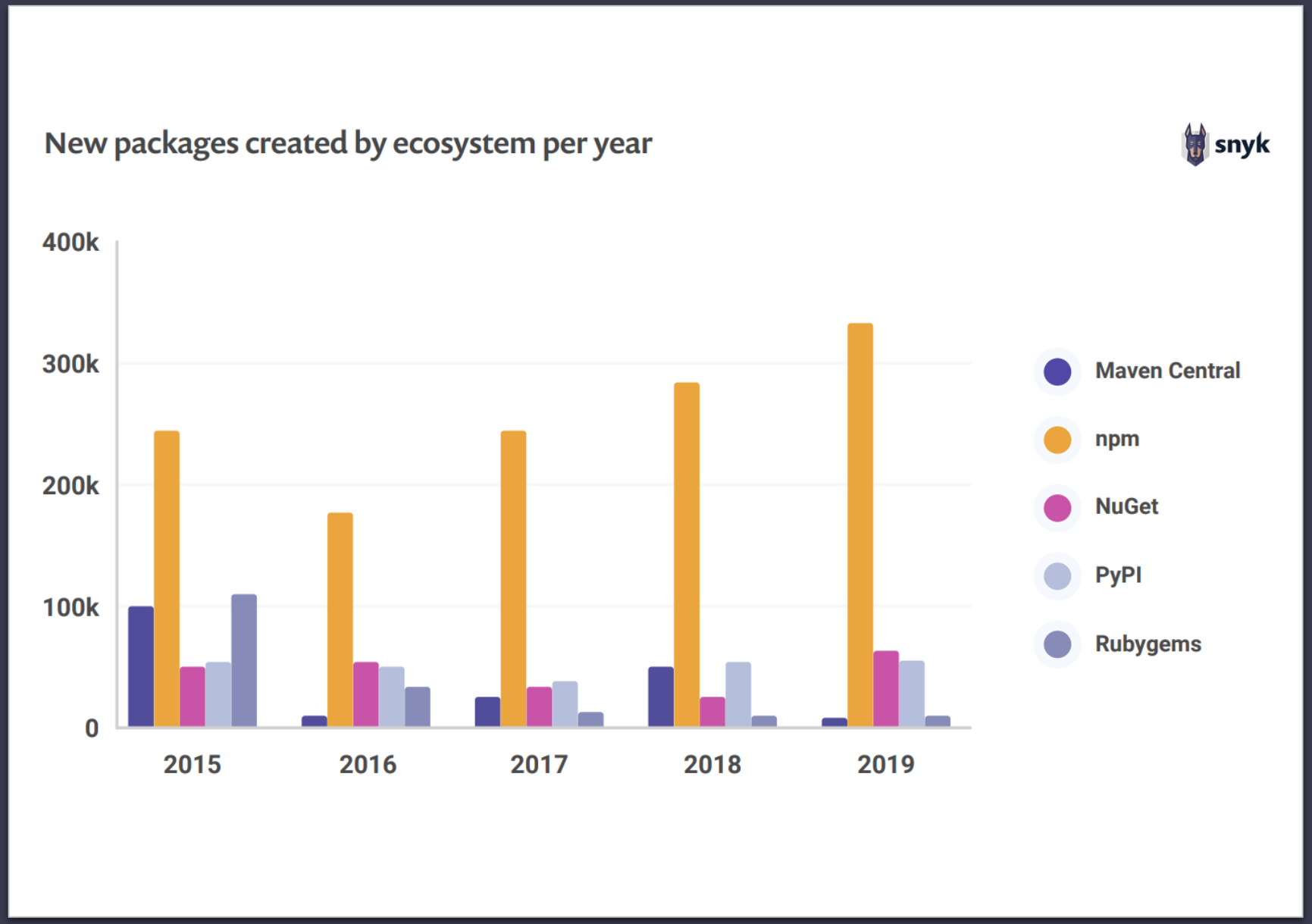
