MANIFEST

Product & Feature Overview

MANIFEST

Manifest is a venture-backed cybersecurity company that helps organizations reduce the risk in the technologies they produce and procure. Our platform allows organizations to ***operationalize*** – derive value from – SBOMs, helping identify actionable insights in the novel SBOM data from their first- and third-party software. Manifest customers use our capabilities to find and ship more secure software, evaluate the cybersecurity of vendors and their products, respond faster to vulnerabilities in third-party libraries, and find other issues like problematic licensing.

CRITICAL CAPABILITY OVERVIEW

Below is a list of what we believe are capabilities critical to establishing an enterprise SBOM program. The Manifest platform is designed to address each core capability in a lightweight, user-friendly platform that requires little to no technical background or expertise.

Generating SBOMs

Manifest allows organizations to generate SBOMs manually or automatically during the continuous integration / continuous delivery (CI/CD) pipeline, so your engineers can focus on writing and shipping code. We natively support Github Actions, CircleCI Orbs, and have an extensible, all-purpose command line interface (CLI). We can generate SBOMs in CycloneDX or SPDX formats, and across more than a dozen programming languages/ecosystems, such as python, go, javascript, typescript, npm, and more.

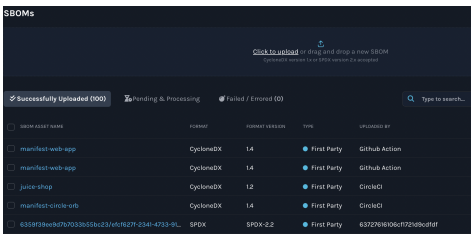
Merging SBOMs

Since SBOMs are most helpful to software consumers when they map one-to-one with a piece of software, organizations that have started to operationalize SBOMs have a strong need to merge SBOMs to create a single, comprehensive SBOM for their software application. This is immensely helpful for organizations that use multiple code repos or folders (e.g. in Github) to deploy a single application for customers, as well as or organizations with lots of third-party software suppliers, such as industrial control systems (ICS) vendors and automotive manufacturers.

Ingesting & Normalization

SBOMs come in two predominant formats, CycloneDX and SPDX, and can be output in a variety of file types like json or xml) with additional formats likely to come in the future. Manifest can ingest and import SBOMs across multiple formats and store them in a normalized fashion that makes it easy to search, filter, and analyze.

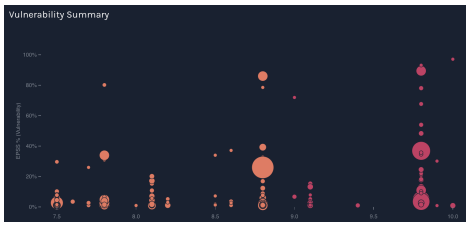
Aggregating SBOMs



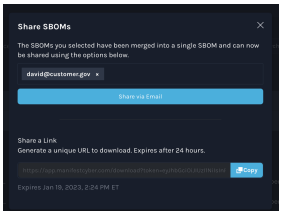
Instead of storing your SBOMs in Google Drive or Microsoft Teams, Manifest is a purpose-built SBOM aggregator where SBOMs can be populated manually (e.g. via drag-and-drop) or automatically via our zero-click SBOM generation capability. We can track who generated each SBOM, who uploaded them, and other important metadata.

Enriching SBOMs

SBOMs contain limited information - mostly basic application metadata and a lengthy list of the names, versions, and licenses of software dependencies. Manifest integrates with other data sources to bring in information about software components (such as problematic licenses) and matches dependencies to known vulnerabilities. In addition, incorporate novel vulnerability intelligence, such as exploitability data, to help our users prioritize which vulnerabilities are worth mitigating and which are less risky for the enterprise.



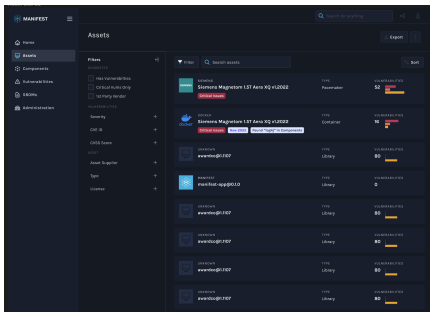
Secure & Selective Share SBOMs



Software vendors or developers need a way to share SBOMs with their customers in a selective and secure manner. Rather than sending SBOM attachments in emails or stapling them to contracts, Manifest customers can securely share time-bound links to download specific SBOMs based on specific needs, whether for a government agency, regulator, or insurance company.

Visualization and Reporting

Manifest makes machine-readable but ugly-to-humans SBOM data into user-friendly pages in our app. These pages help even non-technical users understand product risk and what actions to take next. The content can then be easily turned into reports shareable in a PDF or via a read-only web view.



WHY YOU SHOULD CARE ABOUT SBOMS

Healthcare and medical devices

The FDA's latest draft premarket cybersecurity guidance lists SBOMs as a preferred artifact for software-enabled medical devices to receive FDA approval.

Software development best practices

SBOMs are recommended as a best practice in separate guidance from the NSA, CISA, and the IT Sector, as well as from NIST.

Selling to government

Executive Order 14028, signed in May 2021, introduced the requirement that all companies selling tech to the U.S. government must soon provide SBOMs for their technology.

Buying tech with long lifecycles

SBOMs are a key method of highlighting the relative (in)security of technology that organizations may have to manage for decades. That's why both the OT/ICS and energy sectors are embracing SBOMs early.

USE CASES

- **Smarter & Faster Vulnerability Management**
  Find all impacted assets and vulnerable software versions in seconds, not weeks. And go beyond CVSS to assess how much impact a new vulnerability may have on your unique environment, based on a vulnerability's prevalence and exploitability.
- **Vendor Due Diligence**
  Manifest can help your organization identify risk in your legacy products, as well as for new product procurement. By requesting SBOMs from your vendors, you can purchase more secure products, or negotiate with vendors for better security, SLAs, or patch support. It's an easy way to view and assess each of your vendor's security practices and performance.
- **SBOM Generation and Regulatory Compliance**
  Make it easy to comply with the Cyber Executive Order, FDA requirements, or customer procurement questionnaires.
- **Licenses and Software Issues**
  Quickly identify problematic licenses (such as copyleft), no-longer supported libraries, or other concerns.
- **Staff Augmentation**
  By adding automation to the above use cases and serving as a centralized SBOM management tool, Manifest can save your staff valuable time triaging vulnerabilities or performing vendor due diligence, so they can focus on more critical tasks.