



KubeCon



CloudNativeCon

North America 2024

Breaking Free from Vulnerability Scanning Noise: Automated VEX Aggregation for Accuracy

Teppei Fukuda, Aqua Security

- Exploitable Vulnerabilities
- What is VEX?
- VEX Challenges
- Introducing VEX Hub

About me



Teppei Fukuda

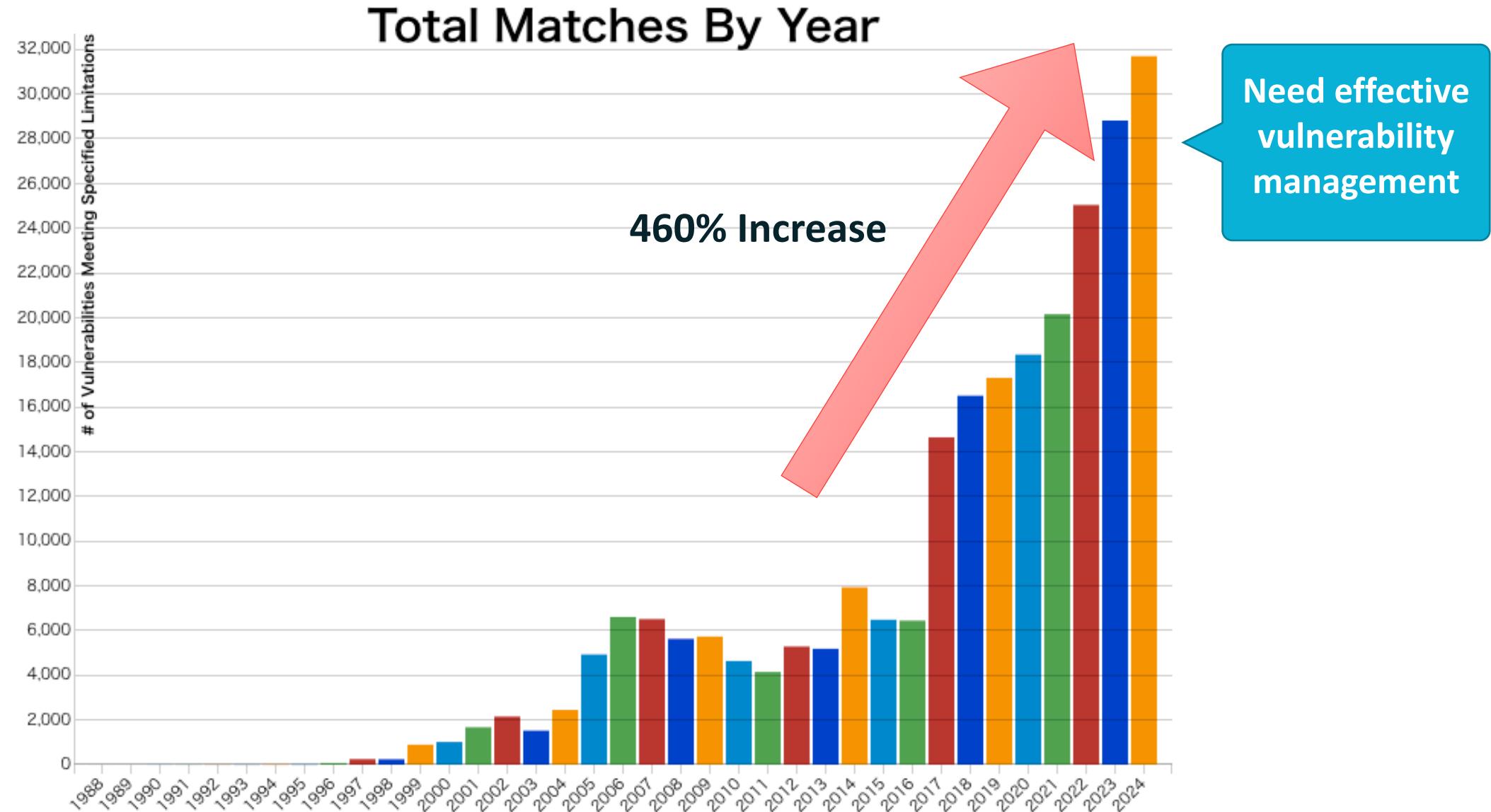
Open Source Team, Aqua Security

 @knqyf263

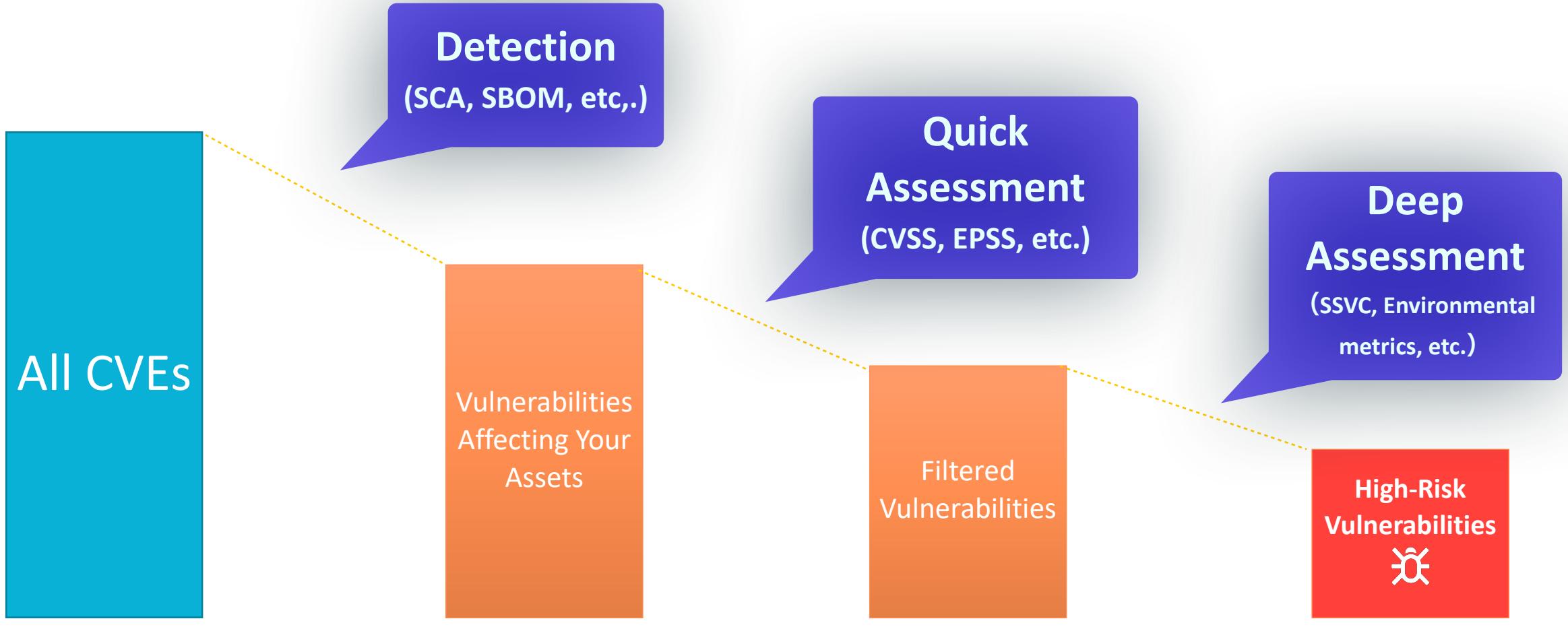
Creator of

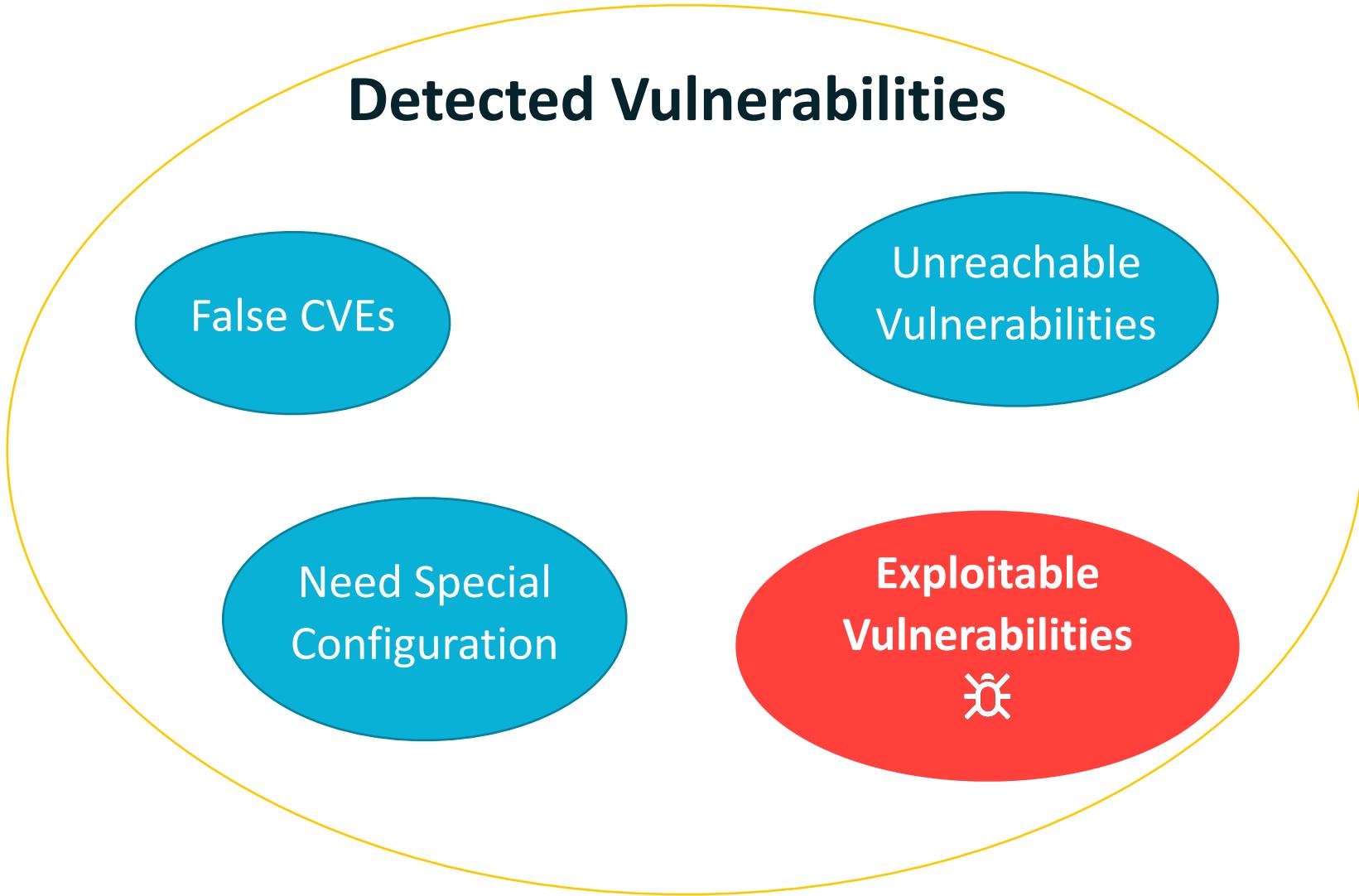


Total CVEs published by year



Vulnerability Management







liborm85 commented on Mar 7

Collaborator ...

@joaooviictorti This is essentially true. But [CVE-2024-25180](#) totally wrong because it says there is vulnerability in npm package, but that is not true, npm package is safe, that's the point.

Arbitrary Code Injection

