DEVOPS DONE…RIGHT?

now with 22% more security

ME

- Approach DevOps w/ InfoSec view.
- 20 years of IT
- Sys admin, product manager, consultant, QA tester, IT guy, PR guy
- Security advocate featured on CNBC, Forbes, Business Week, the Christian Science Monitor as well as many other publications.
- CISSP and graduate of the FBI citizens academy.
- @St0rmz
- DevOps.com
- Between jobs

DEVOPS DONE RIGHT?

- What the <bleep> is DevOps anyway?
  - Silo busting
  - Automation
  - Agile
- Everything is awesome

SECURITY IS BAD

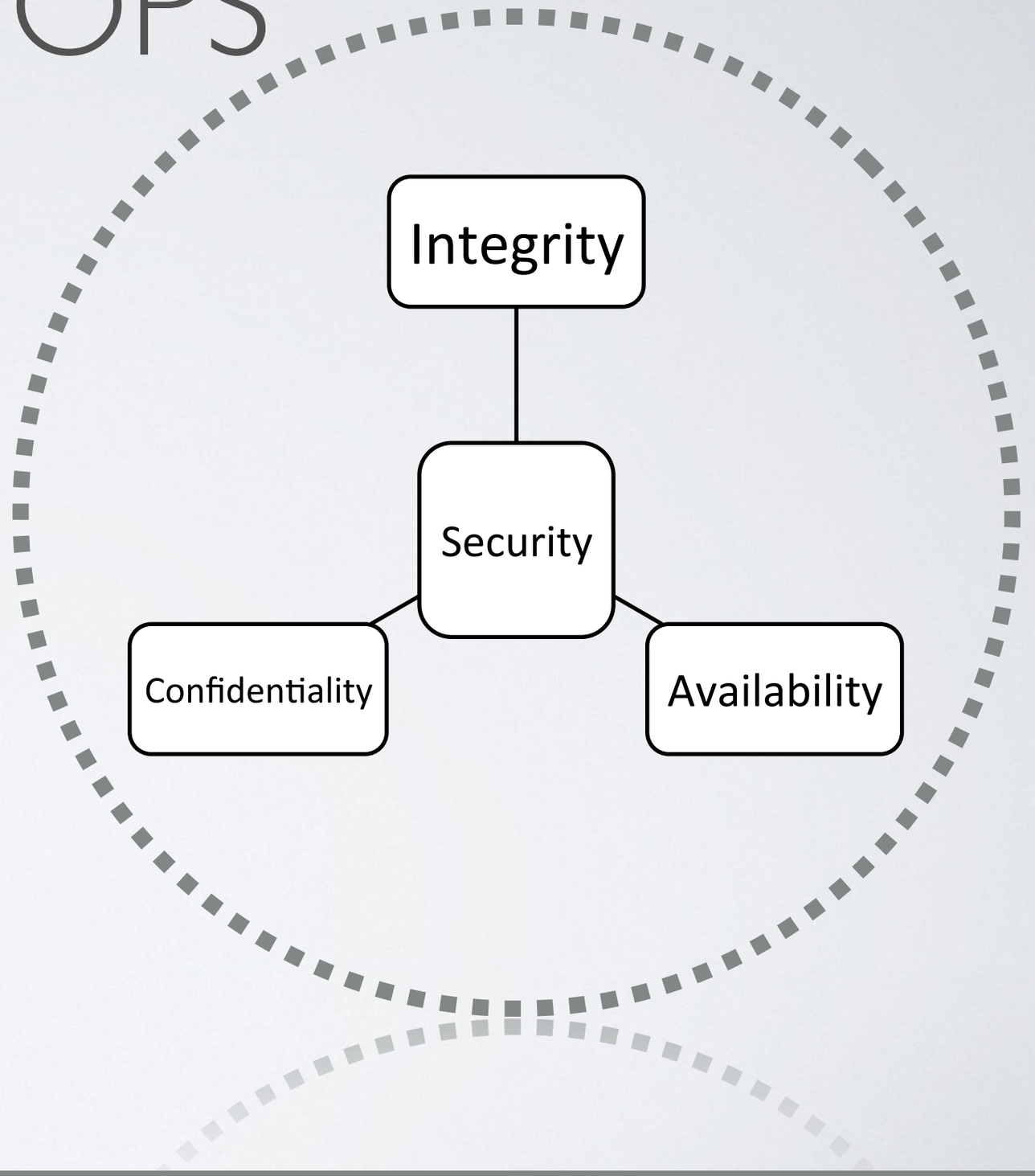
- Slows down progress
- Full of FUD
- Steal sprint points
- Too complicated
- Too controlling
- Too costly
- Interrupt driven
- Don't know Jack
- Cube critters
- Wrong kind of geek
- Too many "standards"
- Lack usable metrics
- Compliance != security
- Like silos

