

Enforcing the OpenSSF Ecosystem

Enforcing the OpenSSF Ecosystem

with



Hello, I'm @puerco! 🙌

- ▷ Software Engineer @ Carabiner
- ▷ Technical Lead on the Kubernetes Release Engineering team (SIG Release)
- ▷ Technical Lead of OpenVEX and Protobom (incubating in OpenSSF)
- ▷ SPDX Project Contributor
- ▷ I like to ride my bike around the world! 🚴

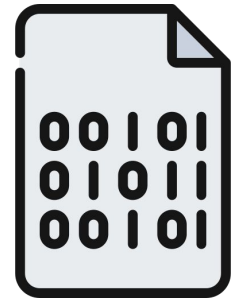


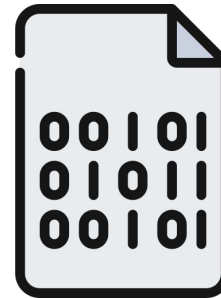


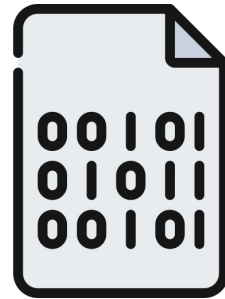
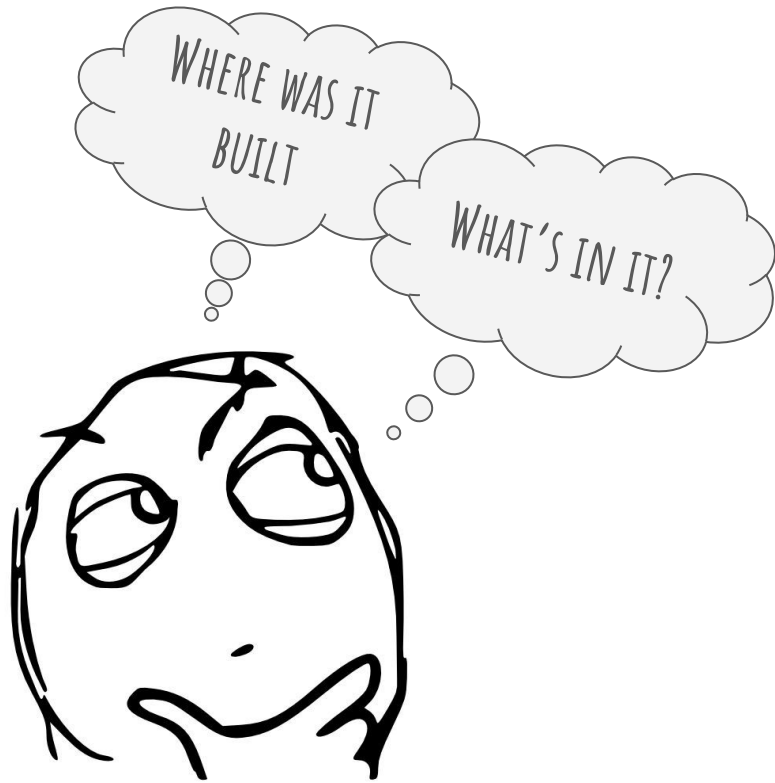
carabiner
systems

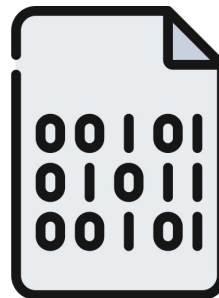
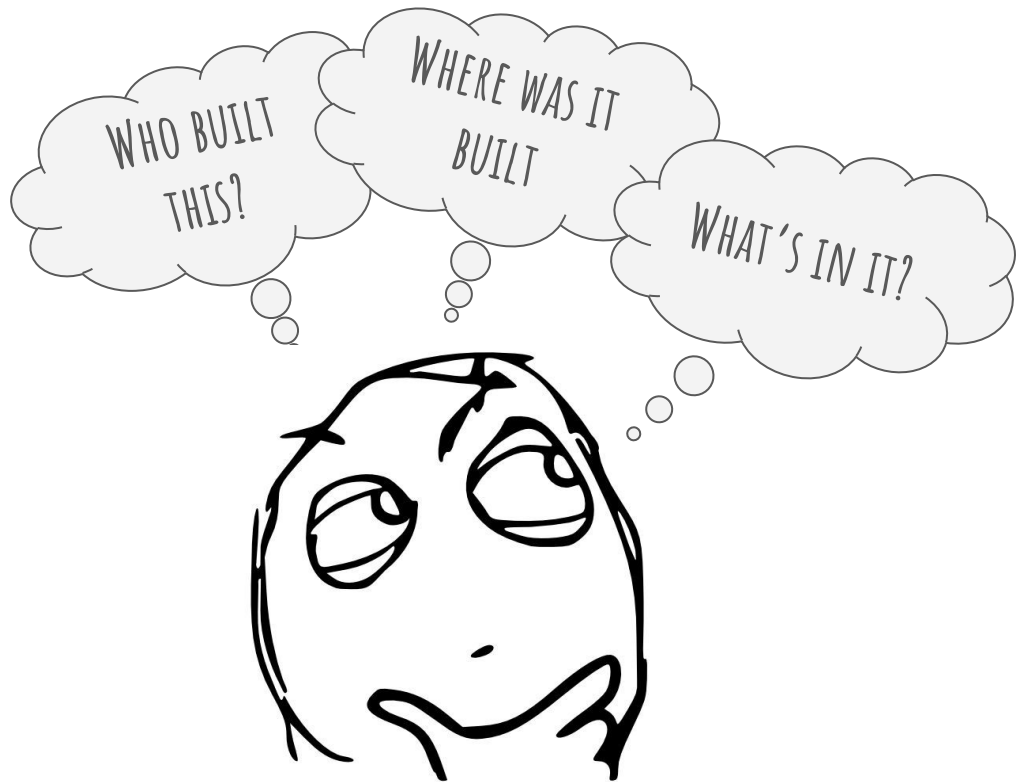
Supply Chain Transparency

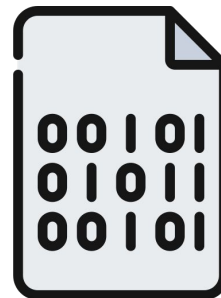
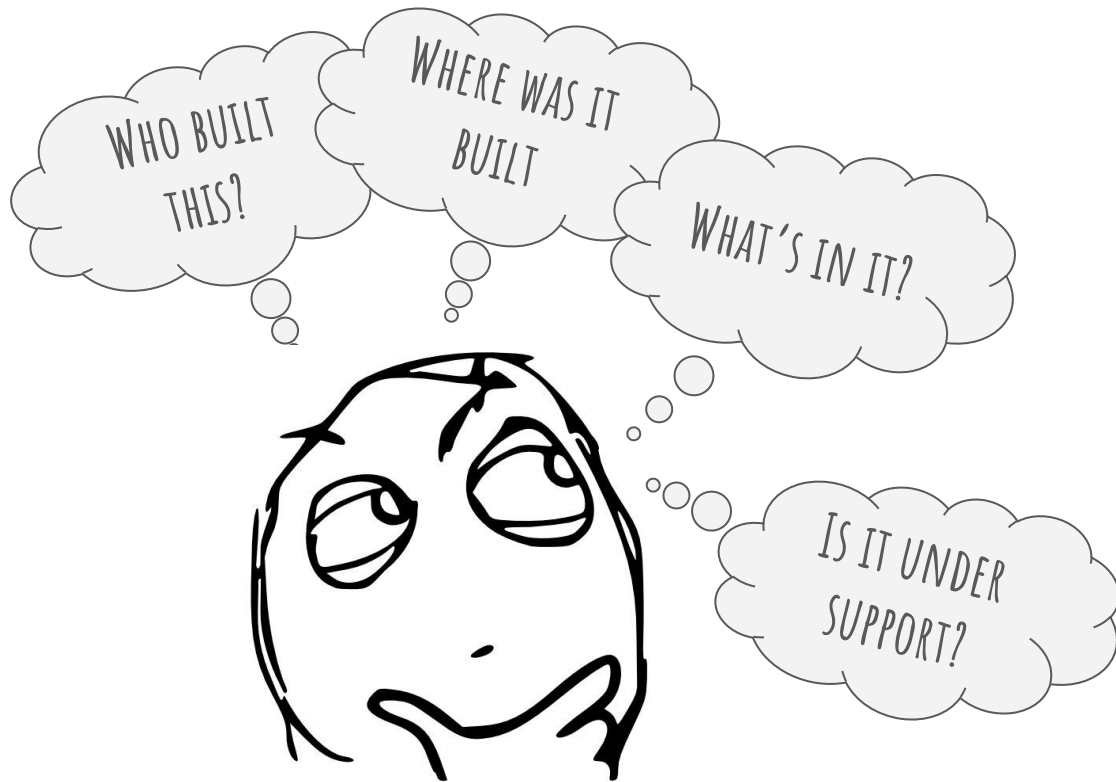
or, verifiable software consumption

