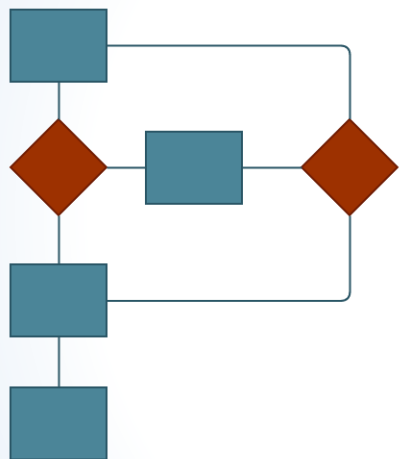


Tests Your Pipeline Might Be Missing



**Build confidence that you have a
viable candidate for production**

It's about process, not tools

@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

1

1

About Coveros



- Coveros helps companies accelerate the delivery of secure, reliable software using agile methods
- Agile & DevOps Services
 - DevOps Implementation
 - DevSecOps Integration
 - Agile Transformations & Coaching
 - Agile Software Development
 - Agile Testing & Automation
- Agile, DevOps, Testing, Security Training
- Open Source Products
 - SecureCI – Secure DevOps toolchain
 - Selenified – Agile test framework

Development Platforms



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

2

2

Selected Commercial Clients



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

3

3

Selected Federal Clients



U.S. Immigration and Customs Enforcement



U.S. Citizenship and Immigration Services



@CoverosGene #CodeMash

VED.

4

4

Delivery Pipeline



Process of taking a code change
from developers and getting it deployed
into production or delivered to the customer

**automated,
manual,
or a mix**



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

5

5

Delivery Pipeline



Do we have a
viable candidate for production?



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

6

6

Everything can't be first or last



**Do just enough
of each type of testing
early in the pipeline
to determine if
further testing is justified.**

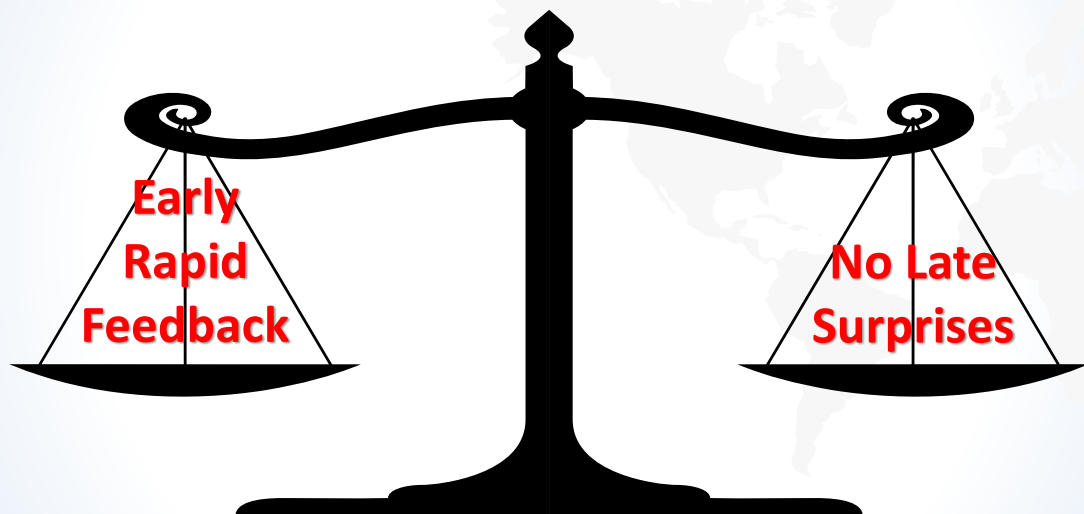
@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

7

7

Goal is to Balance



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

8

8

Check your code footprint



```
mvn dependency:tree
mvn dependency:analyze
mvn com.ning.maven.plugins:
maven-dependency-versions-check-plugin
```

@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

9

9

Are your libraries up-to-date?



DEPENDENCY-CHECK



DEPENDENCY-TRACK



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

10

10

Poor quality code is harder to maintain



... and harder to secure



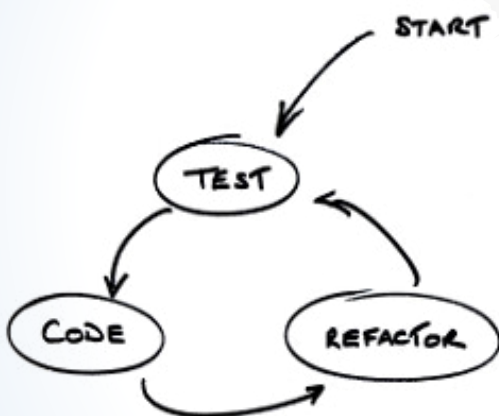
@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

