Q&A

Executive Viewpoint

A conversation with **Hannah Hunt**

Chief Product and Innovation Officer, Army Software Factory, Army Futures Command

This interview continues at carah.io/

What is the mission of the Army Software Factory, and how does it reflect the changing nature of the battlefield?

The Army Software Factory's mission is to upskill soldiers so they can build and deliver software capabilities across the force. In the future battlefield, in 2030 and beyond, we're not going to have the opportunity for contractors and civilians to move across the battlefield like they did in conflicts in Iraq and Afghanistan, for example. So it's critical, from a strategic-imperative perspective, to have that organic skill set within the force itself so that we can develop software at the edges of the battlefield.

What's been really exciting is that we've been able to take a lot of talent that currently exists within the Army and invest resources and time in upskilling those soldiers in modern software development practices so they can build and deliver capabilities that provide value to soldiers just like them.

How does the Army use DevSecOps to continuously deliver secure software in a sustainable way?

I oversee all the application product teams that our soldiers work on. Identifying the problems we're going to tackle is part of my role as well. None of the software we're developing works unless we have the ability to rapidly iterate with our user base. What's important about DevSecOps in the context of a continuous risk management framework or a continuous authority to operate is that we are setting a standard for what security measures need to be in place. As long as an application team meets those security guardrails and thresholds, it can continuously push to production.

It's a real game changer because we are setting a relatively high bar for the level of security prowess an application team needs to have before it can go to production for the first time and for subsequent pushes. It allows for a continuous delivery of software capabilities. Right now, our teams are pushing out new features on a weekly basis, which is incredibly fast in comparison to other organizations within the Defense Department. That's because we utilize this continuous risk management framework approach and DevSecOps methodologies where we're shifting security skills left, having application teams really care about security and providing a platform in conjunction with the Army CIO that allows for rapid iteration.

What advice would you offer other agencies as they adopt or evolve their use of DevSecOps?

My main recommendation is to start small and iterate. Rather than trying to boil the ocean and build a big system all at once, think about a particular output or outcome you want to achieve and then think about how you can rapidly iterate by utilizing DevSecOps methodologies and technologies such as continuous integration/continuous delivery pipelines, container orchestration or an inheritance model you can leverage with existing infrastructures or platform layers.

My other advice is to celebrate the small wins. It's really hard to hack through bureaucracy. But there are small wins you can achieve each and every day, and they build up to being large, game-changing wins. Being comfortable with those small wins keeps your morale up and keeps your teams going. It also allows you to capitalize on each win exponentially until you have a larger transformation effort. ■