CISA: Update from the Financial Industry

Jon Meadows - Tech Fellow, Citi

Agenda

01 Progress – Early Days and Vendor

02 Issues – SBOM Quality and Naming

03 Internal SBOM’s

04 Future

Progress – Early Days

Heightened awareness of supply chain issues

Many Financial Institutions taking risk-based approach

Evaluating SBOM technologies amongst other capabilities, still early in terms of SBOM adoption

Building capabilities to manage and review SBOM's as part of wider strategy

Using SBOM’s Internally

Generate SBOM’s at the continuous build / deployment stage of the Software Development Life Cycle

Gain understanding of where and what open-source software is deployed, building open-source inventory

Advanced teams now able to leverage SBOM’s for vulnerability management

Component systems - use SBOM’s from upstream team

As teams shift left, must ensure that any SBOM’s created in the development environment correlate with SBOM’s generated later in pipeline

Next Steps – Vendor SBOM’s

Industry starting to look at vendor SBOM’s leveraging internal capabilities

Attempts made to obtain and analyse SBOM’s

Building pressure to require engagement and SBOM data

Two main issues identified so far…

Issues to address - SBOM Quality

SBOM data quality is inconsistent between vendors

Lacking quality benchmarks

What does good look like?

Issues to address - Naming

Complexity of understanding what component name refers to

When plugging into inventory systems to identify potential areas of vulnerability, can’t match on names

Often can’t match on hash as library may have been rebuilt

Future?

Stronger evidence of vendor security posture, attested and delivered in conjunction with SBOM’s.

Provenance metadata available for software and SBOM’s

However, need to continue working with industry on quality and naming solved

See CISA as driving force behind this…

Thank you