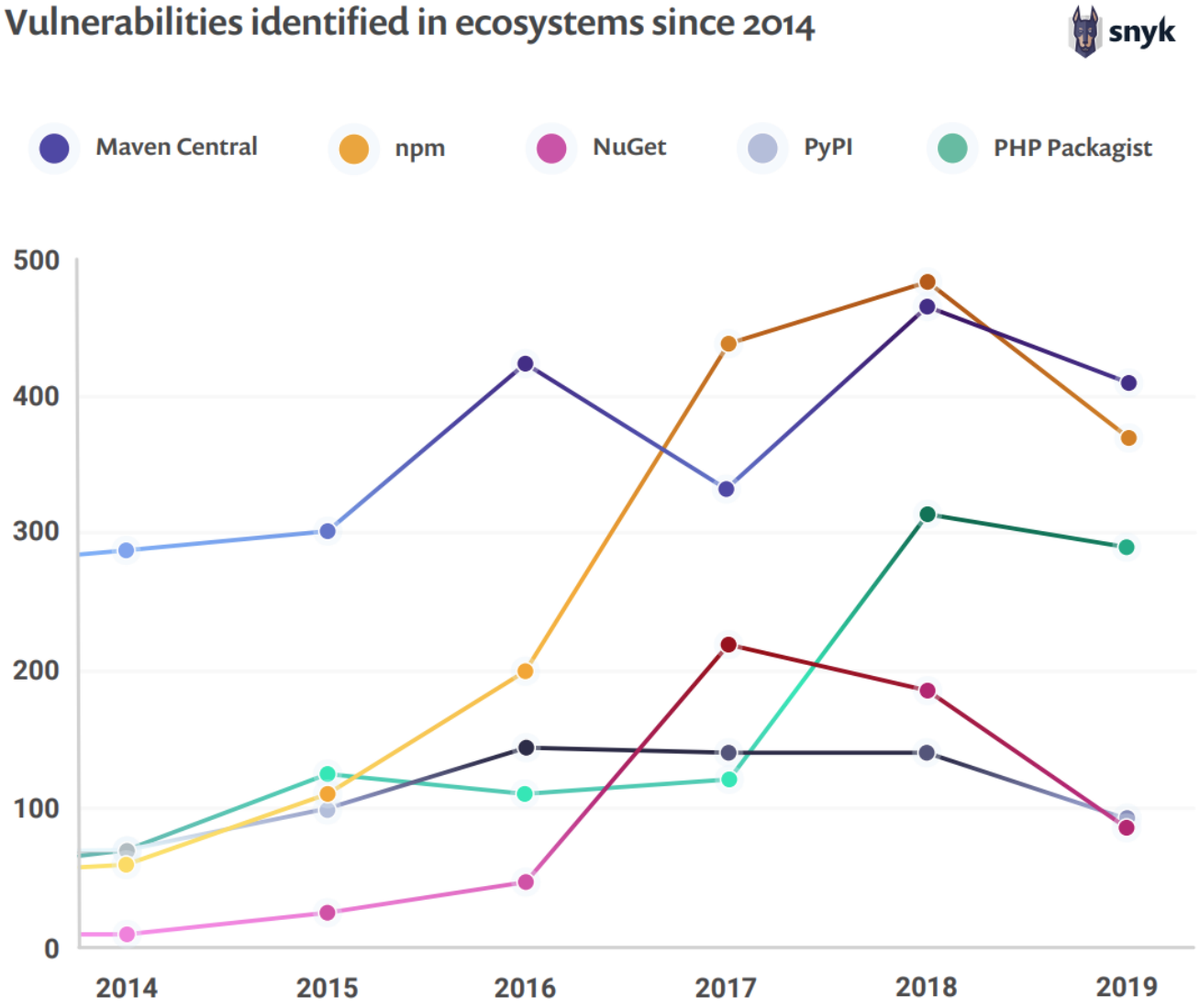
PORSCHE
INFORMATIK

