TLP:CLEAR

CSAF, VEX, and SBOMs a Today's Cybersecurity Acronym Soup

Omar Santos

Cybersecurity Peasant @ Cisco PSIRT // CSAF Chair

@santosomar

Agenda

- An Update and Overview of the Common Security Advisory Framework (CSAF) 2.0
- Traditional and New CSAF Use Cases
- The Relationship between SBOMs and CSAF and the Vulnerability Exploitability eXchange (VEX)
- VEX Justifications in Advisories?
- Informational Security Advisories?
- Dynamic vs. "Static" Security Advisories
- APIs, ROLIE Feeds, etc.
- CSAF Open-Source Tools
- An Interactive Discussion of the Future of Security Advisories

The Common Security Advisory Framework (CSAF)

An open and definitive reference for the language which supports the creation, update, and interoperable exchange of security advisories as structured information on products, vulnerabilities and the status of impact and remediation among interested parties.

Spec, Docs, Tools, Presentations, FAQs: https://csaf.io

OASIS OPEN

TLP:CLEAR

Early Adopters

- Many of you are already using it.
- CERTs (including VINCE support).
- Government organizations such as BSI.
- Recommended in CISA and NTIA references.
- Support in other standards (i.e., SPDX, CycloneDX, etc.)

Is CSAF a Replacement or Alternative to CVE?

