Scribe

Deliver Secure Products Faster

How Scribe’s SSC Platform Meets the NSA’s *Recommendations for SBOM Management*

Overview

The National Security Agency (NSA), in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA) and other partners, has developed comprehensive guidelines for SBOM Management.

This guidance emphasizes leveraging SBOMs to inform decisions in Risk Management, Vulnerability Management, and Incident Management. To support these objectives, the document delineates the essential capabilities of an ideal SBOM Management System.

This white paper details how Scribe Security meets each requirement established by the NSA for the effective management and utilization of SBOMs.

NSA KEY RECOMMENDATIONS

- Software producers must take ownership of their customers' security outcomes rather than treating each product as if it carries an implicit caveat emptor.
- SBOMs and SBOM management tools play a major part in enforcing the requirement to make software secure by design. They provide a mechanism to determine software component risk and establish a level of confidence in the software's freedom from vulnerabilities.
- Integrate data from SBOMs with acquisition security, asset management, threat intelligence, and vulnerability management in critical systems.
- The inclusion of a container manifest should be required for all software with container components.
- Use digital signatures or authenticated hashes to validate components' (and SBOM's) integrity.
- Inclusion of contract metrics that enable tracking and assessment of the software suppliers' "secure by design" performance.

SCRIBE SECURITY - KEY CAPABILITIES TRUST HUB PLATFORM

Scribe Security offers a comprehensive platform that supports software producers and consumers in managing their software supply chains. The key features and capabilities include:

SBOM Management: Scribe allows the generation, inventory management, and sharing of SBOMs, encompassing critical security aspects such as vulnerabilities, severity, known exploitations, VEX advisories, licenses, reputation, known fixes, and more.

Vulnerability Risk Management: Scribe integrates with multiple data sources to provide up-to-date intelligence, continuous monitoring and alerts on new risks throughout the entire product's lifetime.

Impact Analysis: Scribe provides the tools and data to perform prompt impact analysis (AKA "blast radius") to identify where a CVE is found across the product inventory and how old images are affected by new vulnerabilities.

Build and Deploy Secure Software: Scribe ensures continuous software integrity assurance by continuously signing and verifying software artifacts throughout the CI/CD pipeline from developer to delivery.

Automated Sharing Workflows: Scribe offers automated sharing workflows for SBOMs and attestations through its SaaS Trust Hub to help you easily share your SBOMs, advisories, and other evidence-based compliance requirements in a controlled manner.

Enforce Policies and Demonstrate Compliance: Scribe verifies and enforces SDLC policy and governance at every stage in the pipeline to produce products that are secure by design and by default and ensure compliance.

NSA SBOM REQUIREMENTS AND THE SCRIBE TRUST HUB

SBOM input

#	Requirement	Scribe Comments	Exist
1	SBOM format versions: CycloneDX, SPDX	*Supports CDX, SPDX 2.3 formats*	√
2	Import SBOMs as JSON or XML file types	*Scribe Supports JSON;* *XML support, on the roadmap*	√
3	Check SBOM structure and syntax for compliance	*Scribe validates the SBOM structure prior to signing it as an attestation*	√
4	Alert user of SBOM's compliance with relevant structure and syntax	*Scribe alerts on SBOM compliance violation*	√
5	Include an auto-correct option to assist the user	*On the roadmap*	Planned

Table 1

SBOM output

#	Requirement	Scribe Comments	Exist
1	Export SBOMs using either the CDX or SPDX format	*Supports CDX, SPDX*	√
2	Export SBOMs as JSON or XML file types		√
3	Convert one SBOM format to another		√
4	Convert one SBOM file type to another	*On the roadmap*	Planned
5	Aggregate multiple SBOMs from the SBOM tool's repository into one SBOM	*Scribe offers an Aggregate SBOM capability to manage multiple components collectively*	√

Table 2

Generating SBOMs

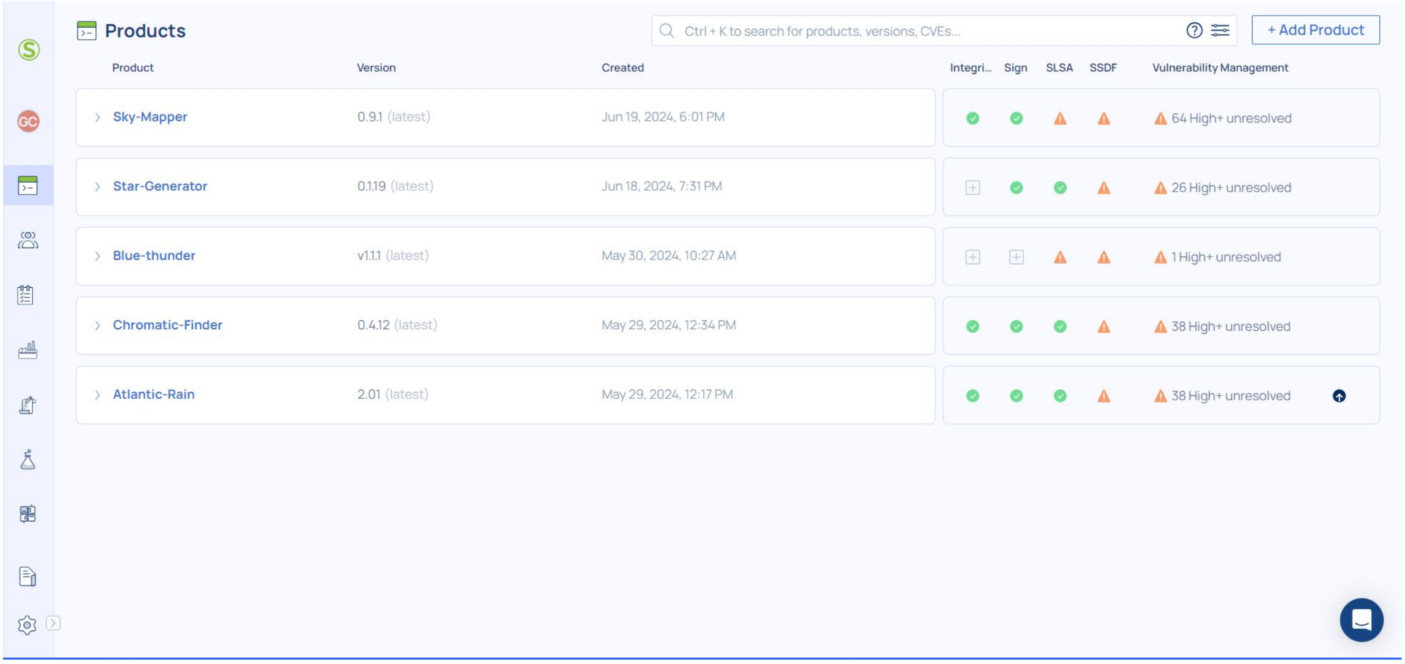
#	Requirement	Scribe Comments	Exist
1	Generate SBOMs from various types of software development process outputs	*CLI tool to generate SBOMs in multiple steps of pipeline (SCM, Build, Image)*	√

