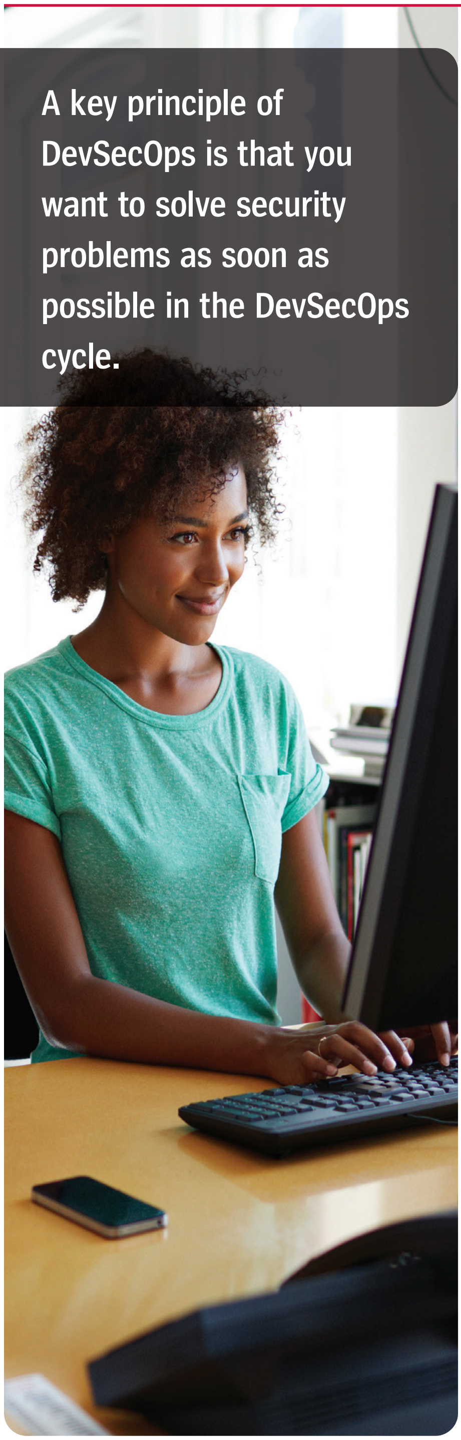
UNISYS | Securing Your Tomorrow®

Now That You Are in the Cloud, How Can You Get DevSecOps Right?

By Anupam Sahai



A key principle of DevSecOps is that you want to solve security problems as soon as possible in the DevSecOps cycle.

The adoption of cloud technology has changed everything — and that's good for businesses and customers. Agility and speed of innovation are much higher with the cloud versus on-premises.

The agile software manifesto and the proposed methodology allow businesses to quickly iterate and use customer feedback to expedite the release and iteration of their software-based solutions on the cloud. The lean business model further enables speed of innovation. This minimizes waste and encourages teams to deliver results faster by better managing flow and limiting the amount of work in the process to reduce context switching and improve focus.

Cloud brings in a higher velocity of data, with a higher volume, and a higher variety of computing and services. The above three trajectories are the market drivers for adoption of DevSecOps.

Gartner projects (via TechTarget) that by 2022, 90% of software development projects will claim to follow DevSecOps practices. Also, 25% of projects will follow a DevOps methodology from conception to production by that same year. DevSecOps provides companies with greater velocity, safety, and ease of software operation. It also decreases code defects and lowers costs.

Traditionally, organizations had separate development/engineering, quality assurance (QA), security and cloud operations teams. The developer team would pass work to the QA and security teams. They would then hand off to the cloud operations team. If things didn't work at that point, the deployment job would have to go all the way back to the development team. Now the boundaries between development, security, and operations are disappearing. Organizations are mashing them up into a single department called DevSecOps.

Within a year of Amazon's adoption of DevSecOps, its engineers were deploying code every 11.7 seconds on average. Netflix uses DevSecOps to deploy code thousands of times per day.