The advisory has been revoked. It doesn't affect any version of package [pdfmake](#)

Backport docker/distribution patch to k8s 1.26 and 1.27 #122457

Closed

gburton1 opened this issue on Dec 22, 2023 · 7 comments



skitt commented on Dec 23, 2023

Member ...

You can see the code used (in the 1.28 branch) by looking in <https://github.com/kubernetes/kubernetes/tree/release-1.28/vendor/github.com/docker/distribution> – none of that code is affected by the CVE (the `/v2/_catalog` endpoint in Docker) in question.



Only 3% of Open Source Software Bugs Are Actually Attackable, Researchers Say

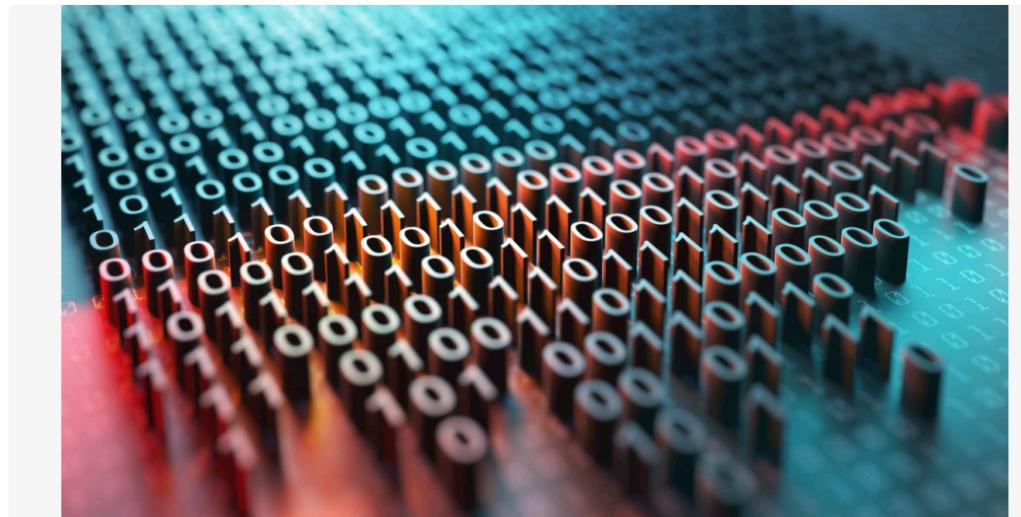
A new study says 97% of open source vulnerabilities linked to software supply chain risks are not attackable — but is "attackability" the best method for prioritizing bugs?



