SECRETS OF DEVELOPER PRODUCTIVITY

CODE ANALYSIS AT THE TECH GIANTS

Stephen Magill | CEO, MuseDev

CONTINUOUS

CONTINUOUS INTEGRATION

CONTINUOUS DEPLOYMENT

CONTINUOUS ASSURANCE

CONTINUOUS ASSURANCE

QUALITY

SECURITY

COMPLIANCE

THREE STORIES

GOOGLE

FACEBOOK

NIST

Experiments with Static Analysis
2006 - 2011

PAIN POINTS | AT GOOGLE SCALE

One Week of "Batch Mode"

Hundreds of Google Engineers worked through 3,954 issues in one week.

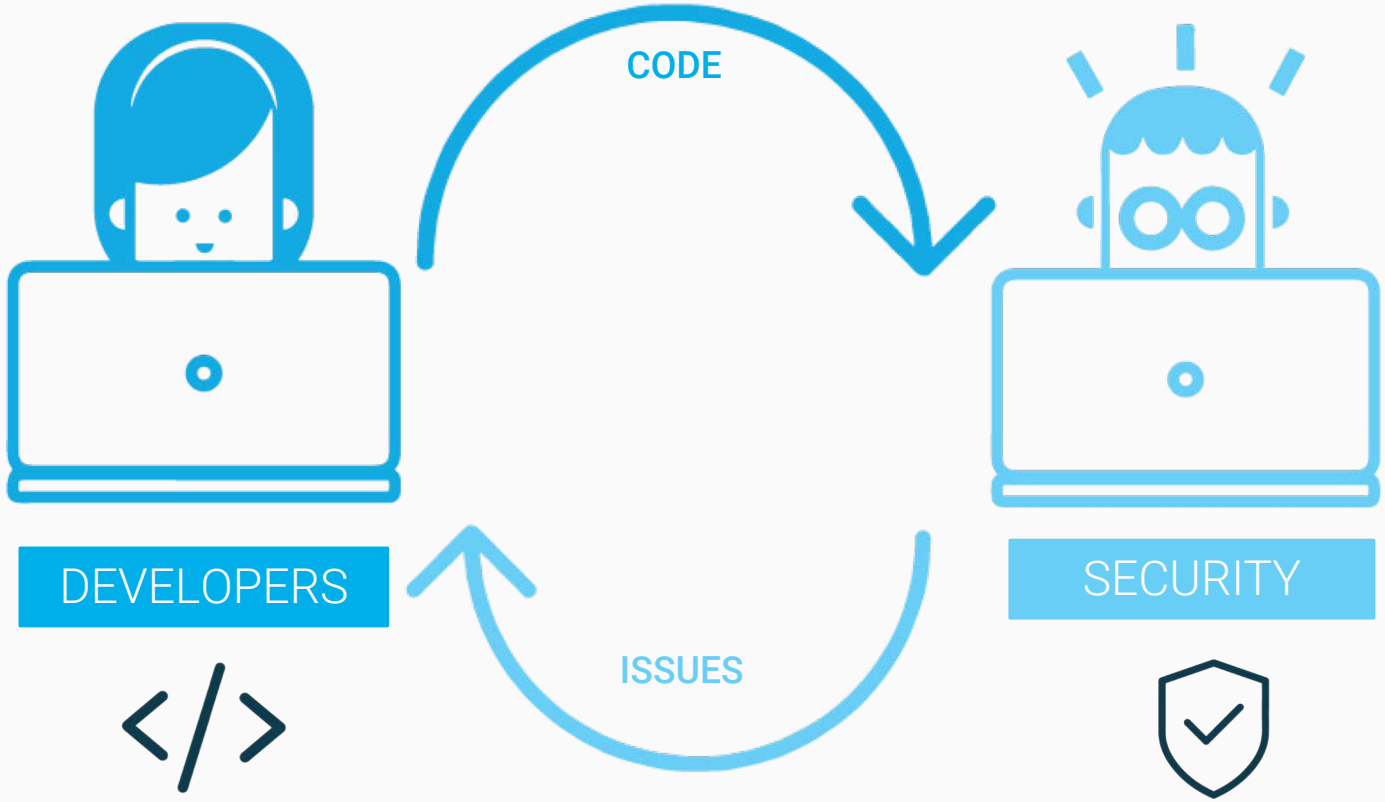
Only 16% of those issues were fixed. Another 5,519 were never examined.

