

DevSecOps: Why security is essential

An approach for integrating application security into your DevOps process and implementation



Digital is rewriting the rules of business. To stay in the game and move ahead of the pack, enterprises need a secure approach to building, testing and releasing modern applications at speed using a DevSecOps approach. Here are four steps to achieving DevSecOps success.

Digital transformation is well underway in virtually every industry, led by a host of new IT approaches that are redefining, and in many cases disrupting, the way business has traditionally been conducted with partners, suppliers and customers.

The need for speed with security

Social, mobile, analytics and cloud have radically changed how customers consume content, communicate, and choose products and services. They have also dramatically changed expectations for how quickly businesses bring new products and services to market. This requires enterprises to rapidly adapt their applications, which are playing an ever-increasing role in how business is being conducted.

At the same time, the cyber security threat has never been greater. We've evolved from a world where hacking is done by individuals looking for personal fame to hacking by organized groups that are often criminal or state-sponsored. These groups have access to sophisticated tools and software frameworks that make their jobs even easier — resulting in attacks that are far more sophisticated and organized. More importantly, these bad actors are beginning to collaborate, sharing intelligence and selling tools to make the art of the hack even more fearsome.

Further enhancing the threat is a dramatic increase in the attack surface brought about by new architectural standards such as cloud and mobile. This has led to an orders-of-magnitude rise in the number of devices that need to be protected, as well as the applications running on them. Devices such as laptops, tablets, smartphones and, more recently, smartwatches have become ubiquitous in enterprises both large and small. Plus, the internet of things (IoT) has brought about an explosion of sensors, appliances and other smart devices operating intelligently at the edge.

But this explosion of devices is just part of the story. Expectations for how quickly new applications are developed and released have also increased. Speed has become the new currency — and DevOps has become a critical enabler needed to develop and release applications at digital speeds.

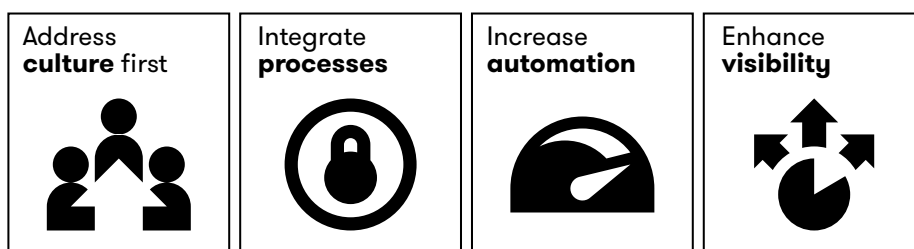
However, you cannot apply DevOps sustainably without addressing application security along the way. Failing to do so will result in a buildup of hidden “technical debt” in the form of unidentified security defects and vulnerabilities in your applications. This hidden technical debt may not be discovered until too late — that is, after a breach occurs, when the cost to the business may be overwhelming. And perhaps as important, failing to address application security runs the risk of undermining the trust that is crucial among your development, operations and security teams, who must work collaboratively to rapidly deliver business value.

DevSecOps is the term used to represent the seamless integration of security into the DevOps approach.

A four-step approach to DevSecOps

DXC Technology has defined a four-step approach for integrating application security into DevOps, the software delivery approach that unifies the once-siloed worlds of development and operations. (See Figure 1.) Our DevSecOps approach is based on our own DevSecOps adoption journey and more than four decades of experience in securely developing applications for thousands of businesses around the world.

Figure 1. A four-step approach to achieve DevSecOps



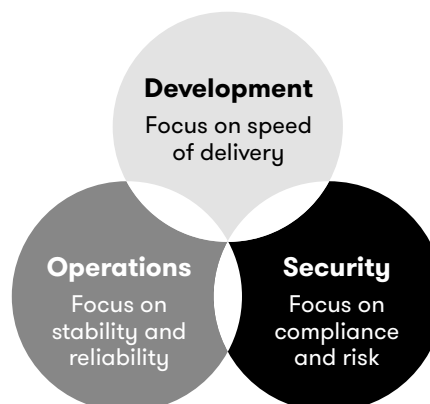
It begins with the realization that DevSecOps, like DevOps before it, is not a new technology. DevSecOps is a change in how application development, operations and security teams work together to build, test and release applications and application changes. It is a highly collaborative approach that accelerates business value by delivering secure and high-quality applications to business users much more quickly than traditional, less collaborative approaches.

DevSecOps doesn't happen all at once for most organizations; it is a journey. Although the DevSecOps journey is enabled by technology, the journey starts with culture change.