Table 3

SBOM component handling

#	Requirement	Scribe Comments	Exist
1	Display NTIA-minimum SBOM fields (Supplier Name, Component Name, CPE, PURL/Hash, Component Version, Component Dependency Relationship, Component Author)		√
2	Enrich SBOM information using additional reference sources	*Supports CVSS, EPSS, KEV, Open SSC reputation, licenses, etc*	√
3	Include mechanisms to graphically represent component dependencies	*Scribe supports advanced BI capabilities*	√
4	Display component provenance information, including external enrichments	*Supports full provenance and SLSA In-toto attestations*	√

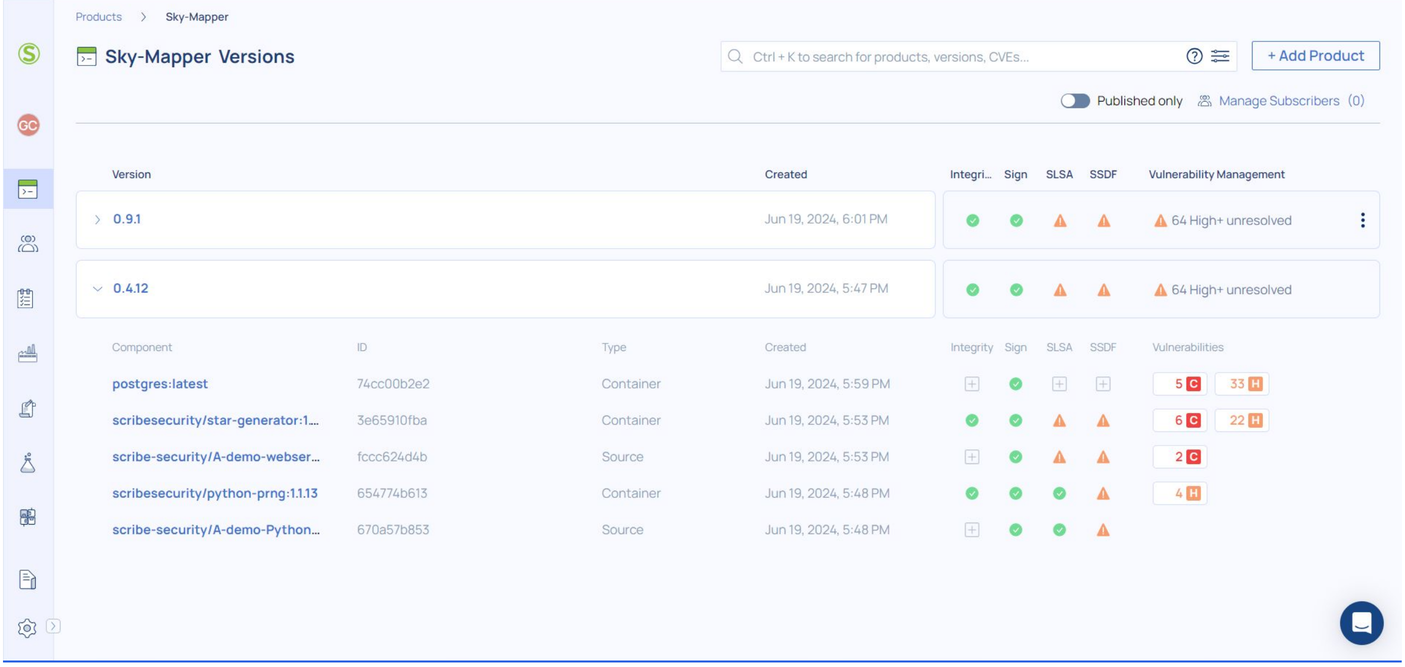
Table 4



Product	Version	Created	Integri...	Sign	SLSA	SSDF	Vulnerability Management
Sky-Mapper	0.9.1 (latest)	Jun 19, 2024, 6:01 PM	✓	✓	⚠	⚠	⚠ 64 High+ unresolved
Star-Generator	0.1.19 (latest)	Jun 18, 2024, 7:31 PM	⊞	✓	✓	⚠	⚠ 26 High+ unresolved
Blue-thunder	v1.1.1 (latest)	May 30, 2024, 10:27 AM	⊞	⊞	⚠	⚠	⚠ 1 High+ unresolved
Chromatic-Finder	0.4.12 (latest)	May 29, 2024, 12:34 PM	✓	✓	✓	⚠	⚠ 38 High+ unresolved
Atlantic-Rain	2.01 (latest)	May 29, 2024, 12:17 PM	✓	✓	✓	⚠	⚠ 38 High+ unresolved

Figure 1.

