KubeCon | CloudNativeCon

North America 2024

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

Teppei Fukuda, Aqua Security

Agenda

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

About me

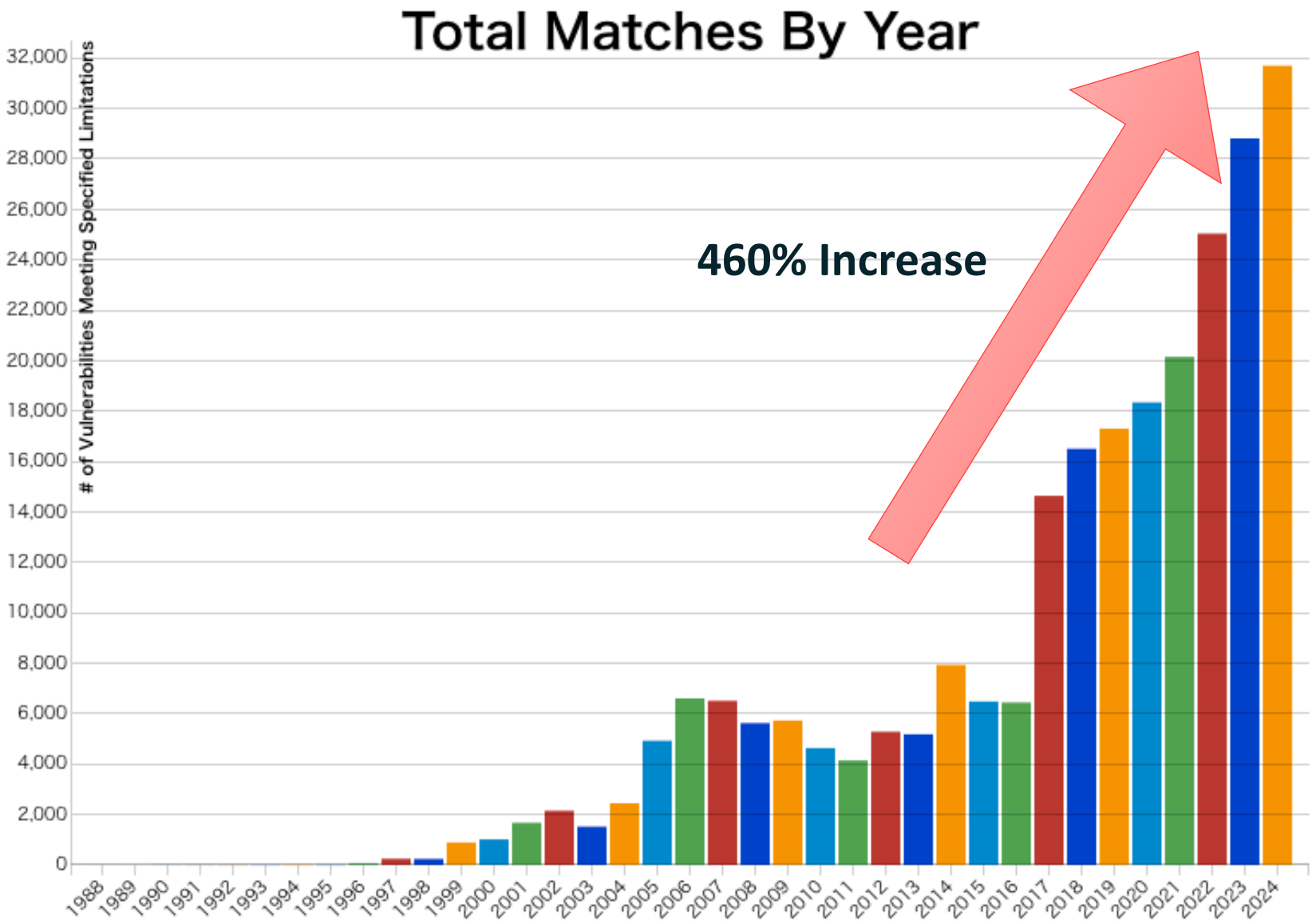
Teppei Fukuda

Open Source Team, Aqua Security

@knqyf263

Creator of aqua trivy

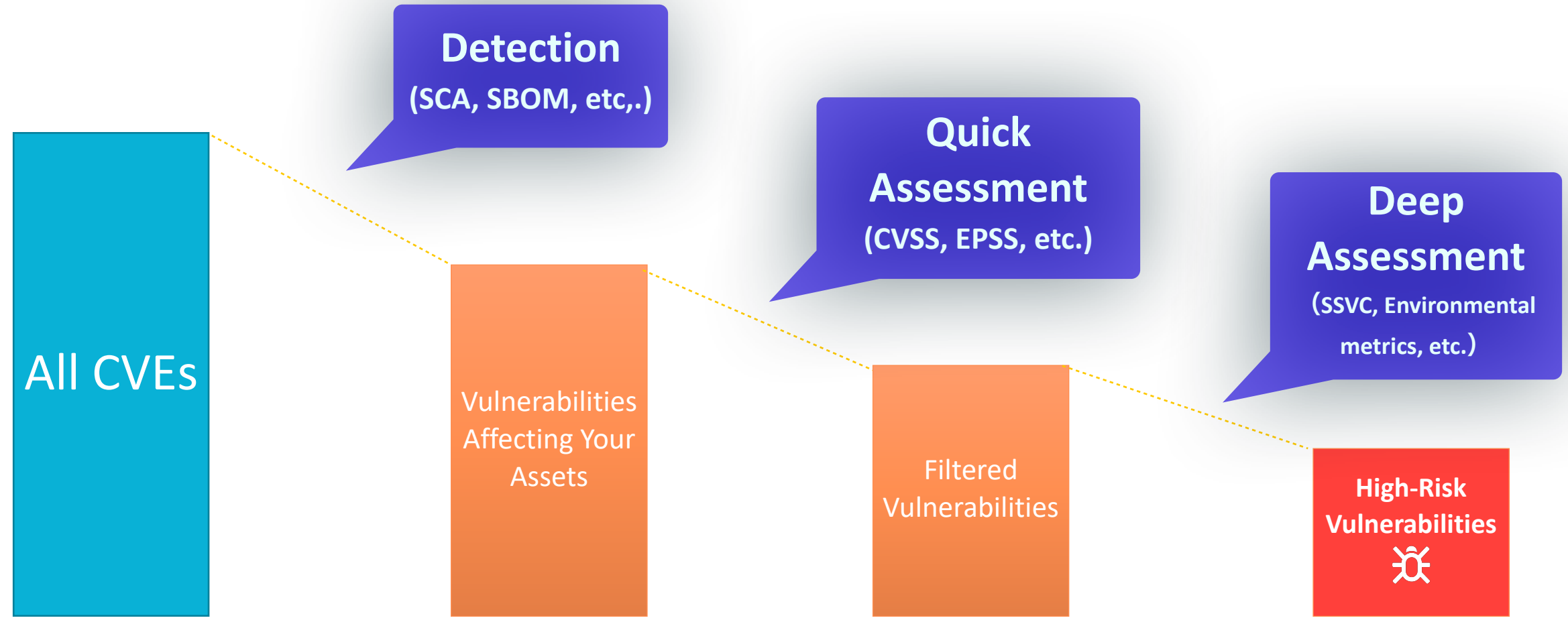
Total CVEs published by year



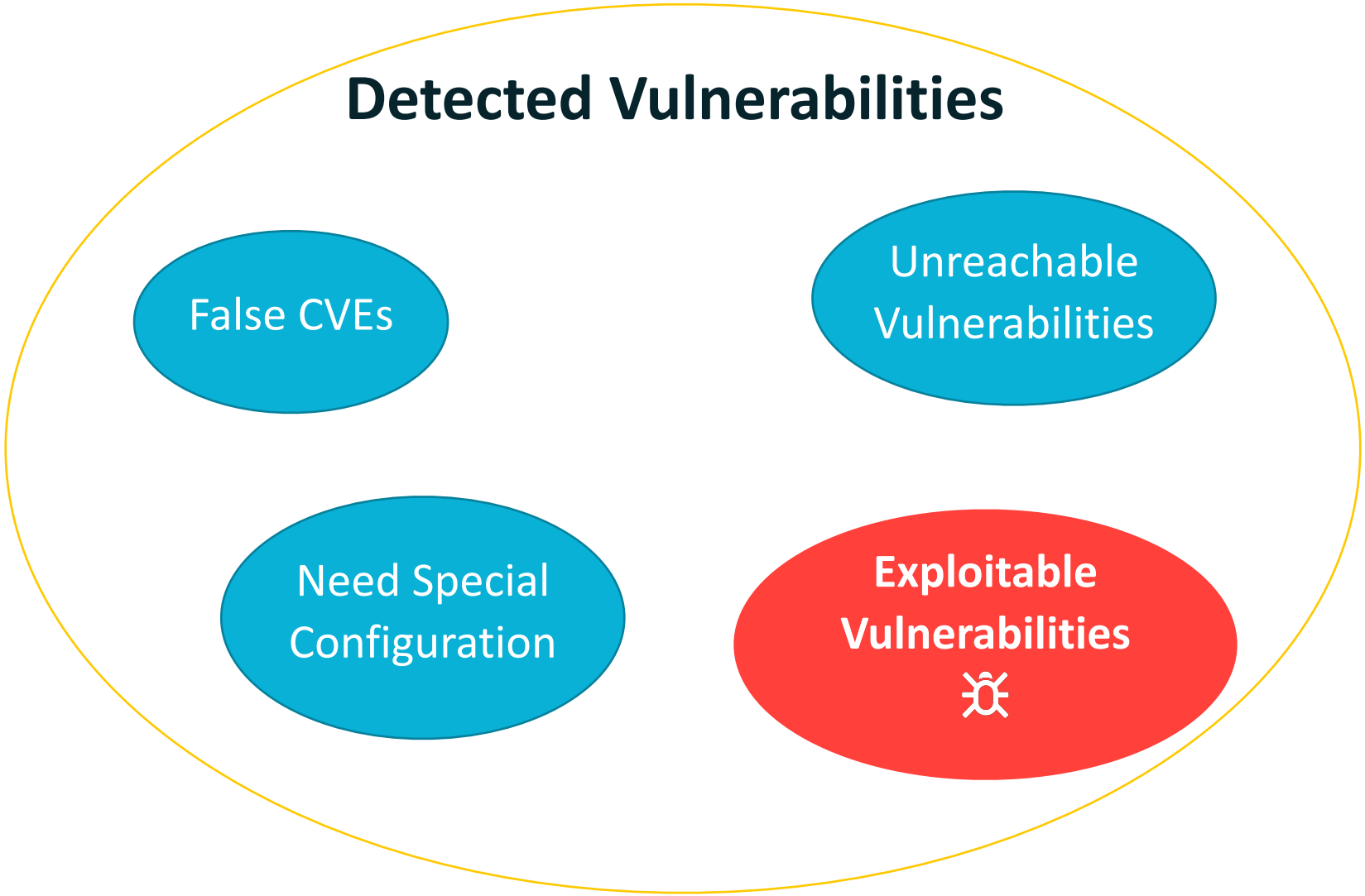
Need effective vulnerability management

https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all&isCpeNameSearch=false

Vulnerability Management



