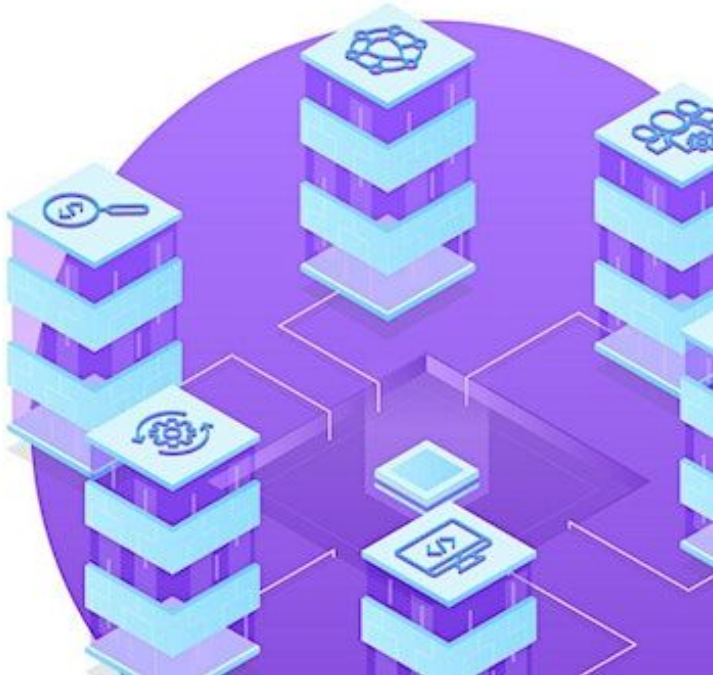
CSA | Netherlands Chapter

+

catawiki

DEVSECOPS

21/06 Amsterdam @Catawiki



Agenda

15:30 - 16:00 Walk-in/coffee
16:00 - 16:10 Opening
16:10 - 16:35 Aristide Bouix - CSA DevSecOps & Catawiki journey
16:35 - 17:00 Garima Agrawal - Microsoft DevSecOps experiences
17:00 – 17:05 Break
17:05 - 17:30 Sebastiaan van der Meer - Sustainability by well architecting workloads
17:30 - 17:55 Wouter van der Houven - Generative AI in DevSecOps
17:55 – 18:00 Wrap-up
18:00 - 19:00 Networking drinks and snacks

catawiki

CSA DevSecOps & Catawiki's journey

Aristide Bouix

21/06/2023

catawiki

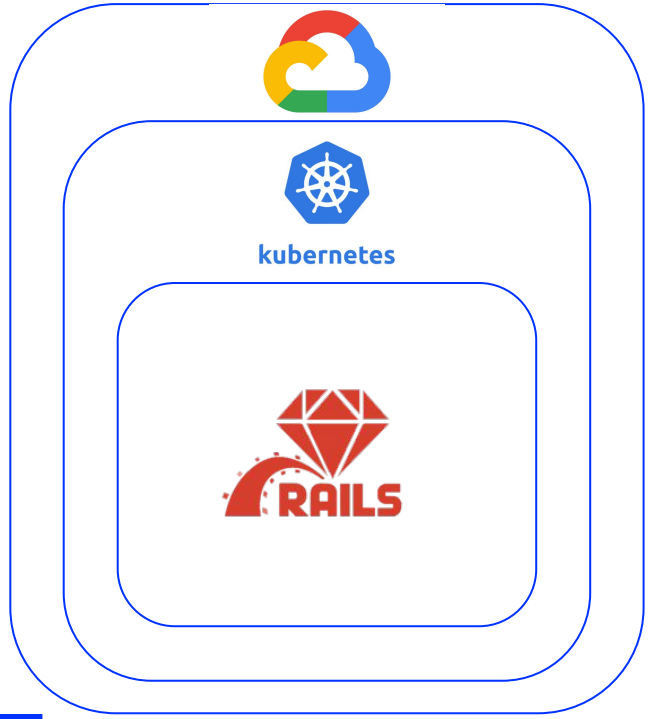
Agenda

1. About Me
2. About Catawiki
3. CSA Six Pillars of DevSecOps
4. Problems we're trying to solve
5. Selecting our security tooling
6. Pragmatic Implementation
7. Fostering adoption
8. Lessons learned

