Checkmarx
MAKE SHIFT HAPPEN

Build #DevSecTrust

7 Steps

to Prioritize AppSec for the Greatest Impact

AppSec is not just about finding vulnerabilities. It's also about fixing them. Your developer experience needs to build trust between AppSec and developers to succeed. The first step? Prioritize—both your efforts and theirs—where you can make the greatest impact.

THE TRUST DEFICIT

The Core Challenge in Application Security

Application security is not just about finding vulnerabilities. The hard part is also fixing them.

These two critical roles—finding and fixing—are typically performed by two teams: AppSec and developers. Those teams don't always work well together, but the reasons why can be elusive. Approaching this problem from a human perspective can help you better understand the core issue—a deficit of trust.

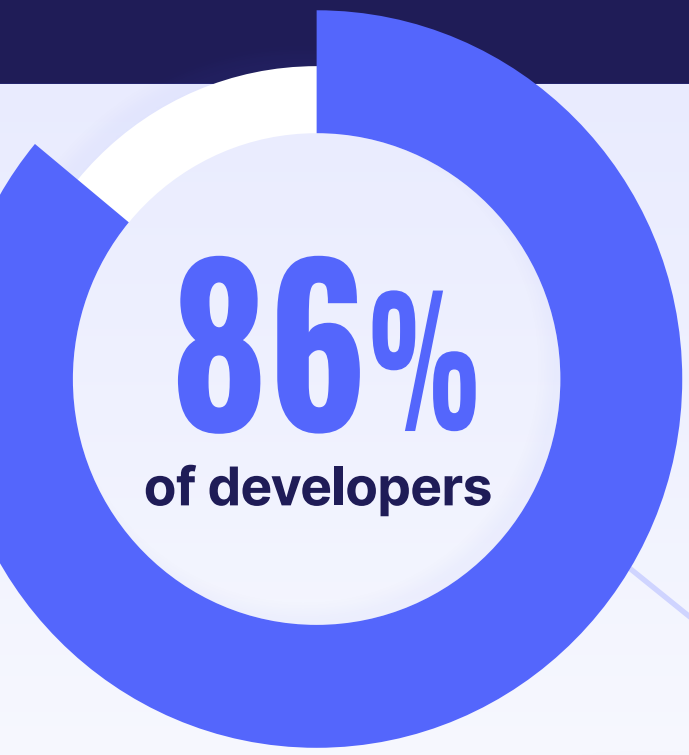
CISOs and AppSec teams are tasked with reducing risk in the applications their developer teams build. Yet, they often face hurdles in persuading developers to remediate the vulnerabilities they find. For an AppSec team, it can be frustrating to invest the time and effort to deploy an AppSec solution, find security issues, and then not see those issues fixed. However, the challenge is generally not as simple as developers not taking security seriously.

In modern enterprises

Development teams are under tremendous pressure to deliver software fast. Every day they face hurdles just getting code out the door.

In the Checkmarx 2022 Pulse of Application Security report, 86% of developers admit to shipping known-vulnerable code. For developers, fixing security issues takes them away from their core focus. They don't always have the knowledge. Security can require new tools that they must learn. And the issues they're sent may have false positives and lack clear prioritization on where to start. In that situation, it's easy for trust to break down. In fact, how could it not?

But by understanding the core issue, you can design a developer experience that actually builds trust between AppSec teams and developers and helps everybody succeed.



Admit to shipping known-vulnerable code.

Why is that? Keep reading to learn more ⟶

BUILDING #DEVSECTRUST

Through Developer Experience

The trust deficit can prevent any organization from succeeding in application security. AppSec teams can find vulnerabilities on their own. But you need your developers' trust to fix them. This needs to be seen as a human problem, one that can be approached within the framework of the developer's experience.

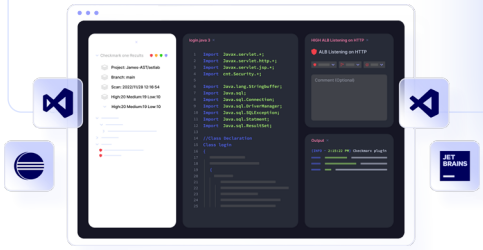
The Three Pillars

Through which every enterprise organization must think about the elements of your developer experience are:

CONTINUE READING

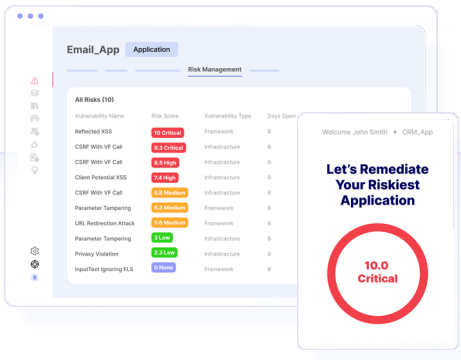
Meet developers where they live

Seamlessly integrate AppSec into developers' ecosystem and workflow to make it easier for them to fix vulnerabilities without slowing them down.