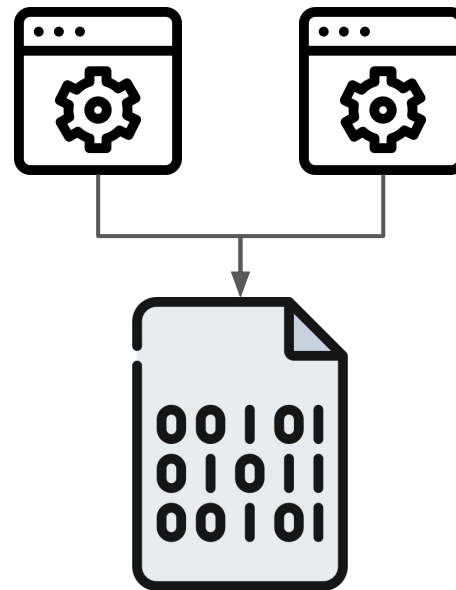
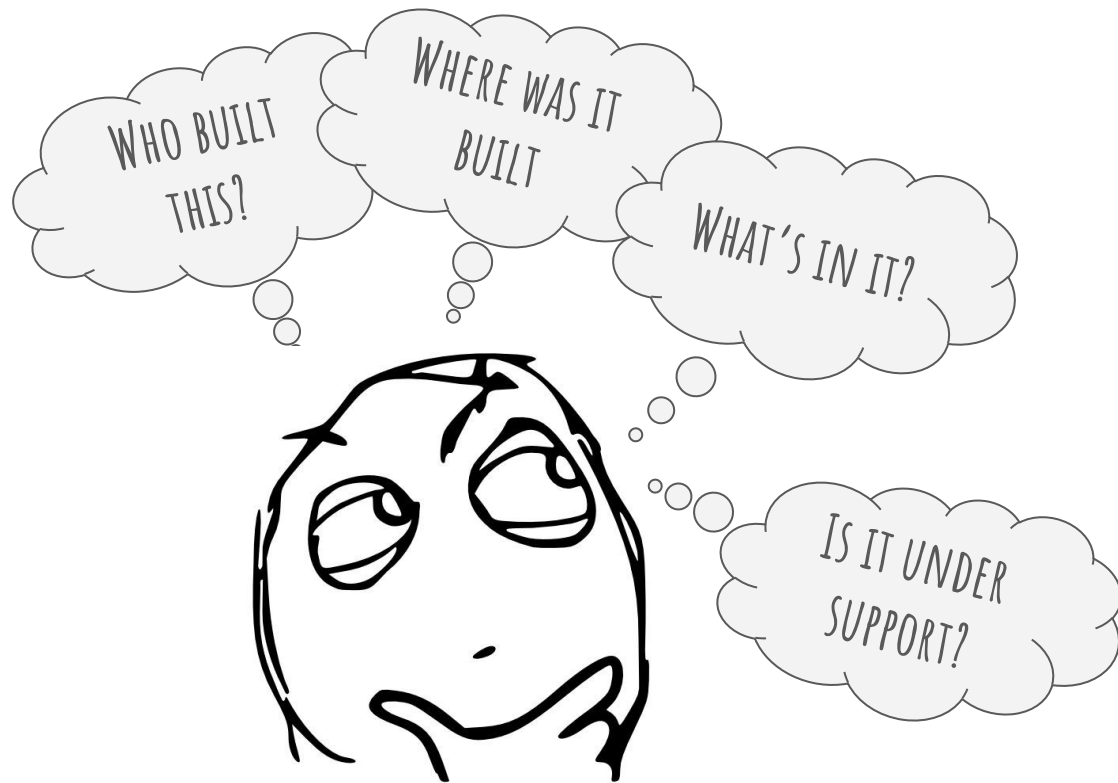


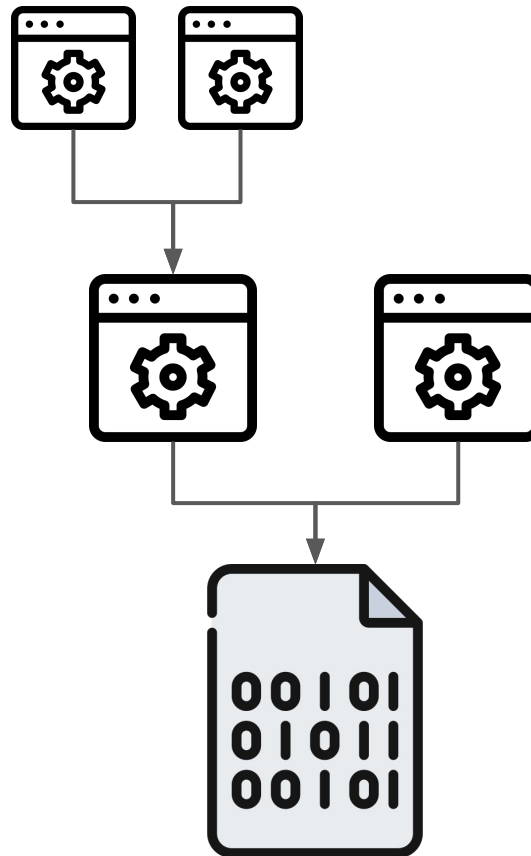
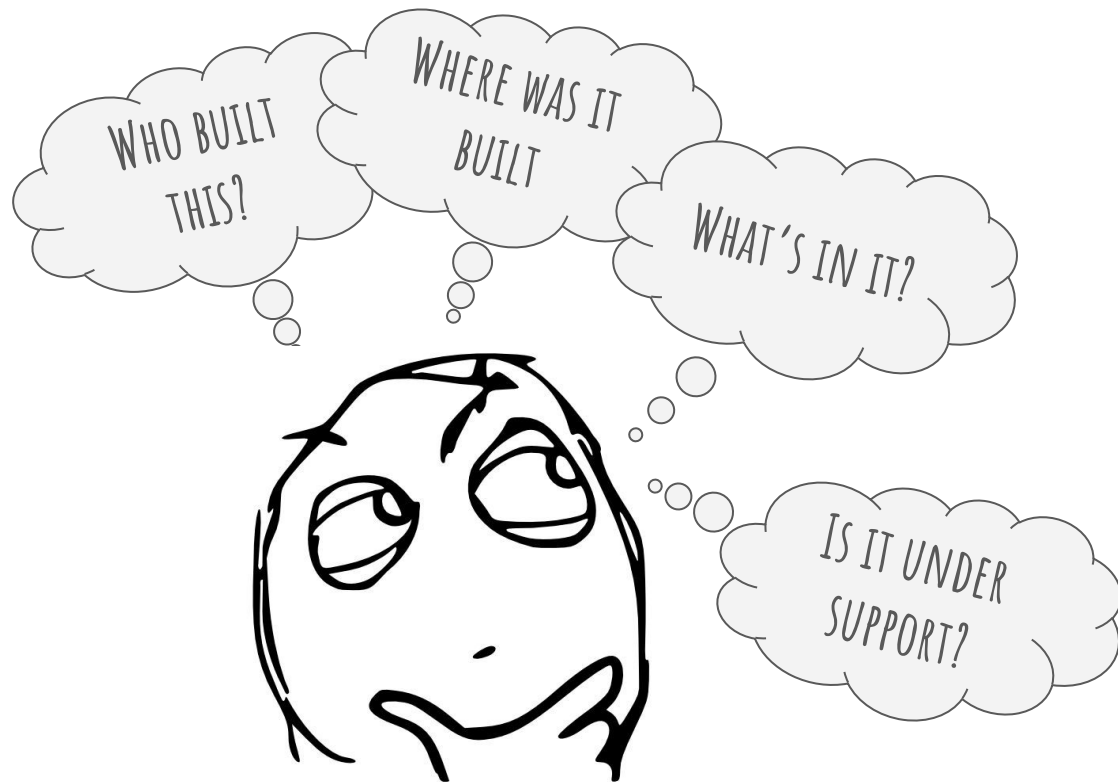


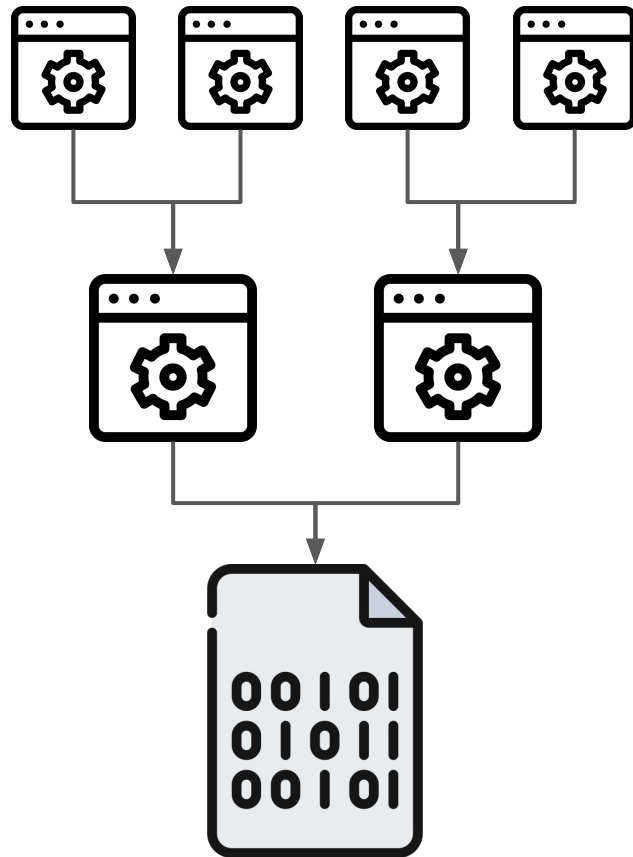
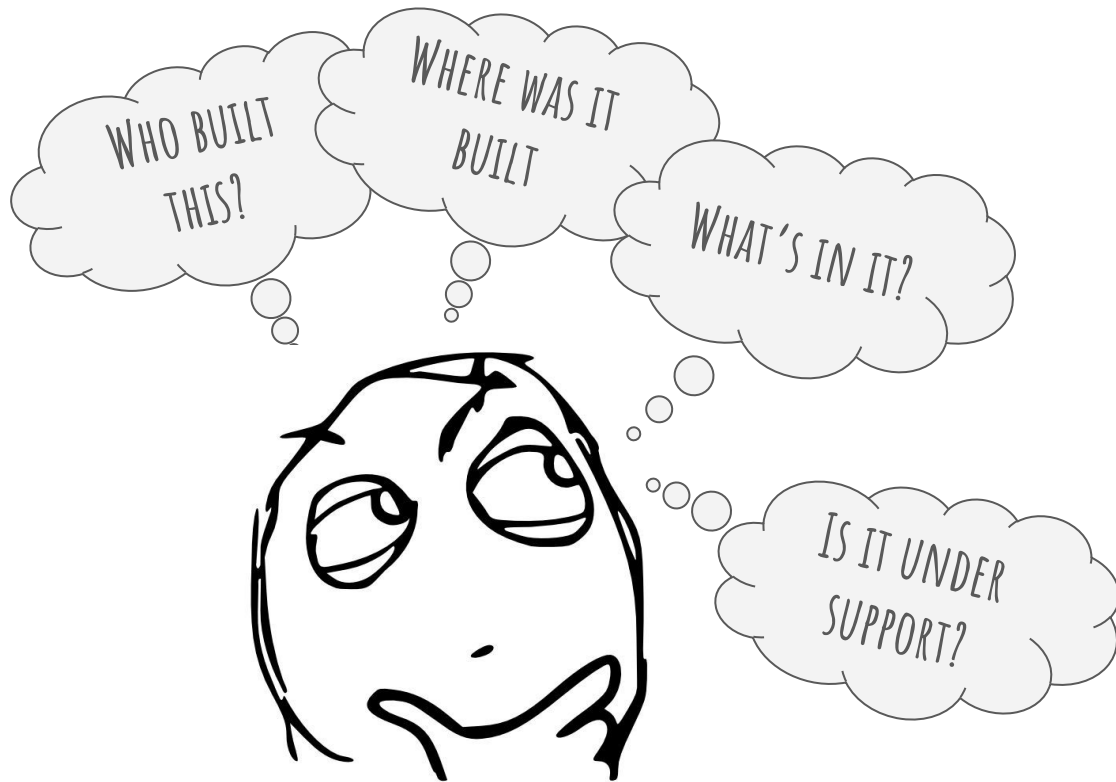


