OpenElements

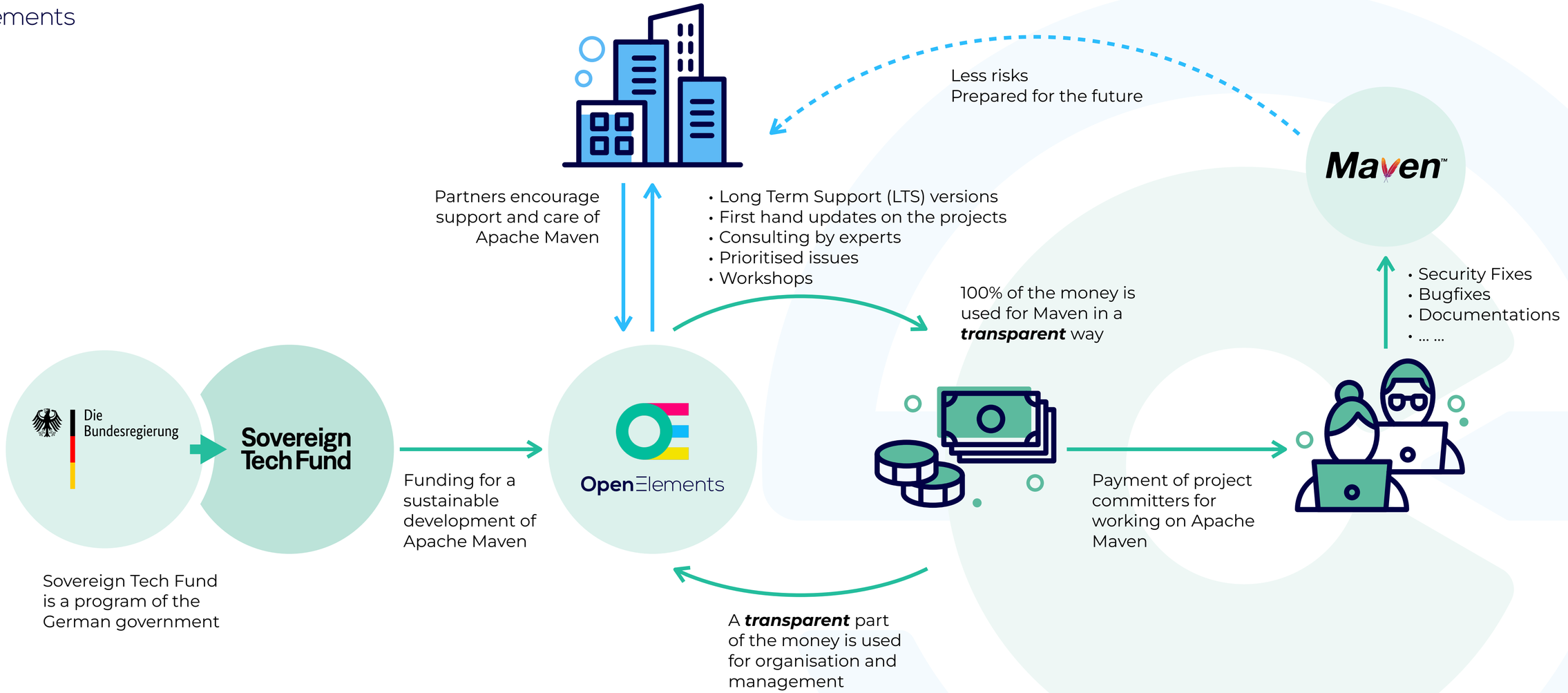
Supply Chain Security

OpenElements

Sebastian Tiemann

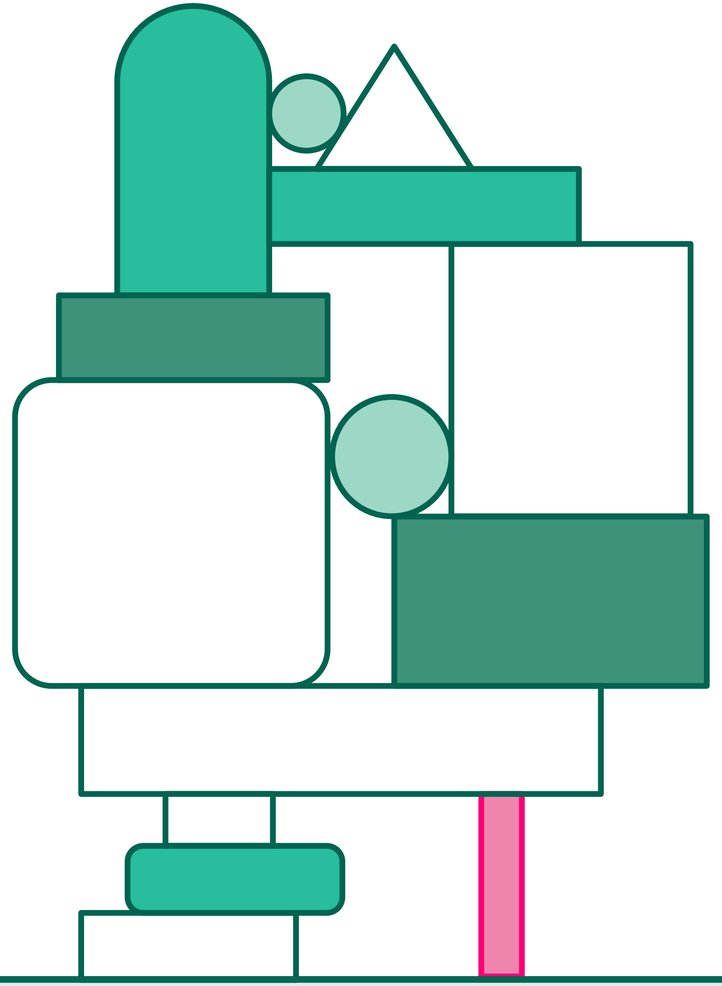
- Organizer Java User Group Dortmund
- Open Source Contributor
- ORCWG
- IT-Professional since +15 Jahren

OpenElements



Becoming a Sustainable Program

- Around **70%** of a software product **lies beyond direct** control of the maintainer
- Developers frequently **lack visibility** into dependency origins and maintainers
