SATURN 2018

14th Annual SEI Architecture Technology User Network Conference

MAY 7–10, 2018 | PLANO, TEXAS

Implementing Secure DevOps Assessment for Highly Regulated Environments - HRE

David Shepard | Software Engineer | Software Engineering Institute | Carnegie Mellon University

Document Markings…

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-0664

Topics

- Background
- What is an HRE and why is it different?
- Common Pitfalls
- HRE Assessment Approach and Plan
- Requirements Analysis and evaluation
  - People, Process, Platform
- Moving Forward

Background

- The Software Engineering Institute (SEI) is a Federally Funded Research and Development Center (FFRDC)
- Research and practice in software development, acquisition, and maintenance practices
- Assisted numerous government organizations in modernizing their software development practices in the spirit of DevOps principles.
- Application security is the principle quality attribute of the software they produce.

DevOps and How it started

DevOps is a set of principles and practices emphasizing collaboration and communication between software development teams and IT operations staff along with acquirers, suppliers and other stakeholders in the life cycle of a software system [1]

- Patrick Debois “Agile infrastructure and operations: how infra-gile are you?”, Agile 2008 Conference
- John Allspaw “ 10+Deploys per Day: Dev and Ops Cooperation”, Velocity 2009
- DevOps Days, October 30th 2009, #DevOps term born

[1] IEEE P2675 DevOps Standard for Building Reliable and Secure Systems Including Application Build, Package and Deployment

Dev

Follow Agile methodologies and use shiny and new technology

- Scrum, Kanban, and other modern development approaches
- Self-directed, self-managed, self-organized
- Each developer may have their own development environment

Ops

- Operations
  - Support applications and services
  - Manage infrastructure
  - Provide Service Strategy, Design
  - Secure Systems

Dev wants to deliver new software features faster.

Ops wants to maintain stability, operations up-time.

DevOps has four Fundamental Principles

Collaboration: Between project team roles

Infrastructure as Code: All assets are versioned, scripted, and shared

Automation: Deployment, testing, provisioning, any manual process

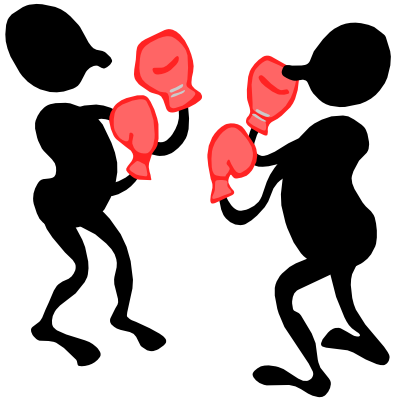
Monitoring: Any metric in the development or operational spaces that can inform priorities, direction, and policy

Without a Collaborative Culture, You Don't Have DevOps

Ask yourself:

- Do your Devs know **exactly** what **actual** production looks like?
- Does Ops know how Devs package a build?
- Is it **consistent**?
- Can both Dev and Ops collaborate on server configuration and apply it automatically to both **development and production environments**?
- Do business analysts **know the cost** of feature addition or modification?
- Can project managers measure project status **at any point in time**?
- Can the customer measure project status **at any point in time**?

Enabling Effective Collaboration



- Blame-Free Culture
  - No Hiding of Problems
  - Culture of shared responsibility
  - Collective decision and continuous learning
- Cross-Silo Goals
  - Incentivize Collaboration
  - Reduce “Not My Job”
  - Increase Sense of Purpose
- Optimize Ease-of-Use
  - Tools: Chat, ChatOps, Wiki
  - Integrated Pipelines

A Common Question

How can I implement a Secure DevOps process and platform in my team / directorate / project / organization / unit?

How to assess the current state?
Where are the productivity bottlenecks?
Whom to train on what?
What and how to measure?
How to monitor?

Current State of practice

- With Surveys;
  - DevOps State of report last couple years
    - 2014, 2015, 2016 and 2017
- Lead to research for Performance and ROI;
  - Dora (DevOps Research and Assessment);
  - Performance Matrix against industry practices
- Maturity Assessment; Ranger4
  - Not Started, Starting, Fundamental, Managed and Optimizing DevOps
- And others like
  - Tool approach based assessment
  - IBM, CA Technologies, ThoughtWorks or similar