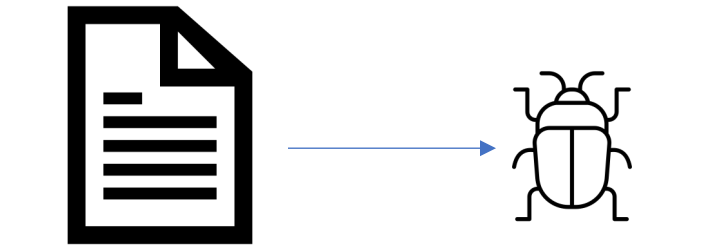
NO

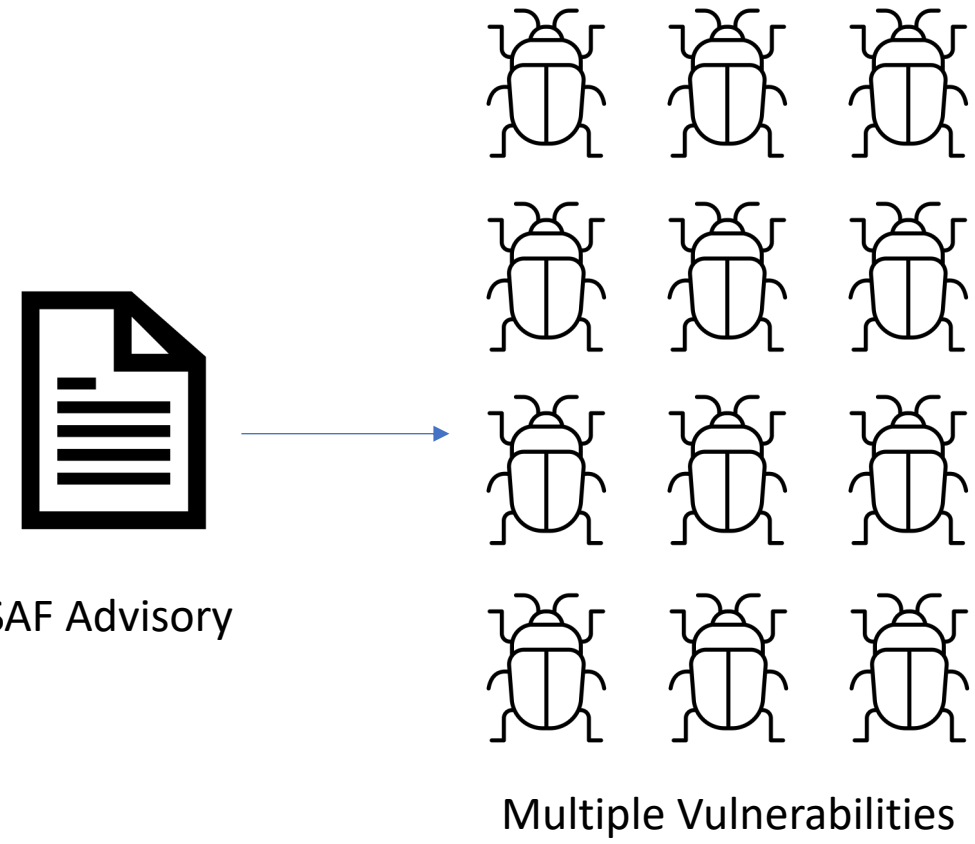
CSAF vs. CVRF

CSAF is the replacement for the Common Vulnerability Reporting Framework (CVRF).

However, it introduces a completely new ecosystems and several additional features.

CSAF Traditional Security Advisories





Profiles

- CSAF Base
- Security Advisory
- Informational Advisory
- Security Incident Response
- Vulnerability Exploitability Exchange (VEX)

CSAF Base

This profile defines the default required fields for any CSAF document.

A "catch all" for CSAF documents that do not satisfy any other profiles.

Furthermore, it is the foundation all other profiles are build on.

Security Advisory Profile

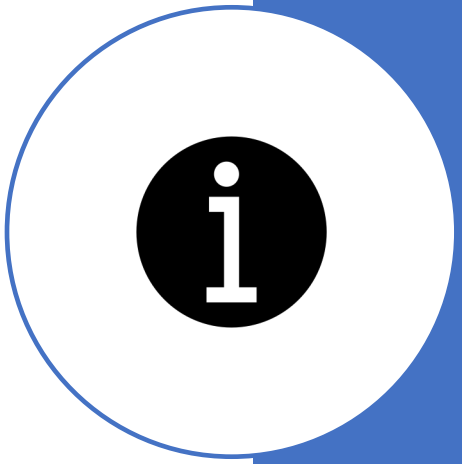
Traditional Security Advisories Similar to CVRF

This profile is used to provide information which is related to vulnerabilities and corresponding remediations.

Informational Security Advisory Profile

This profile is used to provide information which are not related to a vulnerability.

For example: misconfigurations, security responses to an "external" event or disclosure, etc.



CSAF

Security Incident Response Profile

This profile can be used to provide a response to a security breach or incident.

May also be used to convey information about an incident that is unrelated to the issuing party's own products or infrastructure.

For example: Company X might use a CSAF document satisfying this profile to respond to a security incident at ACME Inc. and the implications on its own products and infrastructure.

VEX Profile

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 CSAF relates to SBOMs?