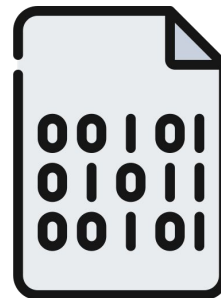
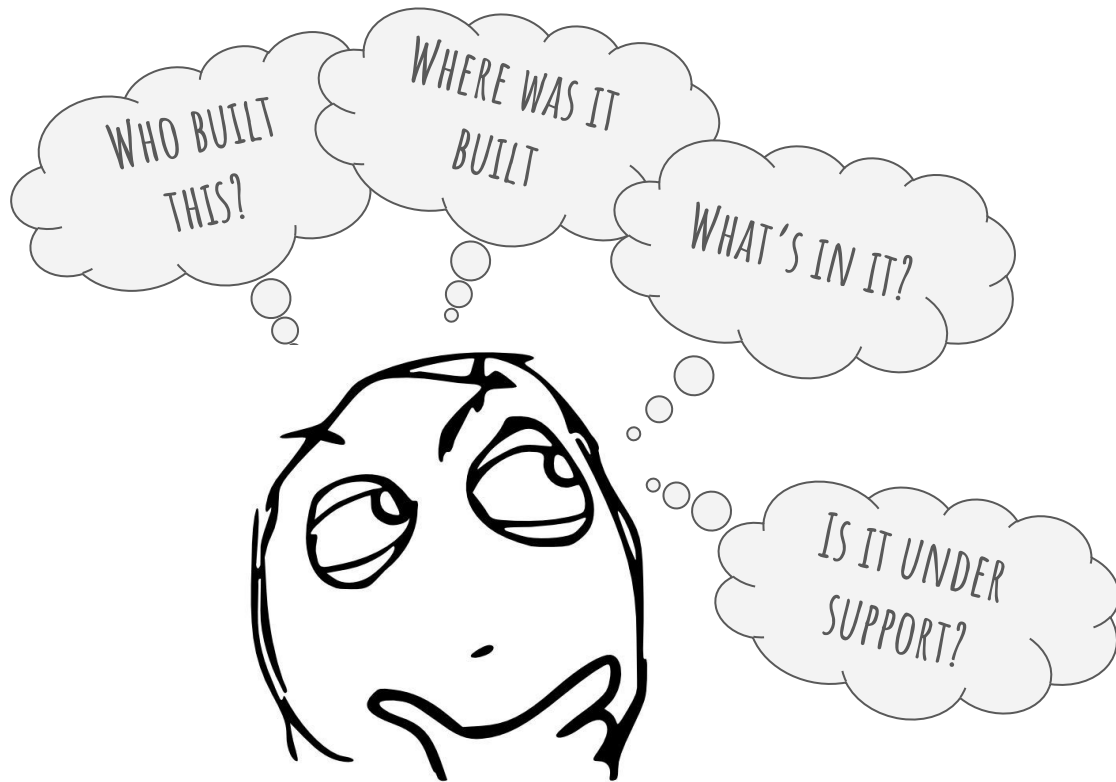








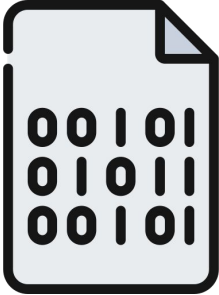




WHO BUILT THIS?
WHERE WAS IT

- ✓ Verifiable
- ✓ Unforgeable
- ✓ Non-repudiation
- ✓ Cryptographically linked

HERE'S WHAT YOU NEED TO KNOW!

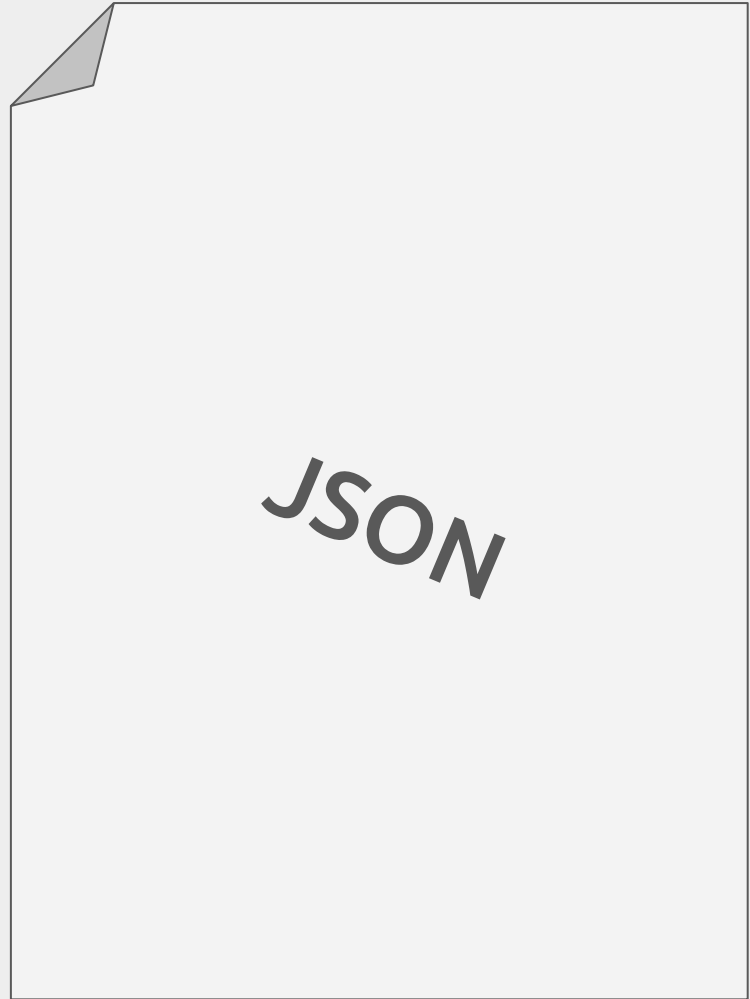


What is an Attestation?

Understanding signed claims

What is an Attestation?

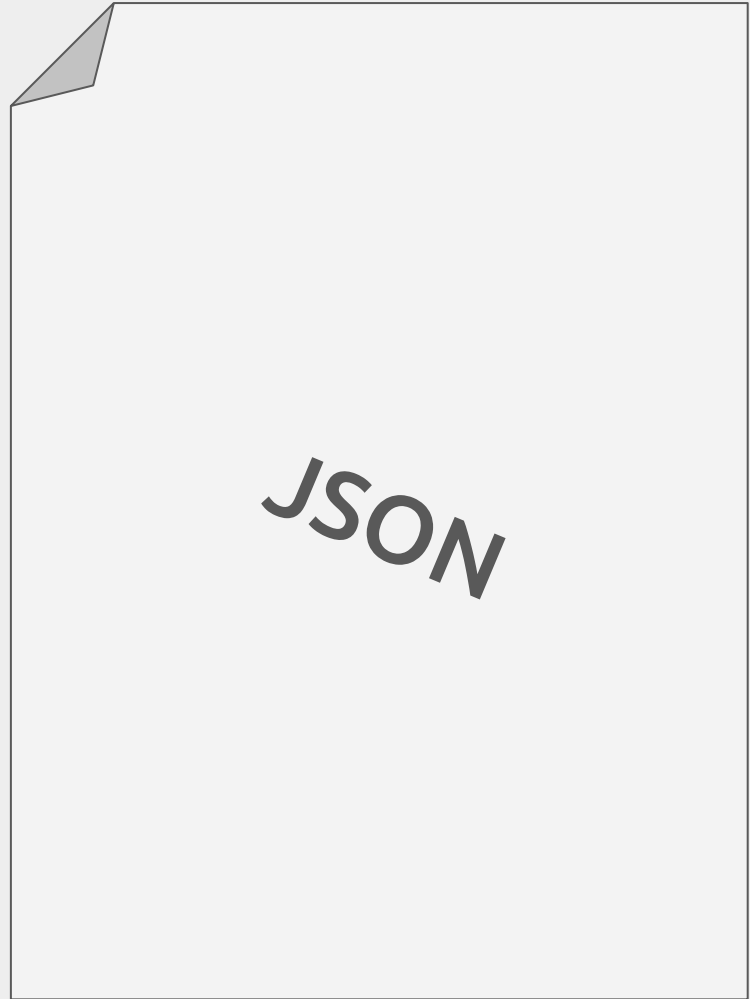
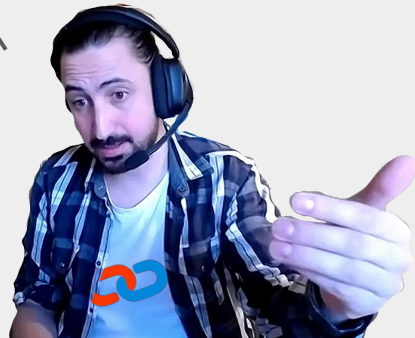
*“A signed set of claims
about a subject ”*



What is an Attestation?

