SBOM on Rails

How Leading OT Security Company Shift5 Automated its SBOM Management with Manifest

By Manifest and Shift5

WINTER 2024

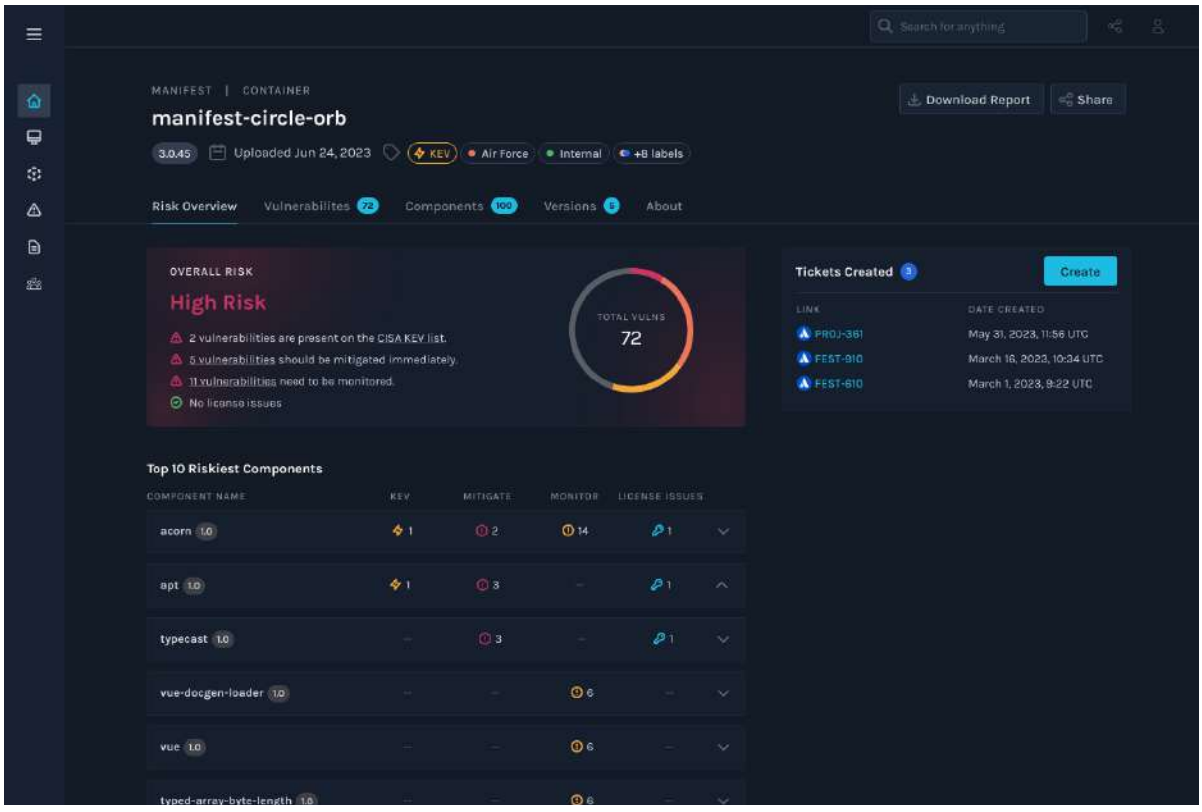
Background

SBOM requirements and initiatives are proliferating in almost every corner of the world: in Europe, in Japan, India and Australia, and most thoroughly in the United States. Defense contractors are confronted with a beguiling patchwork of agency requirements and an alphabet soup of policies such as CRA, NIS2, M-22-18, UNECE 155, and EO 14028. With government contracts potentially at risk, the stakes are enormous, but the complexity and subject matter expertise required to navigate these shifting regulations can feel insurmountable.

Below is the story of how a next-generation OT cybersecurity company used Manifest to automate their SBOM program, generating SBOMs within 90 seconds and automating SBOM compliance.

Choosing a Solution

As a defense tech company with many competing business priorities, Shift5 needed an SBOM management solution that prioritized **ease of deployability**, **walk-up usability**, f**eature completeness**, and an **aggressive and forward-leaning future product roadmap**. Shift5 evaluated several tools in the market, matched them to internal requirements, and determined that Manifest's existing platform and product roadmap offered the fastest onboarding, most user-friendly experience, and greatest likelihood for innovative future product features.