- Many critical software components are **maintained by a single developer** in their free time — far more common than expected.



Risk of Software Development Today

"Beware of little expenses.
A small leak will sink a great ship."
Benjamin Franklin

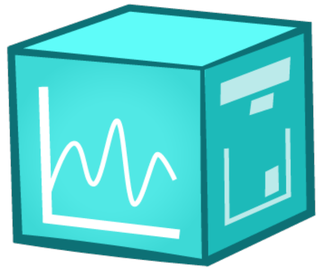
OpenElements

OpenElements

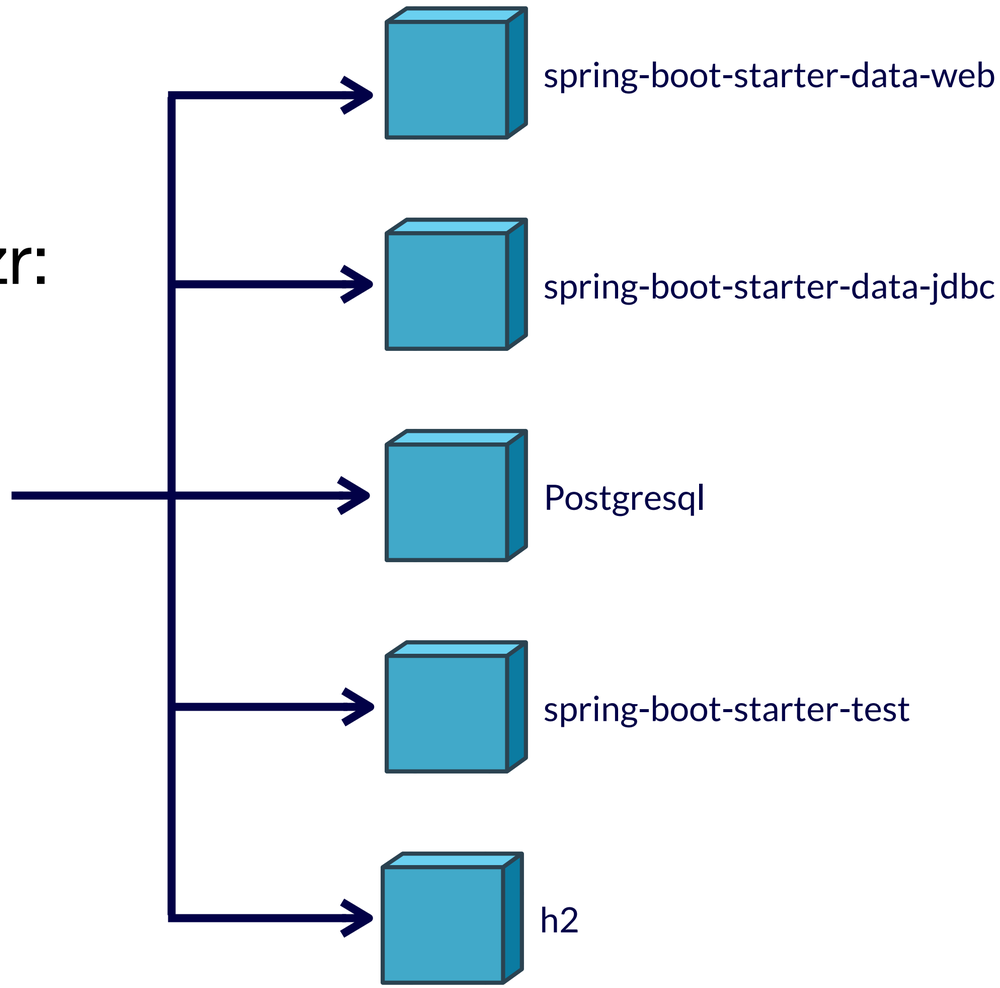
Software Development

—Software

Basis:
Spring Initializr:



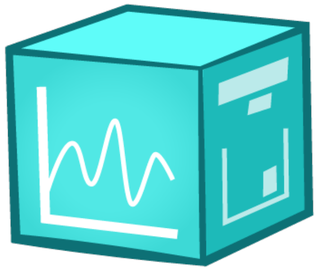
spring-boot-hello-world



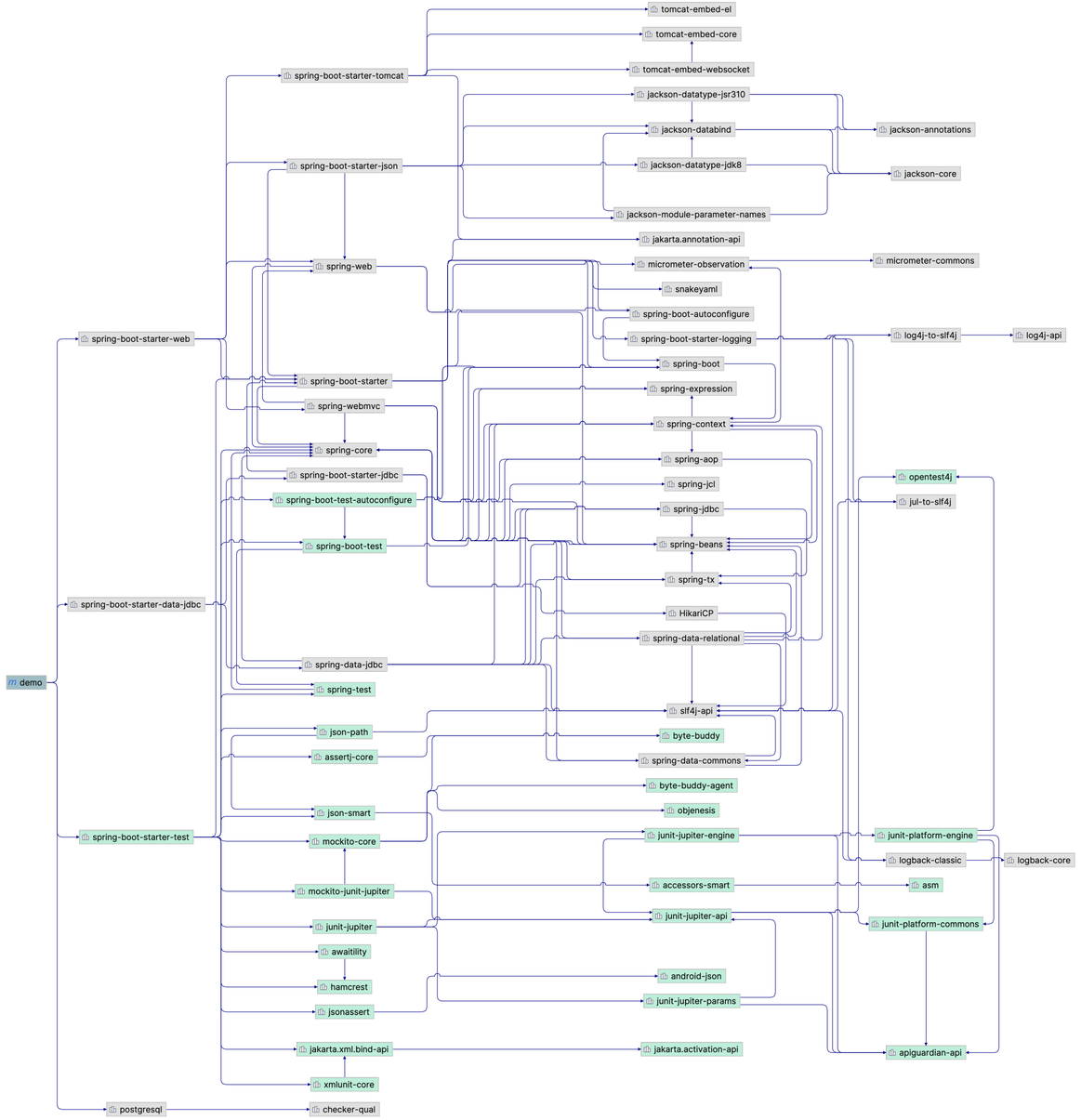