Ericka Chickowski, Contributing Writer

June 25, 2022

6 Min Read



Editor's Choice



Unfixed Microsoft Entra ID Authentication Bypass Threatens Hybrid IDs

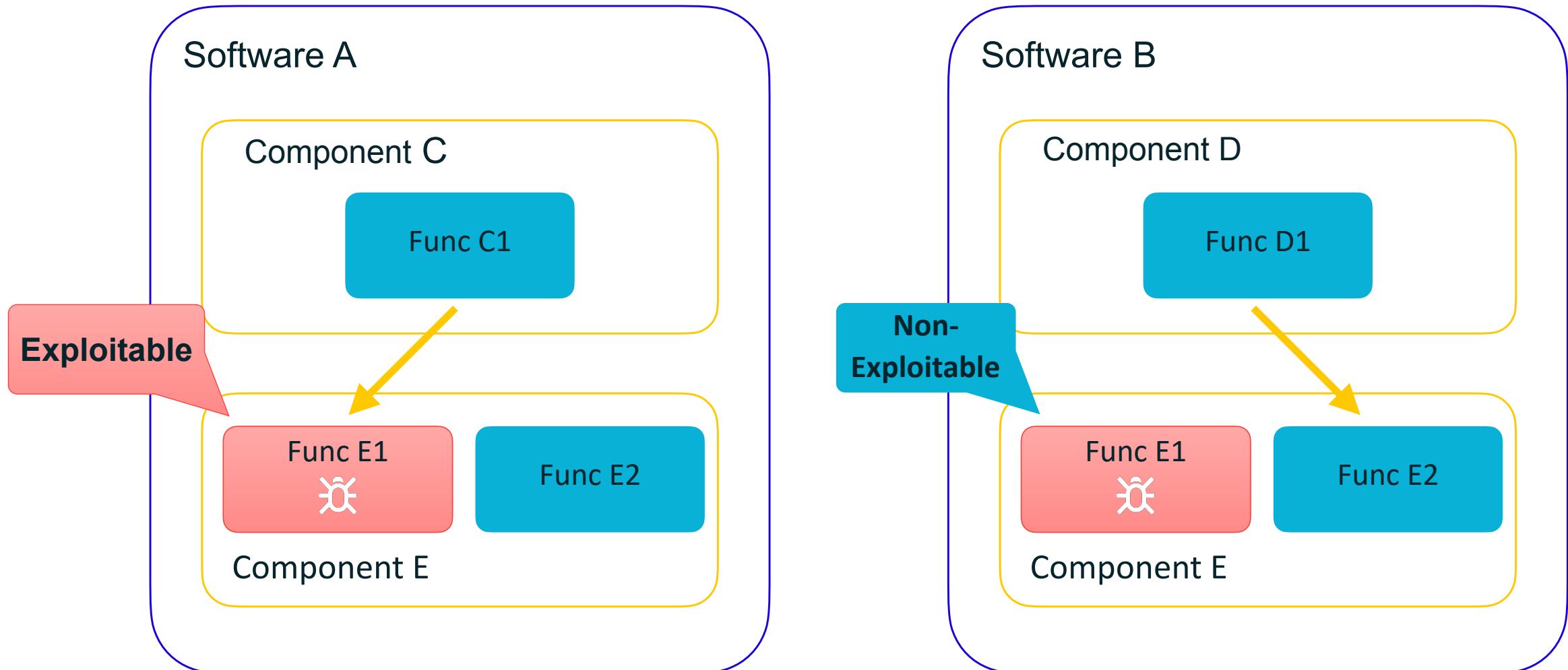
by Jai Vijayan, Contributing Writer

AUG 15, 2024

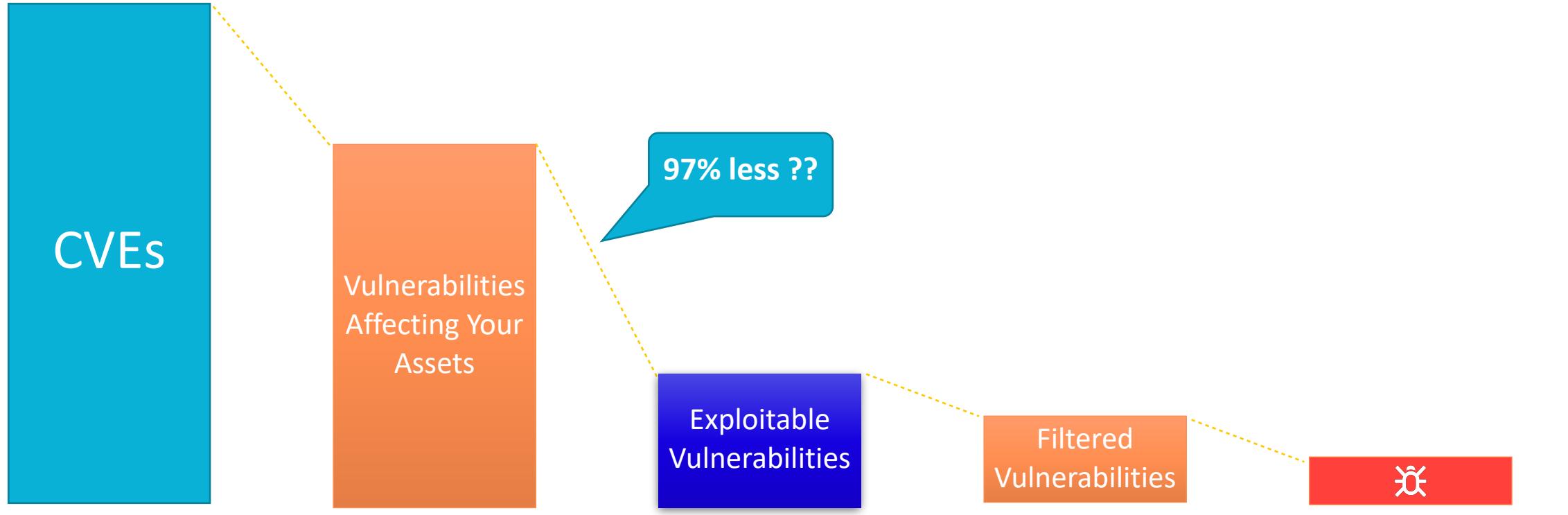
4 MIN READ

To that point: The report noted that **96% of vulnerable Log4J dependencies were not attackable.**

Reachability of Vulnerable Dependencies



Evaluate Exploitability





KubeCon



CloudNativeCon

North America 2024

Vulnerability Exploitability eXchange (VEX)

Vulnerability Exploitability eXchange (VEX)

- Originated from NTIA Multi-Stakeholder Process
- Coordinated by the VEX-WG facilitated by CISA
- Machine-readable format



VEX Statement

Vulnerability

+

Product

+

Status

VEX Implementations



OpenVEX

Example: OpenVEX

```
{  
  "@context": "https://openvex.dev/ns/v0.2.0",  
  ...  
  "version": 1,  
  "statements": [  
    {  
      "vulnerability": {"@id": "CVE-2023-2253"},  
      "products": [  
        {  
          "@id": "pkg:golang/k8s.io/kubernetes",  
          "subcomponents": [  
            {"@id": "pkg:golang/github.com/docker/distribution"}  
          ]  
        }  
      ]  
    },  
    {  
      "status": "not_affected",  
      "justification": "vulnerable_code_not_in_execute_path"  
    }  
  ]  
}
```

