RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: ASD-F01

How Security can be the Next Force Multiplier in DevOps

Andrew Storms

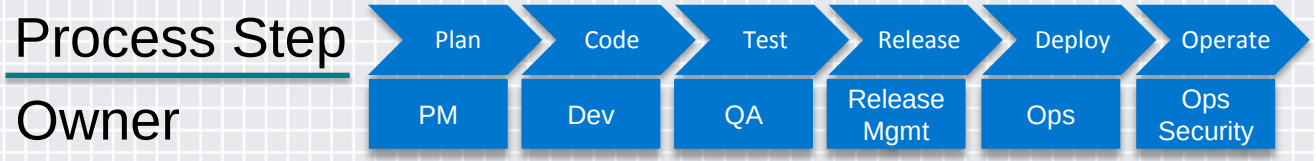
VP, Security Services
New Context
@St0rmz

Make security the reason for DevOps adoption

- Software development challenges
- DevOps doesn't address secure coding challenges
- Its our duty to affect change in DevOps
- Security embedded in DevOps, makes DevOps better
- Don't fear DevOps – Know the people, processes and tools
- Find your positive entry points
- Making a plan

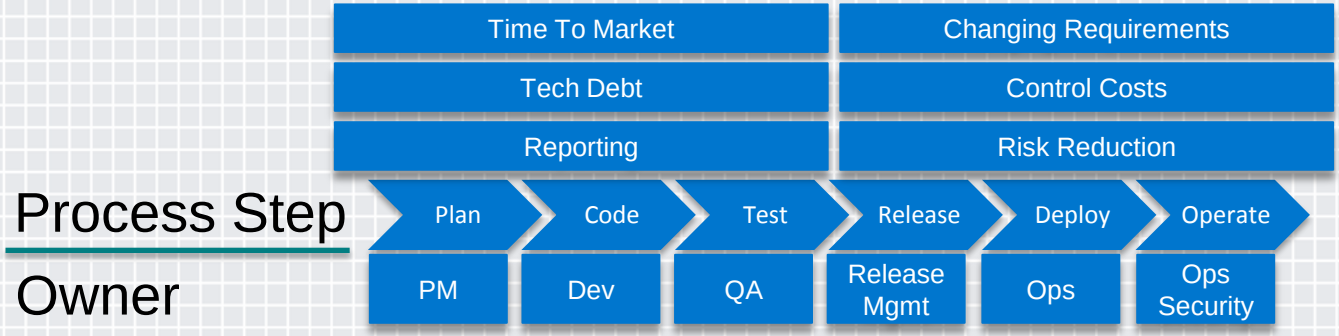
Software Development Challenges

- Non DevOps software development environment
  - Everything is separate



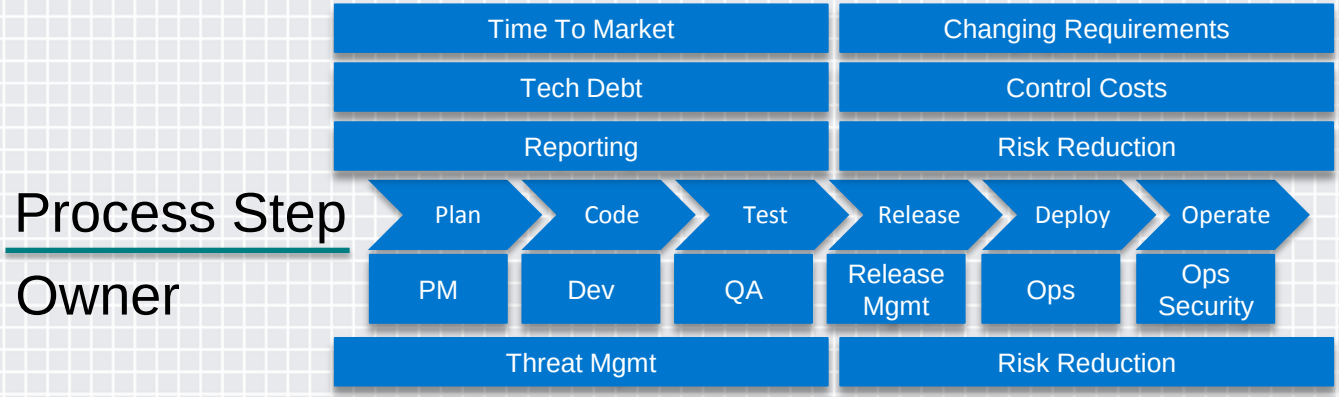
Software Development Challenges

- Downward business pressures

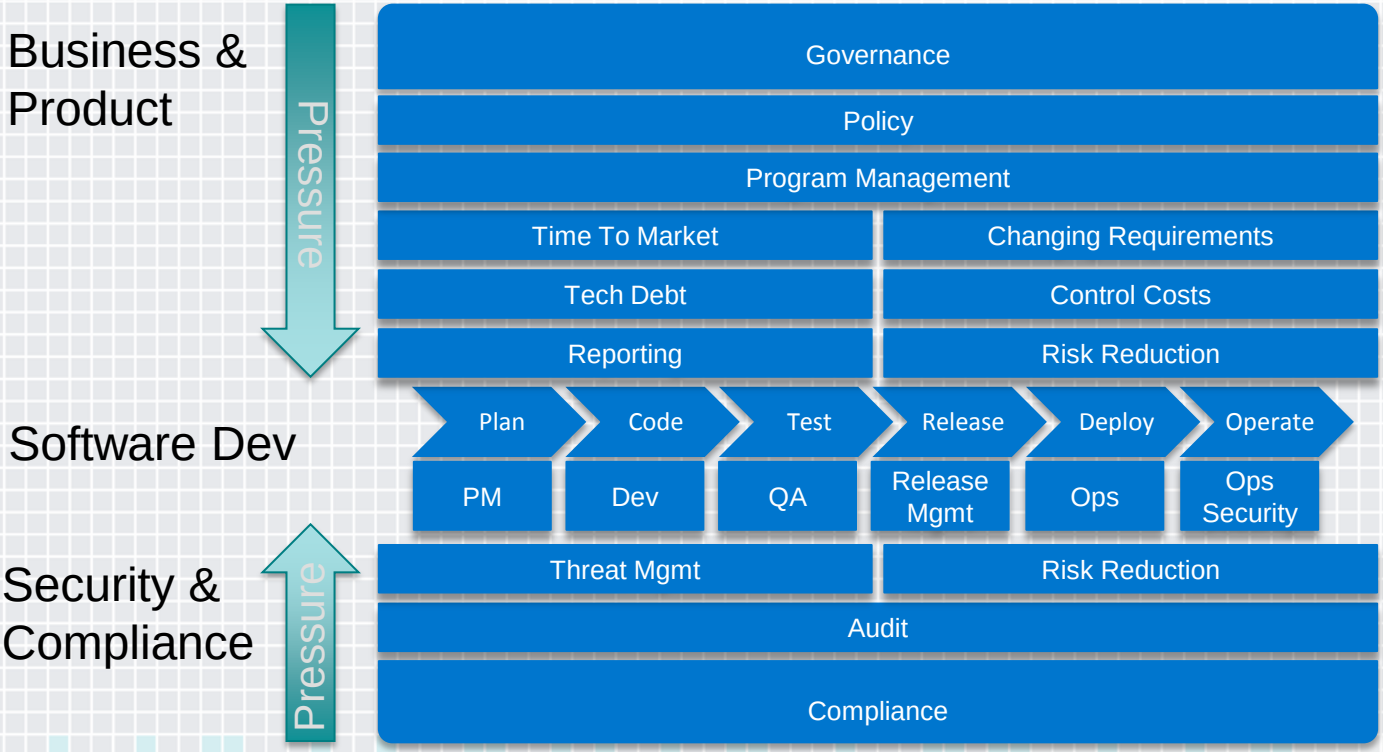


Software Development Challenges

- Upward security pressures

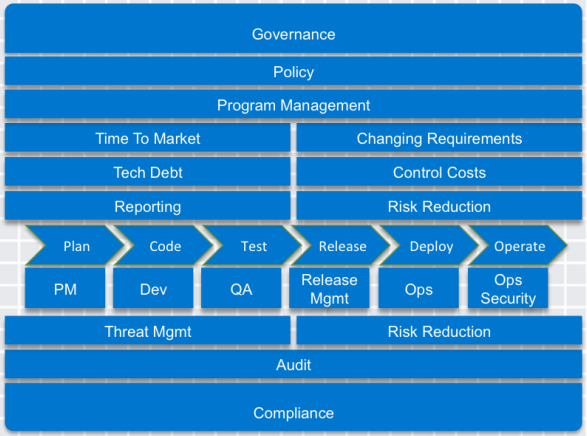


Software Development Challenges



Software Development Challenges

- External pressures
- Disjointed
- Costly
- Siloed
- Opaque
- Complex
- Always late, out of sync, fragile