OpenElements

—Software

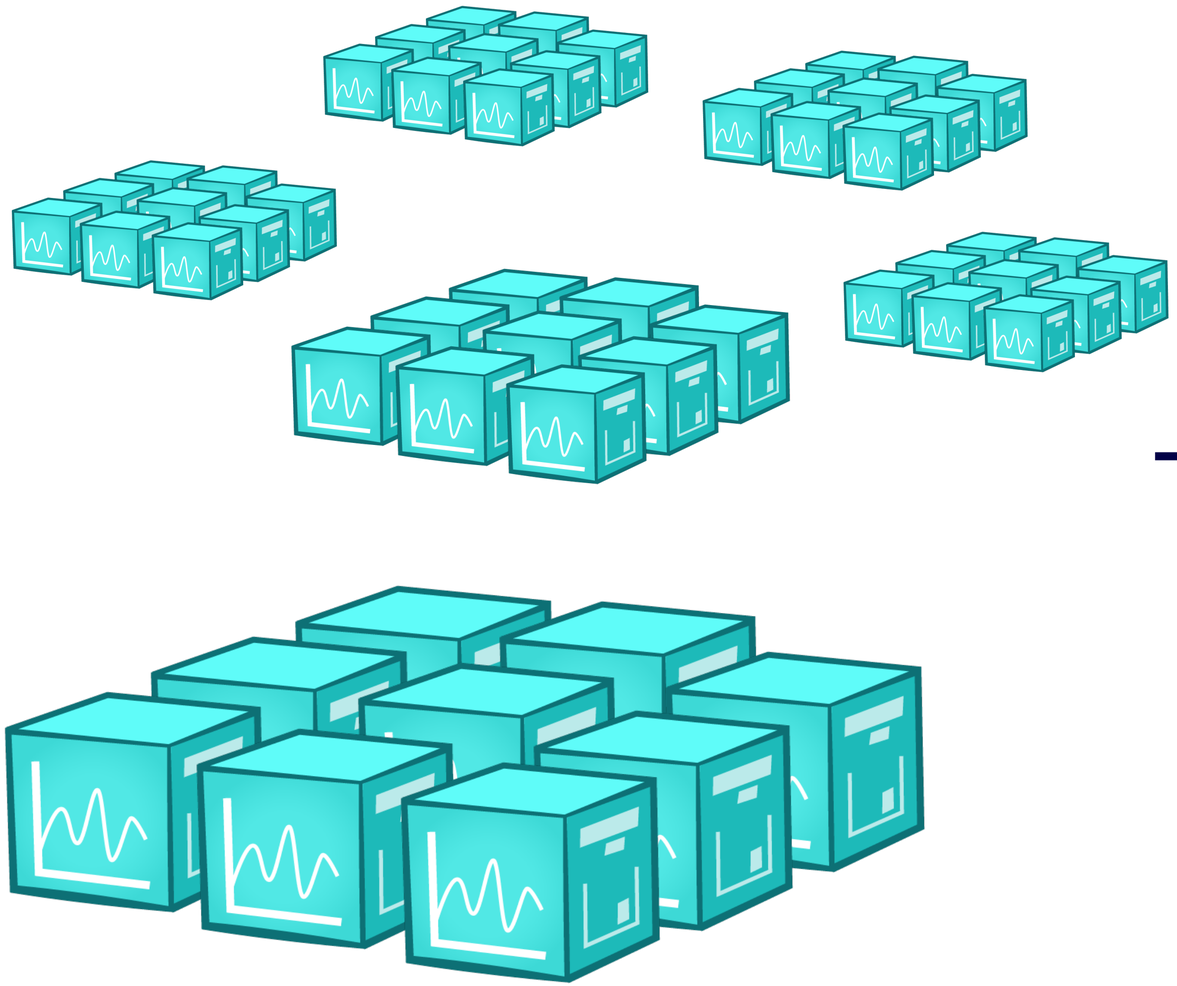
„simple Project“
made with Spring Initializr:



