InquisIT

2019

# DevSecOps
## In The Federal Space

InquisIT, LLC.
14900 Bogle Drive, Suite 203
Chantilly, VA 20151

Info@inquisitllc.com
www.inquisitlls.com

All Rights Reserved.

# INTRO

The goal of development is to make the best thing possible in the least amount of time. Creation is complex often involving many departments and disciplines. The enemy of developmental progress is communication and failure to integrate. These information and functional silos can allow for blatant problems in an application to affect multiple parties. In the Federal IT space, integration and departmental communication is often more segmented and siloed than commercial organizations. The development and implementation of new methods of application engineering in the Federal government is too often guilty of incrementalism. In the private sector, development and operation have gone hand-in-hand so long people got tired of separating the two, instead saving time by referring simply to DevOps.

# Integrate Teams

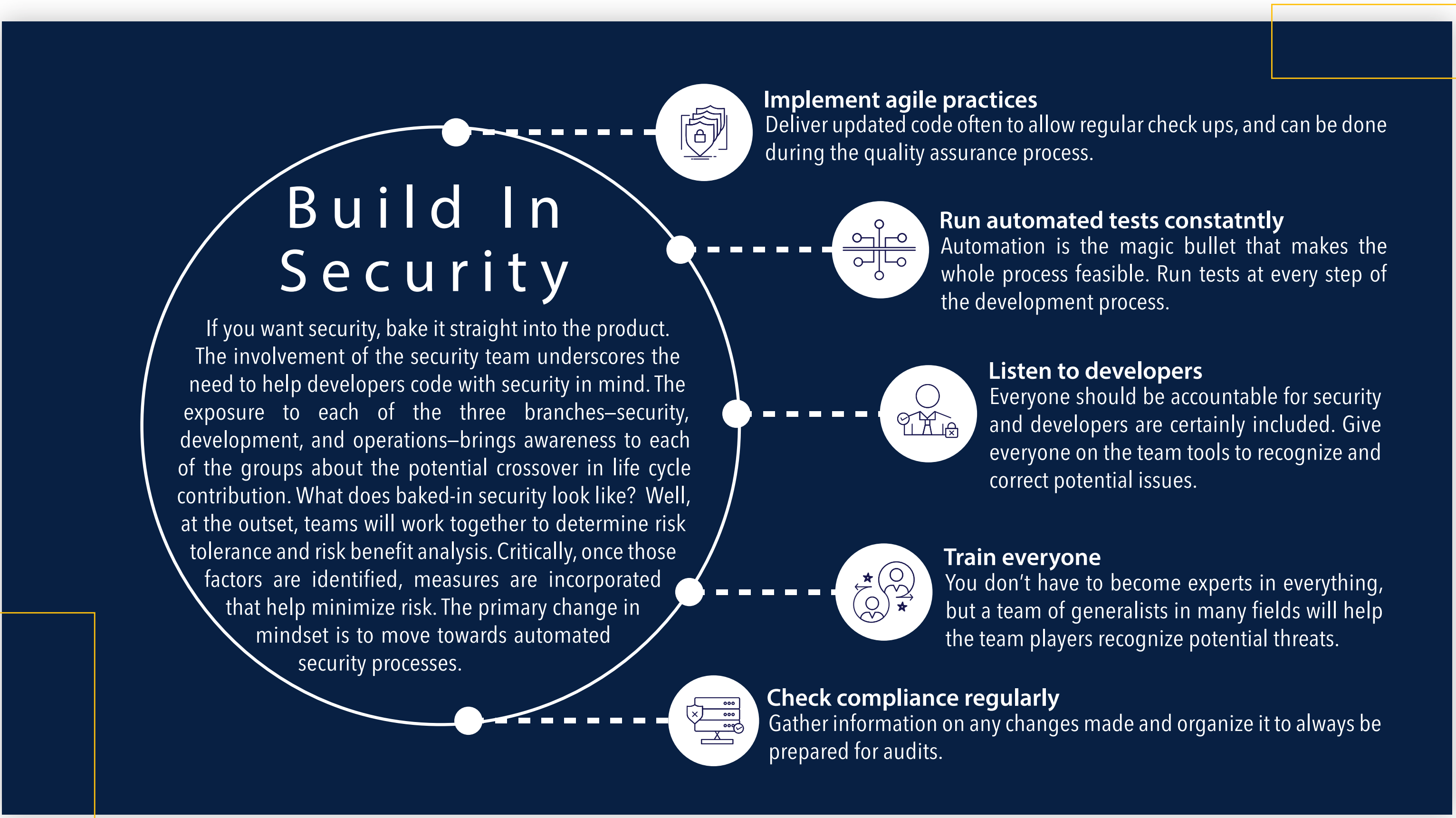
The fundamental goals behind DevOps teams is to integrate the users and the creators for great responsiveness throughout the life cycle of the application.

Teams work in very different, but highly connected roles, each role requiring a unique skill set. Traditionally, only in the last stages of development does security play a role in DevOps; however, the agility of applications is greatly improved when the security team has input throughout the process.

