

EXECUTIVE BRIEFING SERIES Securing software through its entire lifecycle



Securing software through its entire lifecycle

BY JASON MILLER

Agencies have spent much of the last five years extricating themselves from waterfall software development and walking – or in some cases running – to the development, security and operations (DevSecOps) approach.

The reasons for this transition have always been clear: to improve their competitiveness, to move quickly and to address digital sprawl that has resulted in mounds of technical debt.

A panel of federal and industry experts recently offered insights into how DevSecOps and the use of open source software can help agencies produce secure, agile and modernized applications.

Angel Phaneuf, chief information security officer at the Army Software Factory, said creating a successful software development process involves several different pieces that must come together as one.

"The first factor is to ensure that we don't already have a tool that fits your need or use case because digital sprawl is a problem and it can get out of control really quick," Phaneuf said during a **Federal News Network** panel discussion. "Another factor is understanding the licensing model and the ability to scale. Even though some software is only requested by a single team or a single person, we have to make sure that we take into account the possibility

PANEL OF EXPERTS



Manuel Gauto Chief Engineer, Black Pearl, Navy



Angel Phaneuf Chief Information Security Officer, Army Software Factory



Landon Van Dyke Senior Technology Advisor, State Department



Stephen Magill Vice President of Product Innovation, Sonatype

that the entire organization is going to adopt this. We've gone through several cycles of determining what is the right way to do it as someone comes in and uses a new tool."

A third important factor, she said, is documentation. This includes everything from feedback from developers, engineers and security experts to ratings systems to ensure products meet the controls and rigors the Army demands.

Looking for novel capabilities

The Navy's Black Pearl effort, which is more of a DevSecOps tools and assistance provider than a software factory, is less prescriptive about how software is developed and implemented, said Manuel Gauto, chief engineer of Black Pearl. Security, user experience and overall integration are the leading factors that make up the program's successful software process, he said.

"What we're trying to do with Black Pearl is connect not just the high-performing entities within the traditional defense industrial base but also bring in folks that have novel capability on the commercial side that we can just buy as a self-encapsulated capability – and then build a simpler interface to the rest of the ecosystem that we're trying to build," Gauto said. "At the end of the day, the Department of Navy is not in the business of building source code scanners or artifact scanners. We build capabilities that are warfighting capabilities that go on a submarine or warship, so we're constantly trying to allocate our resources as intelligently as possible."

This means the Army, Navy and even State Department make use of open source code to help accelerate certain capabilities.

Landon Van Dyke, senior technology advisor for the State Department, said there are specific security and oversight tools needed to make sure open source software is as safe as possible.

"At the enterprise level, when we're looking at evaluating a company or a product, we're actually evaluating the company themselves. We do start with the procurement process. We look to see what their financial health looks like, what they're doing "We've developed a tech accelerator that brings soldiers from all professions in the Army up to speed on coding and security skills that they need to help implement secure software."

- Angel Phaneuf of the Army Software Factory

in the market, who their partners are. Obviously if it's overseas that matters especially for the State Department," Van Dyke said. "One of the things that we're really looking at for software is the source code. We're looking at things like injection, authentication and session management. That does require a little bit of sophistication in the evaluation by artificial intelligence tools."

Attacks becoming more challenging

Stephen Magill, vice president of product innovation at Sonatype, said as agencies move more toward a DevSecOps model, they need to be aware of two kinds of vulnerabilities: mistakes made in code development and intentional vulnerabilities like zero day attacks such as Log4j.

"Having a good inventory is important because knowing what you're using can be remarkably difficult. And when you're operating at the level of scale that the government does and that larger companies do, then for the new style of attacks, things like malicious codes, that's the most challenging. But it's also where the innovation is happening in the industry right now," Magill said. "There are products out there. We have a product called Nexus Firewall, which sits at the boundary of your network and will quarantine things that you pull in if we've detected malicious commits. Basically, it's a different type of monitoring." Agencies need to rely on vulnerability reports and constantly assess the trustworthiness of their development teams, processes and contributors, he added.

Build vs. buy considerations

For many of the panelists, the build versus buy decision is top of mind.

The Navy's Gauto said every agency, whether defense or civilian, is feeling the pinch of not having enough software engineers, which makes the decision more straightforward.

