ATARC

Powered by GovExec

ATARC DevSecOps Working Group Kickoff Roundtable

Highlights from a recent roundtable, hosted by the Advanced Technology Academic Research Center (ATARC) DeSecOps Working Group, September 2024

The Advanced Technology Academic Research Center (ATARC) recently held the inaugural meeting of its DevSecOps working group. Working group participants from a variety of government agencies and private sector companies discussed the challenges, opportunities, and strategies of DevSecOps in government.

Culture and Leadership

> **“DevSecOps is all about continuous delivery of capability with confidence.”**

Several participants underscored the importance of culture and leadership in fostering a successful DevSecOps environment. Developing a culture where taking a “fail fast”, iterative approach is the norm is essential for agile, continuous delivery, but also challenging to achieve in a risk adverse setting such as government or regulated industries.

Participants noted that there is resistance to change among the workforce, which prevents the collaborative approach inherent to DevSecOps. One participant has found success by calling the concept by a different name and showcasing the benefits of DevSecOps principles. They’ve found that ‘devops’ is a loaded term not well understood by everyone.

Integrated Security

Participants discussed the need to integrate security throughout the entire software development lifecycle, ideally starting from the design phase. Giving immediate feedback on any security issues to the developer is key to remediating security challenges as early as possible.

Participants noted there are tools to help with automating security throughout the entire development process, particularly with checking code for vulnerabilities. While it’s critical to push security even farther left into the design phase, panelists note that doing so can slow the process down, which is counter to the agile process.

> **“There's always that sort of culture shift of getting things out good and fast, and getting them out safe and secure.”**

SBOMs and Open Source

Ultimately, agencies must have visibility into where vulnerabilities exist in the process to identify which products could be affected. Working group participants discussed challenges surrounding maintaining the accuracy of SBOMs in multi-layered, open source environments.

Participants note that there are tools available that build SBOMs by scanning code directly, but there are additional challenges associated with continuously monitoring code and updating SBOMs as new vulnerabilities are introduced.

Legacy System Integration

Participants also discussed various challenges associated with integrating a DevSecOps approach with legacy systems. Agencies often run up against compatibility issues, security vulnerabilities and performance bottlenecks that prevent continuous system integration.

One participant noted that despite knowing systems needed to be replaced, the agency could not match the speed of production. Another participant took an incremental modernization approach, whereby one tier of legacy applications were moved to the cloud and containerized to improve portability and security at a time. Another challenge raised is a resistance to change among legacy application owners.

Continuous Improvement

> **“If you're practicing actual, continuous integration on a daily basis with your builds, then you’ll have the confidence to deliver what’s needed at the speed of relevance.”**

Participants also noted the continuous nature of DevSecOps and the need for ongoing improvement and adaptation. One working group member called out the myth that agile is too fast and loose, and does not allow for proper planning. On the contrary, agencies have proven that an agile DevSecOps process involves planning and retrospectives at each sprint, allowing agencies to course correct as issues arise.

Discussion naturally shifted to the use of AI to bring efficiencies to the entire software development cycle. There are already innumerable ways AI is being used to support development and security. Panelists caution that the use of AI being used by developers is exactly why DevSecOps pipelines must consider cybersecurity as far left as possible. Relying on SBOMs to identify vulnerabilities will be too late.

There are a number of AI use cases agencies can explore, from using AI to create better quality code to inspecting code for AI generated fantasies that make their way into modules. Some participants shared concerns with using public AI models, while others have prohibited all generative AI use in their agency due to challenges with information leakage.

Collaboration and Clear Communication

> **“Trust among the teams themselves, and between the teams and the executives is absolutely foundational to being successful in this business. You cannot go fast if your IT landscape is built on a culture of mistrust.”**

Ultimately, the success of DevSecOps hinges on clear communication, collaboration, and a shared understanding among teams. Participants note that when teams must ask permission multiple times to accomplish work, or address a change board in the middle of deployment, DevSecOps fails. Panelists caution that creating teams can also create silos, but to prevent this, teams should communicate clearly and develop a culture of mutual support.

LEARN MORE ABOUT OUR WORKING GROUPS AT:

HTTPS://ATARC.ORG/WORKING-GROUPS/