A screenshot of the Scribe Hub web application displaying products managed within a specific account. It highlights high-level KPIs for each product based on SBOMs and collected attestations, including details such as the latest version, build date, integrity verification status, attestation signature and verification, SLSA compliance, SSDF compliance, and identified vulnerabilities.



Sky-Mapper Versions

Version	Created	Integri...	Sign	SLSA	SSDF	Vulnerability Management
0.9.1	Jun 19, 2024, 6:01 PM	✓	✓	⚠	⚠	⚠ 64 High+ unresolved
0.4.12	Jun 19, 2024, 5:47 PM	✓	✓	⚠	⚠	⚠ 64 High+ unresolved

Component	ID	Type	Created	Integrity	Sign	SLSA	SSDF	Vulnerabilities
postgres:latest	74cc00b2e2	Container	Jun 19, 2024, 5:59 PM	⊞	✓	⊞	⊞	5 C 33 H
scribesecurity/star-generator:1...	3e65910fba	Container	Jun 19, 2024, 5:53 PM	✓	✓	⚠	⚠	6 C 22 H
scribe-security/A-demo-webser...	fccc624d4b	Source	Jun 19, 2024, 5:53 PM	⊞	✓	⚠	⚠	2 C
scribesecurity/python-prng:1.1.13	654774b613	Container	Jun 19, 2024, 5:48 PM	✓	✓	✓	⚠	4 H
scribe-security/A-demo-Python...	670a57b853	Source	Jun 19, 2024, 5:48 PM	⊞	✓	✓	⚠	

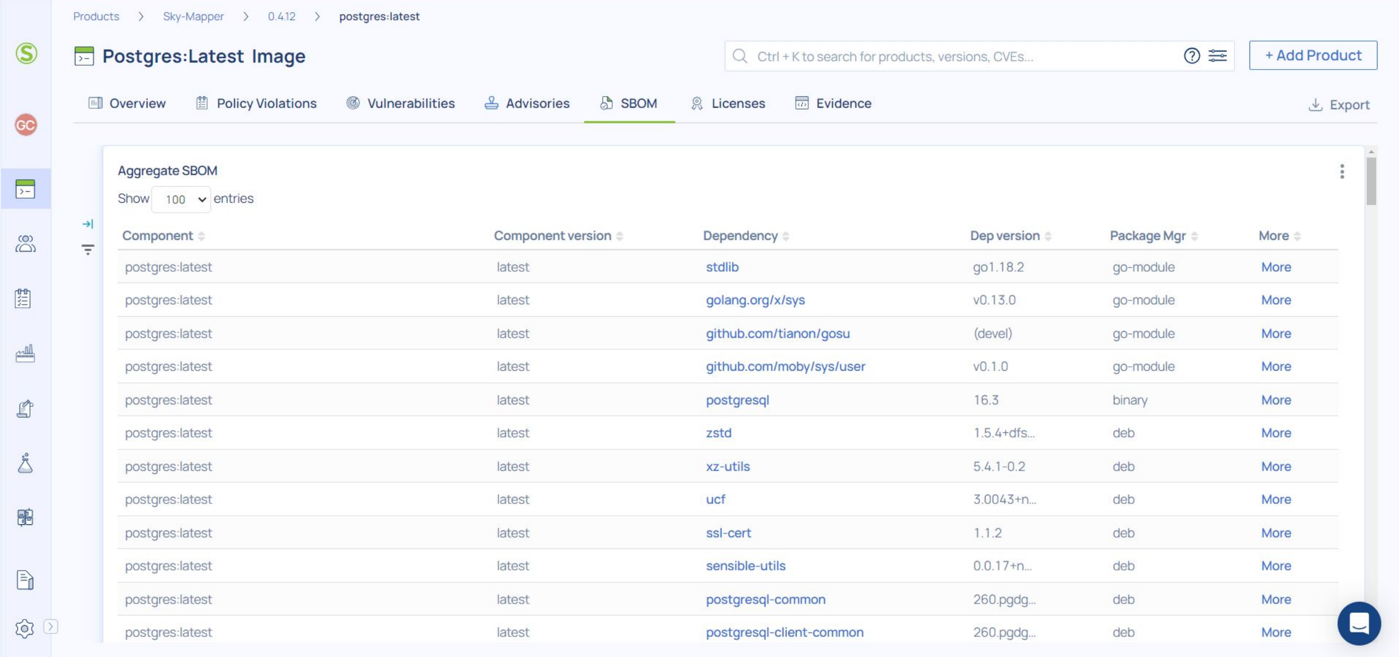
Figure 2.

A screenshot from Scribe Hub, showing a drill-down display into a single product (Sky-Mapper). This display shows all versions of the product documented by the platform - in this case there are two versions - 0.9.1 and 0.4.12. Version 0.4.12 is extended, showing its internal components - these components are based on individual SBOMs collected by the system - the version contains 5 components, 3 of which are Docker image SBOMs and two are source code SBOMs.

