Phased Approach to Securing DevOps for Mobile Apps

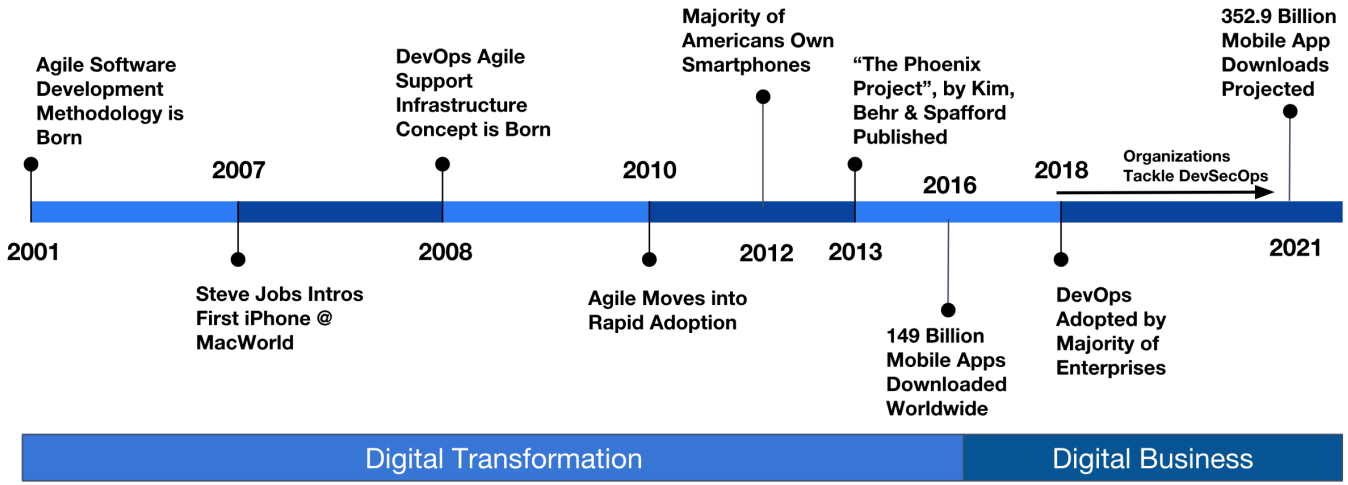
NowSecure™

Introduction

The rapid ascent of agile and mobile technology over the last seventeen years has changed the way we navigate daily life at work and home. Agility and mobility have become synonymous with modern customer expectations for experiences that are simple, fast, and available anywhere, at anytime. These expectations have fueled digital transformations across every industry and, in turn, have accelerated internal efficiency-focused initiatives, such as DevOps. Digital businesses have improved speed-to-market and increased customer engagement by streamlining cross-functional communication and automation to achieve faster results.

Even with the prominence of mobile-first strategies within digital businesses today, however, the speed and complexity of mobile app development continues to create significant challenges for organizations attempting to secure this process. Providing insight and guidance into the underrepresented topic of mobile app security in a DevOps environment, this eBook will help security professionals, DevOps managers, and executives alike find a phased approach that balances the need for security at the speed of mobile development while leveraging investments made in DevOps infrastructure.

In order to understand how to move forward, let's take a look at how we got here.



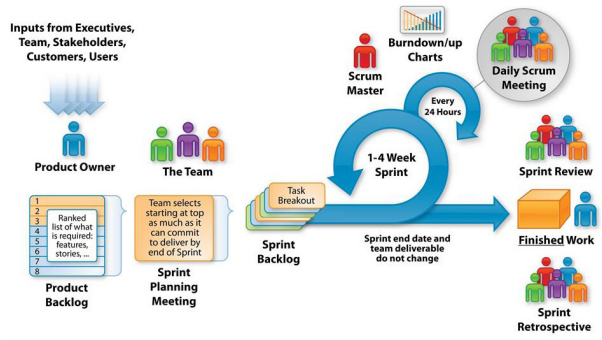
The Rise of Agile and Mobile

"[W]elcome changing requirements, even late in development. Agile processes harness change for the customer's competitive advantage."