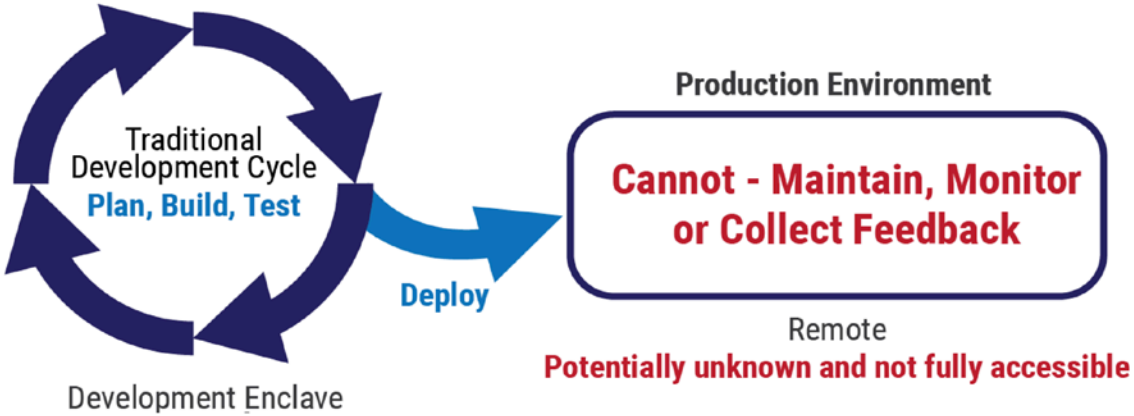
Topics

- Background
- What is an HRE and why is it different?
- Common Pitfalls
- HRE Assessment Approach and Plan
- Requirements Analysis and evaluation
  - People, Process, Platform
- Moving Forward

What is HRE?

- Highly-Regulated Environment (DoD, Health, Finance, etc…)
  - Air-gapped computer system
  - Isolated working Groups
  - Strong physical Security
  - Segregation of Duties
  - Information classification
    - Inability speak, share/collaborate on artifacts
  - Level of Security and Risk management
  - Limitation of Continuous Deployment
  - Physical System Integration
  - Strong Audit Trail on each level of development activities

A closer look at HRE..



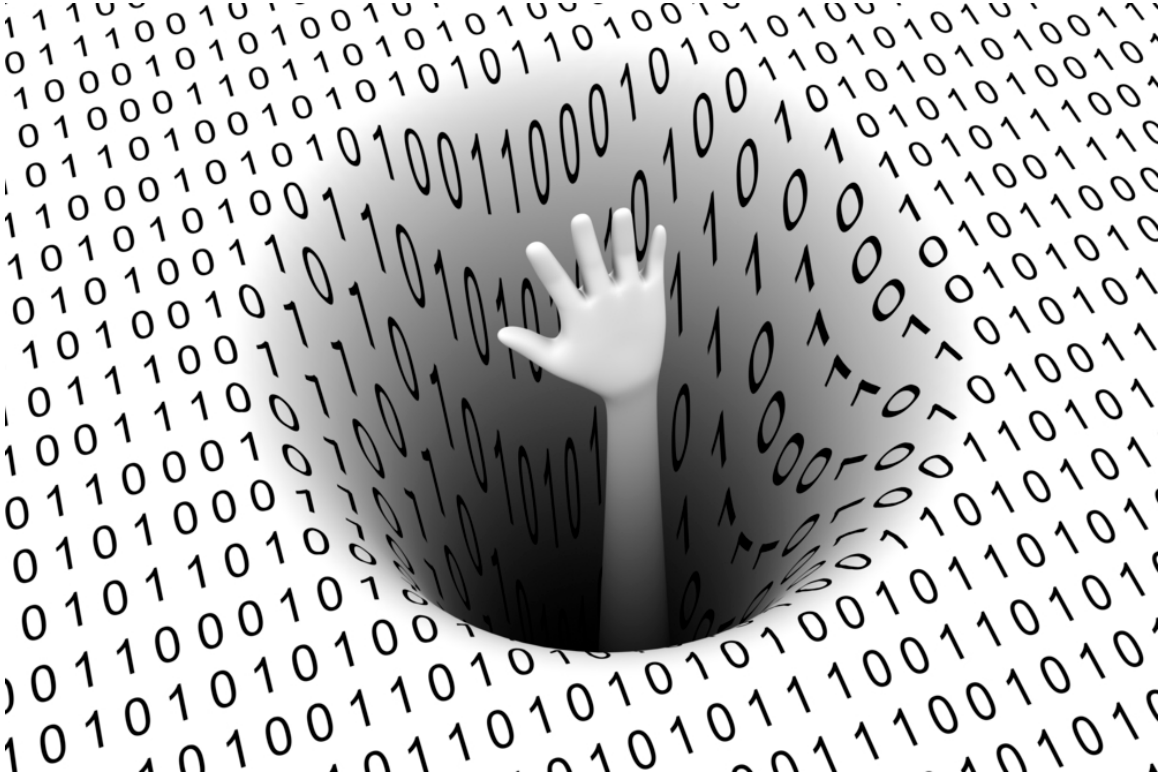
How we can assess these kinds of environments and then deploy Secure DevOps processes and techniques?

