12/15/2020

Manage DevSecOps Projects

“When you change the way you look at things, the things you look at change”
- Mark Planck

Who is Bhanu?

Career

- Guided missile program scientist for Indian Defense
- Technical Staff Officer to the CIO
- Application developer, architect & lead
- Team member for security governance / audit
- Data Analytics and Business Intelligence
- Program Manager
- PMO Manager

Professional

- Member ISSA
- Member PMI, PMISV
- Member Scrum Alliance, SAFe
- Certifications:
- PMP, PMI-ACP, DASM, DASSM, CSM, SASM, SA, POPM, SDP, TOGAF, KMP1, PMI-AH, DPBoK, CCSK
- DevOps PM, Architect, RM, Trainer, Coach

Giving Back

- Mentor and coach for project managers
- President PMI Silicon Valley Chapter
- Guest speaker at SJSU
- Adjunct Professor at GGU SF, Cogswell University

Takeaways - DevSecOps

Why DevSecOps

Predictive

Iterative

Incremental

Chronic conflict between Development, Security and Operations

Huge Technical Debt

Wrong expectations

No fun at work

Single point of SMEs/Failures

Security Terms

Vulnerability

Threat agent

Threat

Risk

Control

Exposure

Safeguard

CIA triad, Shift left Security, Secure by Design

What is DevSecOps

DevOps is a mindset, a culture, and a set of technical practices. It provides communication, integration, automation, and close cooperation among all the people needed to plan, develop, test, deploy, release, and maintain a Solution.© Scaled Agile, Inc.

The approach of integrating and automating security tasks within the SDLC process is called DevSecOps, where the people and technology involved in the pipeline actively contribute to the full lifecycle of the software products. Security must be integrated within the process itself, and not as an additional layer of checklist items that can be automated.

Process to develop, deliver and operate

Can be integrated with any of the frameworks

- Scrum
- Lean
- ITIL

Adapted Techniques from

- Lean
- Continuous Delivery movement
- Agile

What is DevSecOps

DevSecOps mindset and bringing individuals of all abilities and across all technology disciplines to a higher level of proficiency in security.

From testing for potential security exploits to building business-driven security services, a DevSecOps framework that uses DevSecOps tools ensures security is built into applications rather than being bolted on haphazardly afterwards.

By ensuring that security is present during every stage of the software delivery lifecycle, we experience continuous integration where the cost of compliance is reduced, and software is delivered and released faster.

What is DevSecOps

Typical DevOps and DevSecOps workflow:

Perform Threat Modeling to address known security risks before a single line code is written

A developer creates code within a version control management system.

The changes are committed to the version control management system.

Another developer retrieves the code from the version control management system and carries out analysis of the static code to identify any security defects or bugs in code quality.

An environment is then created.

The application is deployed, and security configurations are applied to the system.

A test automation suite is then executed against the newly deployed application, including back-end, UI, integration, security tests and API.

If the application passes these tests, it is deployed to a production environment.

This new production environment is monitored continuously to identify any active security threats to the system.

How DevSecOps Helps

Architect for secure design

Continuous deployment

Organize teams around the mission / business value

Build Systems to deliver business goals

Built-in quality and monitoring

View errors as opportunities to learn and teach

Scalability of Teams

Architect for safer releases

Design

Security built-in

Continuous Exploration

Continuous Integration

Continuous Delivery

Continuous Deployment

Application Security practices

Continuous Monitoring

Trunk based development

- Codebase always releasable
- Small chunks of code for delivery
- Gated commits with test automation validation

Testing

Test automation

- Test Automation should give quick and early feedback about your quality of work- Tests shouldn't generate false positives
- First focus on the validation of key features and benefits
- Avoid slow and periodic feedback for check-in code to your trunk
- Test Driven Development
- Security test cases part of the testing function
- Unit Tests
- Acceptance Tests
- Integration Tests
- Performance and stress Tests
- Non-functional Tests

What you cannot automate – user experience tests

Deployment

Blue-green deployments

Canary deployment (the dark launch)

