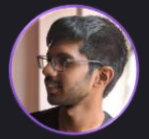
The Digital Bill of Materials

And secure software supply chains

PRESENTERS

Chris Blask
VP – Strategy
Cybeats



Amith K K
Senior Engineer
Unisys Innovation

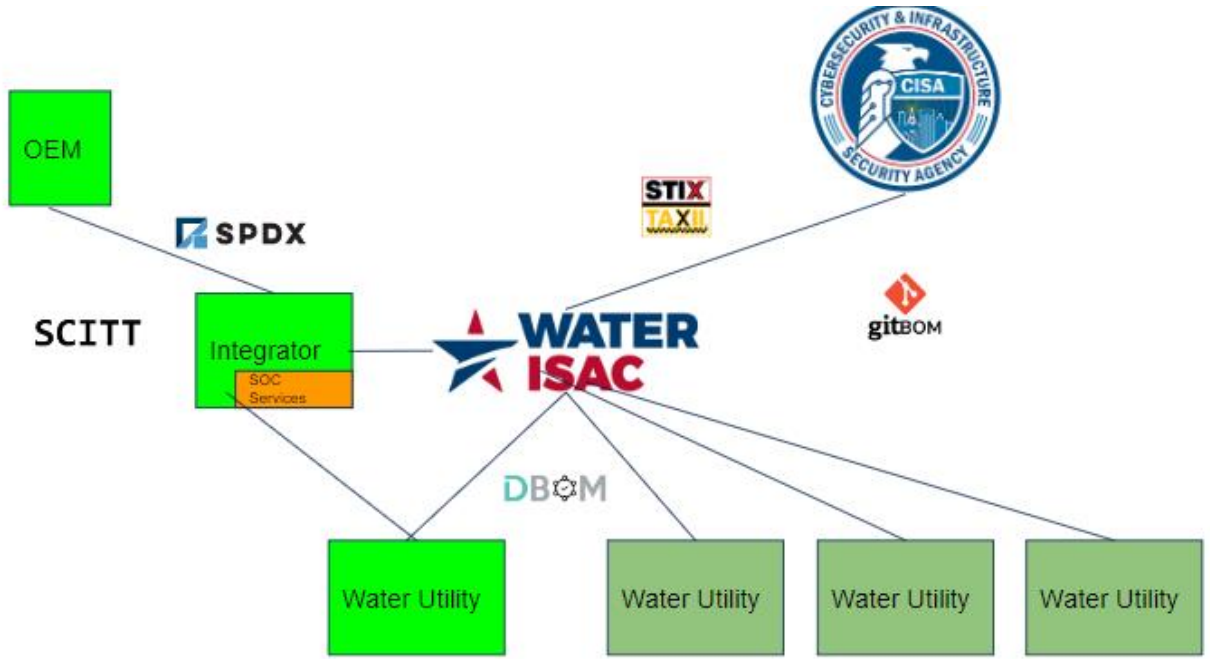
TABLE OF CONTENTS

01

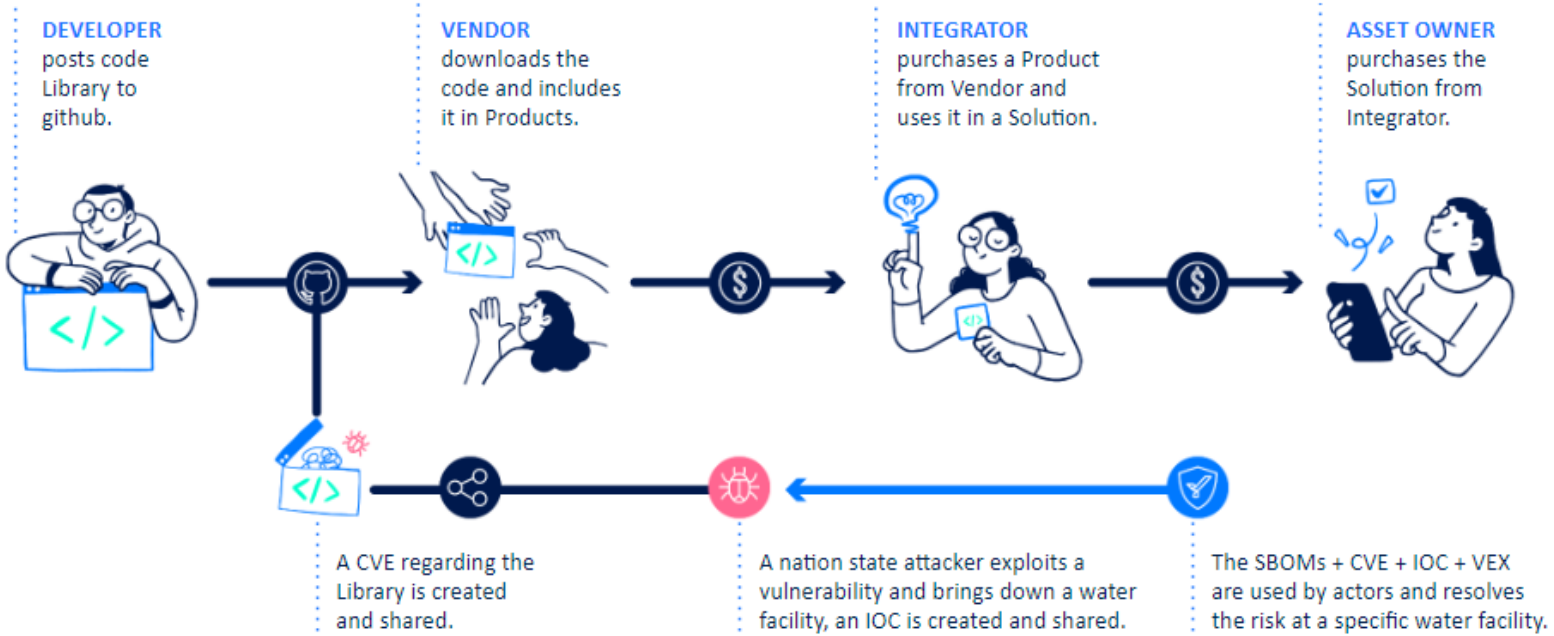
SSC ECOSYSTEM

How DBoM integrates into the Secure Software Supply Chain

Supply Chain Intelligence Supports Incident Response

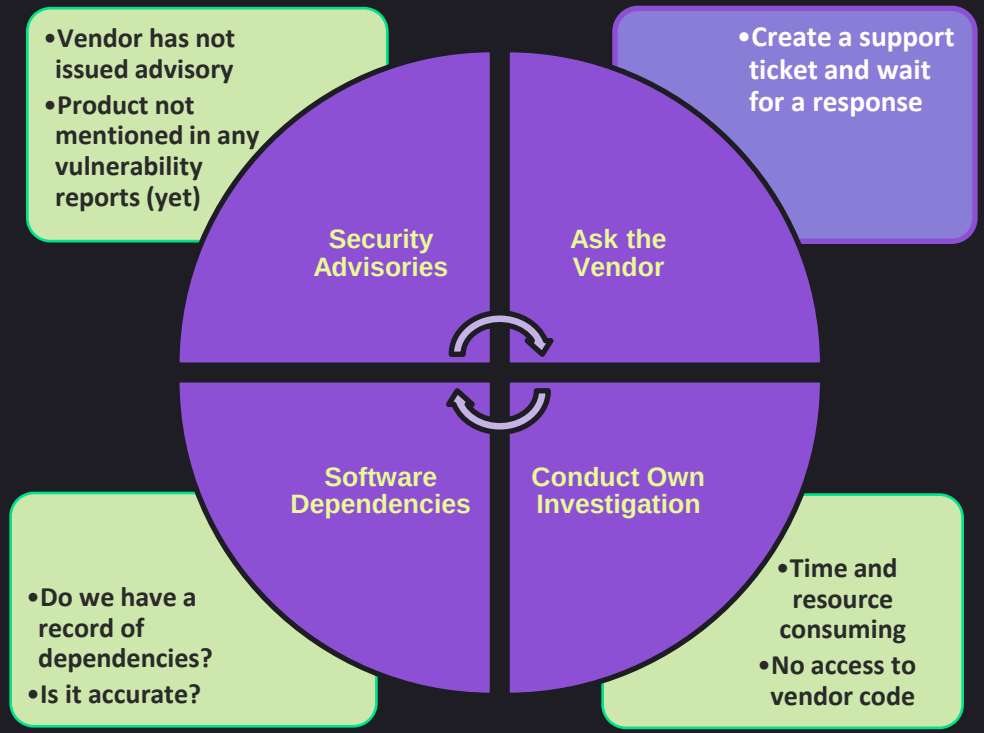


Supply Chain Intelligence Fits Together

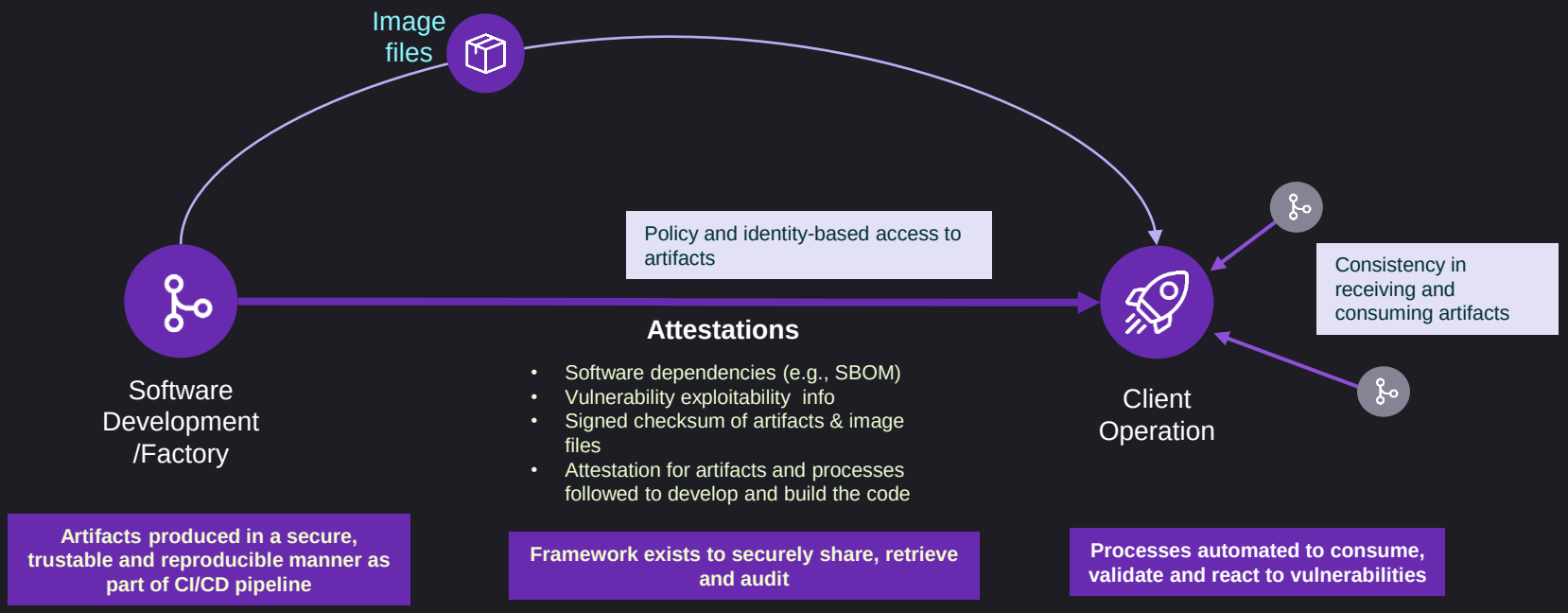


Finding Products at Risk is Ad hoc at Best

Delays significantly increase exposure to cyber attacks



End to End Secure Software Supply Chain



End to End Secure Software Supply Chain

DBoM Can Help Here

	Channels as a structured, query-able datastore	Channels as a Secure Transport	Notarized attestations and tool integrations
Generate [machine readable] SBOMs, vulnerability reports & attestations	**Store & Organize**	**Policy-based Internal & External Sharing & Authorization**	**Validate & Build Trust Through Transparency**

Automated process to generate:
• SBOMs for:
  • Code
  • Tools used to produce the code
  • Running Infrastructure
• Vulnerability reports
• Signed checksum of artifacts
	• Automated process to:
	  • Organize & store SBOMs and artifacts based on products and packages
	  • Manage SBOMs, VEX/VDR and attestations per product release and/or vulnerability exposure
		• Sharing SBOMs and vulnerability reports with internal organizations and external customers based on a set of internal and external policies and agreements	Enable
			• Receiving SBOMs & vulnerability reports in a timely manner
			• Validating the authenticity of the received artifacts (image files, documents, etc.)
			• Build trust & confidence in the production process of software through attestations

02

Architecture & More

High level breakdown of DBoM Concepts and Services

What is DBoM?