Exploitable Vulnerabilities



False CVEs

liborm85 commented on Mar 7 — Collaborator

@joaoviictorti 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The advisory has been revoked.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

https://github.com/bpampuch/pdfmake/issues/2702

Unreachable Vulnerabilities

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.

https://github.com/kubernetes/kubernetes/issues/122457

Attackable Vulnerabilities

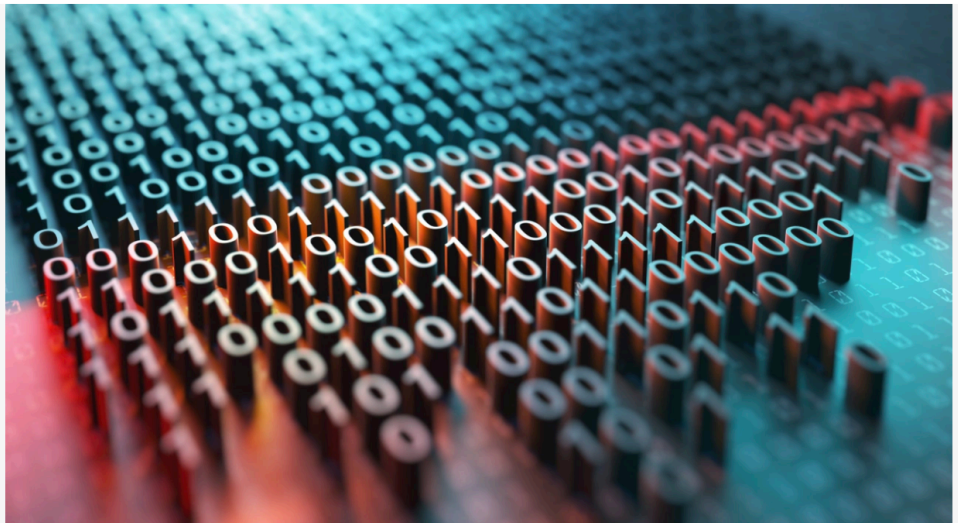
Only 3% of Open Source Software Bugs Are Actually Attackable, Researchers Say

