FullStackS

SOLUTION BRINGER

DEVELOPERWEEK™

cloud-native software supply chain security: the hard truth

CLOUD NATIVE COMPUTING FOUNDATION

SILVER MEMBER

kubernetes CERTIFIED

Diamond Partner

HASHICORP SPECIALIZED PARTNER

CISCO Partner

snyk CERTIFIED GOLD PARTNER

SELECT CHANNEL PARTNER GitLab

VEEAM Value-Added Reseller Registered

aws PARTNER Select Tier Services

splunk>

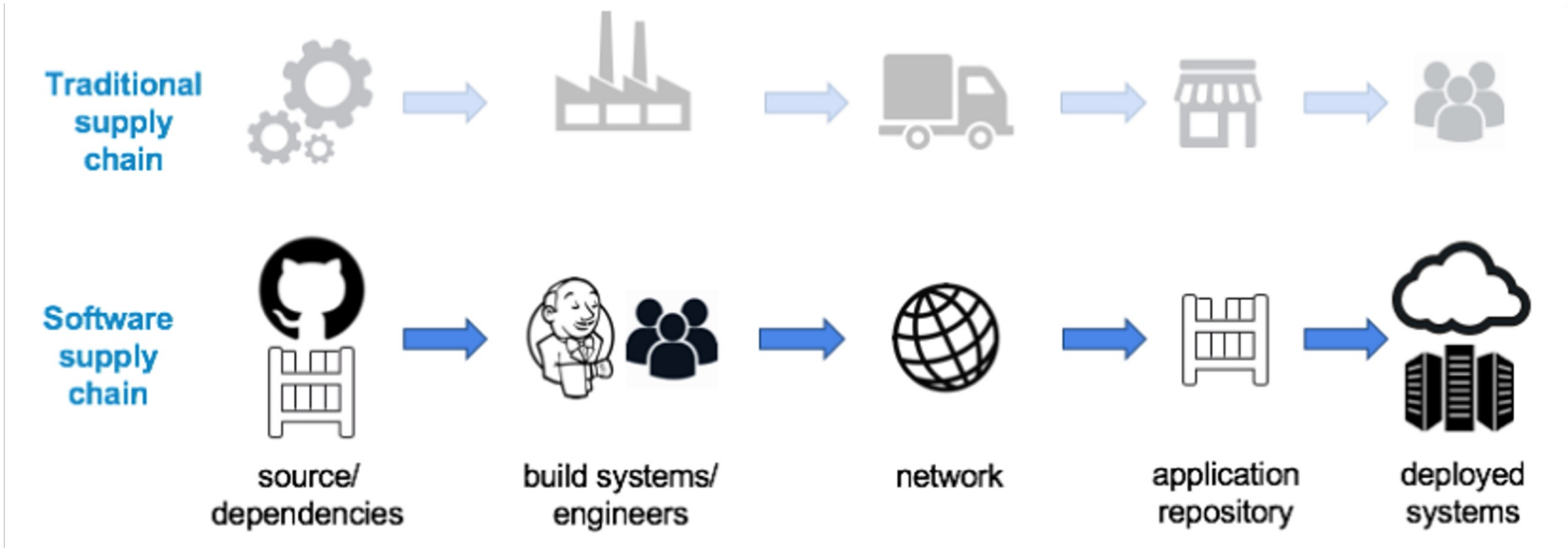
EXOSCALE Partner

Software Supply Chain

The software supply chain involves a multitude of tools and processes that enable software developers to write, build, and ship applications.

