KPMG

Accelerate and stay secure

How to compete and grow the business using secure DevOps

August 2018

kpmg.com.us/cyber

Global CEOs recently surveyed by KPMG rank "Greater speed to market" as their number one strategic initiative.[1] As business models continue to evolve based on emerging technologies and market trends, IT organizations must refine and streamline their ability to plan, develop, and deliver top quality products both quickly and securely. This KPMG white paper explains how to enable your secure acceleration with an approach based on DevOps.

Many organizations are using DevOps methods to serve customers that expect fast and regular improvements and updates to software products and services. New risks often emerge with efforts to accelerate the push of software code to production. Meanwhile, attackers are embracing DevOps to accelerate their ability to create new threats. Now, IT organizations must optimize for speed *and* security to deliver and defend the value they want to provide to customers. Leaders are doing so with the help of Secure DevOps.

Understanding DevOps and Secure DevOps

DevOps, shorthand for Software Development and IT Operations, is a set of behaviors that reduces the "friction" between development and operations so software can be delivered to the market quickly. Organizations that adopt DevOps practices have been shown to outperform their peers in productivity, market capitalization, and organizational performance.[2]

DevOps is commonly considered a natural evolution of the agile movement. By automating as many aspects of the software development life cycle (SDLC) as possible, including testing and deployment, DevOps teams are able to release working code on a continuous basis, rather than at the end of a two-week sprint as may be found in agile environments.

DevOps teams include stakeholders across:

— Product management

— Development

— Quality assurance (QA)

— IT operations

— Information security.

We often find that leaders are confused by misinformation concerning DevOps. To clarify, DevOps is *not*:

— Automation alone. Automation is one of the pillars of DevOps, but focusing on automation at the expense of its other capabilities is limiting.

— Being cloud native. Using the cloud is an enabler for rapid architectural and operational agility, but in and of itself is not the same as DevOps.

— Being good at Dev and Ops. DevOps is about breaking down the silos between organizational domains to accelerate value delivery. The interplay is the focus, not individual performance.

— A tool. No one tool or set of tools alone are sufficient to move at DevOps speed. Process changes and organizational integration are required.

DevOps originally emerged to help organizations that deliver and maintain software to increase their competitiveness. However, there is good news for defenders: the same principles that enable DevOps help security practitioners to enhance their competitiveness against the attackers that threaten their organizations.

---

[1]Source: KPMG International, Global CEO Outlook (June 2017)

[2]Kim, G., Humble, J., Debois, P., & Willis, J. (2016). The DevOps Handbook. Portland: IT Revolution Press I

Secure DevOps is a defined approach that recognizes security's role in enabling better competitiveness while reducing risk. Secure DevOps seeks to make security as frictionless as possible in the application delivery pipeline so the business can deliver value rapidly. It also aims to align risk-reducing security activities to the business strategy via ever tighter feedback loops and by tying system metrics to business metrics. (See graphic on page 5, "Picturing Secure DevOps")

Getting faster *and* more secure

Companies face many hurdles in their efforts to release quality products quickly. Traditional security approaches introduce too much friction, slowing the SDLC. Yet, sacrificing security in response to demands to push code faster is a bad bargain—one that often results in new risks.

Risk can be mitigated by rethinking compensating controls inspired by lean thinking. Velocity can further be accelerated by reducing risk in smaller bits, more frequently across the application life cycle, thereby creating less friction for developers and operations professionals.

Consider traditional approaches to securing applications at large organizations. For many of them, security efforts consist of a best practice checklist, performed by a security expert before the code is deployed, and an annual penetration test once the software is in production. Current approaches consider "spreading" prevention and detection across more phases of the SDLC. One example of "shifting security left," or earlier in the cycle, is to embed application security talent from information security in development teams at the planning stage of sprint cycles. Scanning tools naturally test the code and automate pass/fail decisions before deployment. Well-managed bug bounty programs offer lightweight, 24-7 testing of software in production instead of relying on point-in-time scrutiny by a small team of penetration testers. This reformulation of how security can protect software leads to less risk.