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

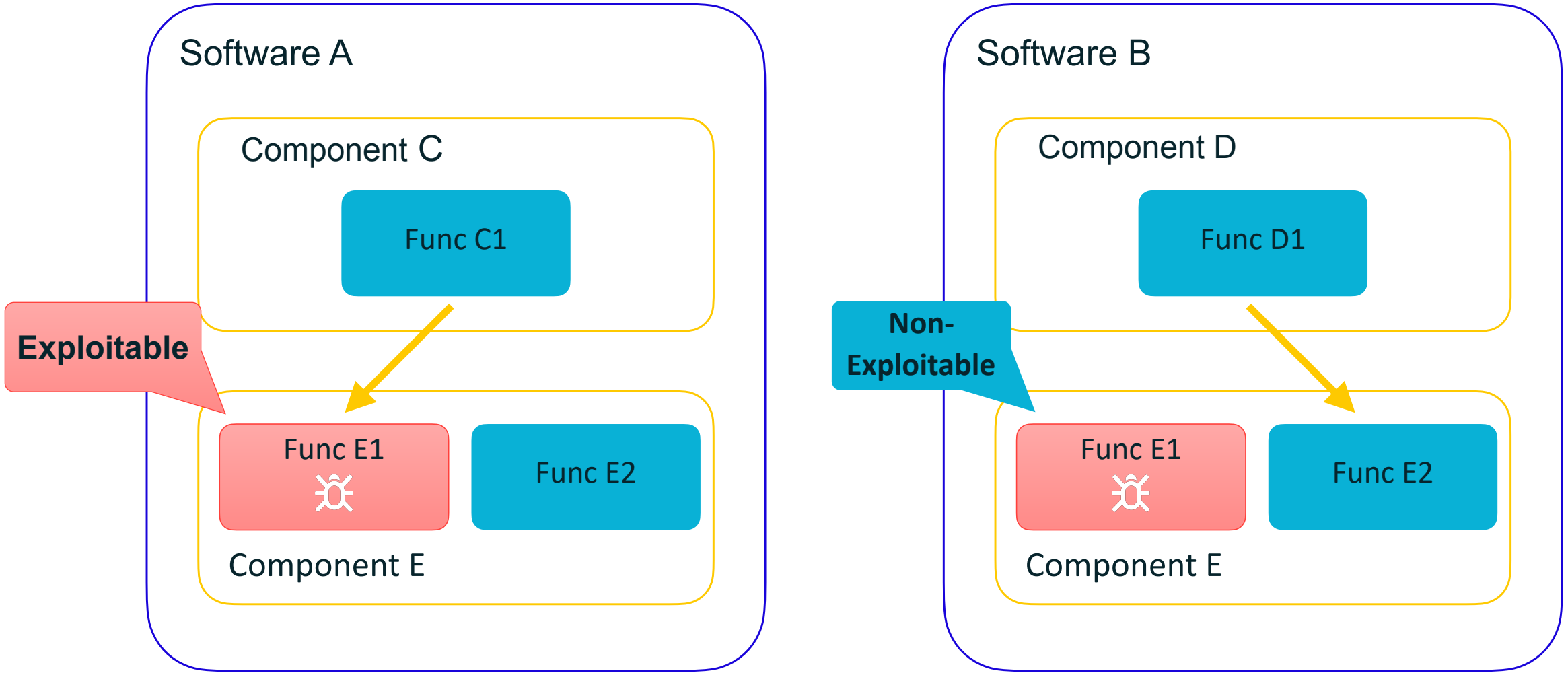
by **Jai Vijayan, Contributing Writer**

AUG 15, 2024 4 MIN READ

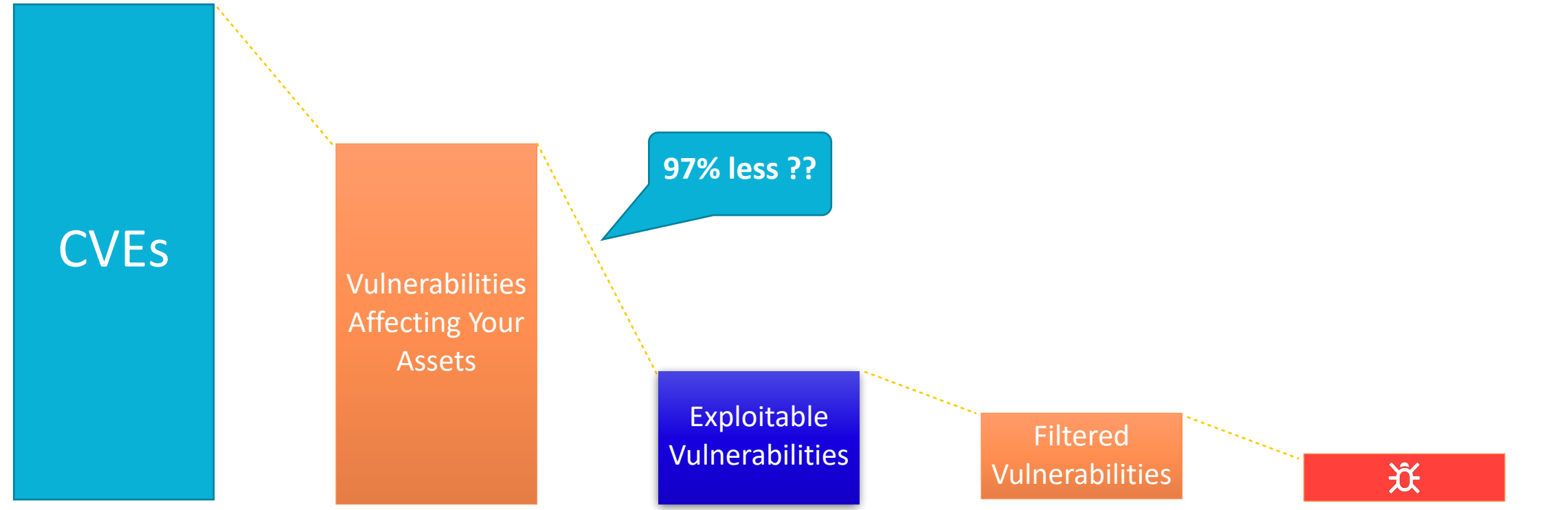
To that point: The report noted that 96% of vulnerable Log4J dependencies were not attackable.

https://www.darkreading.com/application-security/open-source-software-bugs--attackability