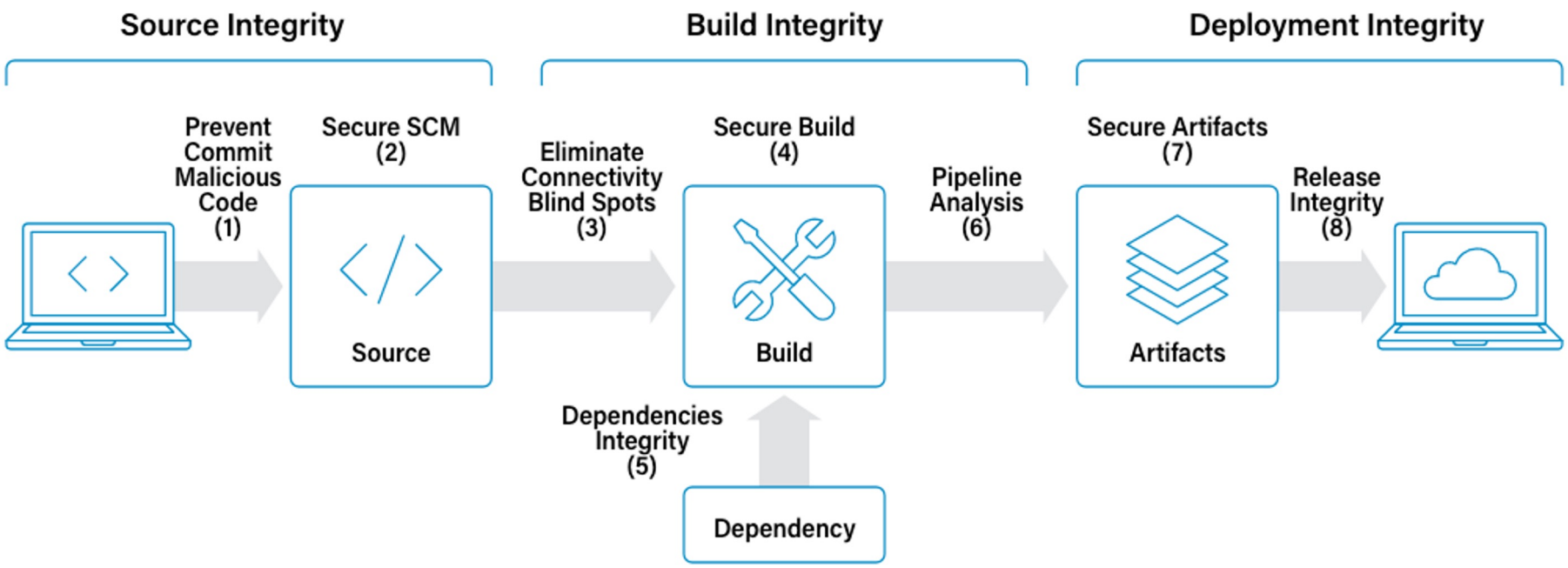
Melara & Bowman, 2022, Intel Labs

CNCF - SSC in a

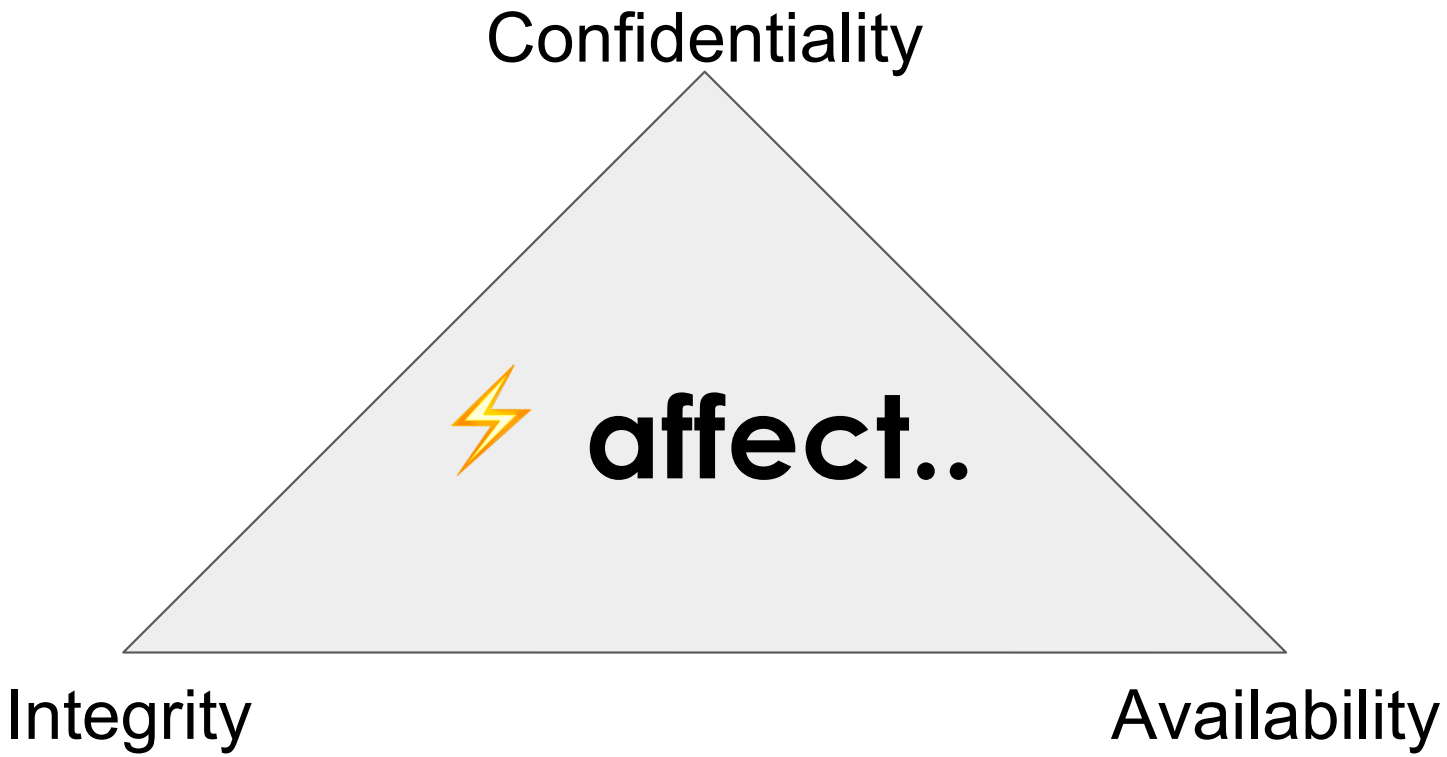


https://github.com/cncf/tag-security/blob/main/supply-chain-security/supply-chain-security-paper/CNCF_SSCP_v1.pdf

CIS - SSC ⚡ in a 🥥



https://www.cisecurity.org/insights/white-papers/cis-software-supply-chain-security-guide


Confidentiality
affect..
Integrity
Availability

Stages of the SSC

Stages/Elements of the SSC

- Code
- Dependencies
- Build
- Artifacts & Distribution/Deployment
- (Runtime)

Stage: Code

code content

code management

Stage: Code - code content

- ⚡ threats
  -  - bugs
