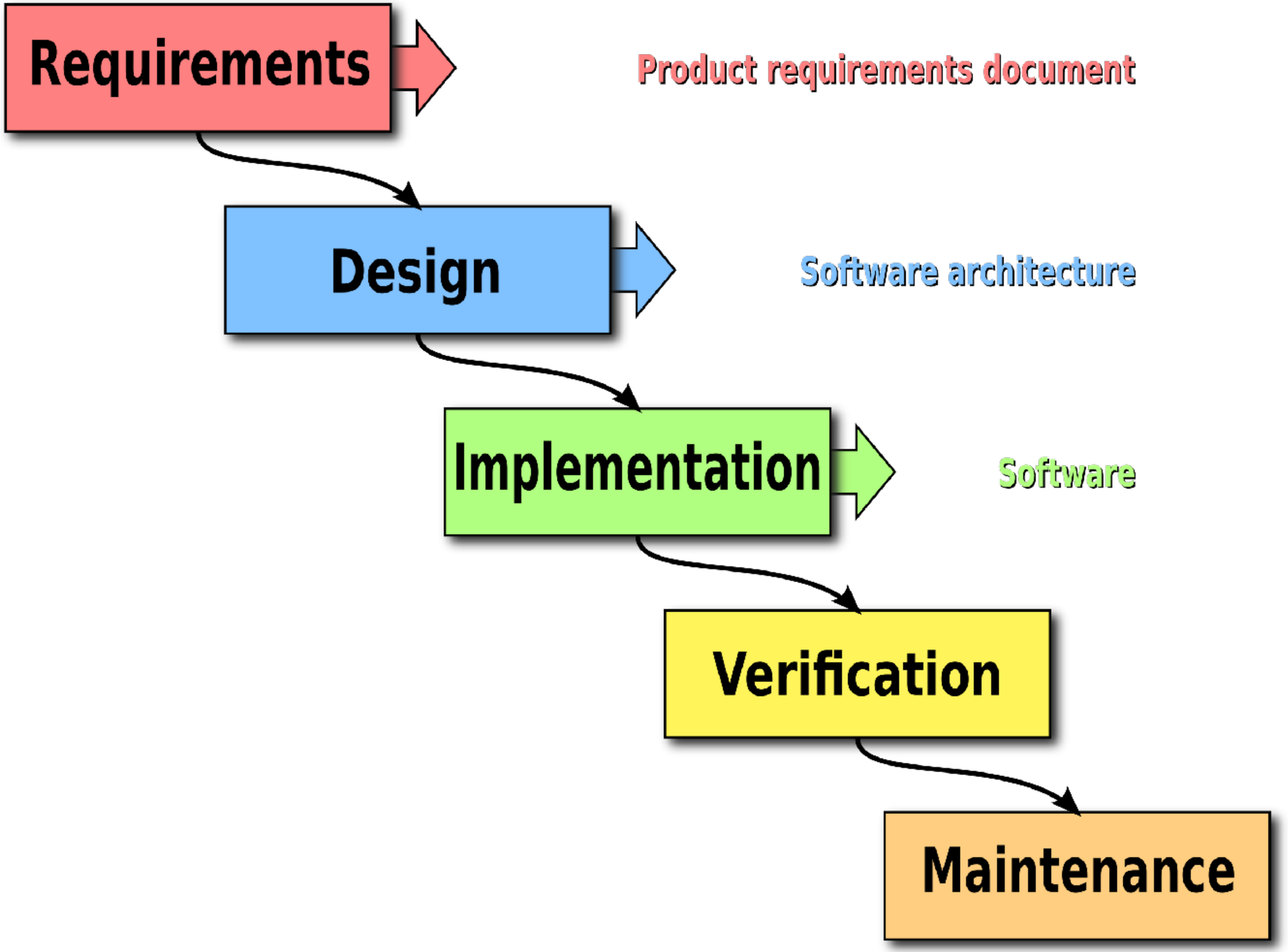
BUILD BREAKERS!

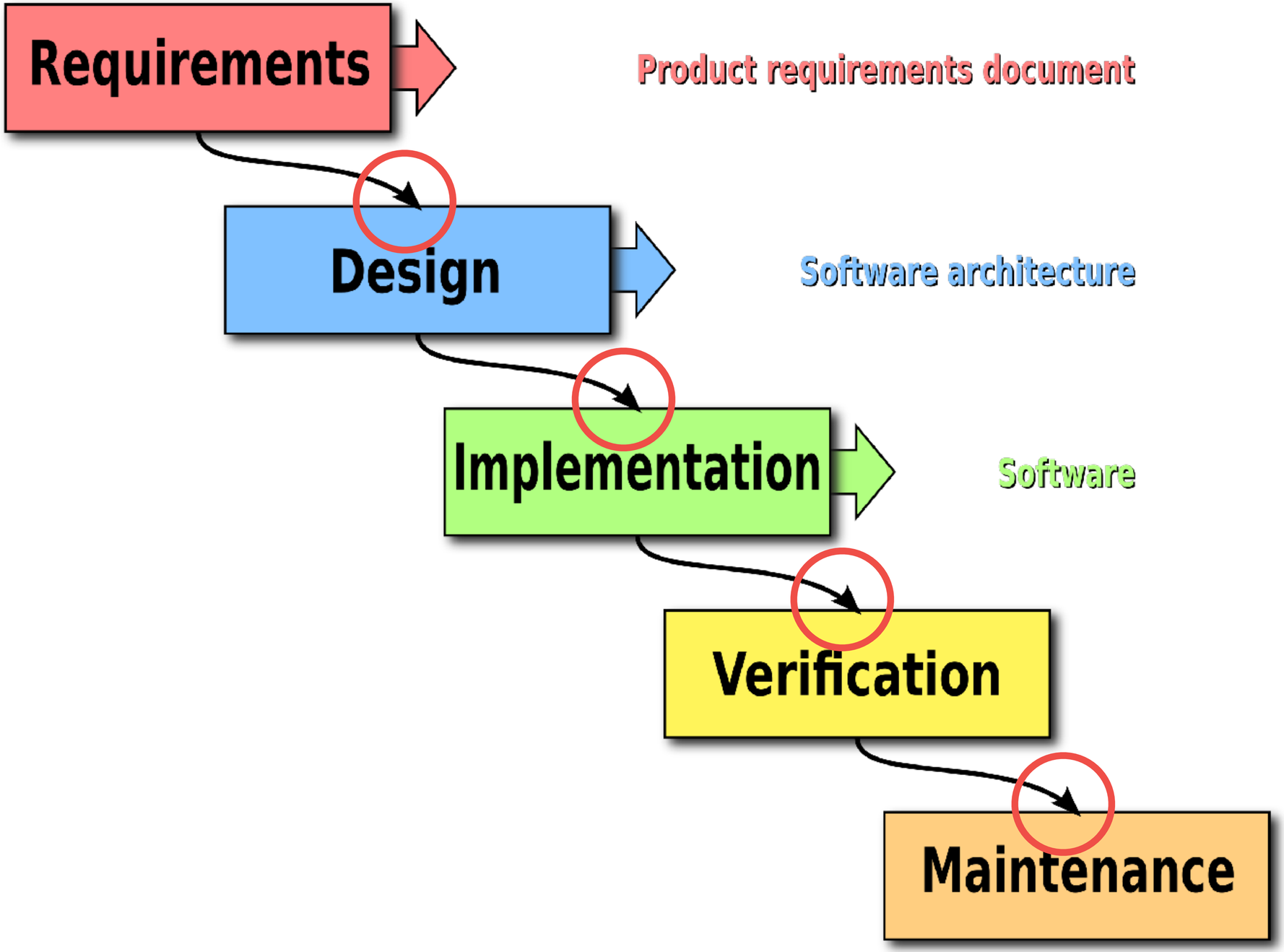
NOT GATEKEEPERS

MICHIEL ROOK
@MICHIELTCS

TRADITIONAL SOFTWARE DEV


Requirements
Product requirements document
Design
Software architecture
Implementation
Software
Verification
Maintenance

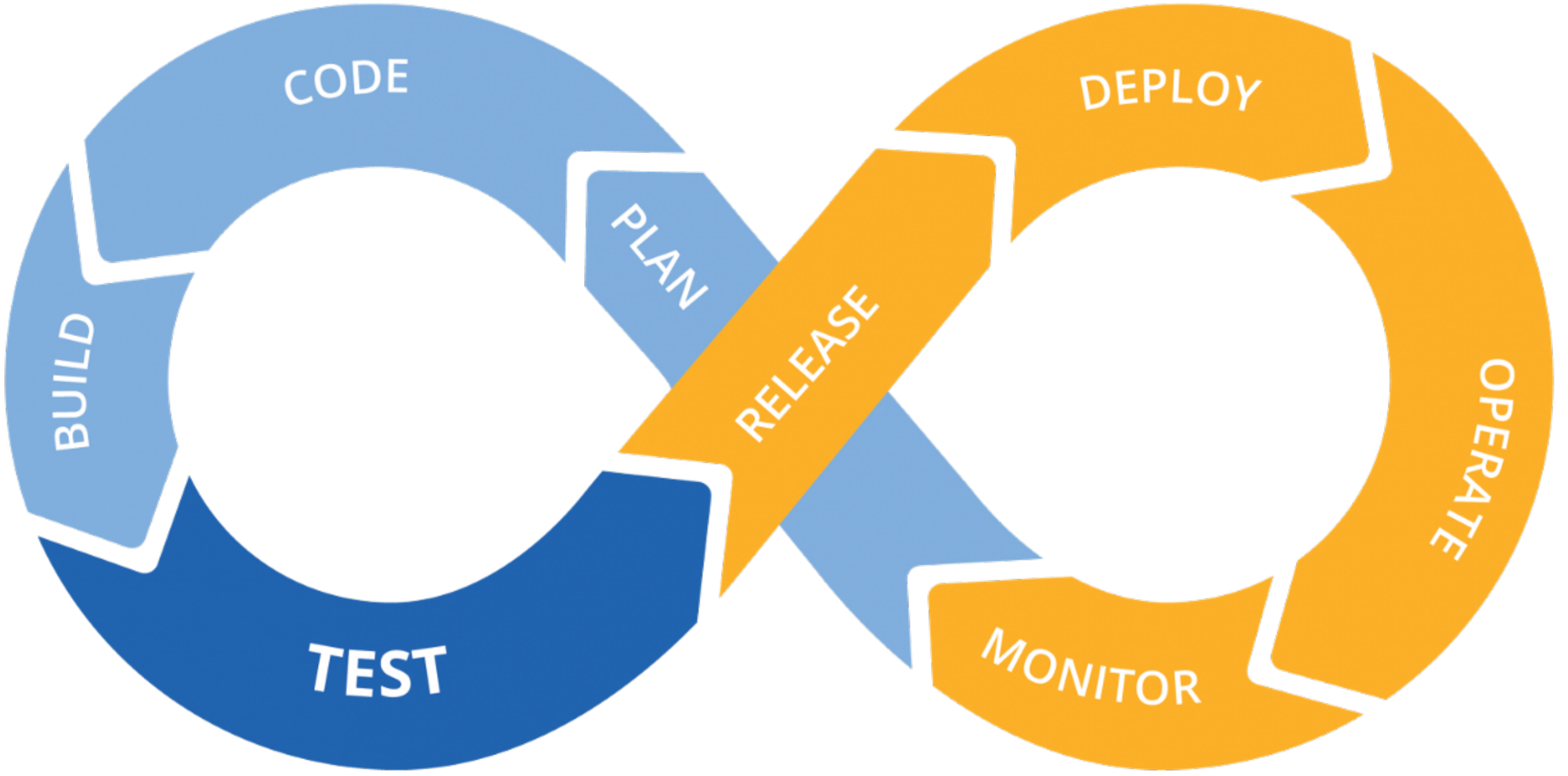

HUMAN GATEKEEPERS


Requirements
Product requirements document
Design
Software architecture
Implementation
Software
Verification
Maintenance

