

SOLUTION SHEET - CAPABILITY SPOTLIGHT

Evidence Collection

Instill Trust to Your Software Releases



THE CHALLENGE

There is an increasing need for attestation of actions, tools, and processes taken against software across the SDLC. Emerging regulations and policies around software development are rapidly evolving, and it's important to stay ahead of the changing landscape.

Some organizations have taken a proactive approach with home-grown solutions or manual processes, but despite best efforts, these solutions often lack scale and eventually falter over time. And inevitably, there's increasing friction between DevOps, GRC, and Development teams, which makes the situation more challenging.

THE SOLUTION

JFrog's new Evidence Collection functionality expands its Release Lifecycle Management capabilities to enrich artifacts, builds, and release bundles with signed attestation metadata that can be easily tracked and verified for governance and compliance.

Evidence Collection generates an audit trail that documents all the security, quality, and operational steps taken to produce a production-ready software release. Seamlessly consolidate information from all the tools and platforms used in software development into a trusted single source of truth.

KEY BENEFITS



Ensure Release Readiness of Software

Easily capture proof of the process software went through as it matured for release, inclusive of all tests, approvals, environments, and processes across the SDLC.



The Single Source of Truth for Attestation

Return time to development and auditing teams by eliminating the need to search across multiple systems for attestation data.



Simplify Auditing and Compliance

Evidence metadata follows the artifact for its entire lifespan, and is tracked and verified before a decision to release software to production. Use attestation metadata, such as signatures or test results, for governance across the software development lifecycle and software supply chain.

PRODUCT CAPABILITIES



Attach evidence to a subject (artifact, package, build, or Release Bundle) via JFrog CLI or API; the evidence follows the subject throughout the promotion process as an attached evidence file.



View the evidence graph of a Release Bundle, which consists of a visual look of all evidence artifacts, subjects, and its relationships.



Export evidence files for easy consumption by cross-functional stakeholders.



EVIDENCE COLLECTION IN ACTION ON THE JFROG PLATFORM

<	odf	NII,	5 4	γy	odl	The	nulC	1616	ease		1.5					~																									action (ons				ĸ
Version	n tin	telin	e	Xra	Y	Ev	ide	ice g	trap	h																																				
	Reb	ase	Bun	sie	0	Bui	id					Evid		e																																
																																					1	1		1	3	1	1	÷.		
														cal	l-m	ode	rat	ion					1		-	g	reen	piza	za-b	uili	1					2	gr	reer	npiz	zza-	bur	ndle	e			
												-	7	10									_	5	0	1.	1.2							L		Ø	10									
												-											1	-		den							~	1	=											
												10	2vic	enc	e fil	le at	tad	he	1			^	J.	3	evi	aen	ce fi	nes	atta	ach	ed		^		4	evi	den	ce	files	s at	tacl	hed		Ξ,	^	5
														sign	atu	re						1			27	bu	ild.s	ien	atur	re				1		D.	cyc	lor	reda	y.sh	200					Ľ
																												-0'''																		L
													Wo	kflo	w			F	zb (26, 3	2024	1			W	orkfl	ow			F	eb 0	6, 20	024	J		Qu	ality	1				Feb	06,	202	24	J
																									-									1		-										ĥ
																									C	chi	arge	elog								0	cyc	lon	ied>	<-ve	łx					L
												-	4			pizz	a-a	pp							W	orkfl	ov			F	eb 0	6, 20	124			Se	curit	y				Feb	06,	202	24	L
															2																			1												1
												1.	evic	end	e fil	le at	tad	he	8			^			0	501	har-i	resu	ılts							ය	Pro	m	otio	n						L
																									W	orkfi	ov			,		6.20	12.4			W	orkfl	ow	1			Feb	06	207	24	L
																																														2
												1	3	sign	atu	re																				0	cyc	lor	reda	x-ve	x					Ľ
													Wo	kflo	w			F	zb (06, 3	2024																									L
																																				Se	curit	У				Feb	06,	202	24	J
+																																														

The evidence graph shows what types of evidence are collected when

Q. Search	▼ Clear			*1	My Favorites Tree view:	10 L.			
산 roni-bundle-test 산 a123-release-bundles-v2 산 Trash Can bank32-release-bund	release-bun		roperties Evidence	Followers Buil		2 *			
ィー ごう catalina-release-bundles-v2	10 Related Evid	ence files	Q Search Evidence						
Catalina-Bundle/1.0.0	Verified ~	Evidence Type	- Category	Time v	Created By v				
release-bundle.json.evd	٥	Test result	Quality	15 May 2020 8	Leslie Alexander				
Catalina-bundle/1.0.0	٠	Vulnerability scan	Security	15 May 2020 9	Wade Warren				
Catalina-michael/1.0.0		Build providence	Workflows	15 May 2020 9	Cameron Williamson				
Demo-Catalina/1.0.0		Approval	Auditing	15 May 2020 8	Darrell Steward				
release-bundles		SBOM	Security	15 May 2020 9	Annette Black				
adam-debian-virtual		Commit	Workflows	15 May 2020 9	Jane Cooper				
adam-docker-flow-virtual		Commit	Workflows	15 May 2020 8	Albert Flores				
adam-docker-virtual	•	Code scan	Security	15 May 2020 8	Ralph Edwards				
🗊 Trash Can		Curation	Security	15 May 2020 8	Jenny Wilson				

The artifact evidence table shows a list of evidence files associated with the artifact

<u>v0.0101124</u>

ABOUT JFROG

JFrog empowers thousands of DevSecOps organizations globally to build, secure, distribute, and connect any software artifact to any environment using the universal, hybrid, multi-cloud JFrog Platform.

LEGAL STATEMENT

Copyright © 2024 JFrog LTD. JFrog, the JFrog logo, and JFrog Artifactory are trademarks or registered trademarks of JFrog LTD or its subsidiaries in the United States and other countries. All other marks and names mentioned herein may be trademarks of their respective companies.





www.linkedin.com/company/jfrog-ltd