

# Agile Dev Better Software DevOps **WEST**

A TECHWELL EVENT

## **DT4**

Integrating Security Into DevOps

Thursday, June 7th, 2018, 11:30 AM

## **A Definition of Done for DevSecOps**

Presented by:

**Gene Gotimer**

Coveros, Inc.

Brought to you by:



350 Corporate Way, Suite 400, Orange Park, FL 32073  
888-268-8770 · 904-278-0524 - [info@techwell.com](mailto:info@techwell.com) - <https://www.techwell.com/>

# Gene Gotimer

## Coveros, Inc.

Gene Gotimer is a senior architect at Coveros, Inc., a software company that uses agile methods to accelerate the delivery of secure, reliable software. As a consultant, Gene works with his customers to build software better, faster, and more securely by introducing agile development and DevOps practices. He has many years of experience with web-based enterprise application design and a variety of development ecosystems, including continuous integration, continuous delivery, and DevOps. Gene feels strongly that repeatability, quality, and security are all strongly intertwined; each is dependent on the other two, which makes DevOps that much more crucial to software development.



# A Definition of Done for DevSecOps

Gene Gotimer, Coveros  
@CoverosGene

## About Coveros



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

### Areas of Expertise



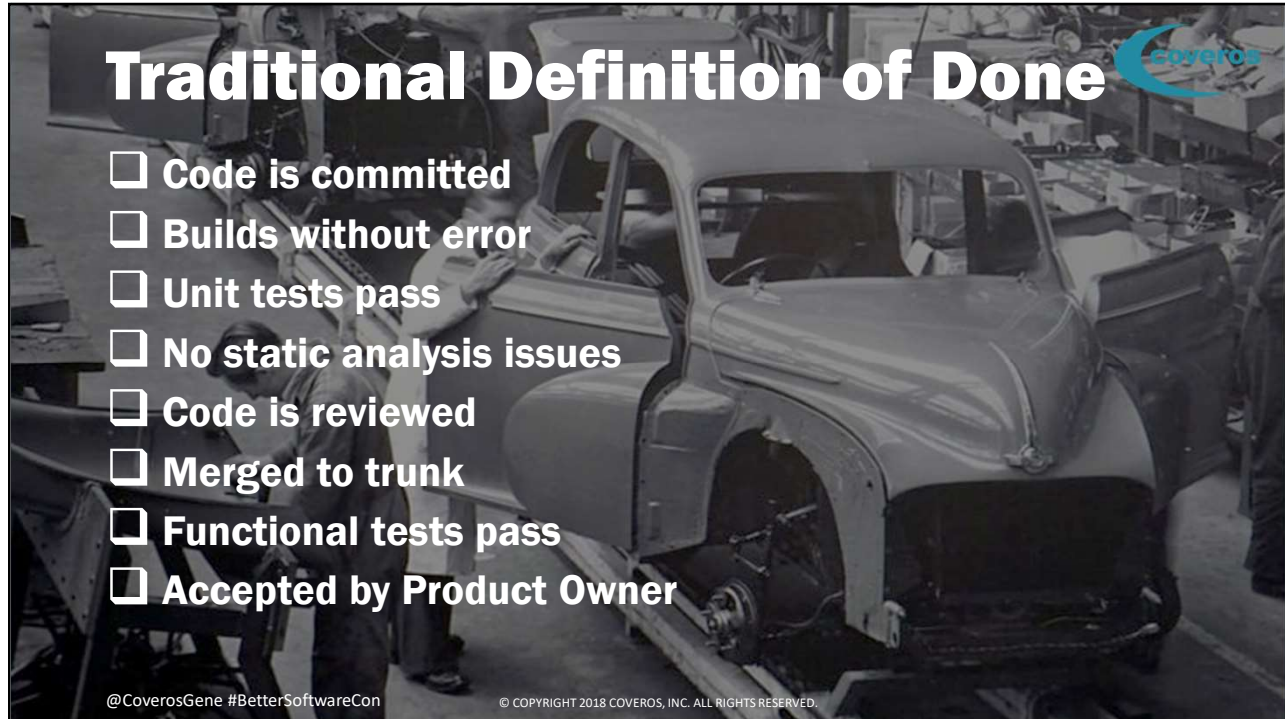
## Selected Clients

@CoverosGene #BetterSoftwareCon  
 © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.

