Security Conference 2022

Software Bills of Materials and Vulnerabilities

Eliot Lear

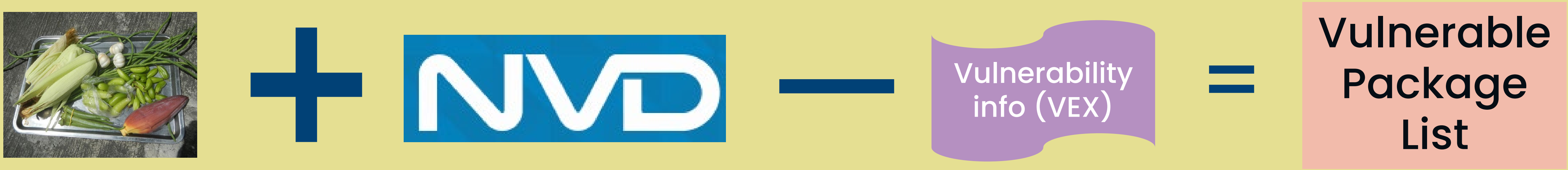
Cisco Systems

03/10/2022

Software Bills of Materials

- A software ingredients list for a product
- Available in several different formats
- If you know what's in your food, and one of the ingredients goes bad…
- … then there's a problem with the dish.

How is this stuff supposed to work?



+ NVD — Vulnerability info (VEX) = Vulnerable Package List

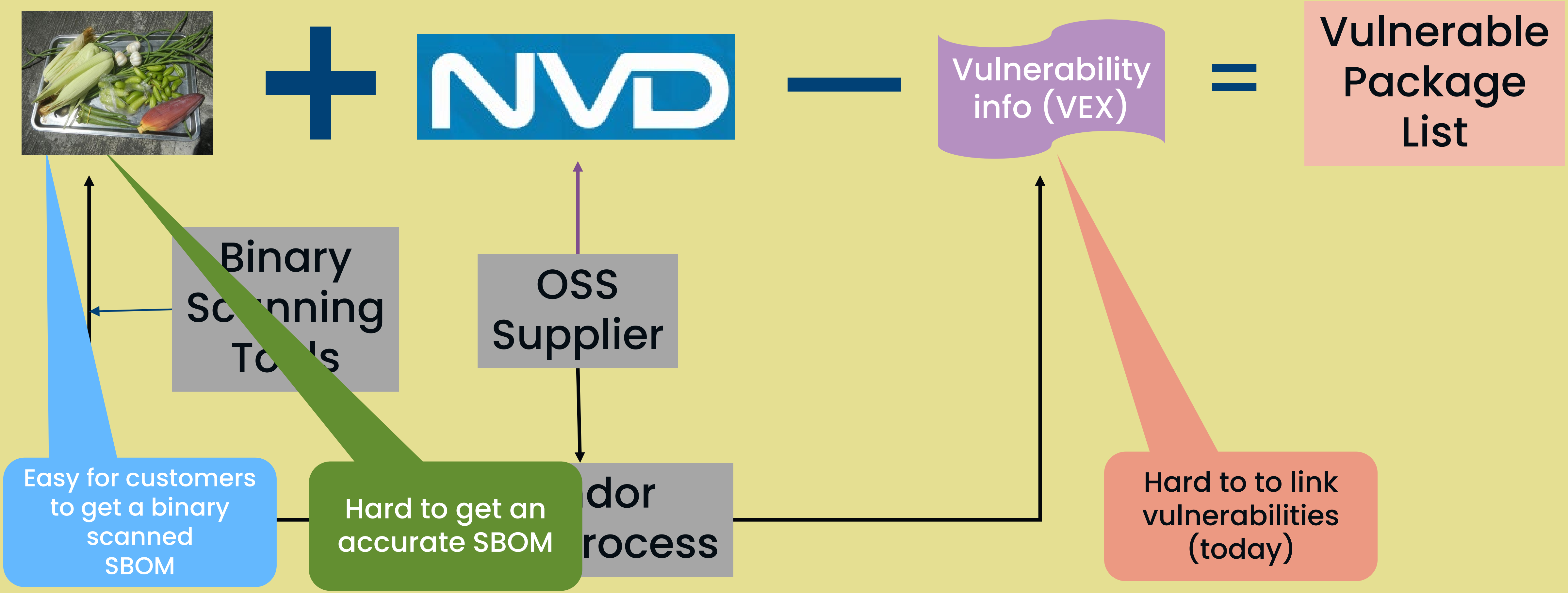
There’s a lot of work going on

- SPDX from the Linux Foundation
- CycloneDX (OWASP)
- Common Security Advisory Format (CSAF) from Oasis
- draft-ietf-opsawg-sbom-access
  - A means to discover where this information lives
- Supply Chain Integrity Transparency And Trust
  - A notarial service for documents
- Digital Bills of Materials (DBOMs)
  - A supply chain publish/subscribe mechanism

What’s not going on?

How do manufacturers go about generating SBOMs so that they can be meaningfully consumed?

What’s easy and what’s hard?



+ NVD — Vulnerability info (VEX) = Vulnerable Package List

Binary Sc nning To ls

OSS Supplier

dor rocess

Easy for customers to get a binary scanned SBOM

Hard to get an accurate SBOM

Hard to to link vulnerabilities (today)

Generating SBOMs

Ingredients From Others + Your Product's Ingredients =

Examples:

- Linux
- Other OSS

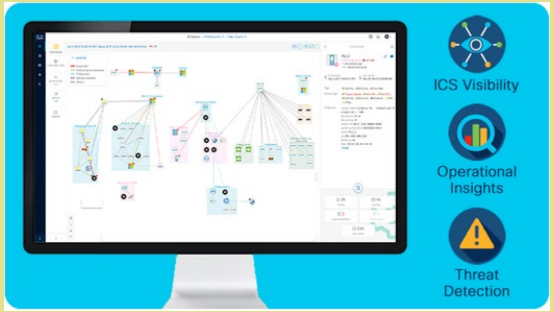
You can generate an SBOM, if you compile

- Commercial binaries/SDKs

You must rely on your upstream supplier or scan

Information velocity

- Pre-sales
- On boot
- On delivery
  - To other suppliers
  - To network administrators



Vulnerability info (VEX)

- On announcement from
  - Vendors
  - Security researchers

Delivering advice to manufacturers

GLOBALPLATFORM®

- We are currently developing a white paper to provide practical advice to manufacturers on how to generate SBOMs and connect them to vulnerability information
- Interested? See https://globalplatform.org.

Thank you!

Questions?

lear@cisco.com