Validation of SBOM and SBOM component integrity

#	Requirement	Scribe Comments	Exist
1	Capture and display hash information for each component. Ideally, this validation should provide a digital signature for the SBOM and provenance information for each component		√
2	Include links to information sources where provenance data was gathered		√

Table 5



Aggregate SBOM

Show 100 entries

Component	Component version	Dependency	Dep version	Package Mgr	More
postgres:latest	latest	stdlib	go1.18.2	go-module	More
postgres:latest	latest	golang.org/x/sys	v0.13.0	go-module	More
postgres:latest	latest	github.com/tianon/gosu	(devel)	go-module	More
postgres:latest	latest	github.com/moby/sys/user	v0.1.0	go-module	More
postgres:latest	latest	postgresql	16.3	binary	More
postgres:latest	latest	zstd	1.5.4+dfs...	deb	More
postgres:latest	latest	xz-utils	5.4.1-0.2	deb	More
postgres:latest	latest	ucf	3.0043+n...	deb	More
postgres:latest	latest	ssl-cert	1.1.2	deb	More
postgres:latest	latest	sensible-utils	0.0.17+n...	deb	More
postgres:latest	latest	postgresql-common	260.pgdg...	deb	More
postgres:latest	latest	postgresql-client-common	260.pgdg...	deb	More

Figure 3.

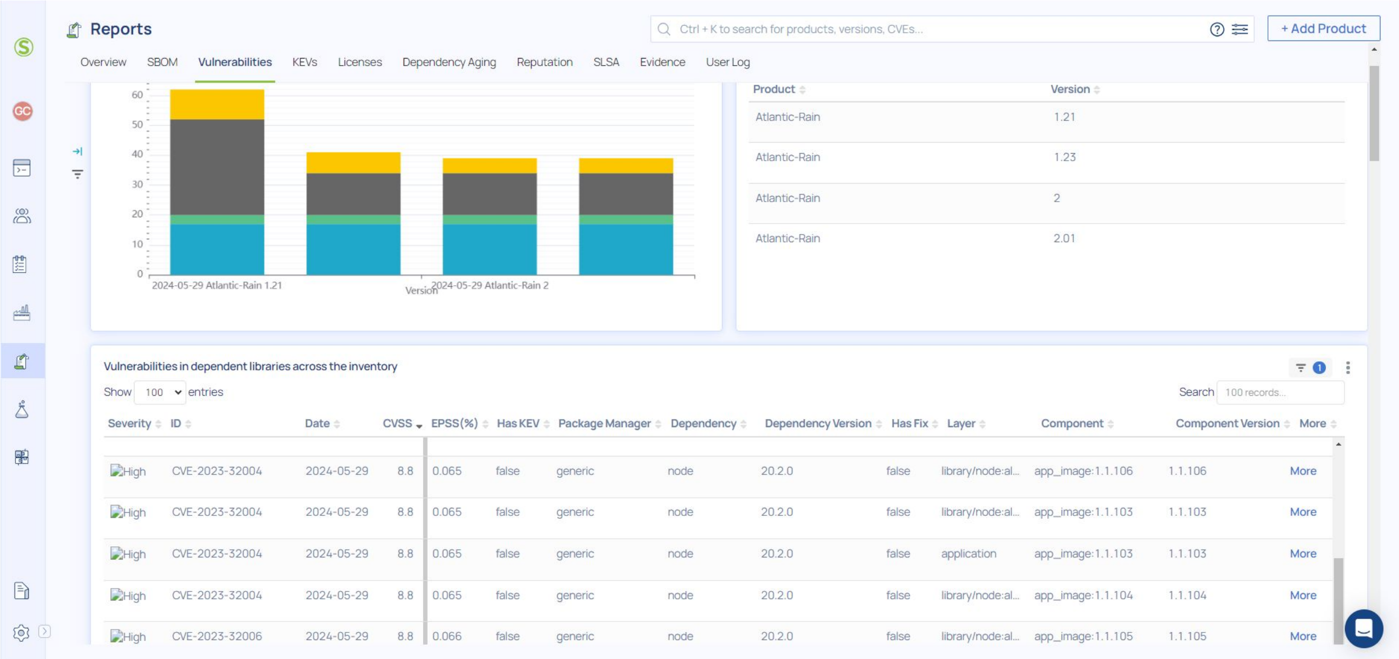
A screenshot from Scribe Hub displaying an SBOM for an individual component within a product. In this example, the component is a public Docker image pulled from Docker Hub, specifically Postgres

. The SBOM lists all dependencies along with their versions, package managers, and additional details. The Scribe platform references such SBOMs against reputation repositories and known vulnerability publications to identify any dubious or vulnerable sub-components.

Vulnerability tracking and analysis

#	Requirement	Scribe Comments	Exist
1	Provide daily updates from the National Vulnerability Database (NVD) and other vulnerability data		√
2	Notify users of new vulnerabilities and updates, including alerts of emergent critical vulnerabilities and their severity	*Notifications can be customized based on the organization's policy*	√
3	Integrate various sources of threat intelligence in addition to the various software vulnerability/weakness databases		√
4	Provide a flexible policy engine, including the ability to apply and update organization-specific policy rules	*Scribe includes a policy-as-code engine to accommodate organization-specific policies*	√
5	Provide multiple ways to identify and research an emergent vulnerability's existence in the user's SBOM repository/asset inventory	*Scribe provides blast radius analysis for known vulnerabilities*	√
6	Support and track the timeliness of vulnerability remediation (including configuration management/traceability to a new SBOM to distinguish the vulnerable, replaced software from the remediated/hardened replacement)	*Scribe offers BI capabilities with customized reports and timeline-based KPI metrics to measure performance across products and teams over time*	√

Table 6



Product	Version
Atlantic-Rain	1.21
Atlantic-Rain	1.23
Atlantic-Rain	2
Atlantic-Rain	2.01

Vulnerabilities in dependent libraries across the inventory

Show 100 entries Search 100 records...