Feature toggles

Deployment and release are not the same

Devops – Release on demand

Project Management

Identify the training needs

Have scope for JIT training sessions

Have scope for JAD sessions

Milestones as separate section

Assumptions as separate section

External dependencies / tasks as a separate section

Internal dependencies as a separate section

Business decision / tasks as a separate section

Project Management

Separate sections(WPs) for DevOps process (CI/CD) in the plan

Separate section for continuous development

Separate section for continuous integration

Separate section for continuous testing

Separate section for continuous deployment

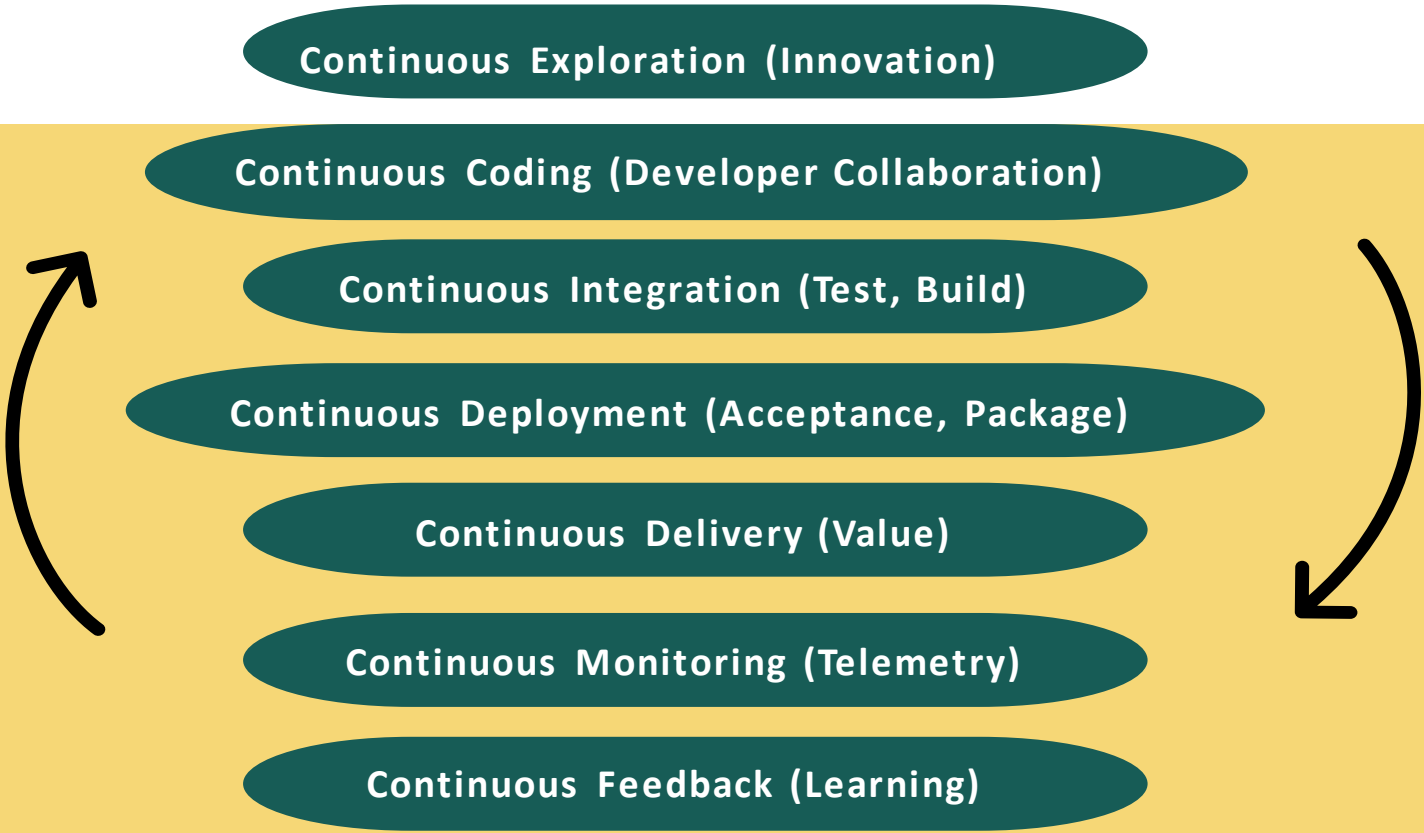
Separate tasks for post deployment monitoring and feedback

Separate section (WPs) for Security tasks

Milestones – to highlight the completion of DevSecOps activity

Define metrics and Kpis to measure the maturity of DevSecOps for People, Process and Tools

Takeaways - DevSecOps



References

- DevOps_Revealed_by_International_DevOps_Certification_Academy By International DevOps Academy
- https://www.forcepoint.com/cyber-edu/devsecops
- Other internet sources

Bhanu

Thank you

Let's get better today @DevSecOps

Additional Information

CI / CD tools

https://www.guru99.com/top-20-continuous-integration-tools.html

Jenkins, Bamboo, GitLab

Version control

https://hackernoon.com/top-10-version-control-systems-4d314cf7adea

GitHub, Gitlab, PerForce

DevOps development tools

https://raygun.com/blog/best-devops-tools/

Ansible, Kubernetes

Deployment Strategies

https://dev.to/mostlyjason/intro-to-deployment-strategies-blue-green-canary-and-more-3a3

- Feature Toggle/ Toggle Switches
- Canary releases
- Blue – Green, Red-Black , A/B
- Rolling, Big Bang