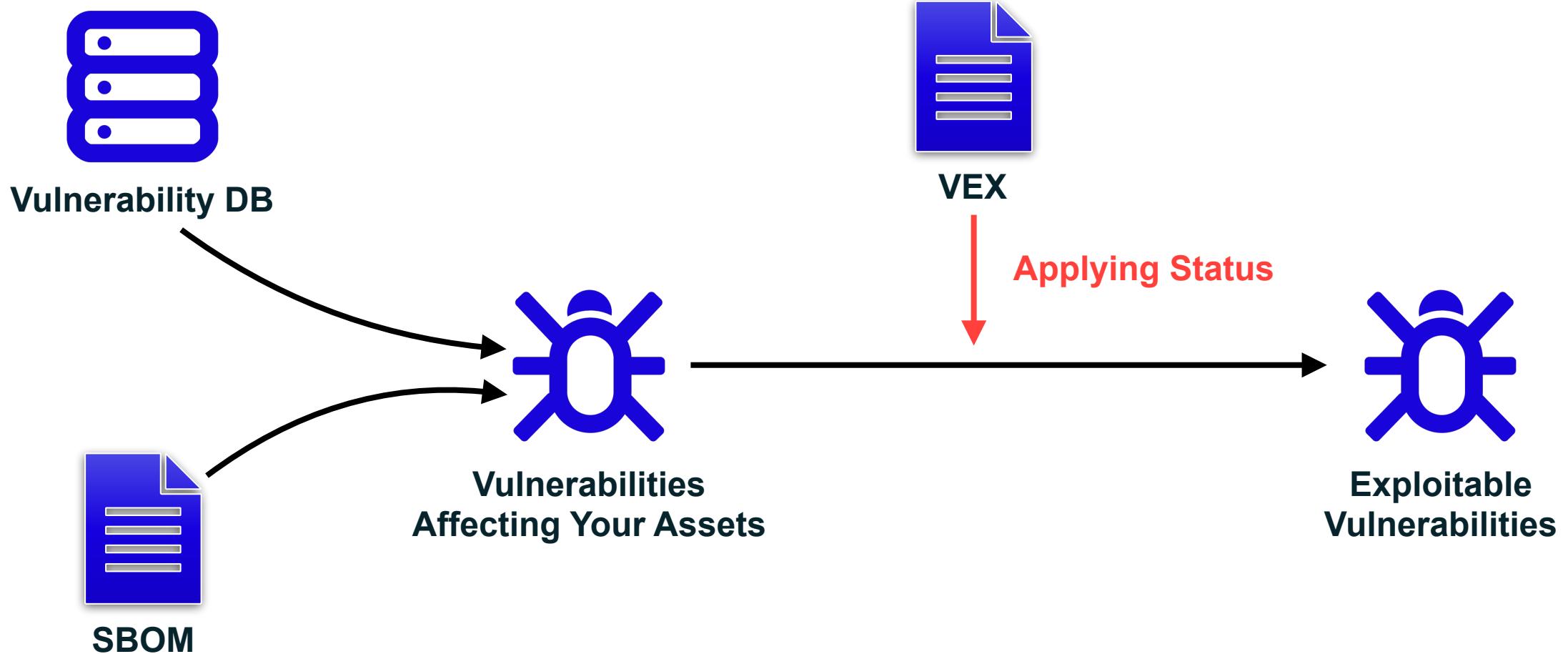
 Vulnerability

+

 Product

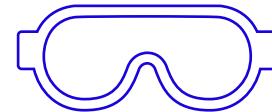
+

 Status

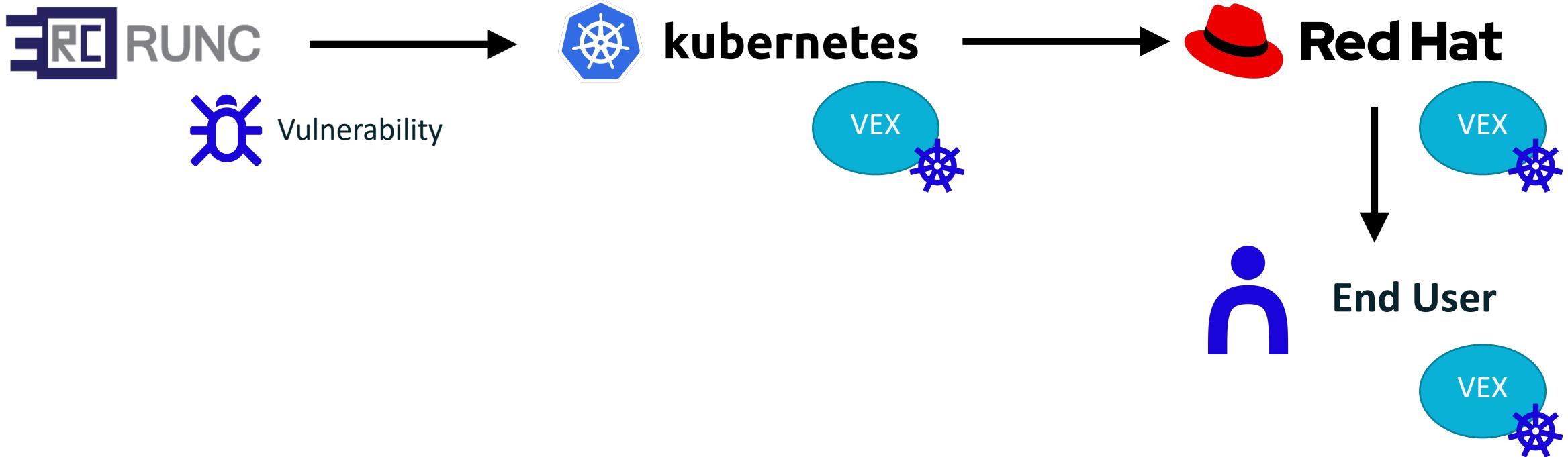


Who Can VEX?