"Why do I care about security?"
"And what is security anyway?"
"What value does security have?"

—lots of people

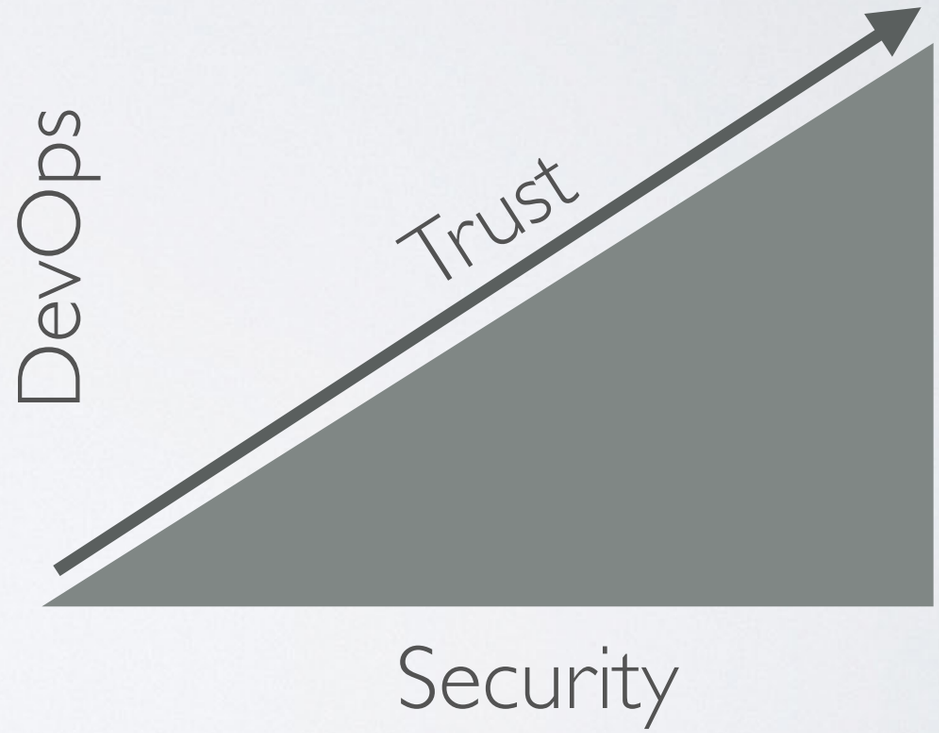
SECURITY GOOD FOR DEVOPS

- Transparent
- Business enabler
- Risk enabler
- Protect privacy
- Accountability
- Regulatory



DEVOPS GOOD FOR SECURITY

- Increases insertion points
- Increases consistency
- Increases predictability
- Increases time to change
- Increases audit ability

