# SLSA 

*The taco dip for software supply chain security*

# recap

*(SBOM meetup)*

# recap | SBOM Meetup

In our previous talk we looked into such things like

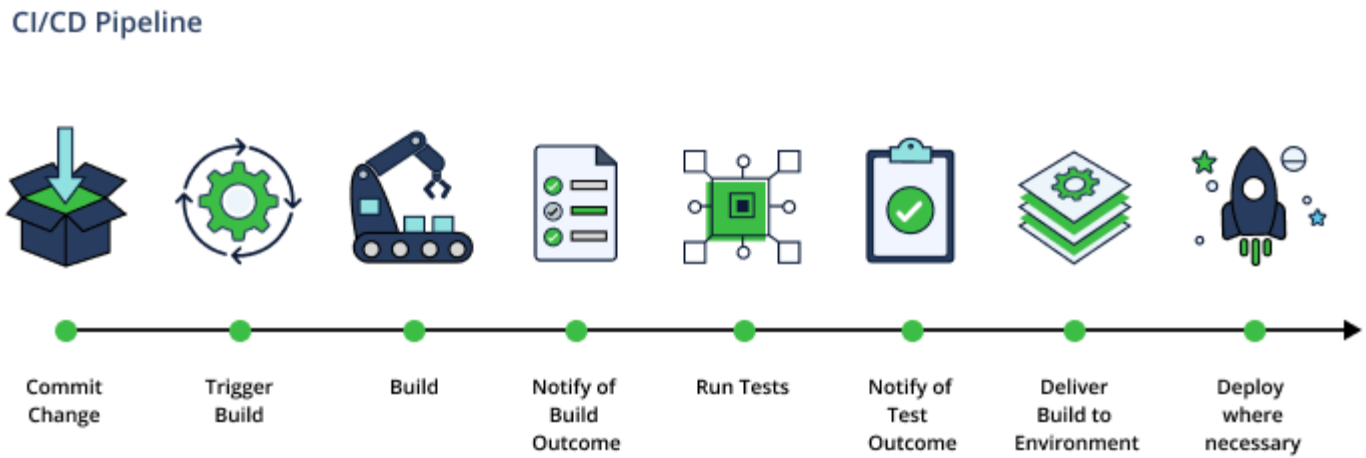
- the need for security in supply chains
- SBOM
- VEX

But we did not (yet) talk about

- how do we use that in production
- more usable approach that scales

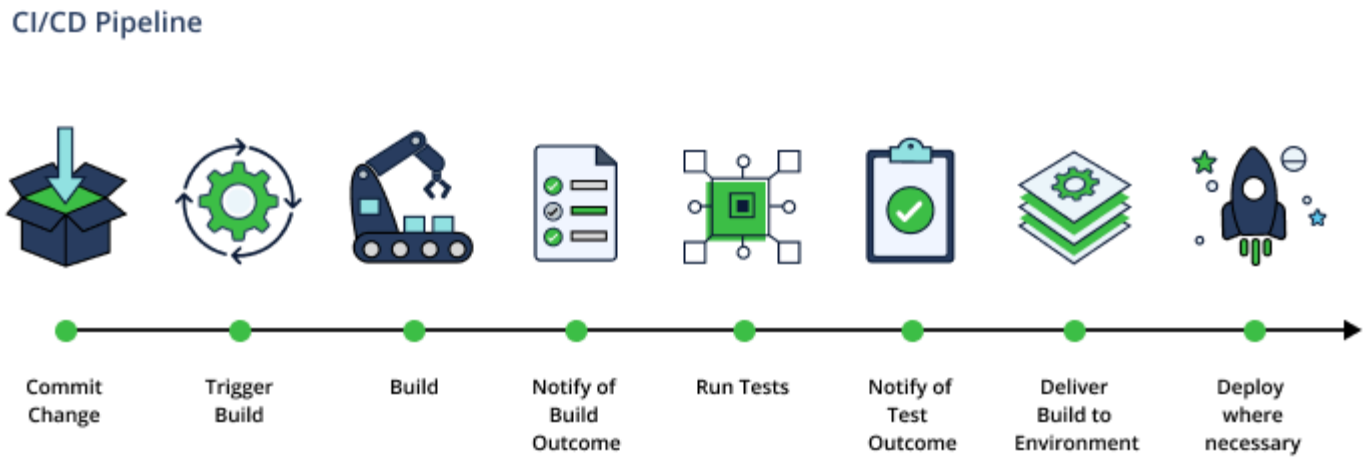
# Intro

# Intro | The Supply Chain




ref: https://jfrog.com/de/learn/software-supply-chain/

# Intro | The Security Issue



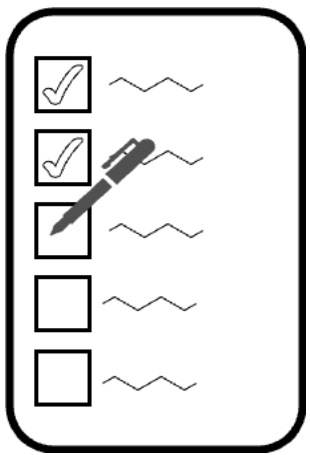

where are the security problems here?