Severity	ID	Date	CVSS	EPSS(%)	Has KEV	Package Manager	Dependency	Dependency Version	Has Fix	Layer	Component	Component Version	More
High	CVE-2023-32004	2024-05-29	8.8	0.065	false	generic	node	20.2.0	false	library/node:al...	app_image:1.1.106	1.1.106	More
High	CVE-2023-32004	2024-05-29	8.8	0.065	false	generic	node	20.2.0	false	library/node:al...	app_image:1.1.103	1.1.103	More
High	CVE-2023-32004	2024-05-29	8.8	0.065	false	generic	node	20.2.0	false	application	app_image:1.1.103	1.1.103	More
High	CVE-2023-32004	2024-05-29	8.8	0.065	false	generic	node	20.2.0	false	library/node:al...	app_image:1.1.104	1.1.104	More
High	CVE-2023-32006	2024-05-29	8.8	0.066	false	generic	node	20.2.0	false	library/node:al...	app_image:1.1.105	1.1.105	More

Figure 4.

A screenshot from Scribe Hub showing a vulnerabilities report based on a set of aggregated SBOMs collected for a single product (named Atlantic Rain) over 4 different versions. The chart displays the evolution of vulnerabilities numbers and severties from version to version. This display also shows the enrichment of the Scribe platform database for external sources - CVSS scores (are collected from NVD), EPSS scores , KEV indications (EPSS and KEV help to focus on exploitable vulns.), whether or not the vulnerability has a fix. Each vulnerability also has an indication regarding the container layer on which it was discovered (application layer or one of the base layers)

Distinguishing identified vs. exploitable vulnerabilities

#	Requirement	Scribe Comments	Exist
1	Indicate whether a vulnerability is actually exploitable and support accompanying evidence and justification for non-exploitable claims. Ideally, it should annotate and update information about the exploitability of a component vulnerability using the Vulnerability Exploitability eXchange (VEX) format	*Scribe fully supports the VEX standard, allowing for the editing of VEX advisories and the consumption of VEX reports. It also integrates EPSS and KEV data to enhance the context of exploitability risk probability.*	√

Table 7

User interface

#	Requirement	Scribe Comments	Exist
1	Provide multiple ways to ‘drill down’ and obtain additional information for software component provenance, vulnerability, license, and risk status.		√
2	Provide means to create structured groupings or categories of SBOMs to facilitate asset tracking, vulnerability management, incident management, etc.	*Supports aggregate SBOM grouping and tagging capabilities*	√
3	Provide the ability to filter/sort/group SBOM information according to user-selectable attributes (such as, by software/BOM type, software/BOM source, software/BOM PoC; component type, component package, component age, component versions, security trend; vulnerability severity, vulnerability count; and organization level, license type, violation).	*Scribe filters any data component across all domains*	√

Table 8

Output forms and methods

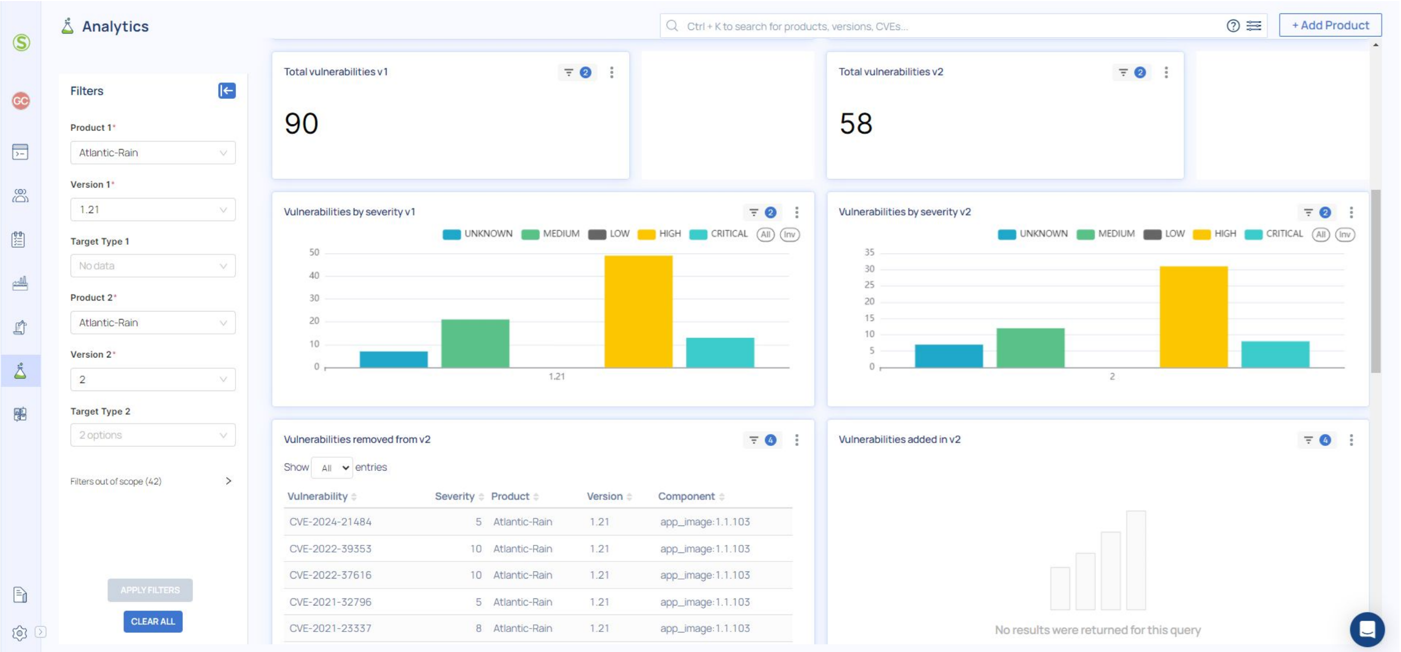
#	Requirement	Scribe Comments	Exist
1	Output standardized reports regarding component attributes, vulnerability information, license information, and component supplier information.		√
2	Export dependency information in graphic and/or text format.		√
3	Output graphic representations of analysis results.	*Comprehensive graphic reports and analytics powered by the Scribe BI engine.*	√