About Me

- 🔐 Lead Product Security @Catawiki
- 💡 Fmly Cloud & Cybersecurity consulting @KPMG Devoteam
- 🤓 SME on AWS Cloud and DevSecOps
- 🌤️ CSA Member and Contributor
- ⛳ Casual Golfer, 🖼️ Art Collector, 🍱 Korean Cuisine

About Catawiki



CSA Six Pillars of DevSecOps

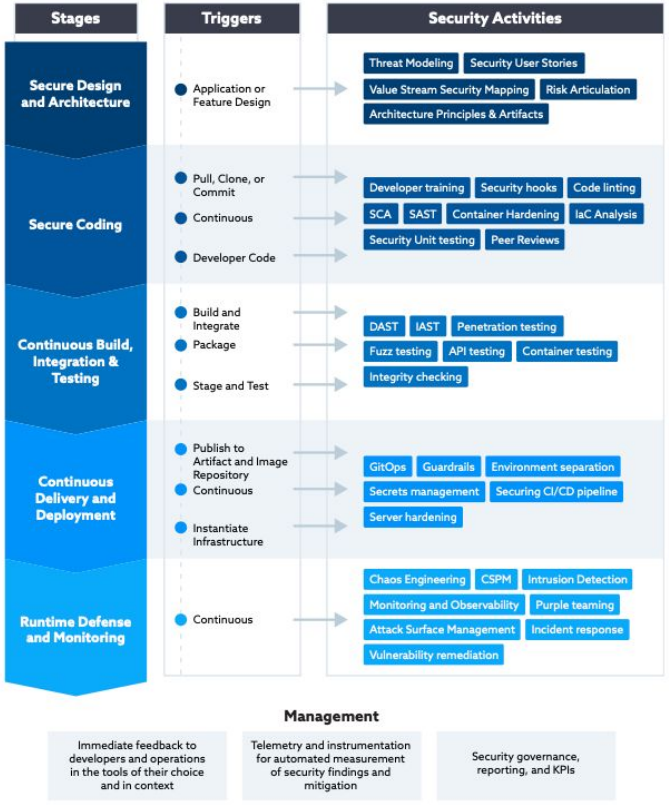


Figure 1: Secure Development Lifecycle

Problems we're trying to solve

Discovery

1. Are we running obsolete systems in production?
2. Are we running obsolete dependencies in production?
3. Is our infrastructure configuration secure?
4. Does our code itself contains vulnerabilities?