spring-boot-hello-world



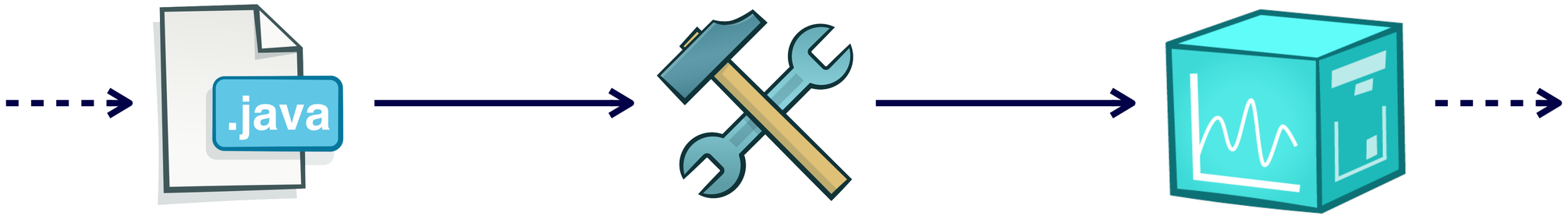
Software Product



OpenElements

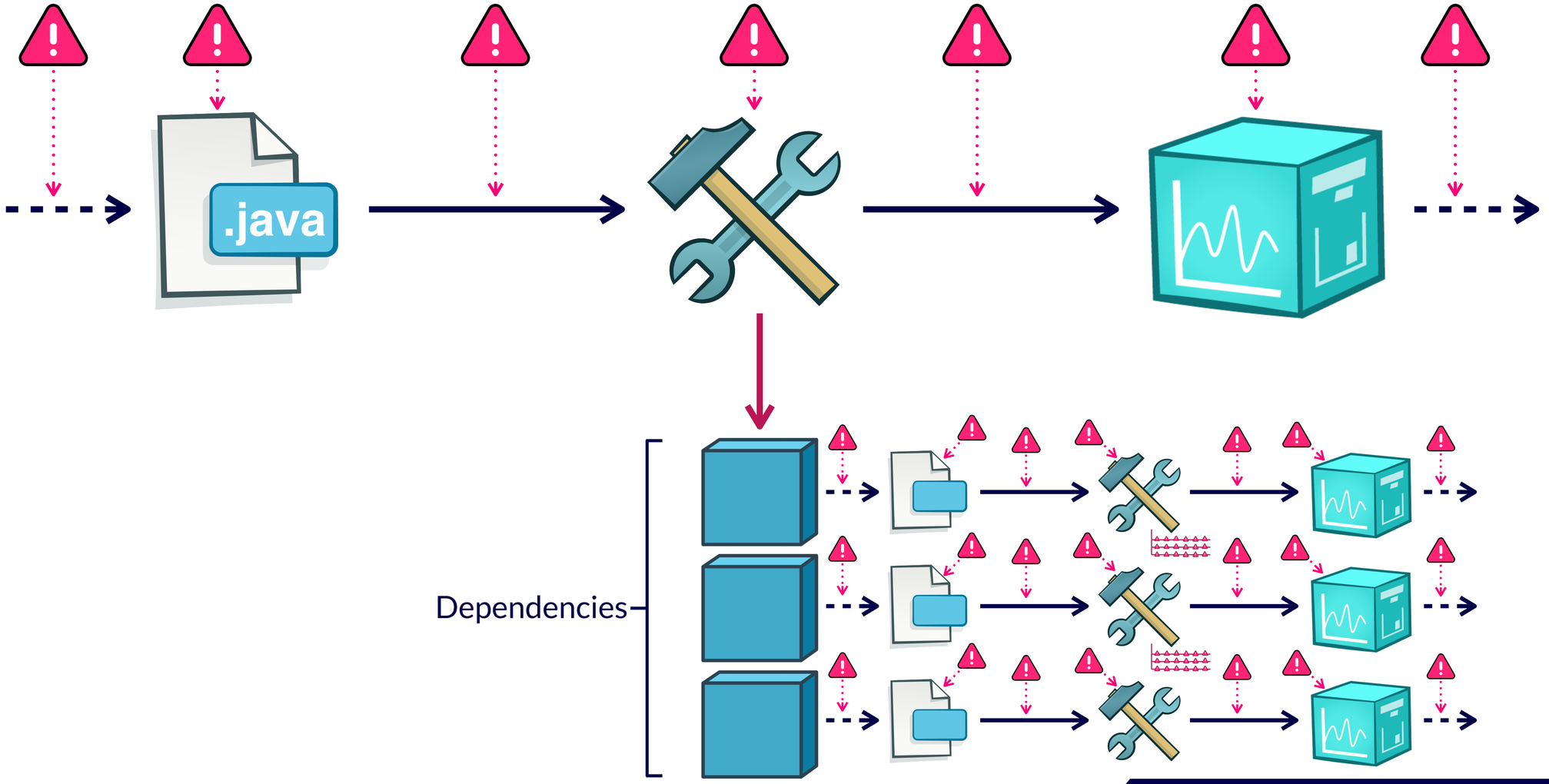
—Software Supply (Chain)

