Unissant

Unissant White Paper Series

DevSecOps– A Key Enabler of Digital Transformation

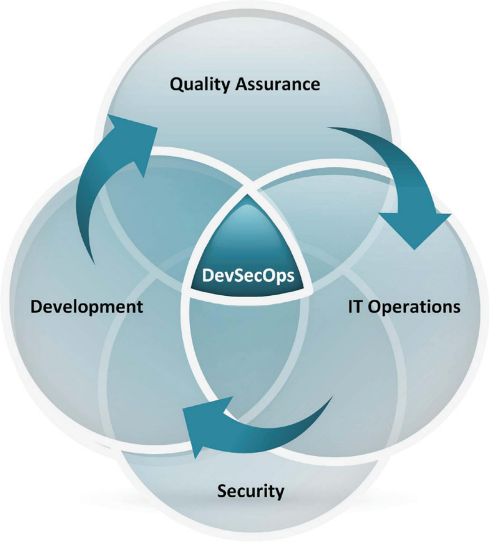
DevSecOps–A Key Enabler of Digital Transformation

Introduction

Digital Transformation is about integrating digital technology into all areas of business of an enterprise to achieve operational efficiency and achieve higher business value. To be competitive in this fast-paced time, it is critical for enterprises to have faster *time-to-market* cycles, be it a product or software features. DevSecOps, together with Agile Engineering, play a major role in this process by aiding digital transformation through combining development and operations and cutting down the time-to-market cycle time.

Federal agencies are increasingly adopting DevSecOps methodology as an Organization-wide Software Engineering culture and practice, that will enhance collaboration between Development, Security and Operations.

The increasing importance of DevSecOps is evident from some of the recent initiatives in the federal sector The National Institute of Standards and Technology (NIST) is considering creating a DevSecOps framework for agencies to make embedding security controls at the beginning of the software development lifecycle a common practice. DoD has published a DevSecOps Reference Design document that provides implementation and operational guidance for DevSecOps. In addition, the term has been included in the National Defense Authorization Act (NDAA) of 2020 encouraging the Secretary of Defense to designating a single official responsible for coordinating DevSecOps.



It is common to see the terms “DevSecOps,” “Agile,” and “Continuous Integration / Continuous Delivery (CI/CD)” to communicate the same software development approach. However, they are not the same. DevSecOps focuses on automation, monitoring and application of security at all phases of the software life cycle. It is a combination of Technology, People, and Processes encapsulating end-to-end engineering processes. DevSecOps culture nurtures increased collaboration, and improves flow of information and feedback between Security, Operations and Development Teams.

The agile methodology is about the collaboration between business users and developers. Agile teams are focusing on iterations of working software that would evolve over time, delivering value along the way. CI/CD is a software engineering practice to integrate and deliver with high frequency with emphasize on automation. DevSecOps takes Agile to the next step. As with Agile frameworks, DevSecOps incorporates lean, synergistic practices, like Continuous Integration and Continuous Delivery (CI/CD), that encourage and support frequent code check-in, version control, sensible test automation, continuous low-risk releases and feedback, often through several tools. DevSecOps best practices include many key processes: CI/CD, Continuous Testing, Continuous Inspection, Continuous Monitoring, Infrastructure as Code, Pipeline as Code and Configuration as Code.

DevSecOps Implementation Challenges

With any new technology or paradigm, adoption organizations must overcome certain challenges. Typical DevSecOps challenges include:

- Humans' natural resistance to change.
- Currently, there are too many tools in the market. Not all of them are useful leading to a resistance to adopt the appropriate tool.
- Moving from legacy monolith to microservices raises multiple technical as well as process challenges.
- Dread the idea of bulk of documentation.
- Provisioning and Configuration is considered tedious.

These challenges are not always uniform across the organization. It depends to a large extent on the current level of DevSecOps maturity and, overcoming these challenges takes time and commitment from both the leadership and the team members. Here are a few approaches we recommend for overcoming these challenges:

