DevSecOps:
The Right Way to Modernize Software Development

The Security Conundrum

In today's highly digitized economy, agility is of the essence. Organizations that cannot provide up-to-date services and continually entice users with new features and new capabilities will quickly find themselves obsolete.

To achieve agility many enterprises have adopted the DevOps model of application development. The focus tends to be on building new capabilities and functionality, with security getting a lower priority. This is not only unwise but can be downright catastrophic, as any number of recent breaches and data thefts has proven.

To truly secure the digital ecosystem, organizations must place security on the same footing as application development by integrating it directly into the DevOps model, enhancing it to become DevSecOps.

The Challenge

Recently, Nimbus Consulting helped guide a key government agency through the transition to a forward-leaning DevSecOps environment. The client needed a solution for an environment that had multiple systems being developed in a shared infrastructure. Over 50 teams were working with a loose collection of more than 30 development tools that were outmoded, not scalable or were no longer being supported by vendors.

Other client challenges:

- Time consuming and chaotic error-prone code deployments delayed feature releases to end users.
- Uneven performance across development teams.
- Issues detected later in the lifecycle, leading to more costly defect resolution and limited ability to implement enhancements.
- Documentation difficult to find and gaps in documentation not easily identified and resolved.
- Development team adoption of DevOps slow as each development team writes their own scripts.
- Silos of inaccessible documentation caused confusion within business and technical teams
- Administrative access to multiple tools was required to understand the current status of developments and deployments.

Finally, there was such a heavy focus on maintaining security that productivity was being severely impeded.

Our Approach

Nimbus took the following actions to unlock the potential of DevSecOps for our client:

- Supplied a hands-on proof-of-concept that identified best-of-the-breed DevSecOps tools that reduced the software delivery time to production.
- Consolidated disparate documentation from multiple siloed systems to a single structured and linked Confluence site, providing greater confidence to the business users on the state of their application.
- Created documentation that promoted standardization so all the teams could record their work in the same manner reducing the state of confusion between teams.
- Created a single Jira project for issues tracking by multiple teams providing greater insights to the agility of the project teams.
- Provided guidance by preparing training materials, documentation, sample scripts, code snippets and tool configuration standards.
- Directly assisted development teams to adopt the new tools and standards and integrate new solutions into existing pipelines.
- Created a reusable open-source ecosystem and produced documentation
- Guided the project teams in achieving low-risk releases by implementing agile methodologies.

We improved the variable system quality of the overall development toolkit by instituting common processes as well as code and security scans to ensure everyone was working with fully secure, high-quality tools. At the same time, we streamlined functions like gap analysis, tool selection and migration support, and then revamped the documentation process around a standard confluence structure to enable a fully auditable documentation environment and to ensure that documentation was up to date.

The Results: IT Empowered – More Secure and More Productive

The result is an agency that is now empowered to improve the flexibility and performance of its software development efforts using streamlined operations monitored through a single pane of glass. But perhaps the most important aspect of this new environment is the way in which it integrates security-as-code early in the process and provides avenues to continually enforce security policies through development and into deployment and operations.

This “shift left” strategy is quickly becoming the norm in commercial operations, and government should keep pace or miss the opportunity to develop more secure software.

This is the crucial goal of agile development and CI/CD environments: ensuring that new features and functions are developed in a steady, straightforward manner, not the chaotic stop-start-revise process of traditional waterfall-style development. From a productivity standpoint, this allows DevOps staff to devote more time to creating advanced capabilities that add value to their projects and less time resolving issues that have occurred in production.

Most importantly, it establishes security as an integral component so that it no longer degrades dev and ops but enhances them to the point at which organizations no longer must sacrifice maximum productivity to keep their IT environments safe.

Value Added

This success is the product of Nimbus’ strict focus on refining a unique set of skills that help clients build value into their development environments and improve outcomes for users. As a member of Gartner’s mentorship program, our goal is to provide complete vendor-agnostic guidance to achieve the best fit of tools and technologies for our clients. We begin by gaining a full understanding of clients’ needs and cultures, working with multiple teams to break down the silos that hamper productivity. As well, we offer full knowledge of all applicable standards and guidelines to quickly devise the right solution on time and on budget.

Our bespoke approach of guiding organizations through the intricacies of digital transformation enables our clients to achieve their goals. Due to the overall shortage of IT talent in the market, it’s important to select a consultant with a proven track record of success in DevSecOps. That partner can then augment your internal staff and help them achieve high productivity and security.

Ultimately, technology alone will not produce a next-generation IT ecosystem. Rather it’s Nimbus’ way of working through which all pieces of the technology puzzle fit together to ensure that progress in development and operations does not come at the expense of security and compliance.