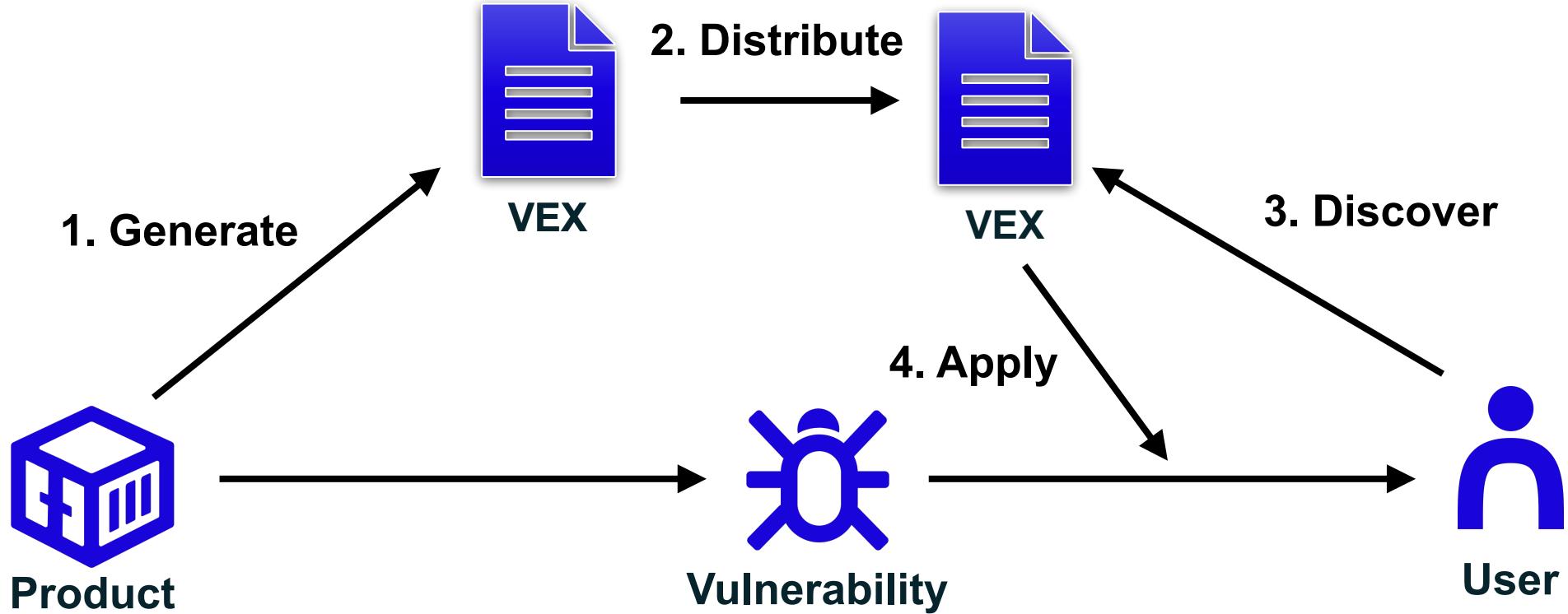
Anybody can VEX



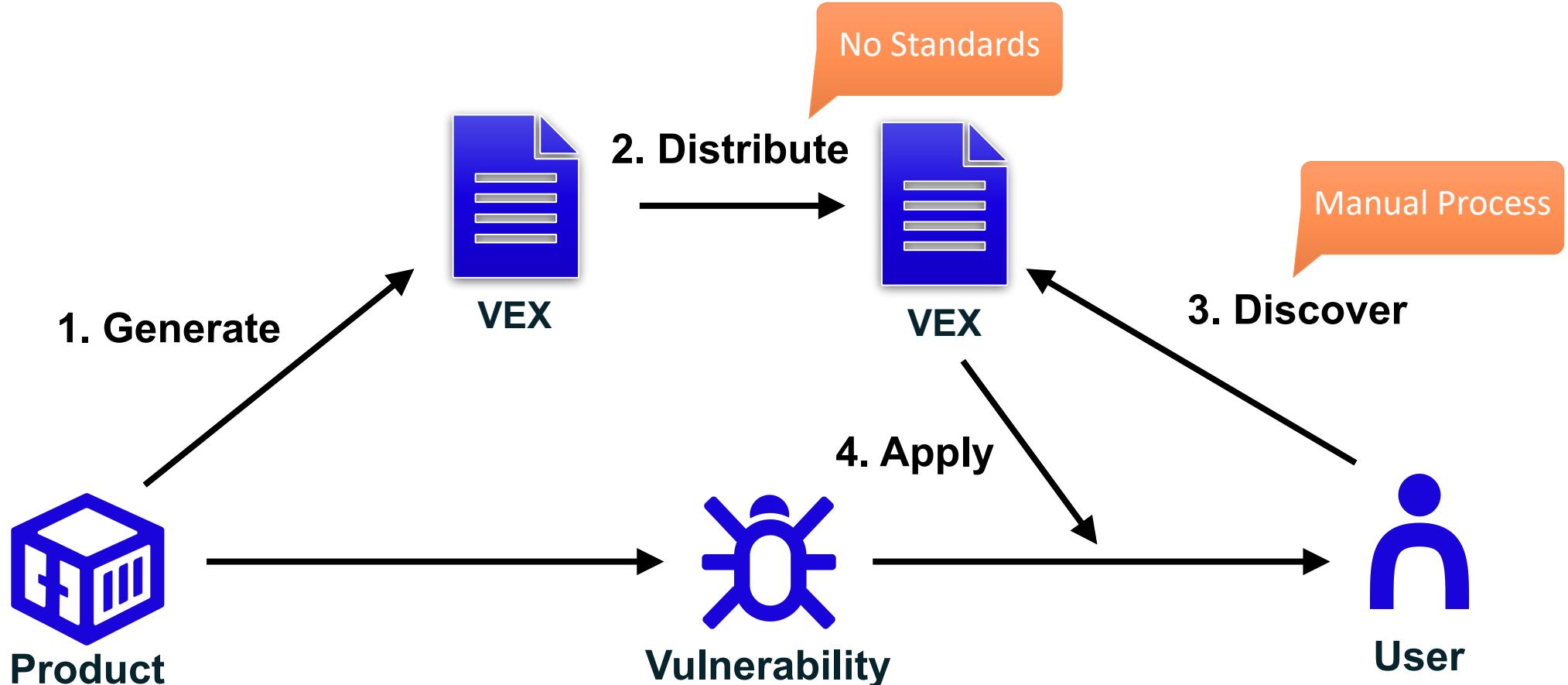
**3rd-Party
Security Researchers**



VEX Supply Chain



VEX Challenges



```
$ trivy image --vex /path/to/vex_file ...
```



KubeCon

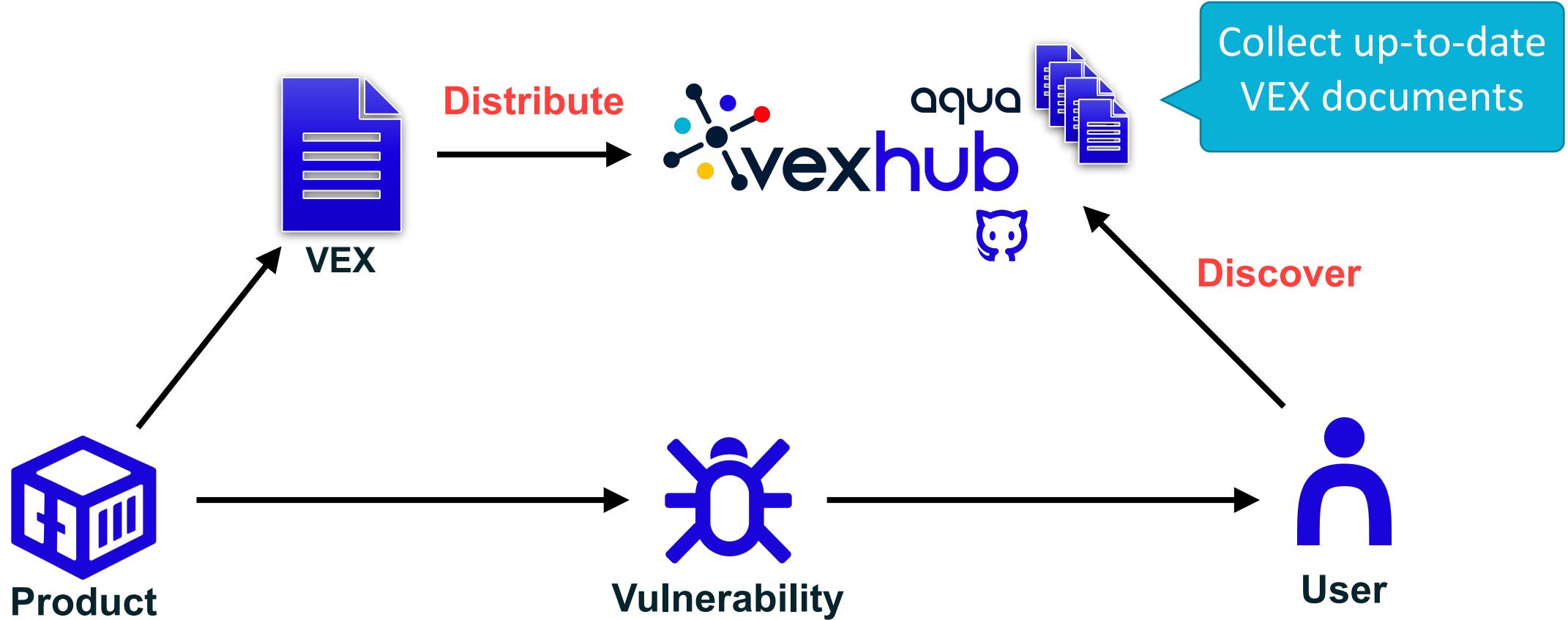


CloudNativeCon

North America 2024

VEX Hub

VEX Hub: Central Repository for VEX



Trivy & VEX Hub

```
$ trivy image --scanners vuln --vex repo -show-suppressed rancher/rke2-cloud-provider:v1.29.8-build20240910  