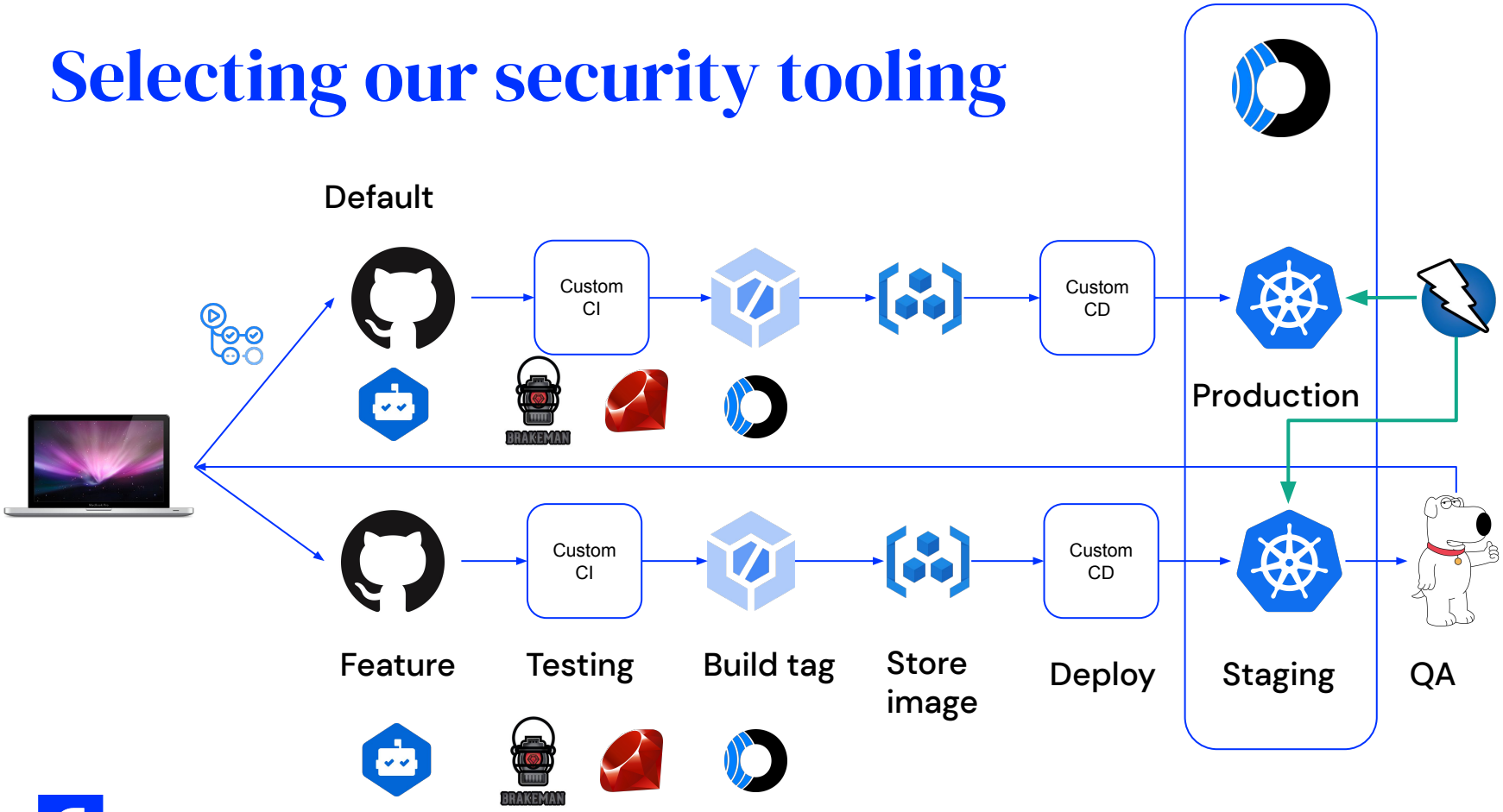
Prioritisation

1. What are our crown jewels? 👑
2. What sensitive data are we storing or processing?
3. Are vulnerabilities actually exploitable?

