Quokka

GUIDE

DevSecOps Adoption for Federal Agencies

Quokka

Guide

DevSecOps Adoption for Federal Agencies

Cybersecurity remains a key topic for the Federal Government, especially in light of the recent publication of Binding Operational Directive 23-01. As outlined on CISA's website, "the purpose of this Binding Operational Directive is to make measurable progress toward enhancing visibility into agency assets and associated vulnerabilities. The requirements of this Directive focus on two core activities essential to improving operational visibility for a successful cybersecurity program: asset discovery and vulnerability enumeration." As more and more federal agencies use apps for internal personnel and engaging with the broader public, each mobile app must meet specific security criteria to ensure data protection and privacy.

The Role of DevSecOps for Federal Agencies

DevSecOps is an operational model that integrates security testing and validation throughout the development lifecycle of an application—from design to development to deployment. Within a DevSecOps model, security experts work in tandem with development and operations teams using automated testing tools to infuse a security infrastructure into the application before it is released to the end users.

According to the National Institute of Standards and Technology (NIST), agencies who adopt a DevSecOps model can:

- Reduce exploitable vulnerabilities, such as malicious or incorrect code and other vulnerabilities quickly without inhibiting software release schedules
- Mitigate the impact of cyber criminals exploiting application vulnerabilities
- Address root causes of vulnerabilities and highlight areas of investment or retraining if needed

For federal agencies, this can mean building more secure applications that are used daily for internal employees and also securely accommodating employees who may be deployed or working remotely. If an application has passed each security test and is approved for launch, in addition to other security measures, access and use of the application should not be limited by location.

Challenges to DevSecOps Deployment and Standardization

With President Biden's Executive Order pushing for an improved National Security posture and standardizing the DevSecOps processes, there is a deep commitment to modernizing how the federal government approaches cybersecurity and using today's tools to make this goal a reality. However, like with most government policies and procedures, agencies will face some inherent challenges during this technology adoption period.

- One challenge will be working with IT leaders and agency personnel who may shy away from new technologies in favor of ones they are more comfortable using. It can be difficult to convince these people that modernizing the development process will increase security and timeliness and may hinder forward momentum.
- A second challenge will be training and building teams with enough skill and agile working knowledge to shift from a traditional DevOps operational model to the new standard DevSecOps workflow.
- The third challenge agencies will face is building modern workflows on legacy systems and tech stacks. Many government agencies cannot access the same modern tech stacks used by commercial companies that combine all the work into a collaborative and visible space.

Three Key Ways to Navigate the Balance Between Innovation and Security

Communication Fuels Collaboration

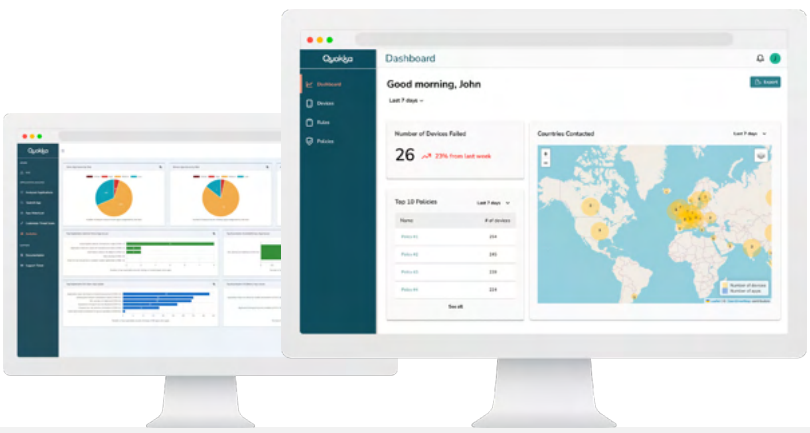
Software development is a living, agile process with constant communication across all mediums—email, message boards, video conferencing, and project management boards. As your team adopts a DevSecOps model, all communications and updates must be housed in a repository that can be easily accessed and managed.

Increase Automation Where It Makes Sense

Security and automation require a delicate balance. As you move forward to a DevSecOps model, analyze how automated workflows in your current DevOps toolchain can integrate security testing. Teams can work together to build on these automated workflows through the development process and determine where more or expanded automation can streamline the process. During this time, it is essential to address any nervousness or anxiety that automation is the equivalent of cost or headcount reduction. Addressing these concerns will also go a long way to building acceptance and adoption of this new operations model.

Prevent Developer Overload

Transitioning to a new operations model can also come with an increased workload for the development team. With many of today's application security testing tools built for security teams, it can require a significant amount of hours on behalf of the development team to deliver findings and remediation plans. Leaders should invest in tools that support the team efforts and include consistent training and workflows that alleviate the potential for overworked and overloaded development teams.



How Quokka Can Help

Quokka's Mobile Application Security Testing platform, Q-MAST, was built with the understanding that application security shouldn't be compromised at any point within the development lifecycle. As the industry leader in mobile app security testing, Q-MAST uses a unique combination of advanced analysis engines that digs deeper and tests more thoroughly than any other MAST solution in the market.

Built for Developers

Designed to integrate directly into the CI/CD pipelines, Q-MAST provides in-depth analysis and reporting for both Android and iOS application software in one unified platform.

Q-MAST is a fully-automated Mobile Application Security Testing platform, detecting security, privacy, and code quality issues on iOS and Android apps without needing to access any source code. Vetted by the NSA, we support the highest compliance standards, including NIAP, CCPA, GDPR, NIST, and OWASP MASVS.

References:
National Institute for Standards and Technology - Cybersecurity Framework
Binding Operational Directive 23-01
Executive Order to Improve National Cybersecurity