Reachability of Vulnerable Dependencies



Evaluate Exploitability



aqua

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

CSAF

SPDX

CycloneDX

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

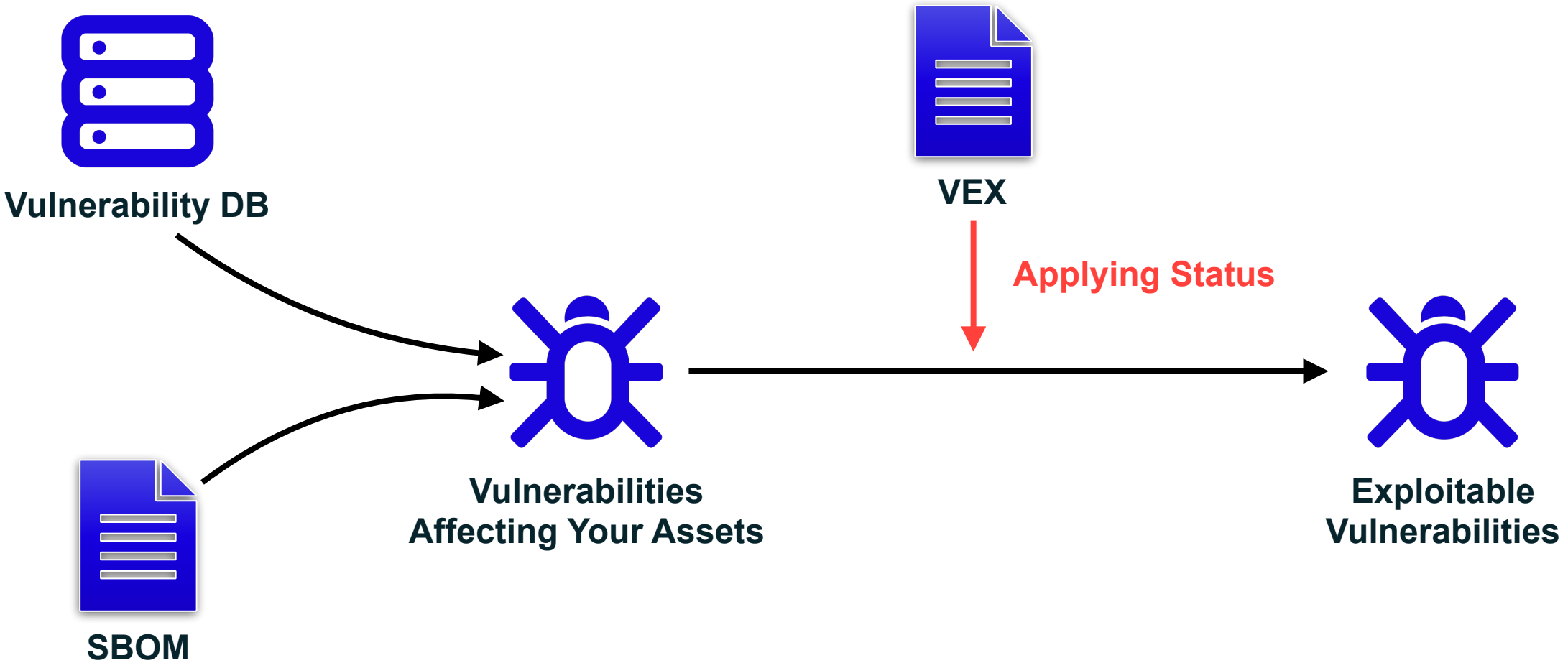
+

Product

+

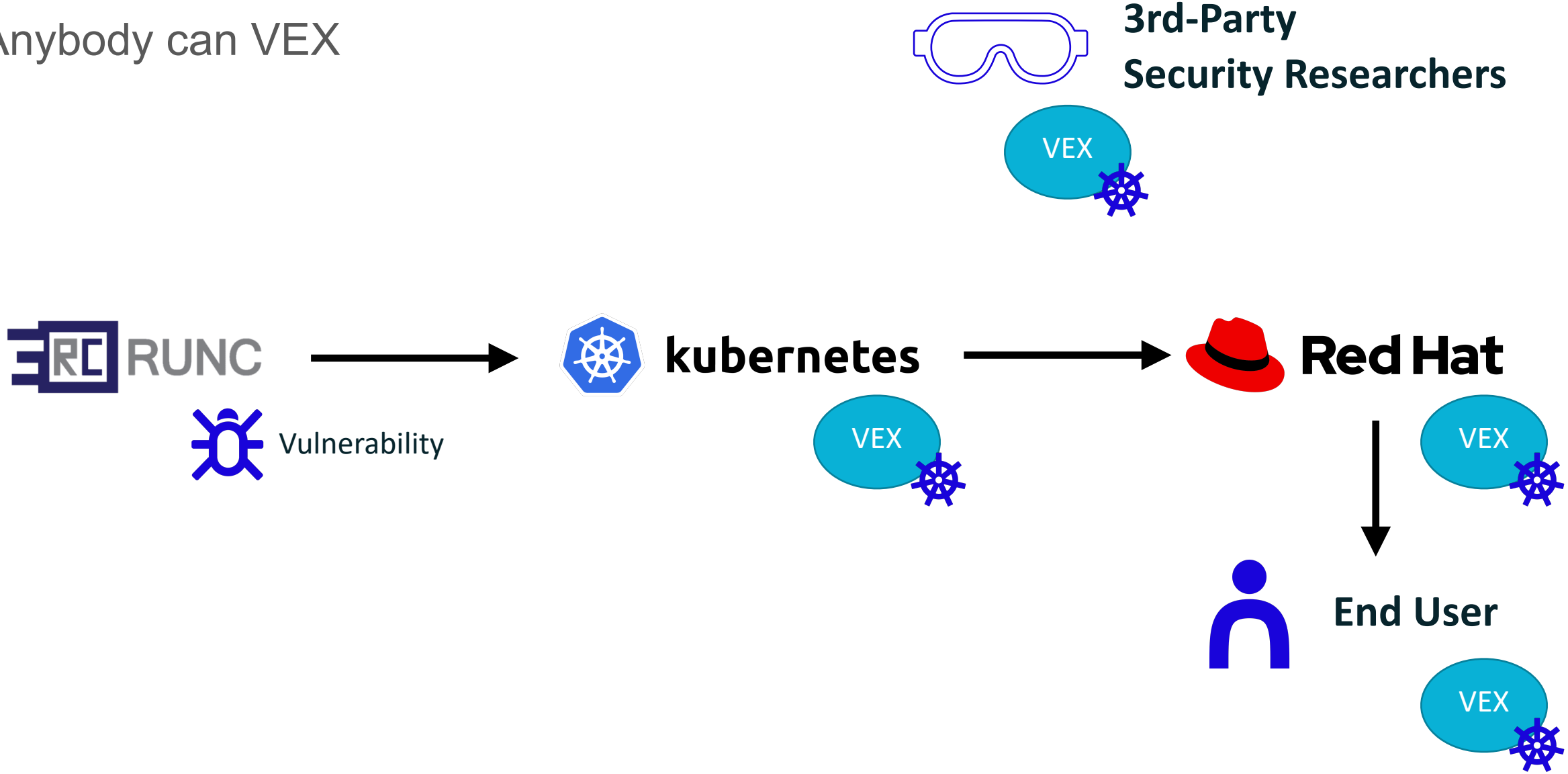
Status

VEX Workflow

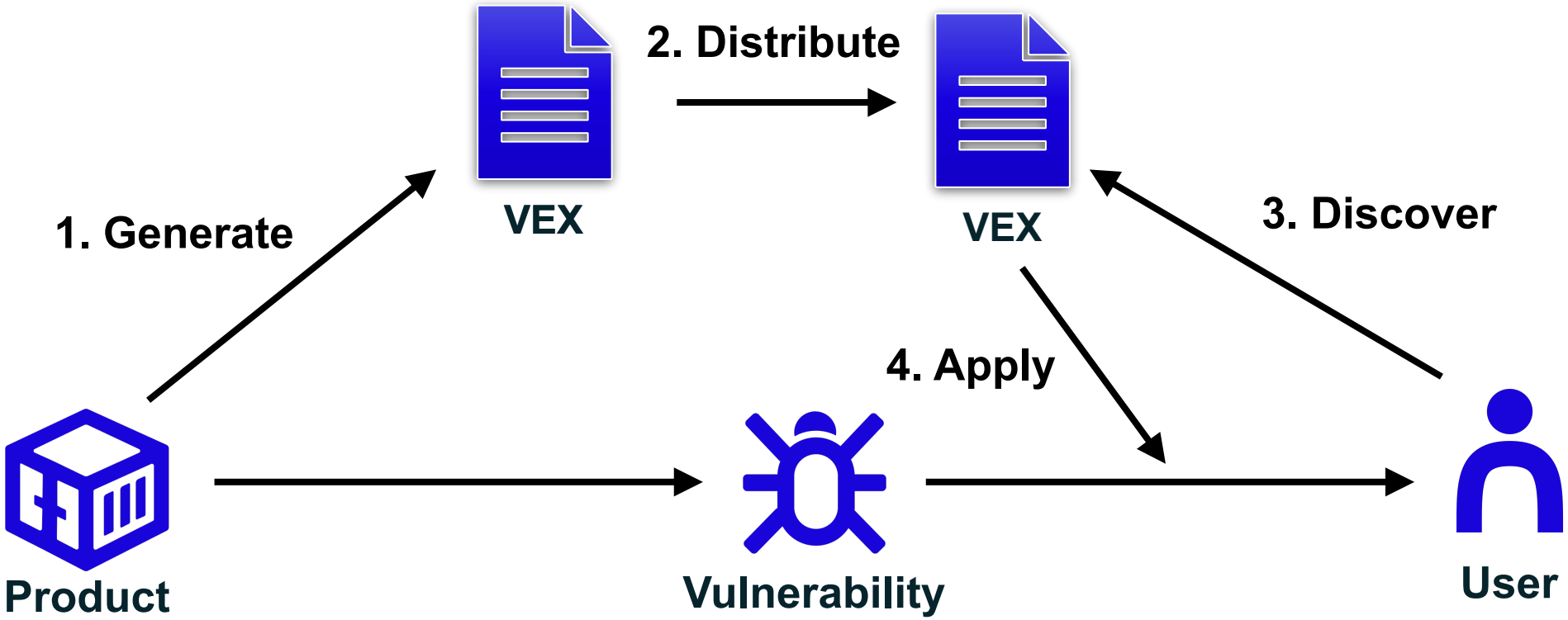


Who Can VEX?

