GROWTH ACCELERATION PARTNERS

DevOps Without Security is Like a Door Without a Lock: Getting it Right with DevSecOps

Infrastructure automation has moved from being a nice-to-have to a necessity: 60% of organizations will use infrastructure as code (IaC) tools as part of their DevOps toolchains in 2023, according to Gartner.

This greater speed and efficiency, as well as the easing of complexity as infrastructure sprawls, has a side effect: As developers shift right, and ops moves further up the stack, security needs to shift left.

Just as DevOps combines development and operations, breaking the classic paradigm where developers handed apps off to ops with a wave and a “Good luck!,” DevSecOps integrates security into emerging, agile IT and DevOps as seamlessly and as transparently as possible through a culture of collaboration and shared responsibility. The “Sec” needs to be the transparent part. And with a trusted technology solutions partner such as GAP, combining DevOps and security experts, that transparency is a given.

WeAreGAP.com

WHAT TO CONSIDER

Even though DevSecOps is a relatively new concept, some organizations are further down the road than others — even if they might not know it yet.

One current GAP project — for a privately held e-commerce company specializing in luxury mattresses — is a good example. Some teams within the client's organization have more mature processes than others. In these types of cases, security staff are beginning to be integrated among the already-established DevOps team, with CI/CD (continuous integration and delivery) pipelines, secure coding techniques and associated tools in place. The key, from an advisory services standpoint, is to create a smooth process across all teams.

So what are the key techniques, best practices and tools should you look at if you are looking to incorporate DevSecOps? Some of the general best practices align with that of IaC security, such as the principle of least privilege and encyrpting data both in transit and at rest. Other basics include input validation, sanitizing the data, and using trusted security certificates.

One thing to consider is regarding how applications are created. As Gartner puts it in its checklist for successful DevSecOps, modern software is more assembled than developed, through pre-built components, libraries and frameworks. Many if not most projects also rely increasingly heavily on open source tools, with various community contributors. Scanning component libraries for known vulnerabilities and configuration issues can be a major boon.

GROWTH ACCELERATION PARTNERS

BEST PRACTICES AND SPECIFIC TOOLING

Another part of solution partners' DevSecOps expertise is not only in future-proofing applications with security best practices, but also retrofitting them if security was not previously part of the regular build process. There are two ways to do this: either (1) apply common best practices around encryption, password hygiene and understanding the application's most sensitive information, or (2) follow a specific framework, such as PCI compliance for websites.

In terms of specific tooling, static application security testing (SAST) and dynamic application security testing (DAST) tools are important to alert teams of a breach or misconfiguration before the application is released into production. The former are tools to test and scan application code at rest, while the latter can dynamically check both an application's internal state and external environment.

Navigating the plethora of available tools can be daunting. For the infrastructure layer, you have SIEM (security information and event management) offerings, which enable security and risk management professionals to aggregate and analyze volumes of application data in real-time. Cloud infrastructure providers will have their own identity and access management (IAM) toolsets, particularly with regard to role-based access control (RBAC). A common scenario could see production access limited to a severely isolated or restricted account. Jack the Janitor doesn't need the password for the AWS admin console.

For the development workflow, tooling can be implemented to ensure code is going to be built and deployed in a very specific way. Tools from this kit range from SonarQube and Checkmarx for continuous inspection of code quality, to tools that facilitate CI/CD, such as Jenkins, GitLab and CircleCI. If certain standards are placed on the development workflow, then deviations from that workflow can be spotted and used to understand anomalies.

EXPERTISE MATTERS

Things move fast it, and it can be hard to stay current. Is it best to learn it all on your own, or bring in some help? Frankly, production apps are no place for a learner's permit. The collective experience of different projects, tools and technologies is much more valuable here than with other disciplines. As DevSecOps is more of a culture, there is no one-size-fits-all approach. And expertise only comes with practice and experience.

If you have to research a tool while implementing it, take it from those who know: it will not be good enough for a production environment. To go full circle on infrastructure as code, let's use Terraform as an example. It is no good deploying one standalone module for Amazon RDS (Relational Database Service), another for EC2, and so on. The whole point of IaC is the convenience of a complete infrastructure that can be replicated among multiple environments. It should be possible to use the same configurations for managing production and non-production environments.

DEVSECOPS IS ALL ABOUT MAKING SECURITY TRANSPARENT — BUT DON'T MISTAKE THAT FOR SIMPLICITY.

If you have a big complex infrastructure, then it is better to have it in a single set of code, instead of being spread among multiple repositories. This, however, requires more advanced knowledge. If you haven't worked with Terraform much, it is understandable to adopt a simpler approach. But that simplicity can go against security and standardization.

Don't be tempted to make such a trade-off. A trusted solutions partner like GAP can build a strategic cloud architecture plan that can maintain workflows and reduce development time, while improving application and data security. As you embrace DevSecOps, make sure you get it right.

To find out more, please visit WeAreGAP.com

company/growth-acceleration-partners/ @GrowthAccelerationPartners @GAPapps