DevSecOps Powers Public Sector Innovation

Continuous improvement and integrated security - at scale

Security is a shared responsibility, integrated from the start

Security used to be the exclusive responsibility of an isolated team–tacked on in the final stage of development. In order to take full advantage of a DevSecOps approach:

- Shift security left, as early as the planning stage
- Identify the security controls necessary within a given app
- Prioritize speed to market for different apps
- Automate security features for repeated tasks to keep workflow from slowing down
- Select the right tools to integrate security and meet your DevOps security goals

DevOps speeds innovation by closing the gap between development and operations, but the speed gained can be undermined by poor security planning.

DevOps is for everyone

While DevOps specifically refers to development and operations, the practice is most successful when spread throughout the agency. DevOps relies on a culture of collaboration that aligns with open source principles and transparent, agile approaches to work.

With the right leadership and incentives in place, your development and operations teams can help facilitate an open culture. Transforming into an open organization means embracing principles that reflect open source values:

Transparency

In transparent organizations, materials, decisions, and processes are open, collaborative, and can be adjusted and revised if necessary.

Inclusivity

Organizations that are inclusive seek out diverse points of view and invite multiple perspectives into dialogue whenever possible.

Adaptability

Flexibility and resiliency are key elements of organizations that are oriented toward continuous learning and engagement, which contributes to greater longevity.

Collaboration

Individuals in an open organization believe that work is better when more parties are involved, and it lends the work to enhancements over time.

Community

Open organizations are communal by default. Shared values and purpose guide these organizations and are integral to their success or failure.

Security's Role in the DevOps Lifecycle

DevSecOps is a philosophy, movement, and culture of continuous improvement and integrated security–at scale. The result delivers powerful advantage for government agencies who are undergoing digital transformation: faster, more secure releases, greater interoperability and the freedom to focus on the mission.

A process of continuous delivery

DevSecOps is not just about speeding up creation of the same old monolithic software, it's about creating new kinds of software better suited to this cadence of continuous delivery and eventual migration of DevOps workloads to the cloud.

Automation:

- Enables an infrastructure to withstand the constant code changes that come with DevOps.
- Allows environments to continuously scale with ease.
- Frees teams to focus more on strategic projects and less on repeatable, predictable tasks.

The Automation to-do list:

1. Maintain short and frequent development cycles.
2. Integrate security measures with minimal disruption to operations.
3. Keep up with innovative technologies like containers and microservices.
4. Foster closer collaboration between commonly isolated teams.

All of these initiatives begin at the human level—with the ins and outs of collaboration at your agency—but the facilitator of those human changes in a DevSecOps framework is automation.

Treat your infrastructure like dev teams treat code

Selecting tools that support your processes is critical for DevSecOps to be successful. If your IT operations are going to keep pace with rapid development cycles, they will need to use highly flexible platforms.

Containers make it easier to move applications between development, testing, and production environments.

Using containers lets developers package and isolate their apps with everything they need to run, including, application files, runtime environments, dependent libraries, and configurations.

Containers support a unified environment for development, delivery, integration, and automation.

The DevSecOps Tools You Need:

Red Hat Ansible Automation Platform

A simple, enterprise IT automation technology that can improve your current processes, migrate applications for better optimization, and provide a single language for DevOps practices across your organization.

Red Hat OpenShift

Red Hat® OpenShift® delivers built-in security for container-based applications, including role-based access controls, Security-Enhanced Linux (SELinux)-enabled isolation, and checks throughout the container build process.

To learn more about Red Hat technologies enabling and driving DevSecOps, please contact:

Red Hat Solutions for Government
Toll-Free: (877)-RHAT-GOV
Main: (703)-871-8570
Fax: (703)-871-8505
Email: RedHat@carahsoft.com

Red Hat carahsoft