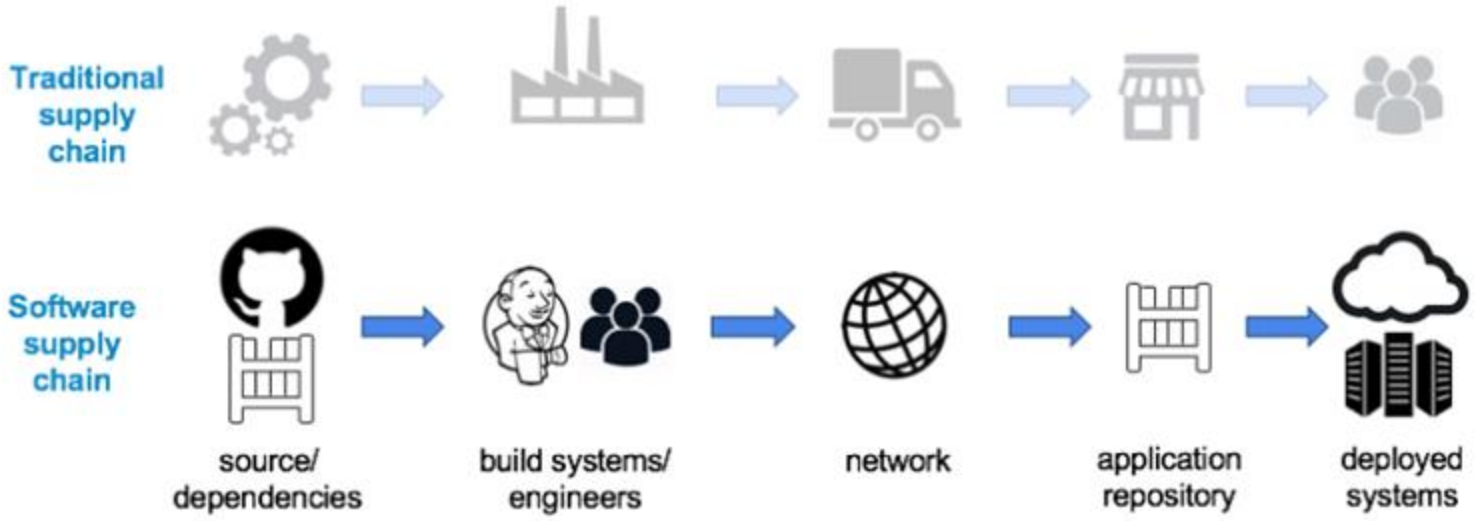
cloud-native software supply chain security: the hard truth