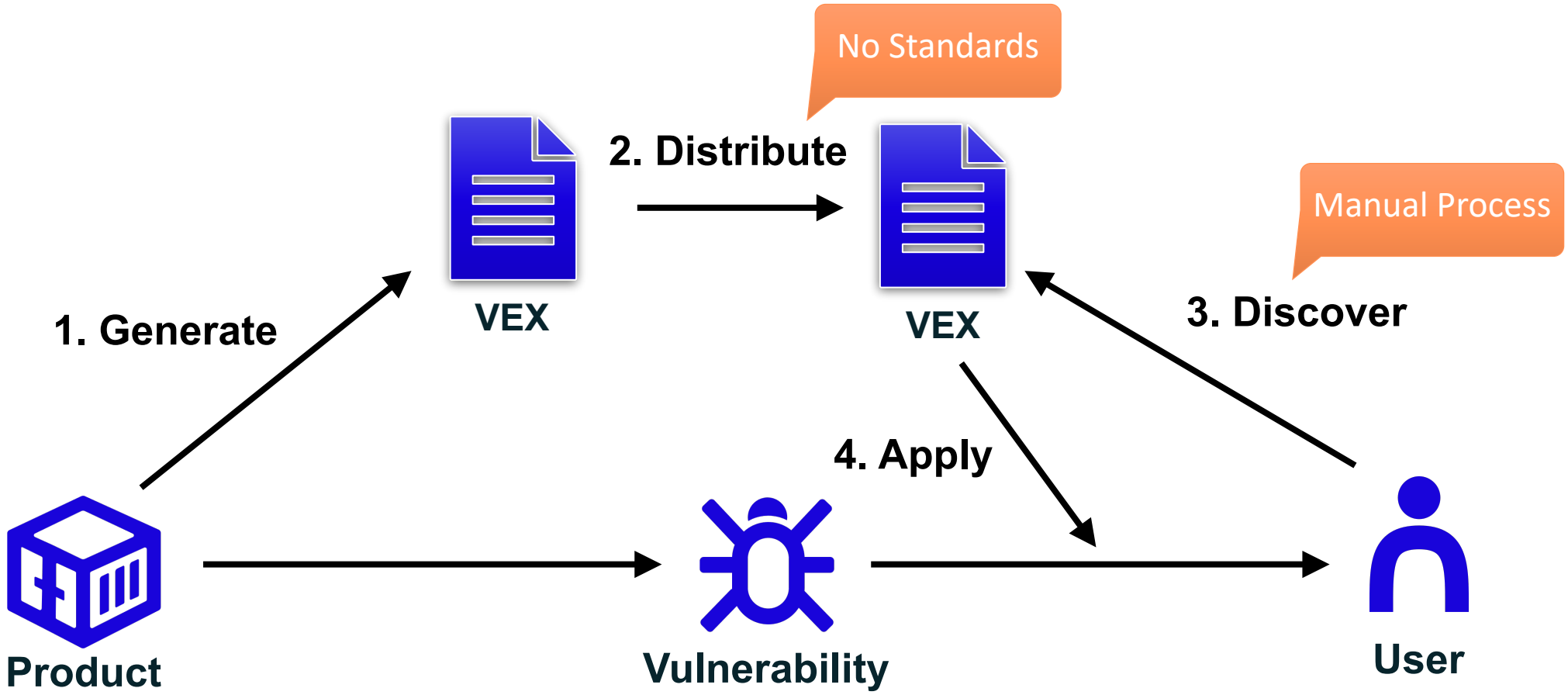
Anybody can VEX



VEX Supply Chain



VEX Challenges



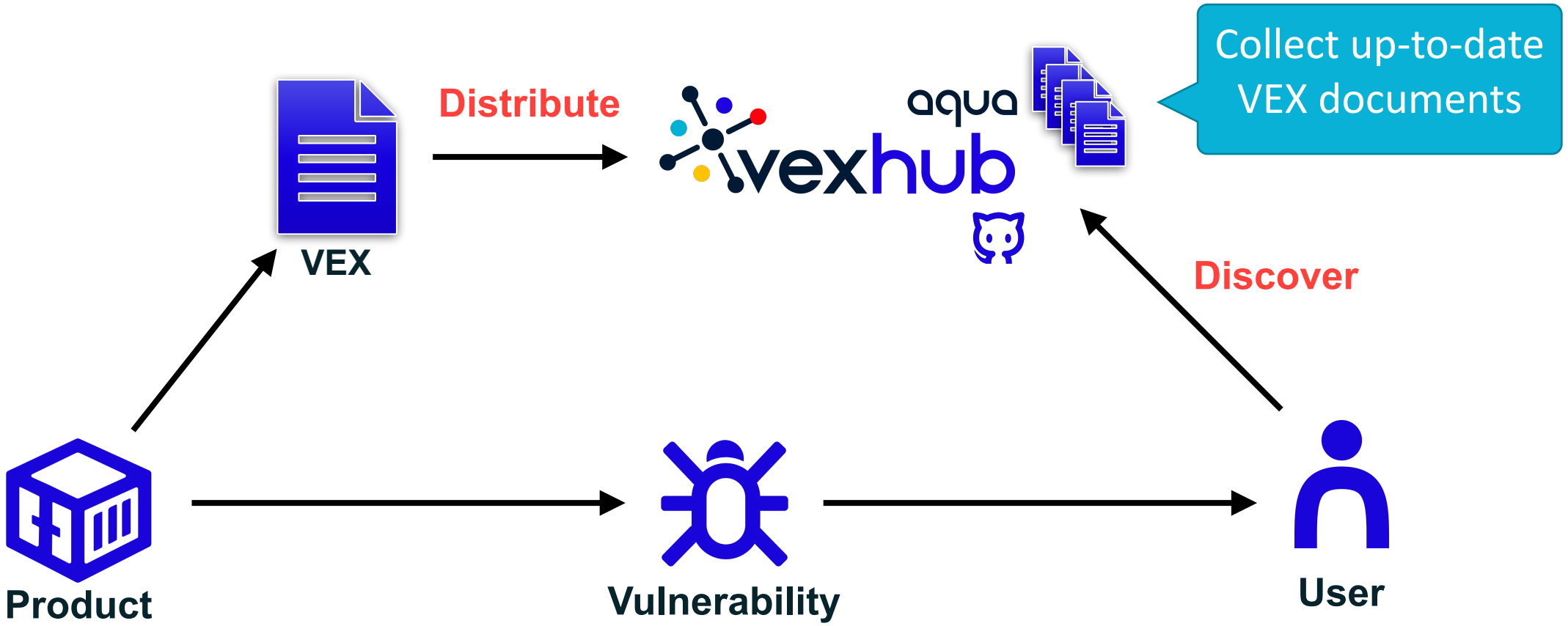

```
$ trivy image --vex /path/to/vex_file ...
```

aqua

KubeCon | CloudNativeCon
North America 2024

VEX Hub

VEX Hub: Central Repository for VEX

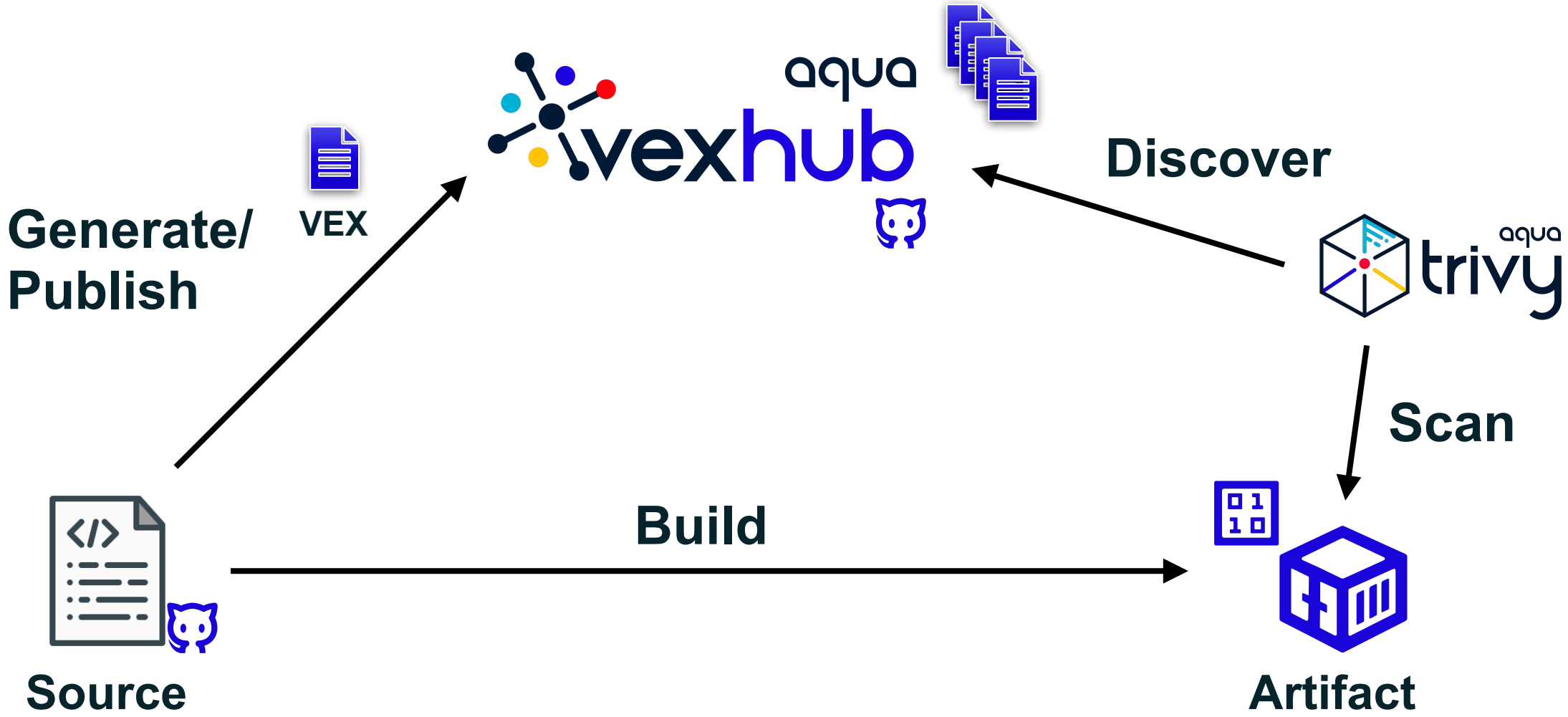


Trivy & VEX Hub

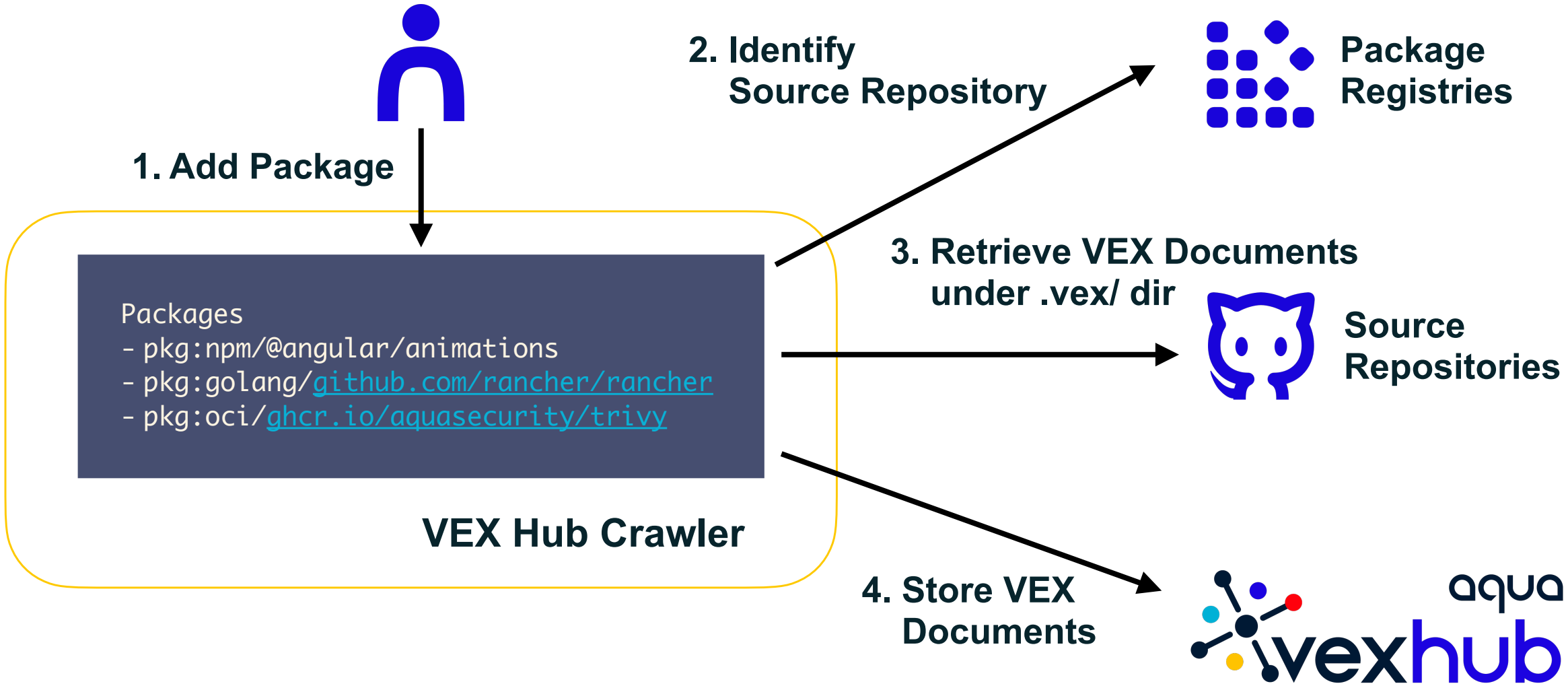

```
$ trivy image --scanners vuln --vex repo --show-suppressed rancher/rke2-cloud-provider:v1.29.8-build20240910
2024-10-26T11:13:02+04:00       INFO    [vex] Updating repository...    repo="default" url="https://github.com/aquasecurity/vexhub"

usr/local/bin/rke2-cloud-provider (gobinary)
============================================
Total: 0 (CRITICAL: 0)

Suppressed Vulnerabilities (Total: 1)
┌──────────────────────┬─────────────────┬──────────┬──────────────┬──────────────────────────────┬──────────────────────────────────────────┐
│       Library        │  Vulnerability  │ Severity │    Status    │          Statement           │                  Source                  │
├──────────────────────┼─────────────────┼──────────┼──────────────┼──────────────────────────────┼──────────────────────────────────────────┤
│ github.com/docker/   │ CVE-2024-41110  │ CRITICAL │ not_affected │ vulnerable_code_not_in_      │ VEX Repository: default                  │
│ docker               │                 │          │              │ execute_path                 │ (https://github.com/aquasecurity/vexhub) │
└──────────────────────┴─────────────────┴──────────┴──────────────┴──────────────────────────────┴──────────────────────────────────────────┘
```

Auto-Discovery

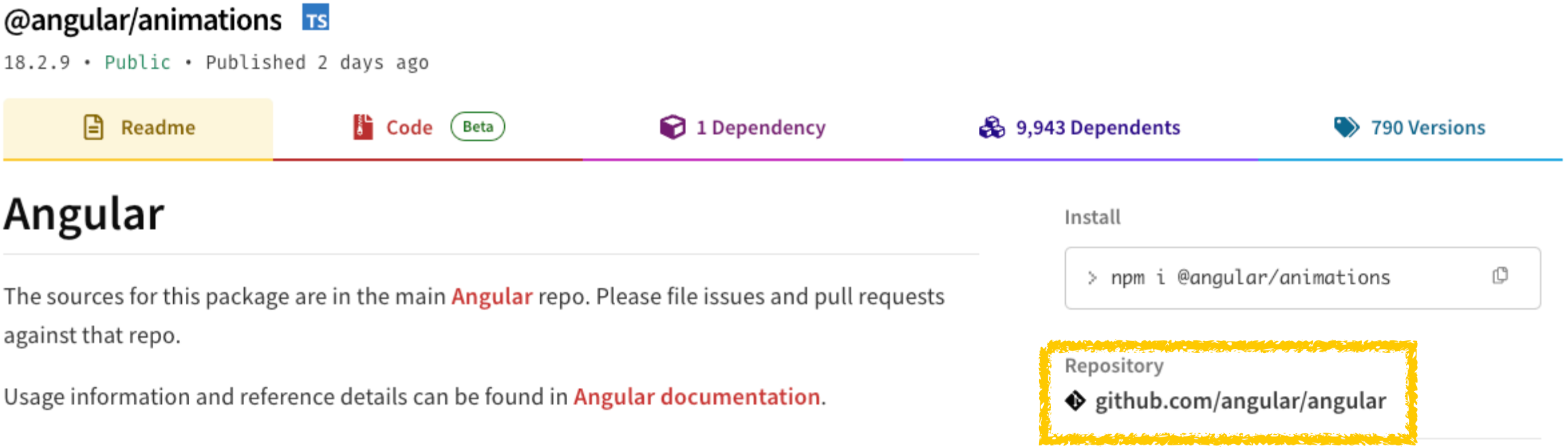
Use Case: Build-Time Analysis for Scanning



VEX Hub Crawler



Source Repository Resolution: npm



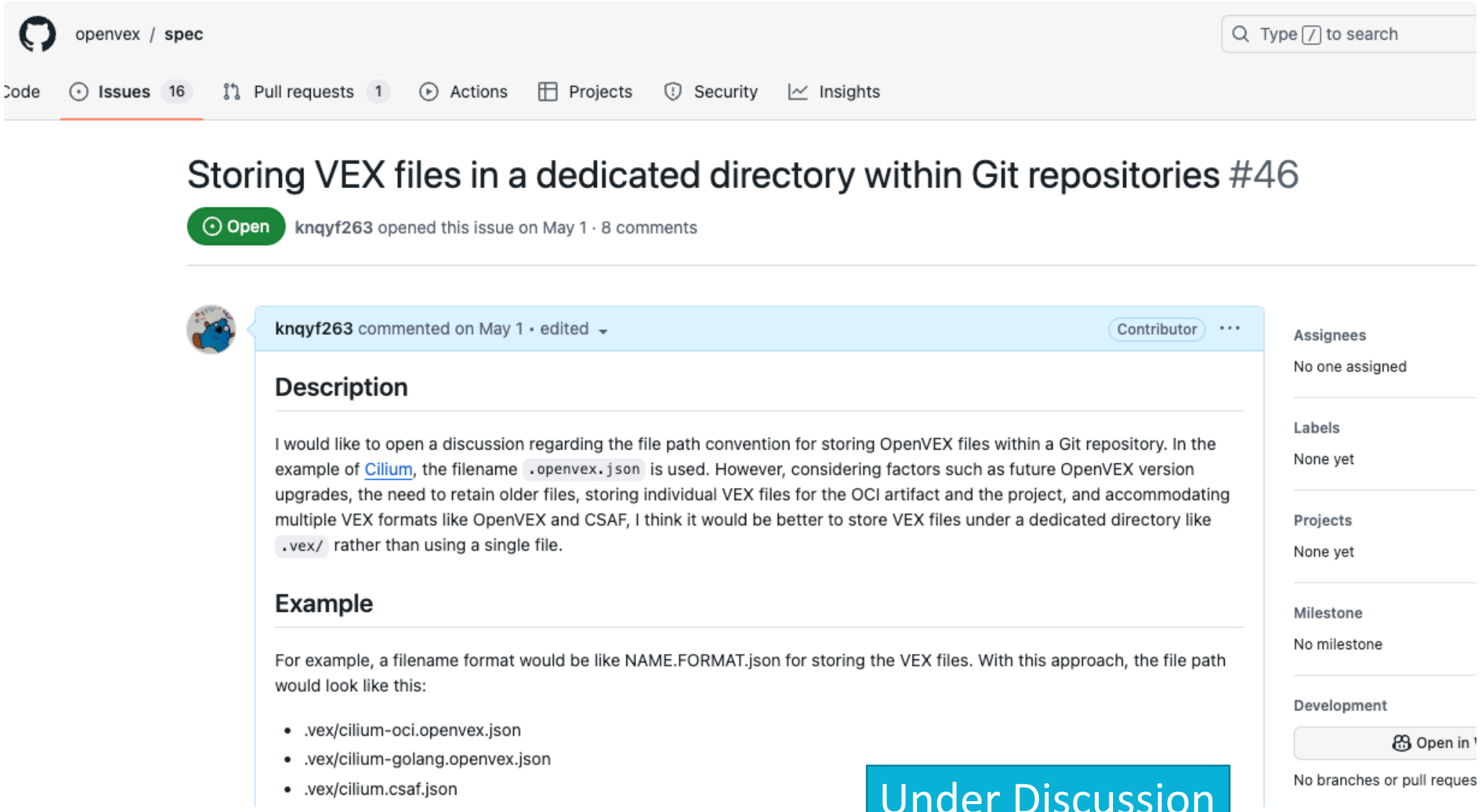
.vex/ Directory

trivy / .vex /

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

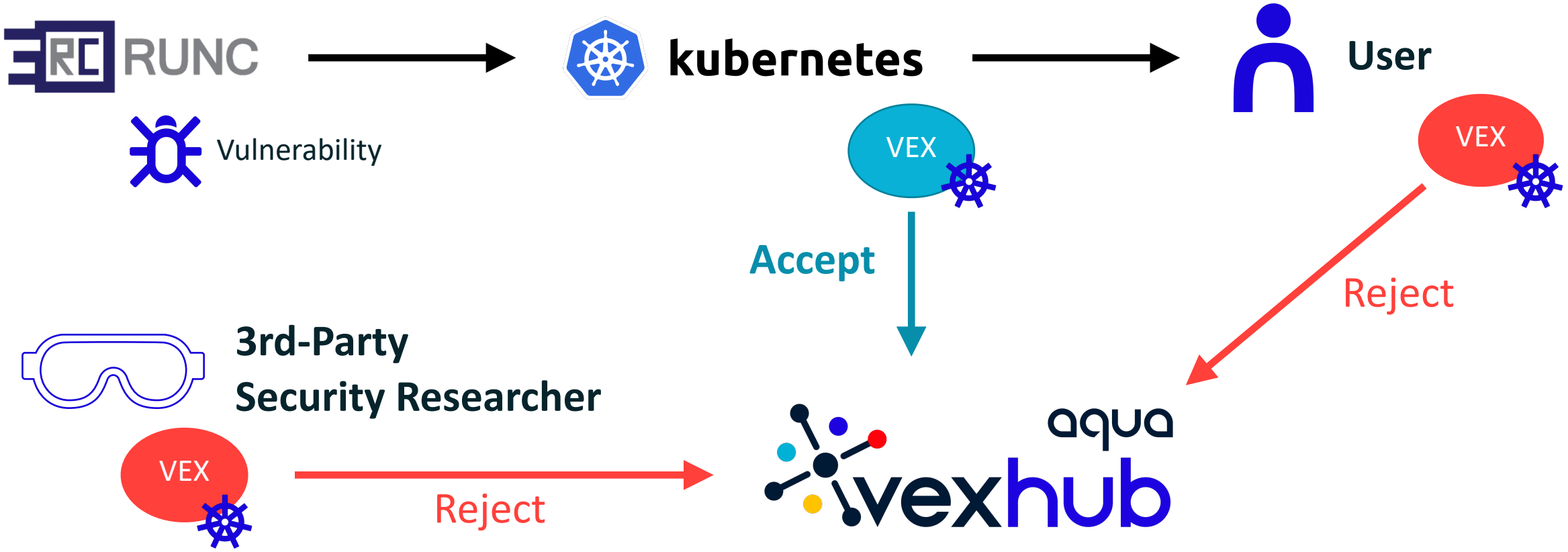
Name	Last commit message
..	
oci.openvex.json	chore(vex): suppress openssl vulnerabilities (#7500)
trivy.openvex.json	chore(vex): add CVE-2024-34155, CVE-2024-34156 and CVE-2024-34158...