COSTLY

SLOW

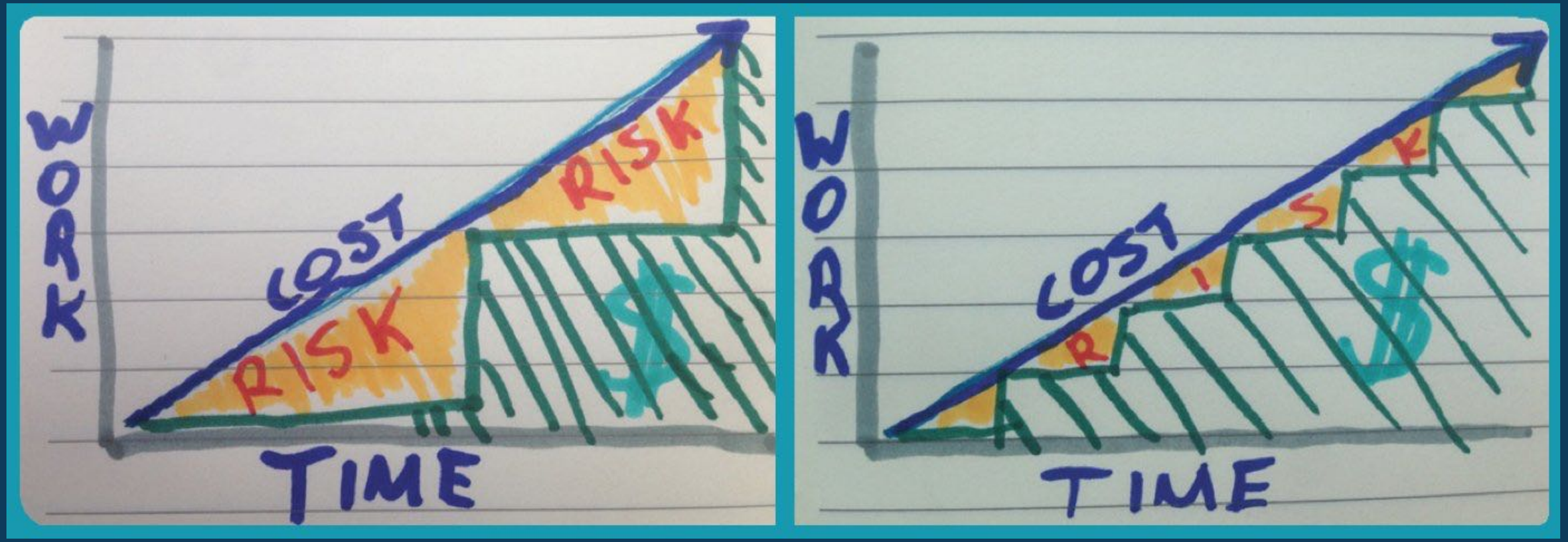
WASTEFUL


CODE
PLAN
BUILD
TEST
RELEASE
DEPLOY
OPERATE
MONITOR

CONTINUOUS & MANY SMALL CHANGES

INTEGRATE
QUICKLY & OFTEN

THIS WILL REDUCE RISK

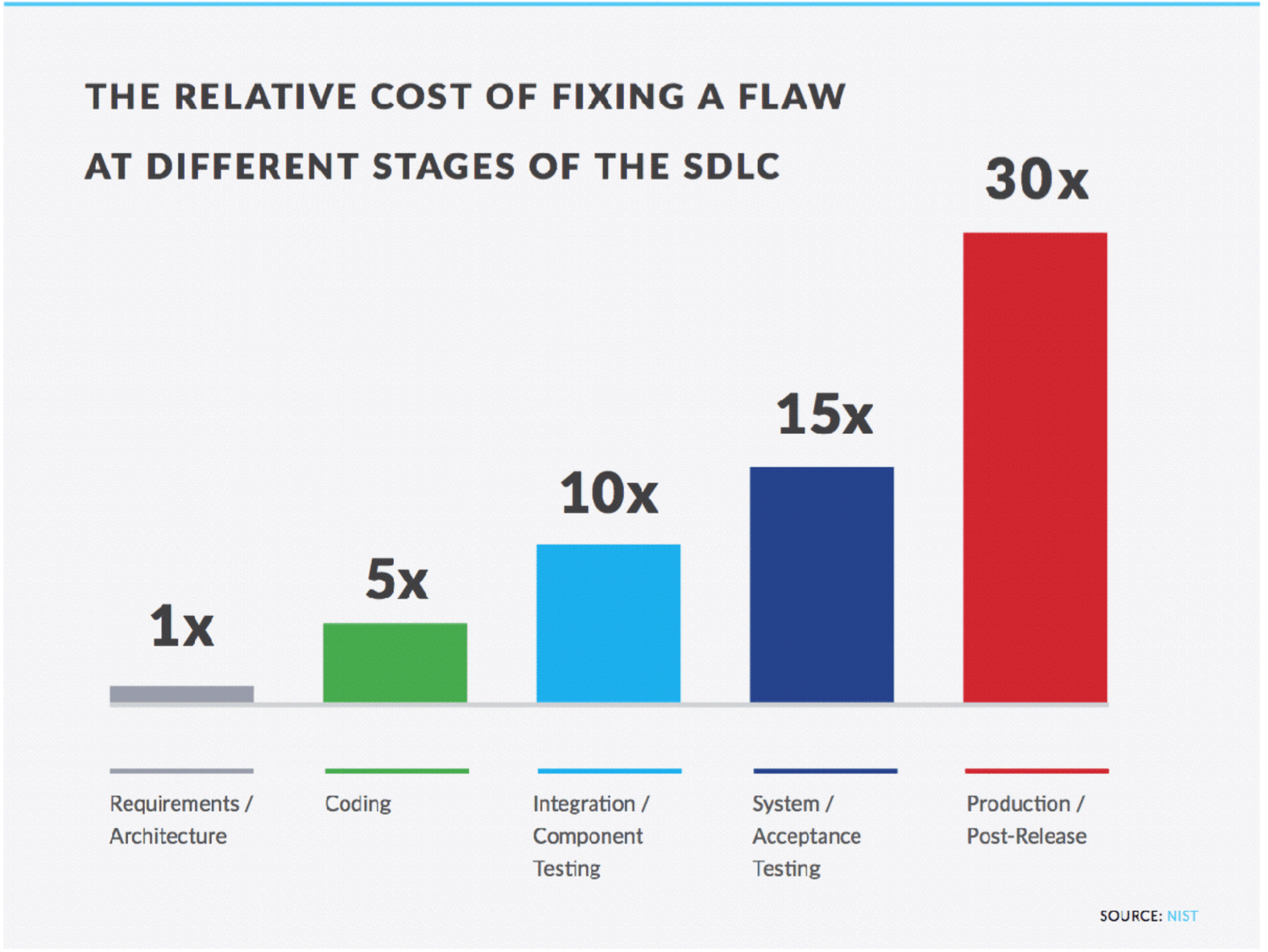


$ = REALIZED VALUE

CREDITS TO @FGOULDING

SHIFT LEFT

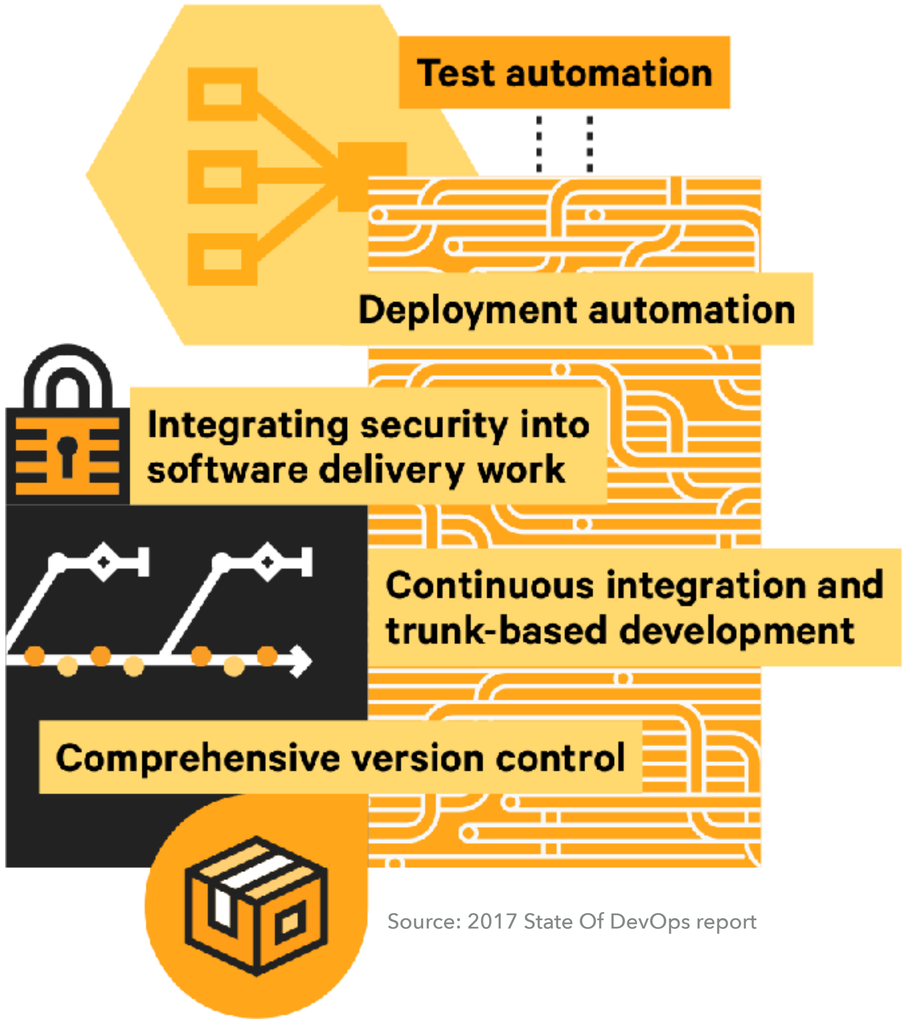
ELIMINATE ISSUES EARLY


THE RELATIVE COST OF FIXING A FLAW
AT DIFFERENT STAGES OF THE SDLC
1x
5x
10x
15x
30x
Requirements / Architecture
Coding
Integration / Component Testing
System / Acceptance Testing
Production / Post-Release
SOURCE: NIST

HOW?

AUTOMATION

Factors that positively contribute to continuous delivery:



Source: 2017 State Of DevOps report

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%

Source: 2019 State Of DevOps report

BUILD BREAKERS

AUTOMATED QUALITY GATES

FAIL

WARN

PASS

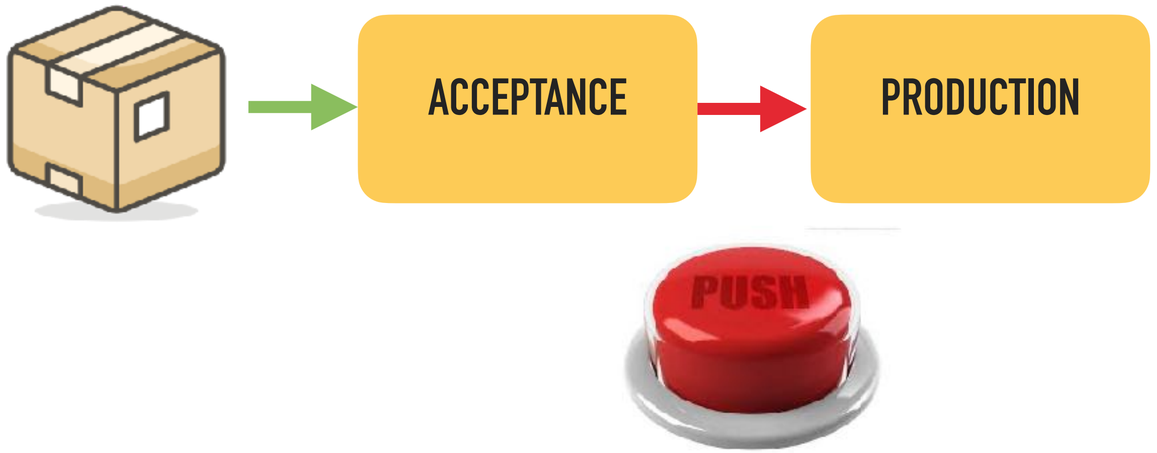
FAIL WARN PASS

PIPELINES

CONTINUOUS INTEGRATION

CONTINUOUS DELIVERY

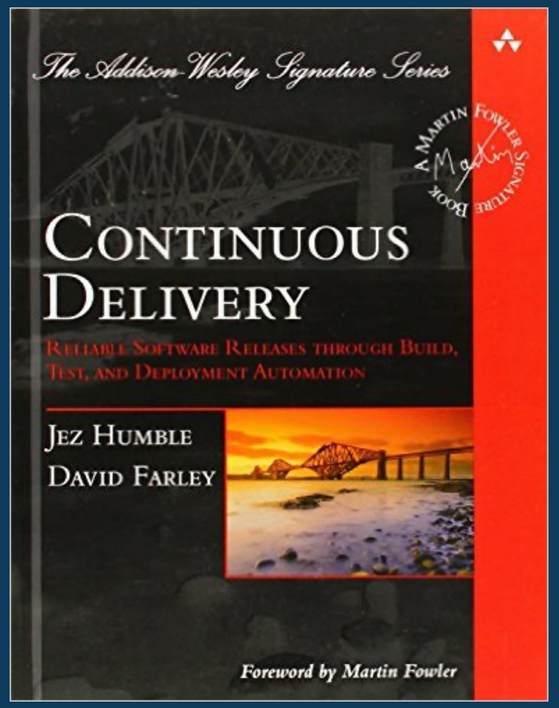
CONTINUOUS DELIVERY



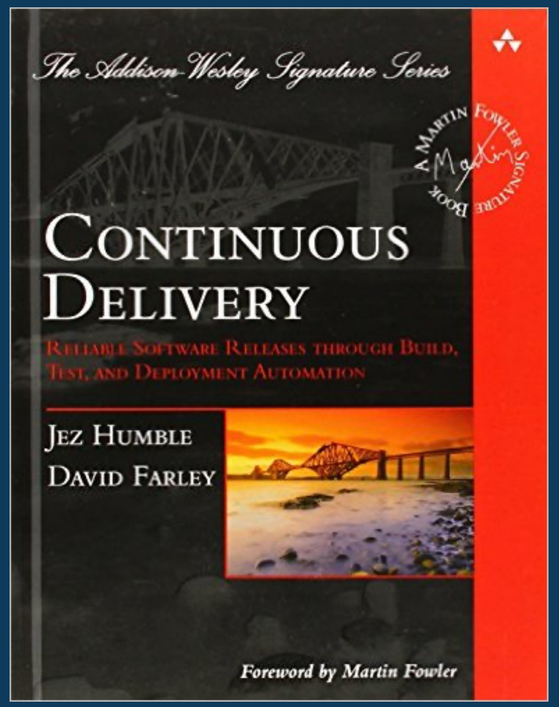
CODE IS ALWAYS IN A RELEASABLE STATE

CONTINUOUS DEPLOYMENT

EVERY VALID COMMIT GOES TO PRODUCTION

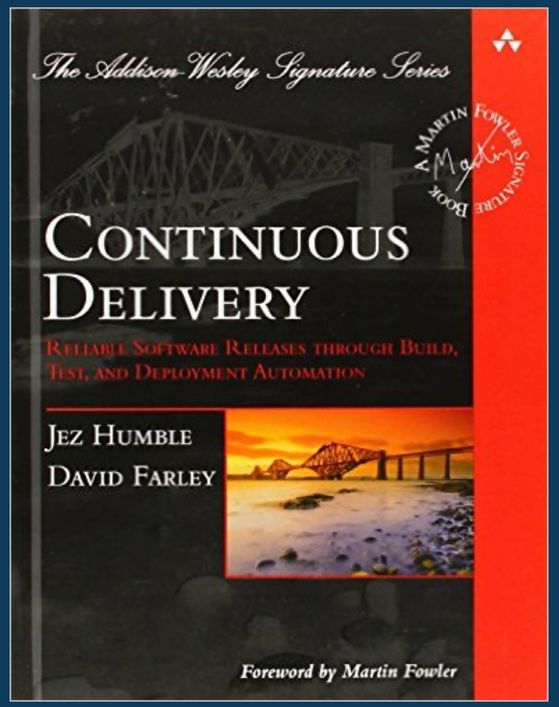


DELIVERING VALUE TO USERS



SAFELY & QUICKLY

@michieltcs

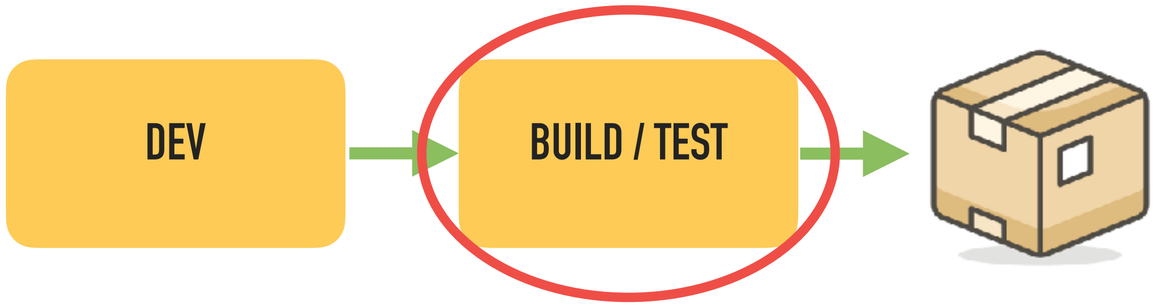


IN A SUSTAINABLE WAY

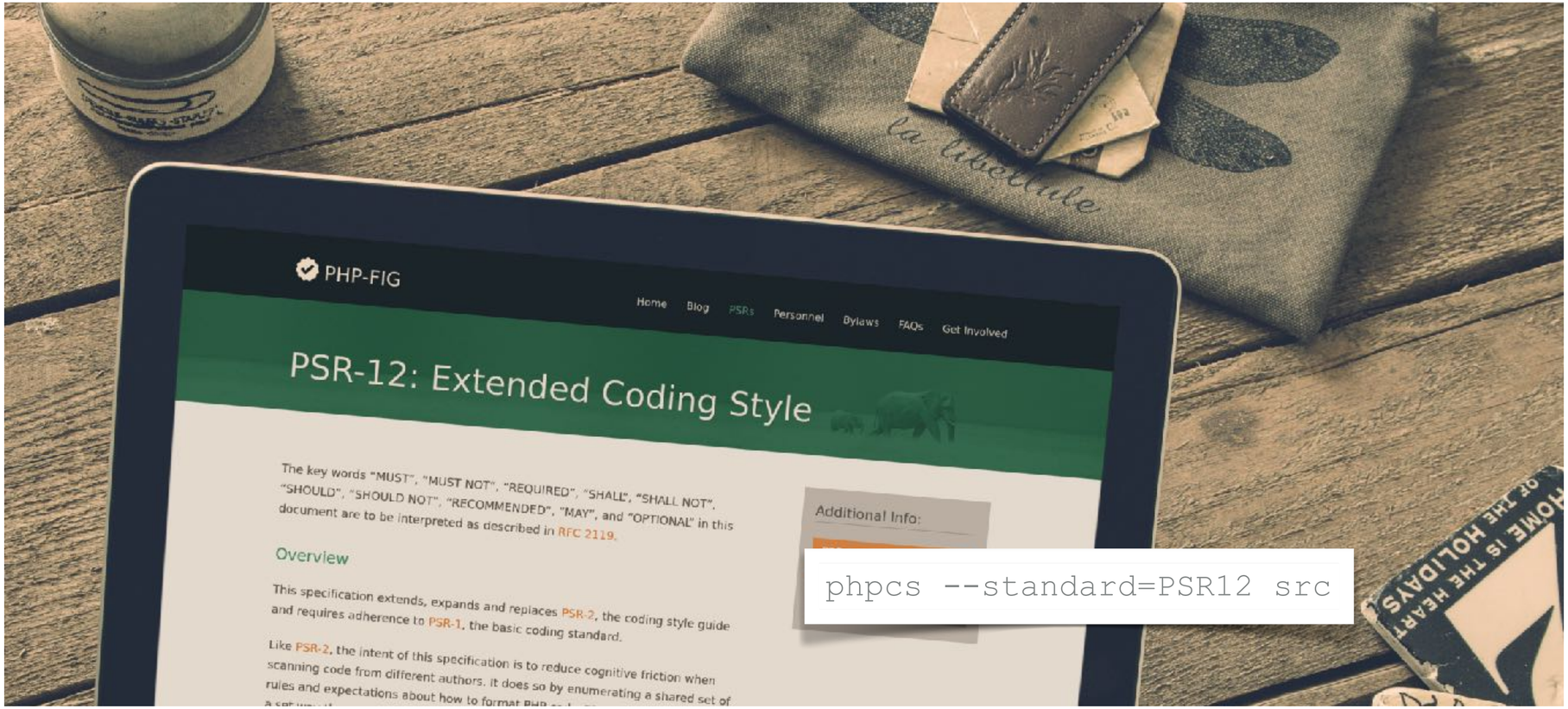
TIME TO ZOOM IN

"VERIFICATION" STAGE

CONTINUOUS INTEGRATION



CODE QUALITY & STANDARDS



CODE STYLE

(PHPCS, Checkstyle)

Modules/Appsflyer/Data/EventEntity.php [ReferralTracking]