  -  - malicious code
  -  - license
- 💡 solutions
  -  - scanning
  -  - testing
  -  - policies

Stage: Code - code management

⚡ threats

- ⌨️ - manipulation
- 🥷 - theft
- 🗑️ - deletion

💡 solutions

- 🔒 - access
  - RBAC
  - Codeowners
  - signatures
  - MFA
- 💂 - repo config
  - push policies

Stage: Dependencies

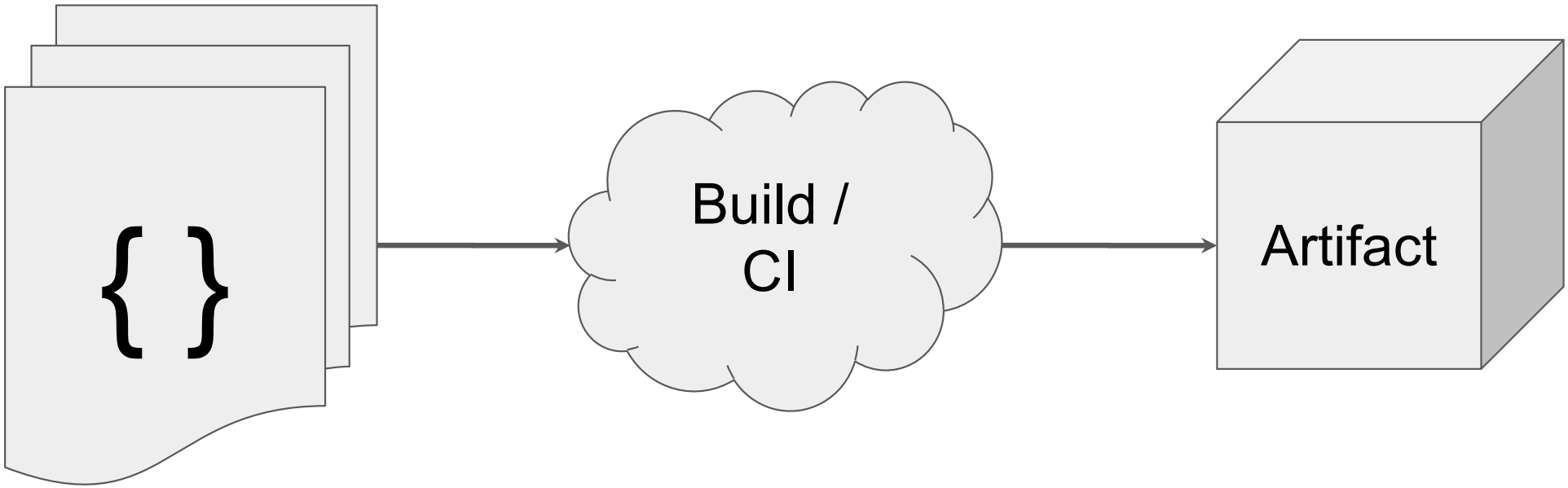
packages, libraries, …

Please use a Package Manager

Stage: Dependencies

- ⚡ threats
  - 🐞 - bugs
  - ☣️ - malicious code
  - ⚖️ - license
  - 🎭 - integrity
- 💡 solutions
  - 🔍 - scanning
  - 🧪 - testing
  - 🚓 - policies
  - 🗃️ - inventory
  - ✒️ - signature
  - 📦 - SBOM
  - 🤿 - airgapping