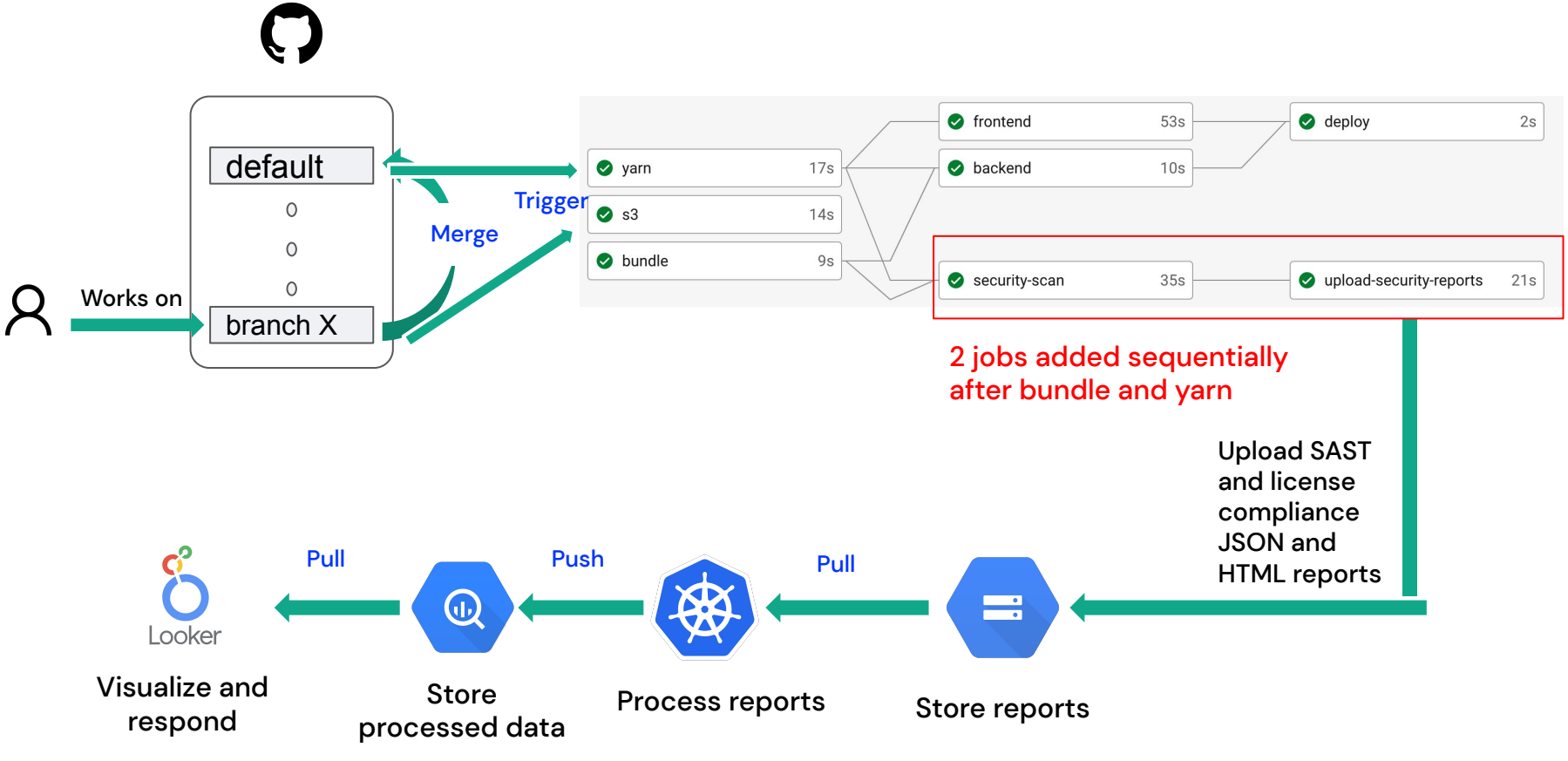
Remediation

1. Who should address vulnerabilities?
2. How promptly should vulnerabilities be addressed?
3. How to ensure they get addressed in time?