“ Little atoms of a Secure Software Supply Chain ”

Dr Santiago Torres-Arias



What is an Attestation?

“A signed set of claims about a subject”

Subjects

```
"subject": [  
  {  
    "digest": {  
      "sha256": "ec5cbb4dfea31ebb0a6..."  
    }  
  }  
]
```

Predicate

```
"your": {  
  "favorite": "JSON data",  
  "Goes_here": true,  
}
```



Signature

What is an Attestation?



Subjects

```
"subject": [  
  {  
    "digest": {  
      "sha256": "ec5cbb4dfea31ebb0a6..."  
    }  
  }  
]
```

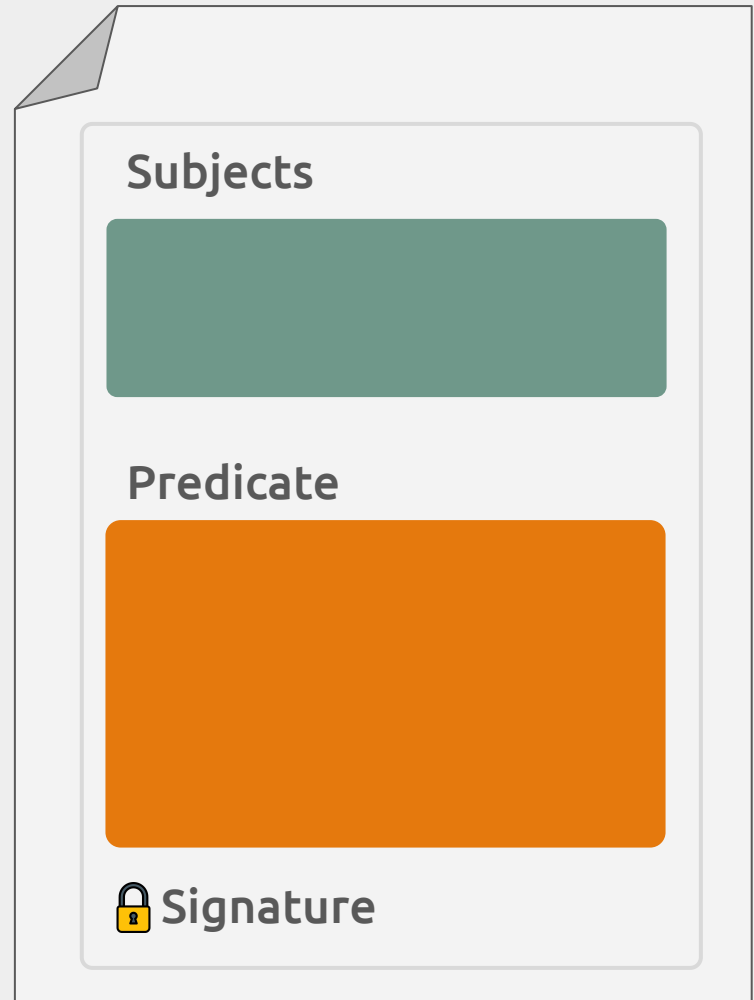
Predicate

```
"your": {  
  "favorite": "JSON data",  
  "Goes_here": true,  
}
```

Signature

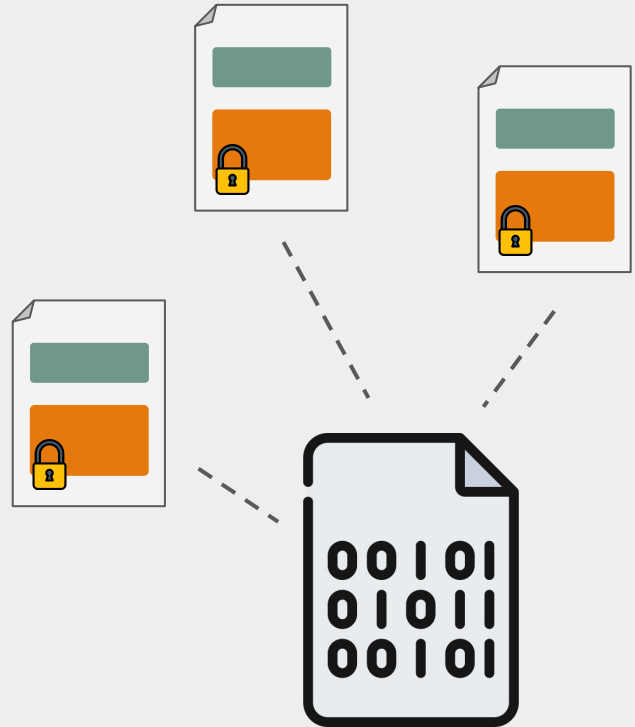
What is an Attestation?

“A signed set of claims about a subject”



What is an Attestation?

“A signed set of claims about a subject”



What is an Attestation?



Highlights - Kubernetes!

SupplyChainSecurityCon
North America

Puerco @puerco · Jul 12
We are now producing the first Bill of Materials for @Kubernetesio with each release cut!

I thought I'd share some facts about the documents we are producing and hopefully hear some opinions and suggestions.

SupplyChainSecurityCon
North America



“There’s no security
without
verification,,

- Trevor Rosen
GitHub



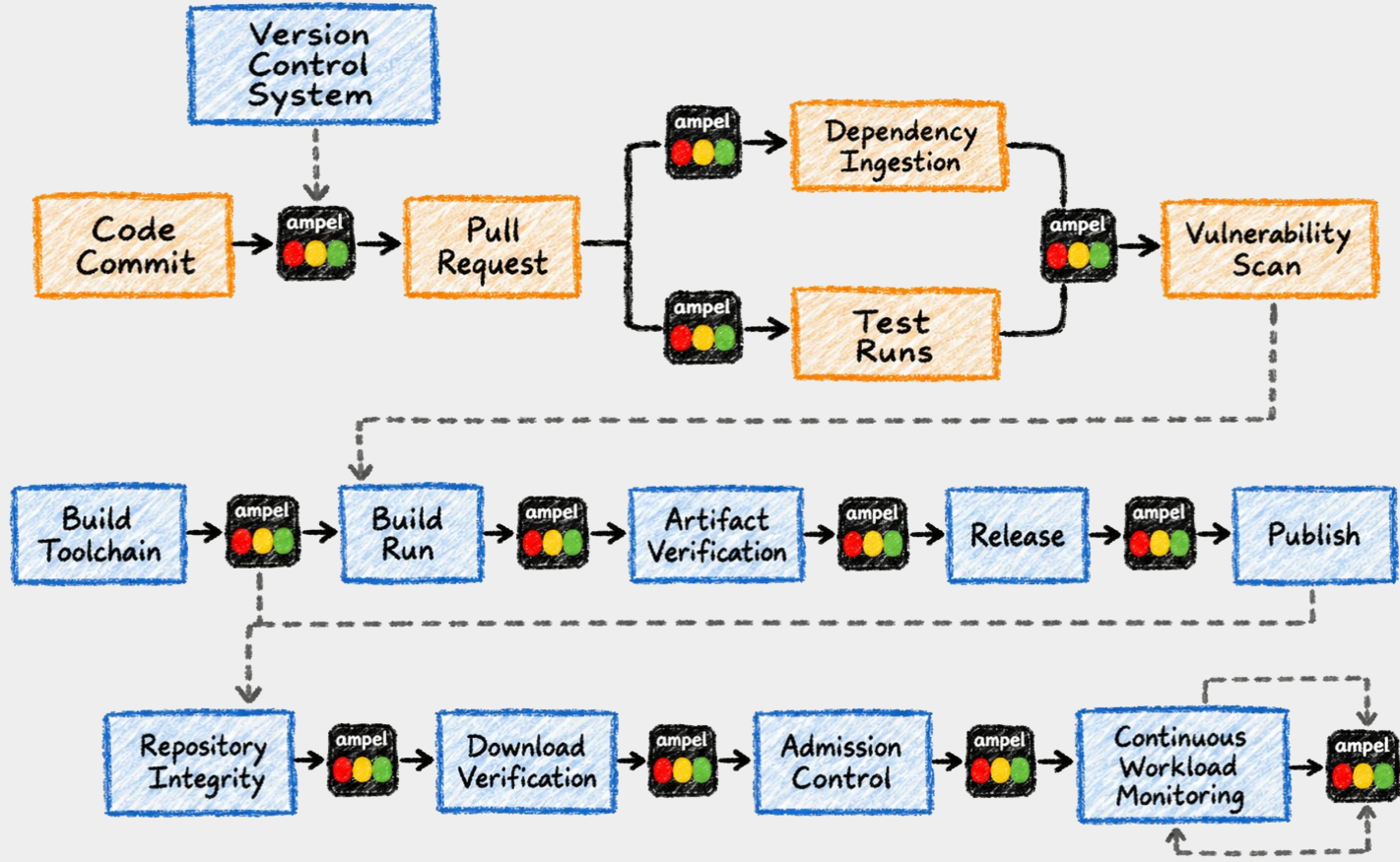




Amazing Multipurpose Policy Engine



Amazing Multipurpose Policy Engine (and L)





With a modular architecture, AMPEL solves some of the problems preventing the operationalization of software supply chain security technologies.

Key Blockers Solved by AMPEL

- Embeddable
- Policy Reuse
- Policy Composition
- Community ecosystem
- Domain-based extensions
- Tool Compatibility

Evidence Diversity

Gimme all the formats!