"We keep our core offering really trimmed down. We have a very specific set of tools, and what we do for folks is really locked in on a specific tool, like a specific code scanner or something. We have a whole architecture for bolting on tools as an additional set of functionality to our core offering, and we can kind of work with the people that really want that to make sure that stays maintained, make sure it stays funded," he said.

"Then, in terms of that core tooling, we're really user experience-centric, and we're really demand-driven. The only times we really challenge our common offering is when we have a large group of people saying

"There are products out there. We have a product called Nexus Firewall, which sits at the boundary of your network and will quarantine things that you pull in if we've detected malicious commits. Basically, it's a different type of monitoring."

- Stephen Magill of Sonatype

the same thing," he continued. "We've developed a process of looking for need and demand evaluation of the specific tool that's being requested, and then there's an integration phase. That's how we graduate products into that common environment."

Ensuring a tool integrates into the Navy's current set of capabilities and the tool's delivery and development pipeline are paramount, Gauto said.

The Army's Phaneuf said many times the decision of build versus buy comes to down to how fast the service needs the software and whether it's for a few or many users.

Finding development and security expertise requires each organization to make trade-offs, and that's why open source can address the speed-to-market challenge, Sonatype's Magill said.

If agencies use continuous monitoring tools and other security capabilities to monitor dependencies, they can stay on top of threats and innovations, he said.

"Each organization has to make that trade-off for themselves and decide where the line is in terms of what makes it worth it to pull in an open source component versus do something else," Magill said. "It's important to really think, when you are adding some new dependency or leveraging some new piece of open source, what is the value that's bringing you? And then what is the maintenance burden that you're setting yourself up for because if you're pulling in a giant dependency and you're using one function, is that really worth it?"

The costs include maintenance, integrating the tool into existing code and addressing any security vulnerabilities, he said. "It's really hard to remove something once it's in the code base, so you're really signing up for a long-term maintenance project."

The move to DevSecOps is more about changing the culture than anything else – security permeating the entire development process, State's Van Dyke said. Plus, agencies must always evaluate building versus buying and software development as part of overall infrastructure modernization efforts.

Previously at State, a lot of these activities were done in siloes so bringing those individual organizations together is a matter of people, process and technology, he said.

Changing the culture

Gauto works with a lot of engineers who just want to build everything.

"They have a hammer, so to them, everything looks like a nail. They're like, 'Oh, why would we pay for that. I can build that over a weekend,' " he said. "But what we have been pushing for, and that kind of pushes the scale and weights it a little more effectively for us, is that we push for a certain level of quality for internal tooling. Like, if we're building something, it needs to almost be a product in its own right. It needs documentation. It needs to pass the robust tests that we do on any piece of open source software, any piece of commercial software. That usually makes it easier for the individual engineering leaders within the organization to properly evaluate that build versus buy decision."

Commoditizing the software development process as much as possible through software factories, as one example, lets sailors and civilians focus more on mission and less on development, Gauto added.

The Army Software Factory's focus has been on building skill sets around DevSecOps so soldiers and civilians can go back to their mission areas and drive technology change focused on the future force design. "We've developed a tech accelerator that brings soldiers from all professions in the Army up to speed on coding and security skills that they need to help implement secure software that will drive mission impact," Phaneuf said.

That factors into the build versus buy question, she said. "When I think of that, I think, 'Do I want to build something that's going to provide a capability that I can buy?' I need to be able to buy something that has to be able to meet certain standards so that when I put these future soldiers in a war zone — where I'm deploying a developer, a platform engineer, user experience designer and a project manager — soldiers are going out into the battlefield and can build you any application, at any time. ... That comes into play "At the end of the day, the Department of Navy is not in the business of building source code scanners or artifact scanners. We build capabilities that are warfighting capabilities that go on a submarine or warship."

- Manuel Gauto of the Navy's Black Pearl

when we think, 'Do we build a software product that is already out in the commercial space, or do we just consume that product?' "

The speed of DevSecOps pushes agencies to ensure all of these questions and concepts are addressed during the development cycle.

Sonatype's Magill said this includes ensuring security capabilities factor in too – such as scanning for vulnerabilities and relying on private sector software bills of materials (SBOMs).

"There's the vulnerability database, which will help you know which of those components are vulnerable in which versions and so forth. So when you're thinking about a disconnected environment, you basically need a full copy of that vulnerability database and a process to keep it up to date and have consistency across your development and your deployment and release environments," he said. "That's definitely something I think about when evaluating products and something where there has been some innovation in the industry."