ALL DAY DEVOPS

NOVEMBER 6, 2019

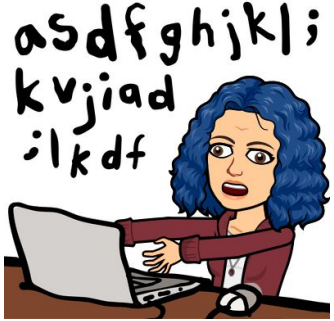
The Science of Compliance

Early Code to Secure your Node

judy johnson
Software Engineer
Onyx Point
@miz_j

About the Speaker

- Programming since the 19XXes when my Dad brought home a PDP-8
- Software engineer for [many] years - Hardware Control, Digital Signal Processing, SatCom, now Security Framework
- Various job titles: Software Engineer, Systems Engineer, Project Manager, ScrumMaster, and a Record Store Clerk
- Onyx Point since 2015
- Interests - baking, hockey, rock concerts, reading, volunteering (especially in events that promote diversity in tech)



So… why is DevOps so important to me?

- Cooperation
- Communication
- Repeatability/Consistency
- Efficiency

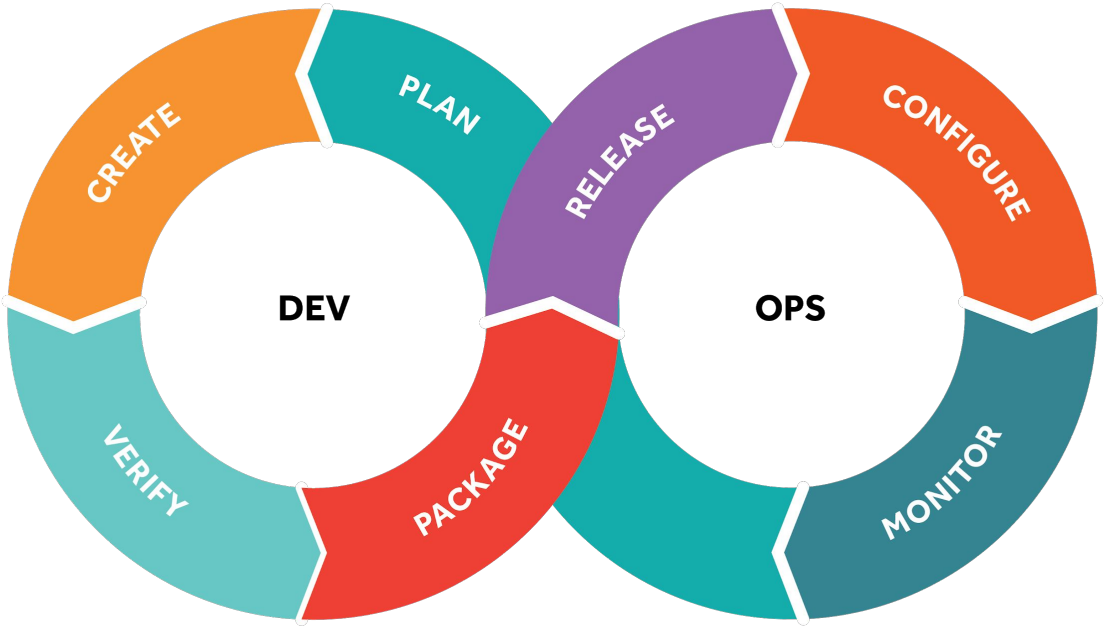
© 123RF

...and why is baking so important to me?

- Fun activity with family and friends
- Stress relief
- Enables creativity
- Makes people happy
- “Practice makes perfect”
- Makes a great analogy to continue through this talk...