Software Supply Chain

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

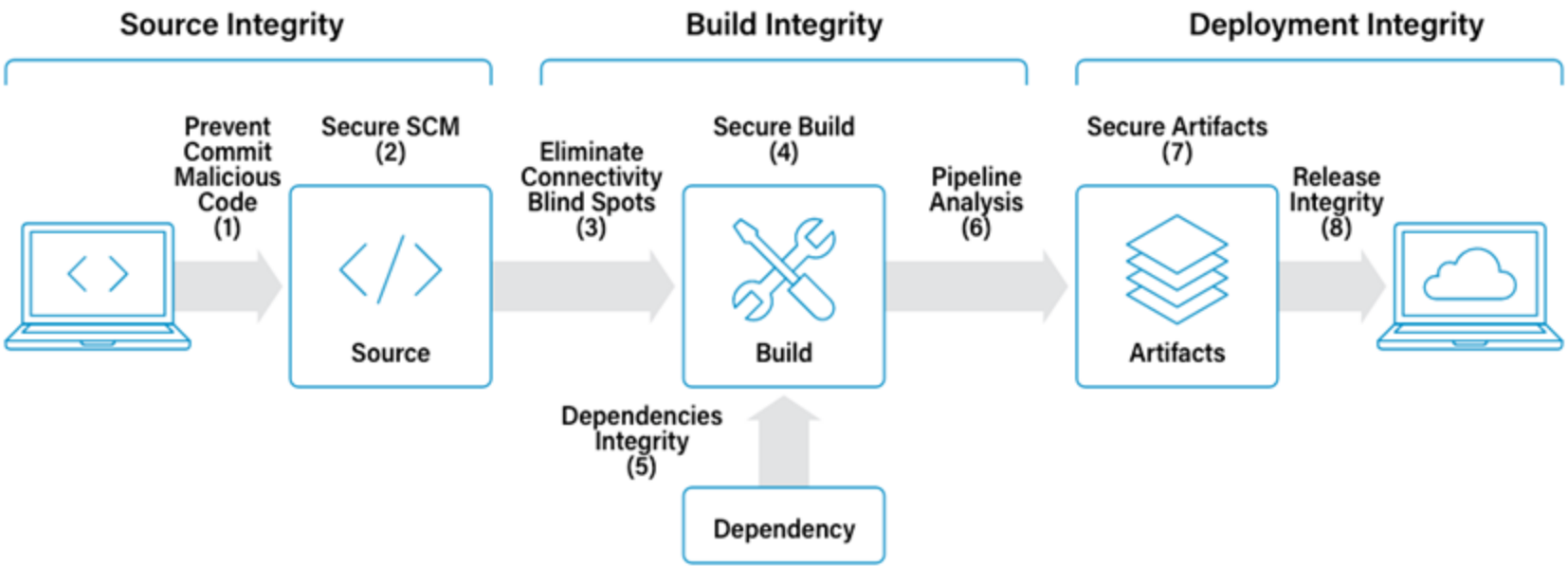
Melara & Bowman, 2022, Intel Labs

CNCF - SSC in a 🥥

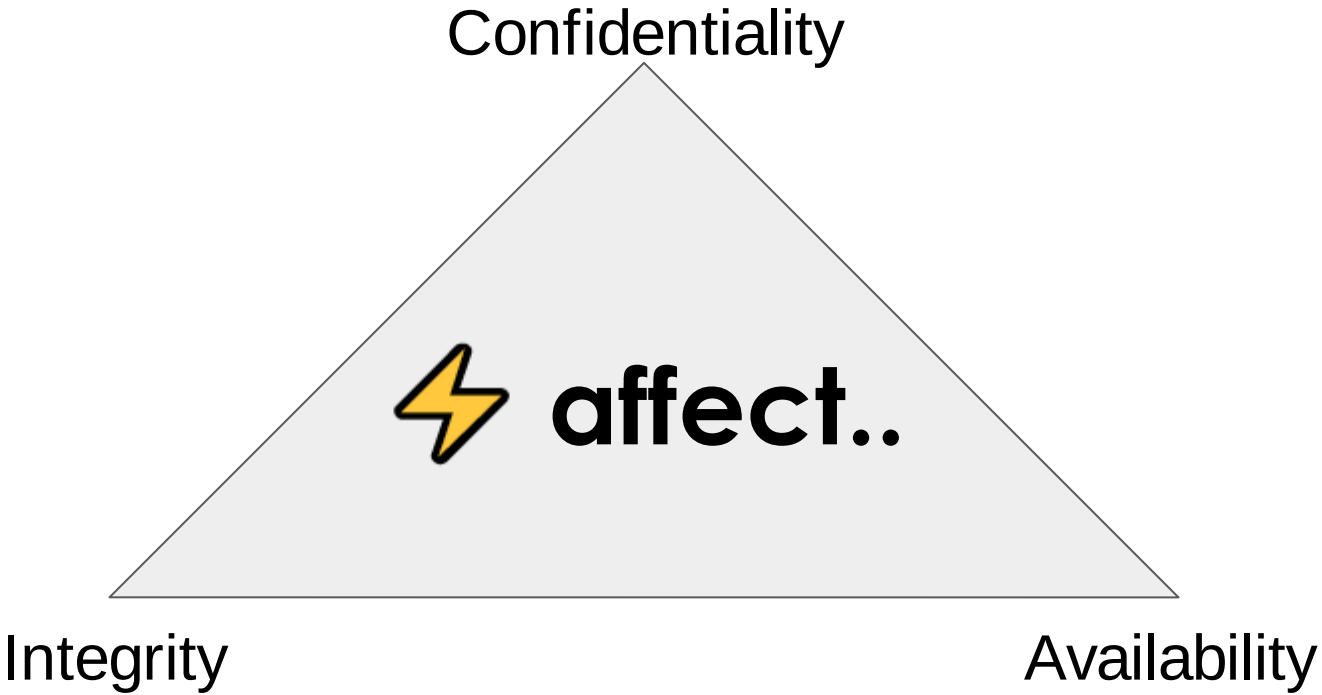


https://github.com/cncf/tag-security/blob/main/supply-chain-security/supply-chain-security-paper/CNCF_SSCP_v1.pdf

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: Code - show of ✋