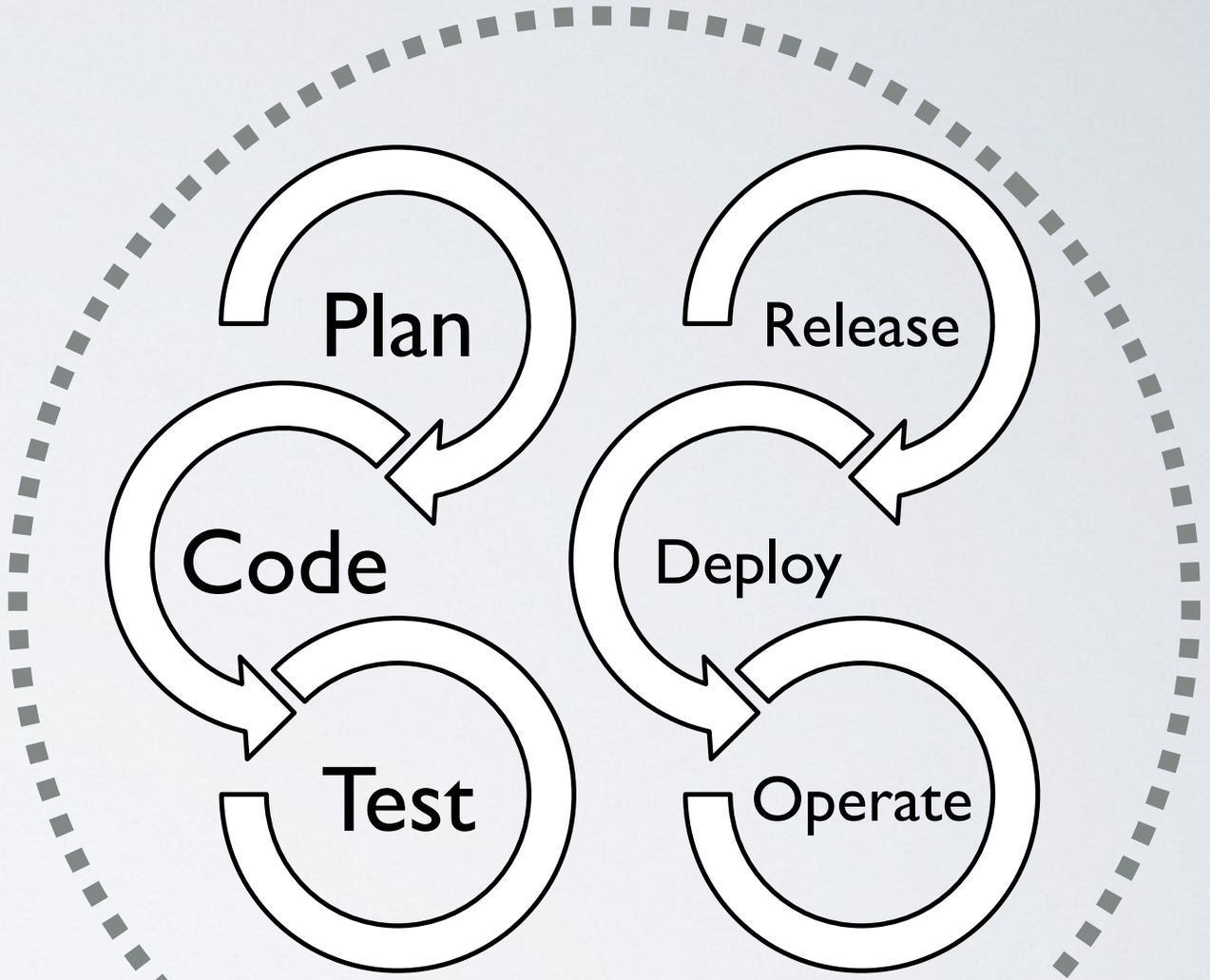


HOW?

- Security has to add value
- Security has to be malleable
- Security has to integrate into DevOps process

