CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENGY, DHS

PUBLIC LISTENING SESSIONS ON ADVANCING SBOM TECHNOLOGY, PROCESSES, AND PRACTICES

CLOUD AND ONLINE APPLICATIONS SESSIONS SUMMARY

Much existing discussion around SBOM, particularly around SBOM use cases, has focused on on-premises software. Cloud and Software-as-a-Service (SaaS)-based software comprises a large and growing segment of the software ecosystem, and integrating current understanding of SBOM with emergent advances in cloud native technologies to tell better stories about SBOM use cases for cloud is an important endeavor. Over the course of two weeks, members of CISA met with participants and facilitated SBOM discussions with the intent of participants driving the outcomes, including specific issues of focus and next steps. CISA prepared these summary points from the participants' individual input.

Possible sub-topics

The following popular sub-topics for cloud and online applications were identified by participants:

- Cross-organizational dependencies (i.e., system architecture is essential to SaaS assurance)
- Spectrum of cloud (i.e., cloud vs. on-prem)
- SBOM granularity
- Impact of shared security model inherent in cloud
- SBOM point-in-time concerns (i.e., transient nature of SBOM)
- Runtime dependencies versus static linkage
- APIs versus SaaS versus service provider
- SBOM delivery synching with continuous delivery model
- Usefulness of SBOMs for cloud and SaaS applications when cloud SBOMs may change continuously

Use Cases

The following popular use cases were identified by listening session participants:

- SBOM accuracy
- How consumers handle application SBOMs
- SBOMs being correlated to specific cloud configurations
- SBOMs being different at different stages
- Procurement (SBOMs may only show part of the cloud service equation)
- Vulnerability discovery (how do we know if service is affected)

Scope

The listening sessions identified the following scoping considerations:

- Role of containers
- Role of open-source software
- Interaction between cloud, SaaS, and potential limitations of CVSS scoring in these circumstances
- Use of SBOMs for products in the cloud
- Role of security scanners.

Related efforts

The SBOM related efforts identified by the listening session participants are:

- VEX and other attestations
- Internet Engineering Task Force (IETF): Supply Chain Integrity, Transparency, and Trust (SCITT)
- Open Cybersecurity Alliance Posture Attribute Collection and Evaluation (PACE)
- Future SBOM sharing and exchanging community work

Potential outcomes

Participants in the listening sessions identified the following potential outcomes for future SBOM work on cloud and online:

- Cloud-centric SBOM best practices document
- Clarity on effectiveness of SBOM use in the cloud