Supply Chain



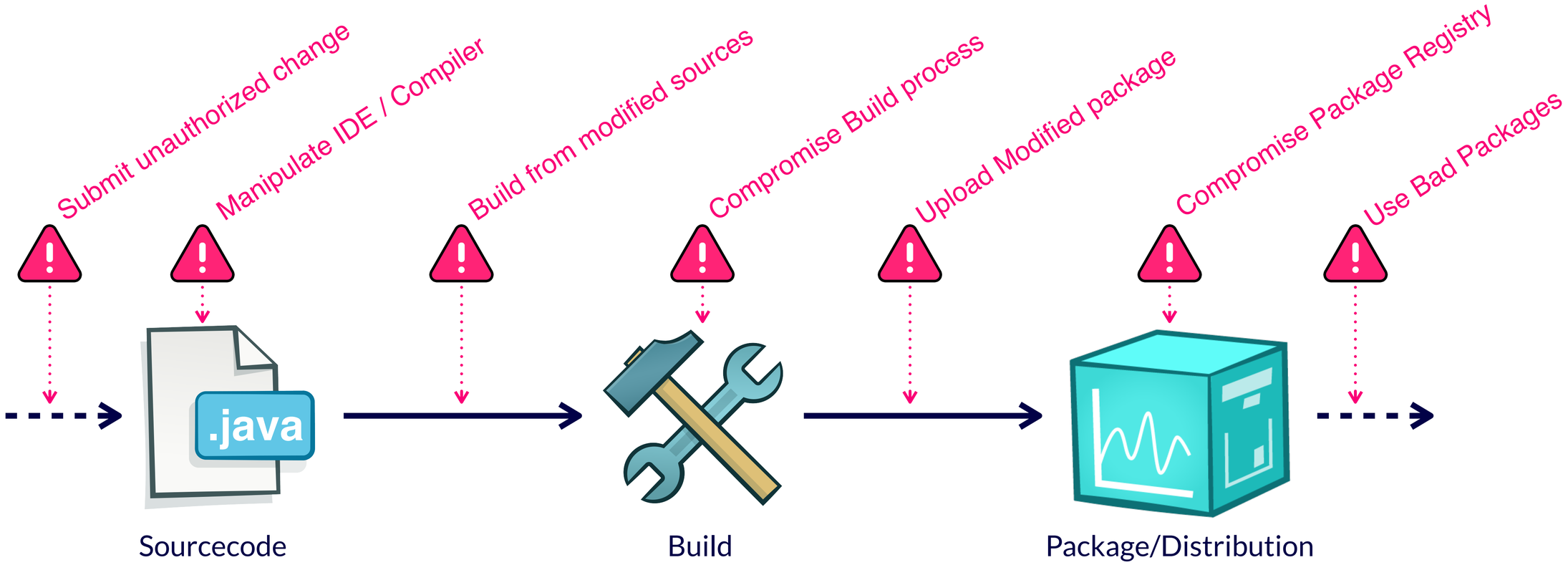
OpenElements

Dependency Supply Chain



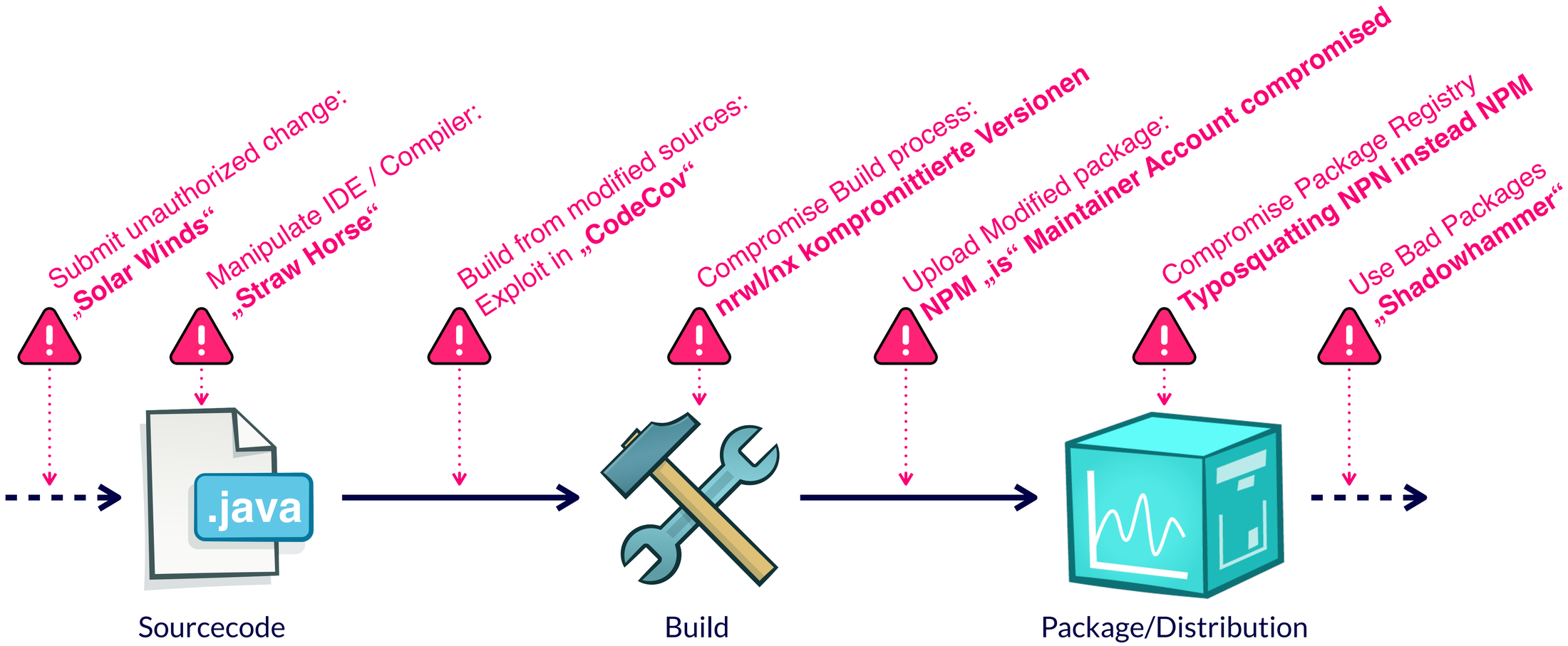
OpenElements

—Supply Chain Security Threats



OpenElements

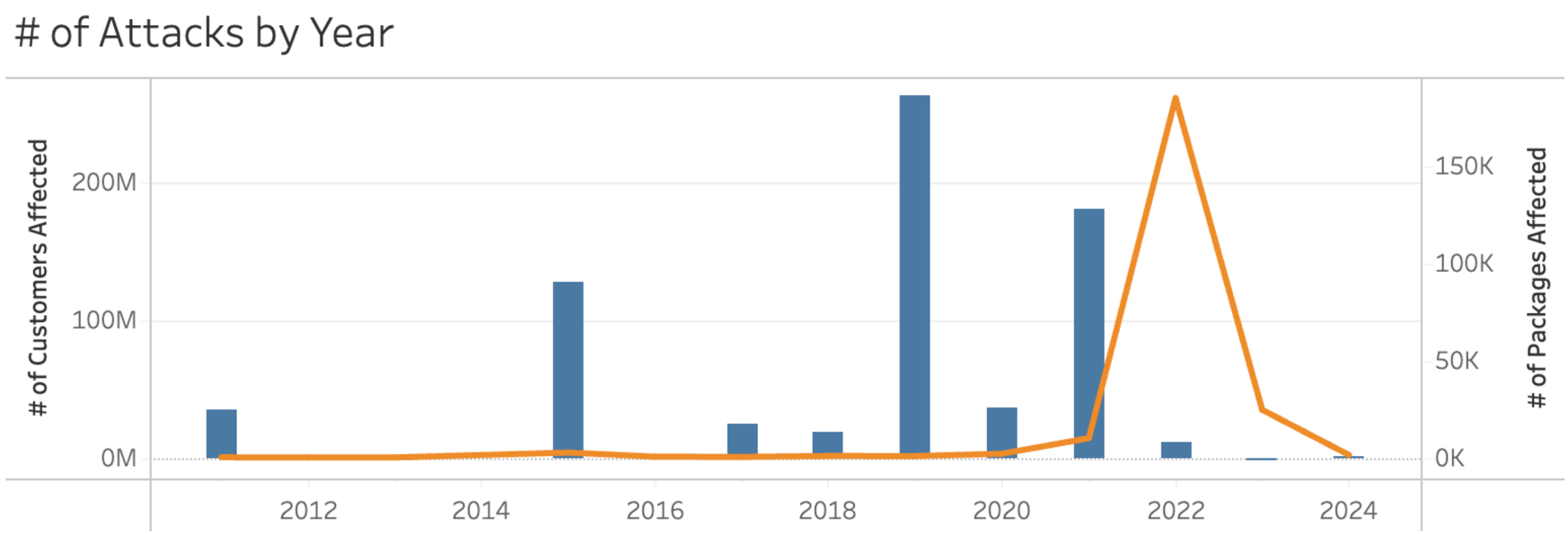
—Supply Chain Security Threats



Supply Chain Attacks

OpenElements

Supply Chain Attacks



19.08.2025, 12:39
https://www.comparitech.com/software-supply-chain-attacks/

Quelle: comparitech.com

Total Packages Affected

228,110

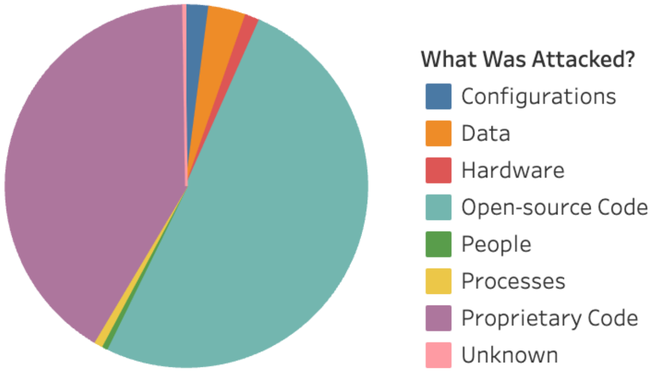