Stage: Build



Stage: Build

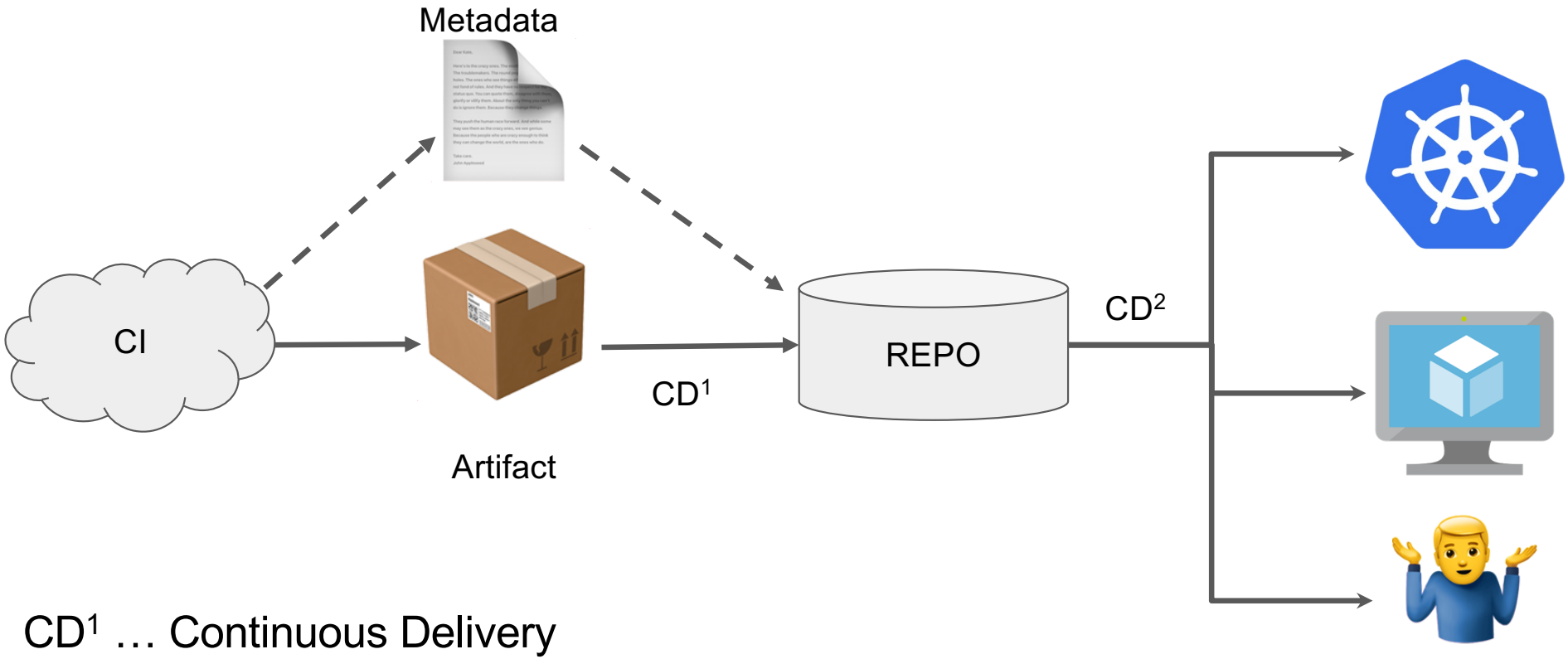
⚡ threats

- 🪲 - build bugs
- ☣️ - malicious env

💡 solutions

- 💻 - dedicated env
- ❌ - zero trust
- ⬜ - single use env
- | - pipelines
- {} - as code
- 👬 - reproducible

Stage: Artifacts & Distribution/Deployment



CD[1] … Continuous Delivery
CD[2] … Continuous Deployment

Stage: Artifacts & Distribution/Deployment

⚡ threats

-  - theft / deletion
-  - replacement
-  - no transparency
-  - updates

💡 solutions

-  - repo security
-  - signatures
-  - attestation
-  - SBOM
-  - TUF

Bottom Line Message

Software Supply Chain has multiple levels → very different threats ⚡

Solutions / Mitigations on different levels of effort and complexity ☝️

in the real world

Context

consulting experience + master thesis input:
“somewhat complete” set of SSCS controls