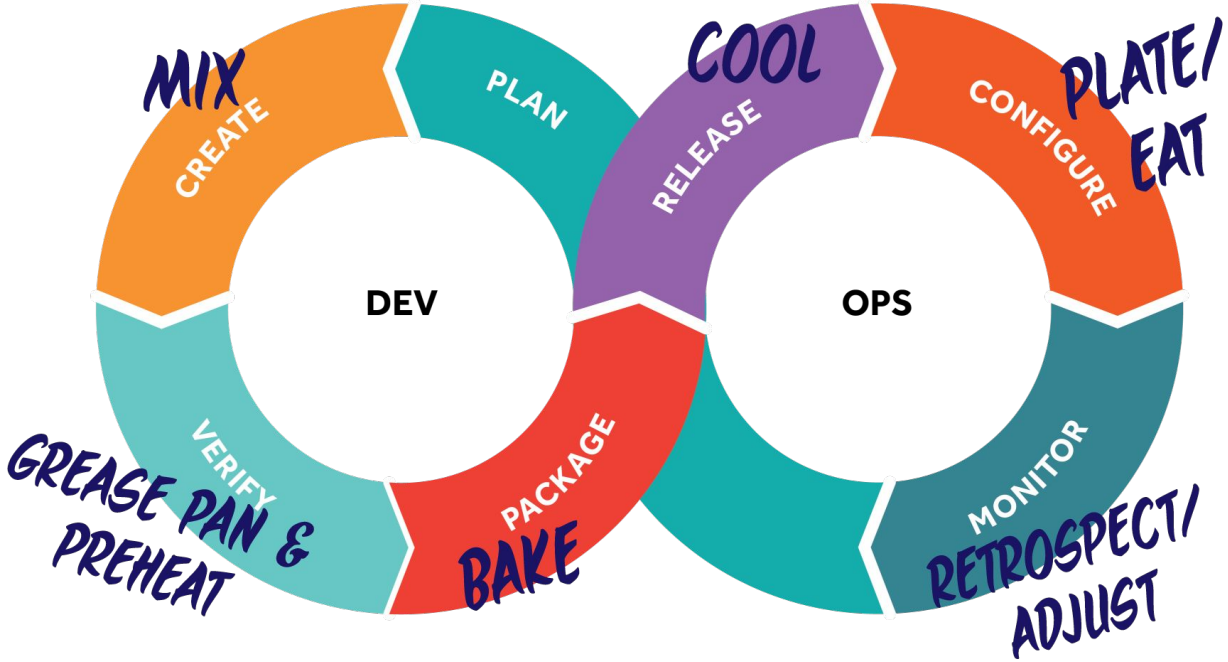
ADDO
ALL DAY DEVOPS

The DevOps Cycle



ADDO
ALL DAY DEVOPS

The Baking Cycle

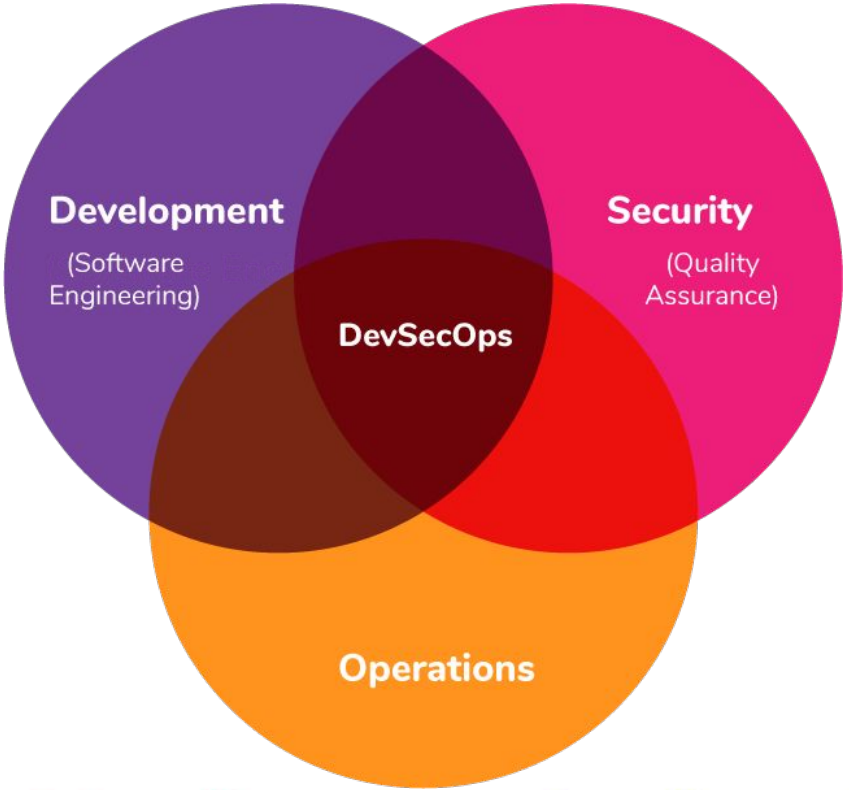


What is DevSecOps?

"DevSecOps means thinking about application and infrastructure security from the start. It also means automating some security gates to keep the DevOps workflow from slowing down.

However, effective DevOps security requires more than new tools—it builds on the cultural changes of DevOps to integrate the work of security teams sooner rather than later."

(from RedHat)



...what does the “Sec” in the middle mean to me?

- “In high-performing organizations, everyone within the team shares a common goal - quality, availability, and security aren’t the responsibility of individual departments, but are a part of everyone’s job, every day.” - Gene Kim