## Definition of Done

- Checklist
- Explicit and unambiguous
- Minimum amount of work to consider a story done
- Periodically reevaluated

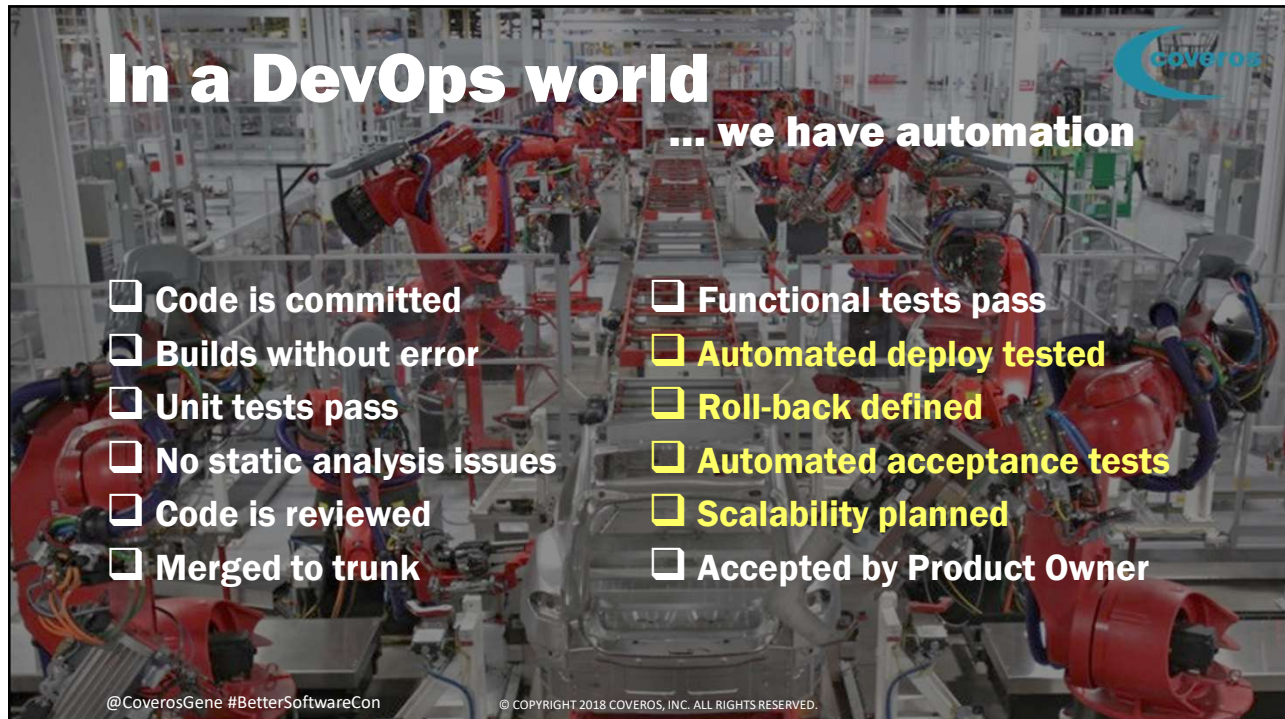
@CoverosGene #BetterSoftwareCon  
 © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.



## Traditional Definition of Done

- Code is committed
- Builds without error
- Unit tests pass
- No static analysis issues
- Code is reviewed
- Merged to trunk
- Functional tests pass
- Accepted by Product Owner

@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.



## In a DevOps world

... we have automation

- Code is committed
- Builds without error
- Unit tests pass
- No static analysis issues
- Code is reviewed
- Merged to trunk
- Functional tests pass
- Automated deploy tested
- Roll-back defined
- Automated acceptance tests
- Scalability planned
- Accepted by Product Owner

@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.



# Do we have a viable candidate for production?



@CoverosGene #BetterSoftwareCon      © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.



# I hate DevSecOps! (the term)



@CoverosGene #BetterSoftwareCon      © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.      8




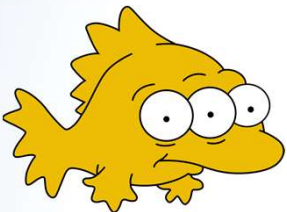

# Security is




@CoverosGene #BetterSoftwareCon


© COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.

# MUTATION TESTING

```
public int foo(int i) {
    i--;
    return i;
}
```

pitest.org



@CoverosGene #BetterSoftwareCon

© COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.

10

# Let static analysis help

The image features a background of a hand skeleton. Overlaid on this are several static analysis tool logos: PHP Mess Detector (with a magnifying glass icon), a red bug icon, SonarQube (with a blue signal icon), PMD (with a gun icon and the text 'DON'T SHOOT THE MESSENGER'), Find Security Bugs (with a bug icon), and Pylint (with the Python logo and the text 'Star your Python code!'). The Coveros logo is in the top right corner.