SBOM
(SPDX/
CycloneDX)

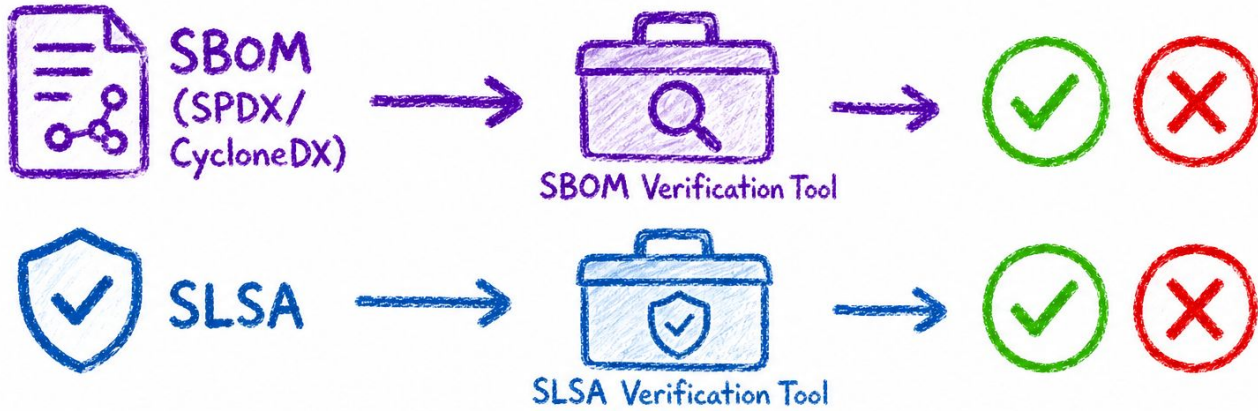


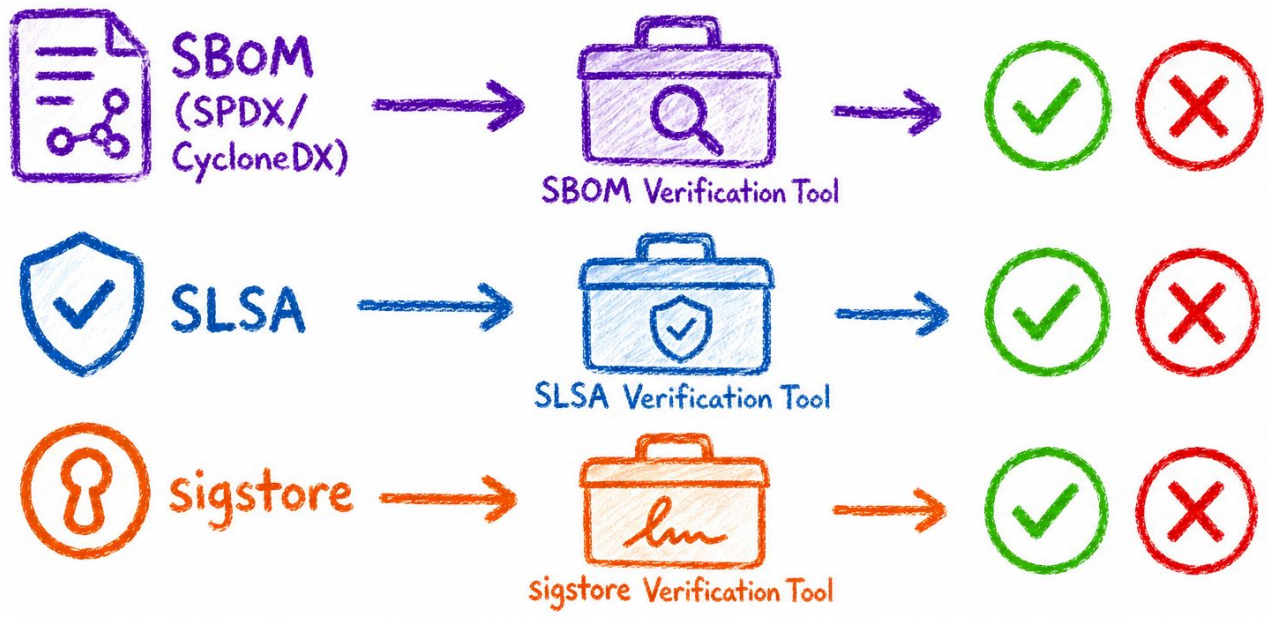
SBOM
(SPDX/
CycloneDX)

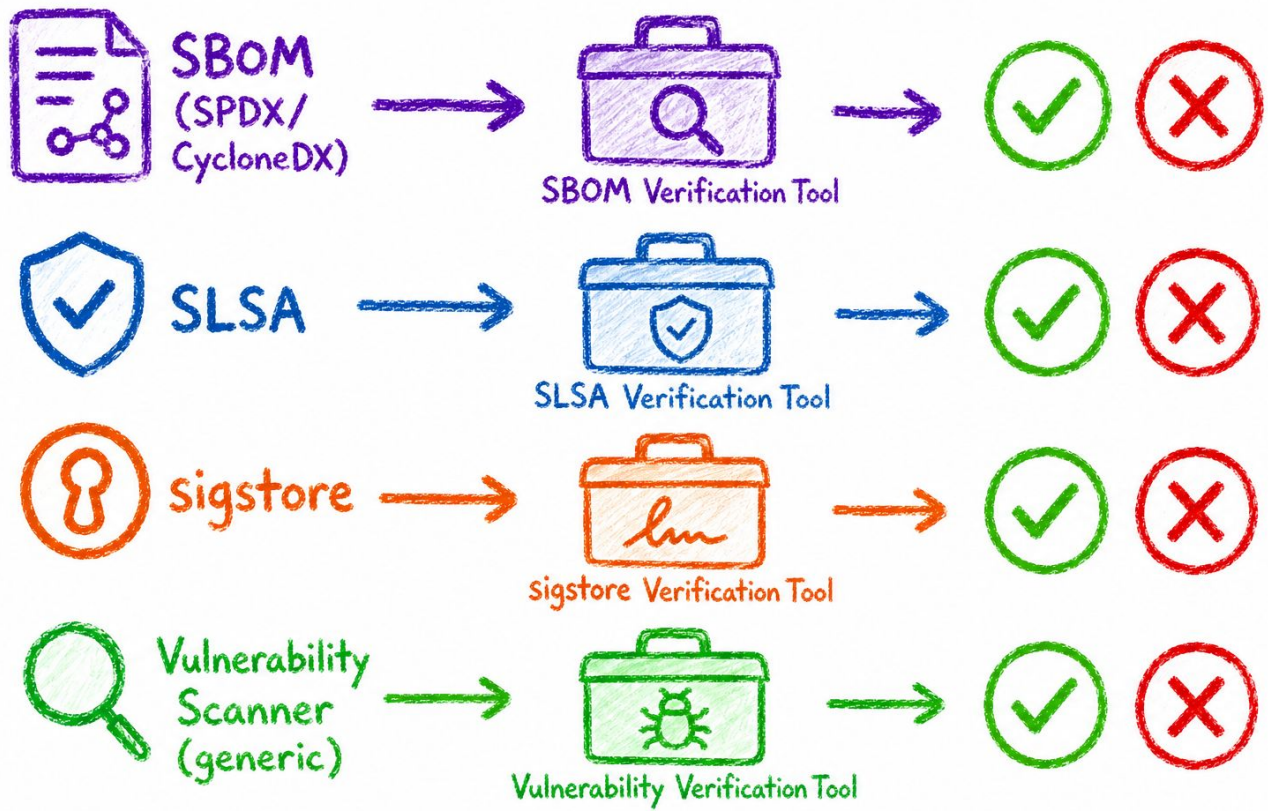


SBOM Verification Tool











SBOM
(SPDX/
CycloneDX)