Topics

- Background
- What is an HRE and why is it different?
- ▶ Common Pitfalls
- HRE Assessment Approach and Plan
- Requirements Analysis and evaluation
  - People, Process, Platform
- Moving Forward

Common Pitfalls

HELP!



What can go wrong? (Organizational Culture)

DevOps is

- A FAD
- Only about tooling
- A Product
- Only about Dev and Ops
- The same for all organizations
- Only continues integration/deployment
- New organizational unit

Topics

- Background
- What is an HRE and why is it different?
- Common Pitfalls
- ▶ HRE Assessment Approach and Plan
- Requirements Analysis and evaluation
  - People, Process, Platform
- Moving Forward

DevOps in HRE Assessment; *Overview*

Interview with functional leads from key areas related to Application Development.

Review of:

- Validation of statements (e.g., through observations of the work environment or shadowing)
- Demonstrations of any software tools used for automation of software development and deployment
- Cultural perspective related to development evolution and Security team
- Legal, Risk Management and all stakeholders

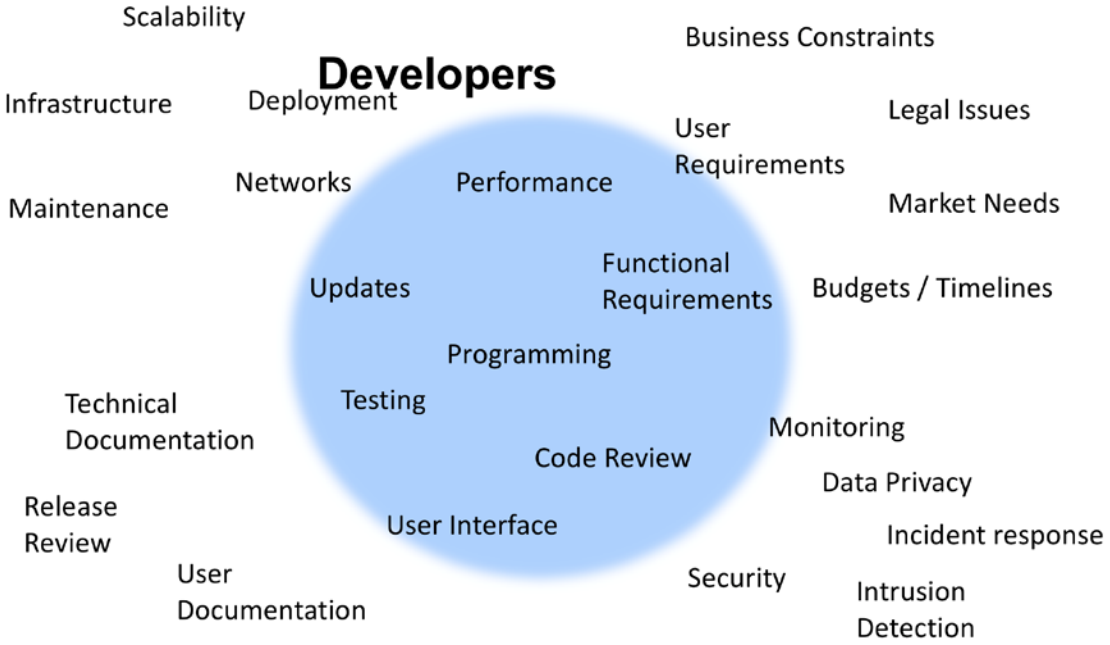
DevOps on HRE Assessment; *Plan*

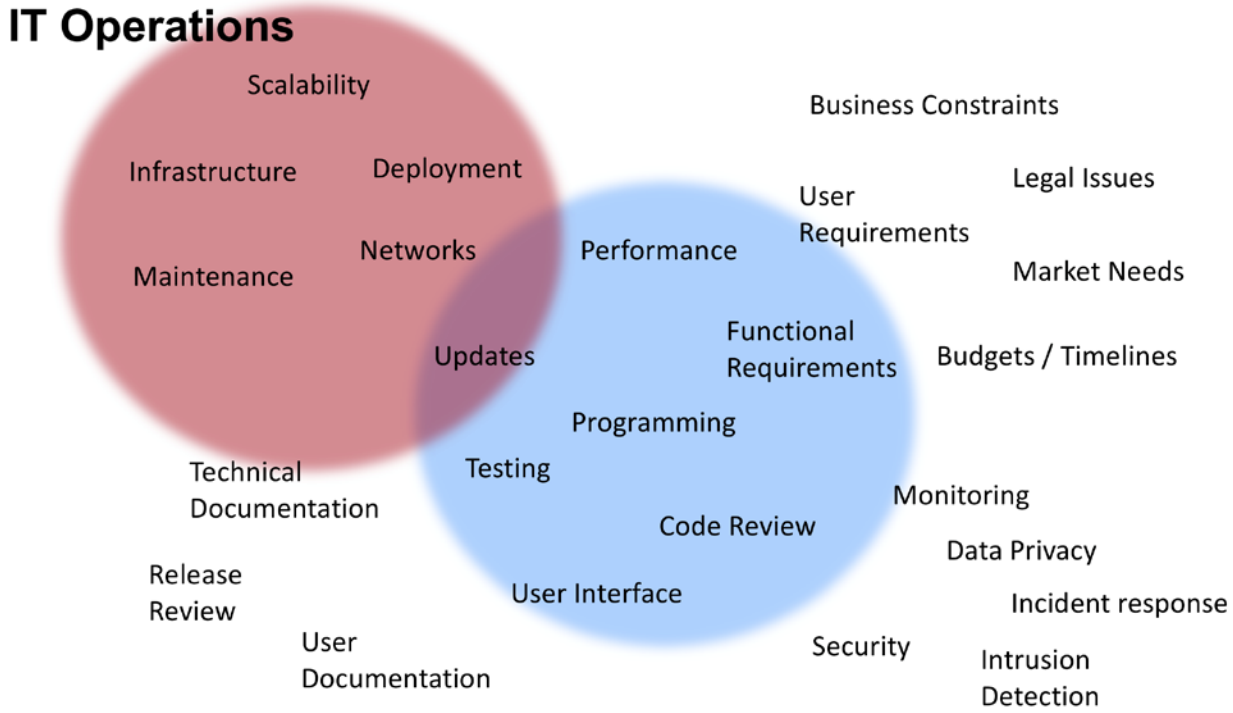
1. Agree on definitions(*DevOps, DevSecOps*) and process
2. Identify stakeholders
3. Perform interviews on each team
4. Identify and analyze technical tool stack
5. Collect key metrics and establish measurement
6. Identify gap areas and develop a roadmap
7. Select a suitable project to implement: *Build , Learn, Evaluate*