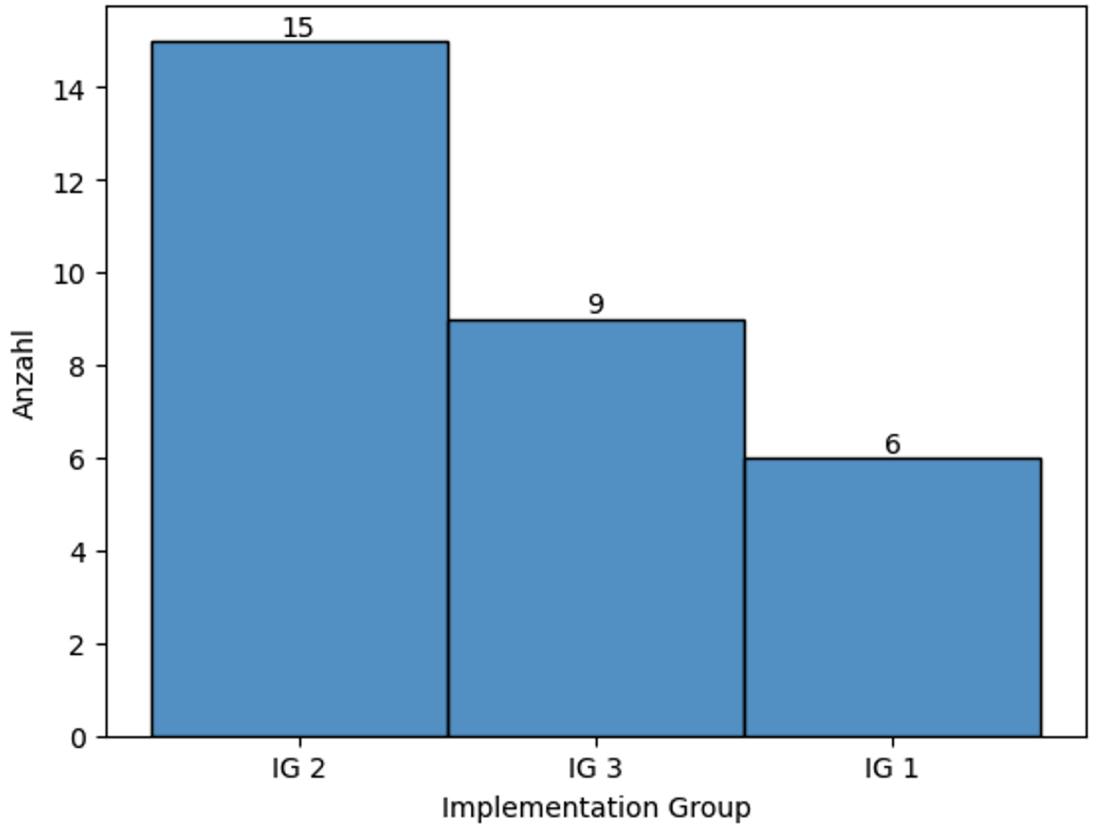
literature input from..

- CIS Software Supply Chain Security Guide
- CNCF Software Supply Chain Best Practices
- OWASP SCVS Software Component Verification Standard
- SLSA Supply-chain Levels for Software Artifacts
- Microsoft Secure Supply Chain Consumption Framework
- DoD Enterprise DevSecOps Reference Design