Then along came the DevOps

Non DevOps

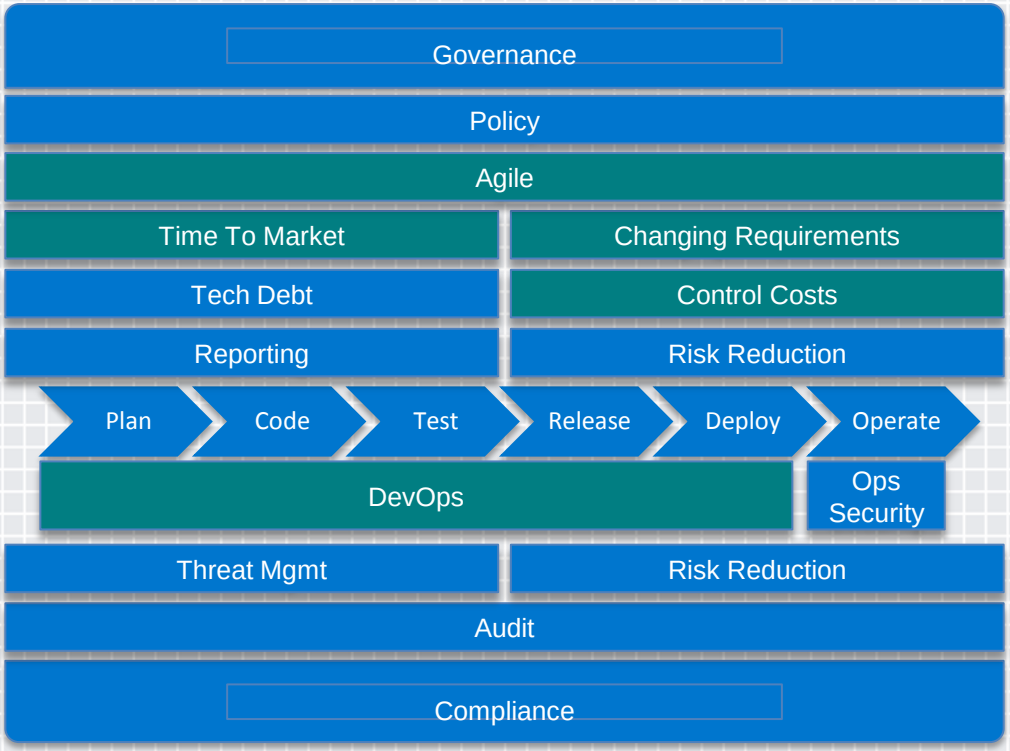
- Disjointed
- Costly
- Opaque
- Always late