Line: 94

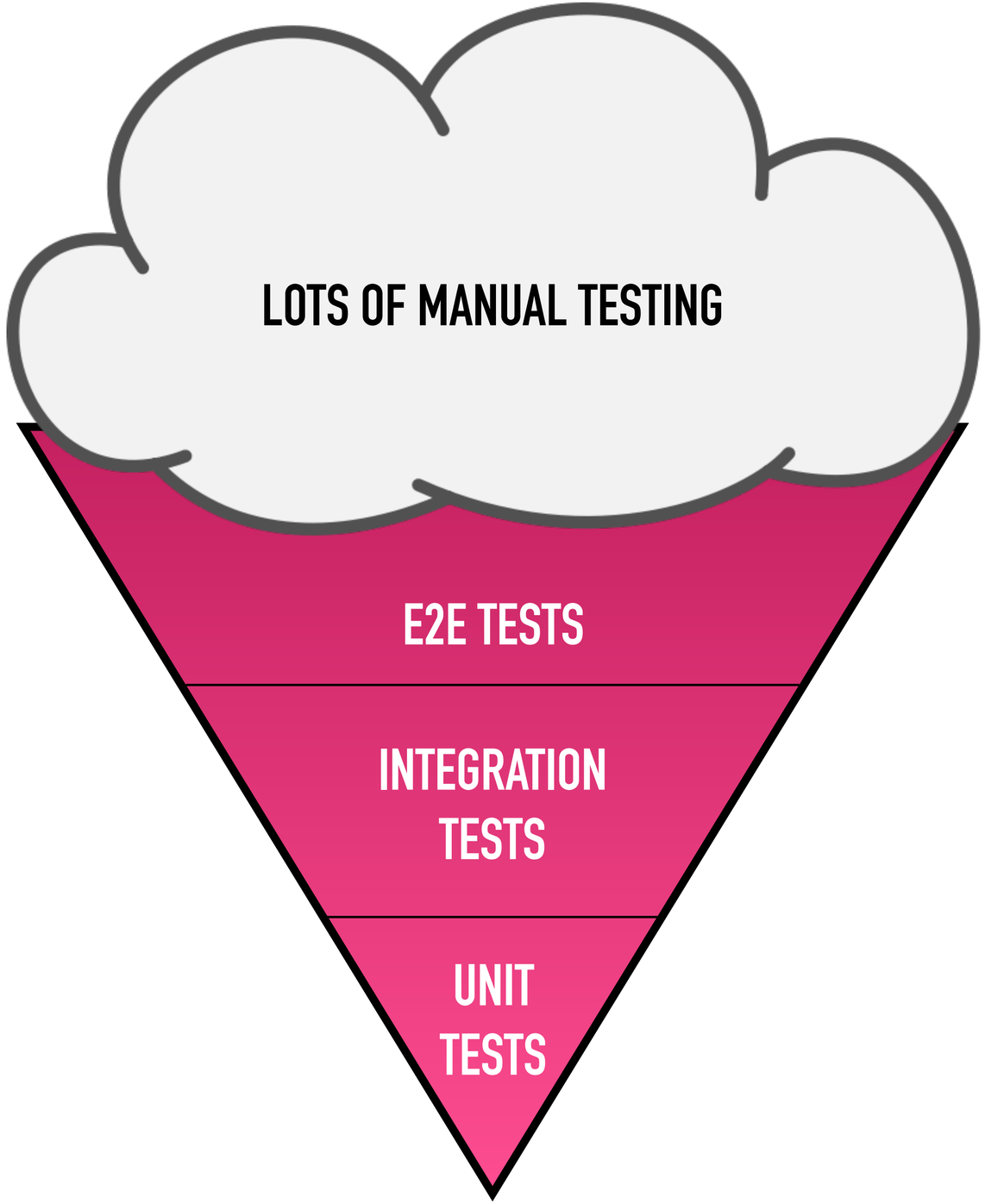
```
return $this->ut;
```

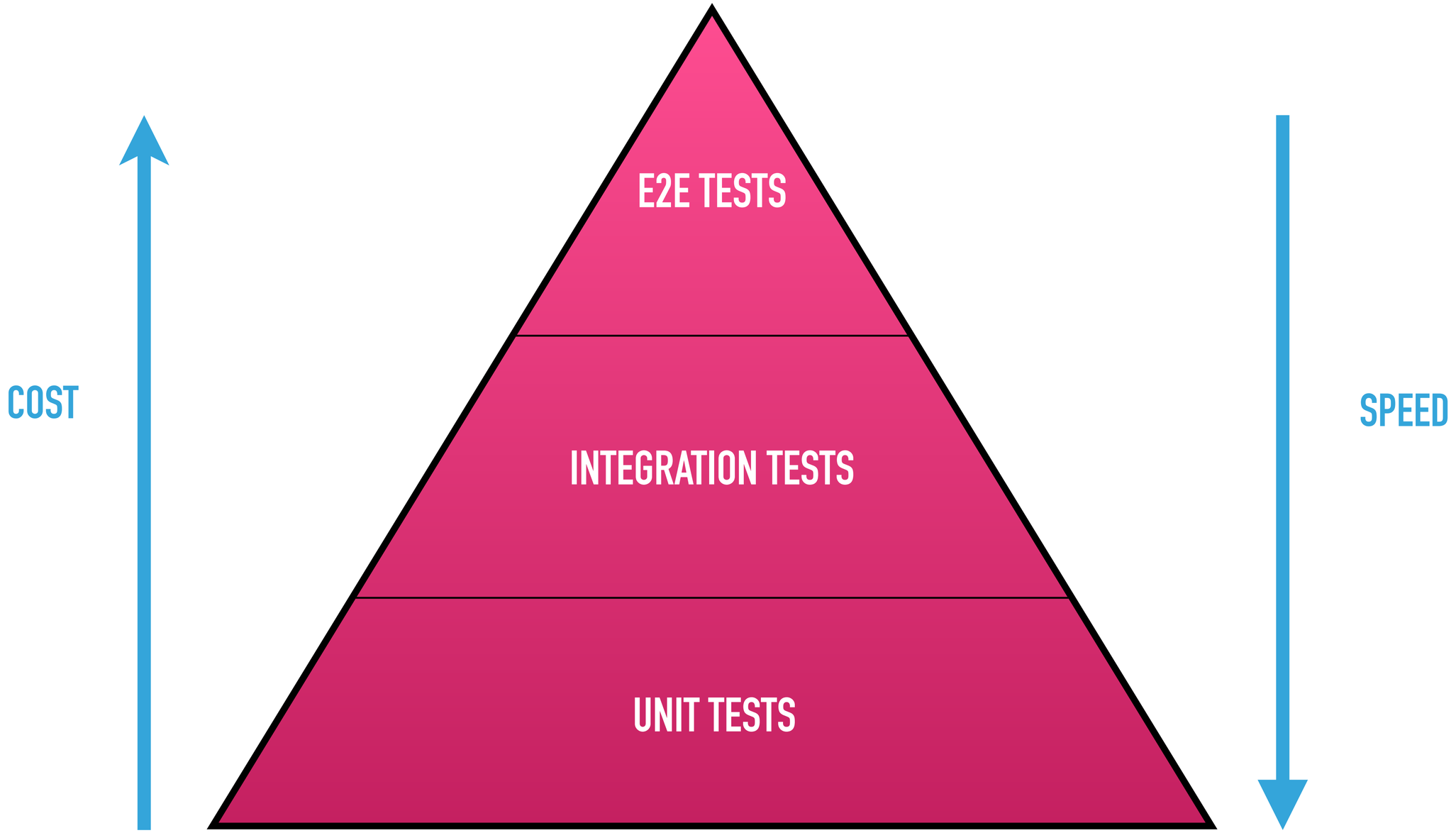
1. Phan TypeError PhanPossiblyNullTypeReturn Returning type int|null but getUt() is declared to return int (null is incompatible)
2. Phpstan Method Modules\Appsflyer\Data\EventEntity::getUt() should return int but returns int|null.
3. Psalm The declared return type 'int' for Modules\Appsflyer\Data\EventEntity::getUt is not nullable, but the function returns 'int|null'

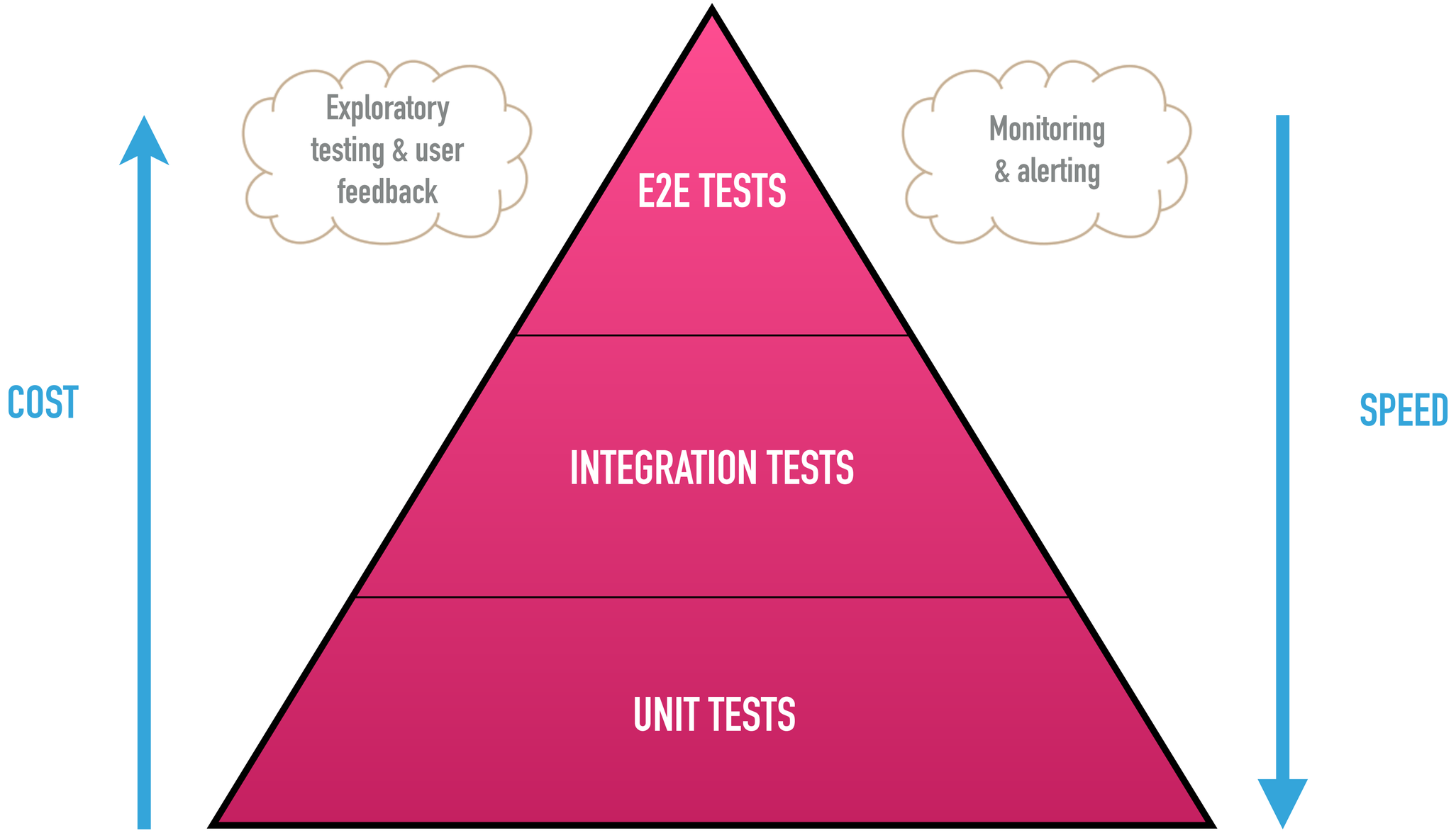
STATIC ANALYSIS

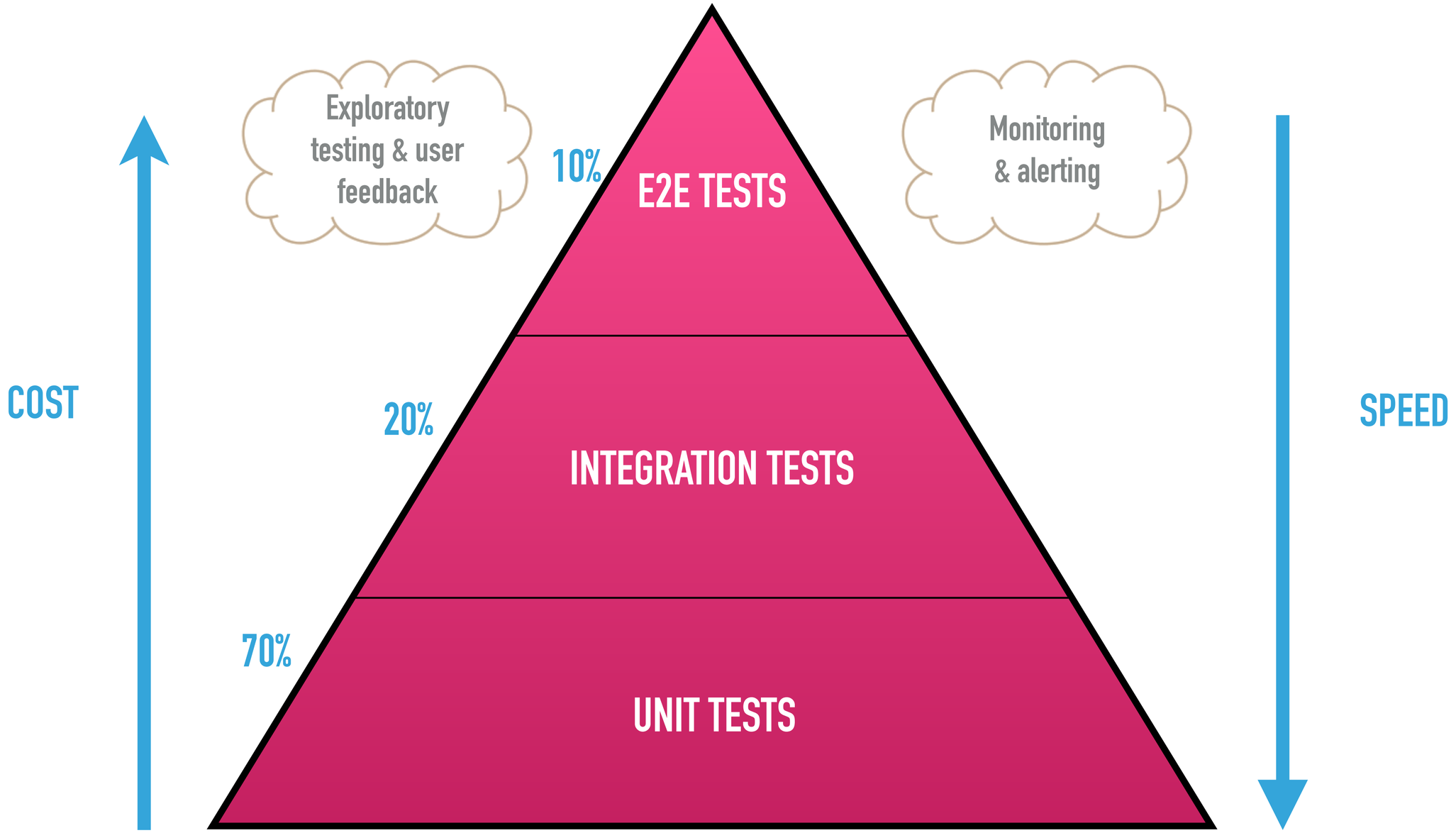
(Findbugs, PHPStan)

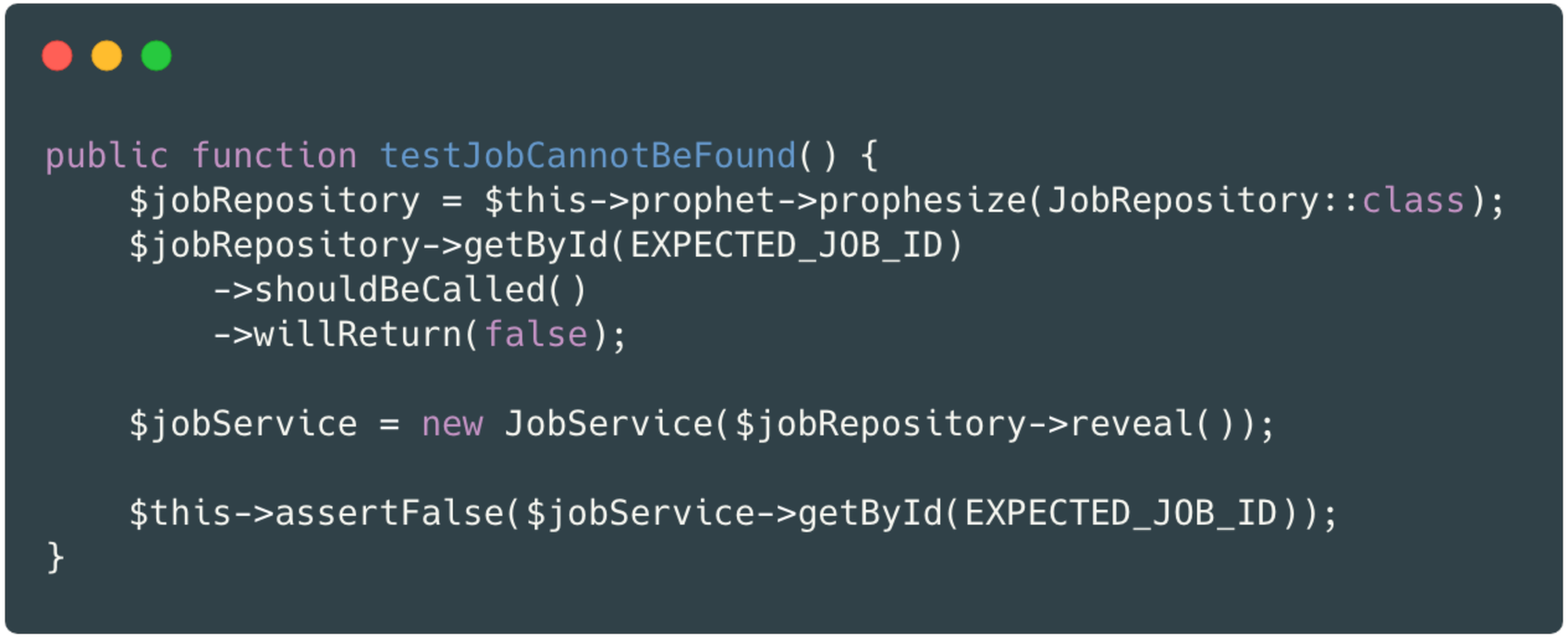
TESTING


LOTS OF MANUAL TESTING
E2E TESTS
INTEGRATION TESTS
UNIT TESTS


COST
E2E TESTS
INTEGRATION TESTS
UNIT TESTS
SPEED


Exploratory testing & user feedback
Monitoring & alerting
E2E TESTS
INTEGRATION TESTS
UNIT TESTS
COST
SPEED


Exploratory testing & user feedback
Monitoring & alerting
10%
E2E TESTS
20%
INTEGRATION TESTS
70%
UNIT TESTS
COST
SPEED



```php
public function testJobCannotBeFound() {
    $jobRepository = $this->prophet->prophesize(JobRepository::class);
    $jobRepository->getById(EXPECTED_JOB_ID)
        ->shouldBeCalled()
        ->willReturn(false);

    $jobService = new JobService($jobRepository->reveal());

    $this->assertFalse($jobService->getById(EXPECTED_JOB_ID));
}
```

UNIT TESTS

(PHPUnit, JUnit, TestNG)