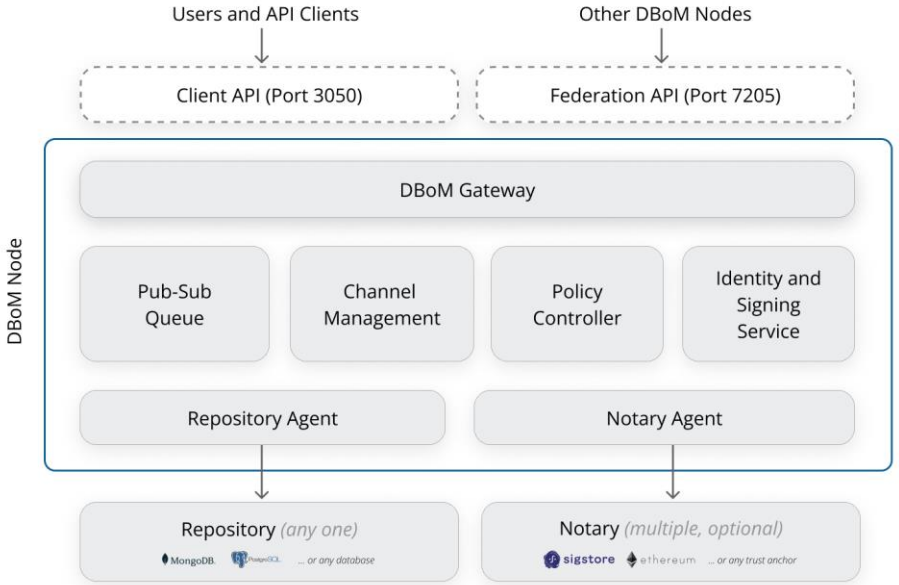
An open source decentralized, federation-based solution to bring

uniformity, automation, security & auditability

to SBOM, vulnerability & attestation sharing

THE LINUX FOUNDATION

DBoM Architecture (v2)