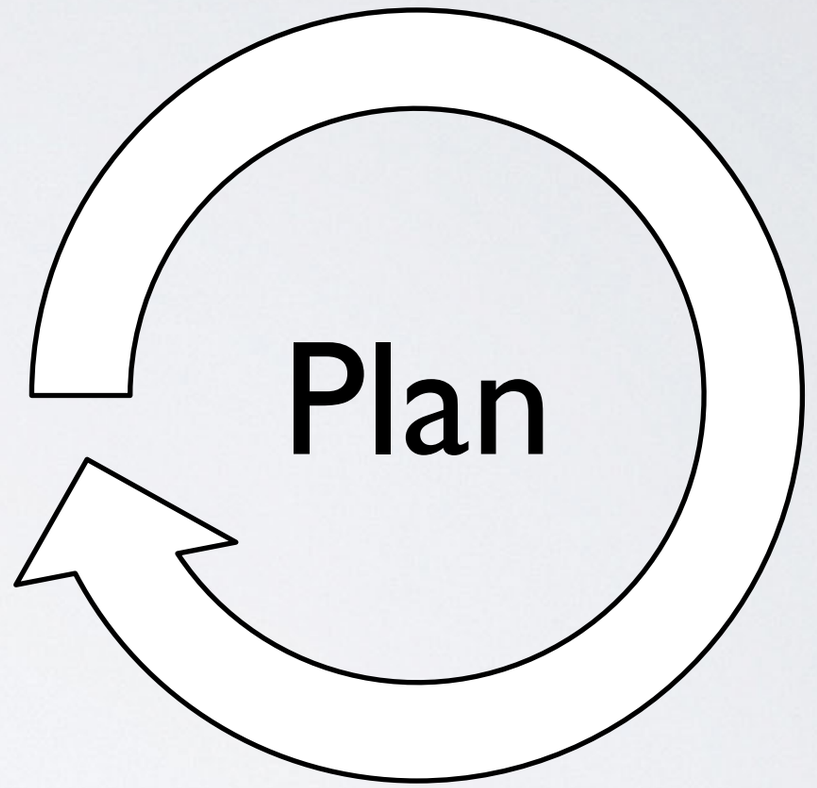
PROCESS

Find insertion points
Find value adds



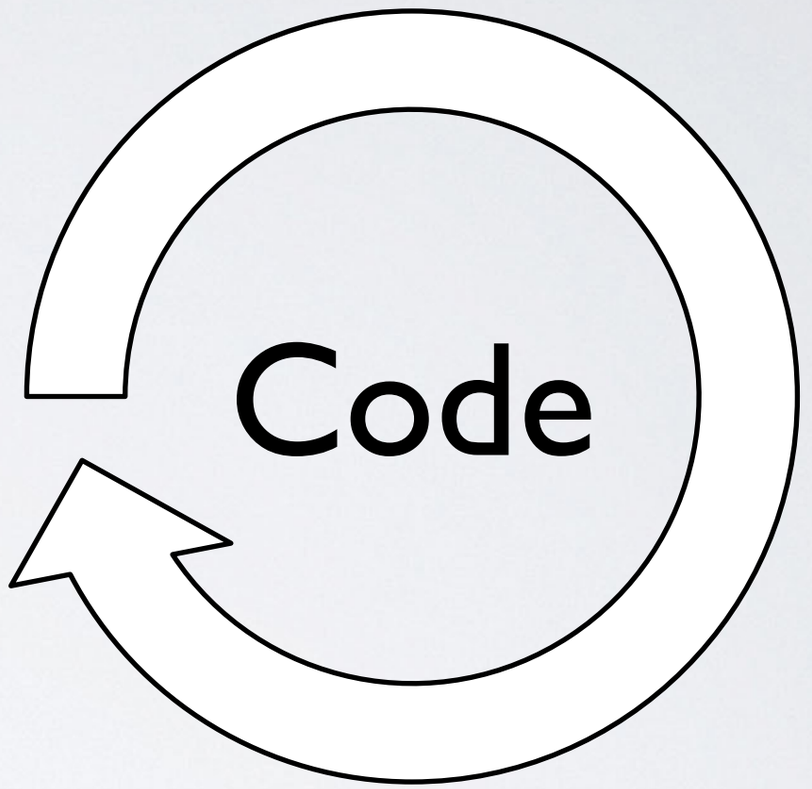
MOVING LEFT

Story review
Who is responsible?
Threat vector analysis
Design & architecture
Infrastructure changes
Security training