DevOps

- Conjoined
- Lean
- Transparent
- Agile

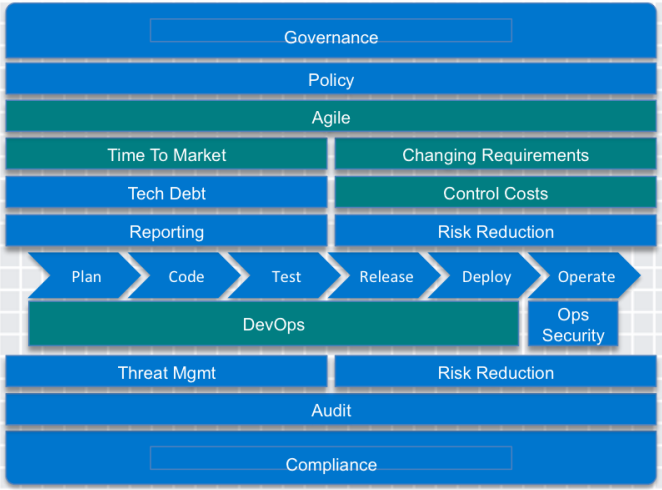
Then along came the DevOps

Green = DevOps



Then along came the DevOps

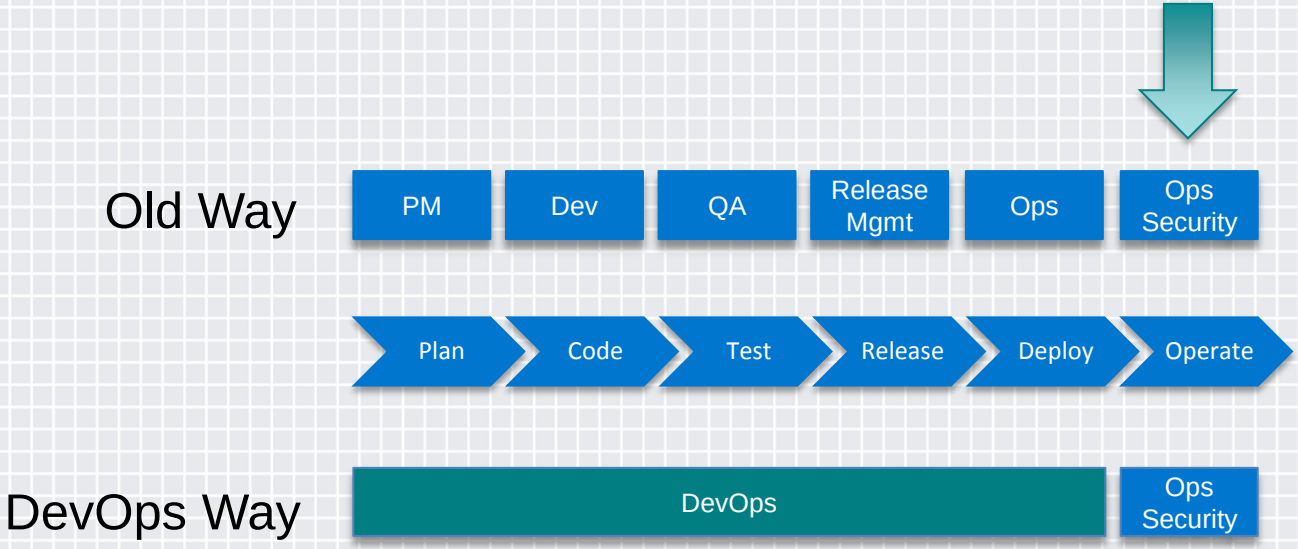
- Meets business & product needs
  - On time within budget
- Meets ops and dev needs
  - Agile, harmonious, consistent
- Fails to meet security needs
  - No attempt to deliver secure application code
  - Security still left out and left last



How popular is DevOps?

- Oct 2014 CA Technologies Survey
  - 88% respondents already have or plan to adopt DevOps in the next 5 years. (up from 66% on prior year)
  - Top obstacle (28%) to DevOps in their organization were security or compliance concerns
- Oct 2014 Rackspace Survey
  - 55% already implemented DevOps. 31% planning to implement DevOps within 3 years.
  - Primary driver for DevOps? Only 2% said audit or compliance

http://rewrite.ca.com/us/articles/devops/research-report--devops-the-worst-kept-secret-to-winning-in-the-application-economy.aspx
http://www.rackspace.co.uk/sites/default/files/devops-automation-report.pdf



Security is still the last guy

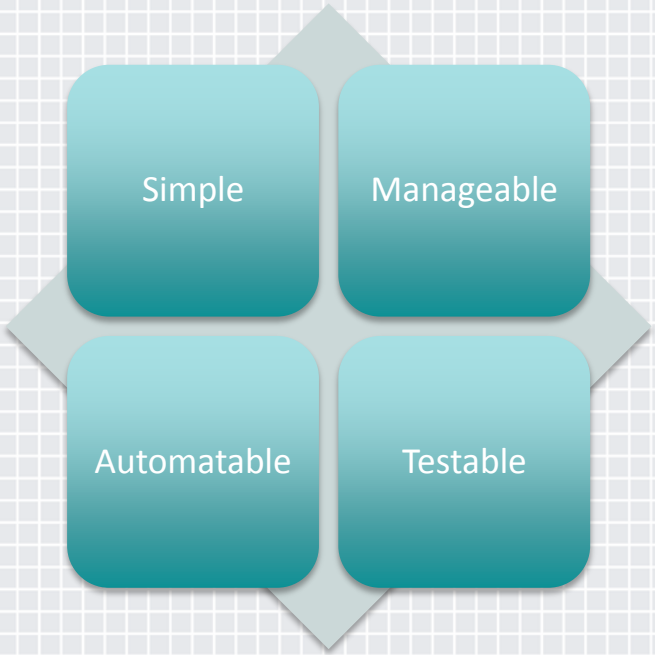
DevOps Kicks The Security Can Down The Road

DevOps Is Bad For Security

- Fast
  - ~50 deploys a day!
  - Faster to production = faster to be pwned
  - Too much complexity
- Unwieldy
  - Everyone has access to everything
  - Full stack engineers
  - Fewer test cases
- Deplorable
  - No audit
  - No control points
  - No process

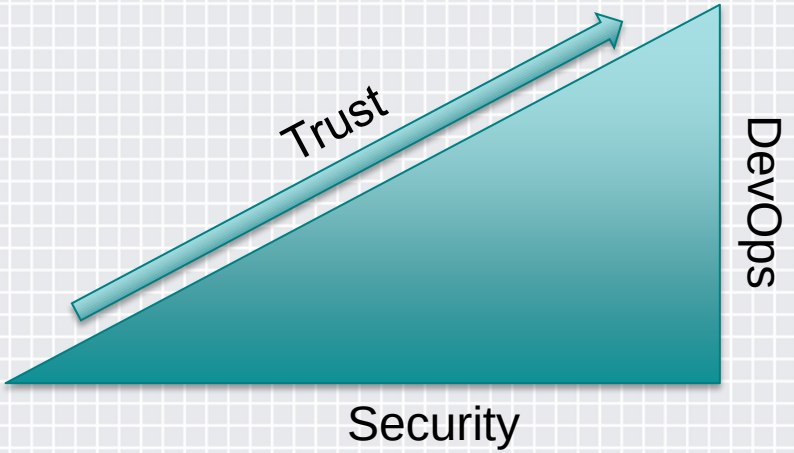
DevOps Is Good For Security

- Increases process insertion points
- Increases consistency
- Increases predictability
- Decreases time to change
- Increases audit ability
- Reduces costs
- Reduces waste