CODE COVERAGE

	Code Coverage								
	Lines			Functions and Methods			Classes and Traits		
Total		29.00%	558 / 1924		37.77%	71 / 188		11.76%	4 / 34
Annotation		n/a	0 / 0		n/a	0 / 0		n/a	0 / 0
Entity		74.68%	59 / 79		57.14%	12 / 21		0.00%	0 / 1
EventSubscriber		100.00%	10 / 10		100.00%	3 / 3		100.00%	1 / 1
Form		0.00%	0 / 130		0.00%	0 / 39		0.00%	0 / 6
Plugin		44.30%	70 / 158		41.67%	10 / 24		20.00%	1 / 5
Tests		6.72%	54 / 804		28.57%	14 / 49		0.00%	0 / 10
AliasCleaner.php		95.24%	120 / 126		71.43%	5 / 7		0.00%	0 / 1
AliasCleanerInterface.php		n/a	0 / 0		n/a	0 / 0		n/a	0 / 0
AliasStorageHelper.php		71.43%	50 / 70		54.55%	6 / 11		0.00%	0 / 1
AliasStorageHelperInterface.php		n/a	0 / 0		n/a	0 / 0		n/a	0 / 0
AliasTypeBatchUpdateInterface.php		n/a	0 / 0		n/a	0 / 0		n/a	0 / 0
AliasTypeInterface.php		n/a	0 / 0		n/a	0 / 0		n/a	0 / 0
AliasTypeManager.php		66.67%	8 / 12		50.00%	2 / 4		0.00%	0 / 1
AliasUniquifier.php		91.89%	34 / 37		75.00%	3 / 4		0.00%	0 / 1
AliasUniquifierInterface.php		n/a	0 / 0		n/a	0 / 0		n/a	0 / 0
MessengerInterface.php		n/a	0 / 0		n/a	0 / 0		n/a	0 / 0
PathautoFieldItemList.php		100.00%	9 / 9		100.00%	2 / 2		100.00%	1 / 1
PathautoGenerator.php		91.43%	96 / 105		71.43%	5 / 7		0.00%	0 / 1
PathautoGeneratorInterface.php		n/a	0 / 0		n/a	0 / 0		n/a	0 / 0
PathautoItem.php		90.91%	10 / 11		66.67%	2 / 3		0.00%	0 / 1
PathautoPatternInterface.php		n/a	0 / 0		n/a	0 / 0		n/a	0 / 0
PathautoPatternListBuilder.php		0.00%	0 / 13		0.00%	0 / 3		0.00%	0 / 1
PathautoState.php		81.82%	27 / 33		62.50%	5 / 8		0.00%	0 / 1
PathautoWidget.php		0.00%	0 / 16		0.00%	0 / 1		0.00%	0 / 1
VerboseMessenger.php		100.00%	11 / 11		100.00%	2 / 2		100.00%	1 / 1

Legend

Low: 0% to 50% **Medium**: 50% to 90% **High**: 90% to 100%

```php
public function testFindJob() {
  $expectedJob = $this->loadFixture('active_job.yml');
  $actualJob = $this->repository->getById($expectedJob->getId());

  self::assertInstanceOf(Job::class, $actualJob);
  self::assertEquals($expectedJob->getId(), $actualJob->getId());
}
```

INTEGRATION TESTS

(PHPUnit*, Spring TestContext, RestAssured)

Scenario: Link to related job

Given a job exists

And there are related jobs available

When that job is viewed

Then a list of related jobs is shown

And each related job links to the detail page of the related job

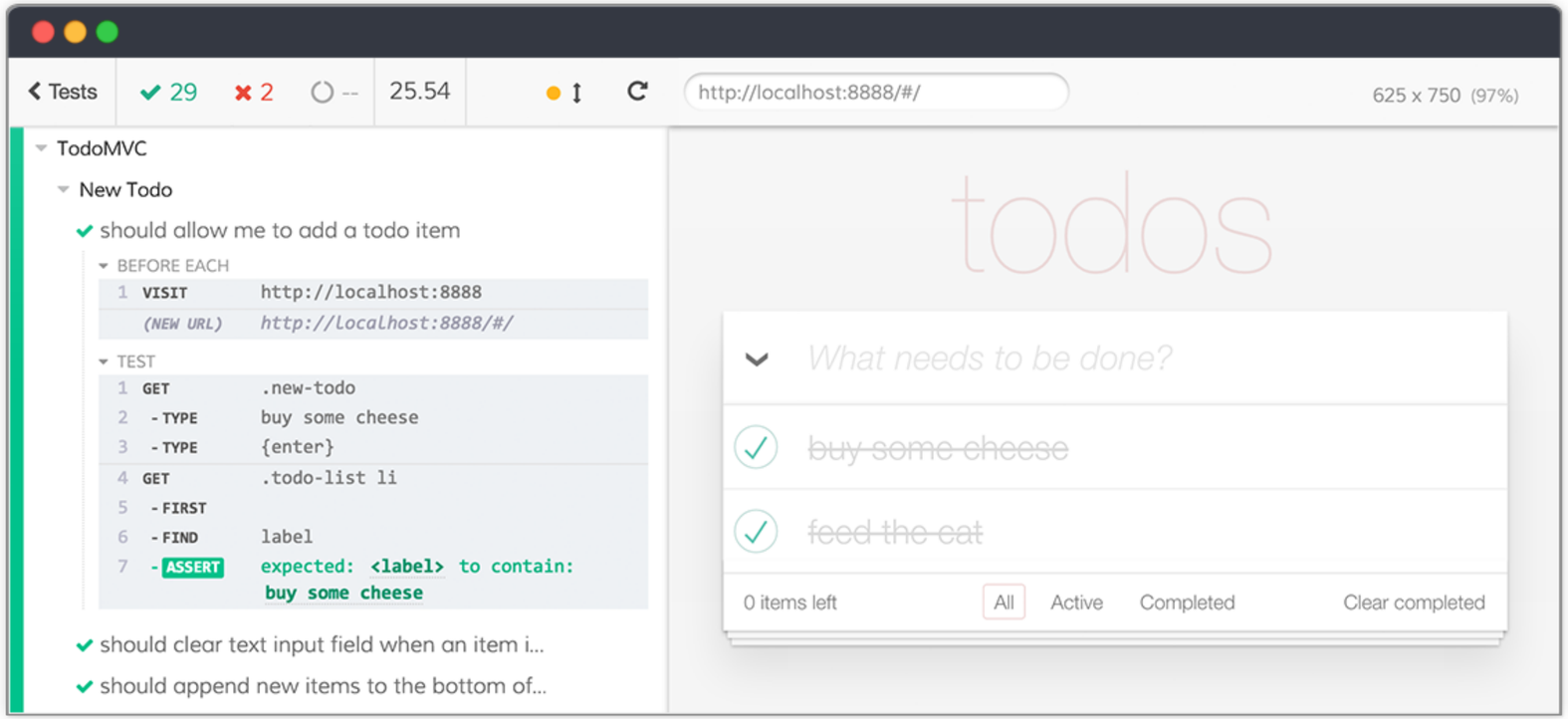
ACCEPTANCE TESTS

(Behat, JBehave, Cucumber)

```php
/**
 * @Then I should see the last book
 */
public function iShouldSeeTheLastBook()
{
    $this->assertSession()->pageTextContains('Our last book');
}
```

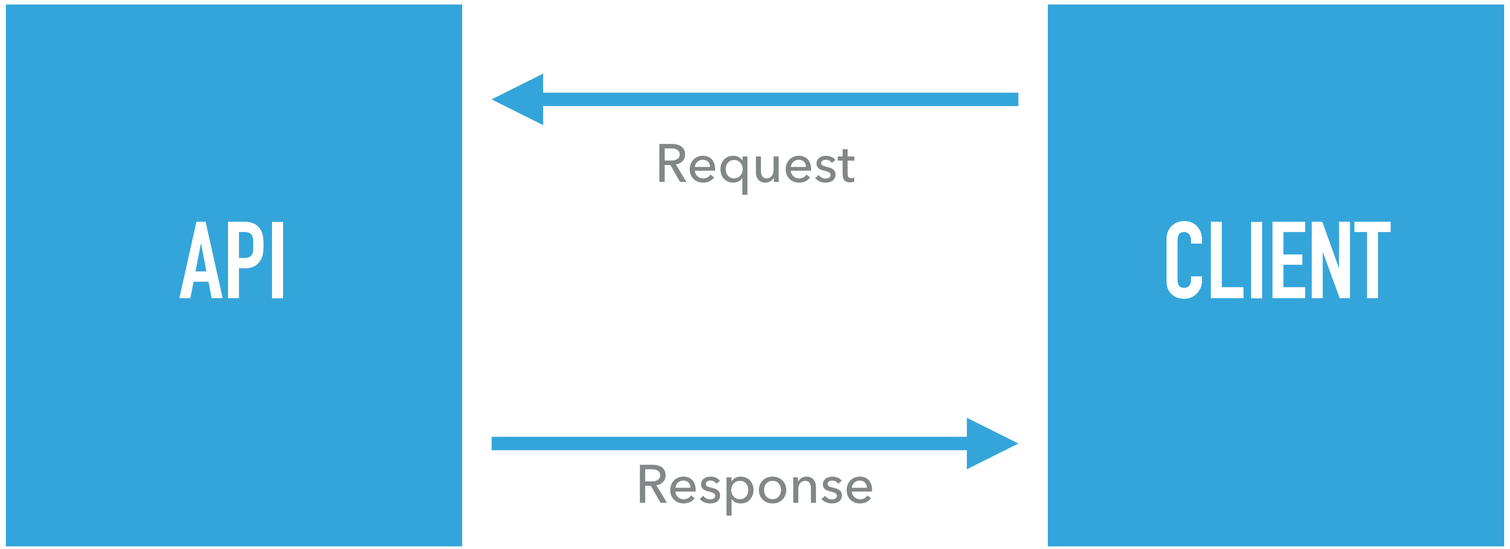
ACCEPTANCE TESTS

(Behat, JBehave, Cucumber)

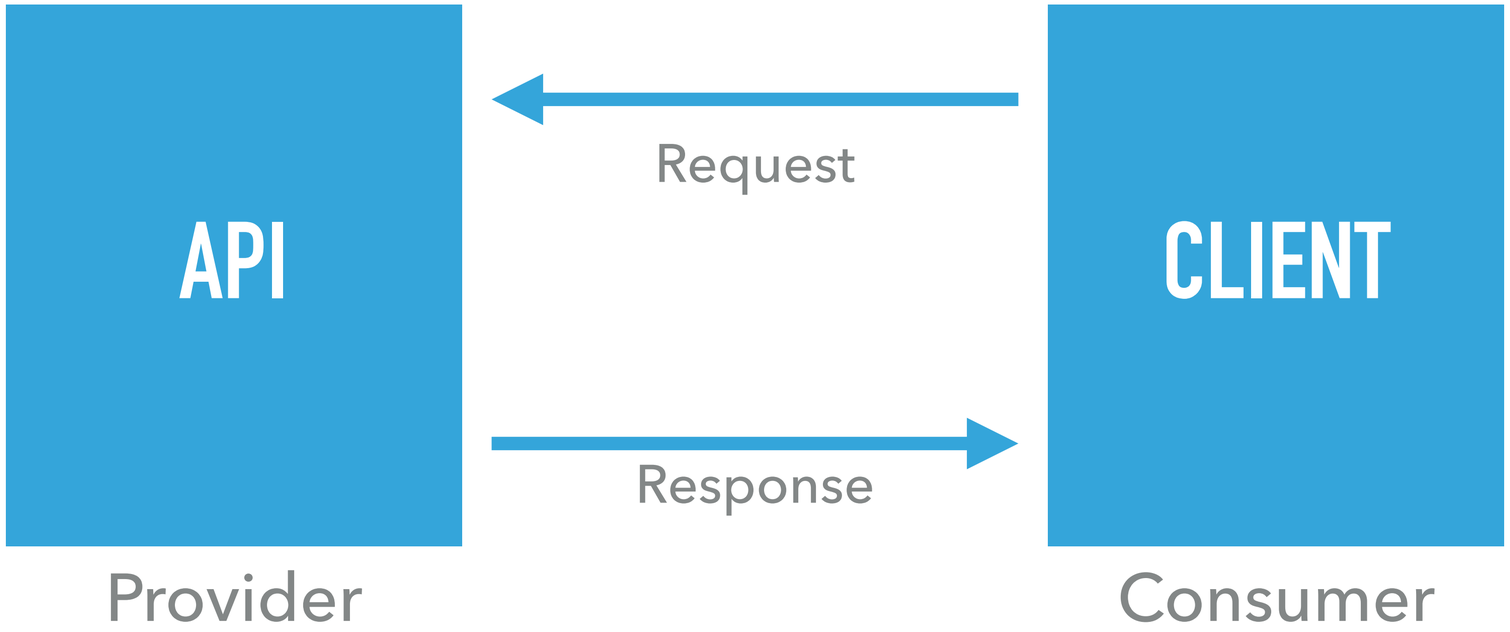


UI TESTING

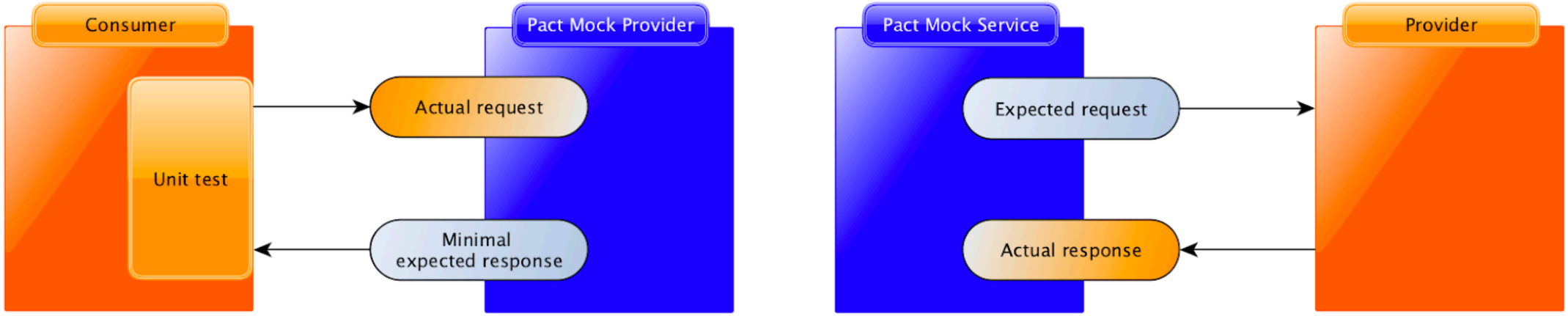
(Cypress, Selenium)