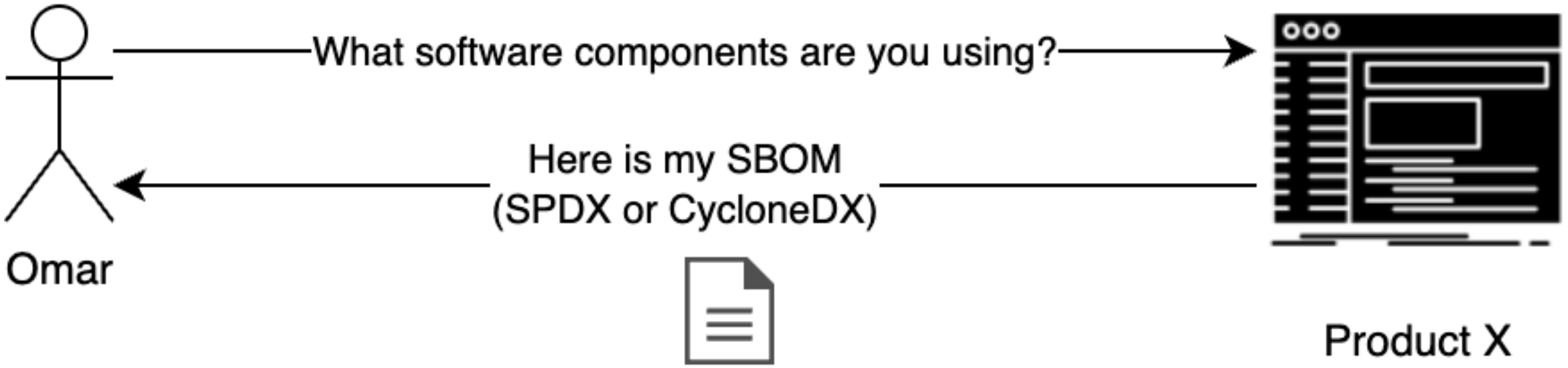
Recap on SBOM Standards

The two “most popular” or “widely-adopted” SBOM machine readable formats are:

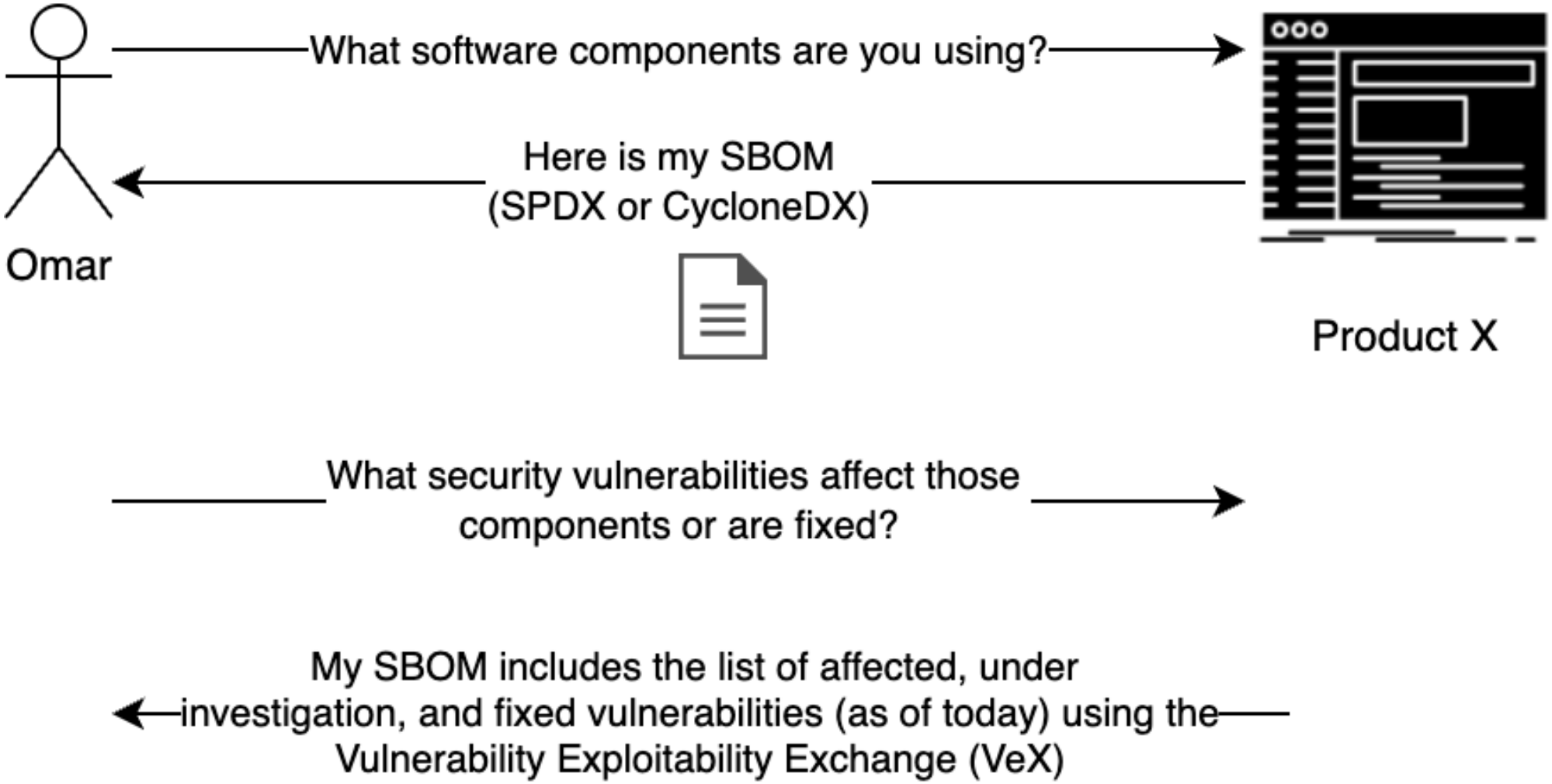
- Software Package Data Exchange (SPDX®): an ISO/IEC standard introduced as a Linux Foundation Project.
- CycloneDX: a lightweight SBOM specification and an open-source OWASP standard.