Security Is Good For DevOps

- Business enabler
- Transparency
- Trust
- Protects privacy
- Accountability
- Regulatory & audit



Let the people focus on their core competencies

Know Your Nemesis

Security Team

- Compliance
- Silos
- Change control
- FUD masters

DevOps Teams

- Security != compliance
- Open
- Lots of change
- Data scientists

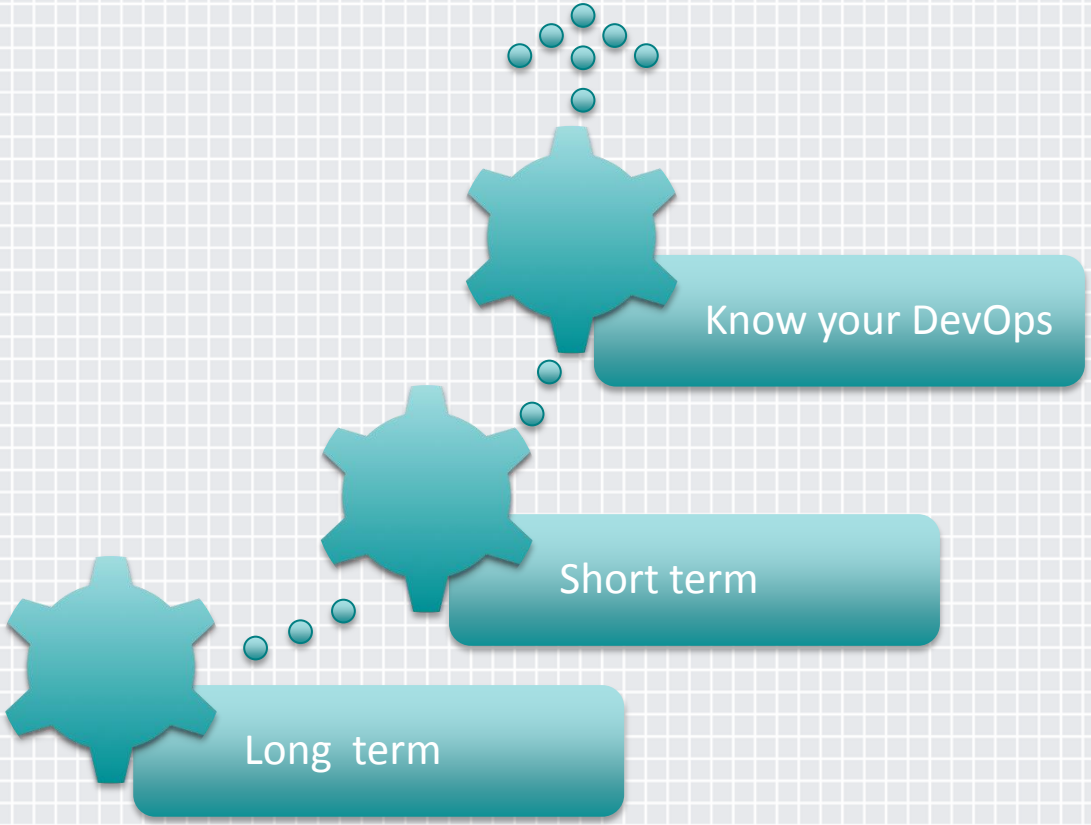
“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.” – Sun Tzu

How do we get these teams to work together?