1. Address culture first

Recognizing that a culture change is needed is critical to successfully adopting DevSecOps. DevSecOps requires a shift in thinking and an evolution in how teams work together to support the business. Traditionally, development teams focused on delivering new application features as quickly as possible, often giving less thought to the security and reliability of the application. Operations teams focused on stability and reliability, with less thought on speed of delivery. And application security teams focused primarily on reducing risk. It is these different and sometimes conflicting goals that DevSecOps ultimately seeks to address. (See Figure 2.)

Figure 2. Conflicting goals with traditional methods



DevSecOps does this by enabling development, security and operations teams to work more closely together, with the common goal to accelerate delivering value to the business through the building, testing and release of secure, reliable, high-quality applications faster and more frequently. With DevSecOps, rapidly delivering business value is king — but it requires everyone in the value chain to be responsible for the security and reliability of the end product.

One way to address the culture change needed is through a combination of top-down and bottom-up approaches. The top-down approach requires that senior and executive leaders understand, support and champion the new approach. Identifying an executive sponsor and gaining leadership buy-in early are key.

Some may equate greater speed with increased risk. To tackle these concerns, it is important to show how DevSecOps doesn't ignore security, quality and reliability, but instead proactively addresses these elements to deliver higher-quality, more secure applications. Communicating this in conjunction with the many business benefits of DevSecOps — including greater efficiency, compliance and responsiveness to changing business demands — is often all that is needed to gain leadership support.

The bottom-up approach requires getting development, operations and security teams to buy into the new, collaborative approach. Having an executive or other senior champion helps, but it is often not enough. Teams need to understand and internalize the change, including the many benefits and how it affects them individually. Teams must trust that their colleagues have also internalized the change so that all are working in lockstep toward a common goal.

During our own DevSecOps journey, we found that a good way to address this is by bringing together development, operations and security teams in a series of interactive DevSecOps awareness and training sessions. These sessions, which we call our DXC DevSecOps Dojos, are interactive, hands-on workshops where teams learn about the benefits of DevSecOps, along with some of the common challenges and pitfalls that can be encountered during adoption. These sessions are led by experienced DevSecOps practitioners, who share real-world insights from their own experiences. They also include guided, hands-on exercises in our DevSecOps virtual lab so that participants can become more familiar with some of the DevSecOps enabling technologies.

Addressing application security proactively and early, as well as throughout the life cycle, helps to deliver applications that are “secure by design.”

2. Integrate processes

The second step of the DevSecOps journey is integrating processes. Many enterprises treat application development, including release management, and application security as two separate processes. This can lead to inefficiency and inconsistency while hindering communication and collaboration within and between teams. A single, integrated, end-to-end process helps teams to work together better, and can also help identify areas where automation can be applied to streamline and accelerate the process.

When integrating application security into your development process, an application security maturity model can serve as a good tool for gauging the right level of security to incorporate into the software life-cycle process, taking into account risk tolerance and any applicable industry or government regulatory requirements.

There are two things to watch out for:

- **Blending old and new methodologies can result in inefficiencies.** Care should be taken to understand how and why security fits into the existing process, and not assume that there will always be an exact one-to-one mapping into the new process. For example, embedding automated security quality checks into the process may eliminate the need for some of the tests from the old process while adding the need for others.
- **Application security should not be solely equated with application security testing.** Although application security testing is important, it is just one part of maintaining a robust application security practice. There are other activities, such as a security requirements gap analysis, that can and should be applied during early stages of the life cycle to reduce costs and ensure that regulatory compliance requirements are being met. Addressing application security proactively and early, as well as throughout the life cycle, helps to deliver applications that are “secure by design.”

3. Increase automation

With the culture change being addressed and an integrated process defined, the third step is to identify the parts of the process that can be automated to drive quality, consistency and speed. Extreme automation should be the goal, focusing not just on the process activities but also on the handoffs and interactions between different steps in the process. Documenting the DevSecOps pipeline will serve as your roadmap to help guide the automation engineering effort. (See Figure 3.)