CONTRACT TESTING

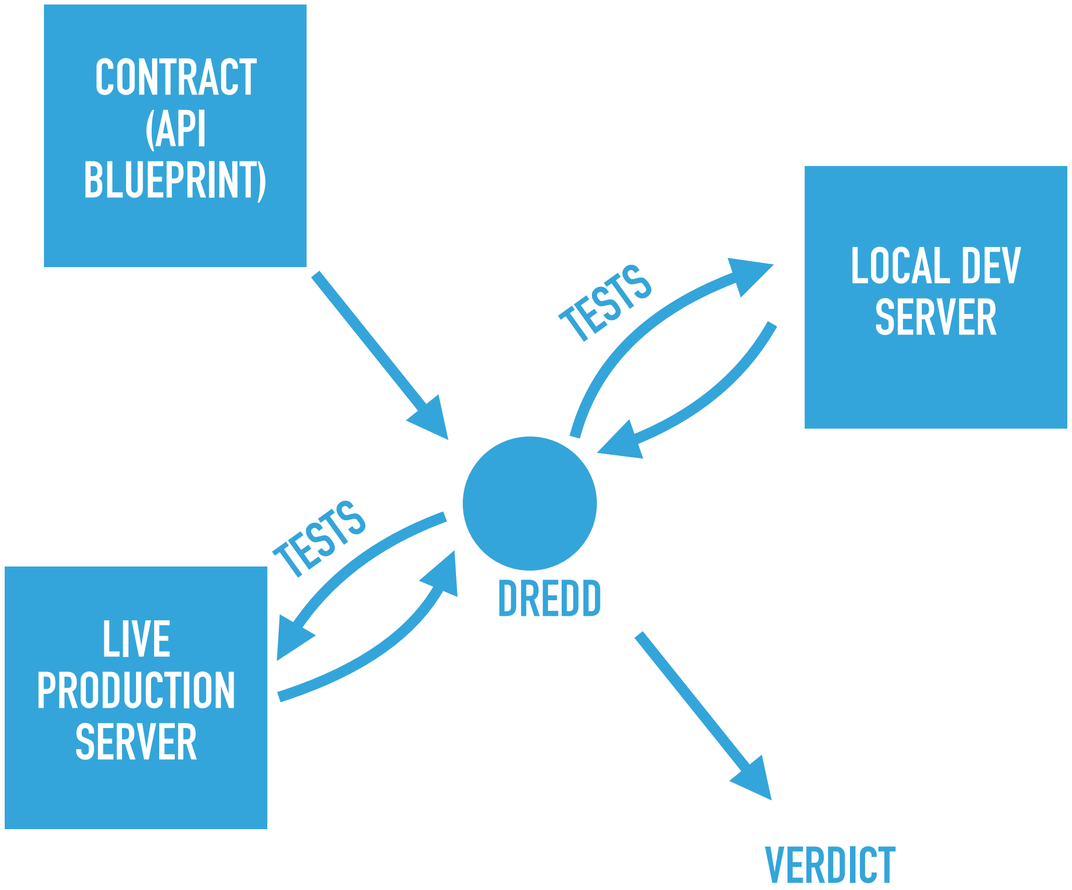


CONTRACT TESTING



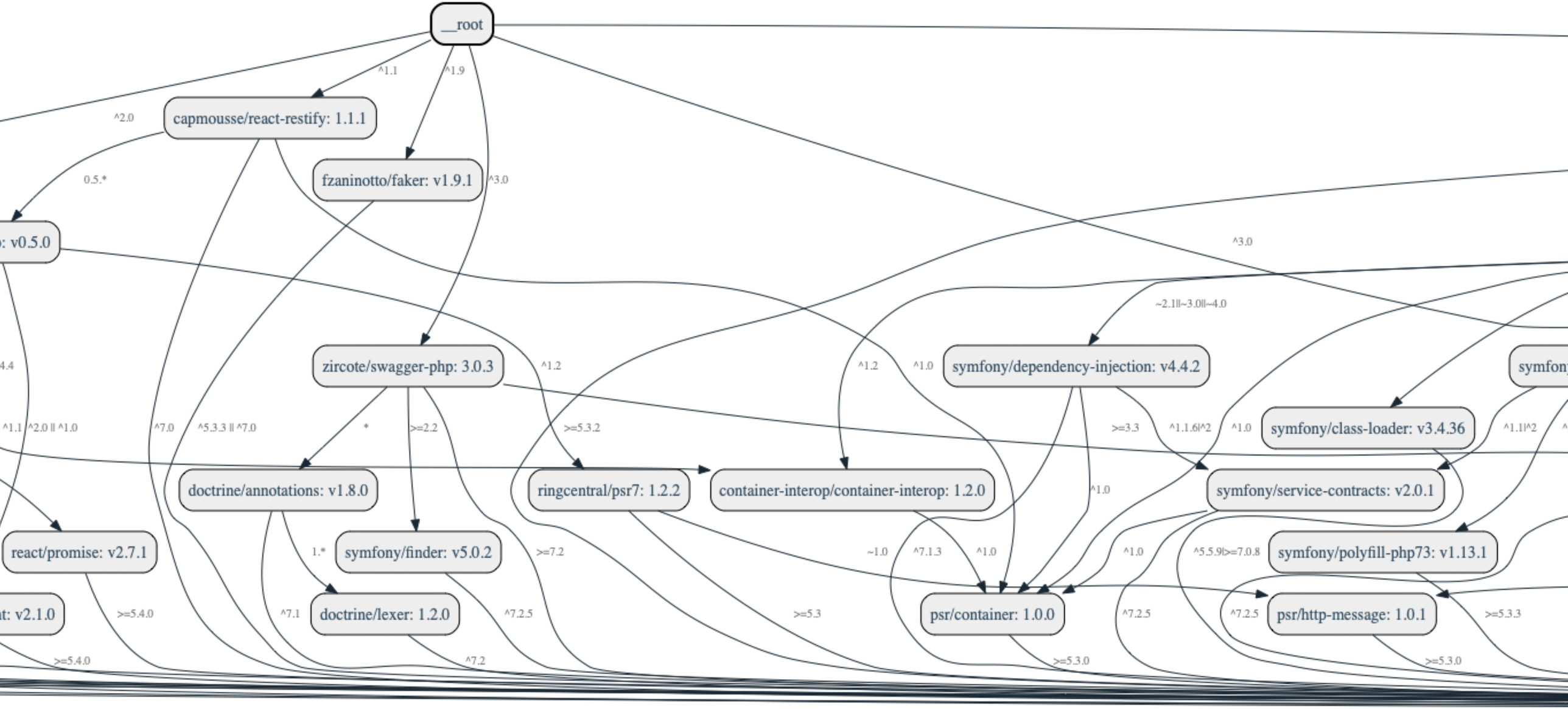
CONTRACT TESTING

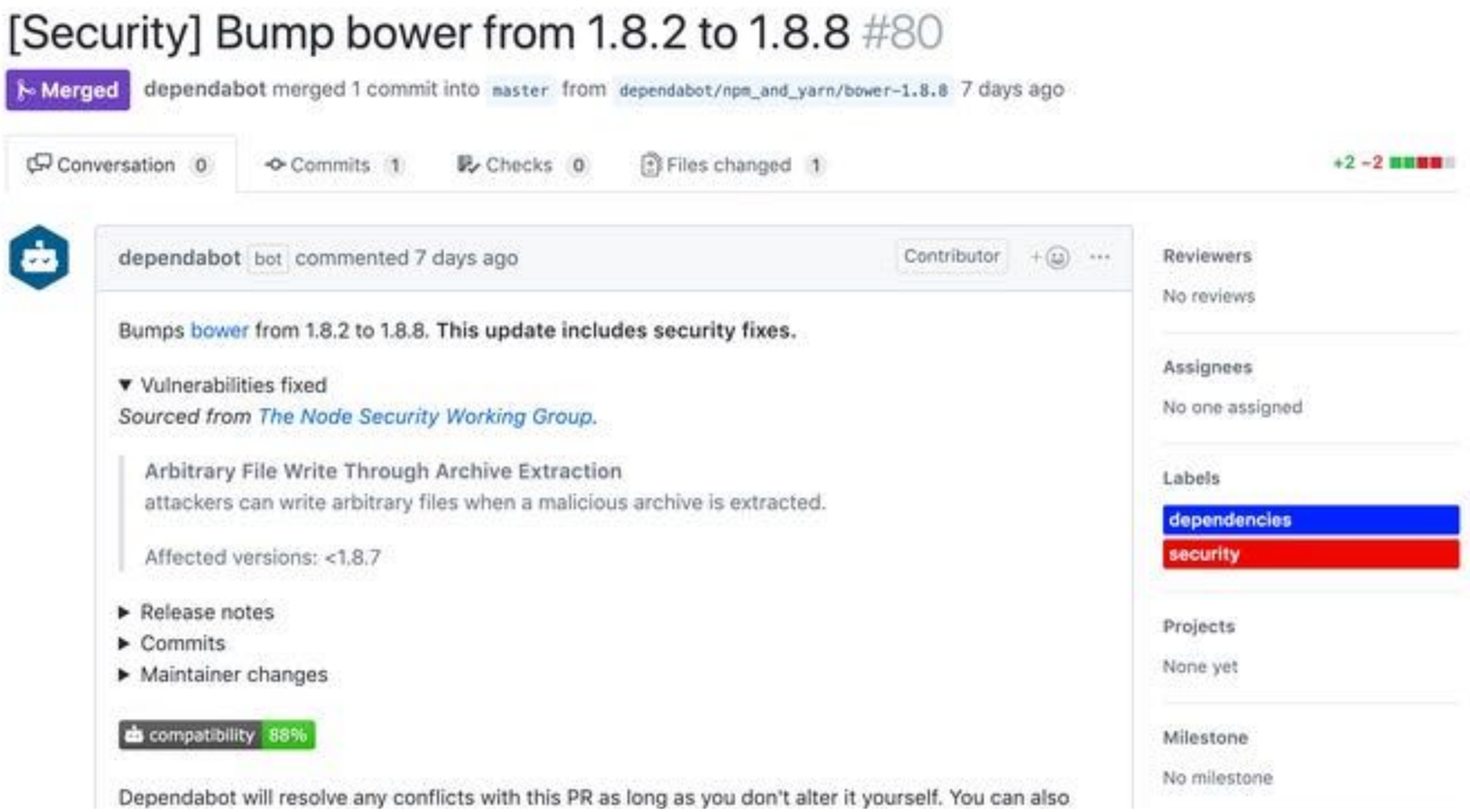
(Pact, Dredd)


CONTRACT
(API
BLUEPRINT)
LOCAL DEV
SERVER
TESTS
TESTS
LIVE
PRODUCTION
SERVER
DREDD
VERDICT

SECURITY

DEPENDENCY SCANNING & UPDATING


__root
^1.1
^1.9
^2.0
capmousse/react-restify: 1.1.1
0.5.*
fzaninotto/faker: v1.9.1
^3.0
: v0.5.0
^3.0
~2.1||~3.0||~4.0
zircote/swagger-php: 3.0.3
^1.2
^1.2
^1.0
symfony/dependency-injection: v4.4.2
symfon
4.4
^1.1
^2.0 || ^1.0
^7.0
^5.3.3 || ^7.0
*
>=2.2
>=5.3.2
>=3.3
^1.1.6|^2
^1.0
symfony/class-loader: v3.4.36
^1.1|^2
doctrine/annotations: v1.8.0
ringcentral/psr7: 1.2.2
container-interop/container-interop: 1.2.0
^1.0
symfony/service-contracts: v2.0.1
react/promise: v2.7.1
1.*
symfony/finder: v5.0.2
>=7.2
~1.0
^7.1.3
^1.0
^1.0
^5.5.9|>=7.0.8
symfony/polyfill-php73: v1.13.1
t: v2.1.0
>=5.4.0
^7.1
doctrine/lexer: 1.2.0
^7.2.5
>=5.3
psr/container: 1.0.0
^7.2.5
^7.2.5
psr/http-message: 1.0.1
>=5.3.3
>=5.4.0
^7.2
>=5.3.0
>=5.3.0



GITHUB INTEGRATION

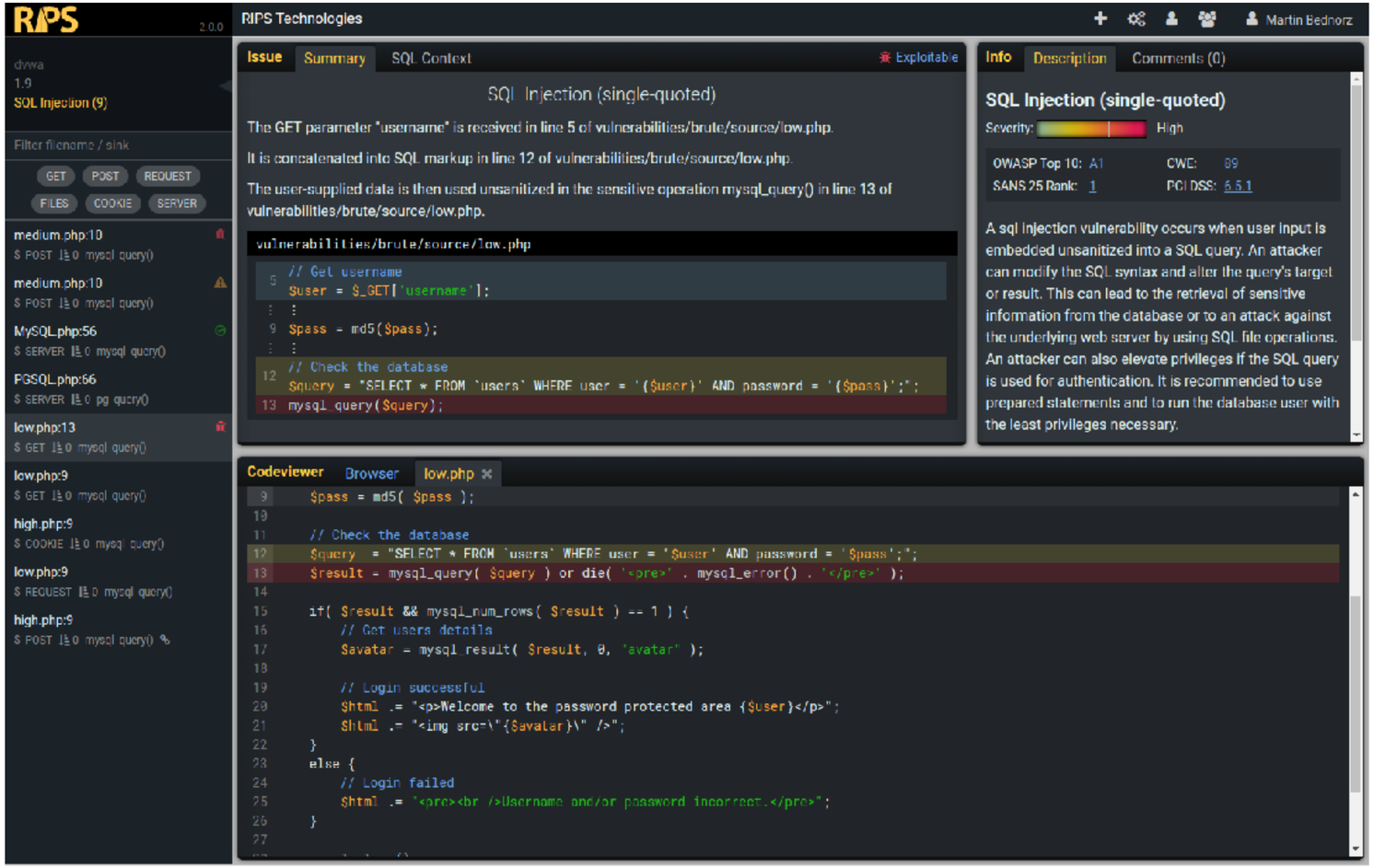
(Renovate, Dependabot)

Search Level	Search Code	Search Component	Search Filename
8	CVE-2017-15095	com.fasterxml.jackson.core : jackson-databind : 2.8.9	jackson-databind-2.8.9.jar
7	CVE-2016-1000341	org.jruby : jruby-complete : 1.7.21	jruby-complete-1.7.21.jar
	CVE-2016-1000341	org.bouncycastle : bcprov-jdk15on : 1.50	bcprov-jdk15on-1.50.jar
	CVE-2017-5929	ch.qos.logback : logback-classic : 1.1.11	logback-classic-1.1.11.jar
	CVE-2017-7957	com.thoughtworks.xstream : xstream : 1.4.7	xstream-1.4.7.jar

VULNERABLE DEPENDENCIES

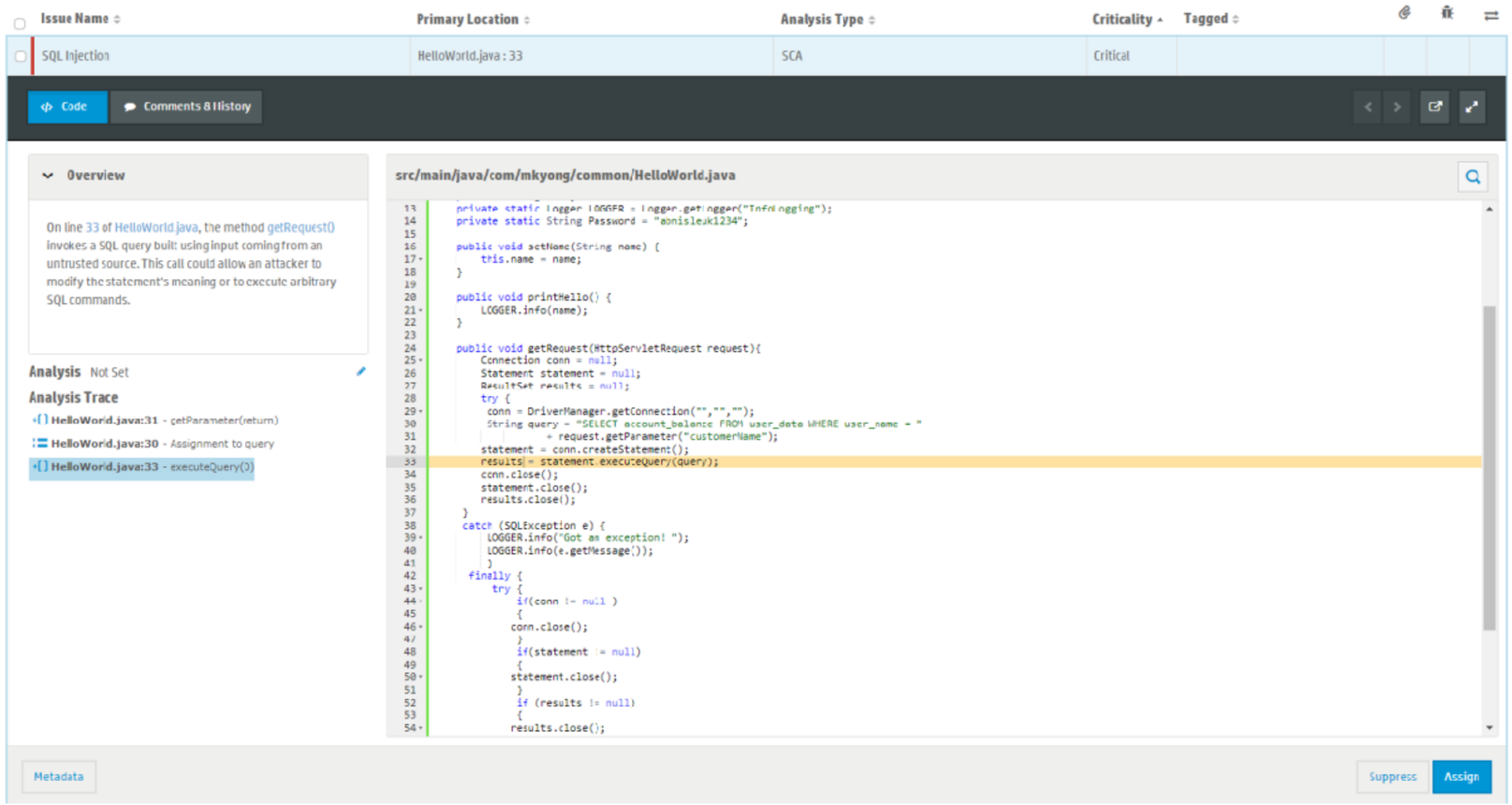
(Snyk, Whitesource, Nexus)