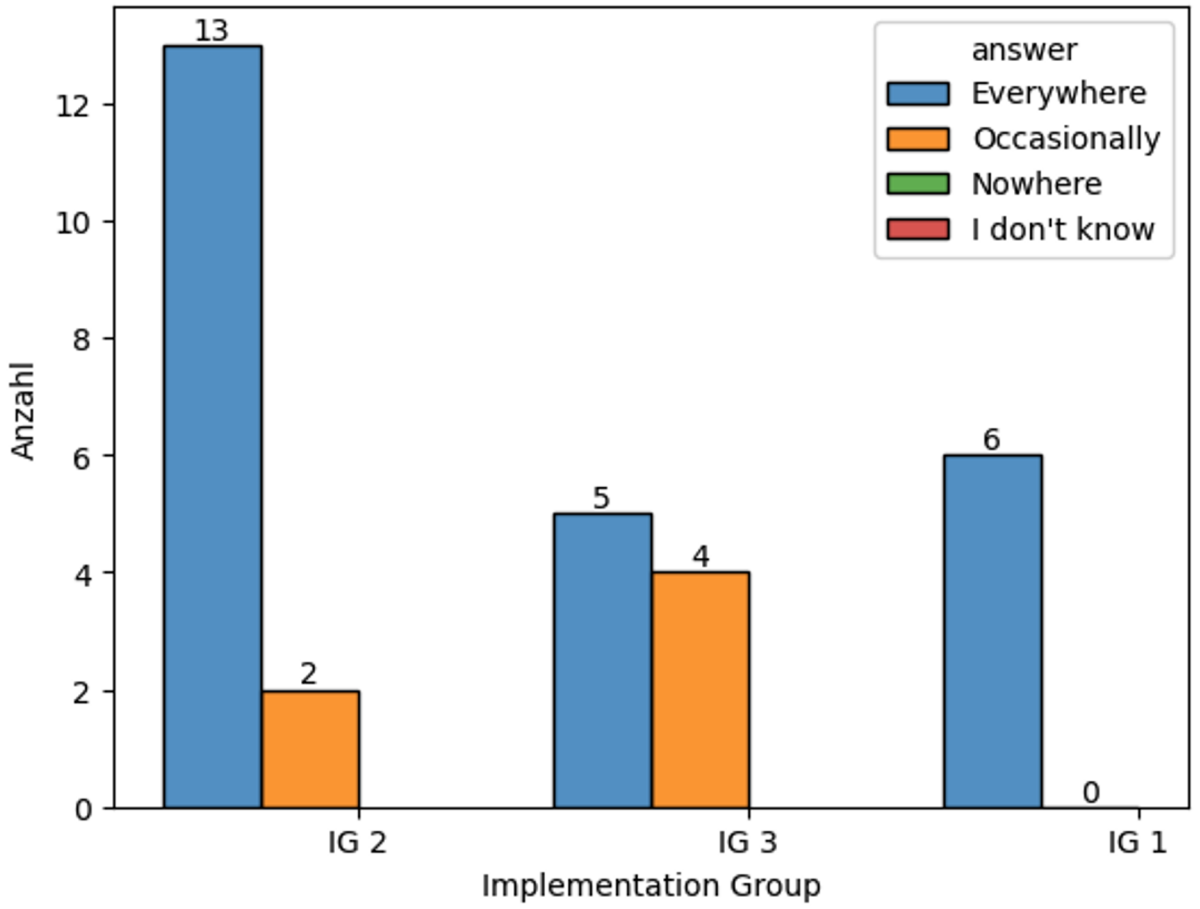
Context – research output

3 Implementation Groups	167 controls 6 categories
83 questions 4 possible answers	30 companies (DACH)

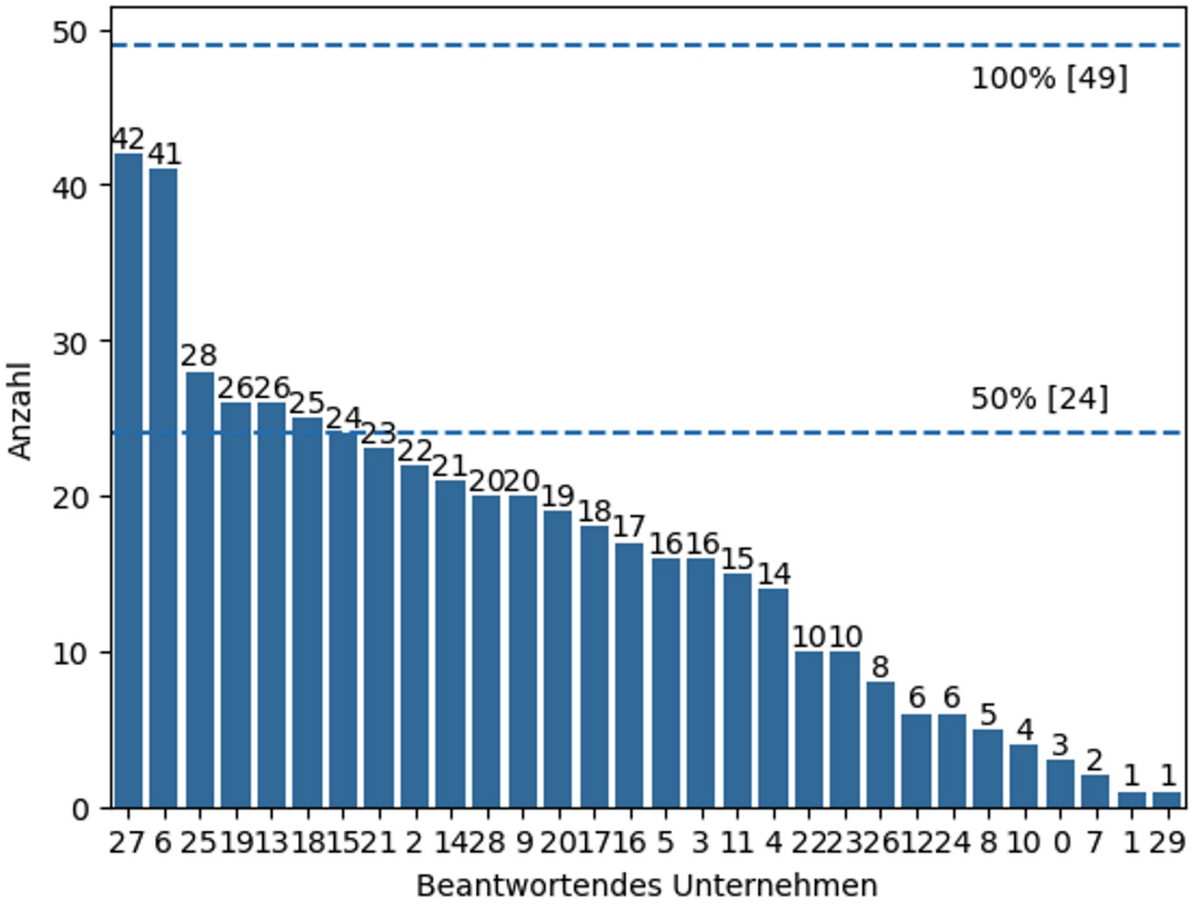
Findings - Companies per IP



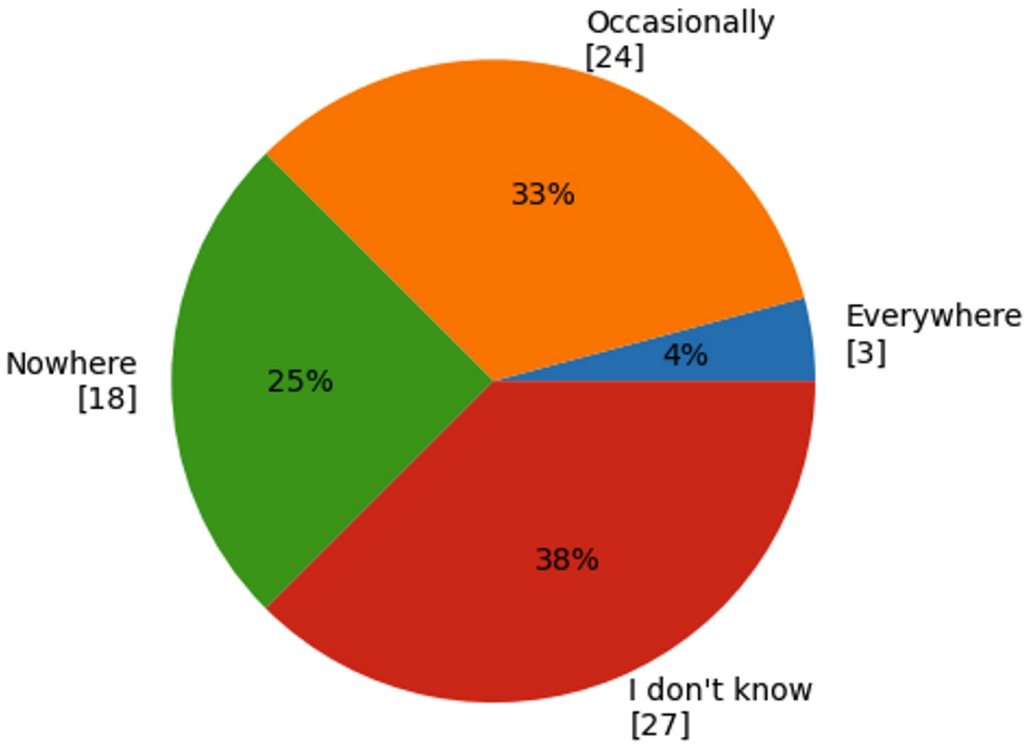
Findings - Using VCS



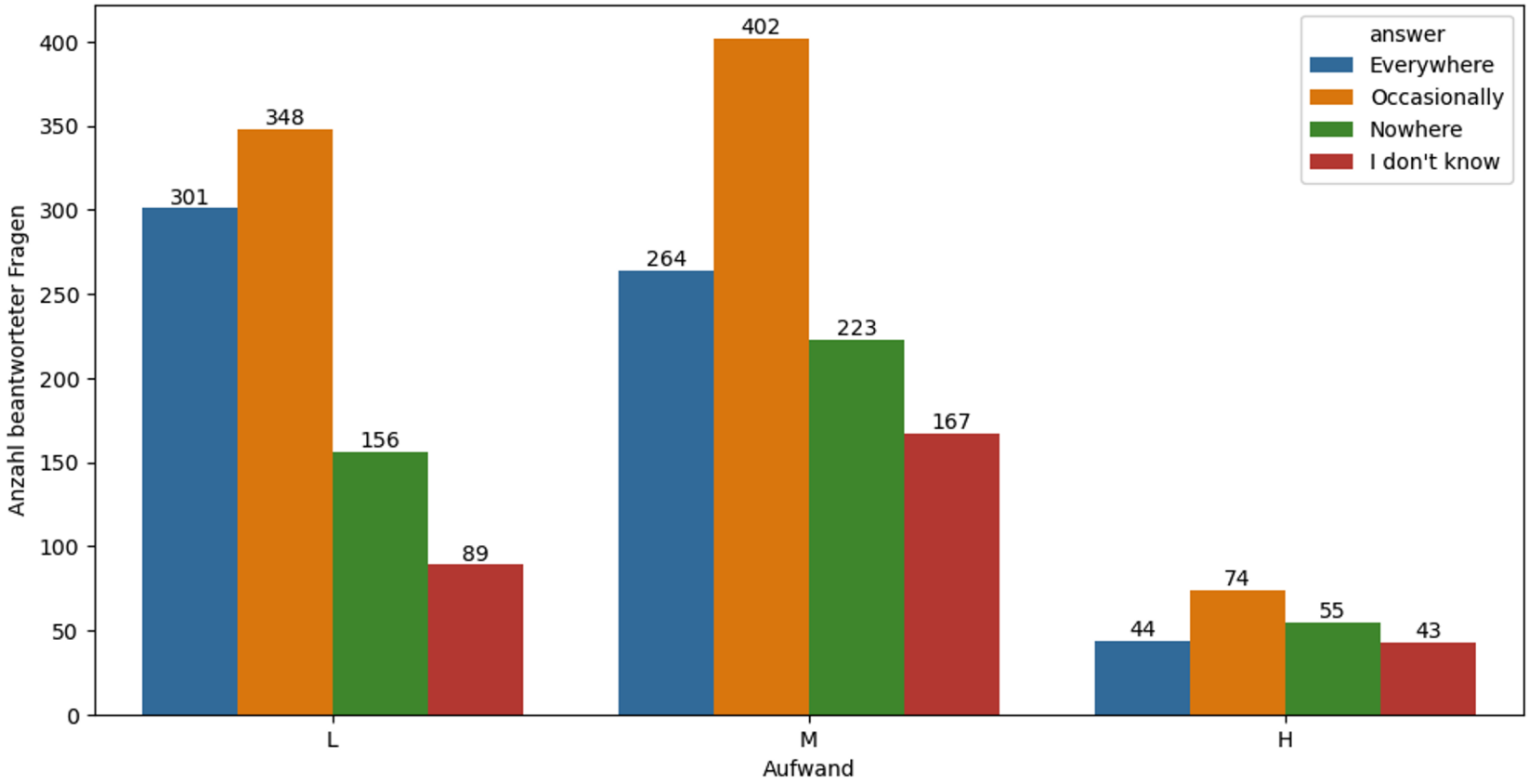
Findings - Implementing all IG1 controls



Findings - Implementing IG3 controls



Findings - Controls vs Effort



Lessons Learned

👆IG / company size 👇Transparency	Low hanging 🍇 not reaped
