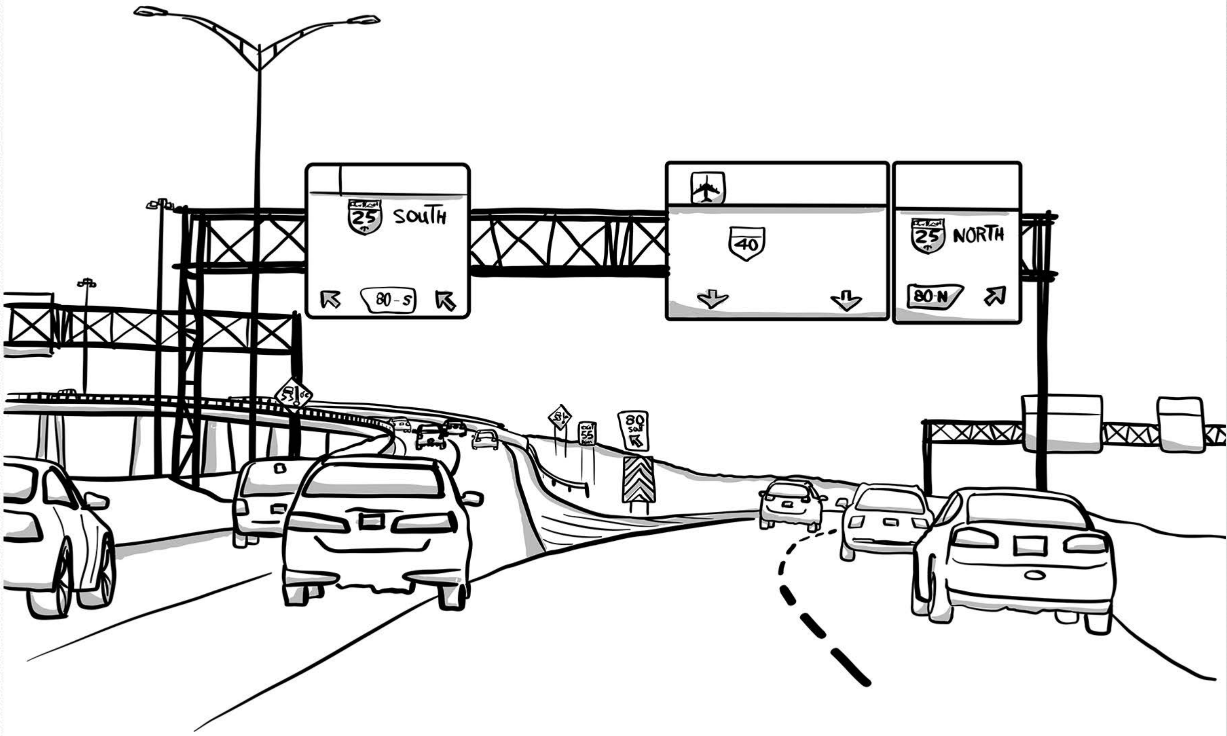
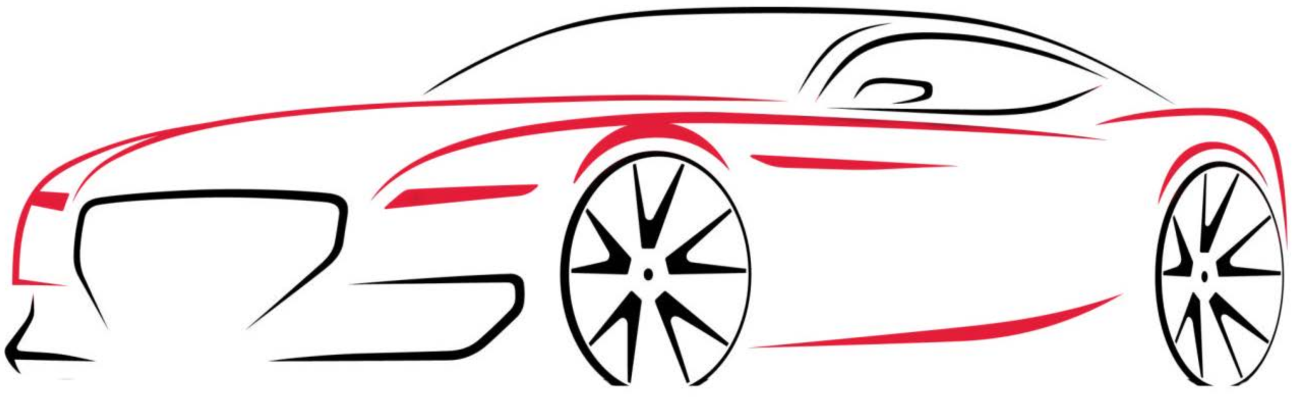


Finding the On-Ramp To the SecDevOps Highway

WHITE PAPER

The journey has been a long and winding one, but federal agencies have embraced Agile development. To further increase speed of delivery, more organizations are adopting DevOps practices such as continuous integration, automated testing, continuous delivery and continuous deployment. Previously separate development and operations organizations have joined on this adventure, driving together in one flashy red sports car toward digital transformation — windows open, top down, wind in their faces.

