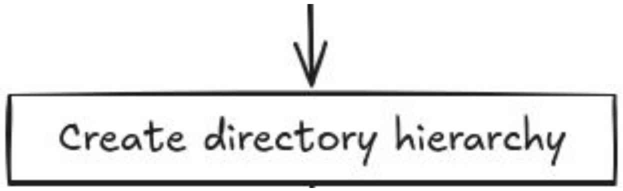
- **Stackable**
  - **amd64**
    - **airflow**
      - **2.6.3-stackable24...**
      - 2.8.1-stackable24...
      - 2.8.4-stackable24...
      - 2.9.2-stackable24...
  - arm64
    - airflow
      - 2.6.3-stackable24...
      - 2.8.1-stackable24...
      - 2.8.4-stackable24...
      - 2.9.2-stackable24...
- rhel
  - openssh
    - 8.7p1-38.el9_4.4
    - 8.7p1-38.el9_4.4
  - openssh-clients
    - 8.7p1-38.el9_4.4
    - 8.7p1-38.el9_4.4

TLP:CLEAR

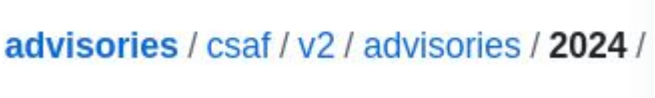
CSAF publishing workflow



CSAF publishing workflow

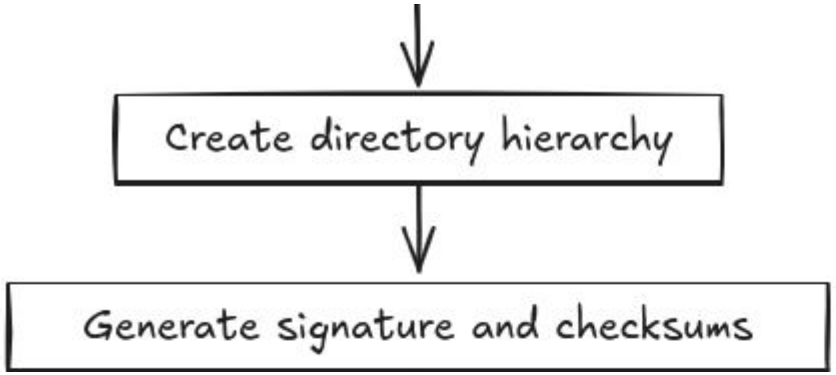


Create directory hierarchy



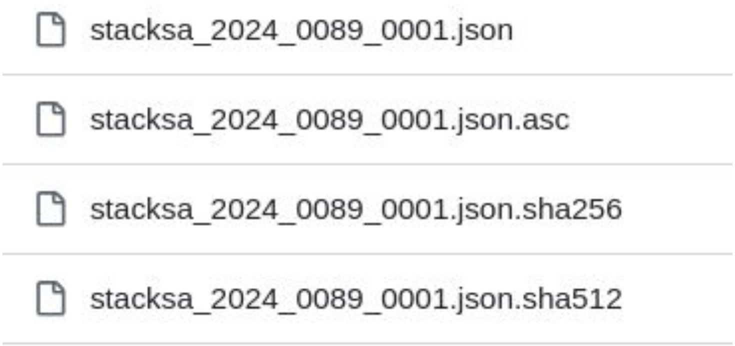
advisories / csaf / v2 / advisories / **2024** /