- Of course security should be part of continuous improvement
- But is the “Sec” necessary, or implied?

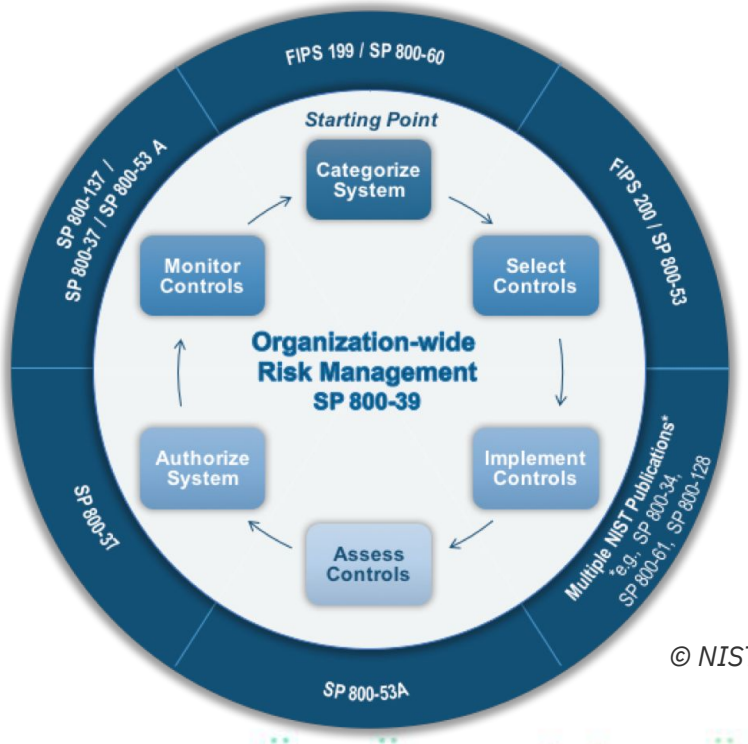
DevSecCodeTestRunDeployMLEtcOps

Security vs Compliance

	PROVABLE	DISPROVABLE
SECURITY	X	✓
COMPLIANCE	✓	✓

- Compliance - enforcing a defined/testable set of rules
- Security - ensuring that your system is not vulnerable
- Both are attempts to minimize risk

Risk Management Framework



Baking and Compliance

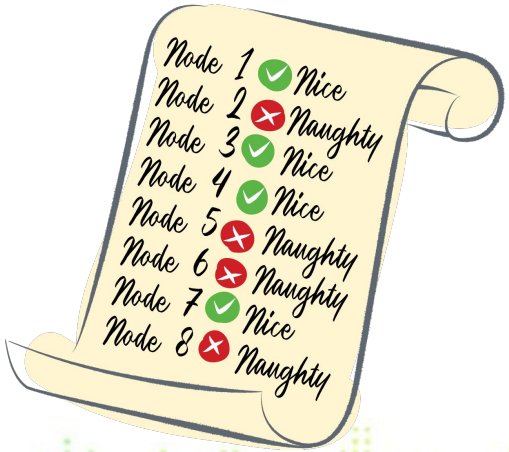
- Compliance is following the recipe
- Correct controls (temperature, measurement, etc), create consistent, predictable product
- A “typo” or incident could ruin your product
- Substitutions - are they valid?
- Mistake? Learn and document
- Minimizing Risk - Follow instructions, Document anomalies

Why do we need compliance?