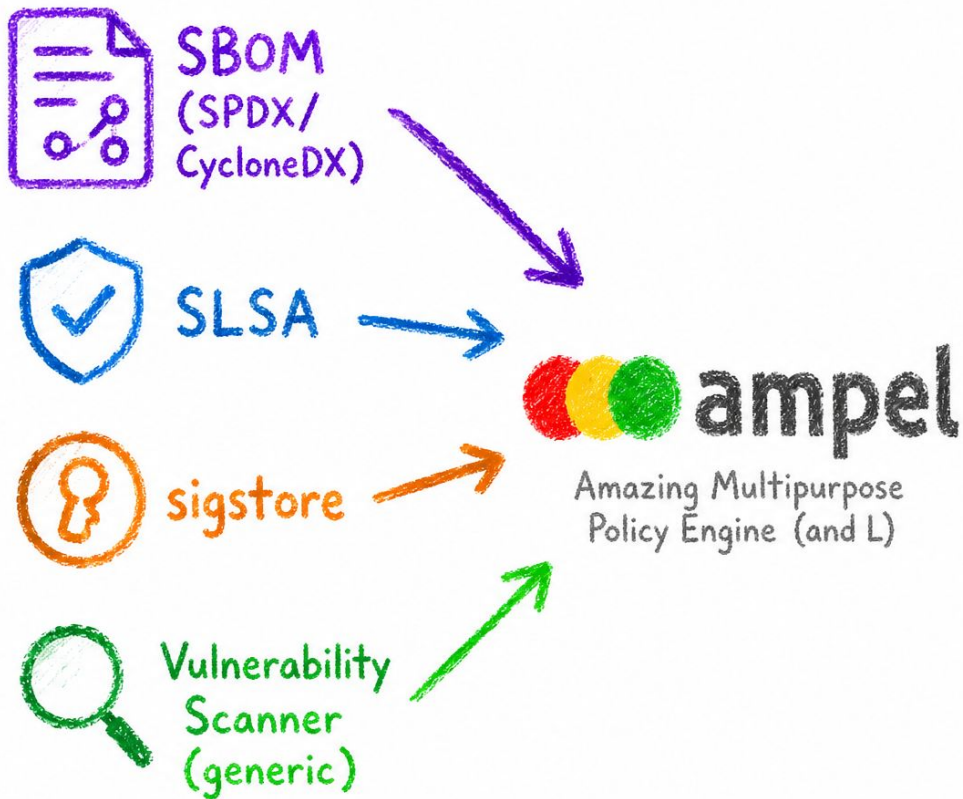
SLSA

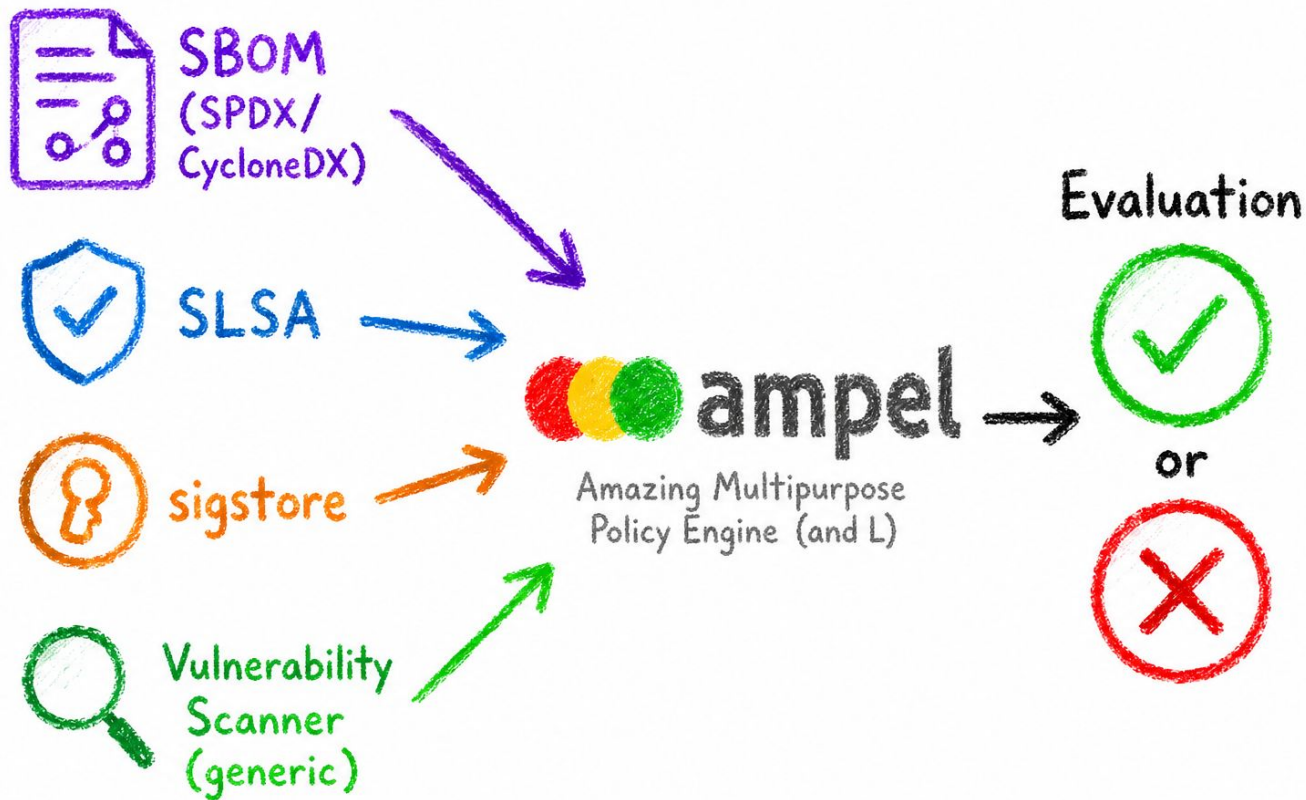


sigstore



Vulnerability
Scanner
(generic)





Full Stack Verification

All them cakes belong to you!

signature/
identity

attestation
data

signature/
identity

framework
control

attestation
data

signature/
identity

framework
control



Why?

attestation
data



What?

signature/
identity



Who?