STATIC APPLICATION SECURITY TESTING



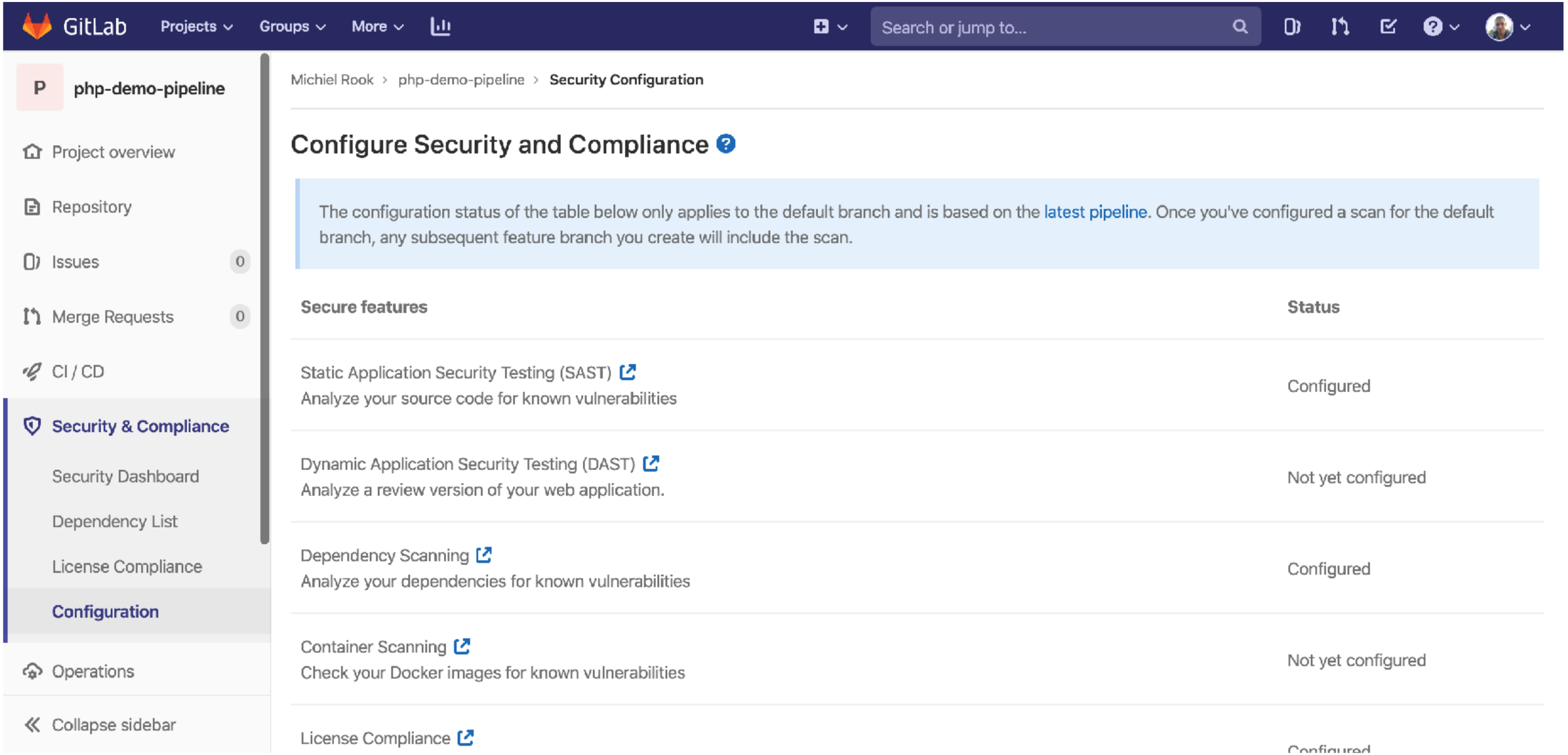
SAST

(Fortify, RIPS, Sonarqube, Coverity)



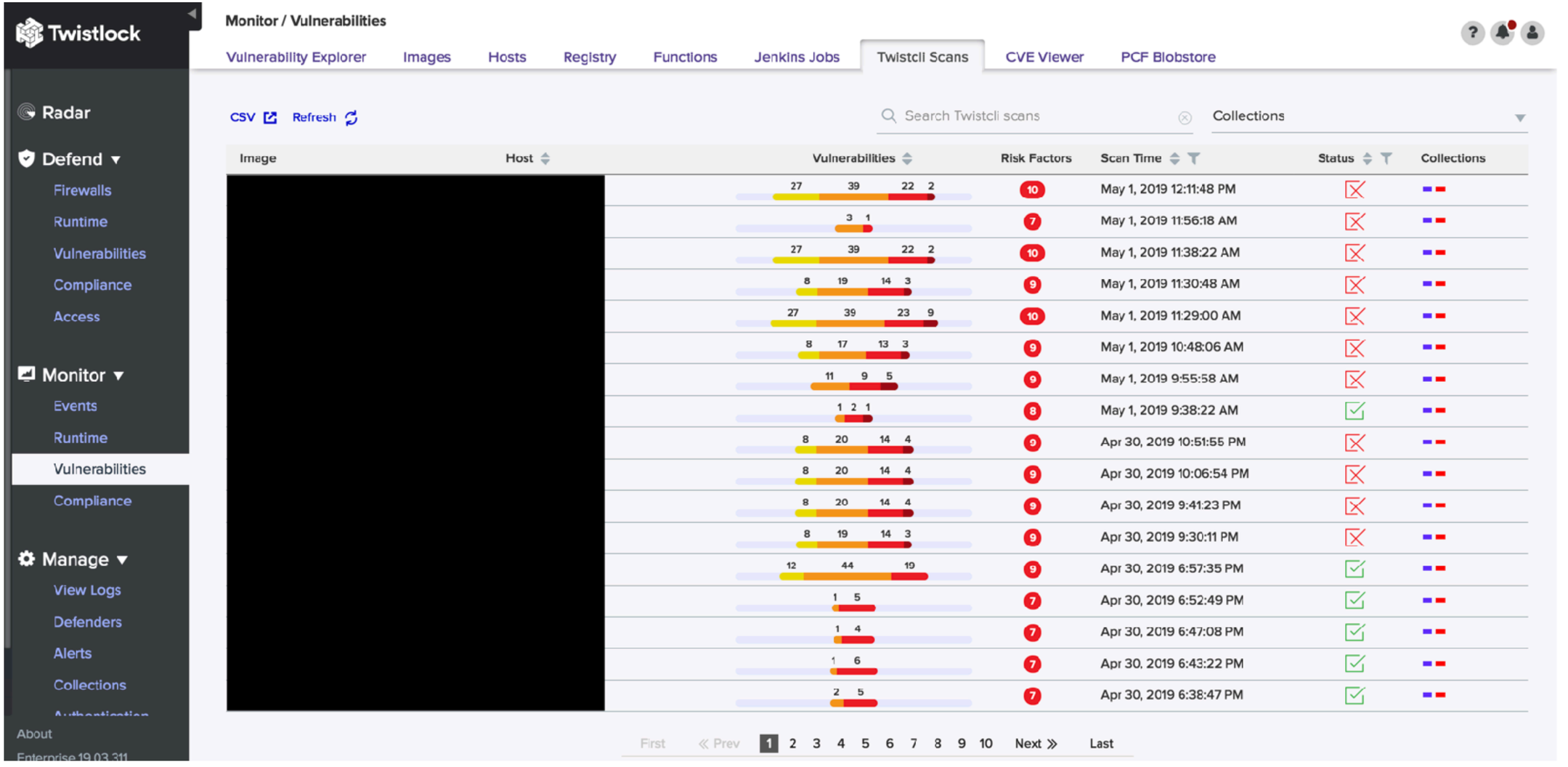
SAST

(Fortify, RIPS, Sonarqube, Coverity)

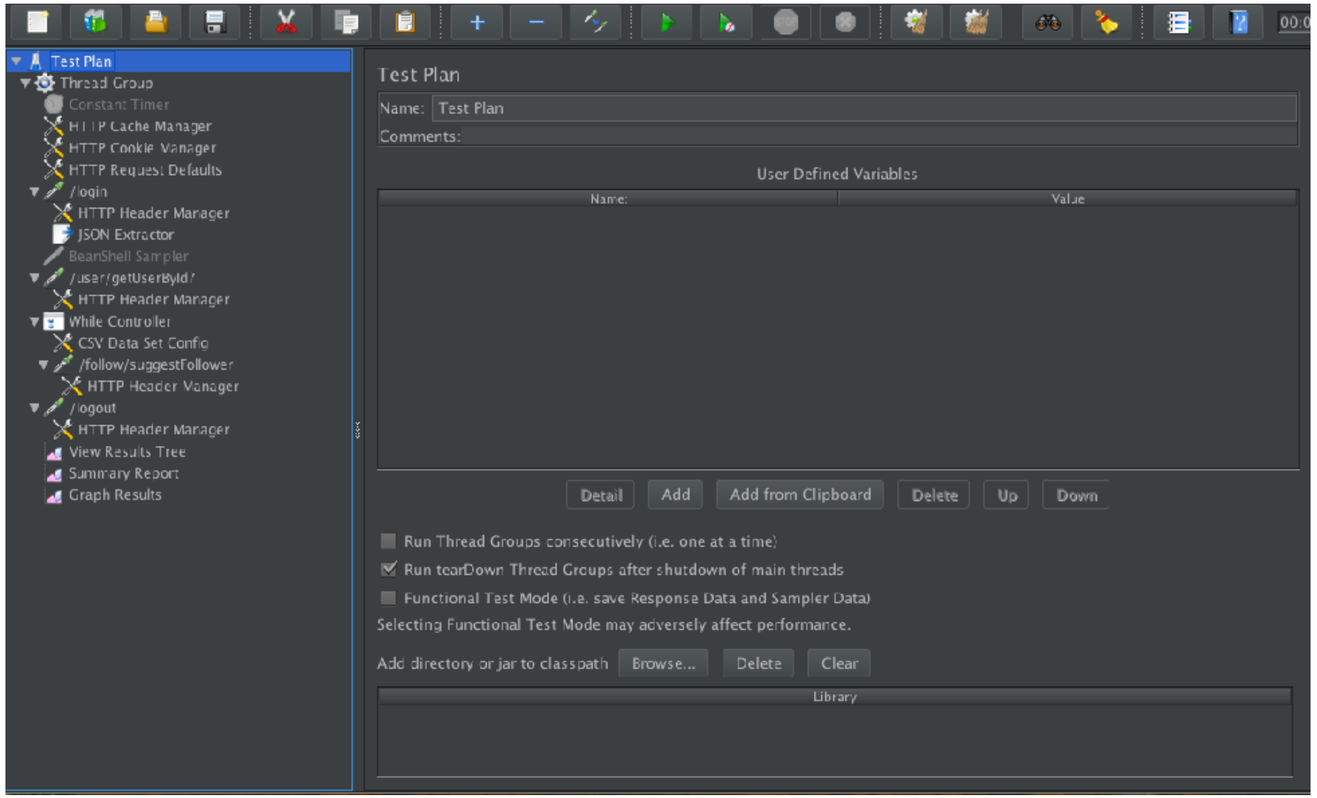

GitLab
Projects
Groups
More
Search or jump to...
P
php-demo-pipeline
Project overview
Repository
Issues 0
Merge Requests 0
CI / CD
Security & Compliance
Security Dashboard
Dependency List
License Compliance
Configuration
Operations
Collapse sidebar
Michiel Rook › php-demo-pipeline › Security Configuration
Configure Security and Compliance
The configuration status of the table below only applies to the default branch and is based on the latest pipeline. Once you've configured a scan for the default branch, any subsequent feature branch you create will include the scan.
Secure features
Status
Static Application Security Testing (SAST)
Analyze your source code for known vulnerabilities
Configured
Dynamic Application Security Testing (DAST)
Analyze a review version of your web application.
Not yet configured
Dependency Scanning
Analyze your dependencies for known vulnerabilities
Configured
Container Scanning
Check your Docker images for known vulnerabilities
Not yet configured
License Compliance

CONTAINERS & IMAGES

```
2019/06/17 18:54:03 [INFO] ▶ Start clair-scanner
2019/06/17 18:54:03 [INFO] ▶ Server listening on port 9279
2019/06/17 18:54:03 [INFO] ▶ Analyzing 0d2eaf4aa1a6112f04f5377ab5faee43703e2ded380b6109478f2db1fe0666bf
2019/06/17 18:54:04 [INFO] ▶ Analyzing f57dc1490b1626f8f8ce34ebaef47342f280ca76e06204e4c1b80712c86074f9
2019/06/17 18:54:04 [INFO] ▶ Analyzing a1abe7ff819fef644734533249aadbe80e9f9a8fb27e5f17cd90d37d347df044
2019/06/17 18:54:04 [INFO] ▶ Analyzing ac9062b378633bcd3edaf1f9c9e271770ded3d5474a68a15ea075d81eb31c016
2019/06/17 18:54:04 [INFO] ▶ Analyzing 104e809f65f73eebb42f5f2c6c4c1ea682874e2aff05b541eac3271e61adb4a1
2019/06/17 18:54:04 [INFO] ▶ Analyzing 0eaf8c4d3452d4d15c7b03839ffc1cc6b07380d05b4e78daf4761c21858e9001
2019/06/17 18:54:04 [INFO] ▶ Analyzing e4ba69b83fd7a2d219a31de2313e885d54cee18924b3682bd3ac3952fe9d89d7
2019/06/17 18:54:04 [INFO] ▶ Analyzing d77b51011fdd85911b79552fbc0484d3c89f2d1e2f1d22a438df1de93c16c04e
2019/06/17 18:54:04 [INFO] ▶ Analyzing 1d9b79ca48a5adac3bdb940715dd182551c6092767be1942e00d3934dca4d51e
2019/06/17 18:54:04 [WARN] ▶ Image [registry.gitlab.com/lucj/sophia.events:3ad2f9c8649096be90cba65710e09bad11218fd4] contains 4 total
vulnerabilities
2019/06/17 18:54:04 [ERRO] ▶ Image [registry.gitlab.com/lucj/sophia.events:3ad2f9c8649096be90cba65710e09bad11218fd4] contains 4 unapproved
vulnerabilities
+------------+-----------------------+--------------+-----------------+-----------------------------------------------------------------+
| STATUS     | CVE SEVERITY          | PACKAGE NAME | PACKAGE VERSION | CVE DESCRIPTION                                                 |
+------------+-----------------------+--------------+-----------------+-----------------------------------------------------------------+
| Unapproved | High CVE-2019-11068   | libxslt      | 1.1.32-r0       |                                                                 |
|            |                       |              |                 | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11068   |
+------------+-----------------------+--------------+-----------------+-----------------------------------------------------------------+
| Unapproved | Medium CVE-2018-14048 | libpng       | 1.6.35-r0       |                                                                 |
|            |                       |              |                 | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14048   |
+------------+-----------------------+--------------+-----------------+-----------------------------------------------------------------+
| Unapproved | Low CVE-2019-7317     | libpng       | 1.6.35-r0       |                                                                 |
|            |                       |              |                 | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7317    |
+------------+-----------------------+--------------+-----------------+-----------------------------------------------------------------+
| Unapproved | Unknown CVE-2018-14550 | libpng      | 1.6.35-r0       |                                                                 |
|            |                       |              |                 | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14550   |
+------------+-----------------------+--------------+-----------------+-----------------------------------------------------------------+
```


Twistlock
Monitor / Vulnerabilities
Vulnerability Explorer
Images
Hosts
Registry
Functions
Jenkins Jobs
Twistcli Scans
CVE Viewer
PCF Blobstore
Radar
Defend
Firewalls
Runtime
Vulnerabilities
Compliance
Access
Monitor
Events
Runtime
Vulnerabilities
Compliance
Manage
View Logs
Defenders
Alerts
Collections
About
Enterprise 19.03.311
CSV
Refresh
Search Twistcli scans
Collections
Image
Host
Vulnerabilities
Risk Factors
Scan Time
Status
Collections
May 1, 2019 12:11:48 PM
May 1, 2019 11:56:18 AM
May 1, 2019 11:38:22 AM
May 1, 2019 11:30:48 AM
May 1, 2019 11:29:00 AM
May 1, 2019 10:48:06 AM
May 1, 2019 9:55:58 AM
May 1, 2019 9:38:22 AM
Apr 30, 2019 10:51:55 PM
Apr 30, 2019 10:06:54 PM
Apr 30, 2019 9:41:23 PM
Apr 30, 2019 9:30:11 PM
Apr 30, 2019 6:57:35 PM
Apr 30, 2019 6:52:49 PM
Apr 30, 2019 6:47:08 PM
Apr 30, 2019 6:43:22 PM
Apr 30, 2019 6:38:47 PM
First
Prev
1 2 3 4 5 6 7 8 9 10
Next
Last

PERFORMANCE



PERFORMANCE TESTS

(JMeter, Gatling, Locust)