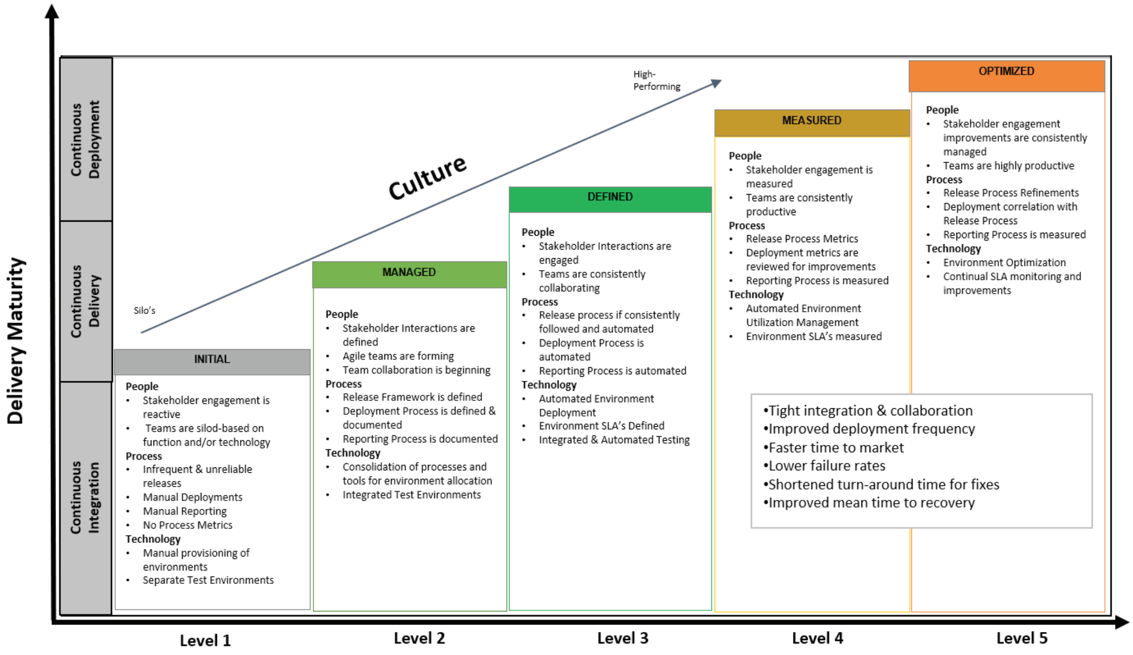
- Enlist full executive support for implementation and training of DevSecOps to incorporate a culture of collaboration.
- Adopt a tool only if you can use the tool effectively. There are tools available for various technology stacks, avoid the 'shiny object syndrome.'
- Adopt small changes and incrementally, pay attention to security, data and performance.
- Define Lean documentation templates and encourage concise documentation rather than bulk documentation.
- Adopt cloud implementation and automate provisioning and configuration

DevSecOps is an evolving IT culture. Challenges are different for each customer. Using the most appropriate combination of technologies, processes, and skilled resources, Unissant team works alongside customers to identify and overcome these challenges to progress their focus on *DevSecOps Implementation*. Our initiatives have helped customers to start adopting elements of DevSecOps that are most appropriate for their position in the DevSecOps journey to reduce the time between design to deployment of software.

Unissant's Approach to DevSecOps

Unissant's approach to DevSecOps begins with an assessment of the current maturity of the organization, to understand and document potential to follow a DevSecOps approach through the lens of "people, process, and technology" and develop a roadmap based on the stage at which the customers are in their DevSecOps journey.

The **Maturity Assessment** helps to identify the gaps between DevSecOps best practices and the current capabilities. Based on our assessment, organizations are assigned to one of the five levels of DevSecOps maturity illustrated in Figure 1: 1. Initial stage, 2. Managed, 3. Defined, 4. Measured, and 5. Optimized. This will guide the development of a roadmap for implementing DevSecOps.



INITIAL

People
- Stakeholder engagement is reactive
- Teams are silod-based on function and/or technology

Process
- Infrequent & unreliable releases
- Manual Deployments
- Manual Reporting
- No Process Metrics

Technology
- Manual provisioning of environments
- Separate Test Environments

MANAGED

People
- Stakeholder Interactions are defined
- Agile teams are forming
- Team collaboration is beginning

Process
- Release Framework is defined
- Deployment Process is defined & documented
- Reporting Process is documented

Technology
- Consolidation of processes and tools for environment allocation
- Integrated Test Environments

DEFINED

People
- Stakeholder Interactions are engaged
- Teams are consistently collaborating

Process
- Release process if consistently followed and automated
- Deployment Process is automated
- Reporting Process is automated

Technology
- Automated Environment Deployment
- Environment SLA's Defined
- Integrated & Automated Testing

MEASURED

People
- Stakeholder engagement is measured
- Teams are consistently productive

Process
- Release Process Metrics
- Deployment metrics are reviewed for improvements
- Reporting Process is measured

Technology
- Automated Environment Utilization Management
- Environment SLA's measured