- Improve Security
- Implement of security concepts in a provable way
- Maintain Trust/Integrity
- Maintain Consistency (process management)
- Maintain Control

How do you know you are Compliant?

- Out-of-the-box testing tools based on a specific set of rules (e.g.Nessus, OpenScap, OVAL)
- Toolkits to test compliance status - more flexible (e.g. InSpec, ServerSpec)
- Manual tests
- Compliance tests from scratch



How do you know you are Recipe Compliant?

- Did your cake rise?
- Were your cookies the right consistency?
- Were your “auditors” - (friends, family, co-workers) satisfied with the product?
- Is the house on fire?

© 123RF

Typical Process - Old School

- Requirements Created
- Code Written
- Code Reviewed and Tested
- Security Team runs Tests
- An action plan may be written
- Code is rewritten/re-reviewed/re-tested

- New requirements - do we learn from mistakes?

ADDO
ALL DAY DEVOPS

Ideal Process

- Code and Compliance Requirements Created
- Compliance & Code Written simultaneously
- Compliance code shared/reused
- Compliance tickets reside with target code tickets
- ALL Code Reviewed and Tested
- ALL Code is rewritten/re-reviewed/re-tested

ADDO
ALL DAY DEVOPS

Hardening your O/S

- Hardening begins with O/S
- Non-compliant code will be exposed early
- Development platform has the same rules as target platforms
- Compliance issues and fixes are found early and shared early
- Items such as disk and data encryption, which are hard to add later, are set early

Ensuring your systems are Compliant

- **Development** - Eliminate some of the threats immediately
  - e.g. ports, encryption

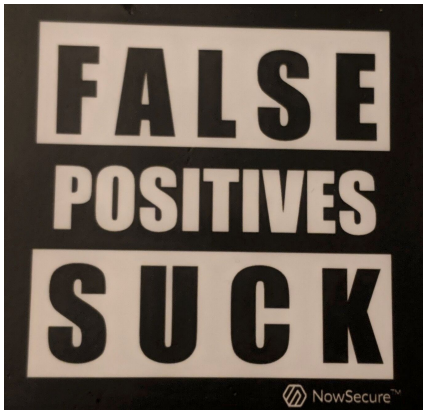
- **Test** - Testing framework and platform (CI)
  - test under varying conditions
  - test all components together
  - last chance to catch issues before code goes live

- **Production** - Your production environment is open to threats
  - “Chaos Monkey”-like tools randomly test for various issues
  - canary deployments and feature flags (small sample)

Adding Compliance to Testing

- Acceptance tests - Beaker/VM/Container tests
- Chef's Inspec
- Manual testing
- Static code analysis tools
- Dynamic code analysis tools

- Use the tools you have!

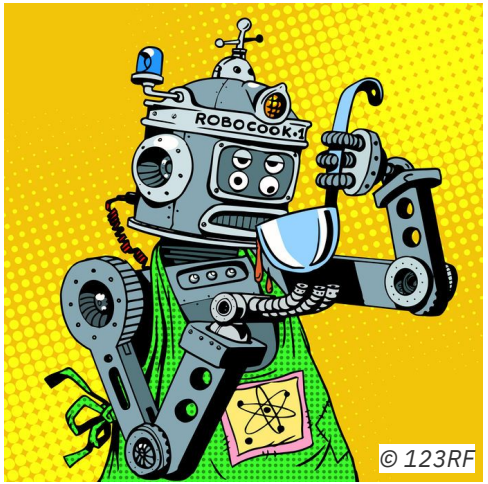


Compliance Testing in CI

- Passing once is not enough
- Ensure that your automated tests (spec, acceptance, integration) run with every check-in and/or periodically