@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.

# Peer review the code



The image shows a hand giving a thumbs up gesture. Surrounding the hand are six colorful speech bubbles containing the following text: Encryption (purple), Authentication and authorization (red), Input validation (orange), Output encoding (yellow), Error conditions (green), and Architecture (blue). The Coveros logo is in the top right corner.

@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED. 12






**Test that each kind of user can do what they are supposed to, and can't do what they aren't supposed to**

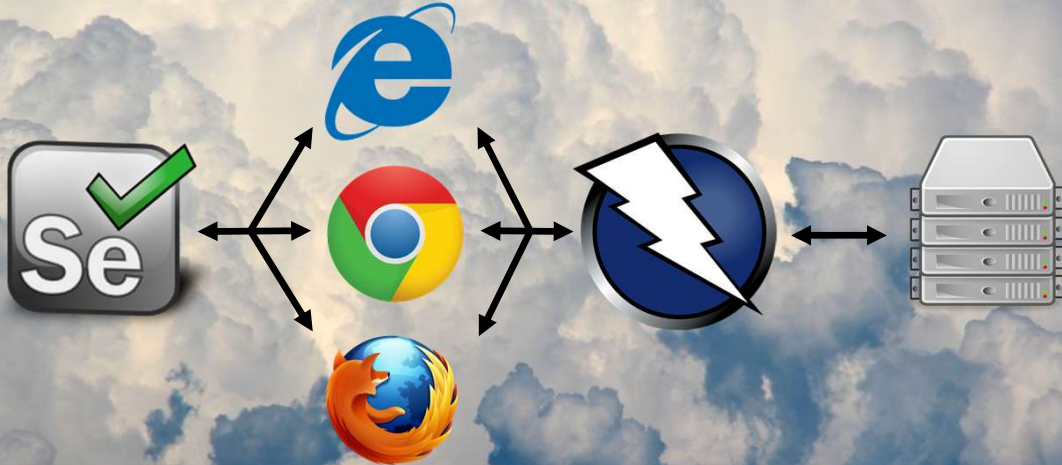


**User role testing**

@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED. 13



# Security scanning



The diagram illustrates the flow of security scanning. On the left is the 'Se' icon with a green checkmark. Three arrows point from it to the logos for Internet Explorer, Google Chrome, and Mozilla Firefox. From these browser logos, three arrows point to a circular icon containing a white lightning bolt on a dark blue background, representing a security warning or vulnerability. A final arrow points from this warning icon to a stack of server hardware.

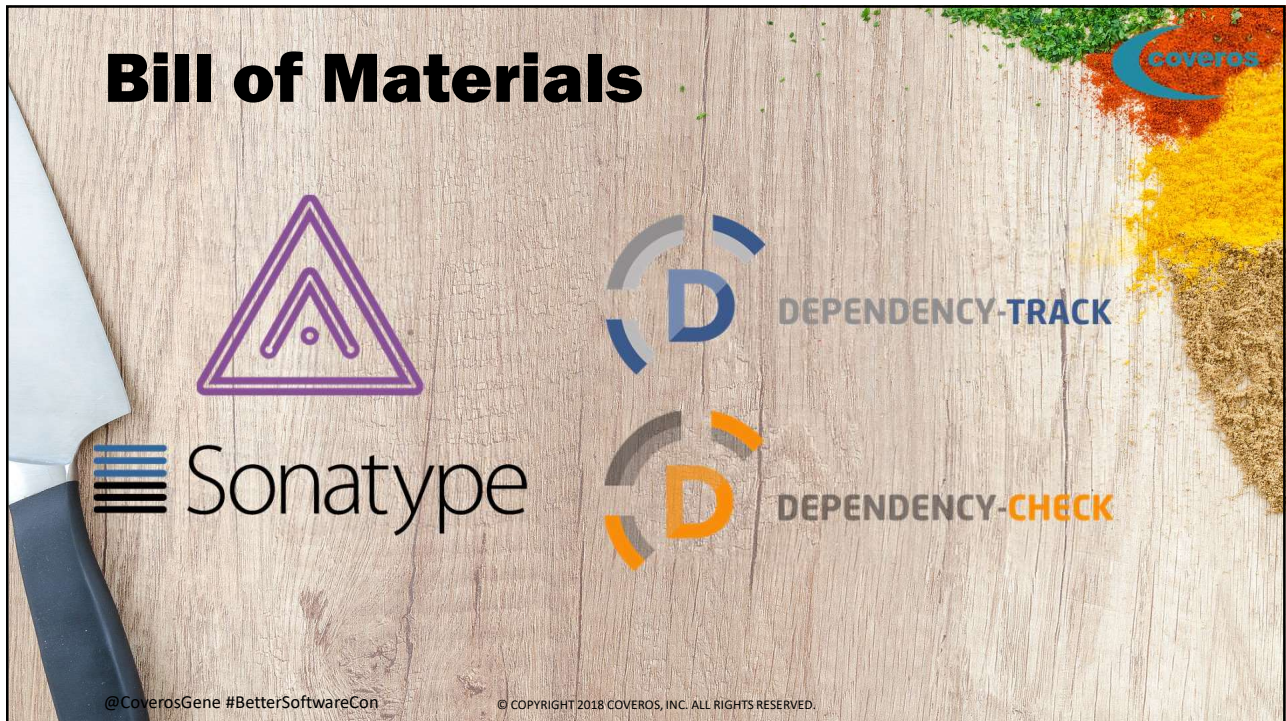
@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.