11

11

Unit Testing



- Unit testing is not QA!
- Developer tool
- Early confirmation of code behavior
- Executable documentation
- Fearless refactoring

@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

12

12

Make sure your code is actually tested



MUTATION TESTING

```
public String bar(String s) {
    if (s == null) {
        // does something
    }
}
```



pitest.org



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

13

13

Functional testing



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

14

14

Test what users can't do



... or at least shouldn't be able to



User role testing



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

15

15

Test the APIs that you depend on



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

16

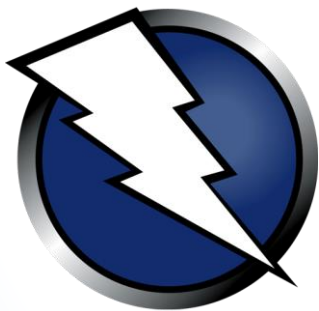
16

Security test



... by piggy-backing on functional and API tests

OWASP ZAP



PASSIVE PROXY
ACTIVE SCANNER
FUZZER

@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

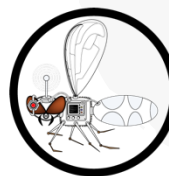
17

17

Mock the external services



... for better error case testing and faster tests



Hoverfly



POSTMAN



mockable.io

@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

18

18

What are your users doing?



Google Analytics



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

19

19

Repeatable, reliable deployments



... and test that through practice



ANSIBLE



docker



Microsoft
Azure



Google Cloud

@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

20

20

Test every deployment



- Smoke test every deployment
- Must be quick
- Test the deployment, not the functionality
- Focus on
 - basic signs of life
 - interfaces between systems
 - configuration settings

@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

21

21

Are your packages up-to-date?



apt-get

yum
yellowdog updater modified



CISA
CYBER+INFRASTRUCTURE



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

22

22

Protect against hackers



... even on dev and test systems

Fail2Ban



OpenSCAP



don't forget the infrastructure

@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

23

23

Audit yourself



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

24

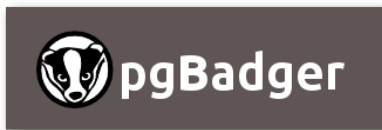
24

Test the database



sqlmap

Automatic SQL injection and database takeover tool



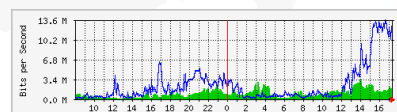
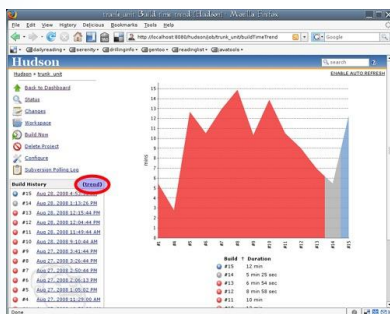
@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

25

25

How's performance?



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

26

26

Doesn't have to be full-blown



... some early checks might be helpful, too

- Short JMeter test
 - On development system, no isolation
 - 10 concurrent users for 10,000 requests
 - Track the trend
 - Answers: "Are we getting slower or faster?"
- Full load and performance test
 - Dedicated environment, no other traffic
 - Production-sized servers
 - 1,000 concurrent users for 4 hours
 - Answers: "What is the sustained capacity and throughput?"



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

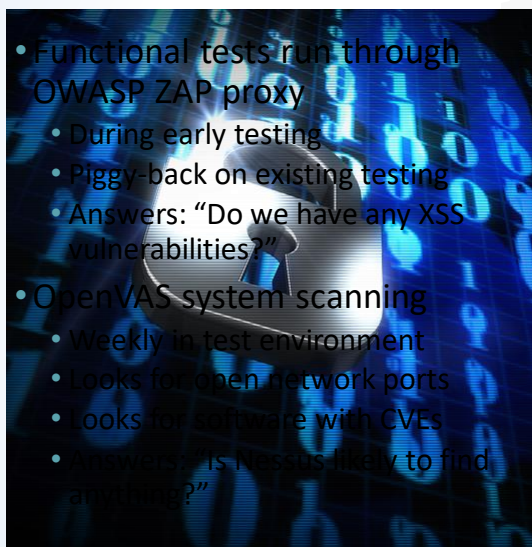
27

27

Same for security testing



- Functional tests run through OWASP ZAP proxy
 - During early testing
 - Piggy-back on existing testing
 - Answers: "Do we have any XSS vulnerabilities?"
- OpenVAS system scanning
 - Weekly in test environment
 - Looks for open network ports
 - Looks for software with CVEs
 - Answers: "Is Nessus likely to find anything?"
- HP WebInspect application security scanning
 - By corporate security group
 - Looks for black-box web vulnerabilities
 - Answers: "Do we have any XSS vulnerabilities?"
- Nessus system scanning
 - By corporate security group
 - Looks for open network ports
 - Looks for software with CVEs
 - Answers: "Is system compliant?"