Continuous testing of your recipe

(check out this great video https://www.youtube.com/watch?v=rfROcNPsb3w)



Tools for Correction

Compliance

- Puppet
- Salt
- Ansible
- Chef
- Any programming language, script, manual

© 123RF

Recipe

- Cake mix (customize within constraints)
- Pre-mixed spices
- Frosting to cover up any goofs
- Salt ;-)

© Paul Prudhomme

OK, it’s passed all the tests, and I’ve deployed...

- Puppet
  - Ensures your setup remains solid by running every 30 minutes (or predetermined)
- Cron job or CI tool
  - Can recheck and reset if there is an issue
- Ensure that reoccurring issues are documented and addressed

Sample Commercial Tools - Development Stages

- SCA – Software Composition Analysis - Dependency Check, Blackduck, NexusIQ, SourceClear, Whitesource
- SAST - Static Application Security Testing (White Box Testing) [Source Code Check] – SonarQube, Veracode, Checkmarx, Coverity, Fortify, and language-specific tools Brakeman (Ruby), Bandit (Python)
- DAST - Dynamic Application Security Testing (Black Box Testing) [running app] - Burp, Zap, Sn1per, Nikto, WebInspect, AppScan, Acunetix, Netsparker

thanks, Thaddeus @thaddeuswalsh)

Other types of tools

- Infrastructure Vulnerability Management – Tenable, Qualys, Rapid7, OpenVAS
- Container – Clair, Trivy, Aqua, Twistlock
- Cloud - Prowler (AWS assessment tool)
- Database scanner - SQLmap (open source SQL Injection and db takeover tool),

(tool listings thanks to

Thaddeus @thaddeuswalsh)

My baking slide (1)

Carrot Cake

- 1 1/2 cups corn oil
- 2 cups sugar (not salt :))
- 3 eggs
- 2 cups flour
- 1 1/2 teaspoons cinnamon
- 2 teaspoons baking soda
- 2 teaspoons vanilla
- 1/2 teaspoon salt (not sugar :))
- 2 cups grated carrots
- 1 cup chopped walnuts

Combine all ingredients.

Pour in greased 13" x 9" pan.

Bake at 350 for 45 minutes.

Cool, frost.

- Carrot cake is one of my favorites!
- Vegetables and security - necessary evils to some
- Carrot - a vegetable and unexpected - are baked in, yet the cake is sweet and moist

My baking slide (2)

Cream Cheese Frosting

- 3 oz cream cheese
- 1 2/3 cups confectioners sugar
- 1/8 teaspoon salt
- 1 teaspoon vanilla

Combine all ingredients. Beat until creamy.

Spread on cake.

- Imagine the frosting as your app.
- Solid base - add your personal touch
- Ensure that you do not alter the foundation that the cake has created when you personalize it

ADDO
ALL DAY DEVOPS

Summary...

- A secure O/S on development and all other platforms allows you to start with an advantage
- Compliance testing can - and should - be done at all stages of your CI
- Watch your test tool - there can be false positives as well as false negatives
- A tool such as Puppet or Cron can run (or run scripts) at regular time increments to check your compliance, and alert you if something needs correction
- Correction can be done with an automated tool or manually
- Ensure that security is integrated into your team and process
- **No matter what you are creating, remember to bake in the goodness!**

Thanks!

Thanks!

To co-workers who teach me every day, and peer review my code, documents, and cookies… to family and friends who inspire me daily… to the friends who helped me put this together and make it pretty

Thanks AllDayDevOps!

Never stop learning – and make sure you have time to spend on things you enjoy!

ADDO
ALL DAY DEVOPS

SPONSORS

Sponsorship packages for All Day DevOps are available. If your organization is interested, please contact us for details.

DIAMOND SPONSORS

GOLD SPONSORS

COMMUNITY ADVOCATES AND VIEWING PARTY SPONSORS

MEDIA SPONSORS