signature/
identity

signature/
identity



Signature/Identity Verification Tool



attestation
data

signature/
identity



Signature/Identity Verification Tool

attestation
data



Attestation Verification Tool

signature/
identity



Signature/Identity Verification Tool

attestation
data

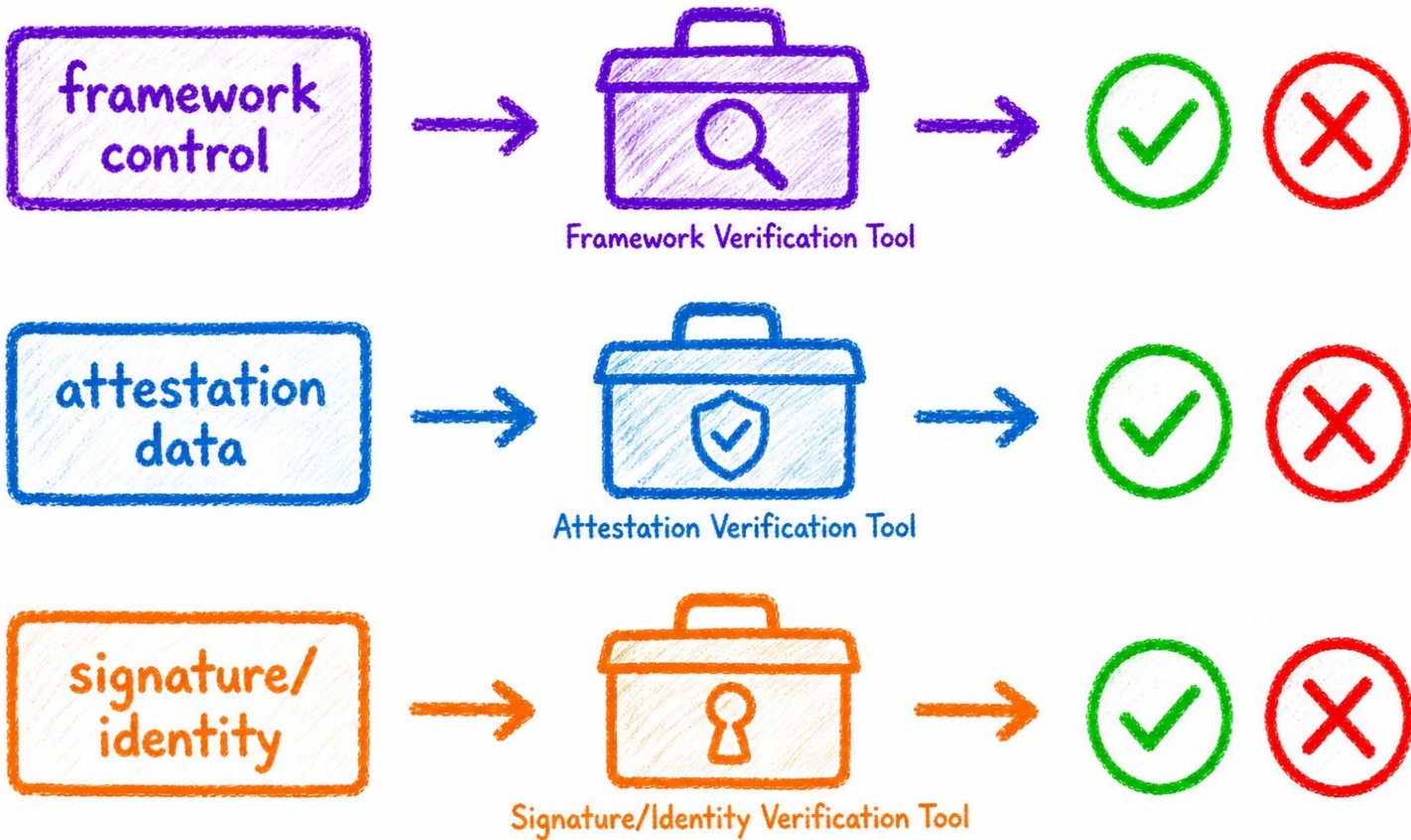


Attestation Verification Tool

signature/
identity



Signature/Identity Verification Tool



framework
control

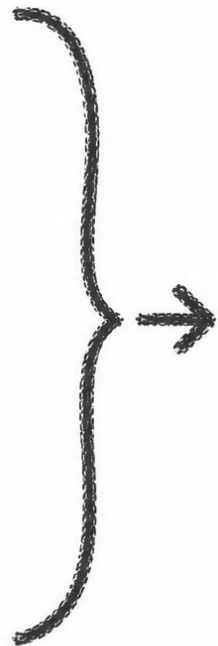
attestation
data

signature/
identity

framework
control

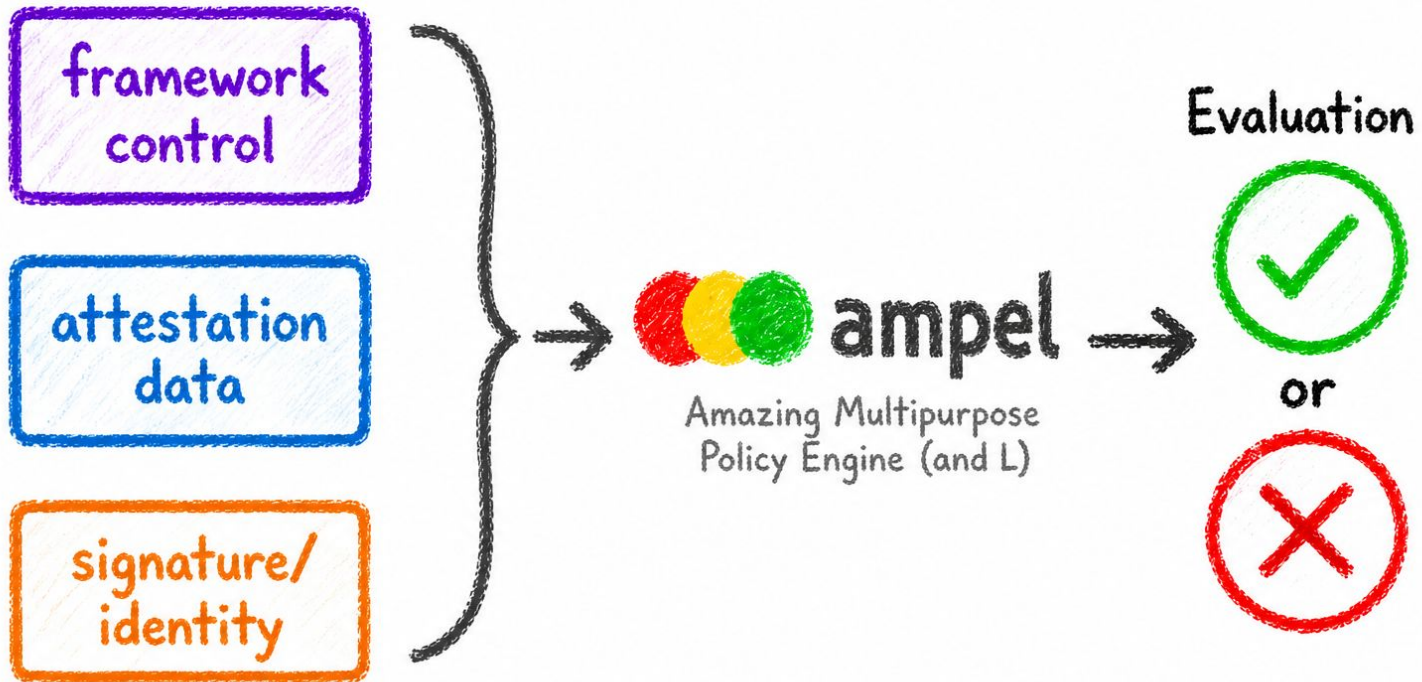
attestation
data

signature/
identity



ampel

Amazing Multipurpose
Policy Engine (and L)

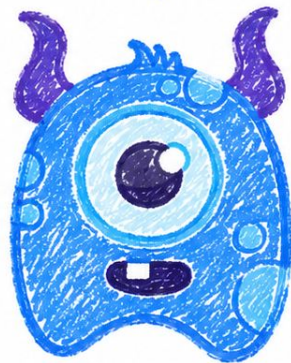


Implementation Diversity

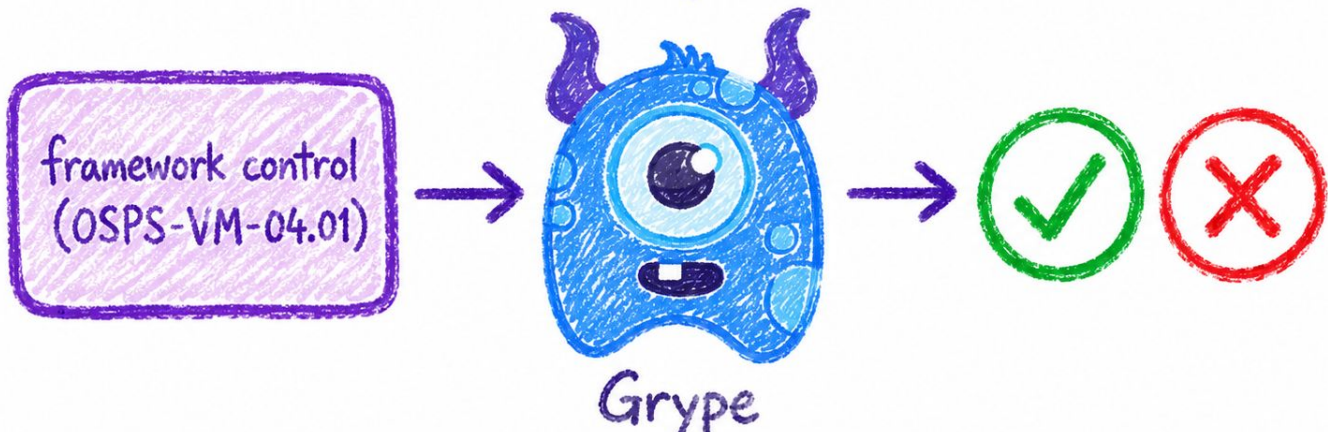
Do what you want, not what they say

framework control
(OSPS-VM-04.01)

framework control
(OSPS-VM-04.01)



Grype





Snyk

framework control
(OSPS-VM-04.01)



Grype



framework control
(OSPS-VM-04.01)



Snyk



framework control
(OSPS-VM-04.01)



Grype





Snyk



Snyk



Grype



Snyk



Grype



ampel

Amazing Multipurpose
Policy Engine (and L)



Snyk

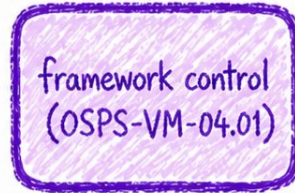


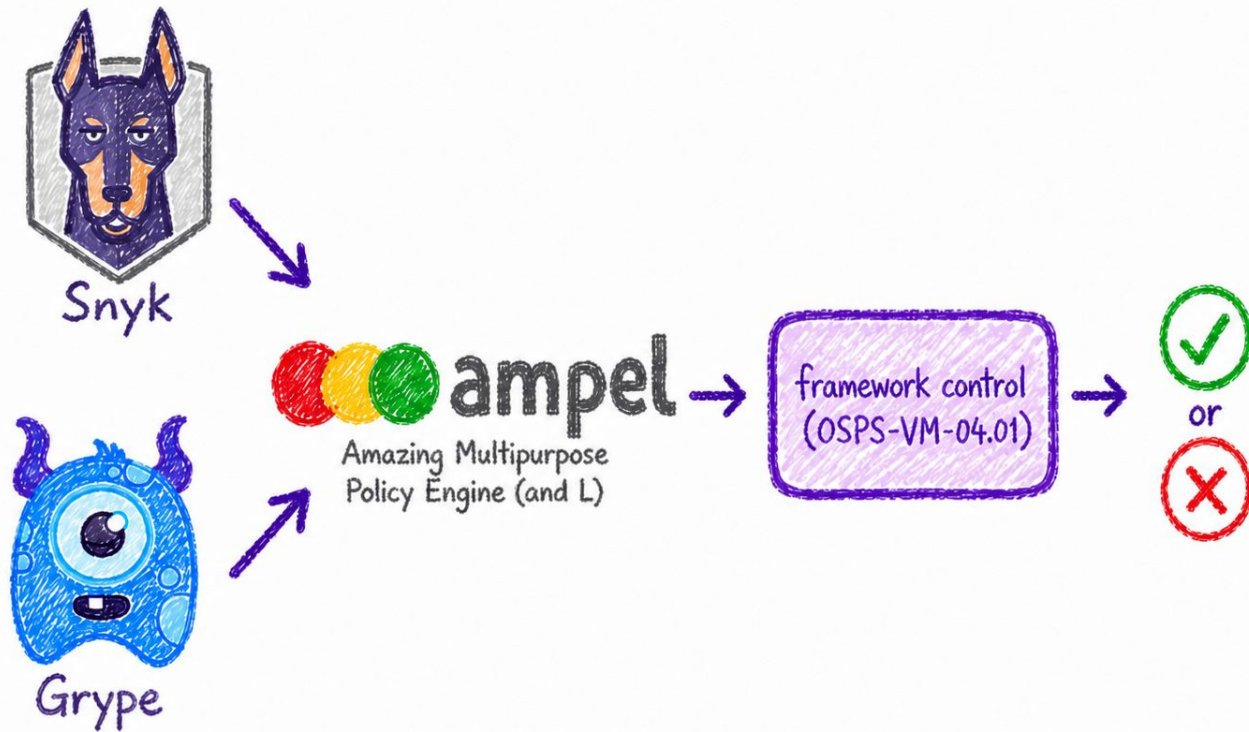
Grype



ampel

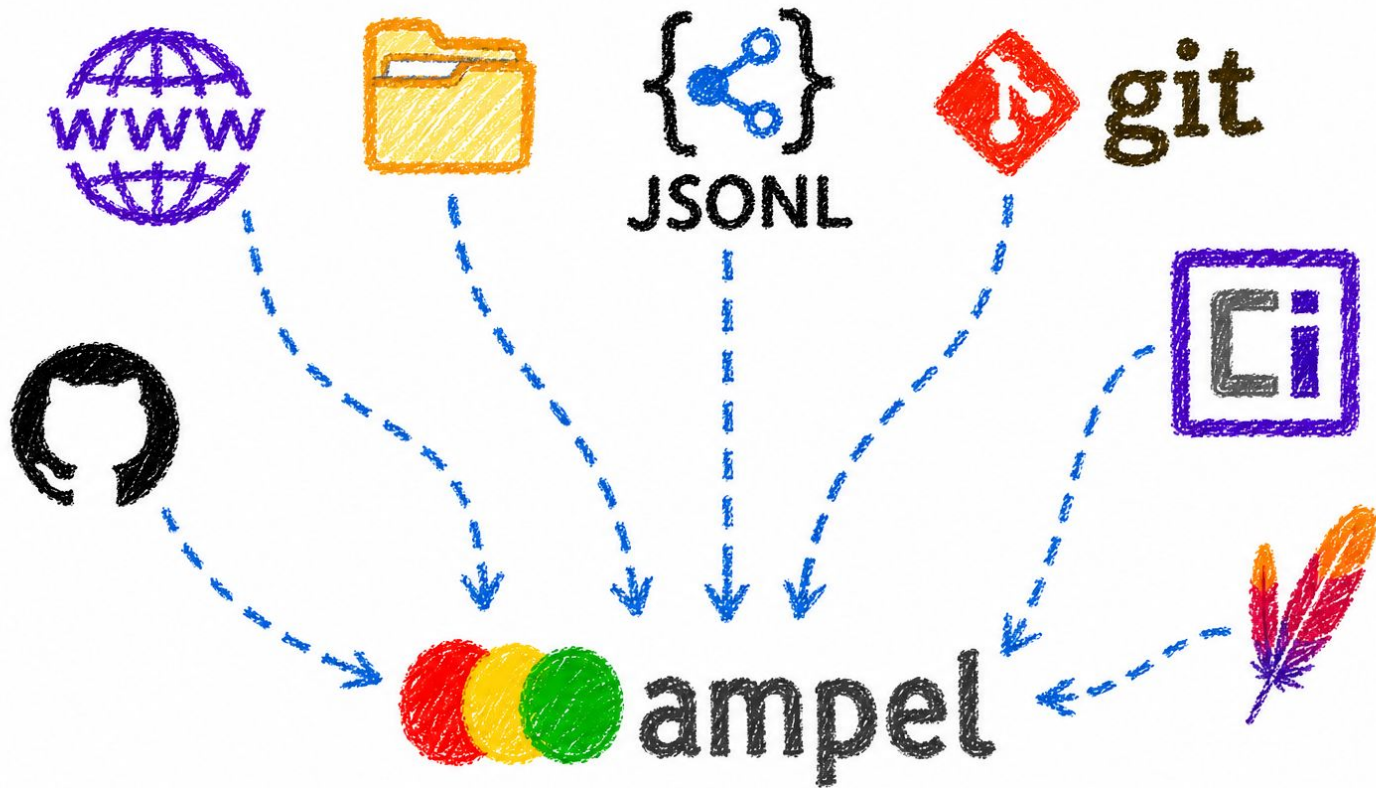
Amazing Multipurpose
Policy Engine (and L)