SCALE IS MASSIVE

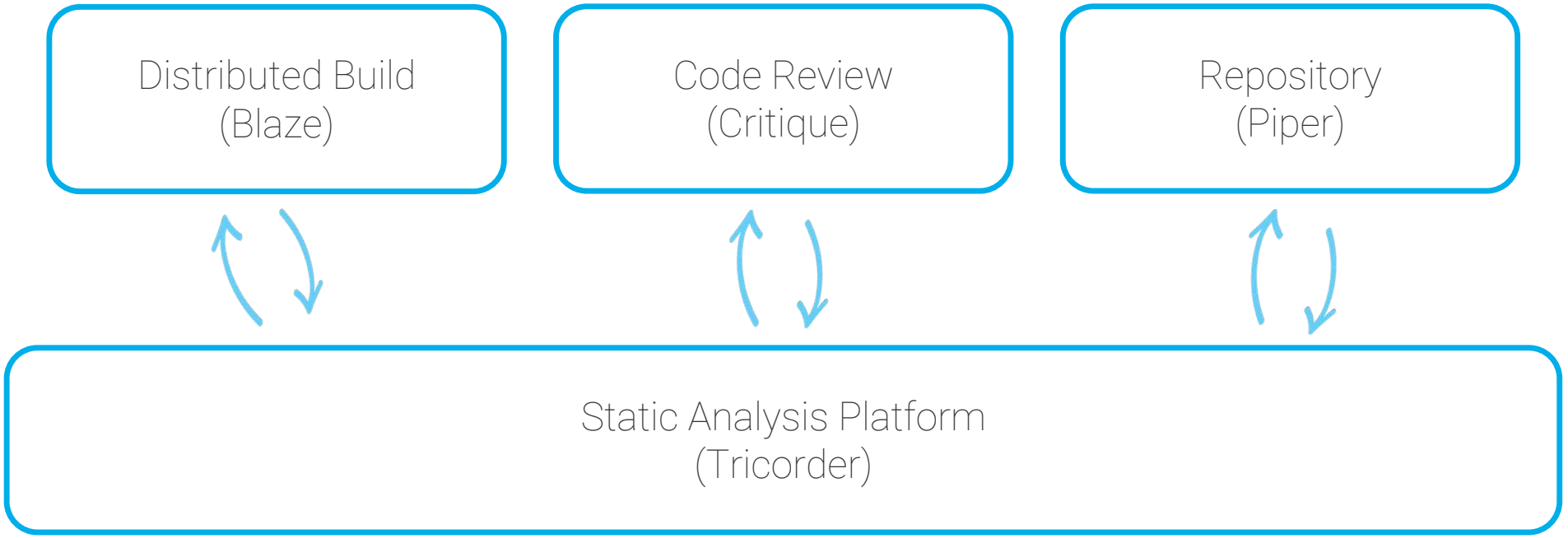
Google has 2 Billion+ lines of code and 16,000 changes per day.