OPTIMIZED

People
- Stakeholder engagement improvements are consistently managed
- Teams are highly productive

Process
- Release Process Refinements
- Deployment correlation with Release Process
- Reporting Process is measured

Technology
- Environment Optimization
- Continual SLA monitoring and improvements

•Tight integration & collaboration
•Improved deployment frequency
•Faster time to market
•Lower failure rates
•Shortened turn-around time for fixes
•Improved mean time to recovery

Figure 1. DevSecOps Maturity Model and Approach

Unissant team completed an assessment of NCI CBIIT DevSecOps maturity. Team has since been actively incorporating multiple process and technology initiatives that have been aiding in improving the posture of DevSecOps maturity in the agency.

Successful implementation of DevSecOps depends to a large extent on using the most appropriate **set of tools to support DevSecOps processes**. The number of tools available in the marketplace to support DevSecOps–both commercial and open source–continue to increase daily making the process of identifying the right mix of tools that integrate into proposed DevSecOps processes quite challenging. In addition, the tools are becoming more and more sophisticated and thus finding skilled resources to effectively use those tools can be a difficult task. The right mix of tools for an organization to achieve DevSecOps maturity depends on an organization's level of integration, availability of labor and product investment resources, and types of infrastructure, e.g., on-premise/cloud, type of development platform, languages, and operating systems. Figure 2 illustrates an example of a combination of tools at various phases of the DevSecOps lifecycle.

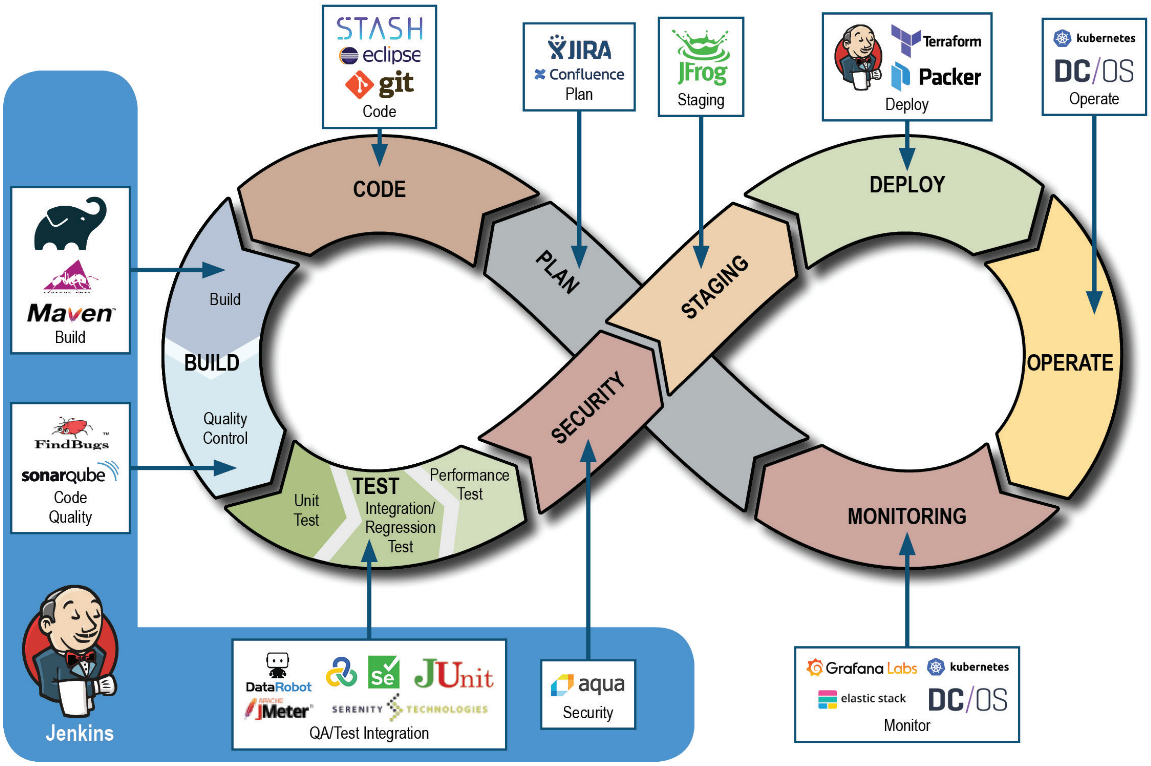


Figure 2: Example of Tools at Various Phases in DevSecOps

In addition to the tools shown above, cloud service providers such as AWS and Microsoft Azure, provide their own set of tools to support the DevSecOps implementation. These tools will become more prevalent in the federal space as agencies continue to migrate their infrastructure to the cloud.