With great energy, these DevOps teams thrive at top speeds, delivering new levels of innovation and user-centricity. Then — slam on the brakes! They experience the jarring effects of progress halting when reaching the final security gates before production release.



BRIGHT RED STOP LIGHTS: SECURITY GATES HERE

Within the federal IT arena, security processes continue to be largely waterfall in nature. The reasons include:

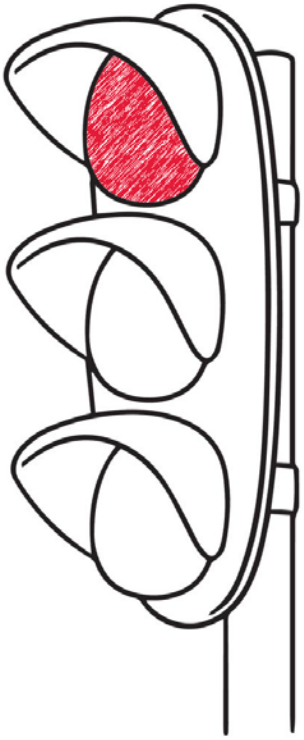
1. Existing policies (often not Agile enough to support DevOps practices)
2. Entrenched gate-driven manual processes
3. A lack of security personnel with Agile/DevOps knowledge
4. A considerable shortage of cybersecurity professionals across the market

As a result, when it comes to release management, the culture continues to be one of retroactive testing, supported by tooling that identifies potential risks based on known patterns.

Unfortunately, tools take a binary approach to their analysis – pass/fail. If tooling identifies a potential risk, all deployment progress comes to a halt. Potential vulnerabilities must then be analyzed (are these findings applicable to this specific product?) and approaches negotiated (fix a defect now or assign a plan of actions and milestones?). Once an approach is agreed upon, the government collects a number of approvals at various organizational levels -- a process repeated for each potential vulnerability identified. In the meantime, end users wait for valuable features that could improve productivity and streamline the work of government. And still security vulnerabilities exist, documented as plans of actions and milestones that can be costly to fix after the fact.

How can we raise the gate and get back to top transformation speeds without increasing risk? That’s what SecDevOps is all about.

Here are some of the ways we need to shift the mindset to get security, development, and operations all in the same vehicle together.



Why “SecDevOps” instead of “DevSecOps”?
While these terms are often used interchangeably, the term SecDevOps puts security first, affirming its importance.

1. PUT SECURITY FIRST BY SHIFTING LEFT

Before code is developed, we must start with a secure architecture. Even sports cars are designed not only for speed but also for safety. Designing for security, including the most appropriate security policies based upon the solution architecture, mitigates the level of effort required for after-the-fact compliance.

In the SecDevOps model, we create a culture focused on secure coding standards. We incorporate secure coding standards into our Definition of Done and employ security testing at the point of build integration. We provide developers with access to static and dynamic code analysis tools, with potential vulnerabilities identified and addressed during the sprint instead of during release readiness testing.

With practice, we become better drivers. Likewise, over time, development teams become more proficient in security. They create fewer security vulnerabilities and identify risks quickly instead of days, weeks or even months later. The result – improved security while maintaining a consistent velocity.

2. LET PRODUCT TEAMS TAKE THE WHEEL

With security at the forefront, developers can take control of balancing risk and speed. With automated security testing as part of the pipeline, product teams gain early insight into potential vulnerabilities. Teams can establish a baseline security scan, categorize by risk, prioritize mitigations and continue this process against the baseline in subsequent iterations. In this way, security requirements are treated just like other aspects of the product backlog.

Working with their government product owners – who understand the business imperatives and solution architectures – SecDevOps teams can advise on the true risks of identified potential vulnerabilities. For example, when security tooling identifies cross-side scripting vulnerabilities, the SecDevOps team can analyze tool findings in light of the overall solution architecture, documenting when tool results do not reflect true risk given the libraries, frameworks and solutions used in the specific product architecture.

Where tool-identified warnings do not pose a risk, product owners can verify that there is no impact. Product owners task their SecDevOps teams with documenting the rationale, providing an audit trail of decisions made and rationales for those decisions. This approach places decisions regarding the tradeoffs between velocity and risk squarely with the product teams who understand the product best.