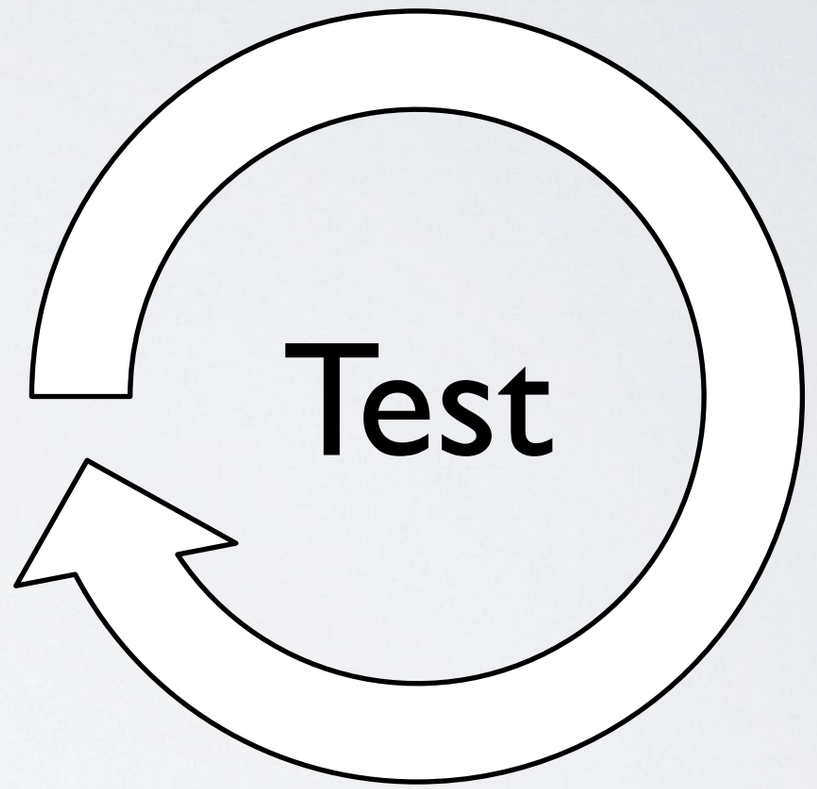
GET INVOLVED

Standards enforcement
Feature branching
Lint checking
Peer review
Static analysis
SDLC
Write some code!
Attend standups



ACCEPTANCE

Automated test suites
External code review
External app testing
Config Checks
Vuln checks

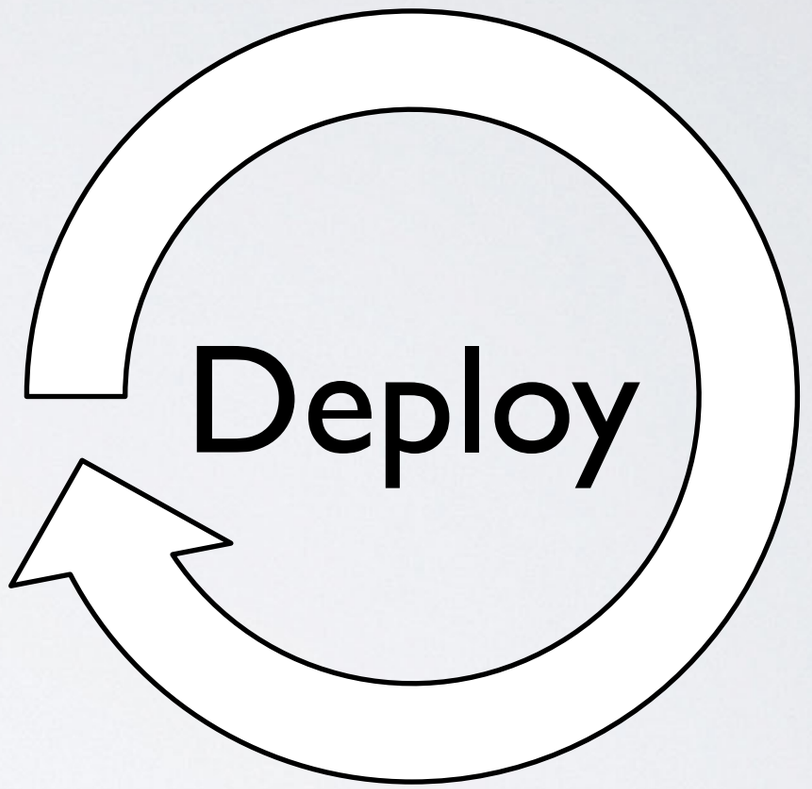


BE WISE

Separation of systems
Segregation of duties
Deploy testing
2-man rule
Approvals
Oversight