Table 9

SBOM versioning and configuration management support

#	Requirement	Scribe Comments	Exist
1	Include a scalable configuration management capability for SBOMs.		√
2	Include user-tailorable mechanisms to organize SBOMs on multiple information attributes (such as by organization, software supplier, type of software, type of BOM, license type, etc.).		√
3	Include a trend graphic showing the number of vulnerabilities for each severity level across each component version and report whether the numbers of component vulnerabilities are increasing or decreasing with each version release.		√
4	Compare SBOM versions for the same software and highlight differences (such as by different components or different component versions, different sources, etc.).	*Scribe includes SBOM diff capability to identify vulnerability and component changes between versions.*	√

Table 10


Analytics
Ctrl + K to search for products, versions, CVEs...
+ Add Product
Filters
APPLY FILTERS
CLEAR ALL
Vulnerabilities by severity v1
UNKNOWN
MEDIUM
LOW
HIGH
CRITICAL
All
Inv
50
40
30
20
10
0
1.21
Vulnerabilities by severity v2
UNKNOWN
MEDIUM
LOW
HIGH
CRITICAL
All
Inv
35
30
25
20
15
10
5
0
2
Vulnerabilities added in v2
No results were returned for this query

Product 1*: Atlantic-Rain

Version 1*: 1.21

Target Type 1: No data

Product 2*: Atlantic-Rain

Version 2*: 2

Target Type 2: 2 options

Filters out of scope (42)

Total vulnerabilities v1

90

Total vulnerabilities v2

58

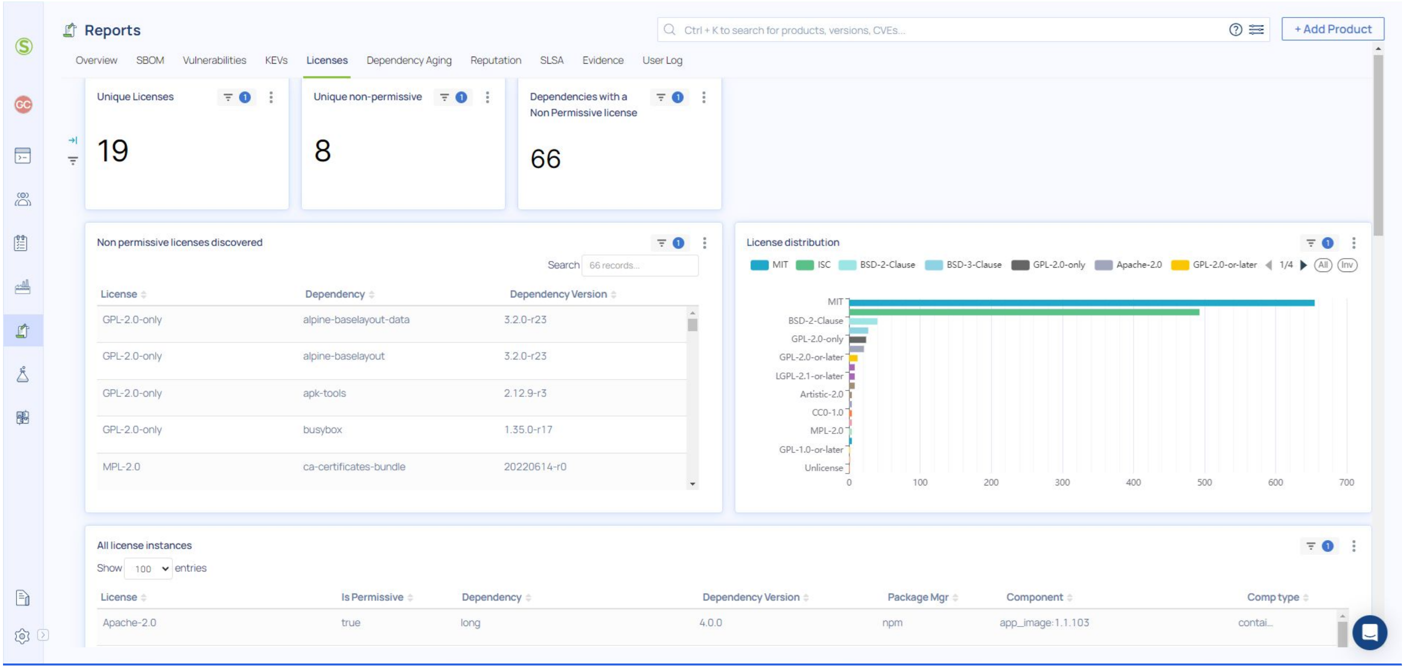
Vulnerabilities removed from v2

Show All entries

Vulnerability	Severity	Product	Version	Component
CVE-2024-21484	5	Atlantic-Rain	1.21	app_image:1.1.103
CVE-2022-39353	10	Atlantic-Rain	1.21	app_image:1.1.103
CVE-2022-37616	10	Atlantic-Rain	1.21	app_image:1.1.103
CVE-2021-32796	5	Atlantic-Rain	1.21	app_image:1.1.103
CVE-2021-23337	8	Atlantic-Rain	1.21	app_image:1.1.103

Figure 5.