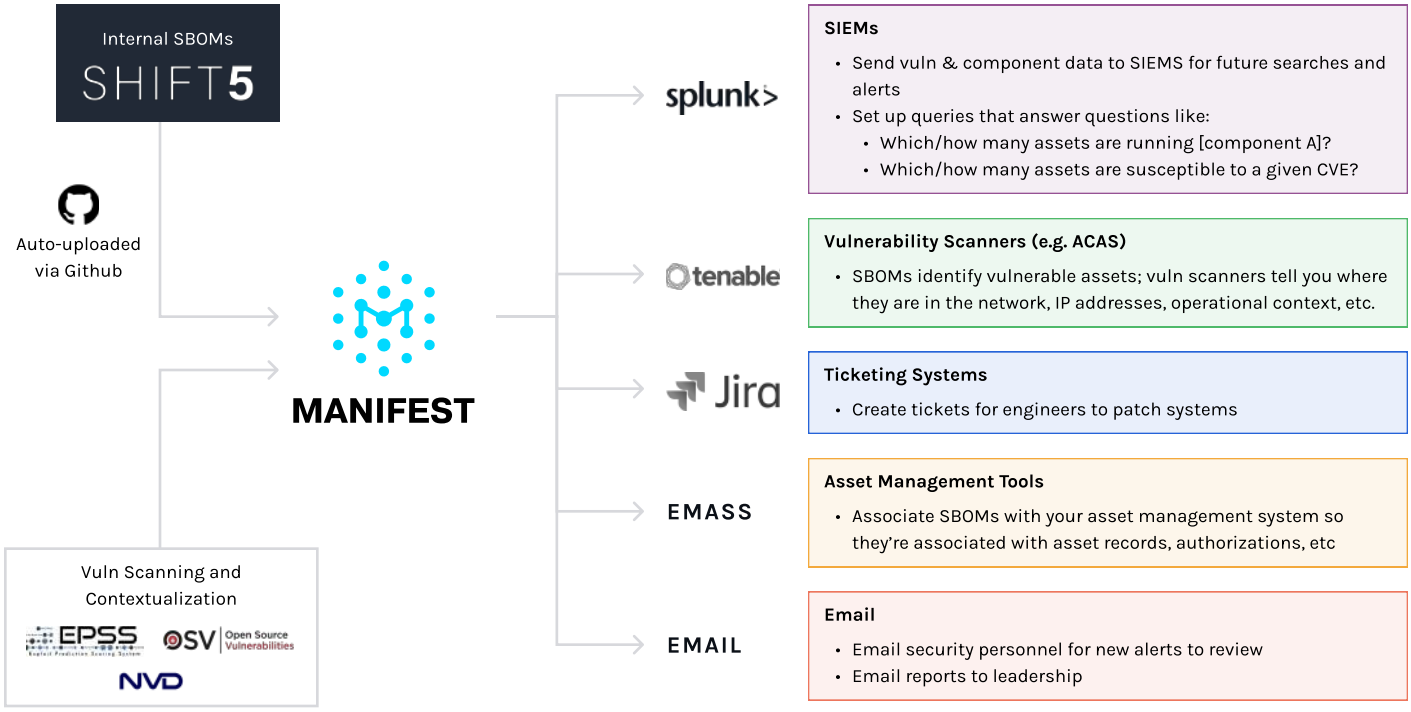
Deployment

To begin the flow of SBOMs, Shift5 utilized two methods for SBOM generation:

1. A lightweight command line interface that embeds within their CI/CD pipelines, which automatically generates an SBOM with each new build;
2. A GitHub integration that provides can be rapidly deployed entirely via the user inferface, without need to write any code.

Shift5 personnel deployed the Manifest application into their CI/CD pipeline and began generating SBOMs. By doing so, each SBOM flows from the build to the Manifest API, where it was stored in the Shift5-specific tenant. With this implementation, Shift5 accounts for each new build of every application going forward, and returns the associated SBOM.

Initial deployment took place in approximately 90 seconds.



Vulnerability Analysis & Continuous Monitoring

Once created and ingested, Manifest enriches the SBOMs with additional data from numerous sources, and then scans them for known vulnerabilities, IP-threatening licenses like copyleft, and other risks.

