What is DevSecOps?

While the fundamental principles of risk management remain the same in a DevOps world, the proliferation of open source components and greatly increased third party risk has significantly changed the journey towards the final outcome.

This journey is defined by DevSecOps, a growing approach within the industry, which integrates security into every part of the development process and allows organisations to manage software exposure at the speed of DevOps. Core security tasks are automated by embedding security controls, testing and processes in the DevOps workflow, rather than bolting them on at the end.

If security is embedded in the design, testing and management of code, the business has a better chance of identifying and fixing vulnerabilities at an early stage.

There are many iterations of what a DevSecOps approach actually consists of, however this can be broken down into 4 key principles:

- **Adapt security tools to the developers workflow.**
- **Secure applications at the source.**
- **Coach developers to adopt secure coding practices.**
- **Adopt an immutable infrastructure.**

These principles can at first glance seem rather difficult to put into practice without requiring more context. That is why we have consolidated these and added three key steps later on which address these principles.

In summary, when successfully implemented, DevSecOps reintegrates security, governance and compliance into the business’s adoption of cloud, IoT, mobile and digital operating models. But implementation is a complex business exercise that affects not just tech and security, but people, processes, culture, and ways of working.

How DevOps drives risk

Rapid innovation is the primary differentiator for companies competing in the digital economy. The race to innovate brought us DevOps, which was designed to encourage closer collaboration between developers and those working in operations – two groups who, historically, rarely worked seamlessly together.

While the ultimate aim of DevOps is to shorten the development lifecycle of systems and to deliver updates and new features that align closely with business objectives, the rapid advancement of digital solutions has put it under strain. As new trends emerged – Agile, the cloud, the Internet of Things and mobile technology – DevOps became the default operating model for implementation.

One of the unforeseen consequences has been a sharp rise in security risk. As corporate leaders aggressively adopt technology driven business models, cyber security programs are increasingly misaligned with the business. According to our 2018 Digital Trust Survey, only 53% of businesses that are executing digital transformation projects ‘bake in’ proactive risk management measures fully from the start. In the meantime, cybercriminals continue to outperform the cybersecurity industry, causing billions of pounds of damage.

The speed of innovation and development has left compliance, governance and security lagging behind. DevOps facilitates rapid innovation and implementation, but the fact remains that many security and compliance monitoring tools simply were not designed to operate at the speed DevOps requires. But the problem goes deeper.

The disconnected developer

The DevOps trend has resulted in IT developers becoming disconnected from security and quality assurance teams. Developers have the autonomy to write their own code at the speed the market dictates and, in most cases, security and governance are not a priority until the code is written.

For example, organisations often introduce a development team to transform a critical underlying business application into a digital and agile application to provide faster time to market. With little overhead and the use of agile cloud native technologies, the application can move swiftly from prototype into a pre production ready state without securing the cloud operating environment, third party code and organic code. The ultimate consequence of this process often means the development team has missed governance, compliance and even basic security needs resulting in potential regulator exposure and possible loss of valuable data.

Functions within IT, Risk and Business need to be included to help the transformation and manage broader risk to the organisation. The security team also need to be transformed into coaches for the developers, supported by automation and transparent integration of security controls into the developers workflows.

The open source problem

This was less of an issue for developers who were creating code from scratch, but the proliferation of open source components has significantly increased the risks. Many developers are now constructing code rather than writing it, borrowing what they need from open source third parties – with little or no process for screening these components. A survey of 1,000 organisations carried out in 2017 found that 96% were using open source components in their applications – and 60% of these had experienced security vulnerabilities².

This has effectively created an open door for cyber criminals, who have turned their attention to this weak spot in organisations’ software and supply chains. According to a recent report³, 77% of all compromised attacks in 2017 came not from downloaded files, but from vulnerabilities hidden in apps and software.

Developers have played a pivotal role in realising the potential of Agile, cloud, IoT and mobile technology, but in the process have left their organisations exposed to far greater risks. The nature of security and risk has changed. Addressing this challenge represents a paradigm shift for security and compliance within organisations.

---

¹ The journey to digital trust, PwC, 2018
² Survey by Black Duck Software
³ The State of Endpoint Security Risk, Ponemon Institute 2017
Three steps to successful adoption

**Step 1: Automate security into the developers' workflow**

Until now, governance has been considered outside the remit of developers. Integrating governance, risk and security processes into the DevOps role doesn’t create an extra step – in fact, it creates the potential for faster delivery and lower costs, as it eliminates the need for bolt on solutions.

The answer is to integrate assurance controls transparently into the toolkit of developers. Extensive automation of all the necessary governance and security checks and controls is the key to this, but it’s also essential to use developers’ workflow as a blueprint. This ensures that the necessary assurance processes are integrated into developers’ workflow without fundamentally changing the way they work.

An added advantage of this approach is that it brings far greater transparency to risk by allowing for multiple views of the outcome, depending on the perspective of each stakeholder. Different people have different priorities when it comes to risk – CROs, for example, are concerned about business risk, while the focus for CTOs is the quality of DevOps. DevSecOps allows each security risk to be translated for each audience to illustrate the potential impact on the business; the right data is presented to the right stakeholder.

**Step 2: Remove risk at its source**

On average, 70% of a typical software application is constructed from code sourced from third parties, and this is one of the biggest security risks for organisations. Organisations need to be confident that all third party code sources used by their developers are reliable and trustworthy.

The creation of a trusted repository that developers can use for third party code should be a priority, creating a secure library of trusted third party code where all sources are pretested and preapproved. Applying an assurance test at the automation stage, as a further safeguard, will allow code that has not come from an approved library to be quickly identified and removed.

**Step 3: Don’t underestimate the scale of cultural change**

‘Immutable infrastructure’ is an important principle of DevSecOps – that when a vulnerability is detected, the infrastructure is never patched or repaired but always shut down and rebuilt. Under DevSecOps, developers ‘own’ every stage of the application, from development to deployment and beyond. There are no stand alone teams that patch problems and eliminate bugs – the management system is strictly vertical and empowers developers to take responsibility for the applications in production.

The immutable infrastructure principle is an excellent example of the scale of cultural and organisational change brought in by DevSecOps. It requires a new way of thinking and a new way of working for developers and project managers, but also for the wider risk and IT functions. Developers, who have traditionally operated in siloes, will arguably feel the transformation most keenly. Their working environment will change, representing a cultural shift that needs to be sensitively handled. DevSecOps is not purely a technical exercise – it will have profound operational and cultural implications that call for careful planning and management.
Conclusion

DevSecOps is built around the three principles of speed, flexibility and risk management. Successful adoption creates, over time, a significant advantage in terms of competitiveness as well as a substantial fall in the risk associated with software vulnerabilities.

DevSecOps represents a new way of thinking and working throughout the organisation and as such, implementation must be handled with care, paying close attention to the three critical steps we have outlined. But once in place, the advantages are clear – safer innovation, greater visibility of software risks, and closer alignment between the organisation’s commercial objectives and developers who are a critical driver of success in a digital world.

Contact us:

Will Semple
Software Assurance – Director
PwC United Kingdom
M: +44 (0)28 9034 6638
E: will.semple@pwc.com

Intelligent Digital

At PwC, we are harnessing the power of Intelligent Digital, helping our clients rethink their futures and reshape their own world.

We’re using cutting edge technology, formidable human insight and industry expertise to protect what matters most to you.

Fear cyber attack? Attack cyber fear. With a risk based mindset we can build a secure digital society together.

pwc.co.uk/intelligentdigital