2024-10-26T11:13:02+04:00 [INFO] [vex] Updating repository... repo="default" url="https://github.com/aquasecurity/vexhub"
```

```
usr/local/bin/rke2-cloud-provider (gobinary)  
=====
```

Total: 0 (CRITICAL: 0)

Suppressed Vulnerabilities (Total: 1)

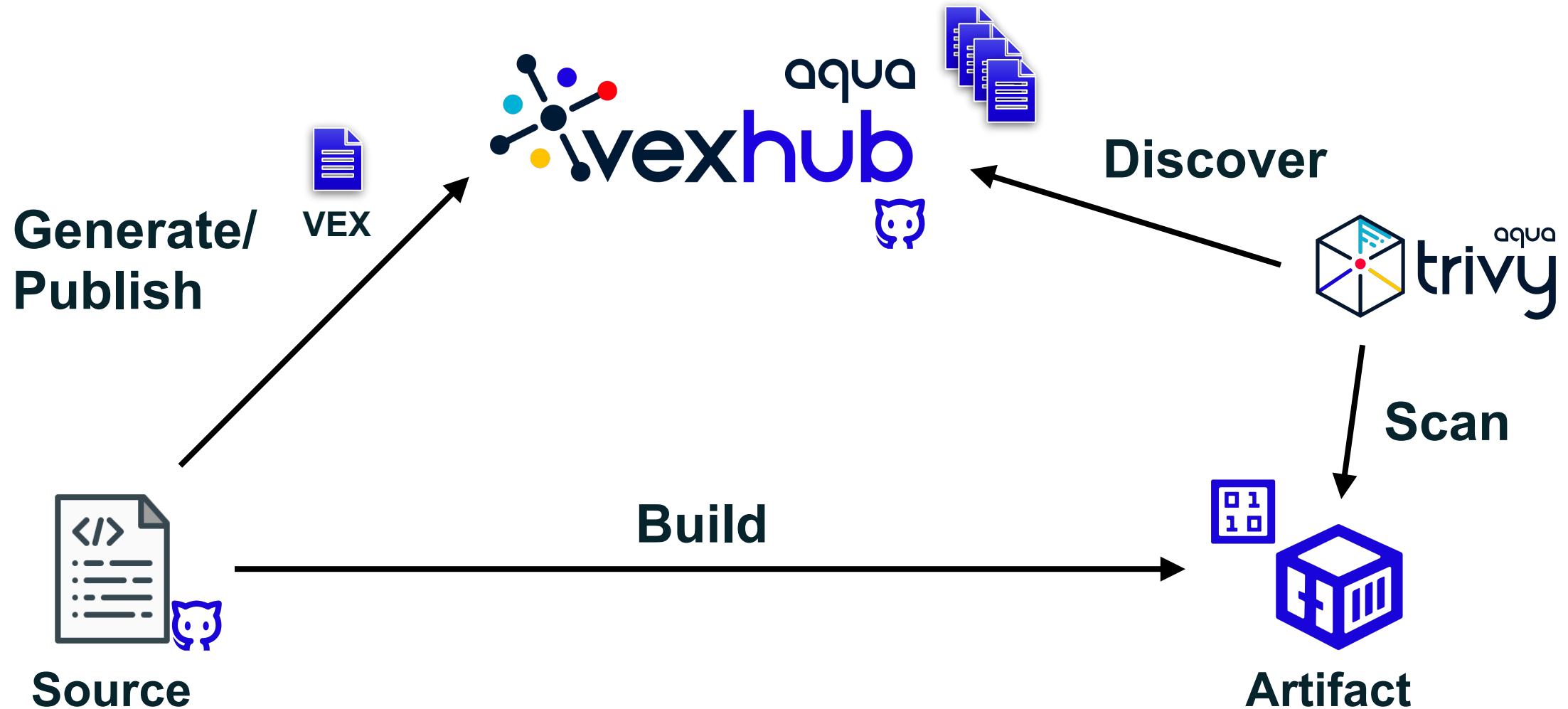
Library	Vulnerability	Severity	Status	Statement	Source
github.com/docker/docker	CVE-2024-41110	CRITICAL	not_affected	vulnerable_code_not_in_execute_path	VEX Repository: default (https://github.com/aquasecurity/vexhub)

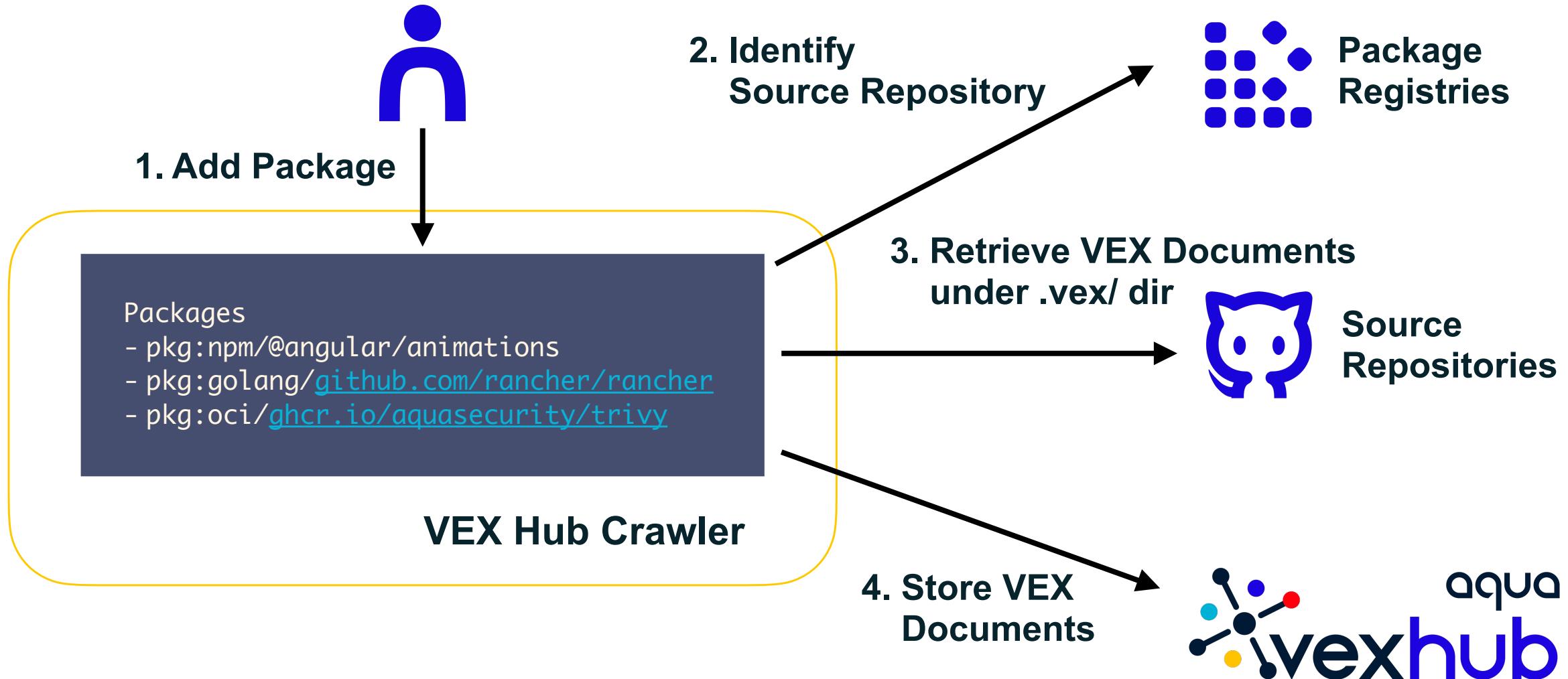


Auto-Discovery



Use Case: Build-Time Analysis for Scanning





Source Repository Resolution: npm

@angular/animations 

18.2.9 • Public • Published 2 days ago

 Readme

 Code  Beta

 1 Dependency

 9,943 Dependents

 790 Versions

Angular

The sources for this package are in the main [Angular](#) repo. Please file issues and pull requests against that repo.

Usage information and reference details can be found in [Angular documentation](#).

Install

```
> npm i @angular/animations
```



Repository

 github.com/angular/angular

.vex/ Directory

trivy/.vex/

DmitriyLewen chore(vex): add CVE-2024-34155, CVE-2024-34156 and CVE-2024-34158... ✎ ✓

Name	Last commit message
..	
oci.openvex.json	chore(vex): suppress openssl vulnerabilities (#7500)
trivy.openvex.json	chore(vex): add CVE-2024-34155, CVE-2024-34156 and CVE-2024-34158...

.vex/ Directory Proposal

openvex / spec Type / to search

Code Issues 16 Pull requests 1 Actions Projects Security Insights

Storing VEX files in a dedicated directory within Git repositories #46

Open knqyf263 opened this issue on May 1 · 8 comments

knqyf263 commented on May 1 · edited Contributor ...

Description

I would like to open a discussion regarding the file path convention for storing OpenVEX files within a Git repository. In the example of [Cilium](#), the filename `.openvex.json` is used. However, considering factors such as future OpenVEX version upgrades, the need to retain older files, storing individual VEX files for the OCI artifact and the project, and accommodating multiple VEX formats like OpenVEX and CSAF, I think it would be better to store VEX files under a dedicated directory like `.vex/` rather than using a single file.

Example

For example, a filename format would be like NAME.FORMAT.json for storing the VEX files. With this approach, the file path would look like this:

- `.vex/cilium-oci.openvex.json`
- `.vex/cilium-golang.openvex.json`
- `.vex/cilium.csaf.json`