1. DETERMINE BASELINE
2. AGREE ON SOFT / HARD LIMITS
3. RUN IN PIPELINE TO CALC % UP/DOWN

OTHER AREAS

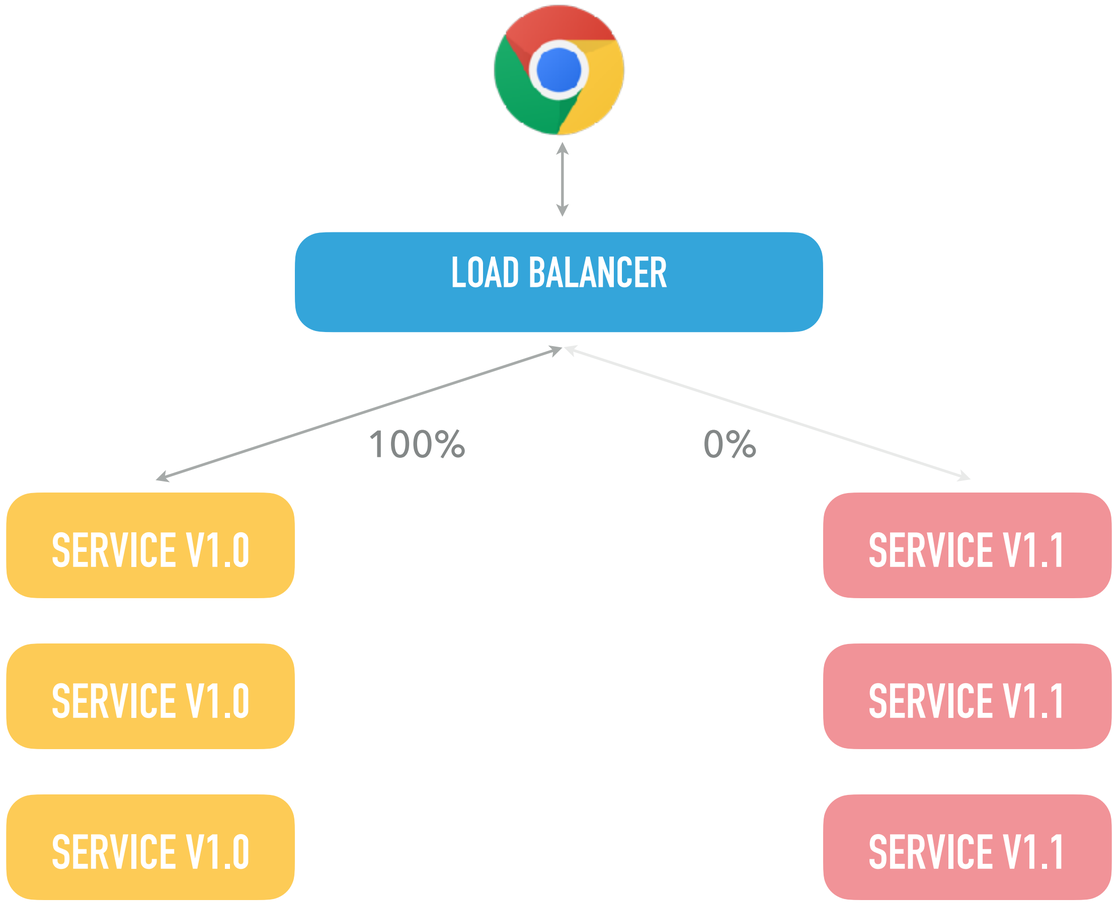
MUTATION TESTING

ACCESSIBILITY

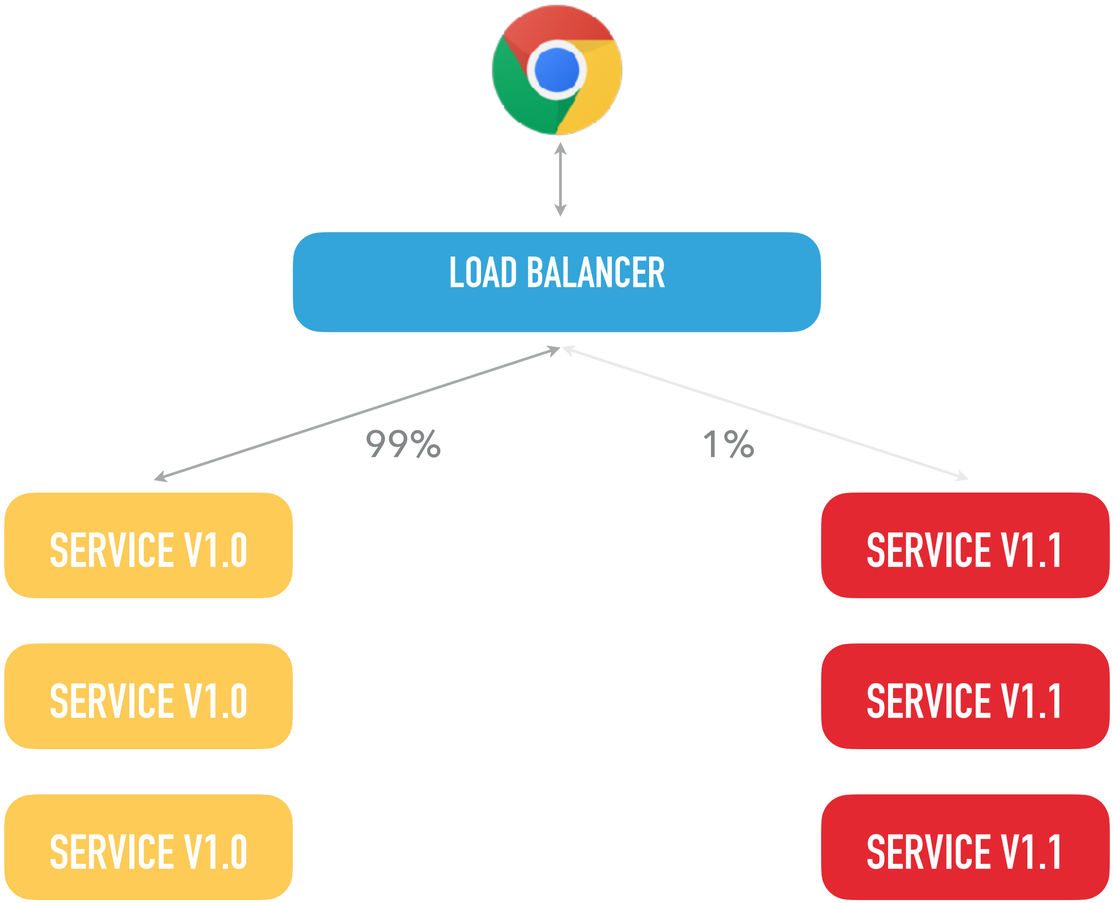
DEPLOYMENTS*

CANARY

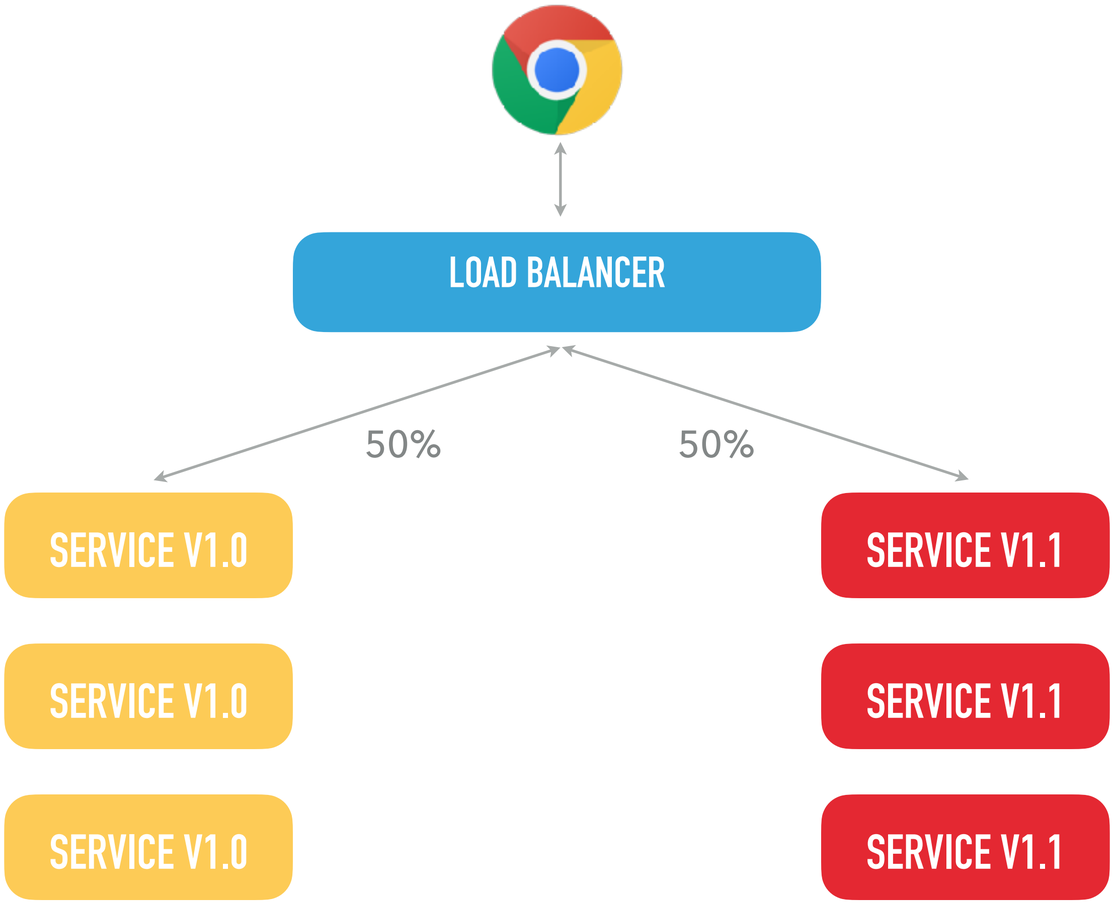
CANARY


LOAD BALANCER
100%
0%
SERVICE V1.0
SERVICE V1.0
SERVICE V1.0
SERVICE V1.1
SERVICE V1.1
SERVICE V1.1

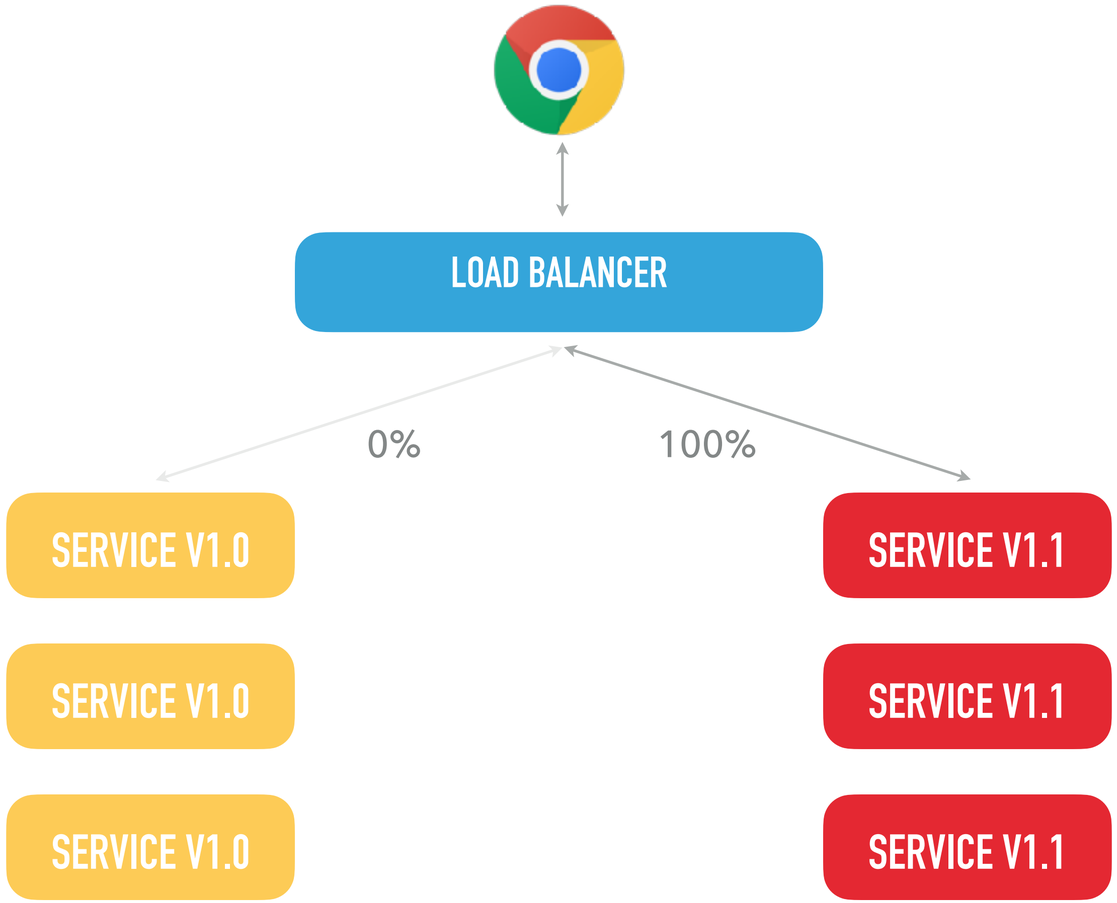
CANARY


LOAD BALANCER
99%
1%
SERVICE V1.0
SERVICE V1.0
SERVICE V1.0
SERVICE V1.1
SERVICE V1.1
SERVICE V1.1

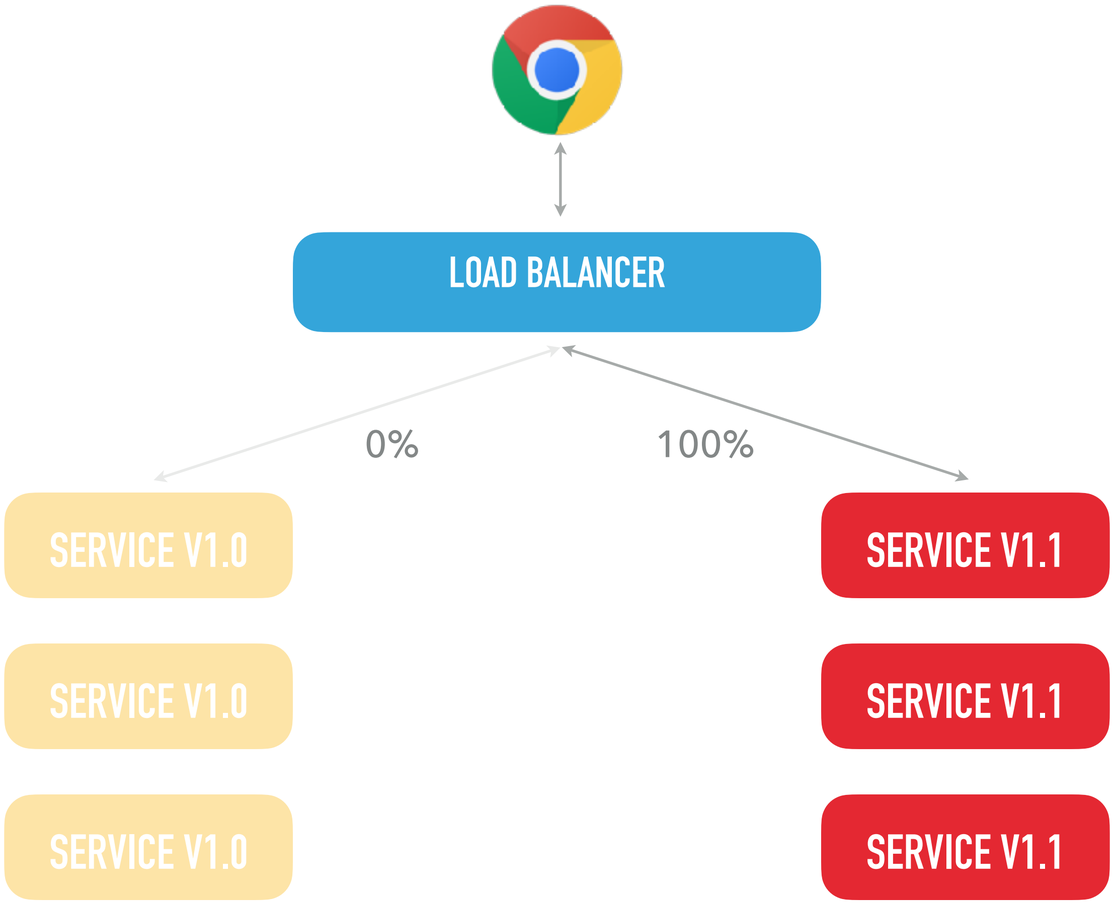
CANARY


LOAD BALANCER
50%
50%
SERVICE V1.0
SERVICE V1.0
SERVICE V1.0
SERVICE V1.1
SERVICE V1.1
SERVICE V1.1

CANARY

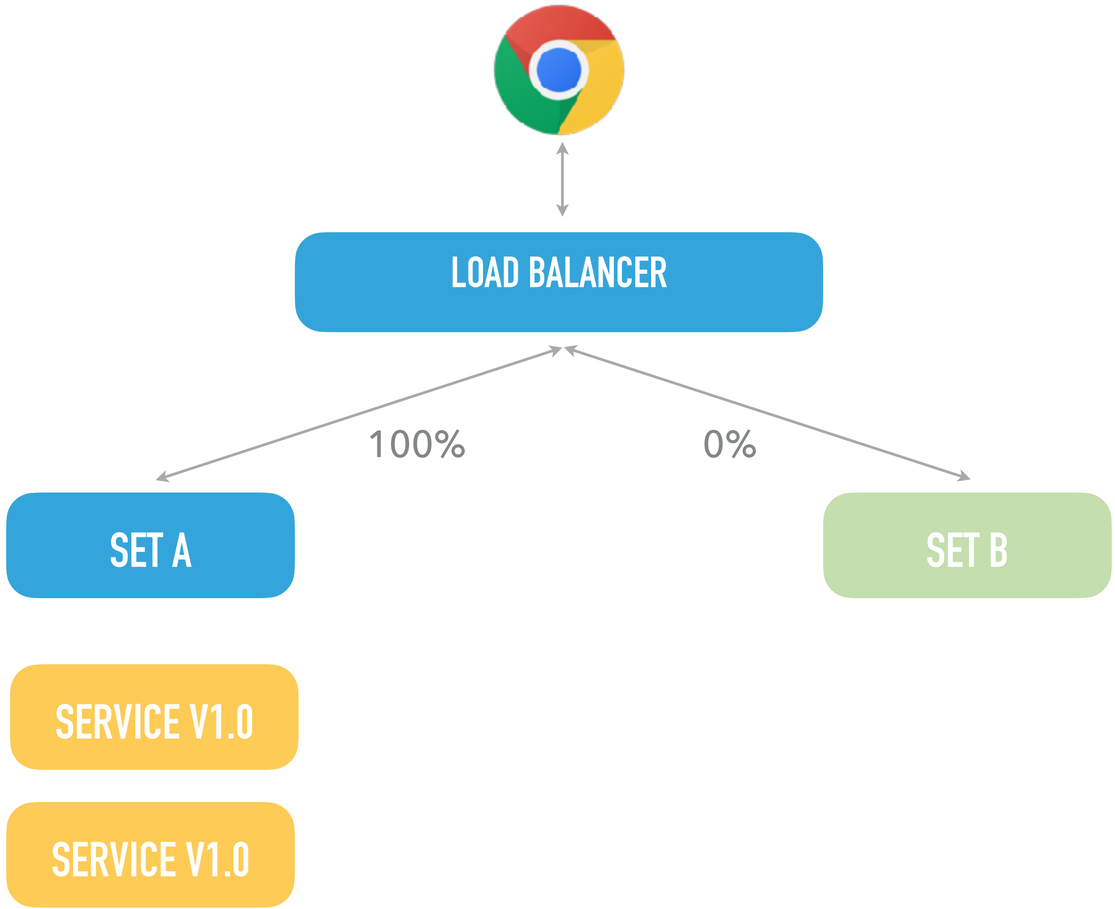

LOAD BALANCER
0%
100%
SERVICE V1.0
SERVICE V1.0
SERVICE V1.0
SERVICE V1.1
SERVICE V1.1
SERVICE V1.1

CANARY

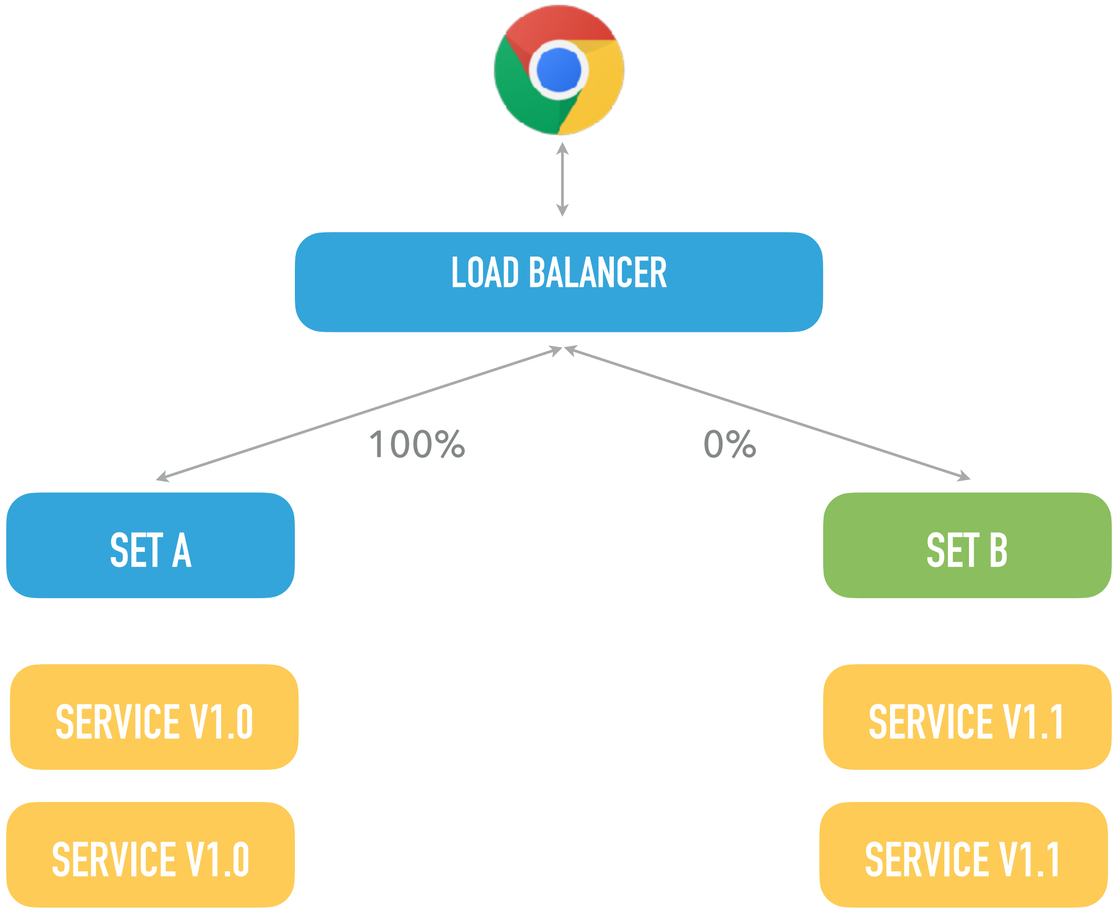

LOAD BALANCER
0%
100%
SERVICE V1.0
SERVICE V1.0
SERVICE V1.0