> "In the same way as using a seatbelt while riding in a car reduces the risk of injury, we can make it safer to go faster using DevOps."
>
> — Caleb Queern, Manager, KPMG Cybersecurity Services

The other team

Against the backdrop of competitive pressures that require organizations to deliver value to the market faster, attackers are also upping their game. Consider these factors in their favor:

1. **The cost of powerful attacks continue to decline.** Toolsets like Metasploit quickly put robust hacking tooling within reach for attackers worldwide just days after vulnerabilities are discovered. Attackers can invest less in innovation, decreasing the time to exploitation.
2. **The low barriers to entry create more attackers.** With easy access to "off-the-shelf" hacking capabilities, more threat actors are in a position to impact our organizations.
3. **The talent to defend applications is scarce.** Information security expertise is in scarce supply, creating shortages of the very skill sets required to defend against an increasingly risky threat landscape.

What does great security look like?

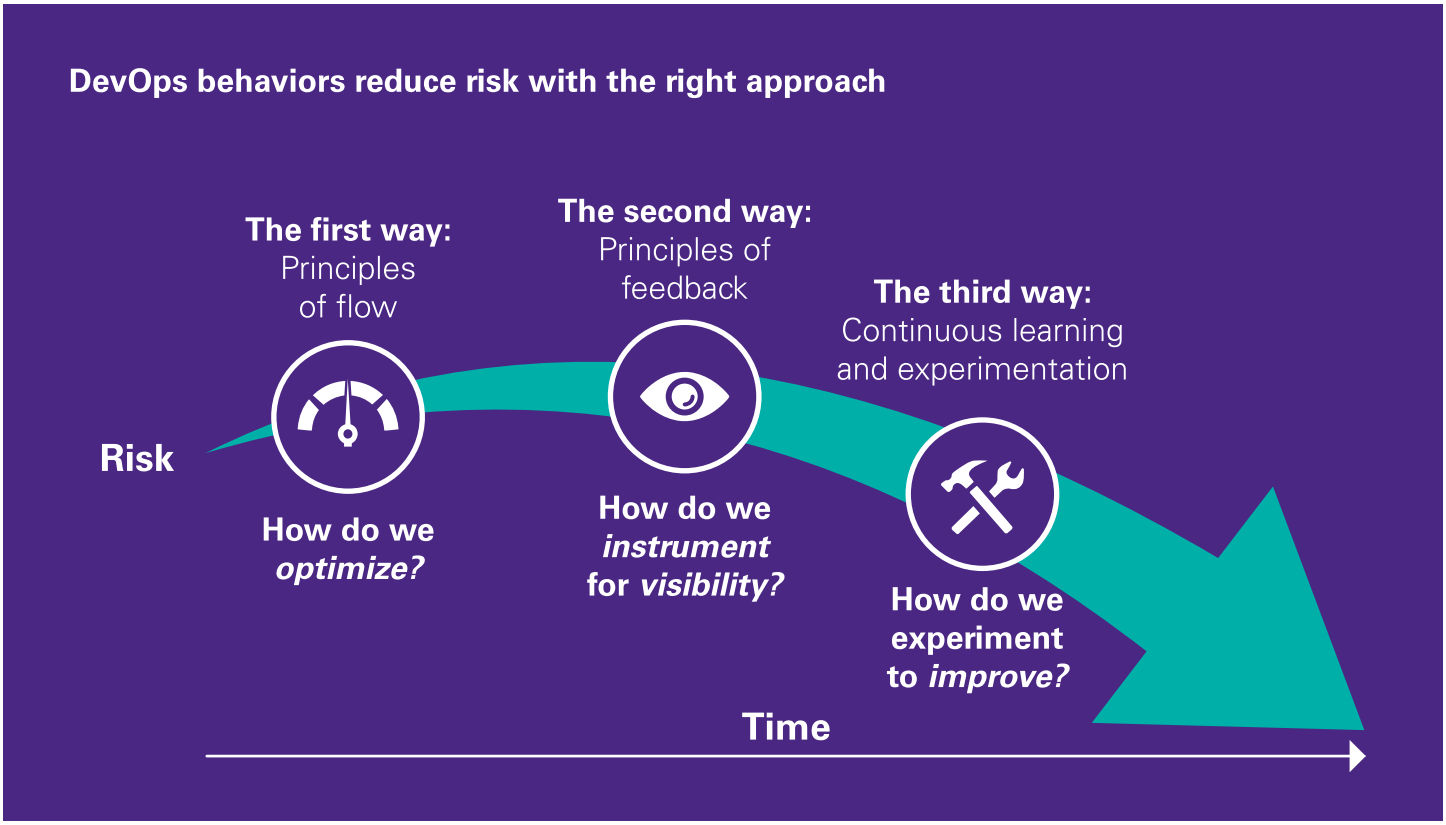
Specific steps help IT organizations achieve security goals throughout the SDLC. Teams focused on Secure DevOps aim to:

— **Reduce the security friction** on software development

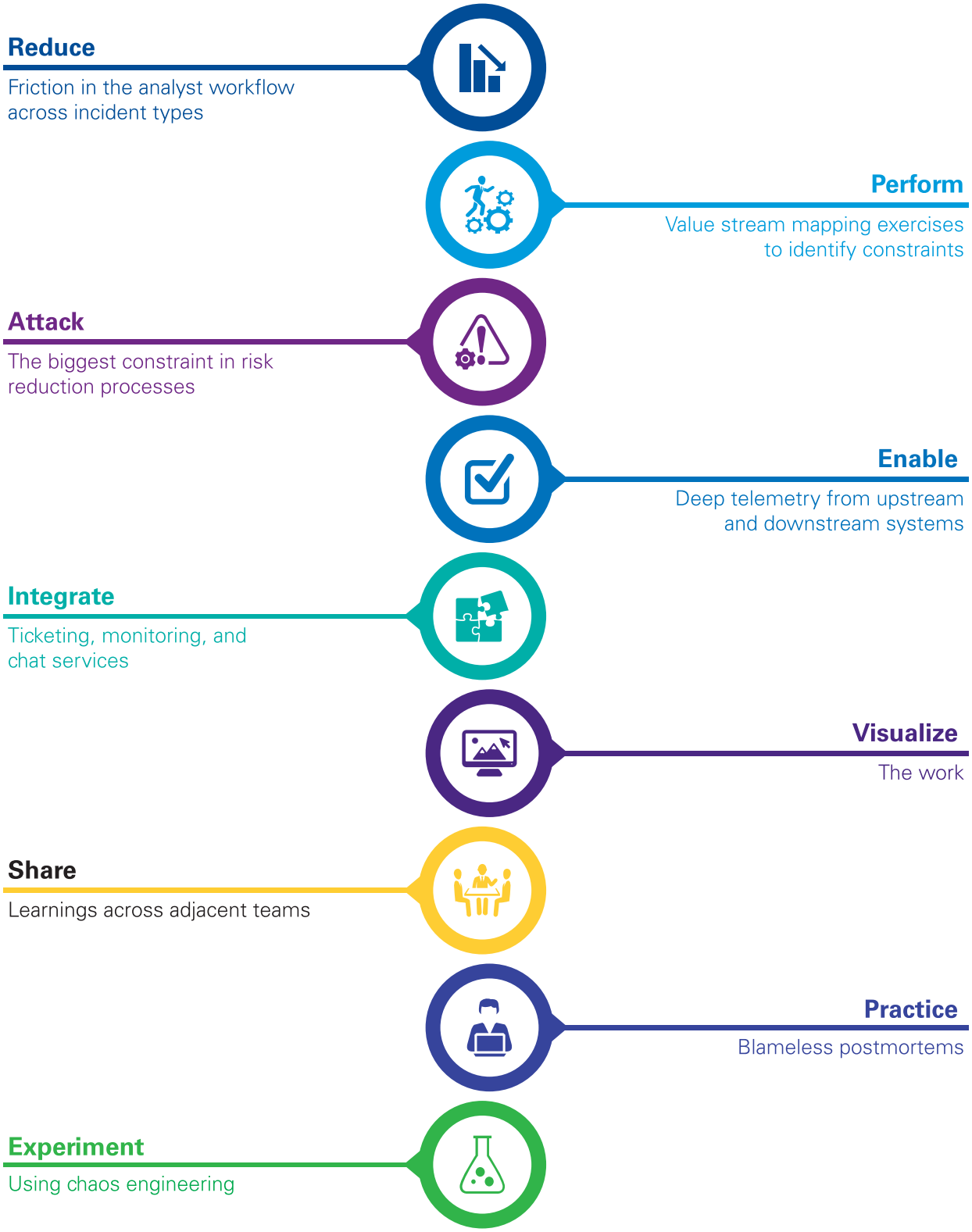
— **Make the work visible** so everyone can better understand where constraints happen and work together to solve them