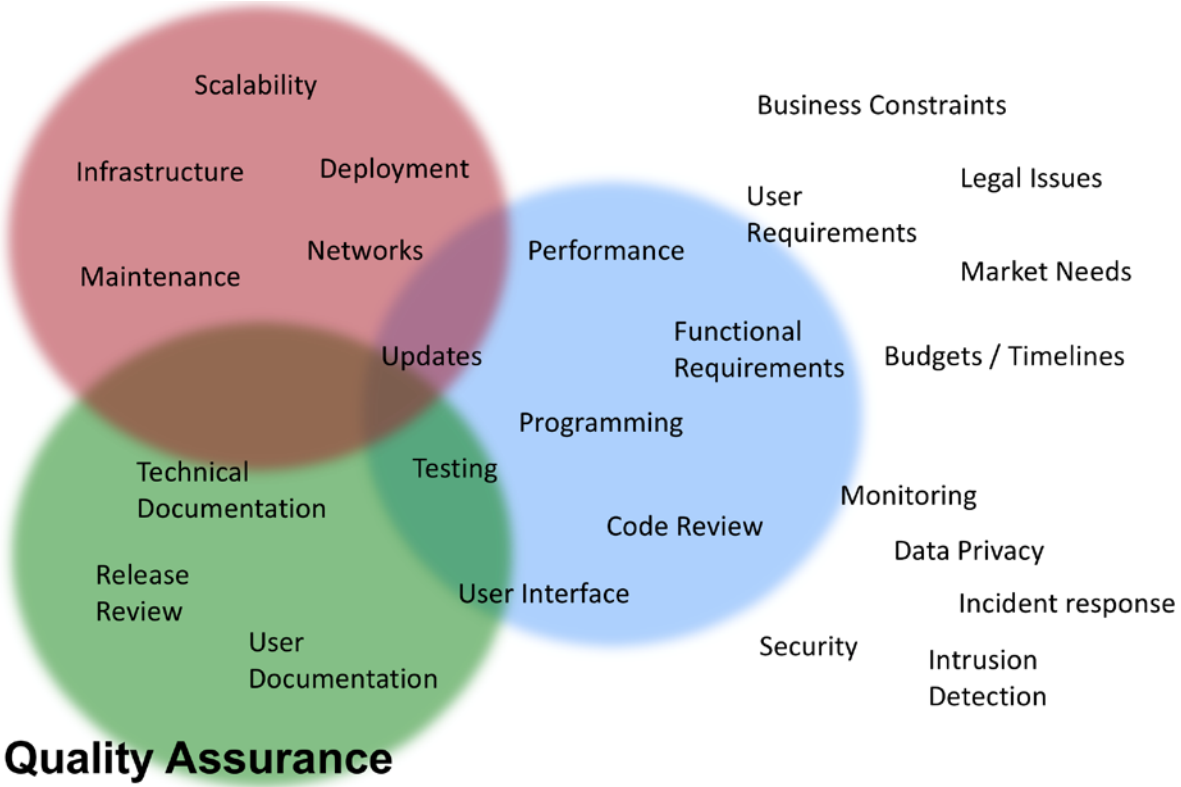
DevOps on HRE Assessment; *Process*

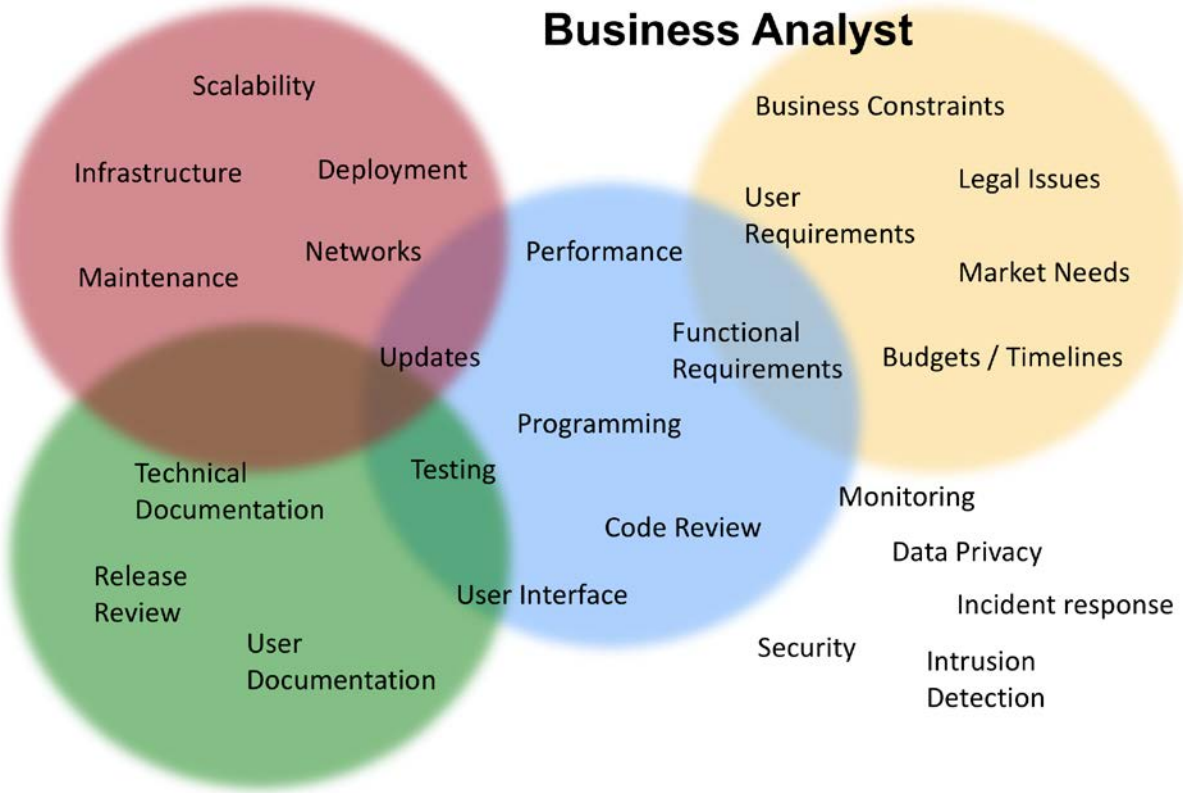
- Scheduling interviews with teams
- Conduct anonymous surveys
- Analyze outcomes
- Provide feedback to the teams
- Brief the executive team