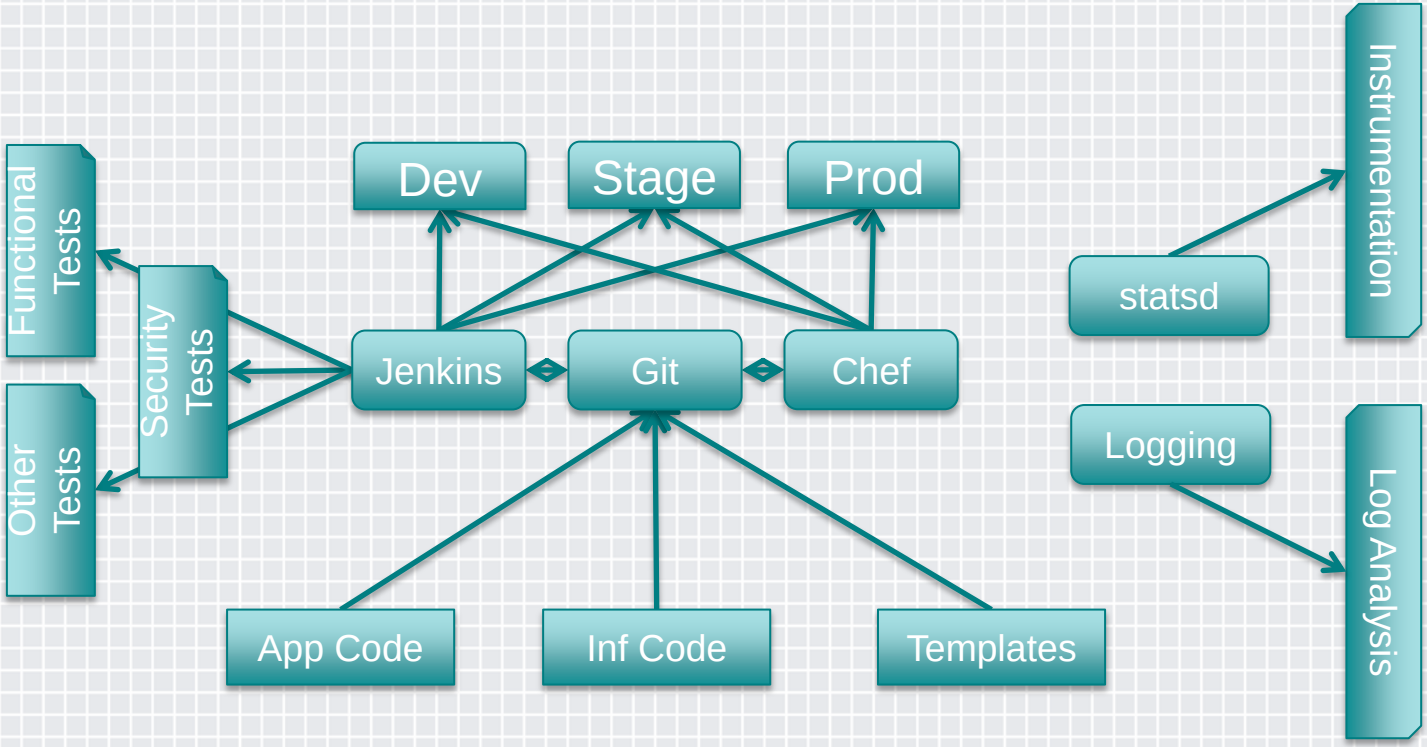
(Every DevOps presentation must have random gears image)

Action Plan

- Pipeline
- Tools
- Processes
- Today's todos



Apply Security Expertise to DevOps Pipeline



Security Makes DevOps Better - Tools

- Git (Source Code Management)
  - Make it the source of truth for everything
    - Sometimes people use Chef for revision control
  - Separate repositories for each cookbook
  - Branching strategy needs to support isolation, rollback, logging
  - Git Hooks
    - Enforce policy at commit time
    - Commit message, additional logging

GitHub

GITLAB

Security Makes DevOps Better - Tools

- Chef (IT Automation)
  - Continuous configuration & compliance
    - Write some code!
      - Map security controls to recipes
      - Apply technical controls. Ex: https://cipherli.st/
      - Add logging
  - Reduces complexity and helps out everyone
    - Ensures consistency (dev, stage, prod)
    - Makes audits easier (most of the time)

ANSIBLE

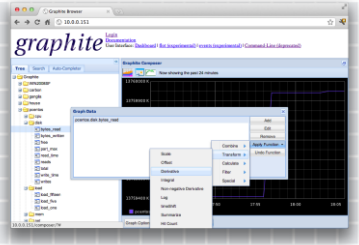
Security Makes DevOps Better - Tools

- Jenkins (Continuous Integration)
  - Automated code security test suites
    - Gauntlt (Ruby), Mittn (Python), BDD-Security (Java)
  - Infrastructure code too
    - Chefspec, test-kitchen
  - External security systems orchestration
    - Network scanners, fuzzers, sqlmappers
  - Test security policies and controls
    - No pass = no go

Security Makes DevOps Better - Tools

- Instrumentation
  - Business logic metrics also good for security
    - Number failed logins in last 24 hours
    - Site performance & availability
  - How do you measure risk management in DevOps?
    - Benchmarking
      - Security test coverage
      - Time to audit
      - Mean time to remediate