We have found that existing out-of-the-box solutions and frameworks are generic and are not always a fit for most of our customers' requirements. Many customers already have a technology stack in place. We leverage that technology stack and complement the tool set to provide the required toolkit for a DevSecOps implementation. This approach applied to the NCI CBIIT DevSecOps helped in identifying gaps in tools and processes, helped us to introduce multiple practices like automated testing using Katalon, performance testing using JMeter. We are incorporating these tools shown in Figure 2 in the build pipeline and development environment prior to implementing in customer's environment, while refining process definitions.

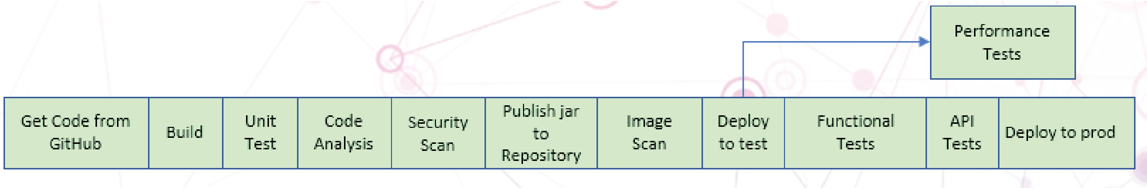


Figure 3. DevSecOps build pipeline

Once an organization has begun their DevSecOps adoption, **measurement and metrics of DevSecOps platform** provide the required transparency, understanding of the issues, and progress towards getting the best return on investment. Unissant team helps organizations to collect and track "High-Value" metrics such as Deployment frequency, Change lead time (for applications), Change volume (for applications), Change failure rate, Mean time to recovery (MTTR) (for applications), Availability, Customer issue volume, Customer issue resolution time, time to value, Time to ATO, Time to patch vulnerabilities; and “Supporting” metrics such as Test coverage, Developer onboarding time, etc., as referenced in GSA Guidelines. Team Unissant helps the customer to interpret current measurement and use it effectively to manage risks and maximize value and business benefits. These metrics helps us to derive maturity of the DevSecOps team and suggest any improvements if necessary.

Why Unissant?

Unissant’ s approach to Agile Engineering and DevSecOps offers our customers the best return on their investments and the most agility in accomplishing their mission. Our services support our customers’ DevSecOps journey by adopting Continuous Integration, Continuous Delivery using DevSecOps delivery methods, tailored to Government standards: enabling agility, productivity and responsiveness to cybersecurity needs.

With a 360-degree view of DevSecOps and Agile enablement, Unissant will provide a full range of offerings in DevSecOps that help organizations to align their business, applications, security and operations teams through our mature services in DevSecOps and Agile consulting and delivery.

At Unissant’s Innovation Center, we continuously experiment with various DevSecOps tools to determine their feasibility to meet our customer’s needs. We collaborate with leading vendors to develop and demonstrate a proof of concept in a safe and secure environment.

About Unissant

Unissant is an advanced data analytics and business transformation services provider with expertise in healthcare and health IT, finance, national security, and energy. The company delivers innovative solutions to assist government agencies and private sector businesses in tackling their biggest challenges. Founded in 2006, Unissant is a prime contractor on various government vehicles such as CIO-SP3, GSA PSS, GSA HealthIT SIN, and GSA 8(a) STARS II and is a CMMI Level 3, ISO 9001 & 27001 certified company headquartered in Herndon, Virginia with a satellite office in San Antonio, Texas. In March 2017, Unissant received the Government Project of the Year award by Small and Emerging Contractors Advisory Forum (SECAF). Unissant has experience with implementing machine learning solutions and full stack implementation on cloud. Unissant is a Select Consulting Partner Public Sector and is leveraging this relationship with AWS to strengthen our ability to support our customers in their Digital Transformation journey. We are already supporting several of our customers in the public sector with their Machine Learning implementations, cloud adoption strategy and implementation.

Copyright

Restricted Rights Legend

Information in this document is subject to change without notice and does not represent a commitment on the part of Unissant. This document is provided “as is” without warranty of any kind including without limitation, any warranty of merchantability or fitness for a particular purpose. Further, Unissant does not warrant, guarantee, or make any representations regarding the use, or the results of the use, of the written material in terms of correctness, accuracy, reliability, or otherwise.

For additional information on Unissant full range of services, please visit our website at www.unissant.com or call us at 703.889.8500.