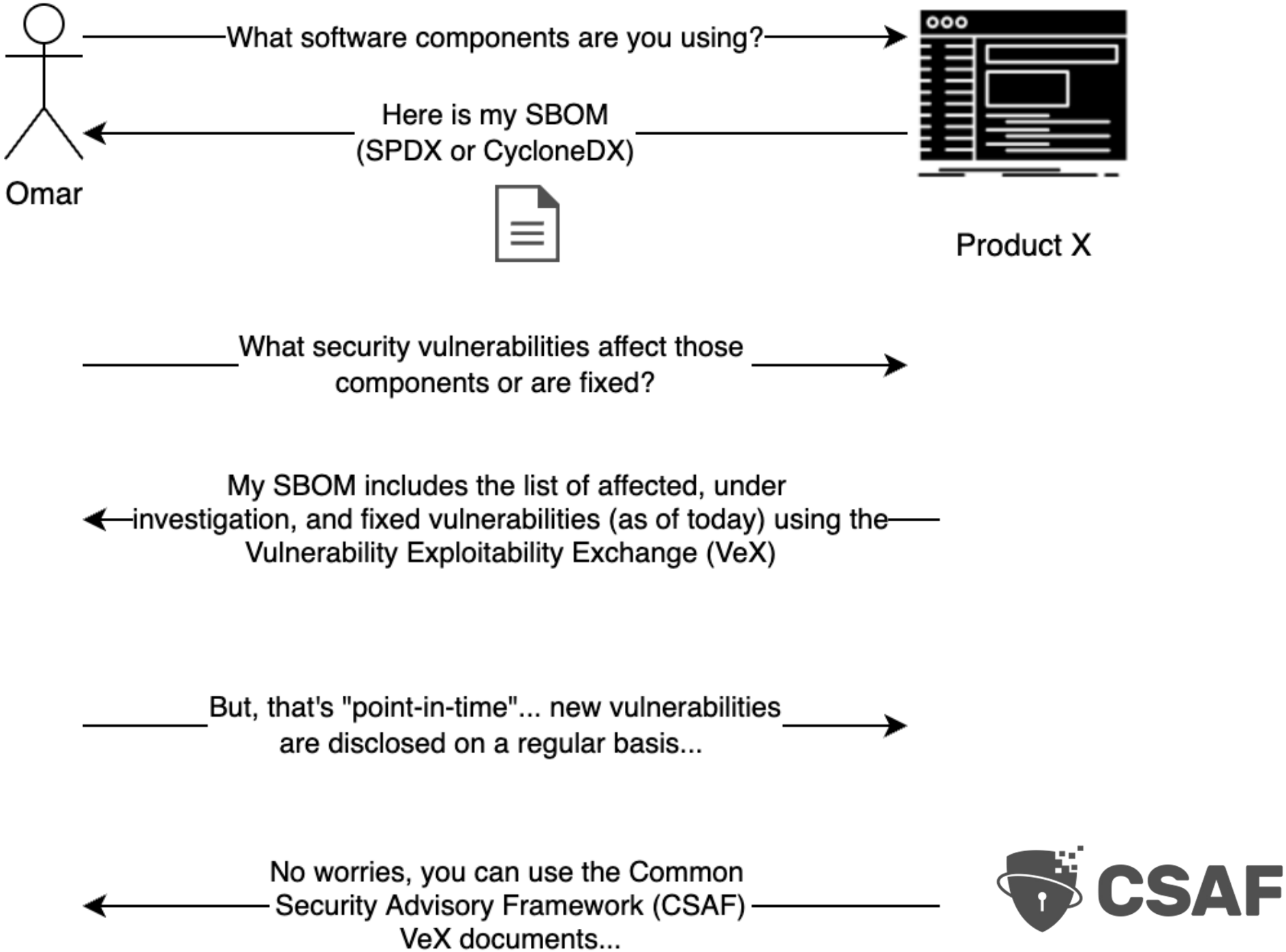
Note: Check out the “Survey of Existing SBOM Formats and Standards”, created by the NTIA and other collaborators, to learn more about how these standards (along with others) are used in the industry.