mandatory MFA for source code access

—

enforced commit message convention

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

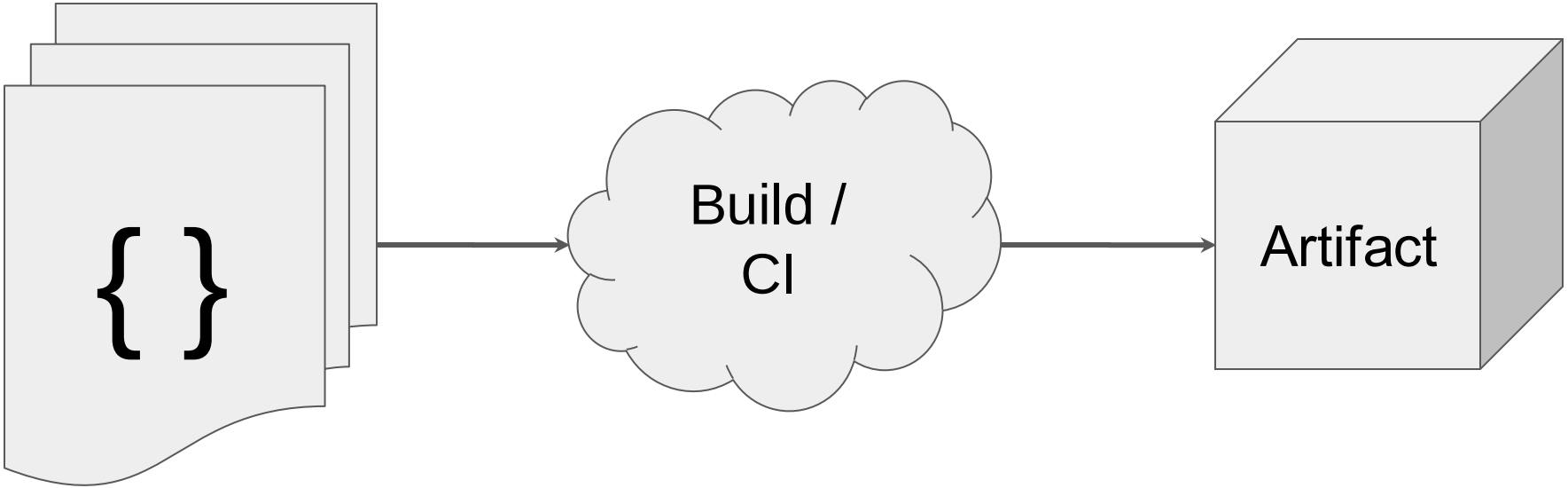
Stage: Dependencies - show of ✋

using a package manager

—

package usage policy in place

Stage: Build



Stage: Build

threats

- build bugs
- malicious env

solutions

- dedicated env
- zero trust
- single use env
- pipelines
- as code
- reproducible

