Executive Viewpoint

A conversation with **David Cantrell**

Chief Information Security Officer, Business and Enterprise System Product Innovation (BESPIN) Software Factory, Air Force

What challenges do teams face when building mobile apps in the government?

As an Air Force software factory, we work with many innovation teams that struggle to bring mobile apps forward. These teams answer the call from leadership to build innovative mobile apps that solve critical mission needs, but then they encounter a maze of security hurdles to get those apps into the hands of their users, halting the very innovation that senior leaders are promoting.

Do team members know how to select and use the correct tools in the correct way to make risk decisions? Do they know which approval pathway to follow to deploy their app? Once an app is approved, do they know which delivery pathway to use to get the app to their users? The answers depend on whether your app is iOS, Android or web and whether it is deploying to a government or personal device, etc.

In addition, the experts needed to navigate these processes are typically locked inside the traditional program management offices (PMOs) because their security teams know the process to achieve an authorization to operate (ATO) for their legacy systems. But even they often struggle with cloud and mobile.

Our continuous ATO reduces a lot of the complexity for development teams by moving that expertise out of the PMO and into an easily consumable shared service along with an automated hardening and delivery pipeline. We've solved many security problems for developers so they can deliver features faster.

My team is proud that we've been able to adapt complex security regulations to meet developer needs while satisfying the Defense Department's risk management expectations.

How can agencies incorporate continuous security testing into their DevSecOps environments?

DevSecOps is all about moving security analysis closer to the point when code is written instead of reviewing it at the end. This means selecting tools that can secure every step in the process, from scanning code to monitoring apps in production use.

It also involves building fully automated continuous integration/continuous delivery pipelines. You want to automate as much as possible. Any step that involves a "human in the loop" slows down feature delivery. Tools aren't perfect so you still need human review for risk, but you can use the tools to dramatically reduce manual friction, which in turn speeds delivery.

We maximize automation at BESPIN — including hardening, building, signing and delivery for both mobile and web apps — through our fully accredited pipeline hosted in the Air Force Cloud One environment.

What features should agencies look for in a security testing solution?

You should start by identifying which aspect of the software or device you want to evaluate. For example, do you want to scan source code, look at your software supply chain or evaluate runtime behavior? Then you want to look for mature tools that have a strong reputation for that type of analysis.

You also want to look for providers who have strong teams of mobile security professionals. Tools are only as good as the people who use them. You want providers who have deep expertise in the mobile security realm because they are more likely to be passionate about working with you to identify and solve your problems together.

At BESPIN, we've built strong public/private partnerships for research and development of innovative new mobile and cloud security testing capabilities. This enables us to shape the design and development of tools to benefit the government. These partnerships in turn drive massive value for our customers, who need to quickly deliver secure mobile and cloud apps. ■