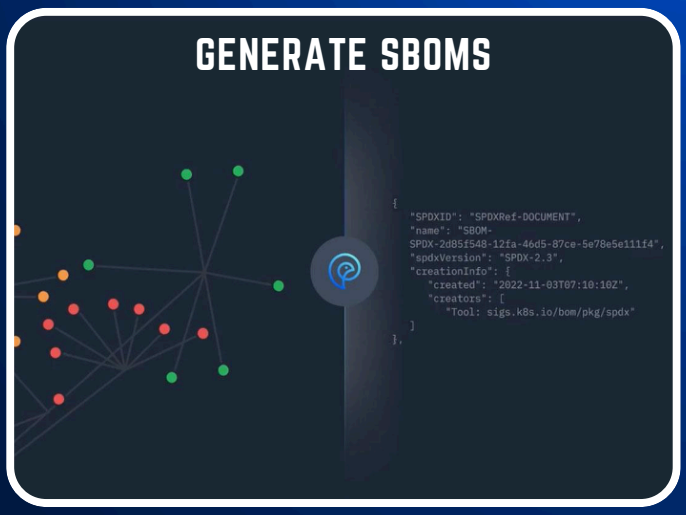
Phylum

THE SOFTWARE SUPPLY CHAIN SECURITY COMPANY



THREE EASY STEPS

1. Define Policy
2. Onboard Stakeholders
3. Manage Findings

OPERATIONALIZE SBOMS, SECURE YOUR SOFTWARE VALUE CHAIN

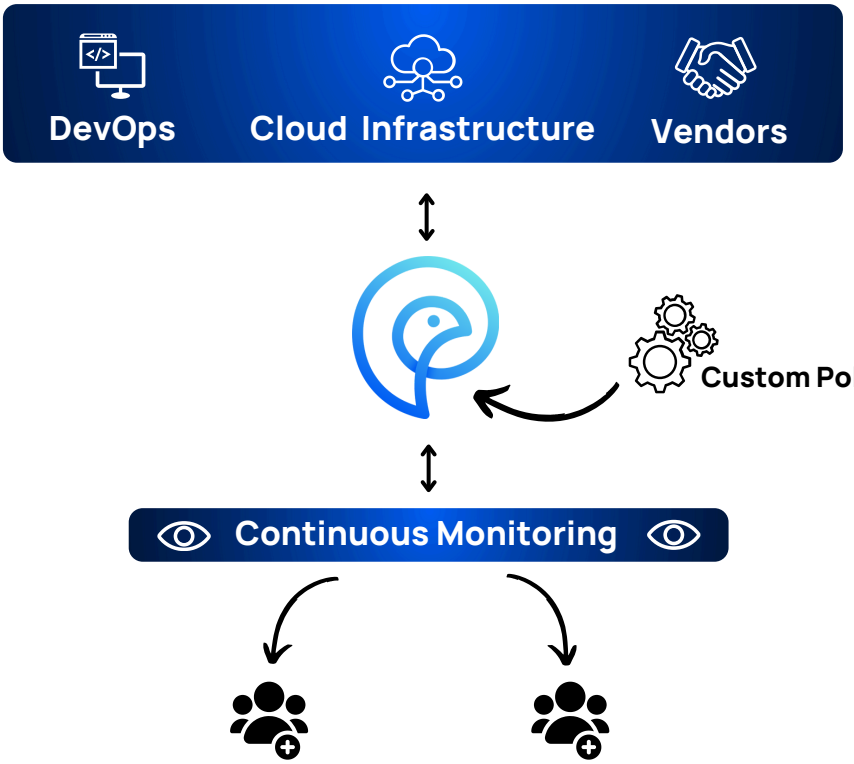
Phylum features a robust, flexible suite of capabilities to define extremely granular policies across various attributes of software value chains. This capability enables organizations to clearly define what "acceptable use" means for software described by an SBOM, and enables near-instant feedback on the risks associated that violate policy. Not only can Phylum facilitate seamless collaboration with third-party contributors, but its suite of integrations and its extension framework enable SBOM data to be collected and catalogued without making operational changes to the development workflow. This gives stakeholders visibility into software supply chain security posture and associated risks, and enables continuous monitoring of impacted artifacts to flag new risks, threats, or other issues as they emerge. Phylum also helps automate guidance for the remediation of issues surfaced from a given SBOM, which can quickly streamline the process of addressing and remediating identified issues.

PHYLUM'S FIVE DOMAINS OF RISK:

SOFTWARE VULNERABILITIES | LICENSE MISUSE | MALICIOUS CODE | AUTHOR RISK & REPUTATION | ENGINEERING RISK

MAKE SBOMS ACTIONABLE

Achieve internal software value chain observability and know third-party application risks



DEFINE POLICY

Phylum's policy framework translates business risks and regulatory requirements that drive risk decisions to surface both acute and systemic risks, and filter out findings that don't matter. Policy can be defined for both individual projects or vendors, as well as across entire groups.

ONBOARD STAKEHOLDERS

Stakeholders can be onboarded either through direct invitation, or via a variety of different integration paths. Phylum also features a robust API and flexible extension framework, enabling deep customization and rapid adaptation to existing workflows and business processes.

MANAGE FINDINGS

Users can easily manage and automate the full lifecycle of SBOMs, which include collaborating on findings, searching through catalogued SBOMs to identify specific projects impacted by a particular software component or vulnerability, and registering to receive alerts if a new issue that violates policy pops up.

SPDX CycloneDX

FINDINGS AND SBOMS CAN EASILY BE EXPORTED FOR USE IN OTHER SYSTEMS AND WORKFLOWS, AND CHANGES TO POLICY OR ISSUE SUPPRESSIONS CAN BE TRACKED AND AUDITED TO ENSURE CONTINUOUS COMPLIANCE.

FOLLOW US

@Phylum_IO @Phylum-IO