SERVICE V1.1
SERVICE V1.1
SERVICE V1.1

BLUE/GREEN

BLUE-GREEN

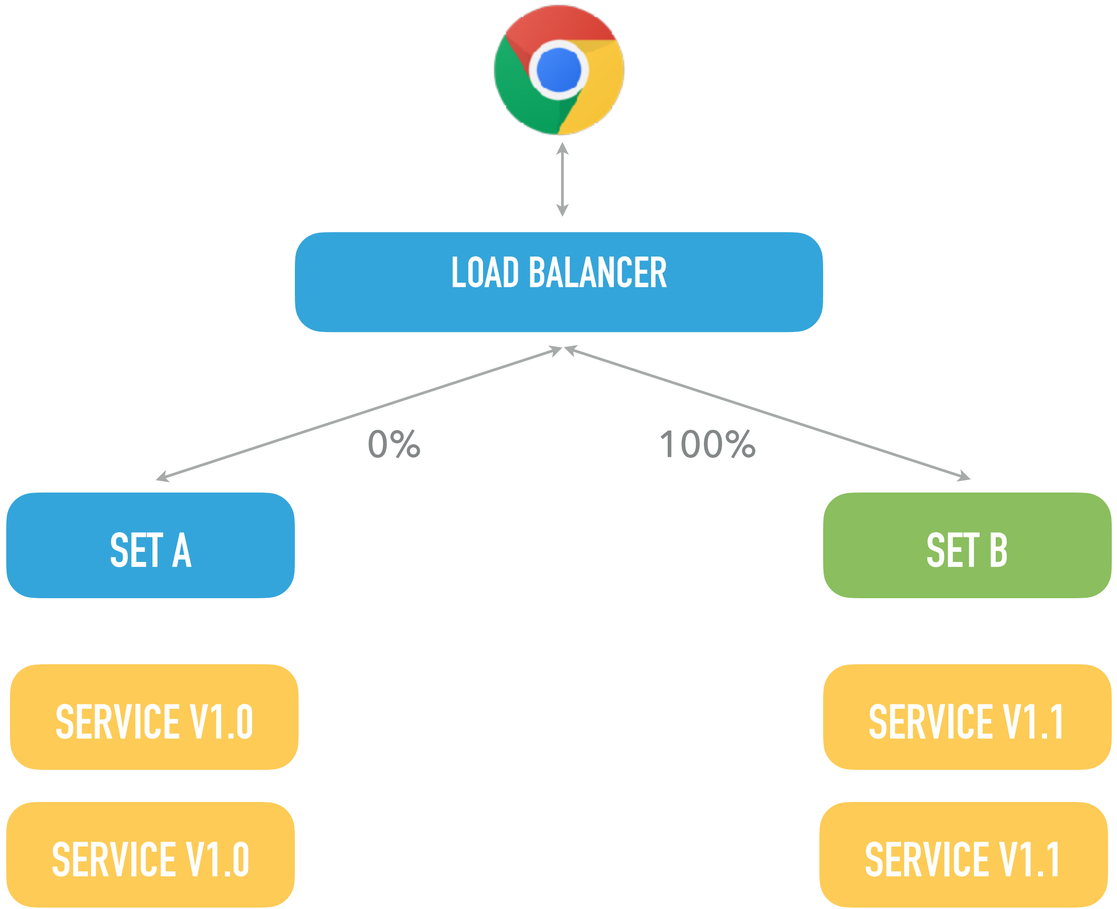


BLUE-GREEN



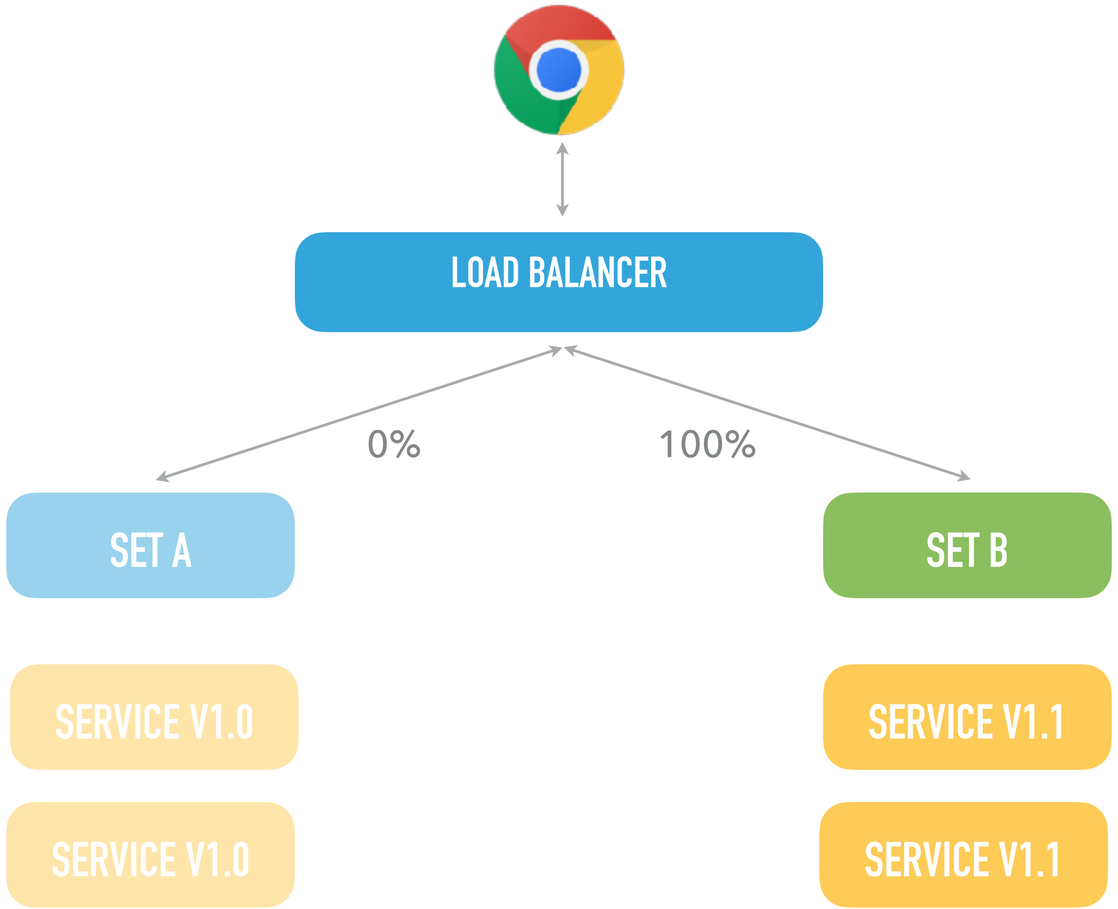
@michieltcs

BLUE-GREEN



@michieltcs

BLUE-GREEN



@michieltcs

TIPS

TESTING IS A FORM OF RISK MANAGEMENT

AVOID FLAKY TESTS

NO TEST SUITE DETECTS EVERY ISSUE

WATCH YOUR BUILD TIME

PIPELINE SPEED = KEY


INVEST-BASE
100% 83/83 (+1)
0
100% 1216/1216 (±0)
0
PEGASUS_TRUNK
66% 289/435 (+1)
146
PEGASUS_V1.4.2
BUILD #94 12%
BUILD #93 30%


Epic Zythos
E2E-aaaa_This_job_fails_every_second_run

FEEDBACK!

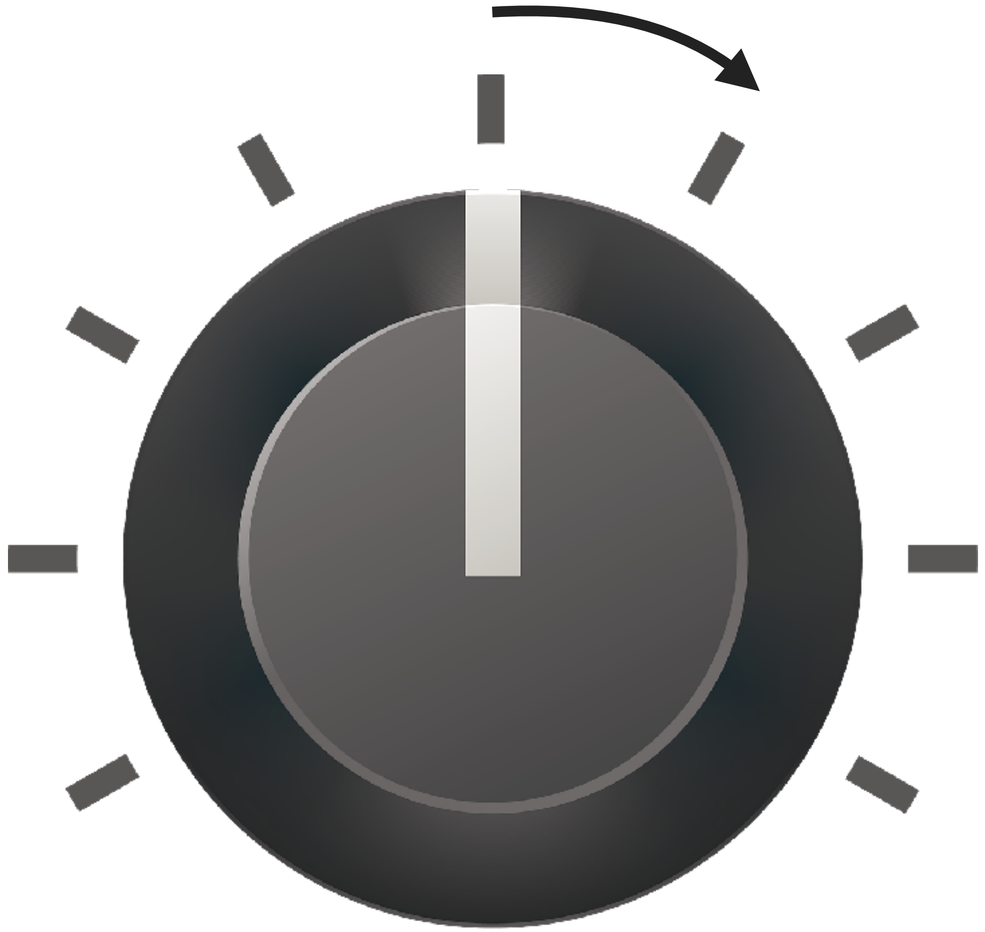
NOW YOU

AGREE ON STANDARDS

BUILD A PIPELINE

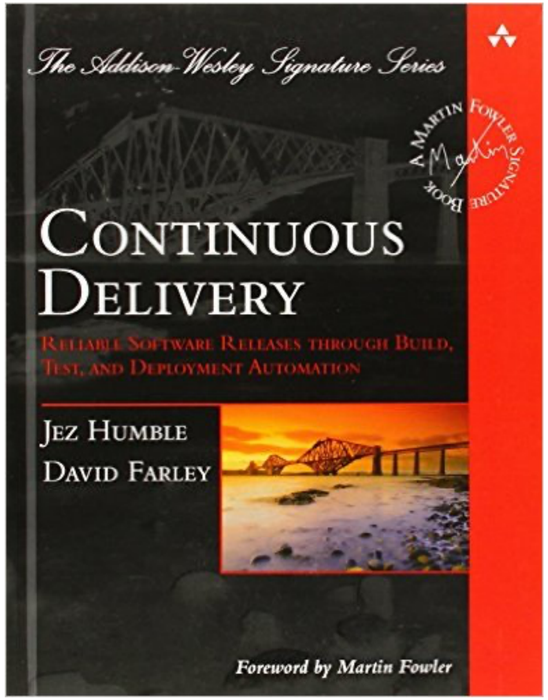
SHIFT LEFT

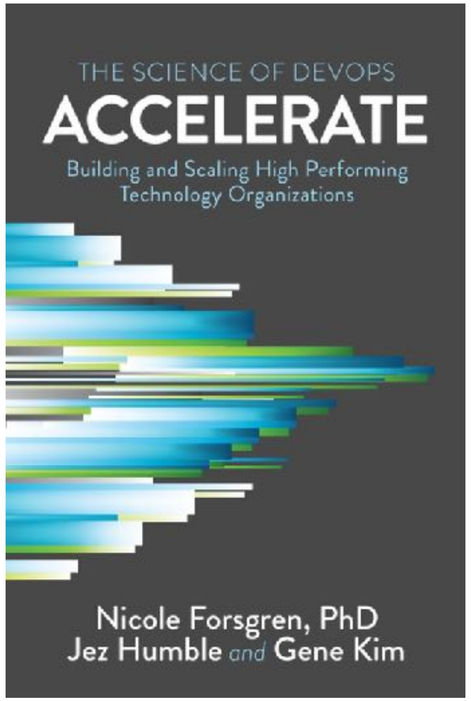
TAKE SMALL STEPS

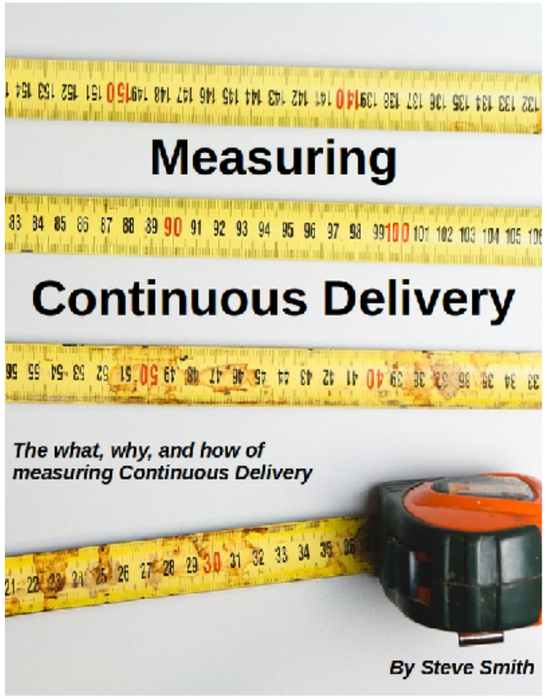


LET'S TURN GATEKEEPERS INTO BUILD BREAKERS!

INTERESTED IN MORE?







THANK YOU FOR LISTENING!

@michieltcs / michiel@michielrook.nl

www.michielrook.nl