A screenshot from Scribe Hub showcasing the SBOM differ tool, which facilitates the comparison of two SBOMs. It provides details such as the number of vulnerabilities added or removed, the licenses discovered, and the total number of dependencies in each SBOM.



Unique Licenses: 19

Unique non-permissive: 8

Dependencies with a Non Permissive license: 66

Non permissive licenses discovered

Search: 66 records...

License	Dependency	Dependency Version
GPL-2.0-only	alpine-baselayout-data	3.2.0-r23
GPL-2.0-only	alpine-baselayout	3.2.0-r23
GPL-2.0-only	apk-tools	2.12.9-r3
GPL-2.0-only	busybox	1.35.0-r17
MPL-2.0	ca-certificates-bundle	20220614-r0

All license instances

Show 100 entries

License	Is Permissive	Dependency	Dependency Version	Package Mgr	Component	Comp type
Apache-2.0	true	long	4.0.0	npm	app_image:1.1.103	contai...

Figure 6.

A screenshot from Scribe Hub showing the licenses report based on analysis of the SBOMs collected. The results of the analysis can be presented in a report (like the one shown here) or used as an input to Scribe's policy engine. The policy results (compliance or violation) can be used to generate alerts or to enforce the policy by stopping a build pipeline or stopping the deployment of a component based on any discovered violations.

Integration and workflow with other systems

#	Requirement	Scribe Comments	Exist
1	Employ "API First" design to facilitate import and export of information with other systems.	*Provides a fully documented API*	✓
2	Integrate with multiple types of SBOM sources and other data that can be combined together for analysis.	*Supports importing and exporting SBOMs in multiple formats.*	✓
3	Leverage format-agnostic, independent, stateless, and scalable API capabilities (such as REST) to automate processes/workflow.		✓
4	Support a secure, integrated Producer/Consumer exchange ecosystem.	*Scribe Trust Hub is a secure Producer/Consumer exchange system on a SaaS platform, certified to SOC Type 2 standard*	✓

Table 11

Supporting access to data sources

#	Requirement	Scribe Comments	Exist
1	Integrate AI/ML engines and associated 'data lakes' that analyze SBOM component information against diverse types of threat signatures and patterns.	*In roadmap*	Planned
2	Include an updatable library of open-source software licenses that the SBOM management tool identifies and tracks where applicable.		√

Table 12

Scalable architecture

#	Requirement	Scribe Comments	Exist
1	Include mechanisms to support distinct sub-organizations within an enterprise that may have different risk tolerance rules or policies.		√
2	Handle other types of BOMs.	*Scribe Hub is an attestation-driven platform that enables the upload and management of any type of attestation, such as Helm charts and other types of security-related files.*	√
3	Be part of or support a suite of tools that work together to accomplish Risk Management, Vulnerability Management, and Incident Management activities.	*Scribe API*	√

Table 13

SBOM tool setup and configuration

#	Requirement	Scribe Comments	Exist
1	Provide mechanisms and supporting materials to easily download, setup, and integrate in Linux or Microsoft environments. Ideally, it should support both environments.		√

