MICRO FOCUS
Government Solutions

Top Reasons
Application Delivery Management
Security

10 Foundational Elements of DevSecOps in Government

Government institutions hold higher standards for security operations and governance than most industry and commercial organizations. Such stringent parameters prevent agencies from becoming fully agile. The following principles offer critical guidance to government agencies in the successful adoption of a DevSecOps culture.

1. **Proactive Continuous Improvement.** Organizations often make reactionary changes when a significant event occurs (i.e. new leadership, restructuring, etc.) However, proactive changes are often done in isolation, with limited data, and without keeping the value stream at the forefront of the conversation. Value Streams must be continuously evaluated for effectiveness in driving improvements and managing costs, resources, and more. Real-time measurements and review of success factors plus retrospectives on a recurring, predictable basis are methods commonly used to drive this behavior.

2. **Culture of Experimentation.** As an organization matures, it strives to adopt a culture of safety, thereby inherently reducing the amount of innovation that is readily accepted. This consequence often inhibits easy and small incremental changes that allow an organization to deliver value faster.

3. **Success through Teaming and Collaboration.** Teaming is the action of practicing teamwork on the fly with dynamic team composition. Collaboration occurs when teams have shared goals and metrics that they are measured on, actively working together to achieve those goals and metrics. These principles in action allow an organization to focus on the value provided holistically throughout the value chain.

4. **Flexibility of Team Methodology.** The methodology of how a team delivers their contribution to a value chain should ultimately be determined by the players. This allows a team to find the best, most effective way to operate. However, in recognizing large organizations are often accountable to external parties, by necessity certain parameters must be defined by the business. For example, the business might need to standardize on two week sprints (iterations) and the various metrics to be reported: yet the team can determine how to meet these standards based on the understanding of the dynamic with which the team interacts.

5. **Complete Transparency of Data, Information, Process and Status.** Visualizing data relating to the delivery of value is key to understanding and providing control and governance over the value chain. In addition, this concept extends to knowing and understanding information and/or details each part of the value chain needs to perform their activities. Possession of this information provides the ability to optimize Work In Progress (WIP), as well as understand the entire value delivery process.

DevSecOps is a cultural movement supported by technology. Within government institutions, there are higher standards for Secure Operations and Governance than in most commercial organizations. These restrictions tend to keep government agencies from becoming fully agile and moving at the speed of multiple releases a day. It is imperative that the culture of organizations shift to focus on critical principles required to successfully adopt a DevSecOps culture.

Contact us at:
www.microfocusgov.com

Like what you read? Share it.

6. **Foundational Definitions and Metrics.** Establishing a foundation of standard metrics and definitions is critical to the successful delivery of value to an organization. Teams are often not aware, nor do they have access to the metrics and definitions, adding confusion and creating rework, or non-value-adding additional work. Providing a clear understanding of the metrics against which a team is being measured allows for leverage of tooling to produce consistent reporting and significantly reduce the amount of rework that occurs.

7. **Lean, Value-Focused Processes.** In many organizations, processes are viewed as barriers to speed and agility. However, this does not have to be the case. For DevSecOps efforts to be successful, an organization should define lean, value-focused processes that enable teams to deliver value efficiently and effectively. These processes must be adhered to and consistently evaluated for effectiveness to target and eliminate bottlenecks in the value chain.

8. **Measuring Success with Value.** In defining success criteria for programs and contracts, the delivery of value should be first and foremost. All too often, contracts are written based on the completion of tasks, which does not drive collaborative behavior. Ultimately, to be successful, the ability to quickly adapt to changing requirements and collaborate throughout the value chain needs to be incentivized and codified in contracts and success criteria.

9. **Security from the Ground Up.** Security is a philosophy and mindset that must be adopted throughout the entire value delivery process in order to reduce the amount of rework and achieve the speed of change demanded by organizations today. Often, security is treated as a tactical reaction, introducing waste into the value stream. Proactively designing and introducing security into the requirements and using automation appropriately throughout the value chain will result in a dramatic reduction of waste.

10. **Integrity throughout the Value Chain.** A value chain's integrity must be secured in order to ensure the success of the ultimate deliverable. Without this integrity, an organization risks having bad actors injecting unauthorized changes and reducing the ability to properly secure and validate the ultimate deliverable.

Interested in discussing how to apply these principles to your organization? Reach out to us at **sales@microfocusgov.com**

Micro Focus Government Solutions
Headquarters
8609 Westwood Center Dr.
Suite 700
Vienna, VA 22182 U.S.A.

Additional contact information and office locations:
www.microfocusgov.com

MICRO FOCUS
Government Solutions