However, as many security practitioners recognize, a match to a vulnerability, or a CVSS Score of 10/10 does not equate to an exploitable vulnerability. For greater context, the vulnerabilities are then matched to the Exploit Prediction Scoring System (EPSS) from FIRST and CISA's Known Exploited Vulnerabilities (KEV) catalog to determine which vulnerabilities are actually exploitable or likely to be exploitable in the future. As a result, Shift5's security and engineering teams save hundreds of hours per year investigating less risky vulnerabilities, and can immediately address the vulnerabilities that actually pose the greatest risk to their products. What's more, every component is monitored every day for new vulnerabilities, triggering alerts as vulnerabilities are updated and newly discovered.

SBOM Management

Tagging and Organization

Many defense contractors end up drowning in their SBOMs, with hundreds if not thousands of JSON files stored in shared folders awaiting a human to hunt and peck when a new RFI comes in. The Manifest automatic and ad hoc tagging capabilities enable Shift5 to label each new SBOM with a purchase order (PO), environment, project name, or other metadata, so that when a customer calls, the right SBOMs are only a few clicks away.

VEX

In the event of exposure, Manifest's application affords Shift5 the ability to create a Vulnerability Exploitability eXchange (VEX) document, attesting to the exposure or lack thereof. The UI generates VEX documents in both of the leading VEX formats: CSAF or OpenVEX, ensuring that Shift5 will be able to provide VEX documents in whatever formats the industry aligns on.

Secure Sharing

The final step in the SBOM lifecycle is secure sharing with DOD stakeholders. Shift5 utilizes Manifest's in-app secure sharing capability to provide DOD counterparts with one-time links to the relevant and requisite SBOMs. This alleviates the need for Shift5 to transmit artifacts as attachments over email and reducing the number of copies of an SBOM that end up in Downloads folders or on desktops even after the requirement has been met.

Enterprise Deployability

Integrations

Integrating SBOM management capabilities into a broader enterprise security and third party risk management programs affords the opportunity for automation in several areas:

CI/CD Pipelines

By integrating SBOM generation into the CI/CD build pipeline, SBOM compliance can be automated and each new version tracked/recorded for future SBOM RFI requirements.

Asset Inventories

By integrating asset management or asset inventory tooling into an SBOM solution, enterprises can retain records of which vendors have and have not complied with SBOM requests, as well as the age and freshness of the SBOM provided.

Vulnerability Management

By integrating an SBOM management capability into a vulnerability management system, VM teams have a single repository through which they can see software supply chain vulnerability information alongside their other VM streams.

Ticketing Systems

Configuring an SBOM management capability to automatically generate tickets when certain criteria or thresholds (severity, exploitability, environment-based) are met.

Access Controls

With any large or mission-critical organization comes a need to restrict or limit access to the smallest required set. SBOMs, with their rich context around software components, are certainly subject to this requirement.

Within an SBOM management platform, it is essential to have a concept of access control and parent-child organization management. Within Manifest, Shift5 can assign users to individual projects or sub-organizations, while retaining an “overwatch” capability for senior leadership and other key stakeholders.

Outcomes

- **Cost Avoidance**

  Generating, aggregating, organizing, analyzing, tagging, and sharing SBOMs to meet government RFIs and contractual obligations can be a time-consuming and manual process, often landing at the feet of highly trained security personnel. For large defense contractors with multiple repositories and various versions of applications delivered to government customers, sifting through hundreds or thousands of SBOMs takes hours per week.

- **Reduced Contract and Compliance Risk**

  By automating each of these phases in Manifest, Shift5 is able to eliminate the manual SBOM generation, aggregation, organization, and analysis burden.

  Additionally, by deploying Manifest, Shift5 was able to ensure that they are compliant with any SBOM RFI going forward. This has eliminated contractual nonperformance risk.

- **Reduced Mean Time to Remediation**

  Lastly, and perhaps most significantly, Shift5 has developed a comprehensive repository of every open source and third party software component in use by any of its internal applications. With software supply chain attacks rising over 700% per year, being able to immediately identify which applications utilize which components is vitally important. By some accounts, Log4j assessments alone cost tens or hundreds of thousands of dollars per enterprise. Deploying Manifest has reduced that effort to a single click.

Conclusions

SBOM management is now both a regulatory requirement and a mission-critical risk reduction need.

For members of the defense industrial base facing a litany of regulatory pressure, a robust SBOM management program has moved from a nice-to-have to a must-have. Such programs must be comprehensive, swiftly deployed, easy-to-use, and address every facet of the SBOM lifecycle.

Moreover, any enterprise - regardless of size or industry - faces exponentially increasing threats from software supply chain attacks. SBOMs afford those enterprises the opportunity to inventory their software supply chains and respond rapidly to zero-days in ways that were previously impossible.