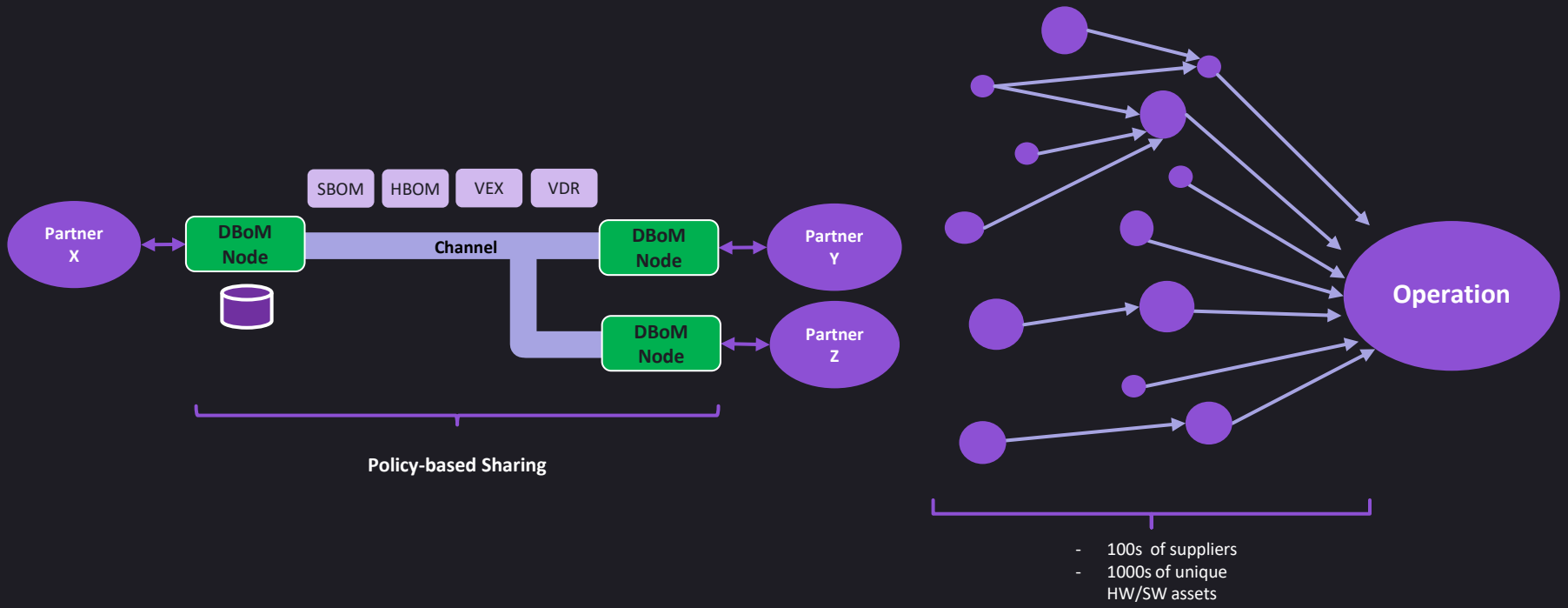


Each Channel

- Is hosted by a DBoM Node
- Can store structured JSON data within a signed JSON Envelope
- Has one or more subscribers with a well-defined access policy (read, write, audit)
- Optionally is associated with one or more notaries
- Unambiguous URI

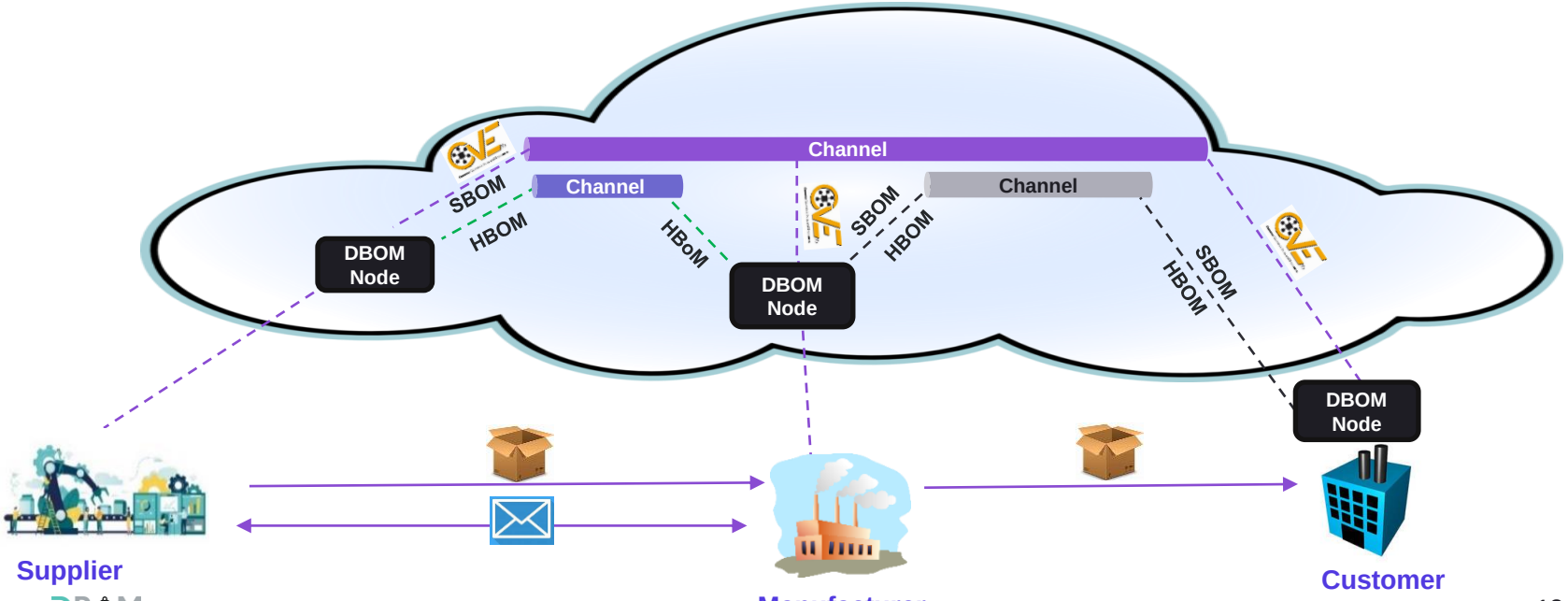
Instantiate a DBOM Node → **Instantiate a repository and setup channel(s)** → **Invite partner(s) subscribe to the channel(s)** → **Integrate with your tooling** → **Record, retrieve and audit attestations**