3. BUILD SOLID GUARDRAILS AND HELP NAVIGATE

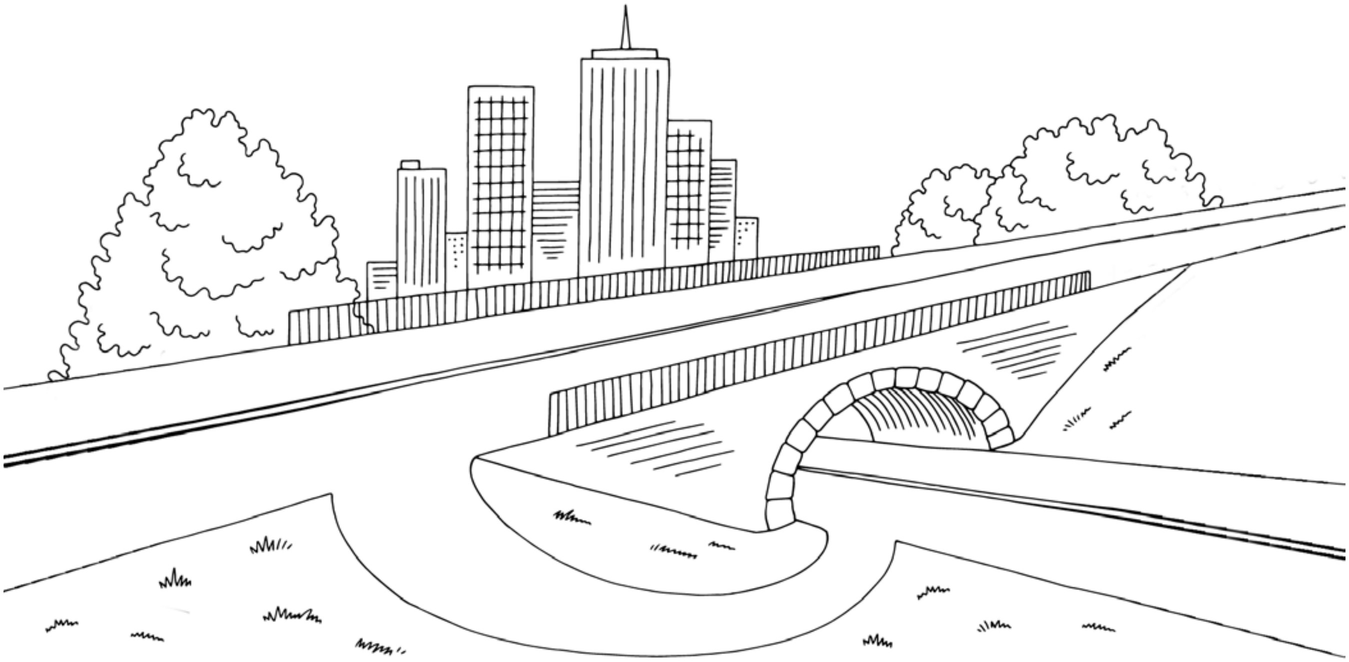
The move to SecDevOps inherently puts new guardrails in place for product teams. Because security testing is automated within the pipeline, testing is never bypassed, even in situations where speed is of the utmost concern. To support this model, security teams must change their focus from gates to guiderails, helping product teams keep the car firmly on the road.

Leveraging their unique expertise, security leaders help design the appropriate rules of engagement for the road, coaching teams to develop and operate products within approved guardrails. They serve as the subject matter experts for the relevant TIC, FedRAMP, NIST, and OMB requirements; approved system configurations (e.g., VM/container images); and secure network cloud configurations using templates such as Azure Resource Manager and AWS Cloud Foundation.

At the same time, the security function pivots from gatekeeper to navigational support. They help establish golden instances that become the model for instantiating new services. Working within product teams, they support SecDevOps practices such as infrastructure as code and policy as code, enabling greater team self-service and improving security postures. They advise on potential road hazards, such as new security risks, as they are identified – much like your car's navigational system warns you of an accident up ahead.

There's Room in the Car for Everyone

In the SecDevOps model, everyone in the car is equally concerned with speed and safety. To successfully travel this road, everyone must agree to jump into the vehicle together – and that our destination is one and the same: new capabilities that enable the mission while securing agency data and systems. Jumping on to the SecDevOps highway will require process and policy changes along with a shift in cultural mindset. The journey will be scenic and at times bumpy as we adapt to this new cultural model. But we learn together on the journey and celebrate as we reach our destination.



ABOUT OUR EXPERTS

Sangram Deshmukh, Director of Consulting Services, has successfully led multiple client Agile and DevSecOps transformations. He currently leads DevSecOps initiatives as part of CGI Federal's International Diplomacy & Commerce (IDAC) business unit. A certified Scrum Master and AWS Certified Solutions Architect Associate, Sangram holds a Master's degree in Engineering Management / Systems Engineering from The George Washington University.

As a Lead Architect within CGI Federal's Regulatory Agency Programs (RAP) business unit, Dave Fladung partners with clients to deliver digital transformation through technology adoption, including cloud-based services and DevSecOps. A Director of Consulting Expert at CGI, Dave holds a Bachelor's degree in Computer Science from the University of Maryland and is a certified Scrum Master.

ABOUT CGI

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world. Operating across the globe, CGI delivers end-to-end capabilities, from strategic IT and business consulting to systems integration, managed IT and business process services and intellectual property solutions, helping clients achieve their goals, including becoming customer-centric digital enterprises.

Learn more at **cgi.com**