ref: https://jfrog.com/de/learn/software-supply-chain/

# SLSA

# SLSA | What is it?

Supply-chain Levels for Software Artifacts, or SLSA ("salsa"). It’s a security framework, a checklist of standards and controls to prevent tampering, improve integrity, and secure packages and infrastructure.




ref: https://slsa.dev/ https://www.activestate.com/resources/quick-reads/software-supply-chain-security/

# SLSA | levels

| | | Required at | | | |
|---|---|---|---|---|---|
| Requirement | | SLSA 1 | SLSA 2 | SLSA 3 | SLSA 4 |
| Source | Version Controlled | | ✓ | ✓ | ✓ |
| | Verified History | | | ✓ | ✓ |
| | Retained Indefinitely | | | 18 mo. | ✓ |
| | Two-Person Reviewed | | | | ✓ |
| | Scripted | ✓ | ✓ | ✓ | ✓ |

# SLSA | Why do we need it?

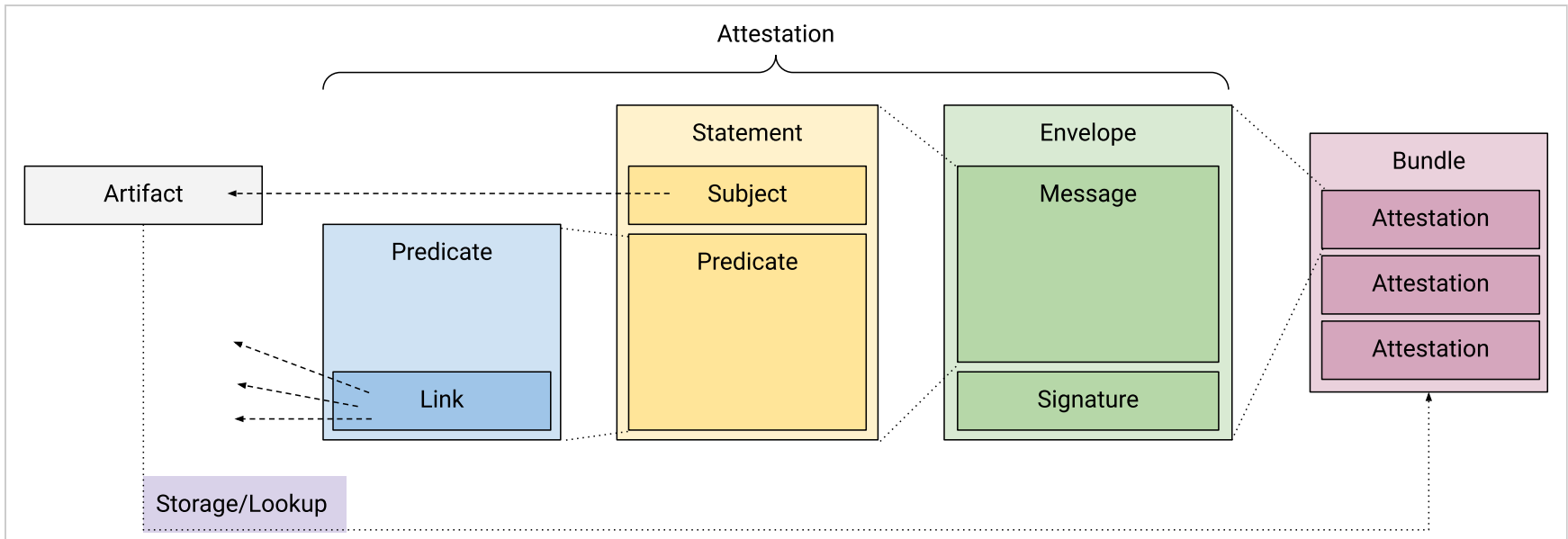


# SLSA | specification

| Aspect | SLSA v1.0 | SLSA v1.1 |
|---|---|---|
| Release Type | Initial stable release | Incremental update |
| Definitions & Terminology | Baseline definitions | Clarified and refined terminology |
| Provenance Requirements | Basic provenance guidance | Expanded, more detailed provenance requirements |
| Build Model Support | Focused on common build scenarios | Better support for ephemeral/distributed builds |
| Security Requirements | Initial requirements | Strengthened and more precise requirements |

# SLSA | specification (attestations)

- authenticated statement about a software artifact
- in reality it's all about artifact/code signing



# DEMO

# Thank You

# References

- https://www.cisa.gov/sbom
- https://www.cisa.gov/sites/default/files/2023-01/VEX_Use_Cases_Aprill2022.pdf
- https://slsa.dev/
- https://www.meetup.com/security-meetup-by-sba-research/events/304127699/
- https://chainloop.dev/