What is DBoM?


SBOM
HBOM
VEX
VDR
Partner X
DBoM Node
Channel
DBoM Node
Partner Y
DBoM Node
Partner Z
Policy-based Sharing
Operation
- 100s of suppliers
- 1000s of unique HW/SW assets

The DBoM Vision

To provide a global, decentralized framework that enables companies to bring trust, resiliency, automation and efficiency into the supply chain of their products (hardware or software)

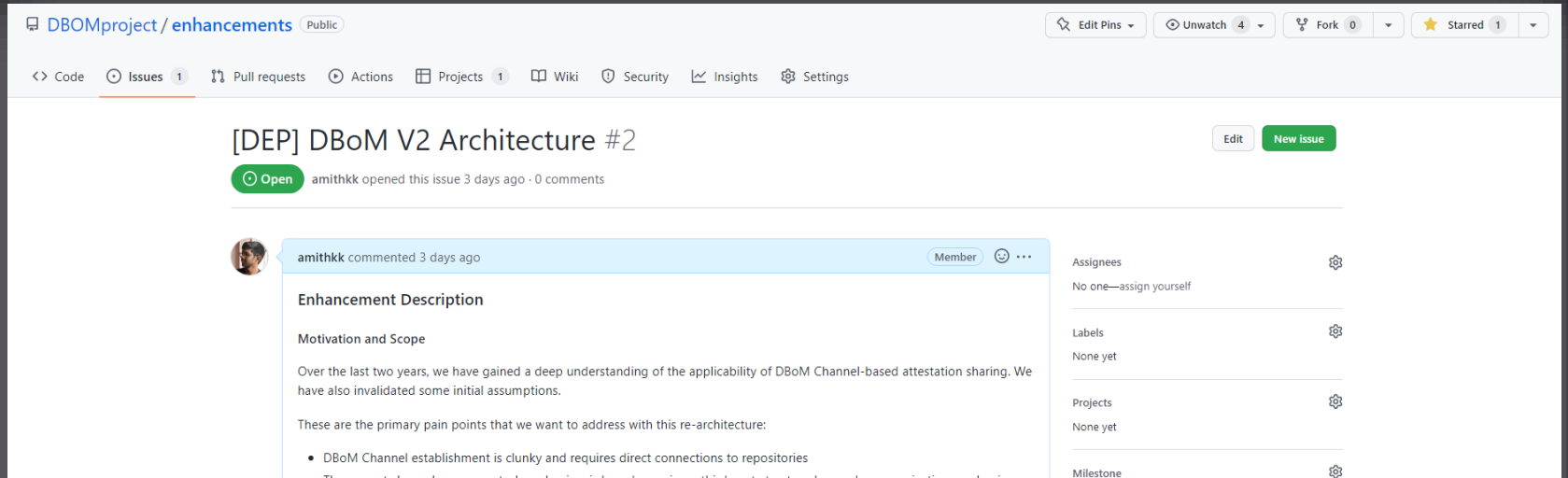


Key Values

- **Secure, Policy Based Attestation Sharing**
  - Decouple your attestations from your artifacts
  - Create channels with configurable sharing policies
  - Encryption in transit & rest
- **Build Trust in your Software Supply Chain**
  - Cryptographically sign attestations
  - Notarize changes to attestations on transparency logs and distributed ledgers
  - Have an audit log for every change and retrieval operation
  - Independently verify veracity of attestations
- **Standardize, Automate and Organize**
  - Your DBoM node is the one-stop-shop to receiving all upstream attestations
  - Standardized APIs allow hooking into automation processes
  - Integrations with popular tools (Dependency Track, in-toto et. al.)
  - Unambiguous name-spacing of attestations