    

**Repeatable, reliable deployments**

@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.





**Bill of Materials**


**Sonatype** **DEPENDENCY-TRACK** **DEPENDENCY-CHECK**

@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.

# Update your system





Windows Server Update Services



**ATTENTION!**

Working on updates  
11% complete

Don't turn off your computer



yum  
yellowdog updater modified

@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.



OpenSCAP



Fail2Ban

# Lock down the system

@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.



# Monitor your logs

splunk > New Relic®

elastic +  + kibana

Nagios® DATADOG

## and the app and server

@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.



# Assess the risk

## STRIDE


- Spooing Identity
- Tampering with Data
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

## DREAD

- Damage Potential
- Reproducibility
- Exploitability
- Affected Users
- Discoverability

@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.


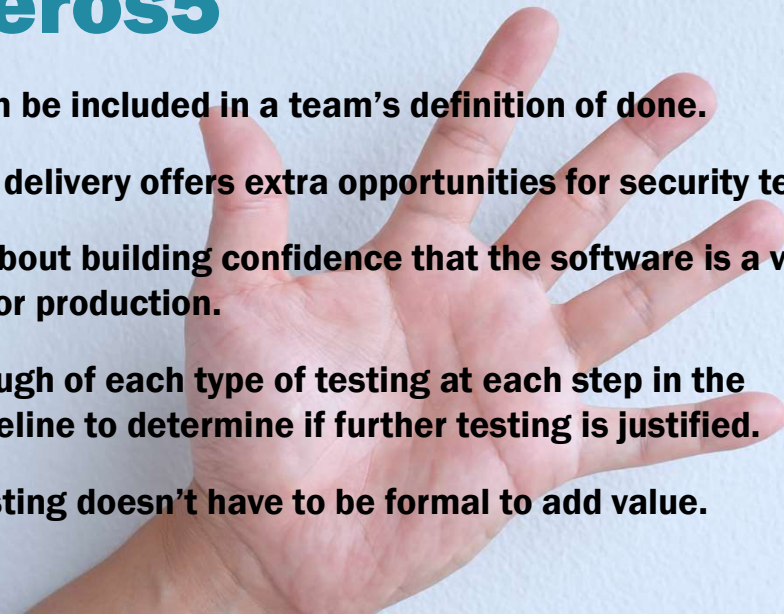
## DevSecOps Definition of Done



- Code is committed
- Builds without error
- Unit tests pass
- Mutation coverage goal met
- No static analysis issues
- No vulnerable components
- Code is reviewed
- Merged to trunk
- Functional tests pass
- Automated deploy tested
- Roll-back defined
- System packages updated
- Servers hardened
- User roles regression tested
- No security issues found
- Automated acceptance tests
- Scalability planned
- Logs and app monitored
- Risks assessed
- Accepted by Product Owner



@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.

## #Coveros5

- Security can be included in a team's definition of done.
- Continuous delivery offers extra opportunities for security tests.
- DevOps is about building confidence that the software is a viable candidate for production.
- Do just enough of each type of testing at each step in the delivery pipeline to determine if further testing is justified.
- Security testing doesn't have to be formal to add value.

@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.



**Reflect.**  
**Consider your situation.**  
**Keep improving.**

@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED.



*Please fill out an evaluation form.*

**Questions?**

**Gene Gotimer**  
**gene.gotimer@coveros.com**  
**@CoverosGene**

@CoverosGene #BetterSoftwareCon © COPYRIGHT 2018 COVEROS, INC. ALL RIGHTS RESERVED. 24