Automation: The key to **secure app development**

Agencies can deliver continuous ATOs by adopting real-time compliance for software supply chains

Prakash Sethuraman

CloudBees

Over the years, agencies have improved the way they build and secure IT networks and infrastructure. However, the natural progression of any threat landscape is to gravitate toward weaker areas. That is why recent government mandates have begun to focus on strengthening software and supply chain security.

It is difficult to ensure consistently high expertise and adoption of best practices across the diverse teams involved in application design, development and operation. It is also difficult to balance the desire for creativity within software development teams and the need to adhere to the stringent rules required to ensure security.

In addition, the adoption of microservices-based architectures delivers smaller units of functionality that are more comprehensible, but those moving parts interact in many different ways, making it challenging to understand the interdependencies and risks of a complex landscape.

Overcoming the challenge of 'going fast but staying safe'

Application software is front and center in the drive to provide high-quality services to citizens and organizational customers. That, in turn, is fueling the need for a different culture, method and tooling capability within agencies.

Those realities are accelerating the adoption of DevOps, which helps organizations be agile in determining what to deliver, how to deliver it and then delivering it. The primary strategic benefit is a significant increase in change/transformation velocity. However, that velocity amplifies the opportunity for human errors that result in security vulnerabilities.

In addition, today's software developers typically write only 10% to 30% of the code an application needs. For the rest, they reuse products that other people or organizations have created. The software supply chain for even simple applications is extremely complex with many opportunities for malicious or unintentional vulnerabilities.

These are not trivial concerns for federal agencies, which provide services that affect millions of people.

Adoption of DevSecOps and "shifting security left" is often prescribed as the answer to these concerns. However, adding software security and compliance to the developers' workload is not sustainable. The only way to address that complexity is through automation, which enables developers to focus on what they do best — building feature sets that customers want.

Toward continuous ATOs

In the world of microservices, public cloud-native applications and high-frequency releases, authorizations to operate (ATOs) that periodically assess the suitability of a process are no longer valid. A vulnerability introduced through a deviation to an approved process or inadequate human oversight could lead to a breach well before the next assessment.

Zak S.

> In the world of microservices, **public cloud-native applications and high-frequency releases,** ATOs that periodically assess the suitability of a process are no longer valid."

To address today's cybersecurity challenges, ATO users must be able to answer three key questions all the time:

- Can we quickly assess whether we are conforming to the rules we are expected to follow?
- Can we attest that we are conforming to those rules across the life cycle of an application, which can often span decades?
- Can we supply evidence that demonstrates that our attestation is valid?

An ATO is no longer fit for purpose if those questions are only answered every six months or annually. Instead, ATOs must become continuous ATOs, and evidence of compliance must happen in real time. Deployments of software to production should be automatically prevented if the required criteria are not met.

When security and compliance are transparent and continuous, the DevSecOps ecosystem creates a safety net that operates in real time to prevent security missteps and ultimately helps boost the productivity and creativity of development teams.

For more information on how CloudBees helps the federal government achieve continuous ATOs, visit our site. ■

Prakash Sethuraman is chief information security officer at CloudBees.