BATCHED PROCESS IS EXPENSIVE

BATCH MODE | THE BACK & FORTH

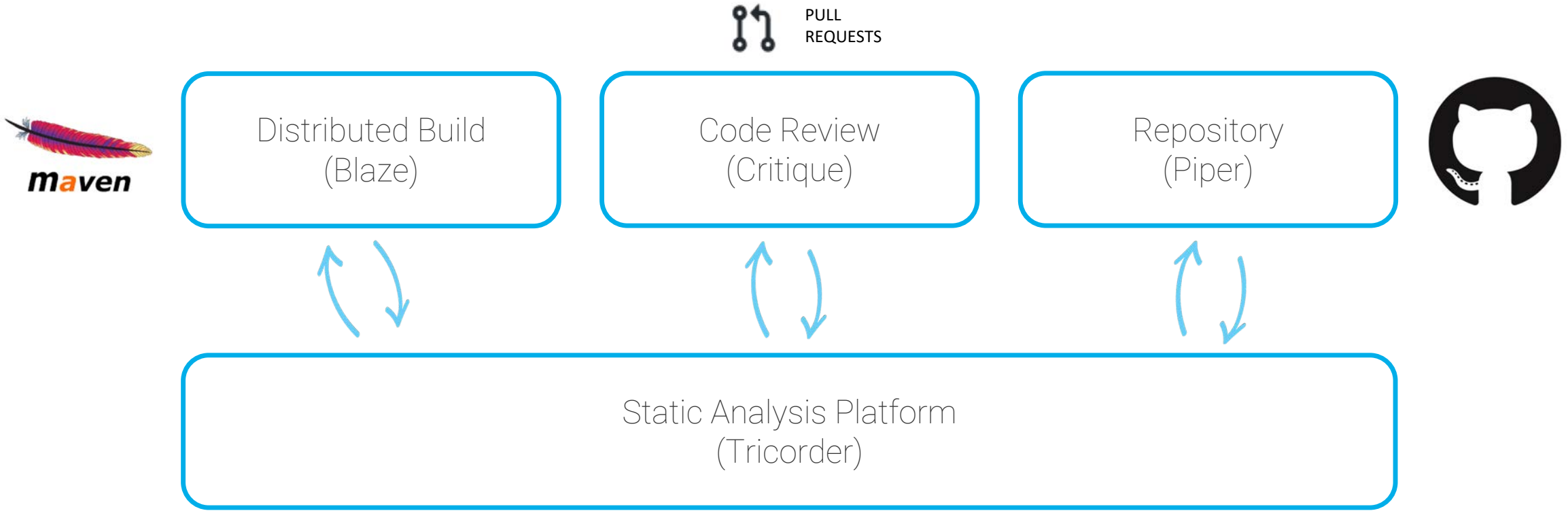


TRICORDER| ANALYSIS AT SCALE



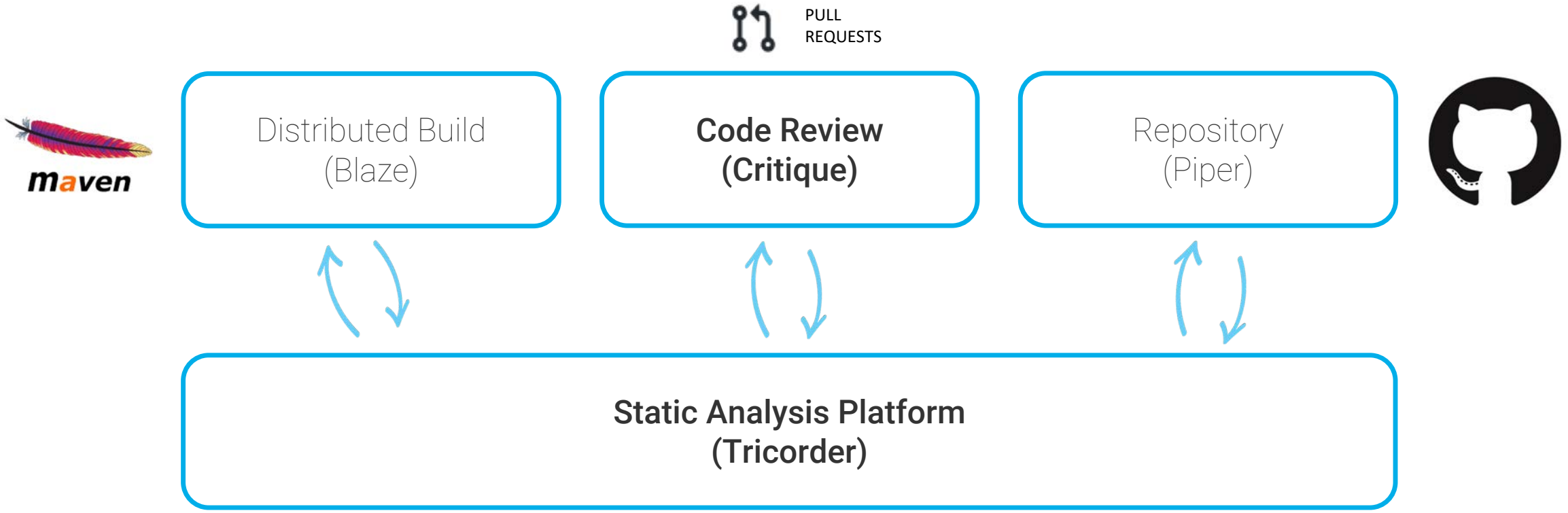
Sadowski, Caitlin, et al. "Tricorder: Building a program analysis ecosystem." Proceedings of the 37th International Conference on Software Engineering-Volume 1. IEEE Press, 2015.

