Guidehouse
Outwit *Complexity*

Moving to a DevSecOps Framework:

Why a Cultural Shift Is Critical to Success

Transforming development, security, and operations silos into pillars of cooperation in the technology environment will yield development cycles that are shorter, more efficient, and secure.

Transforming a tech organization to develop advanced technology solutions more efficiently, and more securely, while also improving employee satisfaction and retention is not a technological problem. At least, technology is only a small part of the story.

DevSecOps combines the three pillars of software development, security, and IT operations into a new delivery model. It is the evolution of DevOps, which brought development and operations into alignment but kept security on the perimeter as a separate function. By integrating security as a key pillar in the development process from the start, DevSecOps ensures that software is developed securely from its inception.

DevSecOps incorporates robust software security with the advantages of Agile methodology and development practices, always-on and available-anywhere cloud computing platforms, and shared data throughout the entire information technology lifecycle. Solution providers have created a strong fabric of support tools and applications for DevSecOps that can help bring almost any legacy, siloed operation into the present day. But just as other revolutions in manufacturing, distribution, and quality-assurance practices took time to propagate, DevSecOps has not yet been adopted everywhere.

That is because the tools and technologies are only a small part of the transformation. Shifting to a methodology that prioritizes integrated security, rapid experimentation, and continuous communication requires a cultural shift as well. Without cultural acceptance of—and commitment to—DevSecOps' pillars, the tools and techniques will not take hold and propagate. Local, closed-box processes will gravitate back to isolation instead of becoming part of the DevSecOps collaboration.

DevSecOps Maturity at a Glance

Think of DevSecOps adoption as a spectrum rather than a rigid set of checkboxes. Every organization's interpretation will be slightly different. But in order to steer the culture in a DevSecOps direction, keep these goals and indicators in mind:

✓ **Shared responsibility underlies every action.** Positive user outcomes, quality, and security are owned by all contributors.

✓ **Security experts must be involved at the earliest stages of design.** They should not swoop in at the end of a development cycle to add security layers.

✓ DevSecOp teams should be **encouraged and empowered to communicate** with each other on a regular basis. Eliminating silos and blind spots through cross-team collaboration is everyone's responsibility.

✓ **Speed and fluidity are more important than perfection.** Keep an emphasis on continuous improvement (CI) and continuous delivery (CD), rather than a single monolithic release.

✓ Ensure that a **high-ranking internal champion** is responsible for leading DevSecOps transformation across the organization.

✓ The champion and other leaders should **drive continuous improvement and refinement** of DevSecOps practices.

Top Traits of Successful DevSecOps

Address resistance from software, security, and IT resources.

Software development, security design, and IT operations generally grew as distinct disciplines. As a result, practitioners feel pride and ownership in their abilities and contributions. Many see themselves as defenders of their technical domain and may (openly or privately) consider their contributions to be more important than the other disciplines. So, resistance or reluctance to embrace DevSecOps practices may come from a fear of loss of identity or sovereignty. Some may feel that their contributions will be swallowed up and made less visible or attributed to others.

DevSecOps in practice should emphasize removing the artificial and unproductive silos between these practitioners and their teams and avoid projecting the sense that individual or group contributions and skills are being masked or subsumed. For the technical-minded, DevSecOps can be positioned as a pathway to reduce the possibility of unforeseen incompatibilities or bugs. For those who prize their contributions to end-user experience, improving the odds of a high-quality delivery with shorter development cycles and fewer security risks should get the spotlight.

Even when technology needs refreshing to support a DevSecOps shift, it should not be the only focus. DevSecOps does not require a particular technology for its own sake. However, approaches that treat infrastructure as flexible rather than fixed set the best cultural tone. Think in terms of cloud environments, containers, and service meshes, rather than fixed, finite equipment.

Build collaborative culture around the DevSecOps pillars.

Another way to ease the cultural shift to DevSecOps is to focus on transforming the separate silos of development, security, and IT operations into the collaborative pillars of the new framework. This approach acknowledges that the silos were constructed and maintained with good intentions at the time, and by and large have been responsibly managed in good faith.

It's easy to feel threatened when hearing the term "breaking down a silo." Thinking of the transition as involving pillars to be built up instead of silos to be destroyed keeps each team focused on what comes next, rather than on defending what has gone before. (Of course, other incentives in the form of additional departmental investments or workplace upgrades may also be needed to speed the shift.)

Software development: Developers should take on more responsibility when it comes to configuration and containerization, tasks that in the past were likely to be the exclusive domain of IT operations. Meanwhile, developers can actively design configurations that will be easier for IT operations to support and maintain, while collaborating with security professionals for security-by-design.

IT operations: Bridging the divide between software developers and operations teams grants software developers more exposure to production-level shipping of code, while allowing operations teams to interface frequently and fluidly with software teams. Automated testing and monitoring practices allow software deployment to be streamlined from the development team to the production environment at a much faster pace.

Security: Automation can either strengthen or attack application security, and there is no substitute for human review and expertise. Experienced security professionals are supported by peers in software and IT operations, so that security can be validated and tested throughout all phases of development. Security becomes a contributing pillar within a well-designed application.

For more information,
please contact:

Bob Dunmyer
Partner
bdunmyer@guidehouse.com

Bassel Haidar
Associate Director
bhaidar@guidehouse.com

Guidehouse Technology Solutions

LinkedIn
https://www.linkedin.com/showcase/guidehouse-technology-solutions/

Twitter
http://www.twitter.com/GHTechSolutions

Address cultural challenges.

It is important to acknowledge that some cultural friction will remain during a DevSecOps transformation. The formerly predominant waterfall methodology of tech development and delivery is comfortable to many because it is both familiar and intuitive. Instead of condemning past practices, focus the cultural shift on the advantages to come: shorter time to resolve change requests, less energy spent managing stakeholder expectations, fewer hours wasted on suboptimal solutions based on outdated information, and eradication of the previously inevitable delays caused by sequential development practices.

Security is a special case, because in many ways the traditional, explicit role of the security team was to act as a roadblock and gatekeeper. In a conventional waterfall method, products must be submitted to security prior to implementation. The security team then either blesses the product, bakes in security layers that may not be well-integrated with the product or the end-user goals, or rejects it and sends it back to the development group for further work. Even in the DevOps approach, security in many cases was still a separate team that coordinated only in the final stages of development.

These approaches gave security professionals confidence that they could control the release cycle and protect the product and the organization's reputation. But, in many organizations, it also established an adversarial relationship between the security and development teams and increased the risk of deployment delays resulting from major revisions demanded by the security team. For these reasons, security professionals can be the hardest to bring into the cultural fold—they simply have had a less-collaborative relationship for longer. As a result, a cultural appeal to rally to DevSecOps will be incomplete unless it addresses the special barriers created by security's historical role as a rigid checkpoint and emphasizes the advantages of security-by-design.

Keep pushing for success.

Technology leaders interested in migrating to DevSecOps must consider the unique cultural challenges and adjustment processes that each team and contributor will face. Organizations that have started a DevOps journey must remember that security will be a new partner and should not be positioned as junior to the entrenched developers and IT operations personnel who have already ironed out some of their communications difficulties.

And all organizations should remember that DevSecOps represents a significant evolution in workflow and management styles, but it is a shift that will reward them with more efficient development cycles and more resilient software. Change management practices from experienced DevSecOps discipline partners, such as the professionals at Guidehouse, can help smooth the individual and collaborative paths to success in this emerging discipline.

To learn more, contact us, or read on for information about some of the unique tools and methodologies that can help make your DevSecOps transformation a success.

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 12,000 professionals in over 50 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit **www.guidehouse.com**.