

OPEN SOURCE SecurityCon NORTH AMERICA

Creating VEX Documents at Scale: A Look into One Supplier's Process

Jeff Mendoza, Software Engineer
Microsoft, Secure Supply Chain Team

What is VEX

- Vulnerability Exploitability eXchange
- Needed for EU CRA compliance, along with SBOM



Photo by Michael Blum on Unsplash

How to VEX

Needed to generate

- List of (open source) components in software (SBOM)
- Look up vulnerabilities in those components
- Exploitability information of those vulnerabilities in the software

Vulnerability management solution

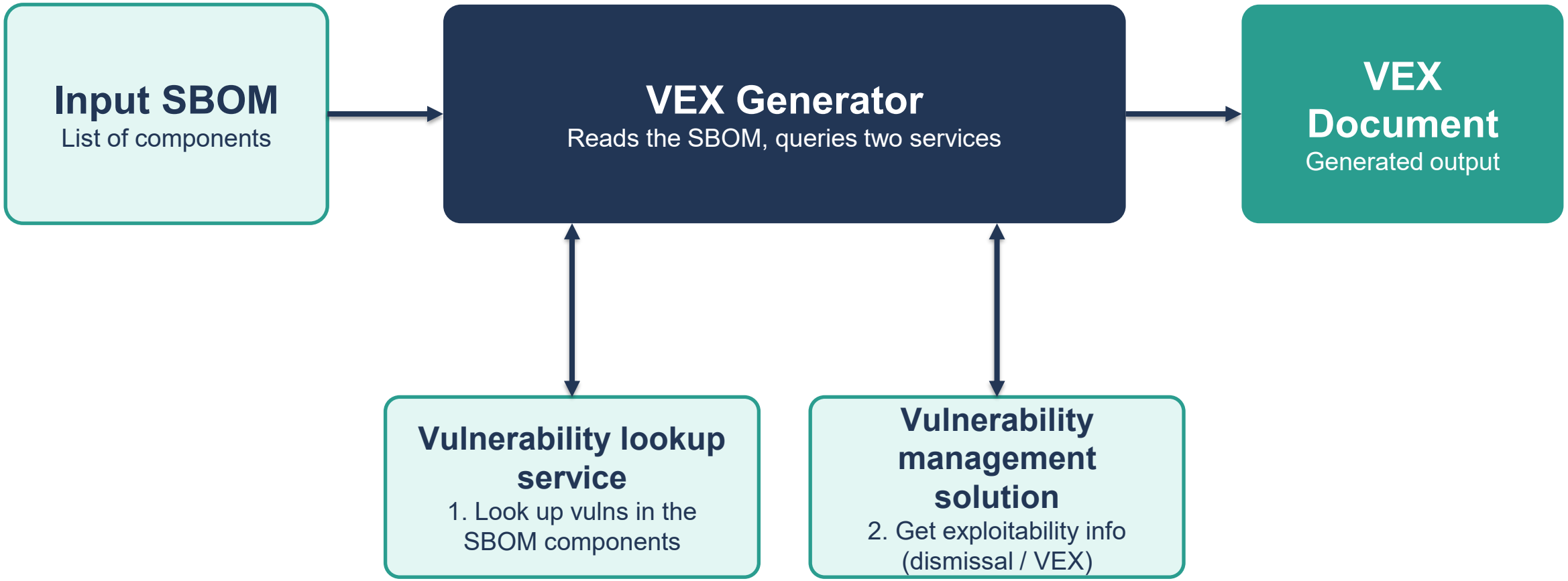
- Way to see what vulns are in software
- Way for devs to attach exploitability to those vulns: dismissal / VEX
- See GUAC

When to generate

- Generate one when you ship your software; make it available to your customers
- May need to re-generate for existing, already shipped software

