Guidehouse
Outwit *Complexity*

Moving to a DevSecOps Framework: How to Make the Cultural Shift

Cultural commitment to DevSecOps is just as essential as having the right tools, talent, and management in place.

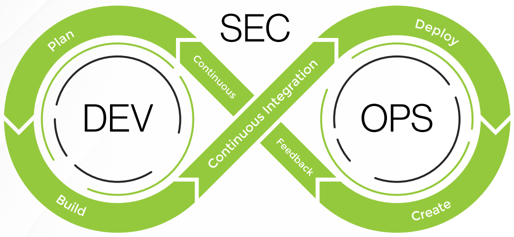
Organizations shift to DevSecOps to combine the advantages of Agile development practices, powerful cloud platforms, and shared data infrastructure. But a DevSecOps transformation requires more than just developing skills and adding tools. A cultural shift is needed to make the most of DevSecOps methodology and truly fuse the three pillars of software development, security, and IT operations to deliver superior digital solutions.

Lead From the Top

In an ideal world, every stakeholder would be equally enthusiastic about the shared-governance and collaborative priorities of DevSecOps. In reality, some of these goals can be difficult to achieve, with barriers ranging from inertia to territorialism to lack of appreciation for cross-functional skills. Clear and unwavering buy-in from top leadership is essential to overcoming these challenges.

Contributors may be asked to take joint responsibility for a result or a KPI that was previously unknown to them or viewed simply as “somebody else’s problem.” At the grassroots level, developers can model behavior but cannot enforce it in others. Middle managers can incentivize, reward, or punish, but ultimately do not set the tone for the entire organization. Those who do must make clear that the DevSecOps shift is both meaningful to the overall mission, and permanent.

This means leading with material support, not just rhetoric. Executive sponsors should be prepared to provide adequate and (if necessary) increased budgets for the talent, skills, and tools identified by practitioners and team leaders as essential to supporting a DevSecOps regime. This includes adequate budgetary support for separate test and production environments, and a cultural understanding that a smooth transition from test to production is a top organizational priority.



Executives should also work with department heads to expand the range of upskilling and learning opportunities to help propagate better understanding of best practices in information security, comprehension of new languages, and opportunities in development and deployment models. As hiring and retention needs change, top leadership should reassess expenditures and standards in those areas as well.

Keys to Security Involvement

As the “new partner” in an existing DevOps scheme, security earns a great deal of the cultural spotlight. To ensure a smoother cultural integration, it’s important to make the process feel authentic and as equal as possible. This may be difficult at first, because developers and operations personnel may feel that security responsibilities are being added to their already full plate. Dedicated security professionals, on the other hand, may feel protective of their domain expertise and not see the immediate advantages of the ongoing collaboration with their cross-functional peers.

A strong initial gambit is to present security with a way to onboard other contributors into security work while reducing a burden. Consider giving security the opportunity to mentor developers and operations experts on the most effective ways they can contribute to code review and improvement. This can help empower security, with the understanding that security-trained developers can be used to make initial vulnerability assessment a shared responsibility at the earliest possibility.

> As these are truly matters of culture and human interaction, there is no single path to guaranteed success. From our experience helping several large organizations with DevSecOps methodology, we can offer field-tested guidance:

✗ **Don’t:** Lead a transition by saying that the KPIs previously applicable only to the security team now apply to all stakeholders.

✓ **Do:** Emphasize that the organization’s goal has always been to minimize vulnerabilities, downtime, and material breaches while also reducing delays in delivering new features and capabilities—and that DevSecOps collaboration gives everyone a stronger hand in advancing toward those goals.

✗ **Don’t:** Assume that security professionals will be unreservedly enthusiastic about being part of a continuous development process.

✓ **Do:** Be diligent in assessing the workload of security personnel during and after a transition to DevSecOps, and expand the roster or reallocate tasks as needed to maintain a positive working environment.

✗ **Don’t:** Assume that developers have always courted the opportunity to take a more active hand in security.