Table 14

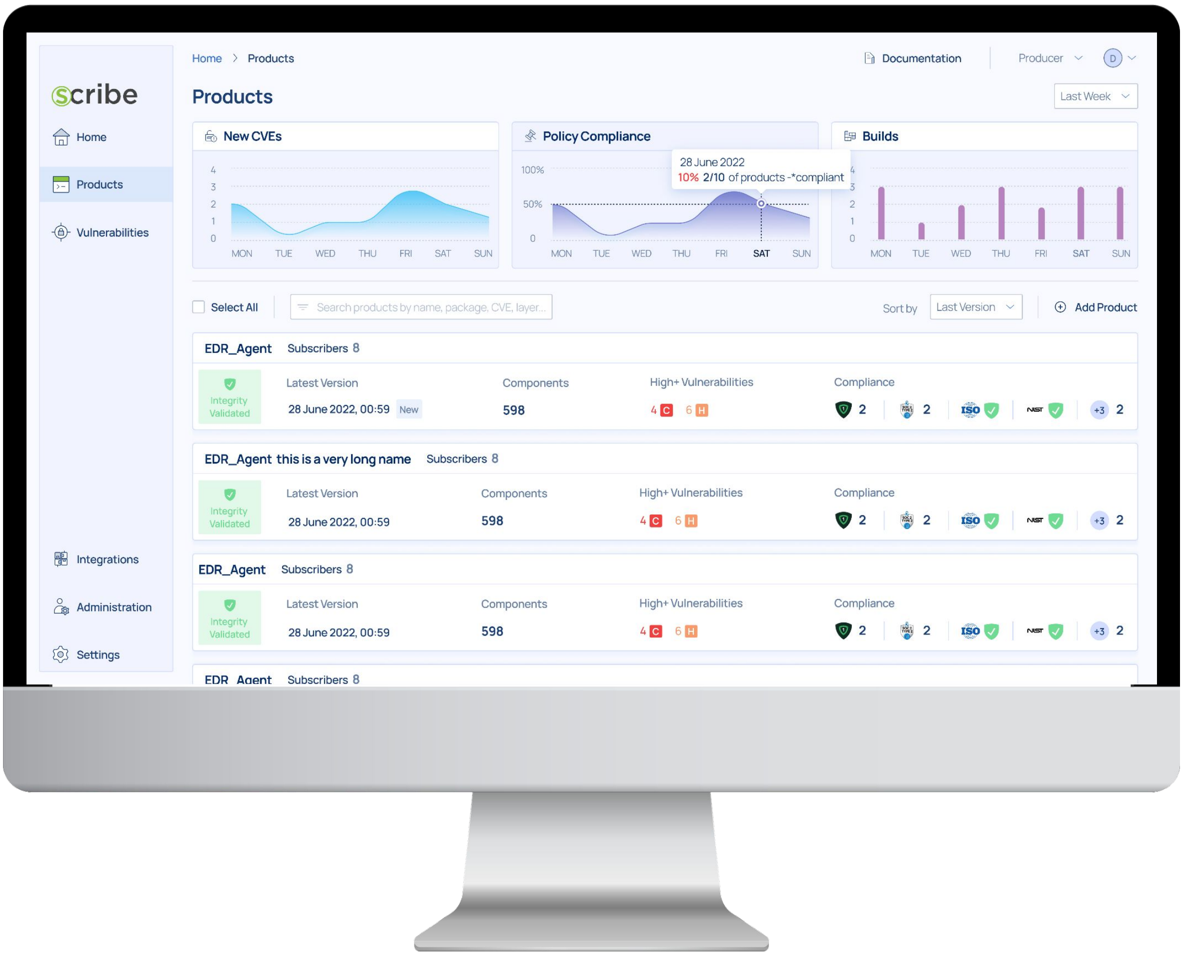
Putting it all together to deploy in relevant use cases as described.

NSA Use Cases	Scribe Solution
Pre-Acquisition Risk Management	Scribe allows organizations to evaluate and manage risks prior to software acquisition. Vendors can confidentially share SBOMs with access control. When an SBOM is not available, consumers can use Scribe to generate and manage SBOMs and associated vulnerabilities. Scribe also supports the ingestion of third-party SBOMs, SCA/AST scans, and VEX advisories. Enhancing this process, Scribe offers reputation scores, license analysis, vulnerability intelligence, and update recommendations.
Post-Deployment Vulnerability Analysis	Scribe monitors SBOMs continuously, identifying vulnerabilities through ongoing scanning of intelligence feeds. It captures SBOMs at various points in the SDLC, merging and de-duplicating them to provide comprehensive security insights. Scribe performs analytics, such as comparing SBOMs of different builds to detect degradations and analyze the impact of new vulnerabilities on old images. Additionally, Scribe provides vulnerability intelligence, including EPSS, CVSS, KEV, reputation scores, and update recommendations.
Incident Management	Scribe features real-time threat detection alerting, and blocking. The platform continuously collects and signs security evidence throughout the SDLC, creating an immutable audit trail to support effective incident response and forensic analysis. This ensures the swift identification and mitigation of security threats and CI/CD exploitations, including blast radius impact analysis.
Software Asset Risk Management	The platform provides centralized SBOM management, application security posture management (ASPM), continuous code signing, provenance, and integrity checks, supporting comprehensive Cybersecurity Supply Chain Risk Management (C-SCRM) strategies. Additional features include reputation scores, license analysis, and base image identification.
Transparency and Lifecycle Management	Scribe ensures transparency through automatically generating and managing SBOMs, offering visibility into software assets and associated risks. Through its SaaS Trust Hub, Scribe provides automated workflows for sharing SBOMs and attestations. Software consumers can enforce their policies and receive alerts about new vulnerabilities relevant to their SBOMs, with SBOMs generated for each release. Scribe also enables impact analysis and continuous monitoring for new known vulnerabilities.
Integration with Best Practices	Scribe integrates industry best practices and standards into its platform, such as SLSA. The platform offers organizations a customizable policy framework security guardrails based on risk analysis and open-source dependency management.

Table 15

SUMMARY

By adhering to the NSA's SBOM recommendations, Scribe Security enables organizations to achieve high levels of security and integrity in their software supply chains. This document illustrates how the Scribe Trust Hub platform meets these requirements and highlights Scribe's dedication to enhancing software supply chain security.



EDR_Agent Subscribers 8

	Latest Version	Components	High+ Vulnerabilities	Compliance
Integrity Validated	28 June 2022, 00:59 New	598	4 C 6 H	2 2 ISO NIST +3 2

EDR_Agent this is a very long name Subscribers 8

	Latest Version	Components	High+ Vulnerabilities	Compliance
Integrity Validated	28 June 2022, 00:59	598	4 C 6 H	2 2 ISO NIST +3 2

EDR_Agent Subscribers 8

	Latest Version	Components	High+ Vulnerabilities	Compliance
Integrity Validated	28 June 2022, 00:59	598	4 C 6 H	2 2 ISO NIST +3 2

EDR_Agent Subscribers 8

If you've made it this far, you're ready to get started!

START FOR FREE

Have more questions?

Contact Us

Want to see it in action?

Schedule a Demo