— **Enable continuous learning** so developers and operations teams can reduce security risks continuously over time.

These "three ways" of DevOps represent the groups of behaviors that lead to high performance in information technology. All too often, however, KPMG sees companies won over by the tooling—particularly automation technologies—which can feel like a quick way to "do DevOps." Secure DevOps is not a box to be checked. If done right, it is a transformation in how work is done across an organization.



Picturing Secure DevOps: KPMG sees patterns in how clients are rethinking how they secure software faster.



Applying DevOps thinking to nontraditional areas

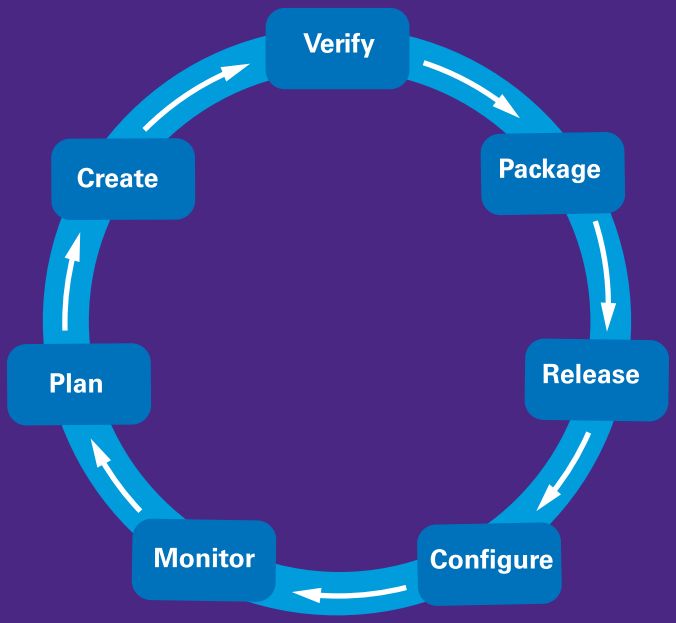
DevOps' roots in lean manufacturing principles sometimes bear unexpected benefits. In addition to accelerating software delivery, DevOps approaches can be applied elsewhere in the enterprise to drive value. For example, both security operations centers and vulnerability management activities are based on cycles that are particularly suited to DevOps optimizations. In the same manner that DevOps thinking can lead to more frequent code deployments, KPMG has applied DevOps approaches to reduce mean time to resolution metrics for security incidents and vulnerabilities detected by vulnerability scanners.

Background

— Delivering software to the market **makes** money.

— As the wheel below turns faster, the business delivers more value to the market.

— DevOps answer, "How can we make the wheel turn faster to **make more money**?"