Generating a VEX Document

OPEN SOURCE SecurityCon NORTH AMERICA



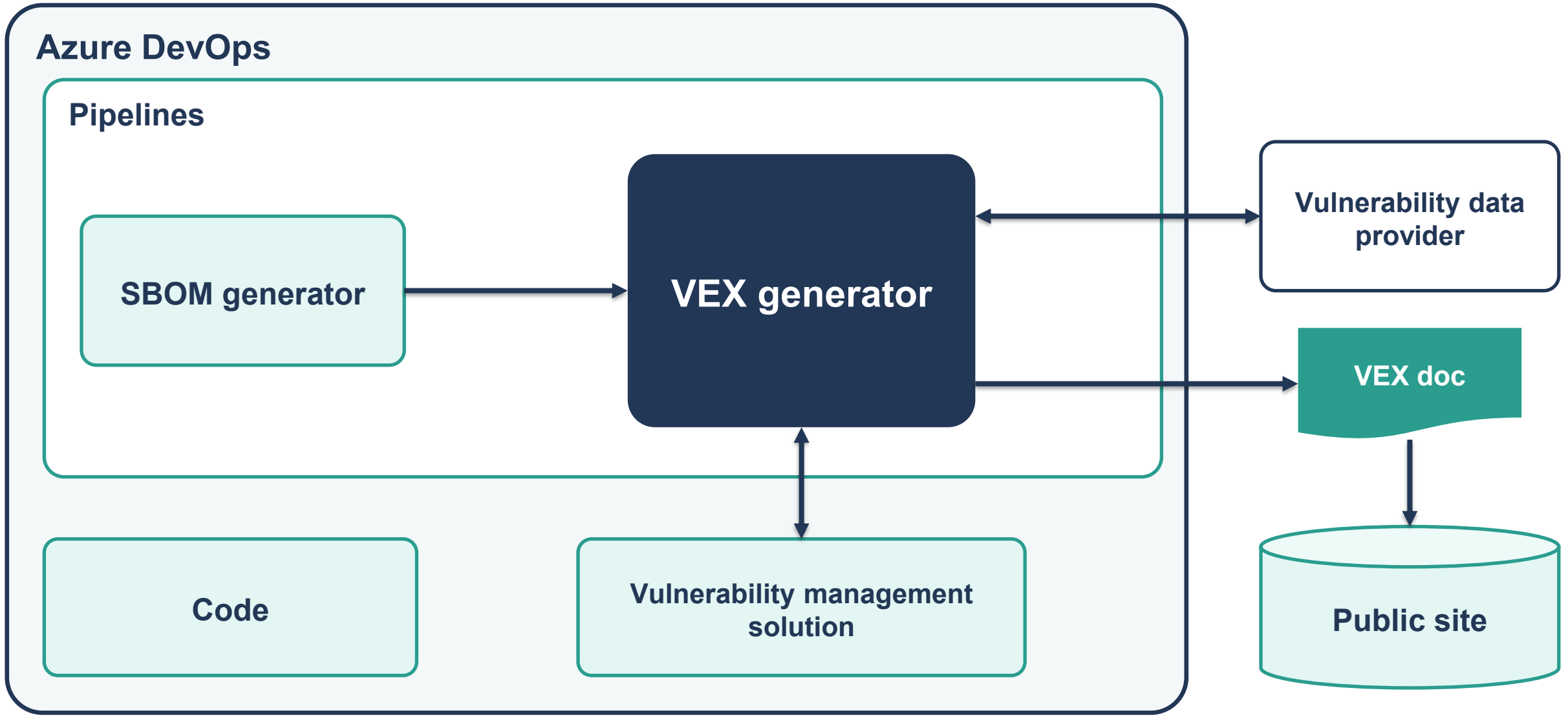
How Microsoft (will) VEX at scale

OPEN SOURCE SecurityCon NORTH AMERICA

- Have internal build/engineering system
  - Contains code and build pipelines
  - Already generates SBOMs and has vuln-management
- VEXTool is injected automatically into release pipelines
- Reads SBOM, accesses vuln providers, reads exploitability from vuln-management, generates CSAF VEX
- Published to public site (same as SBOM)

VEX at Scale in Azure DevOps

OPEN SOURCE SecurityCon NORTH AMERICA



CSAF VEX

What to know

- Spec for multiple docs, kind of confusing
- We should all do “Industry Standard”
- Do the minimum, but need to run the right category tests

Overview

- Fill out the document information
- Fill out the product information
- List all vulnerabilities
- Each vuln status is known_affected or known_not_affected
- Fill out reason for status

OpenVEX

- Simpler overall, VEX only
- Log of statements linking a vulnerability to software and an exploitability enum with justification
- PURL recommended

Resources

- **Jeff's Practical CSAF VEX Guide** https://github.com/jeffmendoza/csaf-vex-guide
- **Red Hat Guide** https://redhatproductsecurity.github.io/security-data-guidelines/csaf-vex/
- **CSAF 2.1** https://docs.oasis-open.org/csaf/csaf/v2.1/csaf-v2.1.html
- **OpenVEX** https://github.com/openvex/spec/blob/main/OPENVEX-SPEC.md
- **GUAC** https://github.com/guacsec/guac
- **GUAC + OpenVEX** https://www.kusari.dev/blog/spooky-enhancements-unveiling-guacs-openvex-feature
- **Microsoft SBOM tool** https://github.com/microsoft/sbom-tool