✓ **Do:** Use educational opportunities and peer modeling to show that the most successful developers at the most successful organizations participate in a DevSecOps-driven cycle of shared responsibility.

Stay Alert for New Opportunities and Challenges

Just as DevSecOps emphasizes continuous improvement, a DevSecOps culture should mirror that priority.

Stay alert for emerging blockers and bottlenecks in development. For example, a well-oiled and seamlessly connected internal team may struggle to integrate cleanly with outside contractors. The organization should be vigilant in assessing whether the barriers are cultural, technological, or both. If contractors have limited access or visibility to the workflow tools used by internal contributors, throughput will suffer.

Keep participants clearly informed of project status. Meetings and emails can have diminishing returns, but configurable dashboards give everyone access to a granular, on-demand view of important tasks and obstacles. For instance, a clear readout of progress for every item in a sprint can be a real boost to DevSecOps productivity.

Don't lose sight of dependencies. The log4j vulnerability exposed a difficult truth: a vulnerability in a core software package can ripple out to literally tens of thousands of other products in the wild. Experts expect it will take years to fully track down and correct all of the affected packages which contain the log4j weakness. Part of the DevSecOps culture should include careful understanding of all of the underlying elements of the technology an organization deploys, and stay alert for security issues which may not surface for years.

Tools and Techniques

DevSecOps culture needs technological support to turn a spark into a sustainable engine. Guidehouse is a vendor-neutral DevSecOps practitioner and consultant, so these are just a sample of the effective approaches we have successfully used and implemented for others:

- **STRIDE -** Short for spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege, this acronym provides a handy guide for the six top security attack vectors a bad actor is likely to use. It can be used as a checklist during security test cycles, as well as an accessible reminder for non-security professionals who need to brush up on security principles.
- **LINDDUN -** Similar to STRIDE, the LINDDUN mnemonic targets privacy threats. It stands for linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, and non-compliance. Privacy and security threats are frequently but not universally linked with one another, and so familiarizing development professionals with both provides important complementary insight.
- **PASTA -** A process for attack simulation and threat analysis that helps developers structure hypothetical attacks on systems with a seven-step process, from defining a target's objective to executing a model attack and analyzing the results.
- **Security modeling frameworks including Cairis, Threagile, and Microsoft Threat Modeling Tool -** Although different in execution, a wide variety of systems can help DevSecOps organizations map potential threats and weave protections into ongoing projects.
- **Code-sharing and version control platforms such as GitHub -** Infrastructure to help contributors from several disciplines share the same codebase has dramatically improved in recent years. Whichever your organization chooses, keeping your contributors trained and actively participating in the platform should be a top priority.
- **Code linting tools -** These check for programming and style errors that can lead to vulnerabilities, loops, or other lurking, hard-to-kill bugs. Today these are frequently integrated directly into the IDEs used by developers.
- **Continuous improvement enablers such as pytest, CircleCI, Jenkins, and GitHub Actions -** These solutions manage and automatically run unit and integration tests, which can save significant amounts of development time and angst by identifying issues early.
- **The Threat Modeling Manifesto –** This document provides a set of high-level values and principles to consider when deciding which threat modeling methods and tools best fit your organization.

For more guidance on tools and methodologies that can assist with both the technical and cultural challenges of DevSecOps, look to the Open Web Application Security Project (OWASP), a nonprofit organization that provides timely analysis and advice on a wide range of threats.

Conclusion

The cross-pollination in DevSecOps is a matter of people as much as one of process. Bringing the two together effectively takes a cultural commitment from all involved. Contact us to learn more about how to best blend leadership, individual effort, team mindset, and technological advances to meet your DevSecOps goals.

Guidehouse
Outwit *Complexity*

guidehouse.com

For more information, please contact:

Bob Dunmyer
Partner
bdunmyer@guidehouse.com

Bassel Haidar
Director
bhaidar@guidehouse.com

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**

Web: https://guidehouse.com/analytics @GHTechSolutions linkedin.com/company/guidehouse-technology-solutions