- Principles behind the Agile Manifesto

The seedling for agile software development started in 2001 with a group of techies who felt there had to be a better way than the sequential, slow waterfall development process to release software.[1] They determined a more iterative process with a continuous feedback loop would be more effective, enabling micro launches every few weeks, compared to months or years.

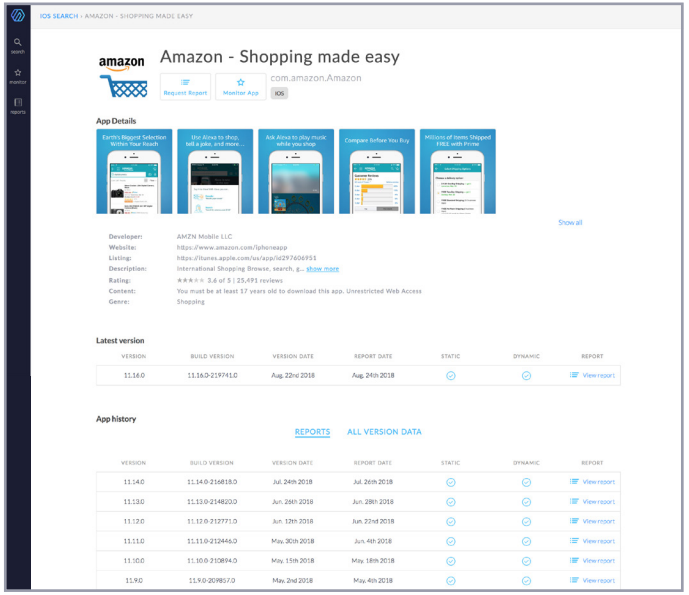
A few years later, in 2007, Apple® introduced the first iPhone[2] followed shortly thereafter with the opening of the App Store®[3]. Almost immediately, a new market category emerged as demand for convenience tech and accessibility grew. Many mobile app developers chose to leverage agile development from the beginning, rapidly increasing the volume of new apps reaching the market.



Above: The Agile-Scrum Framework
Source: C# Corner

By 2010, agile adoption began to sharply accelerate as more companies recognized the value of quicker release cycles or felt pressure from more nimble competitors.[4]

Many of the tech giants that adopted agile mobile app development early, like Apple, Amazon, and Netflix, are now in the top 25 positions on the Fortune 500.[5] Their ability to quickly translate customer needs into mobile app enhancements within days or weeks resulted in sizeable gains in both revenue and market share.



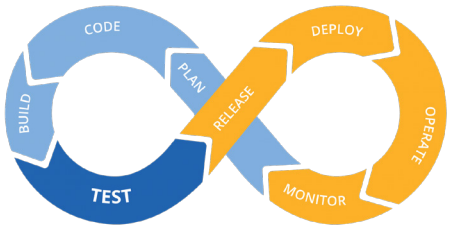
Above: Amazon agile mobile app release cycle
Source: NowSecure INTEL Amazon iOS App Risk Page

DevOps is Born

DevOps is an organizational and cultural shift which promotes people over process, removing obstacles that slow continuous innovation and leveraging integration and automation to create consistent and clear pathways to rapid execution.

When releases started pushing every few weeks or days, many operational resources downstream from developers, such as tech support, security, and QA, were initially caught off guard. This created internal friction while everyone struggled to keep up with the new pace and stay afloat.

Much like the software development pioneers that came together years prior, agile practitioners Andrew Schafer and Patrick Debois bonded at the 2008 Agile Conference in Toronto over their shared belief that there had to be a better way for development and operations to manage the accelerated pace of deployments.[6] They went on to create the Agile Systems Administrator group on Google and the movement soon picked up steam, becoming known as DevOps.

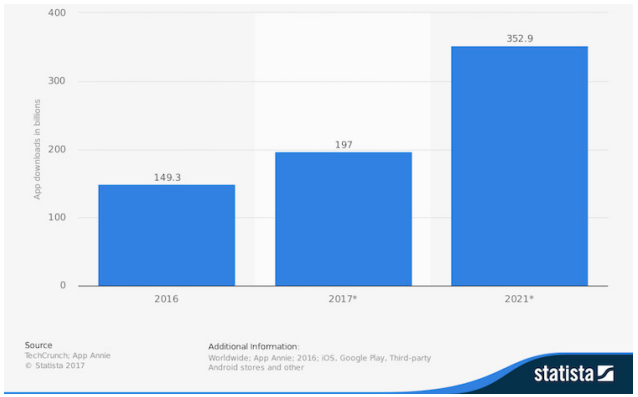


Above: DevOps Process with Continuous Feedback Loop
Source: Hackernoon, "Has DevOps changed the role of the tester?"

Right: Number of mobile app downloads worldwide, 2016, 2017, & 2021
Source: Business of Apps, "App Download and Usage Statistics"

This new agile approach requires Development and Operations teams to align goals, communicate more frequently, and build trust in order to achieve more efficient release processes.

During the early years of the DevOps movement, smartphone usage was also taking off. By 2012, Nielsen reported more than half of mobile phone users owned smartphones.[7] By 2016, the world had downloaded more than 149 billion mobile apps with estimates of upwards of 353 billion mobile apps projected to be downloaded by 2021.[8] The ability to install mobile apps to customize smartphones to individual needs soon made the device an indispensable tool providing instant access to bank accounts, retail shelves, maps, restaurants, and geographically dispersed friends and family.



Many of the early adopters of agile development and mobile-first strategies, like Amazon, Netflix and Facebook, were also among the first to complete a transition to DevOps support infrastructures.[9] As a result, these tech giants achieved a remarkable head start anticipating end-user demands by innovating quickly and dramatically reducing time-to-market.

Today, analysts agree that 2018 marks the year more enterprises have adopted DevOps than have not.[10] And while many of these organizations look forward to less chaos and more innovation, Gartner estimates that fewer than 20 percent of those deploying or planning to deploy DevOps have engaged security architects when planning the initiative. Organizations with mobile apps that contribute prominently to their growth, revenue, and brand, will need to consider in the next DevOps iteration how they certify apps are responsibly developed and secured.

> "[E]nterprise security architects in fewer than 20% of organizations have been engaged to systematically incorporate information security into their organizations' DevOps initiatives."
>
> *- Gartner, "Top 10 Strategic Technology Trends for 2018: Continuous Adaptive Risk and Trust", Analysts David Cearley, Neil MacDonald, Mike Walker, Brian Burke*

A Closer Look at Mobile App Security

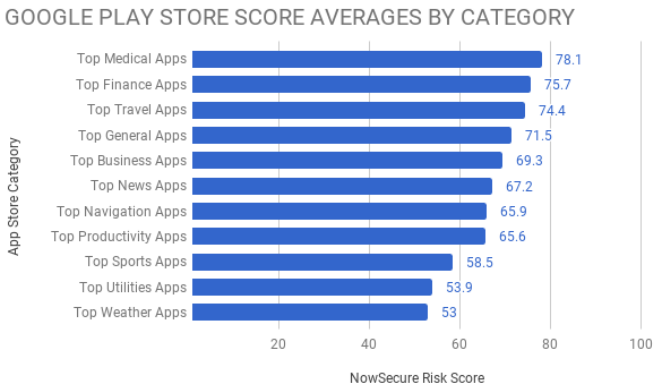
"Zuckerberg, on the call with reporters, said Facebook should have done more to audit and oversee third-party app developers like the one that Cambridge Analytica hired in 2014. 'Knowing what I know today, clearly we should have done more,' he said."

- Reuters, "Facebook says data leak hits 87 million users, widening privacy scandal"

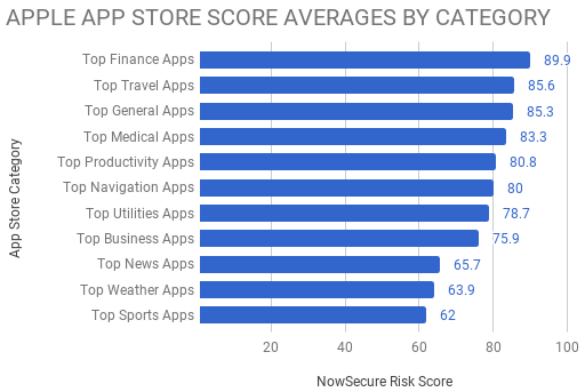
Solving for both speed and security within a DevOps program certainly requires careful thought and planning. Gartner projects that by 2019, only 10% of DevOps initiatives will have achieved the level of security automation required to be considered fully DevSecOps, up from less than 5% in 2017.[11] Unfortunately, security trade-offs and incomplete vetting processes can result in financial ramifications for companies forced to clean up after embarrassing mobile app data privacy or leakage scandals.

In a recent example, Facebook revealed that 87 million users' data was leaked to Cambridge Analytica via a quiz app.[12] The tarnished brand image slowed user growth for the first time in its history and resulted in a $120 billion single-day stock market loss, the biggest single-day loss ever recorded to date.[13]

Additional complexities are introduced as mobile teams look outward for rapid solutions, such as leveraging open-source third-party libraries or outsourcing mobile app development altogether. NowSecure recently conducted an aggregate analysis of the top 10 downloaded apps from the top 11 categories, in both the Apple App Store and Google Play™. Evaluating the apps for security vulnerabilities, compliance gaps and privacy exposure, we



Source: NowSecure Analysis of Most Downloaded Apps in Top Categories on Google Play, June 2018



Source: NowSecure Analysis of Most Downloaded Apps in Top Categories on Apple App Store, June 2018

determined a grade using industry-standard CVSS scores while mapping findings to both NIAP and the OWASP Mobile Top 10. Apps scoring lower than 60 present a high degree of risk, while those scoring 80 or above are deemed low risk.

Many of the top downloaded apps were found to have high risk vulnerabilities, including insecure communications over HTTP, location data leakage, and exposure to man-in-the-middle attacks. For iOS, News, Sports, and Weather apps were weakest, but still scored higher on average than Android, of which none of the app categories scored above 80.

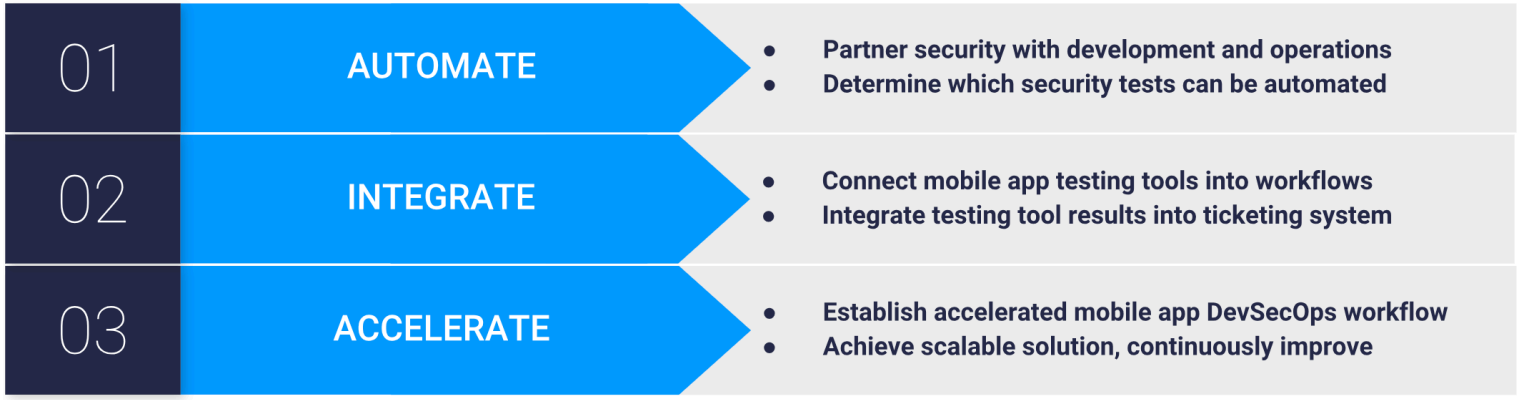
Many assume Apple or Google app stores' vetting process provides enough protection, but this has led to many mobile apps making it into app stores with significant vulnerabilities well into 2018. These issues are serious but can be addressed before apps are released. Given the prominence of mobile-first strategies, it stands to reason that securing mobile apps before they are released to end users should rank as a top priority.

"By 2019, only 10% of DevOps initiatives will have achieved the level of security automation required to be considered fully DevSecOps."

- Gartner, "Integrating Security into the DevOps Toolchain", Analysts Mark Horvath, Neil MacDonald, Ayol Tirosh

Phases to DevSecOps for Mobile Apps

NowSecure is singularly focused on mobile application security and has been in the trenches with top security organizations across the public and private sectors for a decade. We have helped many organizations transition to DevSecOps and understand that everyone is at a different part of the mobile app DevSecOps journey. Our goal is to provide a baseline process directly from mobile app security testing experts and our most advanced customers, from which any organization can grow and improve their program. In the following sections, we share a high level overview of a phased approach many organizations have used to ensure mobile apps are responsibly developed and secured.



Above: NowSecure Phases to Mobile App DevSecOps

Phase 1 - Automate

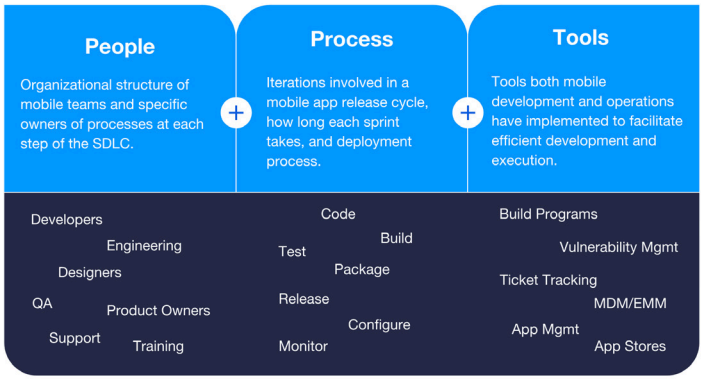
Partner security with development & operations teams and learn process flows

Security professionals often find themselves chasing continuous release cycles and navigating near-constant updates to the mobile app development process. When wading into existing DevOps programs, it's important that security teams adopt a collaborative, agile mindset and look for ways to join in without slowing other teams down.

Above: DevSecOps Manifesto
Source: DevSecOps.org, "DevSecOps Manifesto"

The DevSecOps Manifesto nicely outlines a comparison of the old security approach versus a more modern approach that enables DevSecOps.

Once everyone is in the right mindset, it's time to conduct proper due diligence to determine where security will fit within existing DevOps workflows. Automation tools exist to accelerate the process, but rushing to implement new tools without fully understanding interdependencies of the DevOps ecosystem in which they will co-exist could inadvertently break another workflow. The best first step is for security professionals to learn what people, processes, and tools are involved across the mobile app development lifecycle in order to determine the best path forward.



Above: NowSecure Blueprint for Mobile DevOps Process

Once a blueprint of mobile app development and operations stakeholders' workflow is in place, security can next look inward at the current mobile app testing process. If no process exists today, the next step is to gather the requirements for launching a program.

Determine which security tests can be automated

Automation is required for security teams looking to incorporate testing into a DevOps process. Organizations that have an existing mobile app security program most often rely on a static-only source code analysis tools or cobble together a homegrown solution leveraging open-source tools. Static-only legacy methods have not scaled to the speed of agile nor have they reduced friction between development and security teams, given the high amount of false positives that slow down the pipeline and frustrate developers.

Also, static analysis scans only data at rest and completely misses network issues of data in motion. The only way to truly test data in motion is dynamically on real devices. For example, if the objective of a test is to determine whether the app is logging sensitive data:

- **Static analysis** will flag whether or not certain debugging and logging flags are enabled or disabled
- **Dynamic analysis** will actually run the app and search device logs and network communication for sensitive values (e.g., user credentials)[14]

In this example, if dynamic analysis finds user credentials in cleartext over HTTP or in the log files, there's no denying the existence of an issue. The ability to automatically confirm a result and rule out false positives during the test solves for both speed and depth of coverage at once, showcasing how quickly automation can scale a security operation.

Mobile AppSec Testing Coverage

Data at Rest

Test for sensitive data insecurely stored in places like SQLite databases, log files, SD cards, etc.

Data in Motion

Test for sensitive data insecurely transmitted due to SSL/TLS certificate issues, HTTP transfer of data in cleartext, etc.

Code Quality

Test for code security issues such as buffer overflows, format string vulnerabilities, SQL injection, arbitrary code execution, etc.

As security professionals review options to automate mobile appsec testing, they must ensure the solution can also grow and innovate at the pace of mobile app development. Key considerations should include:

- Combining static, dynamic and behavioral mobile app vulnerability tests on real devices to automate the validation process and exclude false positives.
- Consistent testing of the full mobile attack surface including data at rest, data in motion, and code quality.
- Detailed remediation instructions for developers, and auto-generated, customizable reports, giving time and energy back to security analysts.

Automated security testing solutions must solve for multiple problems such as ensuring tests cover current security threats, uncovering privacy vulnerabilities, and reviewing regulatory compliance. Full testing coverage requires organizations to go beyond source code analysis to ensure consistency and scalability. The intelligence of behavioral analysis means all findings are verified with near zero false positives.

Above: Types of Moble AppSec Testing

Edge cases

Not all mobile app features are the same nor are all vulnerabilities created equal. There are often scenarios like multi-factor authentication, mobile apps with IoT, and USB/Bluetooth connected equipment that require specialized testing solutions built specifically to analyze more complex use cases. There are mobile application testing tools which automate these functions while also giving the analyst full control. Some organizations also choose to outsource these more complex use cases to mobile application testing experts.

Once the mobile security team has incubated a reliable, repeatable automated testing process, they can update DevOps stakeholders and begin planning for the next phase, integration.

Phase 2 - Integrate

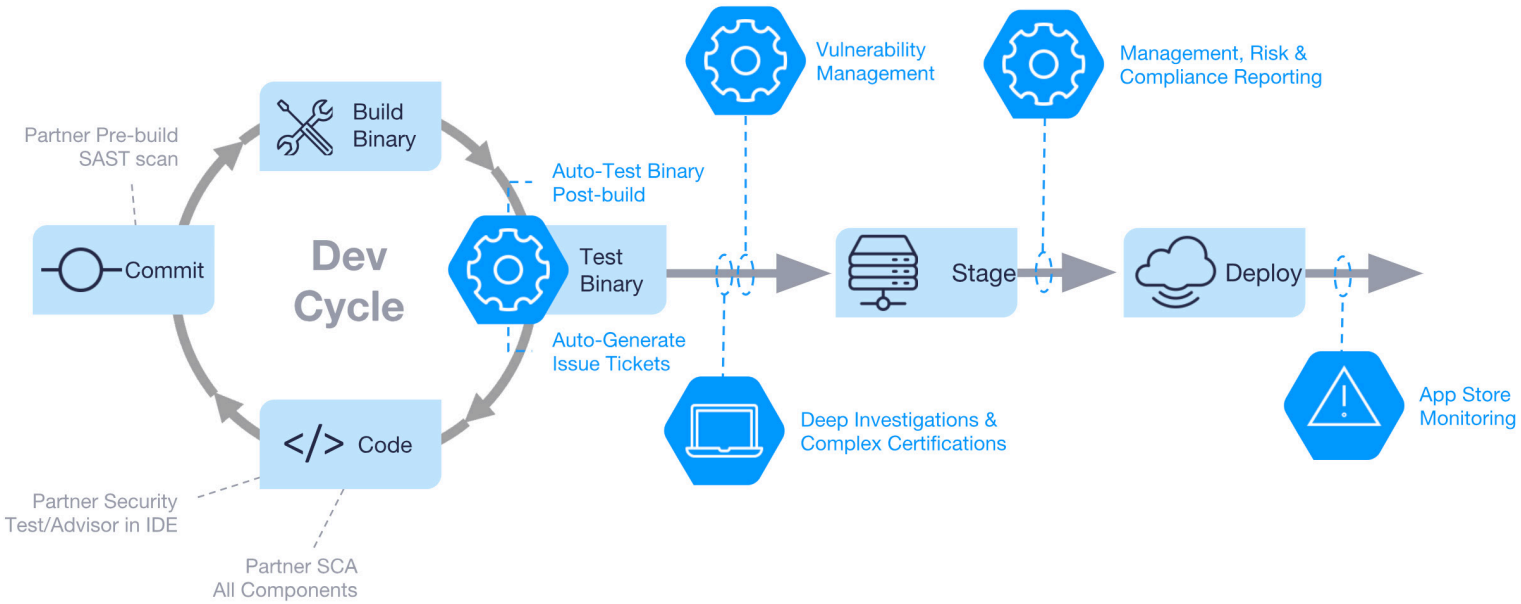
Connect mobile app testing tool directly into workflows

Organizations that have already established some DevOps processes will have automated tools and build-and-deploy solutions already in place. For example, mobile app security test automation might be inserted at the build level and test compiled builds from the CI server, like CloudBees Jenkins[15], Circle CI, GitLab, etc.

Integrating mobile app security automation into existing DevOps processes should be fairly easy given existing tools are purpose-built to be extended and integrated with others. Just ensure the change management process is well understood and a partnership has been established with the owner of the workflow the testing tool will be plugging into.

Integrate testing tool results into ticketing system

Integrating mobile app security testing within issue-tracking software, such as Jira, allows test results to be automatically filed, generating tickets for vulnerabilities. Tickets should include remediation instructions so developers can locate and fix issues quickly, without the need to learn a new security tool. The purpose of integrating automated tools into the toolchain is to accelerate each team's ability to maintain forward momentum, not to expect each team to completely learn new skills from ground up.

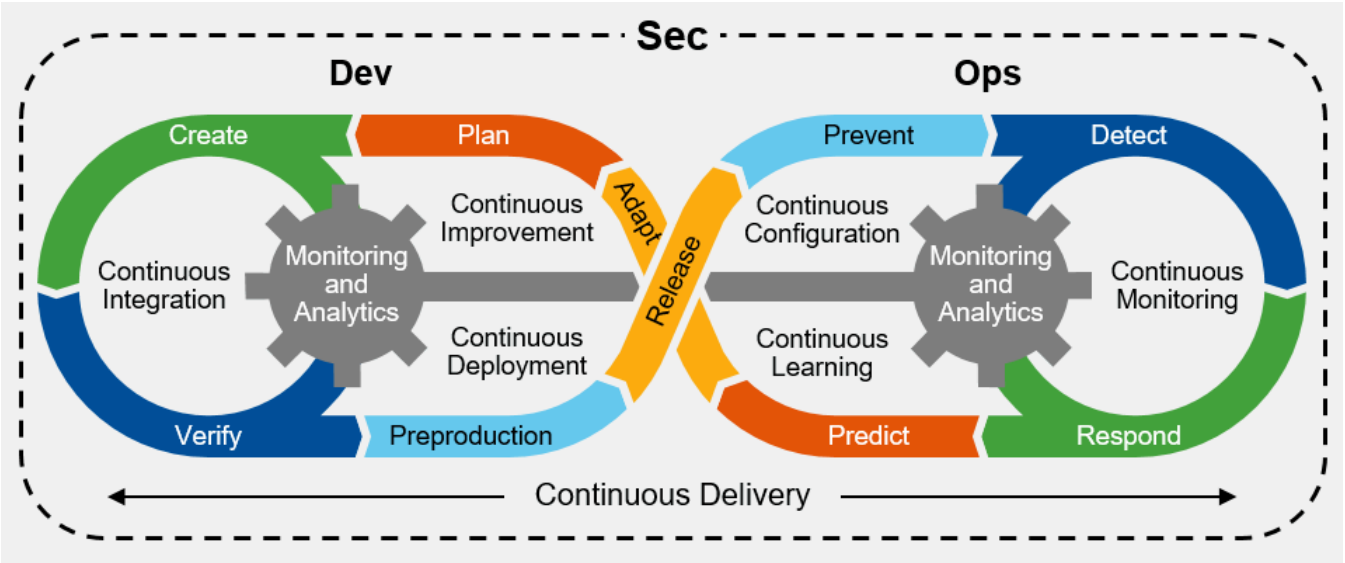


Above: Security Testing within the SDLC

Phase 3 - Accelerate

Establish accelerated mobile app DevSecOps workflow

Removing manual security testing as a barrier to releasing software enables security professionals to take on more of a trusted advisor role, assisting DevOps teams with accelerating a responsible release program. Integrating mobile application security testing within the existing development toolchain and release cycle also results in security teams communicating more frequently and coming away with a better understanding of the development and operational process overall.



Above: DevSecOps - Seamlessly Integrating Security Throughout DevOps

Source: Gartner, "Integrating Security into the DevOps Toolchain", Analysts Mark Horvath, Neil MacDonald, Ayol Tirosh

By developing security as code, we will strive to create awesome products and services, provide insights directly to developers, and generally favor iteration over trying to always come up with the best answer before a deployment. We will operate like developers to make security and compliance available to be consumed as services. We will unlock and unblock new paths to help others see their ideas become a reality.

-DevSecOps.org, "DevSecOps Manifesto"

Achieve scalable solution, continuously improve

Scalable, confident mobile app DevSecOps programs create significant benefits for everyone. Automation enables teams to do more in less time. Full coverage signficantly reduces the headaches of false positives. Security professionals can better manage workloads and transform into a key partner for secure innovation, enabling what the DevSecOps Manifesto calls "security as code," and building more collaborative, efficient programs.

About NowSecure

NowSecure is the mobile app security software company trusted by the world's most demanding organizations. Only the NowSecure Platform delivers fully automated mobile app security testing with the speed, accuracy, and efficiency necessary for Agile and DevSecOps environments.

Through the industry's most advanced static, dynamic, behavioral and interactive mobile app security testing on real Android and iOS devices, NowSecure identifies the broadest array of security threats, compliance gaps and privacy issues in custom-developed, commercial, and business-critical mobile apps. NowSecure customers can choose automated software on-premises or in the cloud, expert professional penetration testing and managed services, or a combination of all as needed.

NowSecure is the fastest path to deeper mobile app security testing and certification. For more information about NowSecure, visit https://www.nowsecure.com.

SOURCES

1. History of the Agile Manifesto, http://agilemanifesto.org/history.html
2. The Verge, “Watch Steve Jobs introduce the iPhone 10 years ago today”, https://www.theverge.com/2017/1/9/14208974/iphone-announcement-10-year-anniversary-steve-jobs
3. Appleinside.com, “Apple details history of App Store on its 10th anniversary”, https://appleinsider.com/articles/18/07/05/apple-details-history-of-app-store-on-its-10th-anniversary
4. TechBeacon, “Survey: Is agile the new norm?”, https://techbeacon.com/survey-agile-new-norm
5. Fortune.com, Fortune 500 list, http://fortune.com/fortune500/list/
6. DevOps.com, “The Origin of DevOps: What’s in a Name?”, https://devops.com/the-origins-of-devops-whats-in-a-name/
7. Mediapost, “Nielsen: US Smartphone Adoption Hits 55%”, https://www.mediapost.com/publications/article/182682/nielsen-us-smartphone-adoption-hits-55.html
8. Business of Apps, “App Download and Usage Statistics”, http://www.businessofapps.com/data/app-statistics/
9. TechBeacon, “10 companies killing it at DevOps”, https://techbeacon.com/10-companies-killing-it-devops
10. Forrester, “2018: The Year of Enterprise DevOps”, https://go.forrester.com/blogs/2018-the-year-of-enterprise-devops/
11. Gartner, “Integrating Security into the DevOps Toolchain”, Analysts Mark Horvath, Neil MacDonald, Ayol Tirosh, https://www.gartner.com/doc/reprints?id=1-4PMXPUK&ct=180125&st=sb&elq_mid=432&elq_cid=199413
12. Reuters, “Facebook says data leak hits 87 million users, widening privacy scandal”, https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM
13. CNET, “Facebook stock’s $120 billion loss is biggest single-day drop ever”, https://www.cnet.com/news/facebook-shares-plunge-after-warning-of-slowing-growth/
14. NowSecure Mobile App Security Program Handbook, https://www.nowsecure.com/ebooks/mobile-app-security-program-management-handbook/
15. NowSecure Blog, “Making Mobile Application Testing Automation a DevOps Reality”, https://www.nowsecure.com/blog/2017/02/28/mobile-app-security-testing-automation-devops-reality/