DATADOG

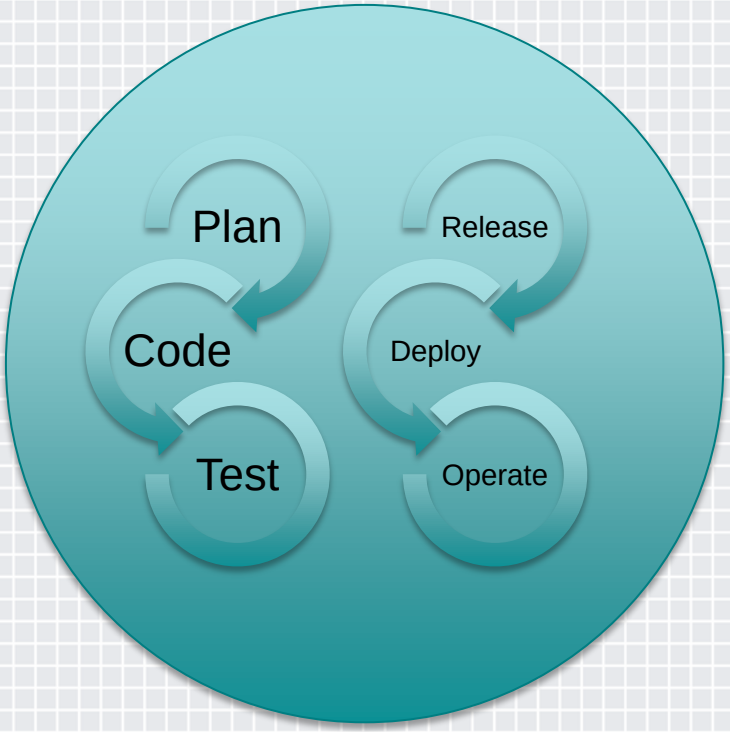


Grafana

Security Makes DevOps Better - Tools

- Monitoring
  - New Relic, PagerDuty, Boundry, Pingdom
  - Performance & availability
  - Create useful alerts and alert the right people
- Logging
  - Splunk, SumoLogic
  - Get your app team to log useful events
    - “There was an error”
    - “RabbitMQ tried to write to DB, but got error…”

Apply Security Expertise to DevOps Process



Security Makes DevOps Better - Process

- Policy
  - Does your SDLC include DevOps tools and process?
    - Definition of done
    - How do devs know they are meeting security requirements?
- Moving security earlier
  - Story review
  - Threat vector analysis
  - Security training
  - Design & architecture

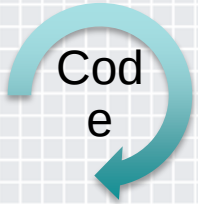
Security Makes DevOps Better - Process

Standards Enforcement

- Lint checkers
- Branching strategy
- Peer review

Get Involved

- Write code
- Attend stand ups
- Peer review
- Pair programming



Security experts can’t expect software experts to be security experts.

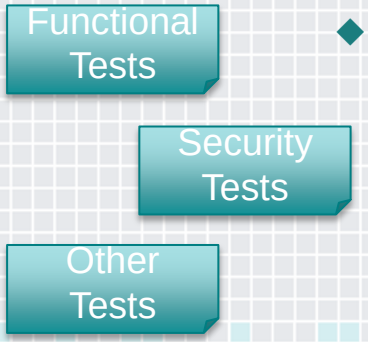
Security Makes DevOps Better - Process

Security Tests

- Behaviors
  - Lock the user out after x failures
  - Must use SHA-256
- Infrastructure
  - Port scans
  - User accounts

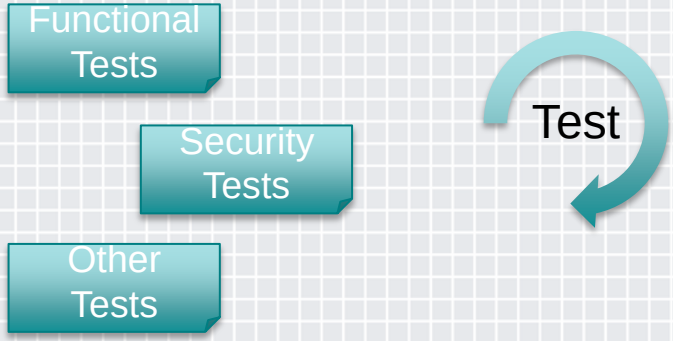
Non Functional Tests

- Performance (Availability)
- System readiness
  - Deploying using latest AMI
  - Latest OpenSSL



Security Makes DevOps Better - Process

- Make tests automated
  - Continuous integration with Jenkins
  - Pick a pluggable framework
- Use TDD
  - Automate security tests up front
- Done-Done includes security
  - What's the definition of done?