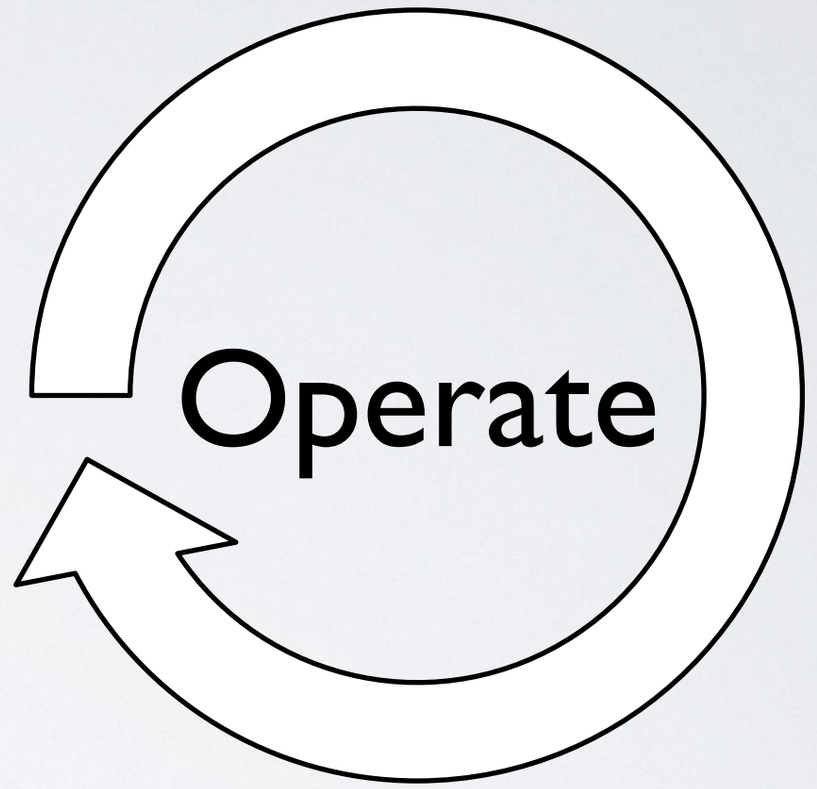
HANDS OFF

Change control mgmt
Assurance
Trust

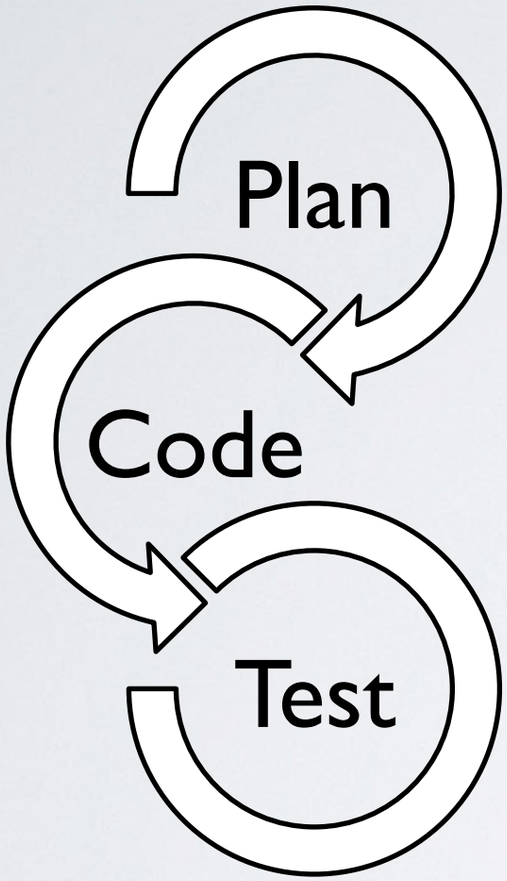


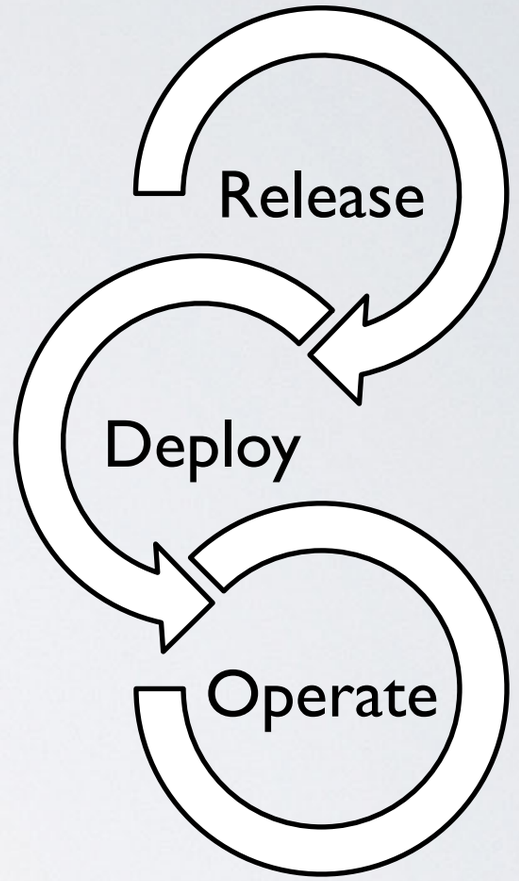
CONTINUOUS

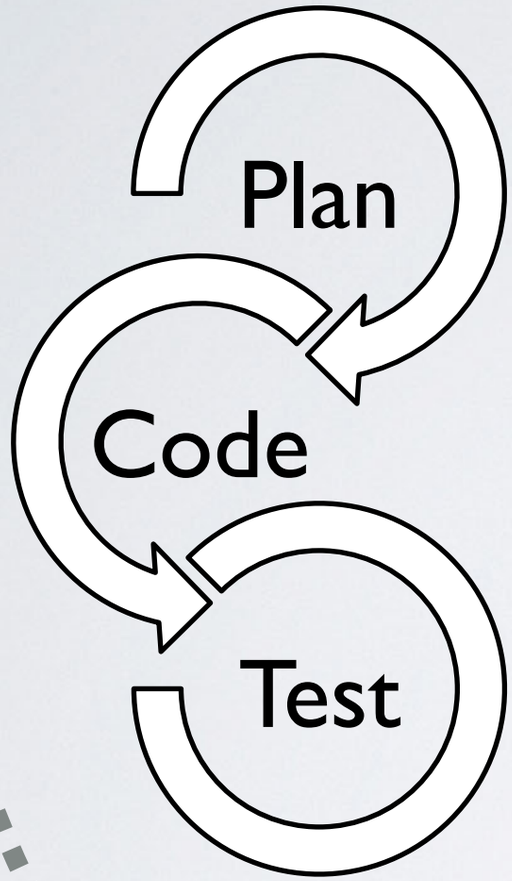
Continuous compliance
Continuous monitoring
Continuous risk assessment