Dependency Management

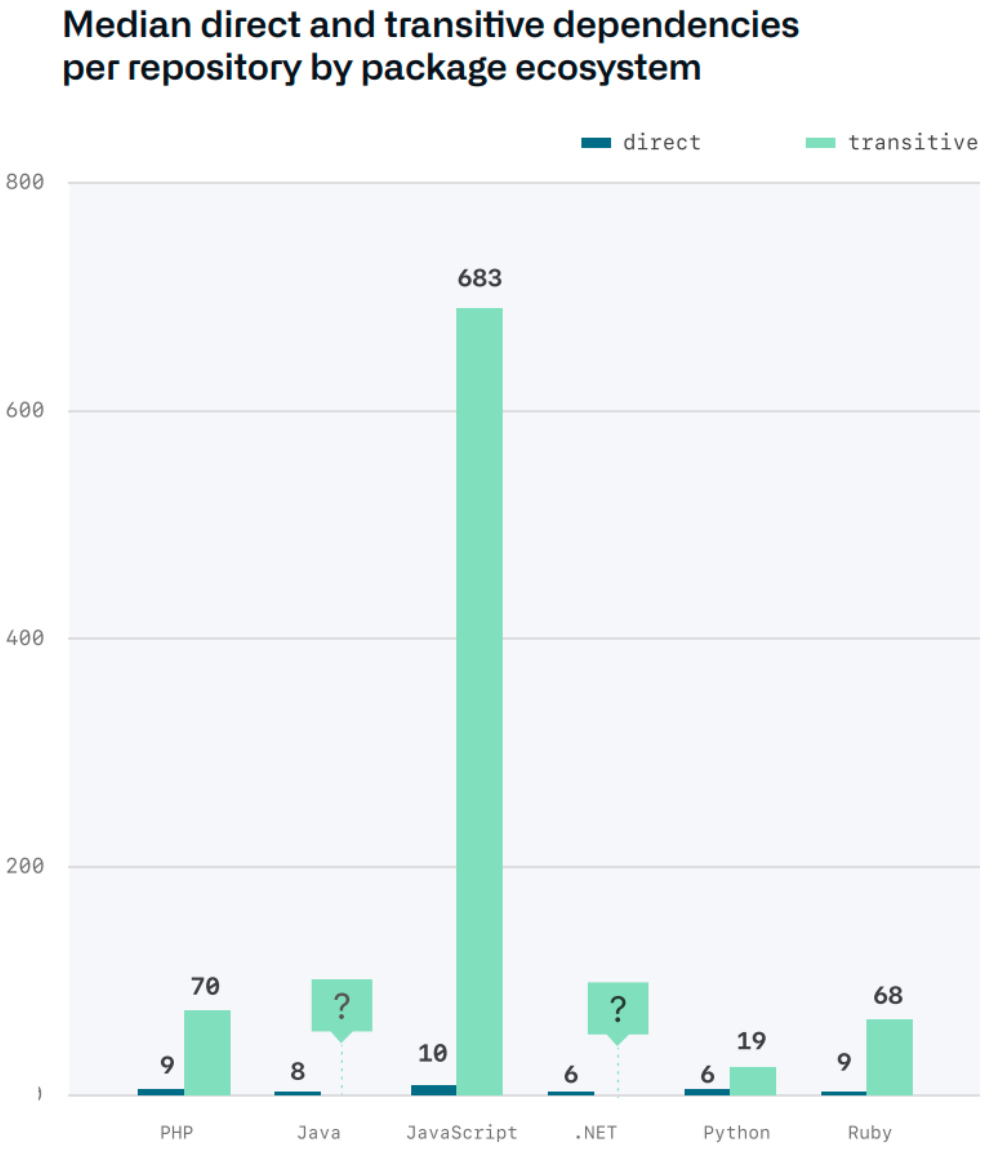
Christian Köberl
twitter.com/derkoe github.com/derkoe