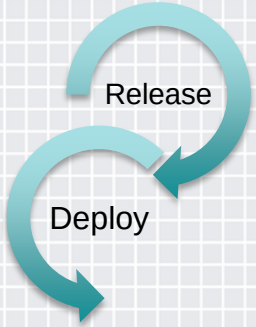
Security Makes DevOps Better - Process

Release

- Separation
  - Systems
  - Duties
  - “Here be dragons”
- Oversight
  - Approvals
  - 2-man rule

Deploy

- Change control mgmt
  - “Here be more dragons”
- Convey assurance
- Convey trust
  - What’s in the change log?
  - What tests were run?



What You Can Do Today

- Get acquainted with popular tools
  - Git, Jenkins, Chef, Statsd, New Relic, PagerDuty
- Read about new concepts
  - Agile, continuous integration, continuous deployment
  - Test driven development
- Think about metrics
  - What metrics are valuable to both DevOps & Security
- Get involved

Do Some Industry Research

- Security people are secretive
- DevOps people LOVE to talk and SHARE
- Watch some videos on YouTube
- Attend a DevOps conference
- Read some articles at devops.com

Remember To

- Be transparent
  - Good security is always transparent. DevOps will amplify opaqueness.
- Be measurable
  - DevOps breeds automation. Find where you can automate metrics.
- Embrace feedback loops
  - Attend retrospectives. Request feedback. Adjust as needed.
- Embrace iterations
  - Nothing is ever 100% done or 100% perfect.

Make DevOps Work For You

DevOps Says

- Collaboration
- Automation
- Agile

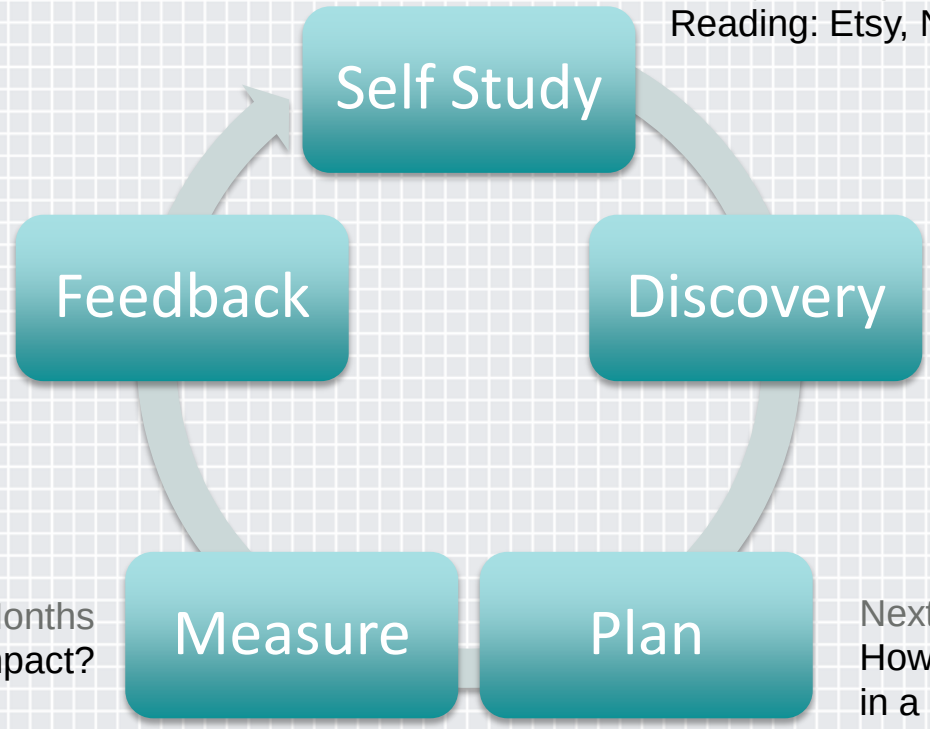
Security Says

- Everyone's responsibility
- Standards, reporting, benchmarks
- Risk management

Use DevOps to create the next generation information security program.

It might just be your only hope in combating the next cyber threat.

Make DevOps Work For You



Today's Assignment
Reading: Etsy, NetFlix

Next Week
What tools, people and processes are in use?

Next Month
How can you impact DevOps in a positive way?

3 Months
Have you made an impact?

3 Months
What can you do better?

Summary

- For many, Security is the after thought in DevOps
- Its your duty to affect change in DevOps
- Security embedded in DevOps, makes DevOps better
- Get to know the people, processes and tools
- Find your positive entry points
- Make a plan & measure the outcome

Q & A

Andrew Storms

@St0rmz

storms@newcontext.com

Devops.com