CSAF publishing workflow



Create directory hierarchy

Generate signature and checksums



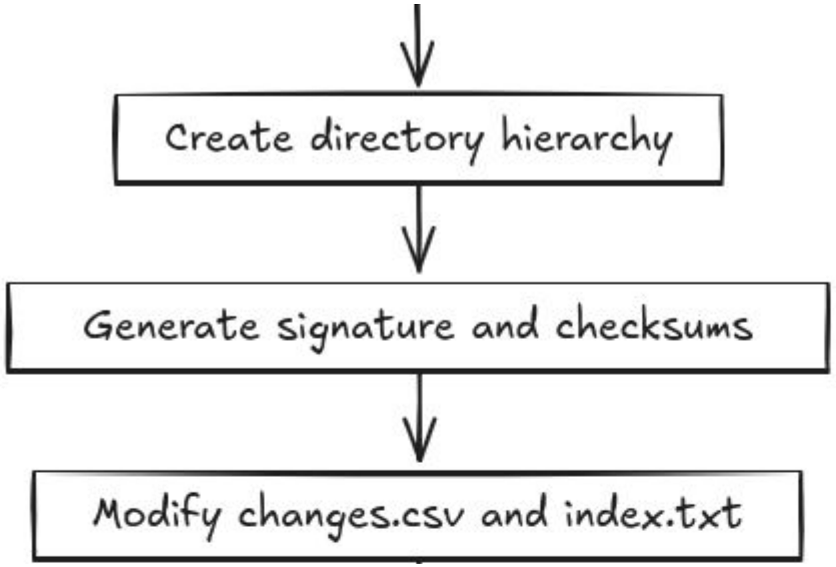
stacksa_2024_0089_0001.json

stacksa_2024_0089_0001.json.asc

stacksa_2024_0089_0001.json.sha256

stacksa_2024_0089_0001.json.sha512

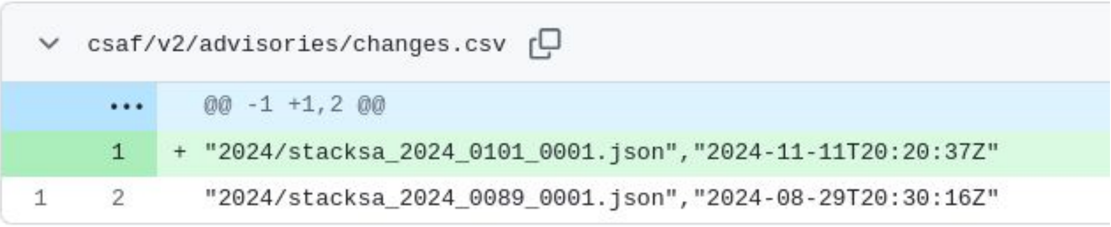
CSAF publishing workflow



Create directory hierarchy

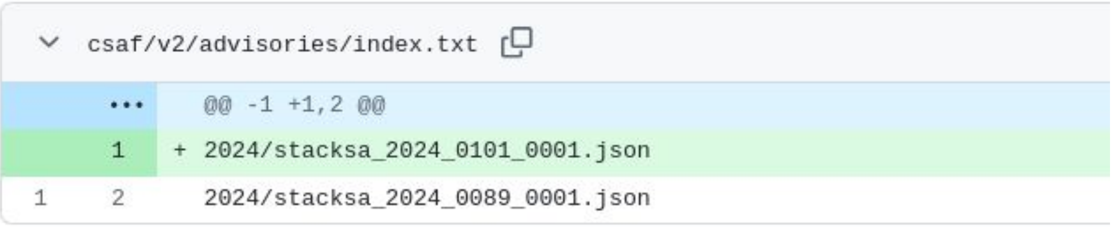
Generate signature and checksums

Modify changes.csv and index.txt



```
csaf/v2/advisories/changes.csv

      •••   @@ -1 +1,2 @@
        1 + "2024/stacksa_2024_0101_0001.json","2024-11-11T20:20:37Z"
1       2   "2024/stacksa_2024_0089_0001.json","2024-08-29T20:30:16Z"
```



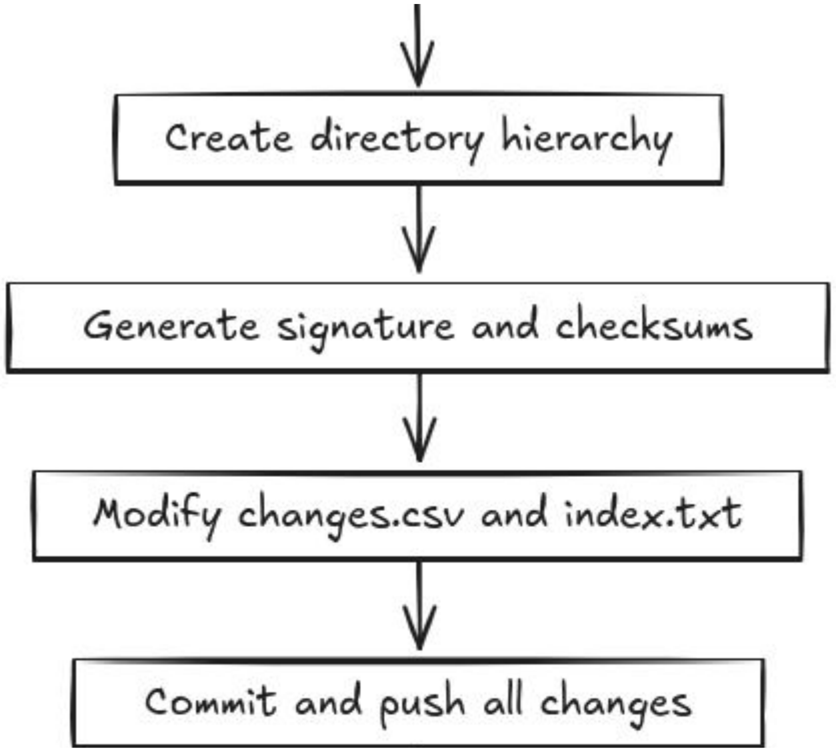
```
csaf/v2/advisories/index.txt

      •••   @@ -1 +1,2 @@
        1 + 2024/stacksa_2024_0101_0001.json
1       2   2024/stacksa_2024_0089_0001.json
```

