# Scribe SOFTWARE SUPPLY CHAIN CONTINUOUS ASSURANCE



#### Scribe will secure your software while improving time to market



Gain **full visibility** of **software assets**, **dependencies** and **security aspects** with a leading SBOM management system

Effectively **Control** and **Mitigate Risks** in your software factory and products by enforcing **automated secure SDLC guardrails**, without impeding dev speed nrevent so

Detect and prevent software tampering and CI/CD exploitations by automating continuous code signing and attestations

#### The first evidence-based software security trust hub

At Scribe, we recognize the delicate balance between security and operational efficiency, where every security decision impacts product delivery, customer service, time to market, and ultimately, your revenue.

				Evidence												
				Time :	Predicate Type :	Target Name :	Pipeline Run :			Labels 0	Signed By 0	Origin Platform :	Origin :	Download :	Project	
				2023-09-14 14-29-08	SBOM OycloneOK	pertest	latest:sha256_u003a878			NEA	Scribe Security	Jerkins	PR/L002/PRO-TEST	Download	NA	
				2023-09-1414-28.58	SBOM CycloneOK	jeniono-pio-example/	2023_09_14t14_u005e28_u003e8	58z		NEA	Scribe-Security	Jenkins	PRAUDO2FPR-TEST	Download	NA	
				2023-09-14 14:28:57	SBOM CycloneDK	jeniono pri examplez.	2023_09_14t14_u003a28_u003a56z			['is_gt_commt']	Scribe Security	Jenking	PKAL000PPRO TEST	Download	NA	
				2023-09-14 14:23:32	SBOM CycloneOK	plotest	latest:sha256_u003a03d			NIA	Scribe-Security	Jerkins	PKIL002FPI0-TEST	Download	NA	
				2023-09-1414:23:23	SLSA Provenence	pei-test	latest-sha256u003a03d	NEA	Scribe-Security	Jenkins	PKAU002FPRI-TEST	Download	N/A			
	Products			Search for products, versions, CVE	a. 📰 f	Documentation	2023_09_14114_L003x23_L0	ViteSuo Version sha1\u003A5772d22114a199836d9475149b270b64bcf92638								
							2023_09_14t14_u003t23_u0	Version shall	u003A5//2d22114	0192638			NA			
cribe	Products							🕒 Overview 👘 Co	mplance 🛞 Vulnerabiliti	es 🐣 Advisories	S SBOM S Li	censes 🗵 Contex	et		NA	
	= Search produc	ts by name, package, CVE, laver	0			Add Product	latest sha256_u003a92e								N/A	
Products							2023_09_14t14_u003a16_u0	T Search by policy, mass	aga	0					NA	
Vulnerabilities	Demo Product	Subscribers 5 💿 Invite Subscr	ibers 📋 Delete Product				latest-sha2560003a821			Policy			Message		Link	
VOINERADEIDES		Latest Westion	Components	High+ Vulnerabilities	Compliance		latest:stva256_u003a821	Status	Compliance		nce Available	No provenance fi			Link	
Subscribers	Integrity	April 24, 2023 at 12:46 PM	779	23 🖪		NET 30/36	2023_09_13115_u003e54_u0	A Failed							Link	
	Validated				•••		2023_09_13115_u003454_u0	🦁 Plasad	SLSA L1	Build Sc			ted github/vorkflows/sneate-unsigned-git-clone-and-unsigned-i	_	Link	
Integrations							2023_09_13115_u003464_u0	Passed	SLSA 12		nce Service Generated		is generated by the build system.		Link	
	EDR-agent N	Subscribers					latest:sha256_u003a1cb	Passed	SLSA L2		nce Authenticated		is authenticated with this a sig.	_	Link	
	-	Latest Version	Components	High+ Vulnerabilities	Compliance		latest-sha256_u003a1cb	Passed	SLSA L2	Build Se			uted by a service 'OitHub Actions'.		Link	
	Integrity	April 24, 2023 at 5 19 AM	573	1 2 12 11		AMP 30/36	2023_09_13115_u001e51_u0	Passad	SLSA 12		Ansion Controlled	The code is many			Link	
	Validated				••		2023_09_13t15_0003a50_00	Passed	SLSA L3		Ratory Verified		lections rules require signed commits.	_	Link	
							252587626267896666293049 2023_09_13t14_c003651_c0	Passed	SLSA 🚺	Build Iso	lated	Scribe determine	ed that the build environment is isolated.		Link	
	Fleet-Manager	No Subscribers				2023_09_13114_0003861_00	Passed	SLSA L3	Source	Retained Indefinitely	Branch main prot	tections rules disallow deletions.		UNK		
	-	Latest Version	Components	High+ Vulnerabilities	Compliance			💙 Passad	SLSA 🗳	Build Ep	hemeral Environment	The build is run in	an ephemeral environment on DitHub-hosted runners.	_		
	Integrity	April 24, 2023 at 5-38 AM	779	11 C 47 11		N#F 30/36		💙 Passed	SLSA L3	Build As	Code	The build is defin	ed and configured as code, github/workflows/create-unsigned-git	-d.		
	Validated	April 2020 10 000 APR	174		A 0	- 30/36		💙 Passed	ST24 12	Provena	nce Non Falsifiable	Provenance carri	not be failsfied by the build service's users. Default checks were per	10.		
								A Failed	S NSTSSOF	Ensured	ode owners are set for e	et For every code re	pository in use, identify particularly sensitive parts of code and cor	a		
Settings	NMEA-gatewar	No Subscribers				0		A Failed	R NETSEDF	Ensure f	orce pushes code to bra	n. For each reposito	ary in use, block the option to "Force Push" code.	0		