TRICORDER| ANALYSIS AT SCALE



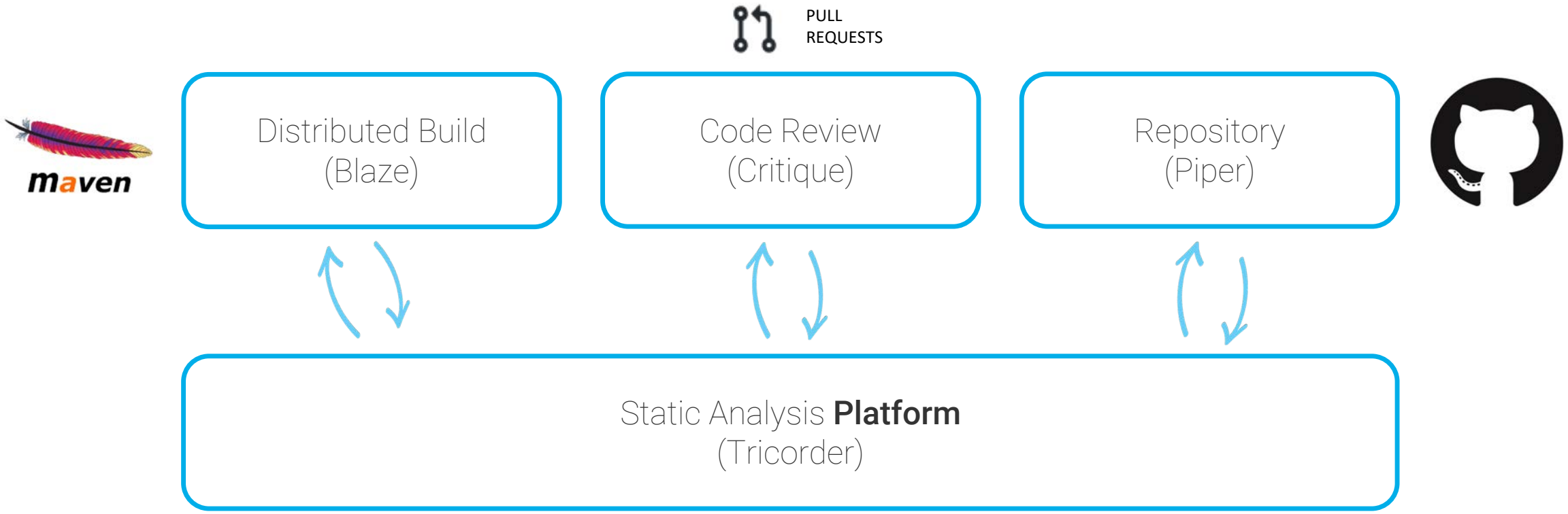
Sadowski, Caitlin, et al. "Tricorder: Building a program analysis ecosystem." Proceedings of the 37th International Conference on Software Engineering-Volume 1. IEEE Press, 2015.

TRICORDER| ANALYSIS AT SCALE



Sadowski, Caitlin, et al. "Tricorder: Building a program analysis ecosystem." Proceedings of the 37th International Conference on Software Engineering-Volume 1. IEEE Press, 2015.