TLP:CLEAR

Stackable

CSAF publishing workflow



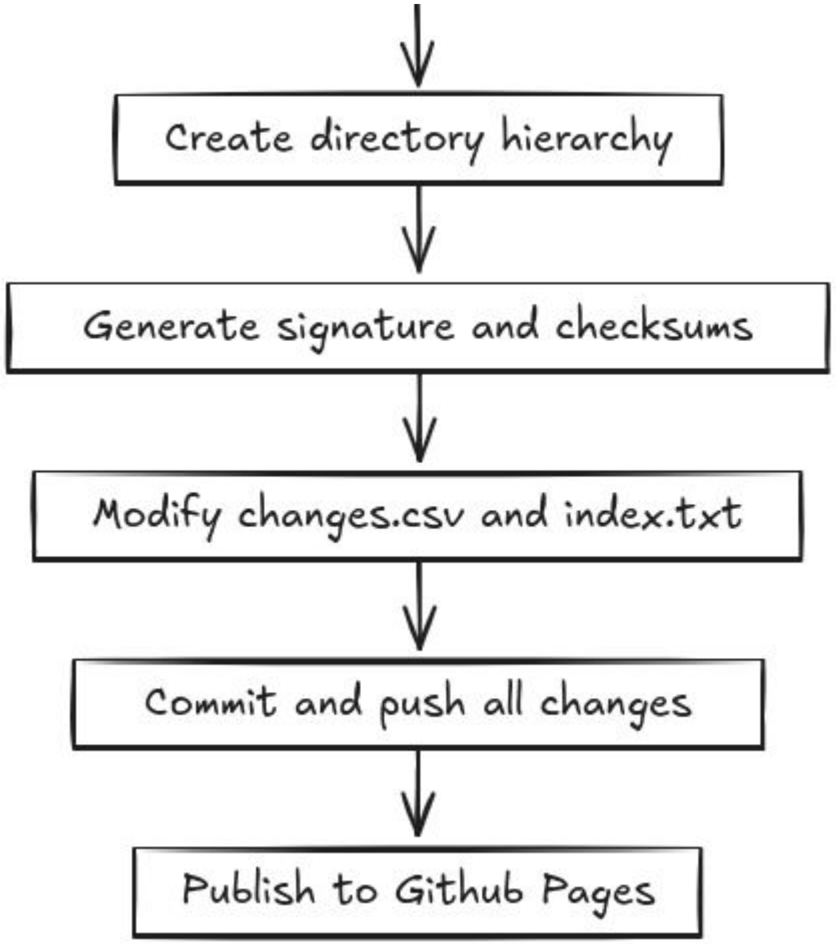
Create directory hierarchy

Generate signature and checksums

Modify changes.csv and index.txt

Commit and push all changes

CSAF publishing workflow



Create directory hierarchy

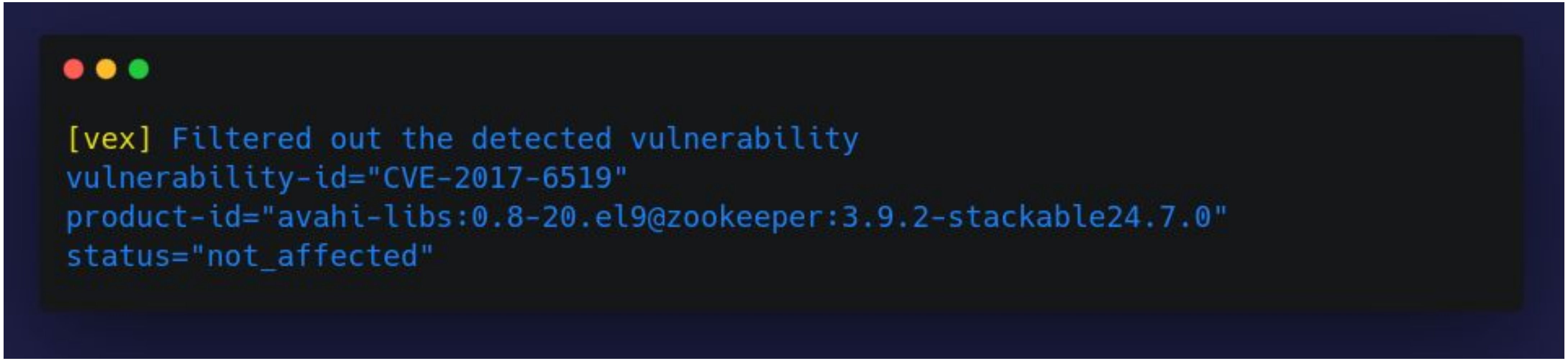
Generate signature and checksums

Modify changes.csv and index.txt

Commit and push all changes

Publish to Github Pages

Provide CSAF to Trivy



```
[vex] Filtered out the detected vulnerability
vulnerability-id="CVE-2017-6519"
product-id="avahi-libs:0.8-20.el9@zookeeper:3.9.2-stackable24.7.0"
status="not_affected"
```