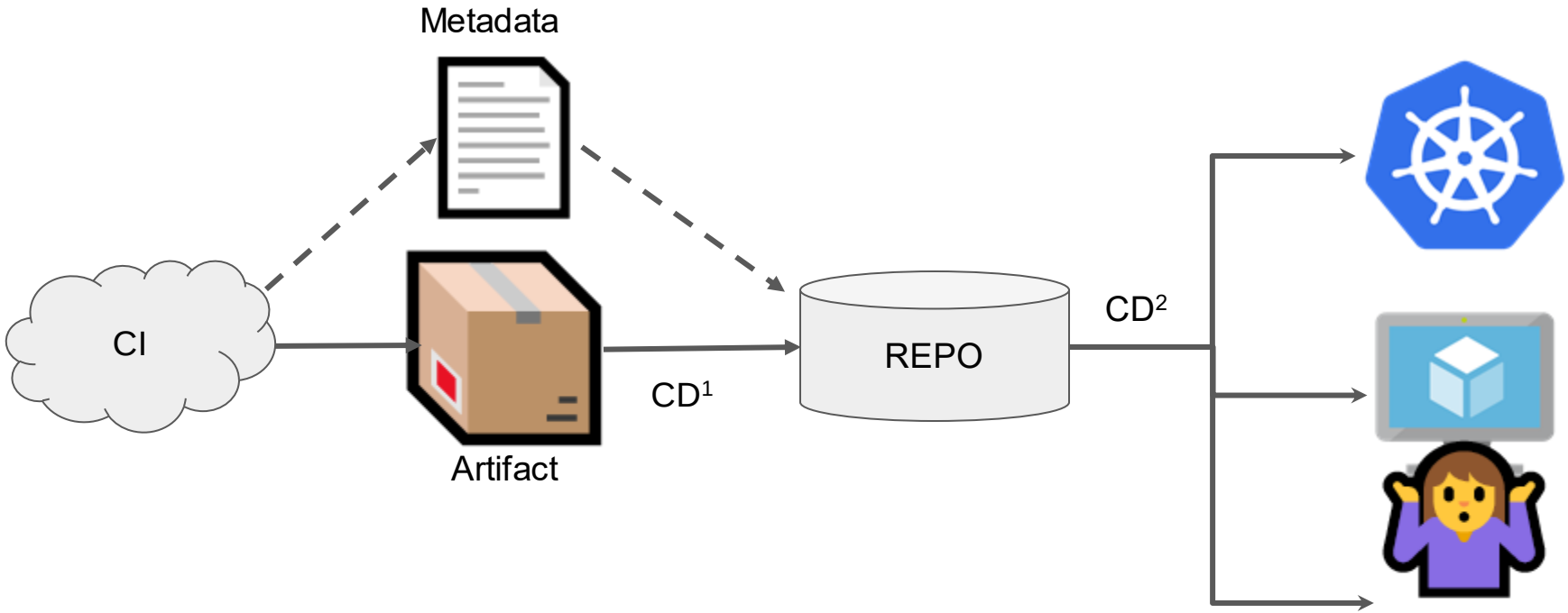
Stage: Build - show of ✋

fully automated build

—

truly bitwise reproducible builds

Stage: Artifacts & Distribution/Deployment



CD¹ … Continuous Delivery
CD² … Continuous Deployment

Stage: Artifacts & Distribution/Deployment

threats

- theft / deletion
- replacement
- no transparency
- updates

solutions

- repo security
- signatures
- attestation
- SBOM
- TUF

Stage: Artifacts - show of ✋

dedicated artifact management

—

create “extended” SBOM

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

MBA Master thesis research, looking for a "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