Going to DBoM V2

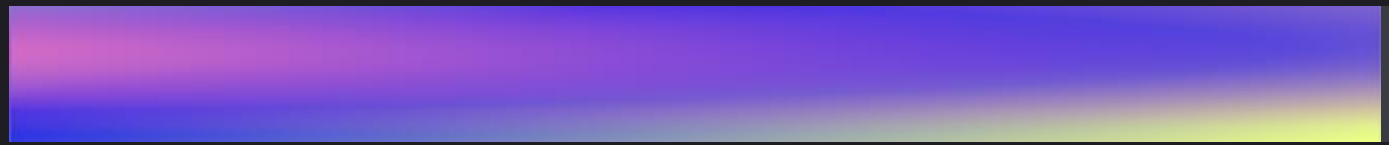
- DBoM v1 has been open sourced in 2020.
- Several PoCs have been conducted both inside and outside Unisys.
- V2 architecture and implementation is being worked on based on feedback.
- We would appreciate comments on the v2 architecture (link here)



02

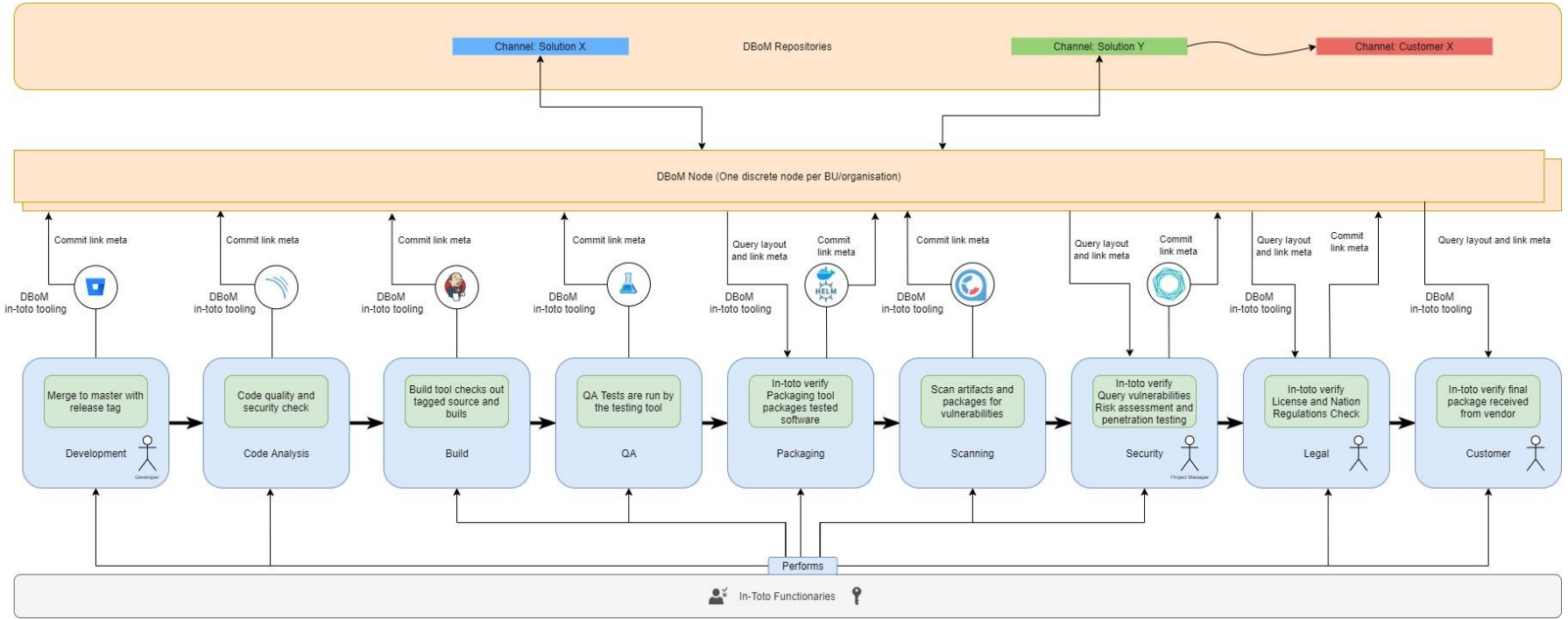
Use Cases & PoCs

See where we have used DBoM, and preview upcoming collaborations



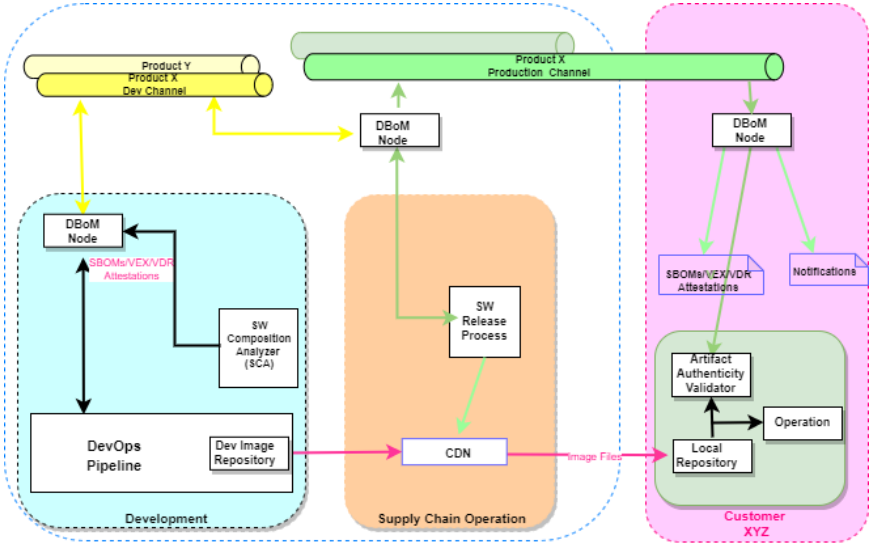
IN-toto & DBoM Integration for CI/CD

Link to Demo: https://youtu.be/uN-tdOpXtXo



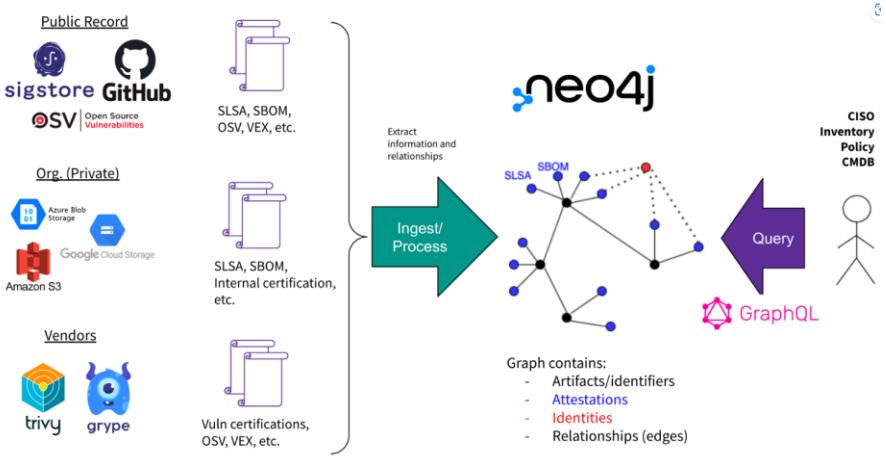
VEX + SBOM PoC

- Separate paths for sharing artifacts and image files
- Policy-based access control
- Notifications upon availability of updated vulnerability report
- Ease of auditability
- Uniformity & automation - Extendable to receive SBOMs and VEX reports from other providers
- DBoM nodes can be instantiated on-prem or in the cloud



DBoM and GUAC

- GUAC – Graph For Understanding Artifact Composition is an Open-Source project to Collect, Ingest, Collate and Query attestations
- Upcoming PoC for DBoM channels to be a source of verified attestations for the GUAC Platform



End Notes and Takeaways

- Special thanks to the Unisys team (Mehdi Entezari, Sanket Panchamia & Rajesh Hegde) for code contributions, documentation & marketing material around DBoM
- Know more about DBoM – https://dbom.io
- Want to continue the conversation? – Join us on Slack!
- We would appreciate your comments on the v2 architecture - https://github.com/DBOMproject/enhancements/issues/2