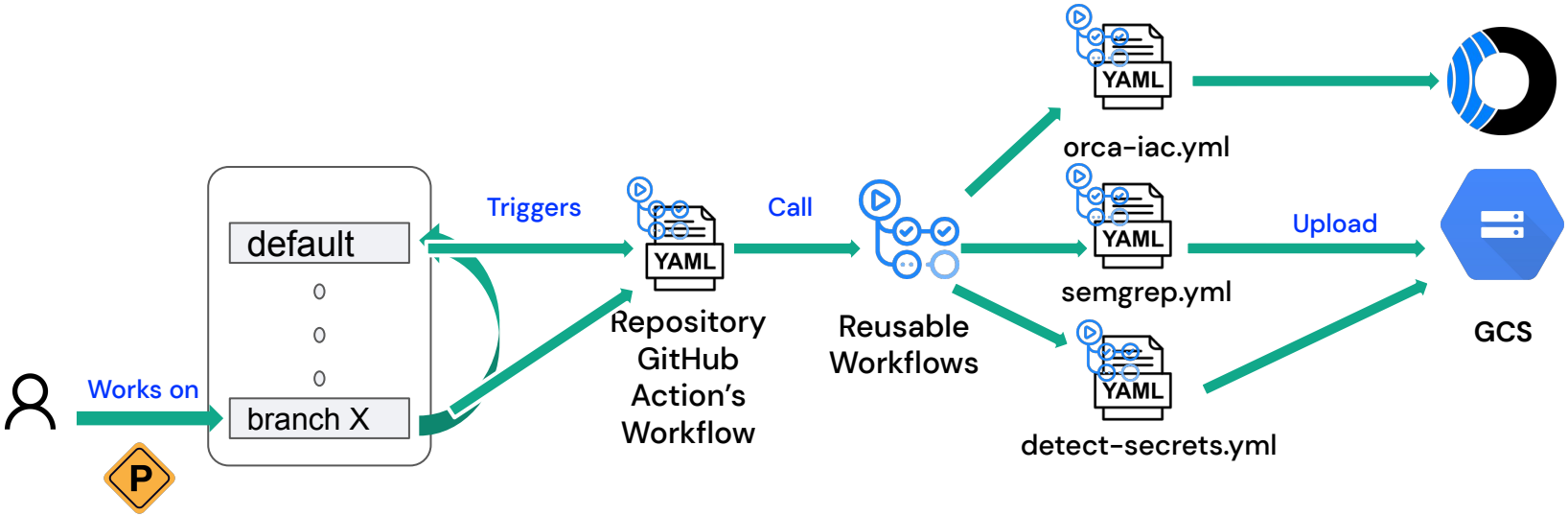
Selecting our security tooling



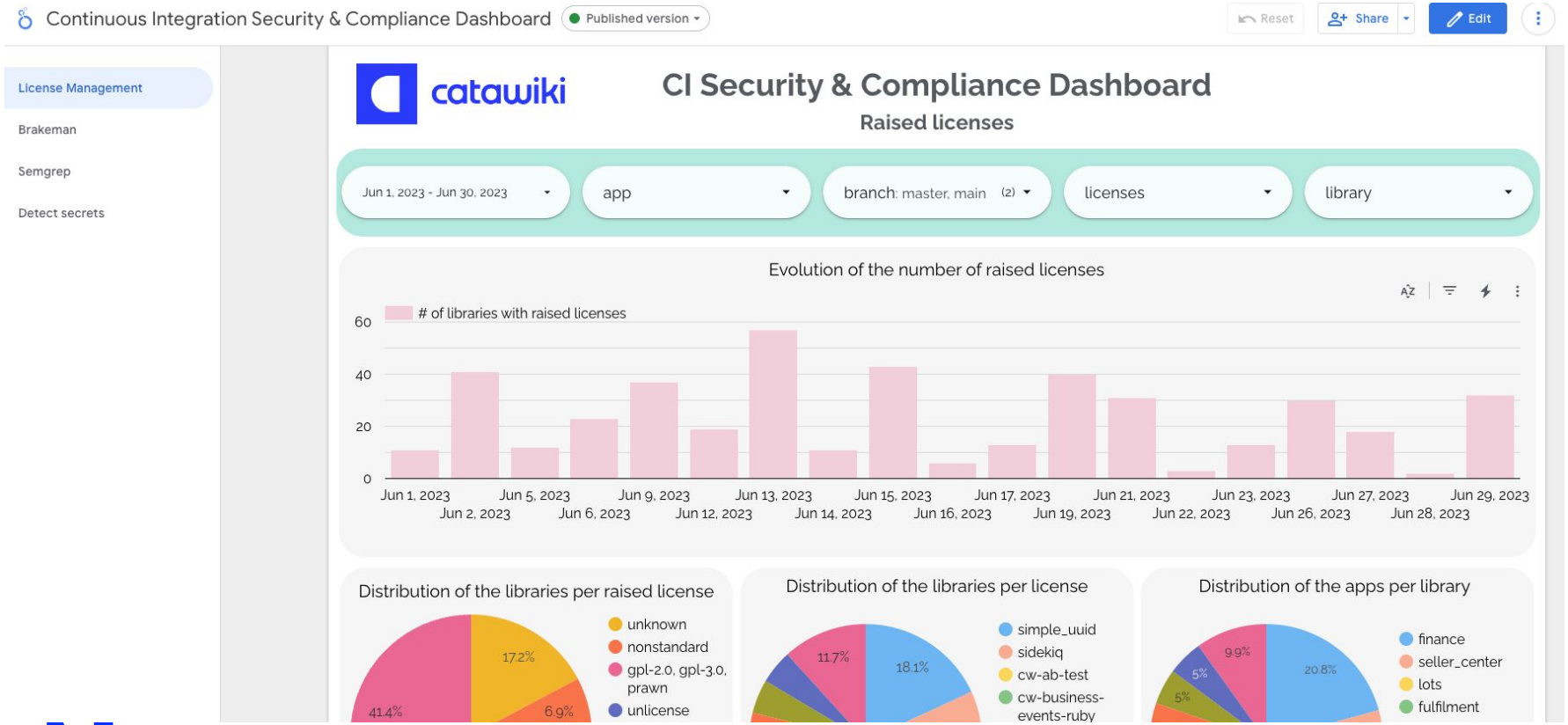
Pragmatic Implementation: Iteration I



Pragmatic Implementation: Iteration II



Pragmatic Implementation: Iteration II

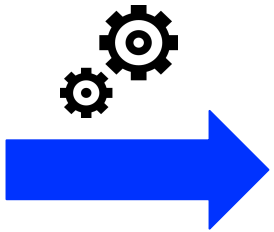


Fostering Adoption: Atlassian

RFC Space

New RFC

Semi-automated



Automated daily exports to Looker Studio

Twilio

Fostering Adoption: Gamifying

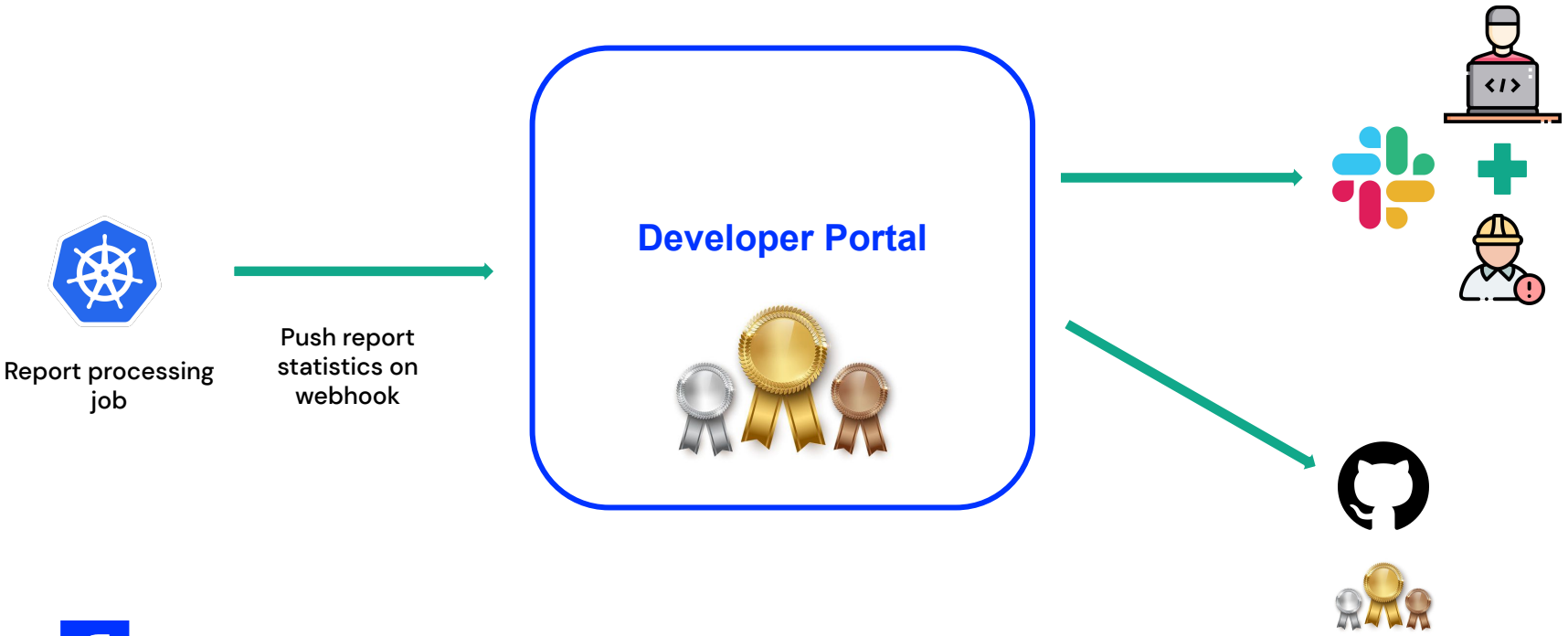
Security and Vulnerability Newsletters

Team and service security leadership board and perks

Developer L&D trainings

Advanced workshops for security champions

Fostering Adoption: Service badges



7 Lessons Learned

1. Not all teams are equals
2. Drifts are acceptable
3. Dependabot doesn't fetch private npm packages properly
4. Dependency confusion is still a thing
5. No vendor supports Ruby  out of the box
6. No one knows how to secure mobile apps
7. **Bug Bounties are more efficient than Pentests**

Thank You!

Aristide Bouix
Product Security Engineer

a.bouix@catawiki.nl
linkedin.com/in/aristide-bouix
@ArisvdZ
@ArisBee
@arisbcollection