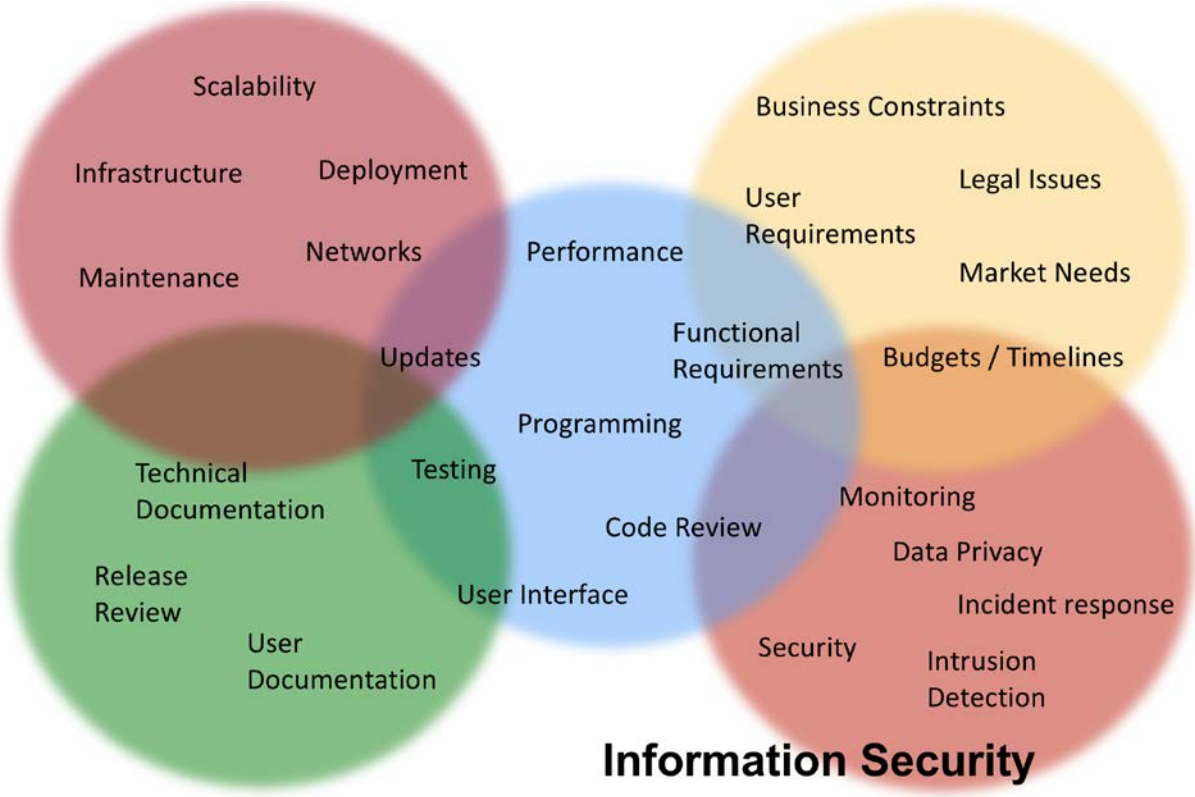
Identify Stakeholders











DevOps on HRE Assessment: *Business Analyst/ PM*

- Requirements development & management
- Acquisition & contracting process
- Risk management process
- Compliances requirements
- Project Planning and tracking

DevOps on HRE Assessment: *Developer*

- Development methodology
  - agile, waterfall, SAFe, EP, Lean, or cowboy coding
- Development environments
- Task assignment/management / completion
- Collaboration with other (internal/external) teams

DevOps on HRE Assessment: *Quality Assurance Team*

- Software testing methodologies
- Software {quality} assurance
- Compliances verification
- Audit requirements
- Feedback to dev team

DevOps on HRE Assessment: *Deployment/Release Mgr.*

- Software configuration management
- Integration process
- Software verification and validation process
- Software review and audit process
- Securing the deployment pipeline

DevOps on HRE Assessment: *IT Operations (not Ops)*

- Software operational process
- Team engagement
- Policy knowledge management
- Assets management
- IT governance
- Service management
- Audit and monitoring

DevOps on HRE Assessment: *Information Security*

- Management and auditing supply chain
- Security controls
- Security polices (compliance requirements)
- Application security testing
- Product security management (PSIRT)
- Security awareness training and knowledge management

DevOps on HRE Assessment: *Technology Stack*

- Development language and tools
- IT solution stack
- Enterprise support services
- Legacy systems
- Application development support tools
- Software reuse process
- Accreditation and approval process

DevOps on HRE Assessment: *Metrics and Measurement*

- Software metrics
- Quality metrics
- Checkpoint diagnostic
  - Qualitative process baseline
  - Quantitative performance baseline
  - Benchmark performance comparison
- Define end-goal as developing a Secure Software:
  - *What that means to all stakeholders*

DevOps on HRE Assessment: *Identify Suitable Project (Rollout Plan)*

Select {new or existing} project as pilot

- Most stakeholders involvement
- Minimize risk to business
- Ability learn/develop/ implement security in the process
- Scalable to the organization

Topics

- Background
- What is an HRE and why is it different?
- Common Pitfalls
- HRE Assessment Approach and Plan
- ▶ Requirements Analysis and evaluation
  - People, Process, Platform
- Moving Forward