.vex/ Directory Proposal



Under Discussion

VEX Hub Trust Model: Trust Maintainers



Want to Trust 3rd-Party VEX?

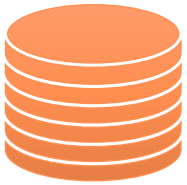
aqua

KubeCon | CloudNativeCon
North America 2024

VEX Repository Specification

VEX Repository Specification

Manifest File



Index File

Collection of VEX Documents

README | Code of conduct | Apache-2.0 license

VEX Repository Specification v0.1

aqua vexhub

https://github.com/aquasecurity/vex-repo-spec

VEX Repository Specification

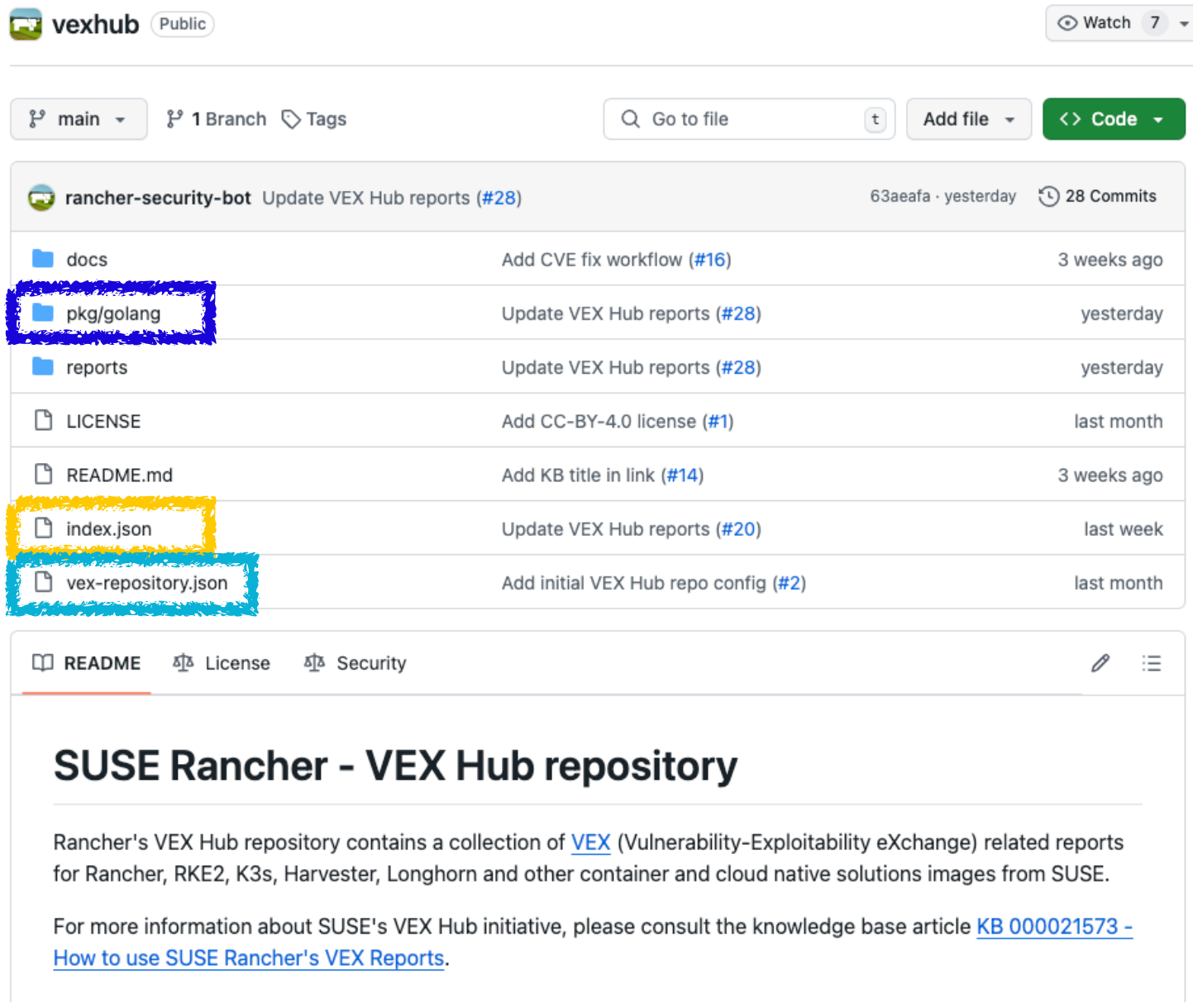
Manifest File

```
{
  "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



https://github.com/rancher/vexhub

Multiple VEX Repositories in Trivy

1. Discover (Primary)

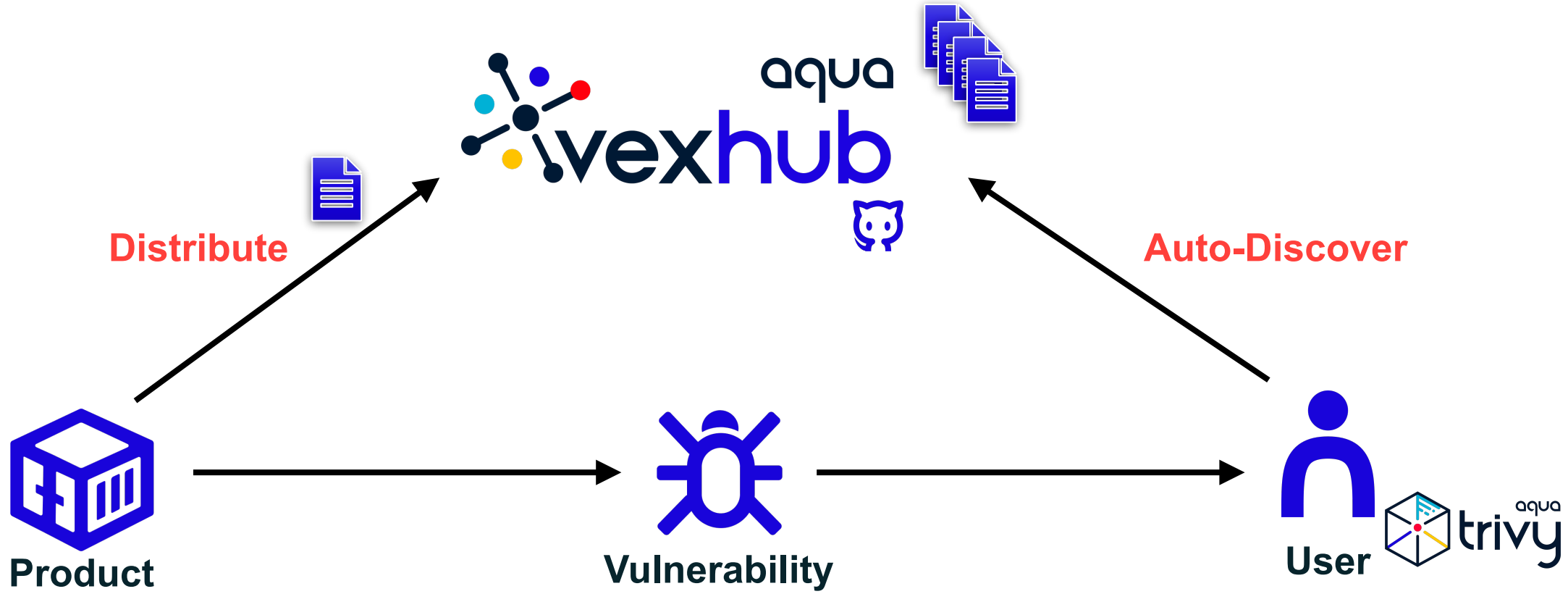
2. Discover (Secondary)

VEX Hub

VEX Repository Specification

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

Summary


aqua
vexhub
Distribute
Auto-Discover
Product
Vulnerability
User
aqua
trivy