Open Source Libraries

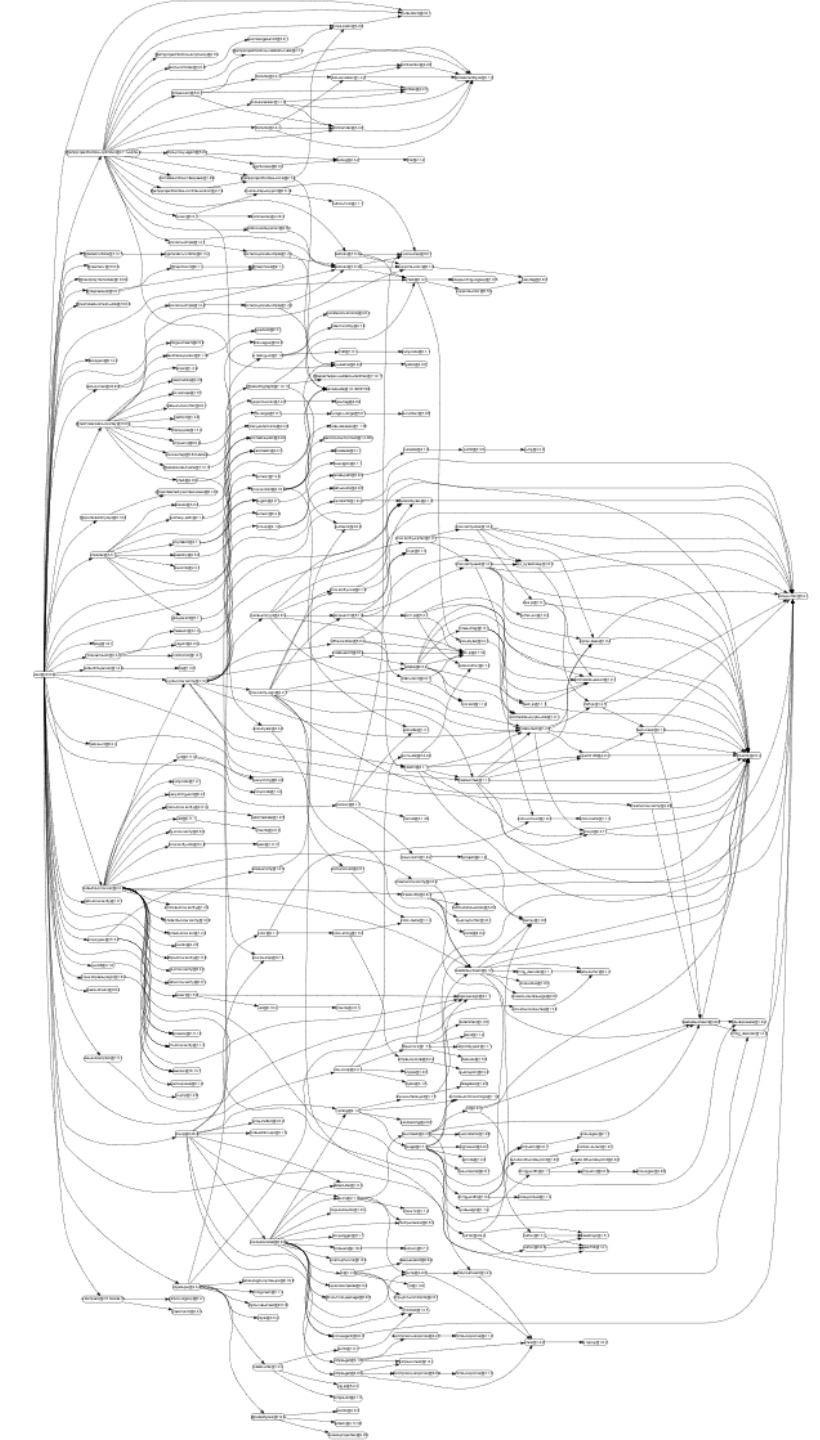


Open Source Vulnerabilites



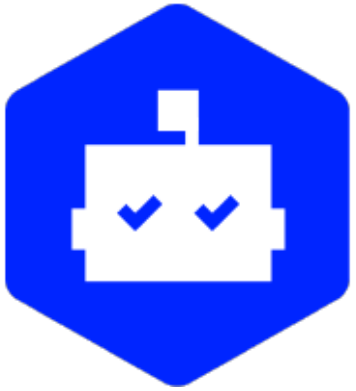
Dependency Count

Next.js Dependency Graph



New Kids On the Block

Ansible
Terraform
Docker
Helm
…



DependaBot

Renovate

Die Lösung: Continuous Updates

Demo: Renovate

Erfahrungen

- Renovate sehr flexibel (regexManagers) und unterstützt mehr Sprachen/Tools
- Auf GitHub: Renovate + Security Updates durch Dependabot
- Zusätzlich auch noch Snyk empfehlenswert
- Renovate OnPrem Setup sehr einfach
  (gratis Lizenzschlüssel notwendig)
- Renovate/Dependabot kann "lästig" sein
  - Gruppierung von Minor Updates
  - Pull/Merge Requests nur jede Woche/Monat/nach jedem Release

Quellen

- Snyk: The State of Open Source Security 2020 https://snyk.io/open-source-security/
- The 2020 State of the Octoverse https://octoverse.github.com/static/github-octoverse-2020-security-report.pdf#page=10
- Mike McGarr (Netflix): Dependency Hell, Monorepos and beyond https://www.youtube.com/watch?v=VNqmHJtItCs
- NPM Graph - https://npm.broofa.com/
- Renovate
  - https://docs.renovatebot.com/
  - https://www.whitesourcesoftware.com/free-developer-tools/renovate/on-premises
- Dependabot - https://docs.renovatebot.com/
- Snyk - https://snyk.io/