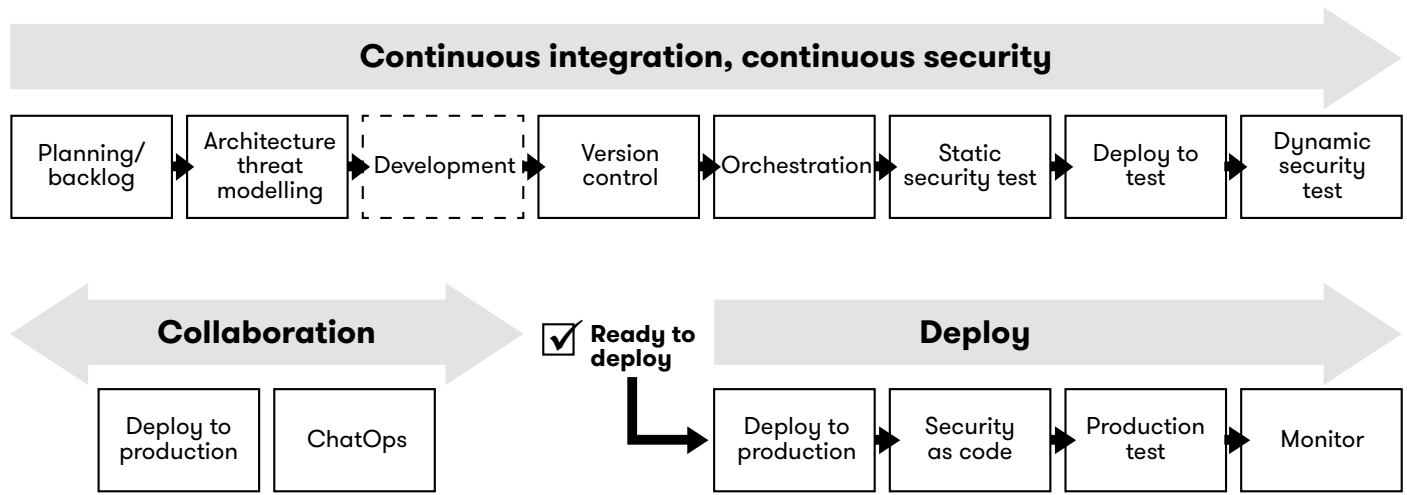


Figure 3. DevSecOps pipeline design example

Enterprises should consider two things during this step. First, because of the wide variety of different application platforms, most enterprises will require more than one type of DevSecOps toolchain to meet the needs of their diverse technology base. Enterprises should consider in advance which components they want to be common wherever possible across all of their DevSecOps toolchains. Having a common code repository, for instance, can help to drive greater consistency and reuse across projects.

The second consideration is that the DevSecOps technology ecosystem is large, growing and continually evolving. The tools you select today to automate your toolchain will likely change over time. This is nothing new; enterprises have been dealing with technology change for decades. Consider ways to minimize the impact of technology change as much as possible. When evaluating products and services, look for ones that support open integration using well-defined APIs for flexible and easy integration.

One area that benefits significantly from automation and integration into the DevSecOps pipeline is application security testing. Such testing should be done early and often in the life cycle to reduce the time and cost of remediating defects. This is enabled through automated security testing technologies that can be readily integrated into the DevSecOps toolchain using continuous integration tools.

DXC Applications Security on Demand is an example of one such service. It provides automated static and dynamic applications security testing using industry-leading application scanning tools hosted securely in the DXC cloud. The service includes open REST (representational state transfer)-based APIs, as well as plug-ins that can be used to quickly integrate into a variety of DevSecOps products.

Although identifying and implementing tools is the last step in our four-step process, this step often delivers the most value in terms of DevSecOps benefits.

4. Enhance visibility

The last step of the DevSecOps journey is about enhancing information visibility for business advantage. One of the many benefits of DevSecOps is the ability to harness the information collected through every stage of the software life cycle, across multiple projects, to gauge the health and effectiveness of the process in real time. Capturing application security testing information — and making it available through a centralized dashboard — can be an invaluable tool for development and security managers to monitor risks and identify trends.

This information can be used by development managers to plan training on how to reduce the introduction of security defects from the start, and to gauge the effectiveness of that training. This information can also be used by security practitioners as a benchmark to measure the effectiveness of the security controls embedded in the development process.

A variety of tools are on the market for capturing and analyzing this information. Although identifying and implementing these tools is the last step in our four-step process, this step often delivers the most value in terms of DevSecOps benefits.

Employ a proven approach

Enterprises are increasingly adopting DevSecOps as a means of delivering modern, secure, high-quality applications at speed. Achieving DevSecOps success is a journey for most organizations. The key to success is employing a proven approach that addresses people, processes and technology, and that prioritizes changing to a collaborative culture.

Learn more at
www.dxc.technology/asod

About DXC Technology

DXC Technology (DXC: NYSE) is the world's leading independent, end-to-end IT services company, serving nearly 6,000 private and public-sector clients from a diverse array of industries across 70 countries. The company's technology independence, global talent and extensive partner network deliver transformative digital offerings and solutions that help clients harness the power of innovation to thrive on change. DXC Technology is recognized among the best corporate citizens globally. For more information, visit **www.dxc.technology**.