The unique advantage of DevOps is to include relevant parties to the production and use of the application, and security has never been more relevant. Therefore, if you're going to DevOps, the smart thing is to include security from the beginning and transition directly to DevSecOps in all processes. This improves the speed of development, allows development teams to find and mitigated flaws 11 x faster, and diversifies the environment in which applications are deployed.

*...the agility of applications is greatly improved when the security team has input throughout the process...*

DevSecOps is a framework of collaboration for development teams to work with security personal from end-to-end. The DevSecOps team helps lay a security foundation by incorporating security principles throughout. When you're building a house, what would happen if you start putting up the walls only to realize you forgot about the foundation? You'd have to tear it down and start over from scratch to do it right. In the same way, DevSecOps lays down a security foundation, so the code does not have to be reconfigured or completely rewritten. The mindset embraces automating security processes to enhance the integration of security tools without sacrificing the speed of development.



## Build In Security

If you want security, bake it straight into the product. The involvement of the security team underscores the need to help developers code with security in mind. The exposure to each of the three branches–security, development, and operations–brings awareness to each of the groups about the potential crossover in life cycle contribution. What does baked-in security look like? Well, at the outset, teams will work together to determine risk tolerance and risk benefit analysis. Critically, once those factors are identified, measures are incorporated that help minimize risk. The primary change in mindset is to move towards automated security processes.

**Implement agile practices**
Deliver updated code often to allow regular check ups, and can be done during the quality assurance process.

**Run automated tests constatntly**
Automation is the magic bullet that makes the whole process feasible. Run tests at every step of the development process.

**Listen to developers**
Everyone should be accountable for security and developers are certainly included. Give everyone on the team tools to recognize and correct potential issues.

**Train everyone**
You don't have to become experts in everything, but a team of generalists in many fields will help the team players recognize potential threats.

**Check compliance regularly**
Gather information on any changes made and organize it to always be prepared for audits.

Automation helps augment the collaboration of teams and facilitates interaction between them to foster a DevSecOps culture. How does automation accomplish this? Many cloud born technologies, like containers and microservices are leading the way. Organizations are asked to examine already implemented solutions such as source control repositories, container registries, the continuous integration and continuous deployment (CI/CD) pipeline, application programming interface (API) management, orchestration and release automation, and operational management and monitoring. The change in design practices is one of adoption. The additional move from local machines to cloud services has created a new and more complex hybrid application environment. The changes affect the way many organizations approach application development.

**So how can the Government adapt?**

It starts with a mindset that everyone is responsible for security. The DevSecOps model that utilizes automation must incorporate version control systems, containerization, continuous testing, configuration management, and deployment–all orchestrated by a team lead. The elimination of silos in the development process creates room for teamwork, vulnerability identification, and more controlled and speedy delivery.

# Set DevSecOps Culture

The Culture of DevSecOps is one of mutual responsibility and open communication. Both horizontal and vertical communication are absolutely crucial to the mission of developing effectively and in a short amount of time. People need to be shown how to communicate with others outside their department. A big advantage of DevSecOps is the collection of opinions that can guide the process andbring fresh insights, allowing subordinates to feel free to give opinions openly. This, as with many management strategies begins at the top. In order to truly experience the benefits of a team, effort must be put into establishing the culture of mutual responsibility and open communication.

**There are technologies that help augment teams and enable them to operate with greater visibility and efficiency.**

**Possible solutions and tools for each phase that help promote DevSecOps mindset include:**

| | |
|---|---|
| BUILD | SLACK GITHUB |
| TEST | SELENIUM JENKINS |
| DEPLOYMENT | ANSIBLE<br>JENKINS |
| OPERATIONS | SOLARWINDS<br>NESSUS<br>AMI |

Dev Sec Ops Culture

Mutual Responsibility

Cross Training

Communication

# Benefits

The processes of DevSecOps are a mindset and before the processes can be implemented with success, the team leads need to understand the paradigm of security everywhere and collaboration throughout. The time for government agencies to adopt this mindset is now! How do you turn the battleship? Simple, it saves money and creates business benefits throughout.

**Will it work on my team?**

The great thing about the methods used in this design is that they create accountability across departments. The production of the solutions created by the development team are now distributed throughout all affected services. The life cycle of the application is seen more holistically, which benefits all departments with greater understanding. Progress takes time, but when solutions that greatly improve the efficiency of a task are discovered implementation is a pleasure. Why are you still using a` rusty old hammer to build your code when you can have an automatic, pneumatic, chrome-plated, industrial-strength nail gun?

1

## DESIGN BENEFITS

- Quick problem resolution
- Reduction and simplification of problems
- Constant development and integration
- Greater scalability
- Increased departmental understanding of implemented solutions

2

## ECONOMIC INCENTIVES

- Quick problem resolution
- Increased speed of development
- Risk reduction and more predictable working environments
- Increased focus on optimization over maintenance and fixes