3 Implementation Groups

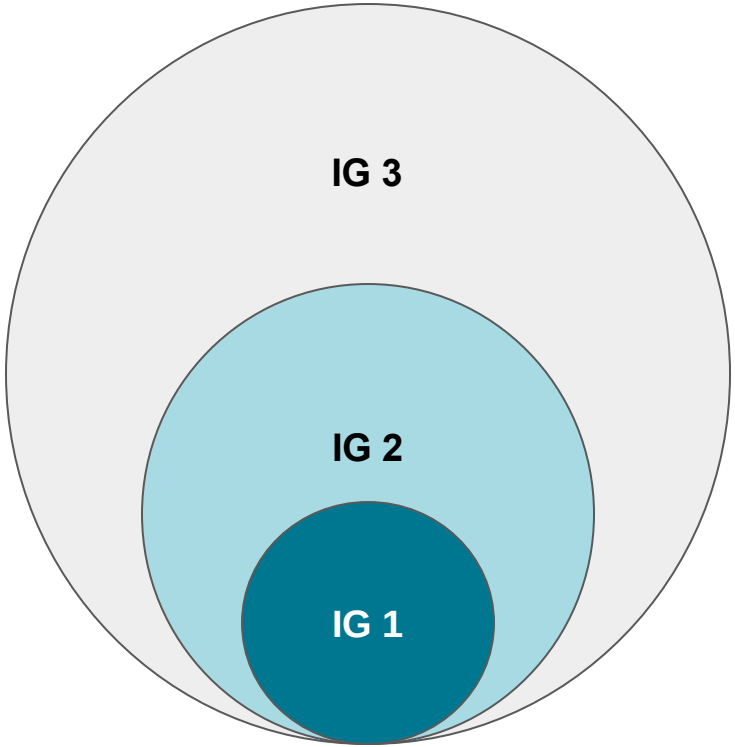
167 controls
6 categories

83 questions
4 possible answers

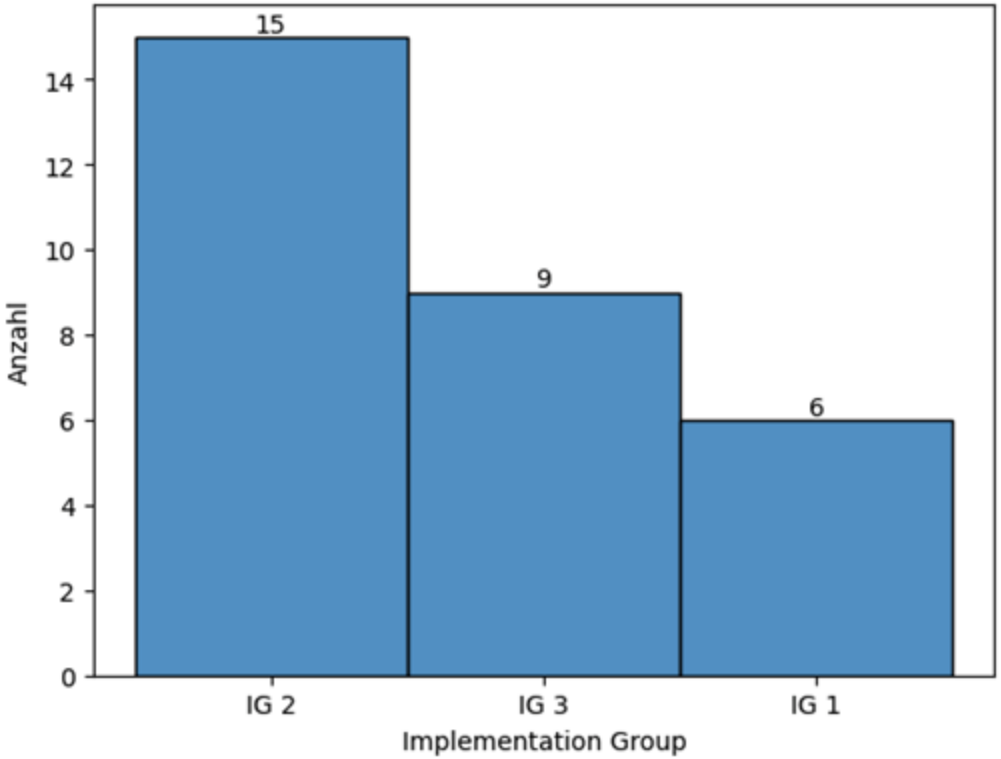
30 companies
(DACH)