Open in Under Discussion

Assignees
No one assigned

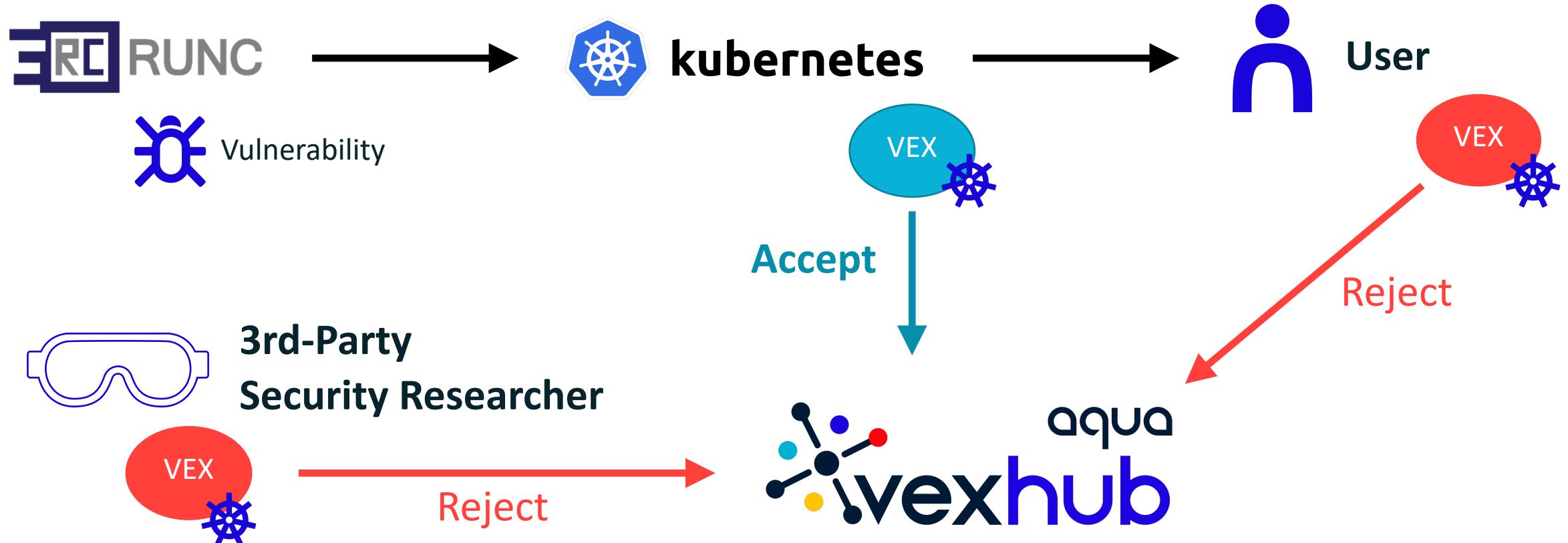
Labels
None yet

Projects
None yet

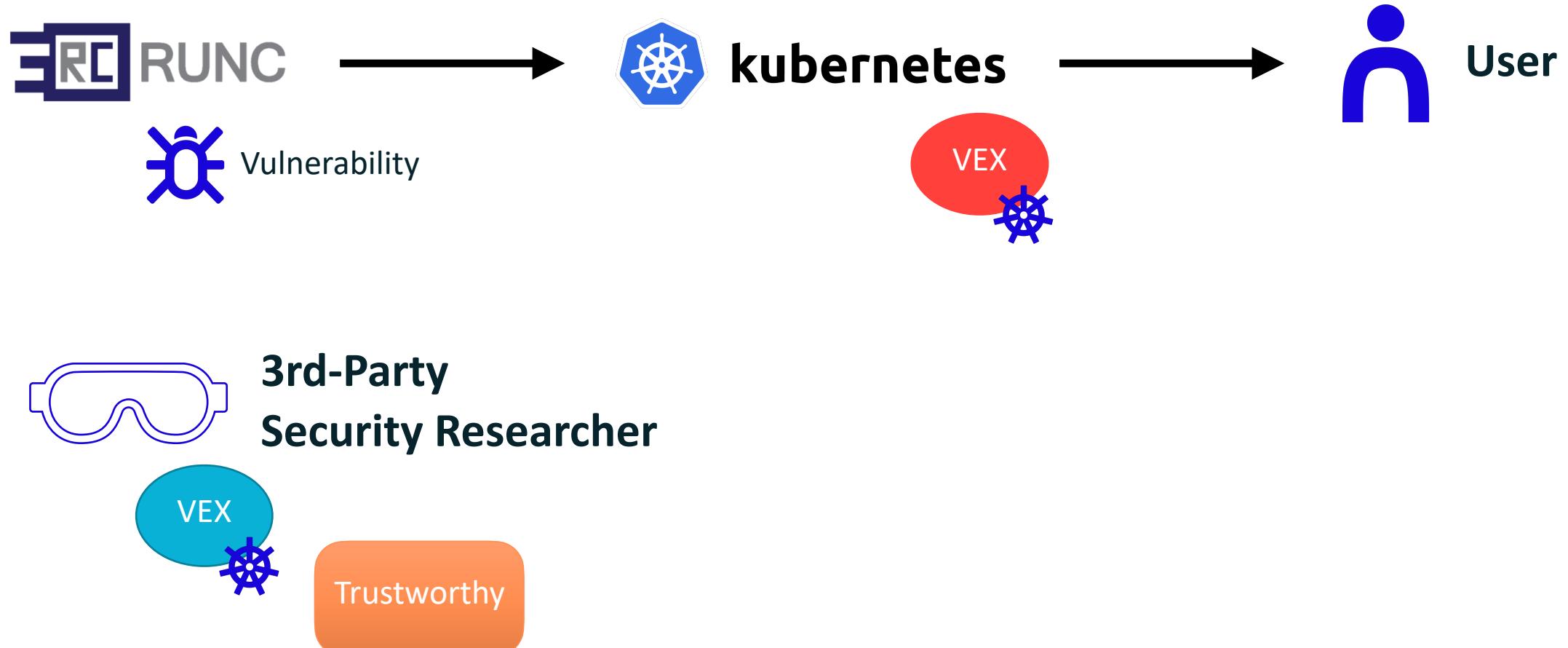
Milestone
No milestone

Development
No branches or pull requests

VEX Hub Trust Model: Trust Maintainers



Want to Trust 3rd-Party VEX?





KubeCon



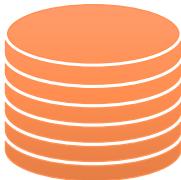
CloudNativeCon

North America 2024

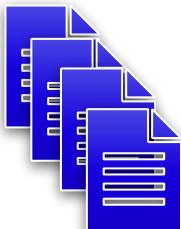
VEX Repository Specification



Manifest File



Index File



Collection of VEX Documents

[README](#) [Code of conduct](#) [Apache-2.0 license](#)

VEX Repository Specification v0.1

- [VEX Repository Specification v0.1](#)
 - [1. Versioning](#)
 - [2. Repository Manifest](#)
 - [2.1 Overview](#)
 - [2.2 File Location](#)
 - [2.3 Schema](#)
 - [2.4 Example](#)
 - [2.5 Field Descriptions and Usage Notes](#)
 - [Main Fields](#)
 - [Versions Subfields](#)
 - [Locations Subfields](#)
 - [3. Repository Structure](#)
 - [3.1 File Structure](#)
 - [3.2 index.json](#)
 - [3.3 VEX Documents](#)
 - [3.4 Usage Notes](#)





Manifest File

```
{  
  "name": "Example Org VEX Repository",  
  "description": "My VEX repository",  
  "versions": [  
    {  
      "spec_version": "0.1",  
      "locations": [  
        {  
          "url": "https://example.com/vex-hub/  
v0/vex-data-v0.tar.gz"  
        }  
      ],  
      "update_interval": "24h"  
    }  
  ]  
}
```



Index File

```
{  
  "updated_at": "2023-07-04T12:00:00Z",  
  "packages": [  
    {  
      "id": "pkg:deb/debian/curl",  
      "location": "pkg/deb/debian/curl/vex.json",  
      "format": "openvex"  
    },  
    {  
      "id": "pkg:npm/lodash",  
      "location": "pkg/npm/lodash/vex.json",  
      "format": "csaf"  
    }  
  ]  
}
```

Example: SUSE Rancher VEX Hub

The screenshot shows a GitHub repository page for 'vexhub' under the 'rancher' organization. The repository is public and has 1 branch and 7 commits. The main branch is selected. The repository contains several files and folders:

- docs**: Add CVE fix workflow (#16) - 3 weeks ago
- pkg/golang**: Update VEX Hub reports (#28) - yesterday
- reports**: Update VEX Hub reports (#28) - yesterday
- LICENSE**: Add CC-BY-4.0 license (#1) - last month
- README.md**: Add KB title in link (#14) - 3 weeks ago
- index.json**: Update VEX Hub reports (#20) - last week
- vex-repository.json**: Add initial VEX Hub repo config (#2) - last month

Below the file list, there are links to **README**, **License**, and **Security**. The main content area features a section titled **SUSE Rancher - VEX Hub repository** with the following text:

Rancher's VEX Hub repository contains a collection of [VEX](#) (Vulnerability-Exploitability eXchange) related reports for Rancher, RKE2, K3s, Harvester, Longhorn and other container and cloud native solutions images from SUSE.

For more information about SUSE's VEX Hub initiative, please consult the knowledge base article [KB 000021573 - How to use SUSE Rancher's VEX Reports](#).

<https://github.com/rancher/vexhub>

Multiple VEX Repositories in Trivy



1. Discover
(Primary)

2. Discover
(Secondary)

```
repositories:  
- name: rancher-vexhub  
  url: https://github.com/rancher/vexhub  
- name: aqua-vexhub  
  url: https://github.com/aquasecurity/vexhub
```



VEX Hub



VEX Repository Specification

Summary