~25-50% of controls per group not implemented	🙃 build, SBOM, attestation
scans, tests & checks 🤝 policies	automation is 🔑 (IaC, pipelines, testing, PaC, ..)

The Hard Truth

👍 lots of information available

👎 many simple controls not implemented
👎 most complex controls not implemented

bigger company = less transparency/adaptation

Daniel Drack

Senior DevOps Engineer @ FullStackS

Organizer / Host
CNCG Graz + KCD Austria

- **BSc MA MBA**
- CK{A/AD}, TFA, VA, GitLab, PSM I, Snyk

daniel.drack@fullstacks.eu
https://drackthor.me
@DrackThor

Further Reading

Code:

- SAST
- (GitLab) Push Rules
- Codeowners
- IaC Scanning Tools
- The Test Pyramid

Dependencies:

- SCA Tools
- SBOM Introduction
- Dependency Track

Build:

- Reproducible Builds
- Zero Trust Paradigm
- container based build

Artifacts, Distribution & Deployment:

- The Update Framework
- In-Toto Attestation
- Sigstore

used Literature (selection):

- CNCF Supply Chain Best Practices
- CIS Supply Chain Security Guide
- NIST SSDF
- SLSA
- OSSF S2C2F
- OWASP ASVS
- SSA Secure Software Controls