How Does This Work?



How Does This Work?




What software components are you using?
Here is my SBOM
(SPDX or CycloneDX)
Omar
Product X
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...
CSAF

CSAF in SPDX and CycloneDX

- CSAF is Supported in SPDX and CycloneDX

SPDX 2.3: https://spdx.github.io/spdx-spec/v2.3-RC1/how-to-use/

```
"externalRefs" : [ {
            "referenceCategory" : "SECURITY",
            "referenceLocator" : "https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/examples/csaf/csaf_vex/2022-evd-uc-01-a-001.json",
             "referenceType" : "advisory" } ]
```

CycloneDX: https://cyclonedx.org/capabilities/vex/#cyclonedx-and-third-party-advisory-formats and https://cyclonedx.org/use-cases/#security-advisories

```
"externalReferences": [
    {
      "type": "advisories",
      "url": "https://example.org/.well-known/csaf/advisory1.json"
    }
```

VEX Statuses and Justifications

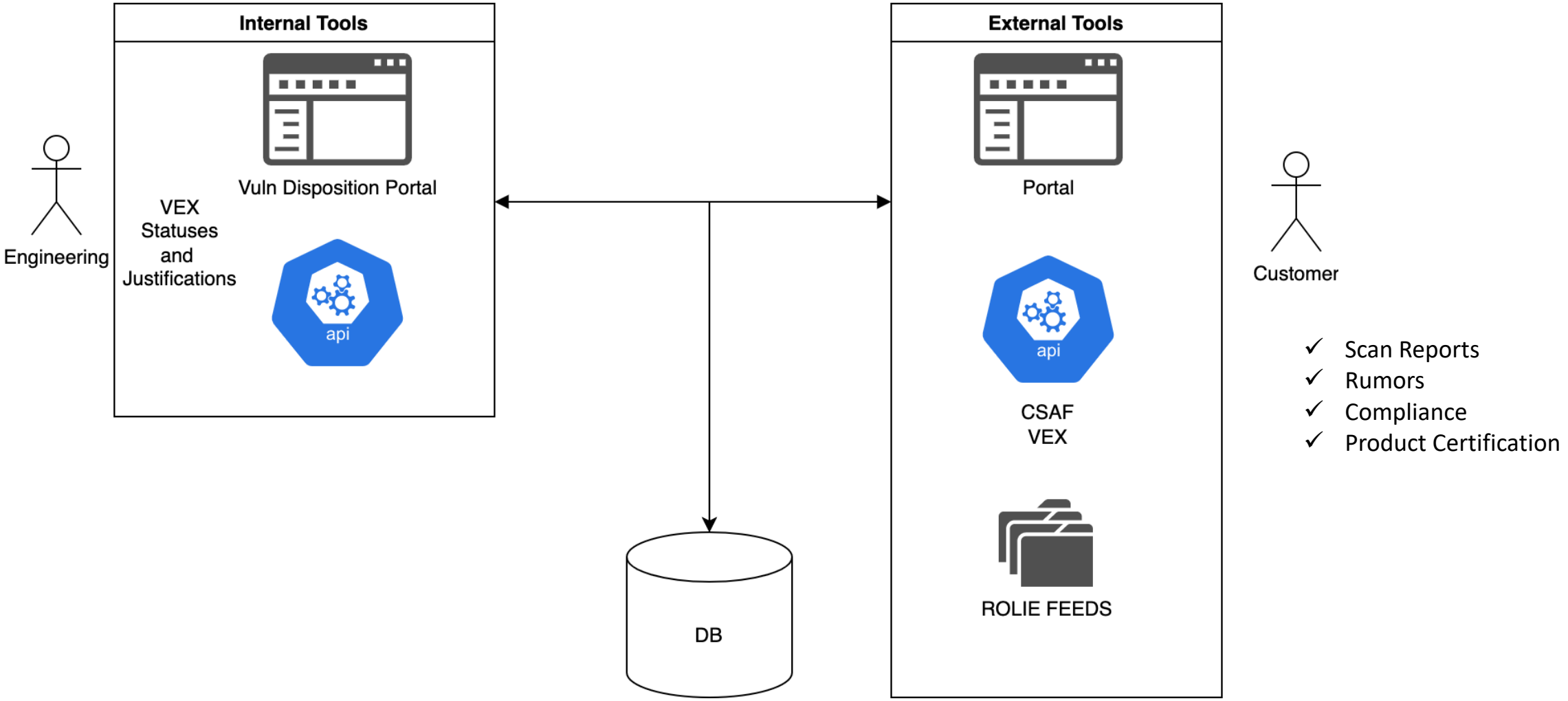
- under_investigation
- known_affected