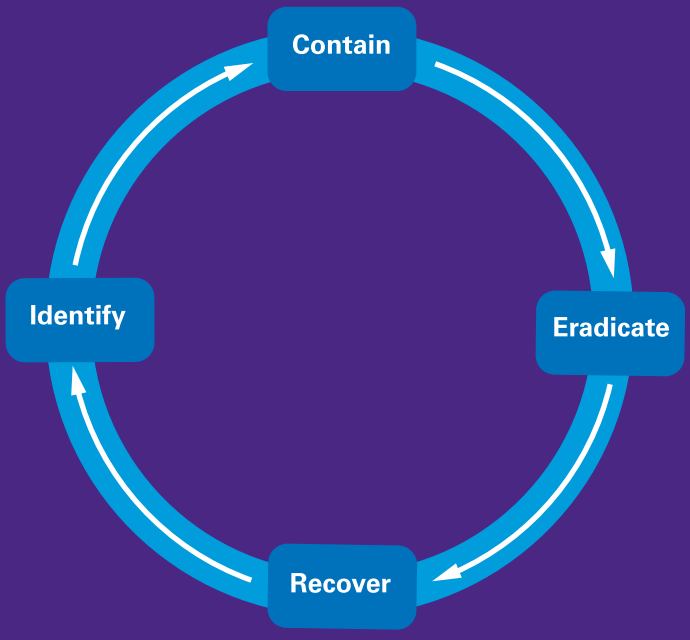
Gap of grief

Background

— Reducing risks saves the company money.

— As the wheel below turns faster, the SOC delivers more value to the company.

— DevOps in the SOC answers, "How can we make the wheel turn faster to **reduce more risk?"**



Historically, DevOps has been a counter to the friction that can emerge when multiple teams have responsibility for one end-to-end activity (value stream). The example seen most often is friction between development and operations, which occupy different organizational silos and may have goals that are not aligned. Security operations centers have similar silos, such as those that might exist between threat intelligence, Tier 1 and Tier 2 analysts, and forensics teams. Vulnerability management activities also often include groups from disparate teams, such as information security and development and operations teams. In both situations, using DevOps approaches to align work in a single, continuous flow can significantly increase the velocity of risk reduction across an organization.

Compliance at high velocity

Critics err when they point to conflict between adopting DevOps principles and achieving compliance. Some organizations do indeed allow developers access to production, but only those with compensating controls in place to mitigate the associated risk are likely to prevent serious incidents or dissatisfied auditors. Here are a couple compensating controls that organizations can adopt:

- Reduce code in small batch size: As the amount of code per deployment increases, so does risk. By reducing the number of lines of functional code per deployment, organizations can increase the likelihood that there are no unintended vulnerabilities or bugs in a given code release.
- Ability to roll back deployments quickly: Pushing new code to production quickly is risky without the corresponding ability to quickly return to a known good state. This may be one of the most underdiscussed aspects of "what great looks like".

Conclusion

Special considerations are required when the business demands and depends on speed. KPMG understands the need for appropriate compensating controls to mitigate and balance risk in the software delivery value stream. A strategic, holistic approach to cyber preparedness will not only protect valuable data but also enhance a company's agility and potential for growth.

Leaders should keep in mind that without a proper balance of people, process, and technology, their cybersecurity efforts are likely to fall short of leadership's expectations. In those situations, leaders should resist the temptation to return to "business as usual."

At the end of the day, the risks of not embracing Secure DevOps are considerable. In a rapidly changing business landscape characterized by quickly emerging new risks, competing successfully depends on your ability to accelerate securely.

Secure DevOps is a rich topic. KPMG Cyber will share more insights in a companion white paper focused on the more tactical "how" to secure DevOps.

Questions for leaders:

1. How frequently does your organization release code into production? Is that pace good enough, or would you like to get faster?
2. Are you confident that your organization can deliver software fast enough to support the business while satisfying auditors?
3. Can you identify the biggest constraint that security imposes on software development? If so, are you prepared to fix it?
4. Are your innovation efforts suffering because of unexpected costs of responding to security incidents?

Contact us

Steve Barlock
Principal, Advisory,
Cyber Security Services
E: sbarlock@kpmg.com

Vijay Jajoo
Principal, Advisory,
Cyber Security Services
E: vjajoo@kpmg.com

Deepak Mathur
Director, Advisory,
Cyber Security Services
E: deepakmathur@kpmg.com

Caleb Queern
Manager Advisory,
Cyber SecurityServices
E: cqueern@kpmg.com

kpmg.com.us/cyber

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia