Ending the Conflict Between Mobile Dev and Sec

By Eric Newcomer, CTO and Principal Analyst, Intellyx
© Intellyx

Introduction

Pressures to release a mobile application can easily conflict with the need to implement security protections. The development process for mobile applications is continuous, automated, and rapid. Too often, release candidates for mobile applications are very close to the scheduled release date when security issues are discovered.

Conflicts emerge between mobile development and cybersecurity team each time the standard DevSecOps process generates findings. One way to resolve the conflict between security protection and time to market is for management to sign off on a risk exception, which allows the release to go forward without protection. Instead, mobile development makes a commitment to resolve the security issue in a subsequent release. But this usually results in a window of opportunity for cybercriminals to execute an attack, resulting in an incident, or a breach.

Innovative technology, such as the defense automation tooling Appdome provides, offers a better way to resolve these conflicts, avoid risk exceptions, and implement protections in a timely manner.

The imperative of mobile applications

Studies show that people today spend 90% of their digital time using mobile apps. 85% of consumers surveyed favor using mobile apps over websites for interacting with businesses, buying and completing transactions with their favorite brands.

Last year, more than half of all online business was conducted using mobile apps. And this figure is growing annually at 14%. Nearly half of small businesses have their own app as of 2022. That's up from 32% in 2021.

The business case for developing a mobile app hardly needs an ROI.

The resulting pressures on mobile app development and security teams are tremendous. They have to release a high quality, secure mobile apps quickly. They also have to continuously update the mobile app to improve it and keep up with the competition.

Unfortunately, these pressures intensify the conflicts between the mobile development and cybersecurity teams. Development wants to ship code and ship it fast; Cybersecurity teams want to protect the code and the business first.

©2023 Intellyx LLC. www.intellyx.com

The Customer's View

Customers evaluate mobile apps for usability, functionality, and security. Said simply, the mobile app must work, include the functionality of all other apps in its category, and protect the user whenever it's used.

Switching costs for mobile consumers are near zero. If an app lacks useful features, becomes difficult to use, returns results too slowly, or is suspected to be a security risk, consumers will quickly switch to a competitor's app.

If two applications offer the same "photo deposit," "transaction history" or security feature, for example, consumers will judge the quality of the business by the quality of the implementation of that feature in the mobile application.

Stopping fraud, IP and data loss, program abuse, credential stuffing attacks, loss of revenues, negative brand reputation, or churn (loss of customers) are equal to other features in a mobile app and become even higher priorities when competitive mobile apps offer similar or better feature protections to the consumer.

In the push to enter and compete in the m-commerce marketplace and make a compelling case that consumers should choose and use an organization's mobile app, the business case for security is starting to emerge as a necessary part of acquiring and keeping customers.

Sparks of Conflict Arising in the Pipeline

Mobile development processes are typically called "pipelines" because they consist of a series of connected automation systems that perform key tasks in the build, test, release and monitor process. An average mobile DevOps pipeline releases 48x per year on each of Android and iOS.

In the center of this, cybersecurity performs its review or set of tests, albeit all too often late in the release process. When the cybersecurity team reports that critical protections are missing, the lack of which could put customer data, transactions, or account control at risk and open the door for fraud, and the next releases are often already stacking up. What to do?

The development team and the organization's management are keenly aware that each day the app is not in production, it can cost the company hundreds of thousands, if not millions, in lost revenues and untold loss of business to competitors.

©2023 Intellyx LLC. www.intellyx.com

The development team and the cyber teams try to figure out how to resolve the deficiencies in the time left before the release. Heated conflict can break out between the mobile dev and cybersecurity teams over the release date and required protections.

This sort of situation is all too common, unfortunately. The focus of development teams is on delivering new features on a predictable schedule while maintaining a standard of quality and performance with each release. They are all about meeting (or beating) each of the successive deadlines for production releases consistently – keeping the pipeline moving at all costs.

The security team has the role of auditor and approver of dev's work, based on company security policy. Security and dev teams are typically in different parts of an organization and their activities are not always well coordinated.

This separation of role and teams is necessary to ensure the right checks and balances are in place but frequently lead to conflicts because dev wants to ship as soon and as often as possible while security will want to delay the release to protect the business.

This conflict typically results in a "risk exception" process, which essentially kicks the can down the road – and the organization agrees to fix issues in a subsequent release.

Management is required to formally sign off on waivers to accept the business risk that comes from putting a mobile app into production that isn't fully protected or compliant with the company's security policy. While this practice is a common way to resolve the conflict between dev and security, it usually results in the release of an application that isn't, or isn't fully, protected against known exploitable vulnerabilities.

Security Team View

A normal review process involves a security expert evaluating an app against the company security policy. The policy is typically driven by factors such as whether the app is externally facing and handles sensitive data. It can also be driven by regulations, such as the SEC regulations on disclosures for cyber incidents for all public companies and other regulations.

Typically, it's a security architect or a TISO, or both, who will review the app against a checklist of items identified as conforming to company security policy. These items

usually include checking for network perimeter defense controls but will also include checking for internal defense controls on the assumption that a certain percentage of cyber criminals will penetrate the perimeter defenses. In mobile specifically, this will also usually involve a DAST/SAST scan, a mobile application penetration test and API Security checks using the APIs dedicated or used by the mobile app.

In addition to these basic checks, there are many other forms of cybercrime to prevent, such as brute force or phishing attempts at stealing login credentials, malware, synthetic fraud, app takeover for ransom or stealing data, fraud, spoofing, and so on. These all must be checked for a major commercial mobile application - especially one that handles customer and financial data (in other words, most mobile apps).

Such reviews can take a long time, and adverse findings can be costly and time consuming to implement.

Preventing incidents and breaches is the security team's mandate. However, when the review process slows down an app release, this mandate runs into conflict with dev team goals to release the app as soon as possible.

Any mobile app released to production becomes an immediate target, and cybercrime is costly. The average cost to a small business of a cyber breach is about $3M – much more for a large business.

Why Traditional DevSecOps Isn't the Answer

In a traditional DevSecOps process, the goal is to include automated security tests in the development and deployment pipeline. The intention is to streamline the security review process by using the pipeline.

While this does speed up the discovery of exploitable vulnerabilities and addresses the "shift left" mandate for most cybersecurity teams, mobile development and cybersecurity teams still engage in heated debate about what protections the development team can deliver, as well as what waivers and exceptions to security policies can be put in place to ship the app faster.

Development teams often don't have the resources, skills, or knowledge to resolve pipeline findings and may assign a low priority to security, since functionality, look and feel, ease of use are the top drivers for them.

©2023 Intellyx LLC. www.intellyx.com

Developers also may not be aware of company security policy in detail, or familiar with some of the more unusual types of cyber threats. They may also overestimate the level of security protections and validation provided by app stores, or device manufacturers.

In the traditional DevSecOps model, the cybersecurity team's job is limited to "review," "report," and "recommend" to the development team which security features need to be implemented.

The cybersecurity team is then entirely reliant on the development team to make the needed changes, updates, or upgrades to the mobile application defenses.

Likewise, any evidence of fraud, account loss, etc. as well as the effectiveness of any protections are often outside of the purview of the cybersecurity team.

Even if the penetration testing, DAST/SAST scans, and other tests, are incorporated into the CI/CD pipeline, the cybersecurity team does not control the means of delivery for the protections.

Each review, whenever or however performed, leads to tasks and tickets that the development team controls. In some cases, cybersecurity teams have resorted to providing pre-packaged SDK-based security libraries, only to be told these don't match the way the development team wants or needs to build the app.

The delivery and the feedback loop for all security features reside outside of the security team. DevSecOps doesn't change this. The process is elsewhere in the organization, not in the team responsible for protecting the business, its brand, and its users.

Defense Automation to the Rescue

The premise of mobile application defense automation is to use the CI/CD pipeline to shift the burden and responsibility for delivering the needed protections in mobile applications from the development team to the cybersecurity team.

In other words, mobile app defense automation allows the cybersecurity team to build, test, release and monitor the protection model in the mobile applications on its own, as and equal and independent part of the SDLC for mobile applications.

Then the pipeline runs as before to automate the mobile app development process – and inside that the security, anti-fraud and other protections are built into the

©2023 Intellyx LLC. www.intellyx.com

mobile app – clearing the backlog of security findings and speeding the release of new protections that come from new tests and reviews. Adding defense automation to the pipeline automates the delivery of protections required by the organization's security policy and certifies that they are in place before the app ships.

Defense automation allows the cybersecurity team to take direct action in the CI/CD pipeline to address tickets and tasks previously assigned to the development team, risk exceptions put off to later releases, new findings from penetration tests or DAST/SAST scans, changes in the security policy, or findings from an actual attack, without putting any added work, burden, or pressure on the development team. It's a groundbreaking concept and technology that changes the game for DevSecOps.

With defense automation, the major source of friction in the traditional DevSecOps process goes away. Security teams take up a new position in the CI/CD pipeline. No longer limited to the outsider role of "reviewing," "reporting," and "recommending" security protections in mobile applications, or "negotiating" waivers and signoffs, cybersecurity teams become integral to the release process and aligned with development and operations in the DevSecOps workflow because the system used to build, test, release and monitor mobile application defenses are the "same as" and "connected" to the CI/CD pipeline used to build, test, release and monitor the mobile application.

The ultimate goal of defense automation is for collaboration to replace conflict, for data to replace debate, and the development team to be left to do what it does best – build, test, release and monitor great mobile apps.

Ultimately, mobile application defense automation improves the overall security posture of mobile applications by eliminating (or dramatically reducing) the need for waivers and signoffs in the traditional DevSecOps process, and speeds time to release.

For example, the process for using Appdome for defense automation is:

- Connect Appdome to the DevOps CI/CD platform
- Select the protections needed (e.g. RASP, anti-bot, anti-fraud, anti-malware, etc.)
- Build the Appdome protection libraries in the mobile app, which happens each time the dev team kicks off a build process
- Generate a certificate of coverage for the protections you chose to show that they are in effect in the app to clear each release
- Monitor the defenses and any new attacks in real time from the production environment.

©2023 Intellyx LLC. www.intellyx.com

Appdome is an entirely no-code and fully automated platform with plug-ins for the leading CI/CD tools so that you can add any of its protection libraries during the build process. The Appdome platform also comes with compliance reporting across users, builds, and events, as well as full change management, role-based entitlements, and other protection histories, making it easy for security teams to show that each release the app conforms to company security policy.

The Intellyx Take

Mobile applications are quickly becoming the new frontlines of cybercrime. Mobile apps and smartphones will continue to be more important to daily life. As they do, developers will constantly chase new capabilities and functionality to release into mobile applications, making them richer and more compelling for users and attackers alike.

One of life's natural conflicts is between people who build things and people who protect things. In many ways, the contrast between mobile app dev and security can be characterized as between optimism (what could go wrong?) and pessimism (whatever can go wrong, will go wrong), and between business opportunity and business risk. It's not easy to find a happy medium and eliminate natural conflict.

Who does the work, how and when are a constant battle in traditional DevSecOps models. Now, businesses can resolve the conflict with defense automation.

Appdome's defense automation platform allows businesses to build, test, release and monitor standard security, anti-fraud, and other protections in Android & iOS apps alongside security tests in the CI/CD pipeline, eliminating the battles, and the back and forth with reviews and waivers that can clog traditional DevSecOps processes.

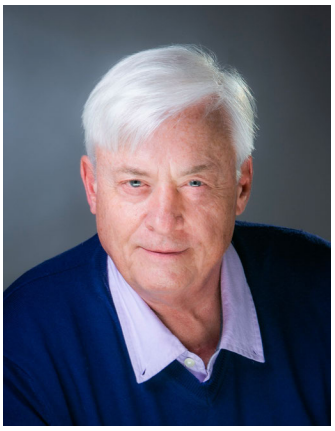
Cybersecurity and development both want to save and reclaim the valuable time and wasted effort that's spent in debate and resolving risk exceptions in mobile applications delivery.

Both development and security teams understand the value and importance of proper protection in mobile applications. What's been lacking is a technology platform to get the work done quickly, efficiently, and consistently.

Appdome is the ideal tool for resolving the conflict between dev and sec: automatically securing and monitoring defenses in mobile apps to reduce conflict and speed time to market.

©2023 Intellyx LLC. www.intellyx.com

About Eric Newcomer



Eric Newcomer is Principal Analyst and CTO at Intellyx, a technology analysis firm focused on enterprise digital transformation.

He previously served as CTO at WSO2 and at IONA, led Security Architecture for Citi's consumer banking and was Chief Architect for Citi and Credit Suisse's trade and investment divisions.

Eric is an internationally recognized expert in transaction processing, integration and cloud migration, having contributed to many industry standards including OSGi, Eclipse, SOAP, WSDL, UDDI, AMQP and more. His textbooks, including Principles of Transaction Processing, Understanding Web Services, and Understanding SOA with Web Services are used at universities around the world.

About Appdome

Appdome, the mobile app economy's one-stop-shop for mobile app defense, is on a mission to protect every mobile app in the world and the people who use mobile apps in their lives and at work.

Appdome provides the mobile industry's only mobile application Cyber Defense Automation platform, powered by a patented artificial-intelligence based coding engine, Threat-Events™ Threat-Aware UX/UI Control and ThreatScope™ Mobile XDR. Using Appdome, mobile brands eliminate complexity, save money and deliver 300+ Certified Secure™ mobile app security, anti-malware, anti-fraud, MOBILEBot™ Defense, anti-cheat, MiTM attack prevention, code obfuscation and other protections in Android and iOS apps with ease, all inside the mobile DevOps and CI/CD pipeline.

Leading financial, healthcare, mobile games, government and m-commerce brands use Appdome to protect Android and iOS apps, mobile customers and mobile businesses globally. Appdome holds several patents including U.S. Patents 9,934,017 B2, 10,310,870 B2, 10,606,582 B2, 11,243,748 B2 and 11,294,663 B2. Additional patents pending.

Copyright © Intellyx LLC. Appdome is an Intellyx customer. None of the other organizations mentioned in this article is an Intellyx customer. Intellyx retains final editorial control of this paper. No AI was used in the production of this paper