- fixed
- known_not_affected
  - component_not_present
  - inline_mitigations_already_exist
  - vulnerable_code_cannot_be_controlled_by_adversary
  - vulnerable_code_not_in_execute_path
  - vulnerable_code_not_present

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

CSAF

You Don’t Need an SBOM to VEX

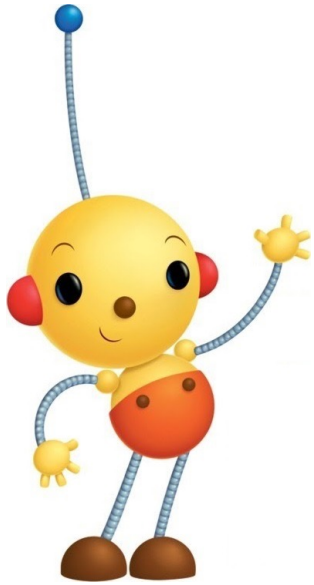
”Dynamic vs Static” Advisories



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

ROLIE Feeds?

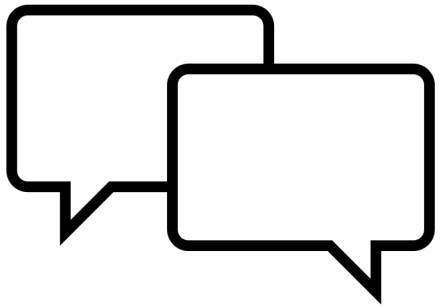
CSAF Supports the Resource-Oriented Lightweight Information Exchange (ROLIE), as defined in RFC 8322: https://www.rfc-editor.org/rfc/rfc8322.html



CSAF Open-Source Tools

- Secvisogram
- CSAF Parser
- CSAF Visualizer
- CSAF Trusted Provider
- CSAF Uploader
- CSAF Aggregator
- CSAF Checker
- CSAF Validator Library
- CSAF Validator Service
- CSAF Content Management System
- CSAF Downloader
- vulnrep

* and more in development!



An Interactive Discussion of the Future of Security Advisories

CSAF