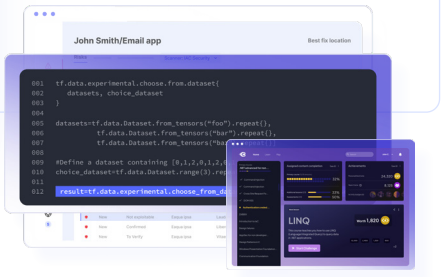
Prioritize the greatest impact

For AppSec teams, these are the vulnerabilities that represent the biggest risk. But for developers, it's where they can make the greatest impact.



Equip them with tools and knowledge

Make it easier for developers to fix vulnerabilities faster, while helping them learn and grow into your next security champions.



WHAT YOU NEED

To Prioritize the Greatest Impact

Whether it's SAST, WAF, or anything in between, AppSec teams are used to thinking about accuracy, for any AppSec solution, in percentages. But accuracy isn't just a statistic; it's corrosive. When you approach developers with a long list of critical issues that must be fixed, and soon they find out that half aren't real, your credibility becomes damaged.

Improving accuracy and then prioritizing the most critical vulnerabilities to fix first will go a long way in rebuilding trust between AppSec and development teams. However, it requires more than just simple fixes.

It requires a holistic strategy, with incremental steps that you can take to demonstrate your commitment to improving the developer experience:

of organizations

have over five different AppSec solutions

01

Customize your AppSec

A fundamental rule of AppSec is that security must be tailored to the application. This is because the root cause behind false positives and false negatives has as much to do with the variation between your applications as it does with the AppSec solution. Different programming languages have different nuances, and what creates a vulnerability in one application may not in another. Tuning your AppSec controls to each unique application is the only way to account for the differences in your applications.

02

Onboard considerately

Experienced AppSec teams know that you can't just turn on an AppSec solution for an application; you must onboard the application into your AppSec program. Onboarding is the first impression you make, and overwhelming developers with false positives right from the start doesn't make a good one. Make sure you follow best practices—from tuning to correlation to integration—when you onboard applications into your AppSec program so you can prioritize the team from the start.

03

Correlate security findings

AppSec practitioners know that AppSec solutions don't find vulnerabilities; they find potential vulnerabilities. Analyzing potential vulnerabilities to confirm what's real can take time and resources that AppSec teams don't always have. Correlation is a technology that can make it easier. Correlating security findings from different AppSec solutions can help you identify what's actually exploitable and send only those to your developers to fix.

04

Unify your dashboards

Correlation can help prioritize, but AppSec teams still need to analyze and triage. That can be challenging when 60% of organizations employ more than five different AppSec solutions. Different AppSec solutions are often managed by different teams, each solution requires its own dashboard, and every vendor reports vulnerabilities differently. Having a unified dashboard for all your AppSec solutions streamlines the process and makes it easier to analyze and triage vulnerabilities from all your AppSec solutions.

05

Eliminate duplication

Software bugs are expected, and bug tickets are an accepted ritual for any developer. A good AppSec solution will log vulnerabilities as bug tickets to put security in the workflow of your developers, but accuracy can still be a problem. What's worse than getting a bug ticket? Getting multiple bug tickets for the same vulnerability. Beyond making sure that the vulnerability is real, the easiest thing you can do is make sure you're only sending one bug ticket for any vulnerability.

06

See the entire picture

When enterprise organizations have hundreds to thousands of applications, managing application security risk requires knowing where to start. Prioritization must consider not just the severity of a vulnerability but also the criticality of the application. You need to quickly understand what your top riskiest applications are and prioritize efforts there to make the biggest impact on reducing business risk.

07

Get additional help

Not every organization has the time or resources to manage an AppSec program, and that's ok. Many of the largest enterprise organizations in the world lean on managed services from Checkmarx to bring in additional AppSec resources and expertise that can complement their teams.

What Next?

Securing digital transformation requires advanced AppSec technologies, but technology by itself is not enough. By approaching the problem through the lens of improving the developer experience and building trust, CISOs and AppSec teams can create a collaborative security culture that doesn't just find vulnerabilities—it fixes them.

The future of AppSec is not just secure code—it's secure relationships, too.

Learn more about

Designing a developer experience that builds #DevSecTrust

Discover How ⟶

Checkmarx

Checkmarx is the Enterprise Application Security provider, offering the industry leading cloud-native platform, that builds DevSecTrust – Checkmarx One™. Fueled by intelligence from our industry leading AppSec security research team, our AI driven technology and services enable CISO, AppSec and Development leaders to prioritize their teams on what impacts their business. Our offering secures every phase of development for every application from the very first line of code until production (Shift Everywhere) while simultaneously balancing the dynamic needs of security and development teams. We are honored to serve more than 1,800 customers, including 60 percent of Fortune 100 organizations, and are committed to moving forward with an unwavering dedication to the safety and security of our customers and the applications that power our day-to-day lives.

MAKE SHIFT HAPPEN