Embracing DevSecOps requires tooling, rethinking and reorganizing how teams work, how processes come together, and how to realize continuous integration and delivery. Here are some tips on how to get the most value from the cloud and DevSecOps.

People are the most important aspect of DevSecOps, which minimizes processes and depends on people to get things right with minimal processes.

Shift to the Left

A key principle of DevSecOps is that you want to solve security problems as soon as possible in the DevSecOps cycle.

Before you deploy software in the cloud, that software goes through multiple stages of validation such as in dev and test, a preproduction cluster, a staging cluster, and then the production cluster. The software goes through a security and deployment readiness gate check at every stage. If it fails that test, it needs to go back to the beginning. Whenever that happens, you lose valuable time.

That’s why you want to shift problem-solving to the left end (or beginning) of the DevSecOps continuum to minimize rework and delays. You want to emphasize the importance of solving as many problems as possible in the development stage. This minimizes rework so it is much more efficient than waiting until later in the DevSecOps process to find issues.

Use tooling and automation to facilitate this. For example, you may want to consider using a source code security analysis tool that does source code scanning for security issues during deployment. It can help you to identify security problems. You can then modify your software right away to address those vulnerabilities.

Embrace Immutable Infrastructure

Another DevSecOps best practice is to embrace immutable infrastructure. That’s just another way of saying use containers, serverless functions and microservices. These technologies are immutable because you are not supposed to change/patch them on the fly.

If you have to change anything due to problems you identify, you have to start from the beginning. This represents a paradigm shift for automation and the DevSecOps process.

This may seem counterintuitive because containers, microservices and serverless technology are all about flexibility and scalability. But immutability means that you don’t patch a container, for example. If you find a problem with a container in production, you create a new container from scratch. You go back to the source code level, build a new container and then deploy it.

Avoid trying to patch or fix containers on the fly. It is a bad practice that bypasses the needed DevSecOps-related checks and gates. If at any stage you fail, for whatever reason, go back to the first stage and start again. This helps ensure your software is secure and works as required.

DevSecOps is crucial now and will continue to be in the future — and it's required for cloud-driven innovation.

Anupam Sahai
Anupam is Vice President and Cloud CTO. He leads the cloud business and product/tech strategy for the company. He started his career as a software developer and earned a Master of Science degree in Engineering and Management from MIT as well as bachelor's and master's degrees from Indian Institute of Technology, Kanpur and Kharagpur.

He can be reached at
Anupam.Sahai@unisys.com

Focus On People

People are the most important aspect of DevSecOps, which minimizes processes and depends on people to get things right with minimal processes. Now, instead of documenting everything, you let people resolve issues.

Have people who are well trained in all aspects of DevSecOps. Understand that you can have people play multiple roles — in fact, you want that. Every person needs to be savvy in development, security and operations.

Gartner advises organizations to train all developers on the basics of secure coding (but it adds that you should not expect these developers to become security experts — and I agree).

Make sure your people understand and are trained in the end-to-end DevSecOps processes, how to develop code and applications, and how to deploy and debug services in the cloud domain. And be sure that they are trained in security. In the past, you had developers, operations, and security people sitting in three different organizations. Now they're all one.

Find persuasive leaders who can explain the business benefits of DevSecOps. Such individuals greatly increase your odds of DevSecOps success. Automated systems are an important aspect of DevSecOps, so make sure to appoint an automation specialist.

The cloud enables innovation, agility and cost savings. Businesses that don't move to the cloud risk becoming irrelevant. Getting DevSecOps right is important, but it's not easy. By following these DevSecOps best practices, you can use the cloud to your greatest advantage. You'll be more efficient and effective, your customers will be happier and your business will thrive.

DevSecOps is crucial now and will continue to be in the future — and it's required for cloud-driven innovation.

For more information visit
www.unisys.com/closingthecloudgap

For more information visit www.unisys.com