Total Customers Affected

700,569,233

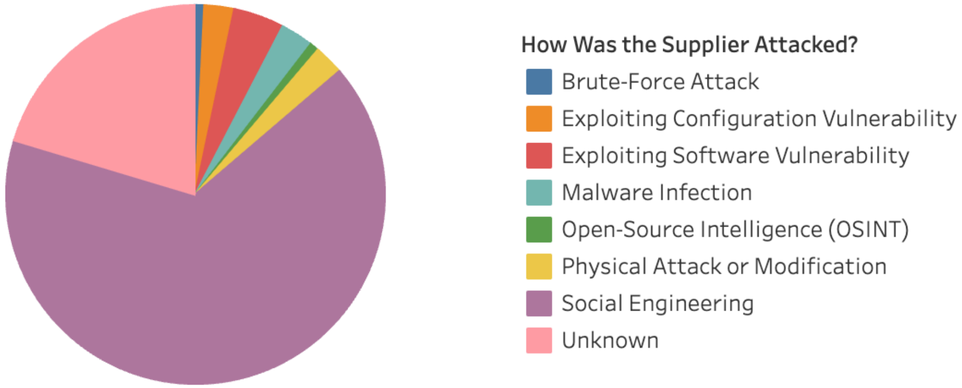
OpenElements

Supply Chain Attacks

Supplier Attacks-Target

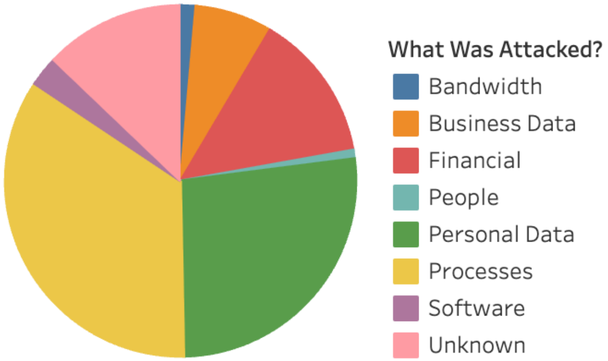


Supplier Attacks-Type

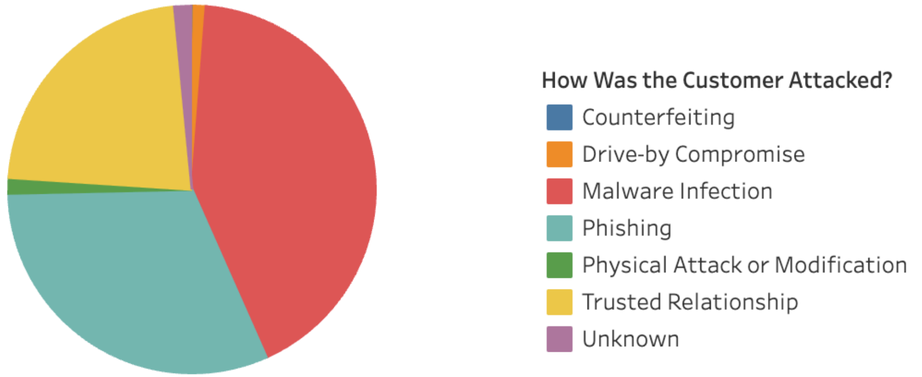


Quelle: comparitech.com

Customer Attacks-Target



Customer Attacks-Type



(How) Can Open-Source help?

Links

- https://www.comparitech.com/software-supply-chain-attacks/
- https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic
- https://theintercept.com/document/strawhorse-attacking-macos-ios-software-development-kit/
- https://www.cyberark.com/resources/blog/breaking-down-the-codecov-attack-finding-a-malicious-needle-in-a-code-haystack
- https://github.com/nrwl/nx/security/advisories/GHSA-cxm3-wv7p-598c
- https://socket.dev/blog/npm-is-package-hijacked-in-expanding-supply-chain-attack
- https://arstechnica.com/security/2025/07/open-source-repositories-are-seeing-a-rash-of-supply-chain-attacks/
- https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/