#### Scribe continuously attests to your software's security and trustworthiness:

- Centralized SBOM Management Platform Create, manage and share SBOMs along with their security aspects: vulnerabilities, VEX advisories, licences, reputation, exploitability, scorecards, etc.
- Build and deploy secure software Detect tampering by continuously sign and verify source code, container images, and artifacts throughout every stage of your CI/CD pipelines
- Automate and simplify SDLC security Control the risk in your software factory and ensure code trustworthiness by translating security and business logic into automated policy, enforced by guardrails
- Enable transparency. Improve delivery speed Empower security teams with the capabilities to exercise their responsibility, streamlining security control without impeding dev team deliverables
- Enforce policies. Demonstrate compliance Monitor and enforce SDLC policies and governance to enhance software risk posture and demonstrate the compliance necessary for your business

# **S**cribe

 $( \mathbf{P} )$ 

#### **Software Trust Hub**

Scribe is a SaaS solution that provides continuous assurance for the security and trustworthiness of software artifacts, acting as a trust hub between software producers and consumers. Scribe centralized SBOM management system allows to effortlessly manage and share products SBOMs along with all their associated security aspects in a controlled and automated manner.

#### **SDLC Governance & Compliance**

Scribe empowers you to implement security by design and by default into your pipelines. Stakeholders can apply any policy over the collected attestations to enforce SDLC policies and governance without hindering agile development and delivery. Scribe allows gauging compliance to any set of policies, standards and requirements, such as SSDF, CIS or SLSA framework.

#### **Software Integrity and Provenance**

Scribe continuous code signing and assurance enables you to proactively detect and address malicious changes and interventions in your software components, artifacts, and development processes and tools. Scribe validates the integrity and provenance of the software build at every stage. All software components are tracked throughout the software development lifecycle, from source to production.

## **Observability and Attestations**

Manage the risk inherent in your software artifacts and gain back control over your software development processes by using the latest attestation concepts and technology. Scribe automatically and seamlessly generates, collects and signs evidence from source code managers, CI tools, build servers, container registries, and cluster admission controllers. It uses signed evidence to attest to the resulting product integrity and security. Your attestations are cryptographically signed utilizing your own PKI or Sigstore.

								Products >	Demo_Prod	uct						learch for products, versions, CVEs	E Documentation
					Scri	be	I Overv	iew Z Si	bscribers								
				Products										Published Only	A Subscribers		
				3. Subscrib	iers	<ul> <li>Versi</li> </ul>	0 Subscribers										
							ation		Al/3556458b     BuildBate June 6, 2023 st 1152 PM								0 New Invites Sent
									conents		nerabilities		Integrity			re Repo URL	O New Protes Sent
						89 Integrati	ons		o-express		4 🖸	18 🖬	A Modifie	d		ned 🖸 https://github.com/8	
								mong	o-express		4 🖸	18 🖬	A Modifie	d		ned 🔄 https://github.com/S.,	
								mong	o-express		40	18 🖬	A Modifie	d		ned Mttps://github.com/S.,	
scri	20							Show7	more								
		nian 55 optic		Compose. 11 option	n v Campon. 19			~ 30	d874615675	Build Date J	une 6, 2023	at 11:46 PM					
					Reputation SLSA-12 Dvda			~ 61	009208/38a2.	Build Date J	une 6, 2023	at 11-43 PM					
neges		Outset	wd.		Dece images		.censes										
1		18k			5		34										
ogregate S	on ercies																
Product :	Vention :	Component	Component	Dependency :	Dependency version :	Dependency latest version	Peckage Manager	· Layer ·	Licenses :	la permissiva :	OpenSSF score :		C+H 580		SCA		
NO-5kgra lemo-	latest sha256_u003a72a		latent.	unid	340	200	nom	library/hode/14- alpine		true .	4.9 2		0 image		scribe		
NO-Sign- terro- insject	intent sha256_u003a92e	pio-tent.	latest.	uti-ja	441	551	.npm	library/hode/16- alpine	RSD-2-Citazon	true	27 0		0 image	NM	acribe		
90-5qn-	latest sta256_u003a92e	po-test	latest.	taugr-conkie	25.0	A13	non.	library-mode 14- alpine	85D-1-Cause	true	6.1 2		0 inage	NA	some		
roject																	
project PIO Skgry demo- project	lotest-priv256_u003a92e	po test	Wast.	request	2882	2.88.2	npm	library/hode 14- alpine	Apache 2.0	0100	5.0		0 image	NA	sorbe		

# SCRIBE KEY FEATURES:

Gain visibility and control the risk of all your products' security aspects.

Trust but verify: streamline security guardrails to verify secure SDLC policy, based on trusted evidence.



Simplify secure SDLC processes, balancing responsibilities between dev and security teams.

</>>

Detect code tampering and software factory exploitations.



Enforce and demonstrate compliance with regulation and best practices.



Share SBOMs and security insights in a controlled manner with stakeholders.

## **ABOUT SCRIBE**

Scribe was established by seasoned veterans in cyber security and cryptography who share a common mission: to develop and offer the ultimate, all-encompassing solution for software supply chain security. Drawing on our extensive expertise, we created an innovative platform that harnesses cutting-edge concepts and modern frameworks. The result is a security solution that leaves no room for compromise – safeguarding your software factory and products at every stage of their lifecycle, from production to delivery.