Evidence Discovery

There is no one source to rule them all :(



Community Policies

Do it once. For everybody.



grype/



grype-no-vulns



grype-no-high



grype-no-high-or-med



trivy/



trivy-no-vulns

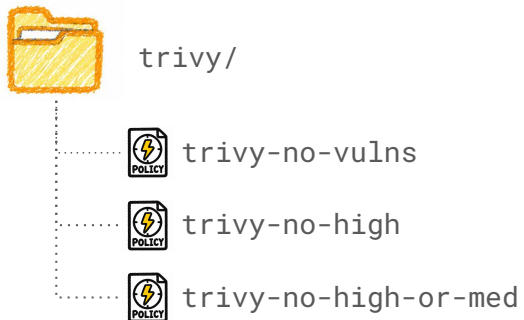


trivy-no-high

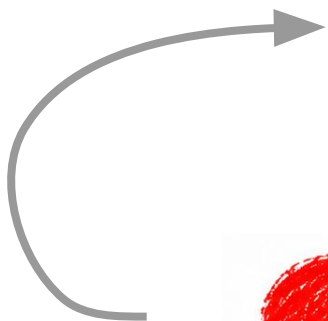
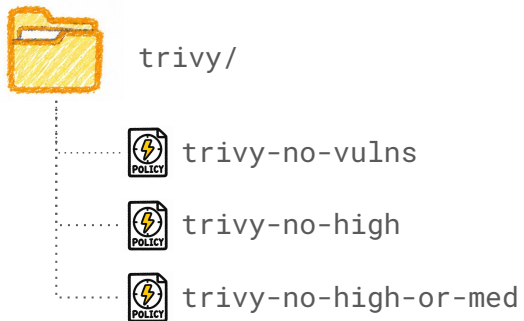
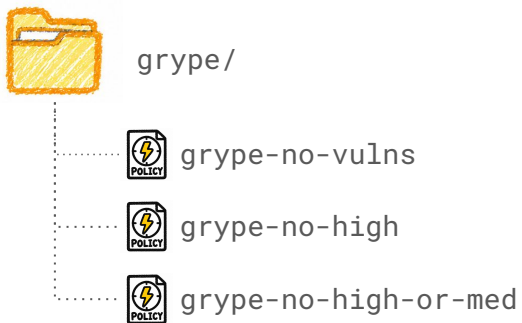


trivy-no-high-or-med









framework control
(OSPS-VM-04.01)





grype/



grype-no-vulns



grype-no-high



grype-no-high-or-med



trivy/



trivy-no-vulns



trivy-no-high



trivy-no-high-or-med

framework control
(OSPS-VM-04.01)



ampel



grype/



grype-no-vulns



grype-no-high



grype-no-high-or-med



trivy/



trivy-no-vulns



trivy-no-high



trivy-no-high-or-med



snyk/



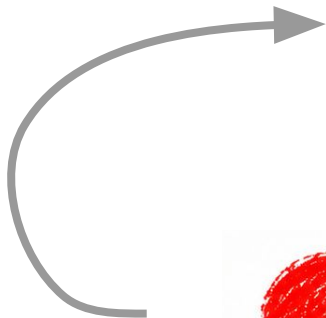
snyk-no-vulns



snyk-no-high



snyk-no-high-or-med



framework control
(OSPS-VM-04.01)



ampel



gype/



gype-no-vulns



gype-no-high



gype-no-high-or-med



trivy/



trivy-no-vulns



trivy-no-high



trivy-no-high-or-med



snyk/



snyk-no-vulns



snyk-no-high



snyk-no-high-or-med

framework control
(OSPS-VM-04.01)



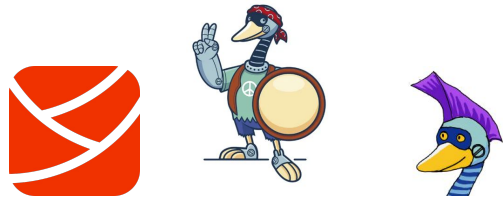
ampel

Let me show you >>>

OK, but why?

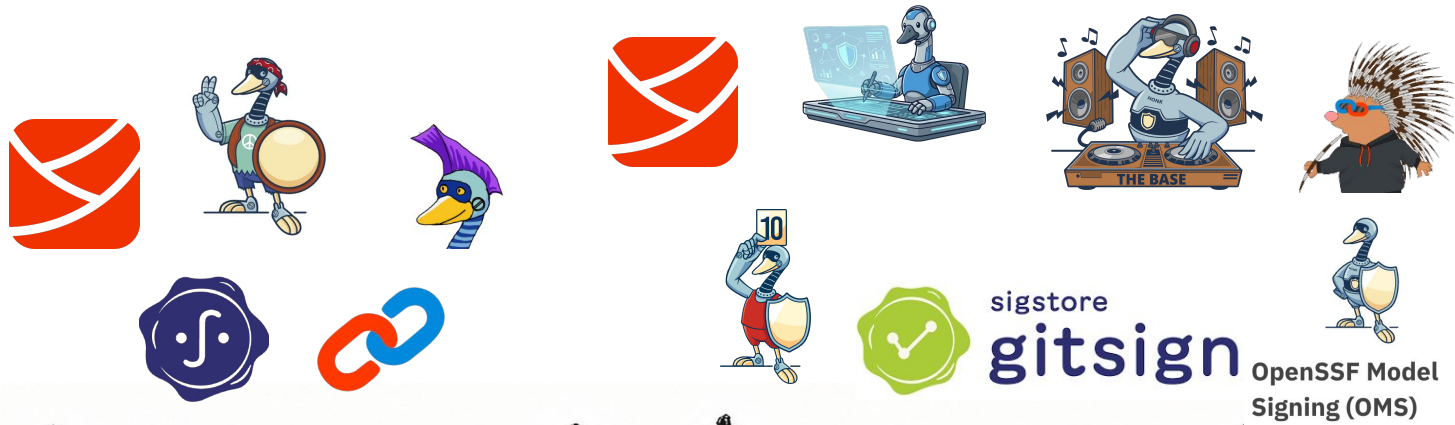
Here's why.

 ampel



integration

Three colored circles (red, yellow, green) followed by the word 'ampel' in a hand-drawn, black, textured font.



integration



application



ampel

carabine-dev / demo-repo

Code Issues Pull requests **Actions** Projects Wiki Security 2 Insights Settings

Release

Release #28

Summary

Jobs

- release

Run details

- Usage
- Workflow file

Triggered via push 5 days ago

Repository	Status	Total duration	Artifacts
puerco -> 238cba2 v0.0.1-pre29	Success	3m 0s	1

release.yaml

on: push

- release 2m 56s

release summary

AMPEL: Evaluation Results

PolicySet	OSPS	Date	
	OSPS	2025-05-08 16:54:06.380807858 +0000 UTC	
Status: PASS	Subject	- sha256:ec5cbb4dfea31ebb0a69499dbdc77dc6...	
Policy	Controls	Status	Details
OSPS-AC-01	OSPS-AC-01	SOFTFAIL	Multifactor authentication is not enabled for some members
OSPS-AC-02	OSPS-AC-02	PASS	GitHub organization found
OSPS-AC-03	OSPS-AC-03	SOFTFAIL	Branch delete protection is not enabled
OSPS-AC-04	OSPS-AC-04	SOFTFAIL	No suitable predicates found
OSPS-GV-01	OSPS-GV-01	PASS	Administrators listed in Security Insights
OSPS-GV-02	OSPS-GV-02	PASS	Found attested repository dataIssues feature is enabled in the repository
OSPS-GV-03	OSPS-GV-03	SOFTFAIL	Repository has no CONTRIBUTING.md file
OSPS-GV-04	OSPS-GV-04	SOFTFAIL	Not implemented yet
OSPS-LE-03	OSPS-LE-03	PASS	Could not detect a license entry in the security insights file.
OSPS-LE-02	OSPS-LE-02	PASS	No licenses found in SBOM or licenses are not OSI approved



gn OpenSSF Model Signing (OMS)



But oh, look 🙄

It's a whole mini-ecosystem!



Amazing Multipurpose Policy Engine (and L)



libraries



utilities

Thank you!

Thank you!

<https://github.com/carabiner-dev/ampel>



Adolfo García Veytia

@puerco