DevOps on HRE Assessment: *Feedback to the team*

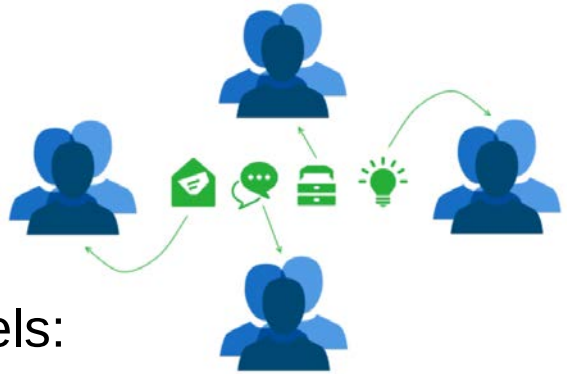
- Collaborate all team leads
- Share identified requirements
- Categorize and prioritize the requirements
- Collectively develop implementation plan:

People + Process + Platform = Plan

DevOps on HRE Assessment: *People*

Heavy collaboration between all stakeholders

- Secure Design / Architecture decisions
- Secure Environment / Network configuration
- Secure Deployment planning
- Secure Code Review



Constantly available open communication channels:

- Dev and OpSec together in all project decision meeting
- Chat/e-mail/Wiki services available to all team members

DevOps on HRE Assessment: *Process*

Establish a *process* to enable *people* to succeed using the *platform* to develop Secure application

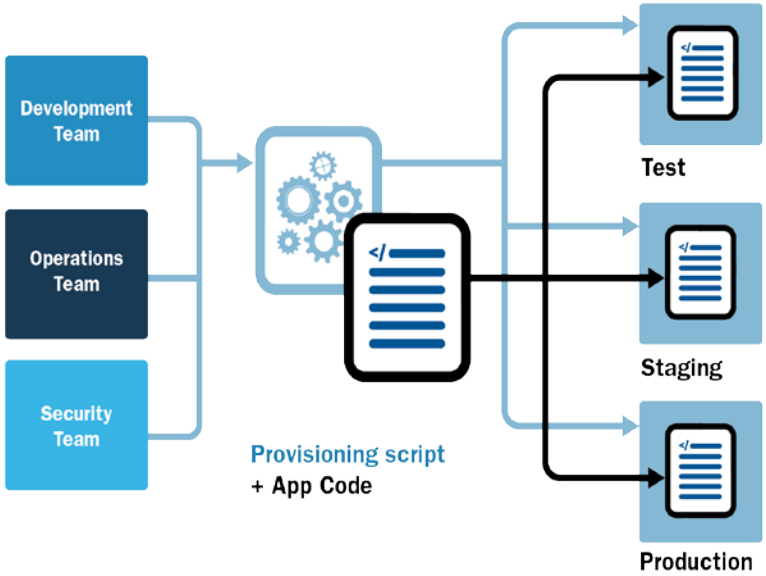
Such that;

- Constant communication and visible to all
- Ensures that tasks are testable and repeatable
- Frees up human experts to do challenging, creative work
- Allows tasks to be performed with minimal effort or cost
- Creates confidence in task success, after past repetitions
- Faster deployment , frequent quality release

DevOps on HRE Assessment: *Platform*

Where *people* use *process* to build secure software

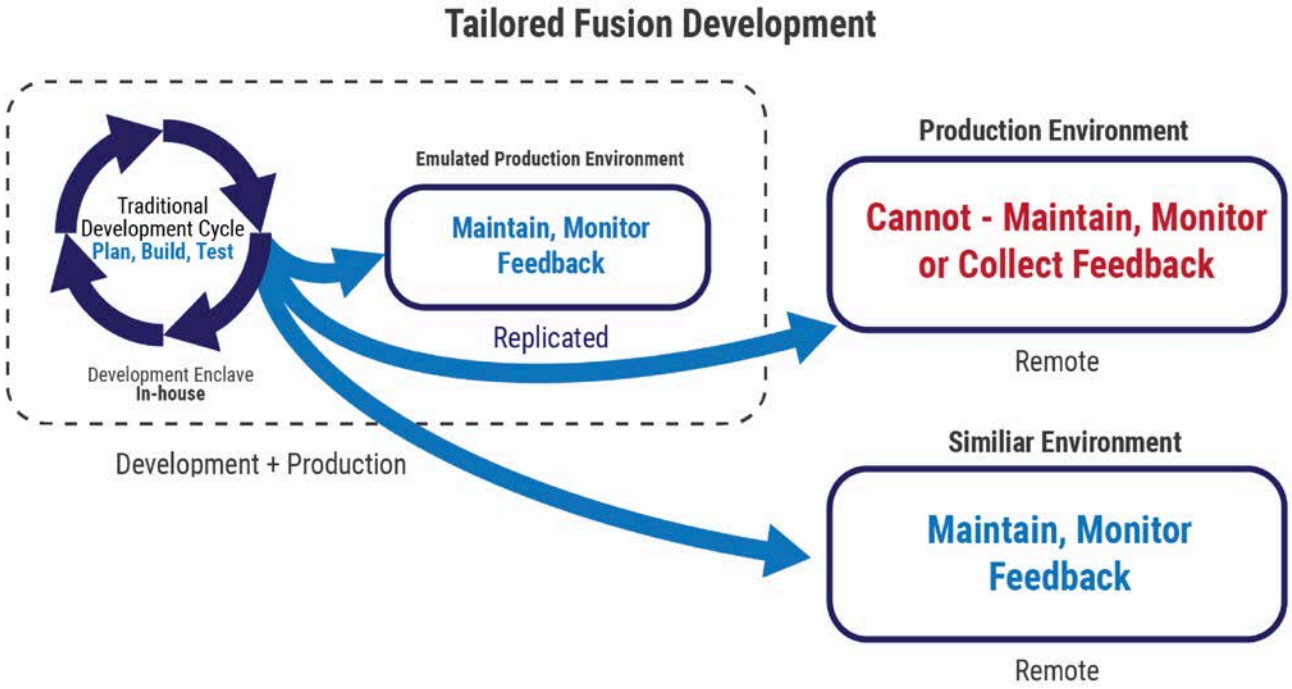
- Automated environment creation and provisioning
- Automated infrastructure testing
- Parity between Development, QA, Staging, and Production environments
- Sharing and versioning of environmental configurations
- Collaborative environment between all stakeholders