Continuous configuration checking



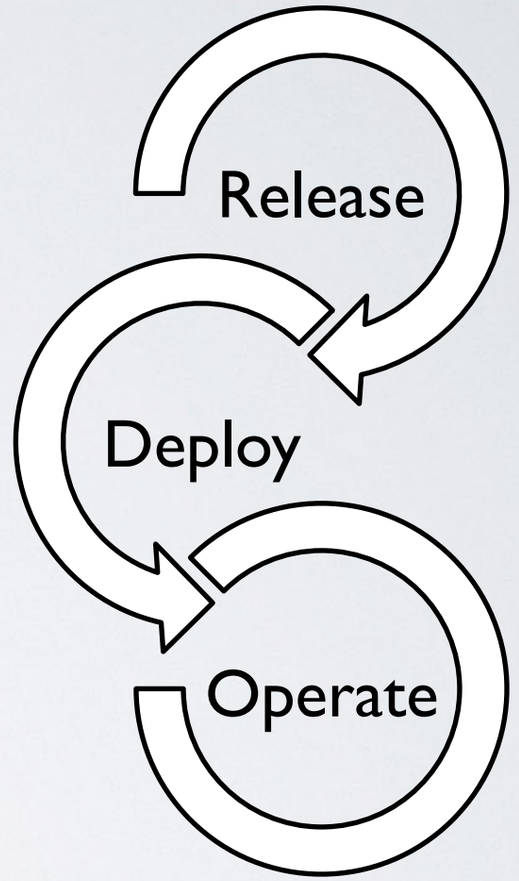
Process
Move Left
Get Involved
Acceptance
Be Wise
Hands Off
Continuous







Security Continuous Process Adapt Add Value



FURTHER READING

- Rugged DevOps
- Securosis
  - Integrating security into Agile
- @St0rmz
- devops.com