TRICORDER| ANALYSIS AT SCALE



Sadowski, Caitlin, et al. "Tricorder: Building a program analysis ecosystem." Proceedings of the 37th International Conference on Software Engineering-Volume 1. IEEE Press, 2015.

INTEGRATION IS KEY

“As of January 2018, Tricorder had analyzed approximately 50,000 code review changes per day.” More than 5,000 code review reports per day are deemed useful with only 250 flagged as “not useful”.

“As of January 2018, Tricorder included 146 analyzers, with 125 contributed from outside the Tricorder team”

“new checks are biased toward those that save developer time”

Sadowski, Caitlin, et al. *"Lessons from Building Static Analysis Tools at Google."* Communications of the ACM 61.4: 58-66.

DEPLOYING NEW STATIC ANALYSIS TOOLS

ANOTHER FAILED EXPERIMENT

- Infer tool deployed in “Batch Mode”
- Even with issue triage and manual assigning of devs to issues:
  - Near 0% fix rate
- ROFL Assumption: “All an analysis needs to do is Report Only a Failure List (ROFL), with low false positives, in order to be effective”
  - Report real bugs
  - Just focus on bugs
- “Bug dashboards are not the answer”

INTEGRATION IS KEY

Fix rate for reports went from almost 0% to 70% following code review integration.

Peter W. O'Hearn. 2018. Continuous Reasoning: Scaling the impact of formal methods. Symposium on Logic in Computer Science (LICS '18).

Zoncolan flagged 46 percent of issues to code authors directly without the involvement of a security engineer; this typically also takes place before the code is landed.

Francesco Logozzo, Manuel Fahndrich, Ibrahim Mosaad, Pieter Hooimeijer. Zoncolan: How Facebook uses static analysis to detect and prevent security issues, Facebook Blog, 2019.

> "The same program analysis, with same false positive rate, had much greater impact when deployed at diff time."

TRANSFORMING CERTIFICATION

NIST FIPS 140-2

- Lengthy external review process
- Slows deployment velocity
  - Including deployment of security patches
- Automated Cryptographic Validation Protocol (ACVP)
  - New approach to certifying crypto
  - Supports collecting evidence directly from DevOps tooling
  - Supports self-certification workflow
  - Soon to be the only supported validation method

NIST AUTOMATED GOVERNANCE

- Collecting certification evidence directly from DevOps tooling
- Continuous assurance via automated
  - Code Analysis
  - Container Scanning
  - Software Composition Analysis
- Instead of manual auditing of the product, manually audit the process.

Michael Nygard, Tapabrata Pal, Stephen Magill, Sam Guckenheimer, John Willis, John Rzeszotarski, Dwayne Holmes, Courtney Kissler, Dan Beauregard, Collette Tauscher

AUTOMATION IS PUSHING INTO SECURITY AND COMPLIANCE
WORKFLOWS ENABLING

CONTINUOUS ASSURANCE

TRANSFORMATION EMERGING

AUTOMATION AND INTEGRATION BY PERFORMANCE PROFILE

	Low	Medium	High	Elite
Automated build	64%	81%	91%	92%
Automated unit tests	57%	66%	84%	87%
Automated acceptance tests	28%	38%	48%	58%
Automated performance tests	18%	23%	18%	28%
Automated security tests	15%	28%	25%	31%
Automated provisioning and deployment to testing environments	39%	54%	68%	72%
Automated deployment to production	17%	38%	60%	69%
Integration with chatbots / Slack	29%	33%	24%	69%
Integration with production monitoring and observability tools	13%	23%	41%	57%
None of the above	9%	14%	5%	4%

> “Low performers take weeks to conduct security reviews and complete the changes identified. In contrast, elite performers build security in and can conduct security reviews and complete changes in just days.”

Forsgren, Nicole, et al. "2019 Accelerate State of DevOps Report."

WORKING TOGETHER

ON CONTINUOUS ASSURANCE

- ACTION| How we get started
- IMPACT | How this affects the DOES community
- INVOLVEMENT | Sharing & Collaboration

THANK YOU

Stephen Magill | CEO, MuseDev

@stephenmagill

MuseDev

http://does.muse.dev/