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

28

28

And other non-functional tests



- Availability testing
- Accessibility testing
- Baseline testing
- Compatibility testing
- Compliance testing
- Configuration testing
- Documentation testing
- Endurance testing
- Ergonomics testing
- Interoperability testing
- Installation testing
- Internationalization testing
- Load testing
- Localization testing
- Maintainability testing

- Operational readiness testing
- Performance testing
- Portability testing
- Recovery testing
- Reliability testing
- Resilience testing
- Scalability testing
- Security testing
- Stability testing
- Stress testing
- Supportability testing
- Testability testing
- Usability testing
- Volume testing

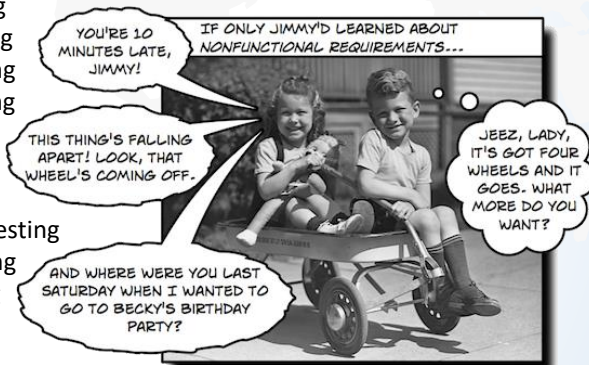


Image by Andrew Stellman via <http://www.stellman-greene.com/2010/02/17/nonfunctional-requirements-qa/>

@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

29

29

Plan for failure



... and practice recovering



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

30

30

Test your pipeline



... if it goes down, everything goes down



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

31

31

#Coveros5



- The pipeline is about **building confidence** that you have a viable candidate for production. **Add tests with that in mind.**
- Do just enough of each type of testing early in the pipeline to determine if further testing is justified.
Early, rapid feedback balanced with no late surprises.
- Use **mutation testing** to make sure your unit tests are actually covering what you need covered.
- **Some testing is better no testing.**
Even just watching trends of some token tests can be valuable.

@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

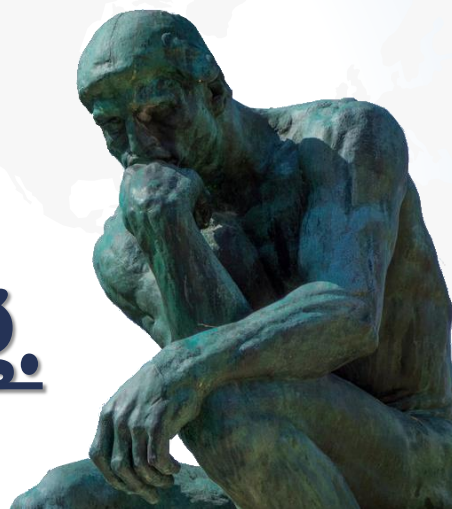
32

32

Don't expect that your pipeline is ever done



**A little better is
still better.
Keep improving.**



@CoverosGene #CodeMash

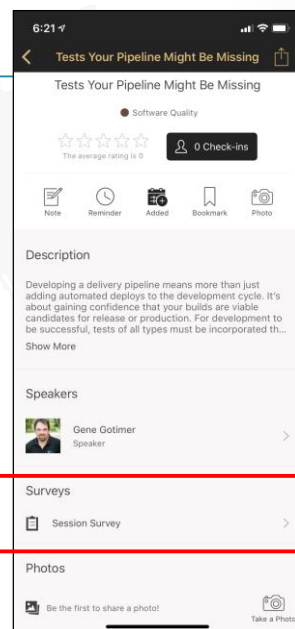
© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

33

33

Session Feedback

- Pull out your phone
- Pull up the AttendeeHub app
- Navigate to this session
- Choose Session Survey
- CodeMash and I want feedback
- Please



@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

34

34


Questions?



- I'll be around CodeMash for the rest of the week

- I am @Gene Gotimer on the TechWell Hub Slack
<https://hub.techwell.com/>



- Email: gene.gotimer@coveros.com
-  @CoverosGene

@CoverosGene #CodeMash

© COPYRIGHT 2020 COVEROS, INC. ALL RIGHTS RESERVED.

35