Context

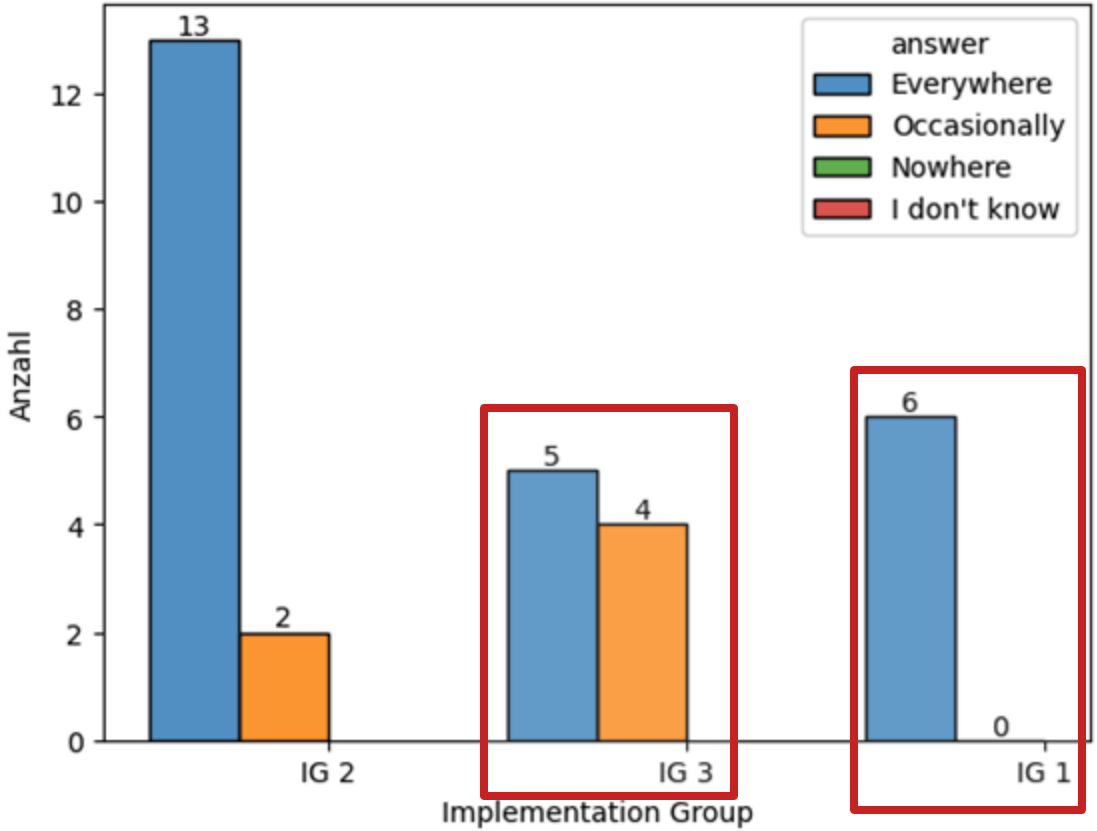
- IG 1
  - small company
  - no sensitive data
- IG 2
  - middle size company
  - some sensitive data
- IG 3
  - enterprise
  - highly sensitive data



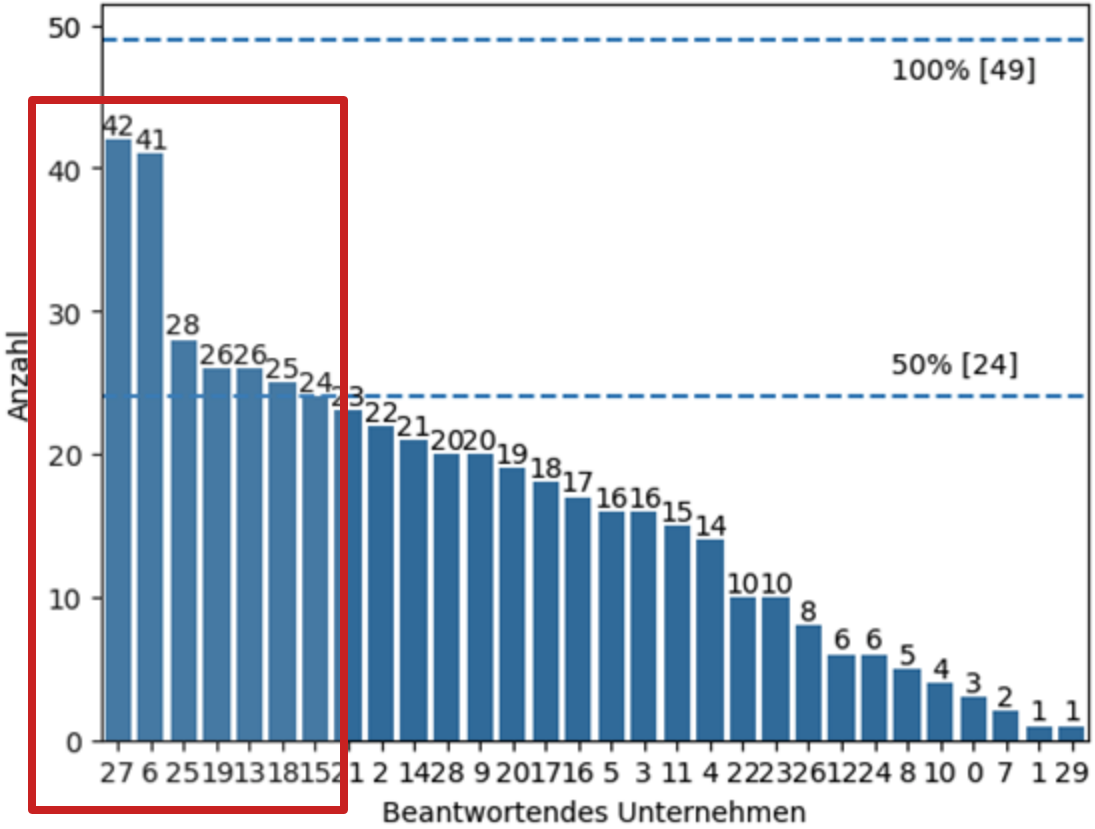
Findings - Companies per IP



Findings - Using VCS

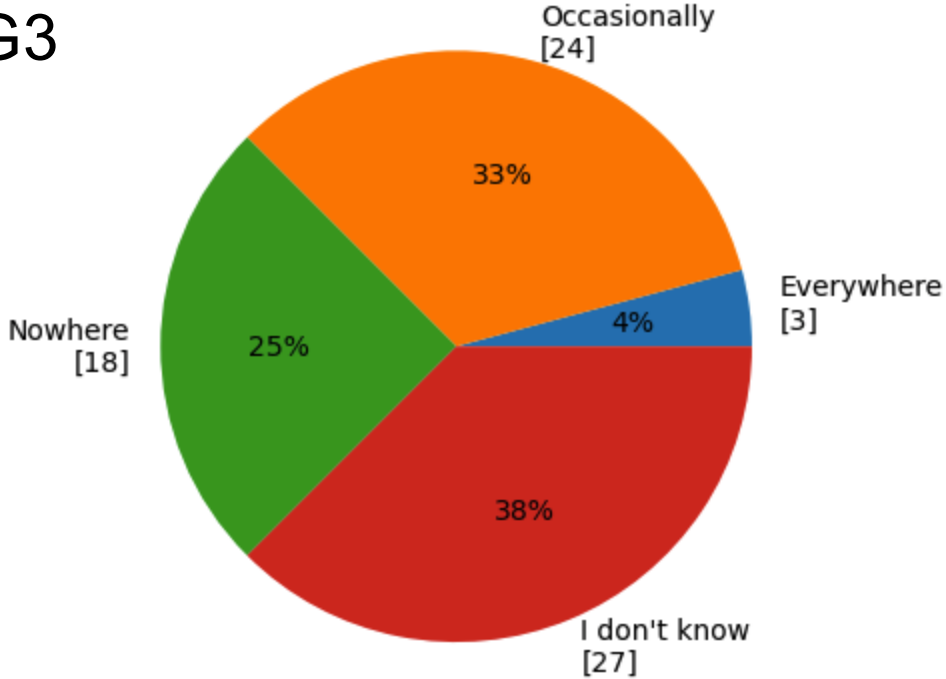


Findings - Implementing all IG1 controls

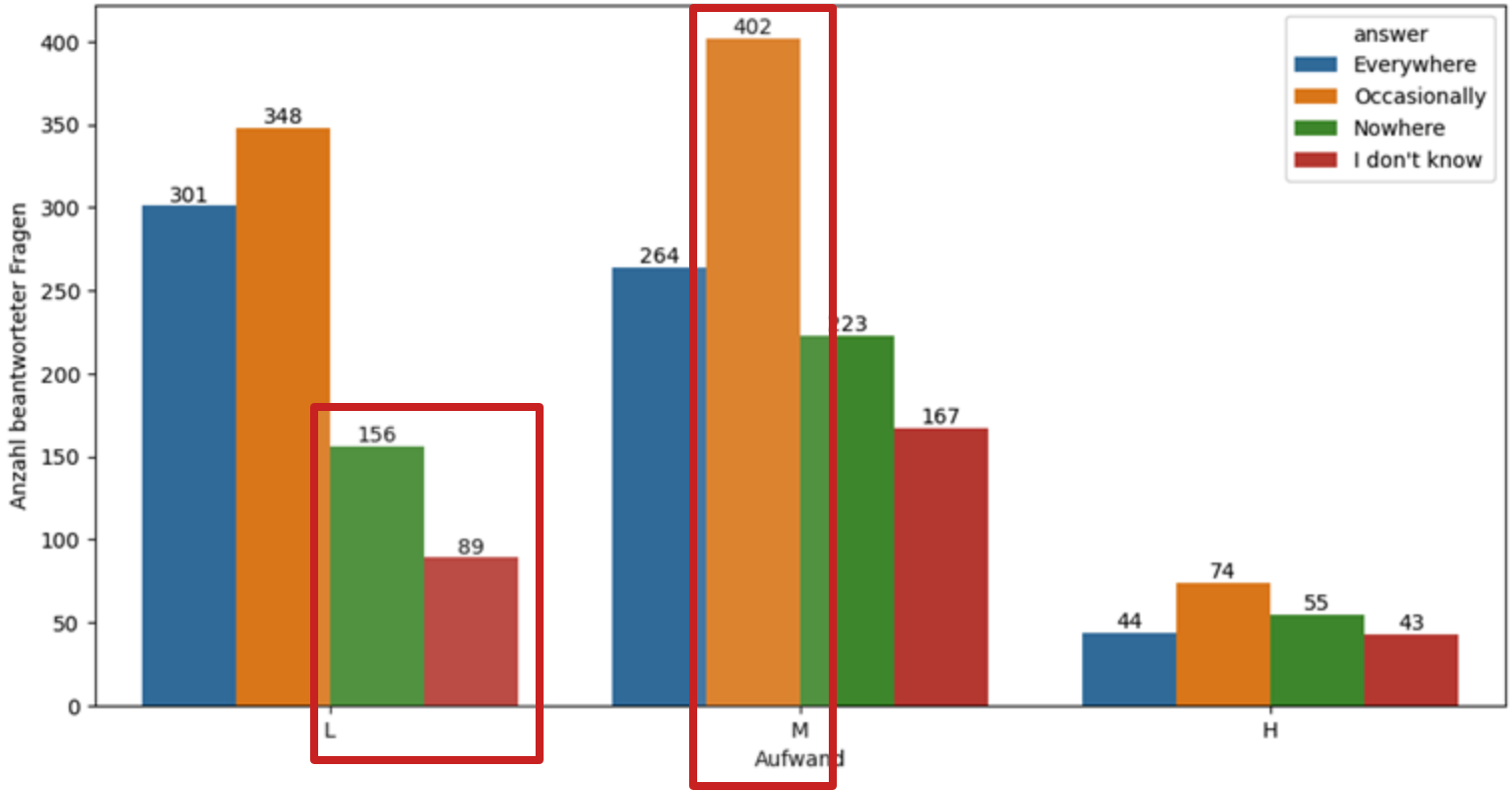


Findings - Implementing IG3 controls

- ☝️ only necessary for IG3 companies
- 😔 25% definitely not implemented
- 👍 ⅓ implemented somewhere
- 🤦♂️ > ⅓ unknown
  - no policy?
  - know how?



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