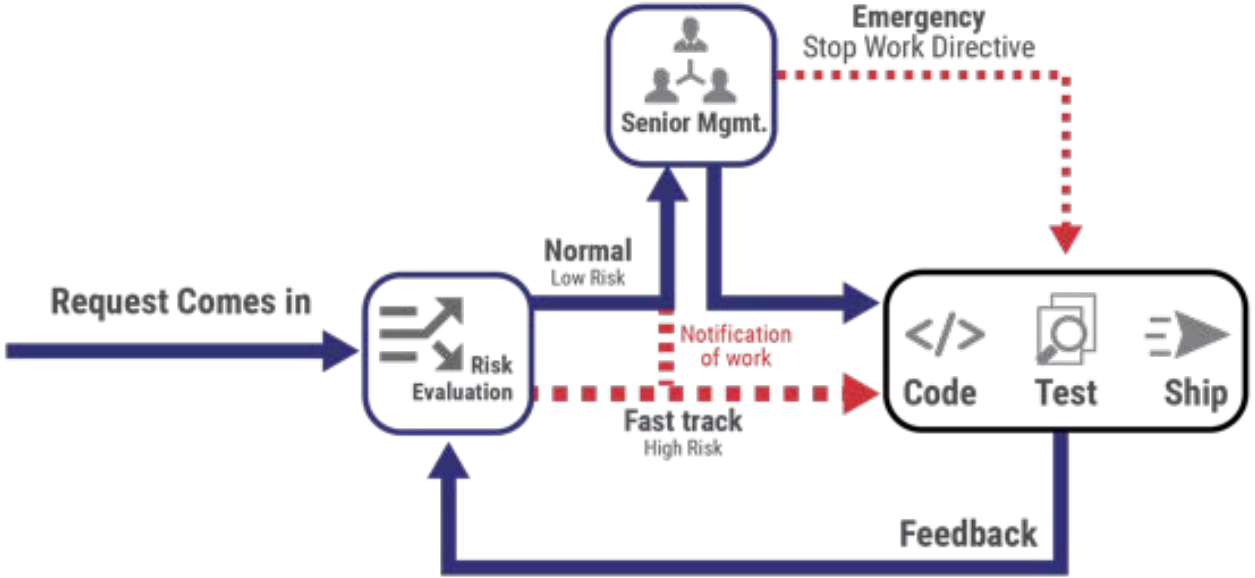
Topics

- Background
- What is an HRE and why is it different?
- Common Pitfalls
- HRE Assessment Approach and Plan
- Requirements Analysis and evaluation
  - People, Process, Platform
- ▶ Moving Forward

DevOps + Environment Parity



Adding Security



SLS team GitHub Projects

- Once Click DevOps deployment
  https://github.com/SLS-ALL/devops-voltron
- Sample app with DevOps Process
  https://github.com/SLS-ALL/flask_api_sample
  - Tagged checkpoints
    - v0.1.0: base Flask project
    - v0.2.0: Vagrant development configuration
    - v0.3.0: Test environment and Fabric deployment
    - v0.4.0: Upstart services, external configuration files
    - v0.5.0: Production environment
- On YouTube:
  https://www.youtube.com/watch?v=5nQlJ-FWA5A

For more information…

SEI DevOps Blog

https://insights.sei.cmu.edu/devops

Contact Information

David Shepard

Software Engineer,
Secure Lifecycle Solutions
djshepard@sei.cmu.edu

@securelifecycle

Web Resources (CERT/SEI)

http://www.cert.org/

http://www.sei.cmu.edu/