



Application Security Champions Report

2022 INSIGHTS REPORT

Contents

Foreword: Successful DevSecOps is the bedrock for digital transformation	3
Introduction	4
Methodology	6
Overall key takeaways	8
Program approaches	9
Best practices for adoption	12
Program timing and timelines	14
Return on investment.	16
Conclusions and recommendations	18

Foreword: Successful DevSecOps is the bedrock for digital transformation

Twenty years ago, internet technology was accelerating at astonishing speed. Known, unknown, and unimagined threats and vulnerabilities were gaining ground, and Microsoft was losing customers. In an infamous internal memo, Bill Gates warned that new viruses and malware were on the run and eroding customer trust.

The world's largest software company was no longer going to tolerate treating security as an afterthought. "Secure development principles should apply at every stage of the development cycle of every kind of software we create," said Gates, and thus the secure software development lifecycle was born – and none too soon.

In 2001, just one year before Gates hit "send" on that urgent email, the Agile Manifesto entered the scene, setting the premise for modern development practices and principles – *but without one mention of the word "security."*

Though AppSec progress has been steady, the industry was slow to learn. Years after Bill Gates' shift-left declaration, Mark Zuckerberg's "move fast and break things" cliché still clung stubbornly to the Agile attitude. Even today, core programming groups rarely involve an AppSec pro from the get-go.

With the move to the cloud and the pandemic, the old-school "Agile, move fast, break things" methodology needs to hasten the paradigm shift where application security is mission critical and integrates into the foundation of code development.

With cutting-edge insight from Coalfire's elite Cloud Advisory Board (CAB), our recent

"Smartest Path to DevSecOps Transformation" report defines this new discipline, what it's all about, and why there's no turning back. The following insights report on AppSec champions programs shows how it can be done successfully within most enterprise development operations.

"Racing to market with products and cleaning up the mess later goes against today's best-practice risk management principles. Buyers, sellers, suppliers, and regulators won't accept this anymore," said Nils Puhlmann, CRSO, MoonPay, cofounder, Cloud Security Alliance, and Coalfire CAB member.

There are many roads to excellence in the continuous integration and deployment of DevSecOps orchestration, and more responsibility than ever falls on the shoulders of CISOs and security teams. One of the best places to start – and a best practice for keeping security front and center at every stage of the development cycle – is to establish an AppSec champions program. These insights from IT executives bring clarity, instill knowledge, and will help spread passion for security into application development from the first scrum.

John Dickson
Vice President, Security Solution Architecture, Coalfire

Introduction

In the last decade, security leaders have observed the emergence of application security champions programs. Known informally as “AppSec champions” programs, security managers use them to influence software developers in their organizations to write software in a more consistent and secure fashion.

“An AppSec champion is usually an application development team leader, architect, or lead developer who has an interest in delivering secure software and the ability to influence their team to adopt secure software development processes and tools.” **Matt Klein**, field CISO and executive advisor, Coalfire

These programs go by different names in different organizations, such as ninjas, embeds, security satellite, and others. They are typically run by a smaller AppSec team operating out of a centralized security organization with minimum control over the organization’s software development activities. As such, the AppSec team uses influence more than managerial control to affect the behaviors of software developers who report to leaders in different reporting hierarchies. In many instances, these AppSec champions programs begin informally and exist despite limited managerial mandates, originating within security organizations not from the top. Most AppSec managers strive to be successful without particularly strong signals from leadership.

An AppSec champions program describes a core team whose common goal is to promulgate secure software development practices across an organization. AppSec champions programs typically exist in organizations with a centralized security function that is responsible for software risk and works with software development teams to increase the security of applications being built.

These programs share common attributes, including:

- The centralized security teams are typically small (sometimes numbering in single digits) while the software teams number in the hundreds, or even thousands.

INTRODUCTION

- Given the numerical mismatch, security managers use AppSec champions as the concept of managerial leverage and informal influence to effect change.
- Measures of success vary across organizations but include metrics such as the total number of software vulnerabilities, vulnerabilities per line of code, or mean time to fix for application vulnerabilities.

AppSec champions programs are not training programs for developers. Instead, they use concepts to enable developers to accomplish what the security teams cannot do: Consistently build software that is less susceptible to exploitation from external attackers. This is particularly important because the number of software developers within an organization usually dwarfs that of security staff focused on application security.

Although AppSec champions programs exist throughout the industry, little research captures

commonalities and best practices associated with these programs. For the first time, Coalfire attempts to capture emerging practices and common attributes that AppSec managers believe will help improve the secure coding behaviors of their peers. The broader intent of this insight report is to quantify and improve the state of application security by highlighting emerging best practices and common practices that exist within AppSec champions programs.

Our hope is that security leaders will be more empowered to justify additional resource needs and organizational focus for application security when armed with industry research and quantitative benchmarking data. If successful, they may be able to change the behaviors of their departmental peers while improving the security of software produced within their organizations. This change cannot come quickly enough.

AppSec champions program maturity



Level 5: Optimizing (established and repeatable, driving ROI)

Level 4: Improving (driving behaviors, being improved, managing process improvement across the organization)

Level 3: Mature (documented, widely adopted across all teams, leadership sponsored)

Level 2: Maturing (established and repeatable but not on all teams, comprising volunteers and assigned staff)

Level 1: Emerging (very early stage, unstructured and unrepeatable)

Methodology

The survey focused on gathering best practices, metrics, and certain commonalities that exist within successful AppSec champions programs.

The survey used a structured research approach to elicit the most impactful results. Certain questions enabled quantitative analysis, while others furnished more contextual answers, including follow-on questions to elicit a deeper understanding of the organization's approach.

To better understand AppSec champions programs and the environments in which they operate, the survey asked about certain program attributes to identify what they had in common. Although these attributes are by no means exhaustive, the survey sought information about them to provide context and a broad sense of program maturity to allow the reader to compare their AppSec program with others.

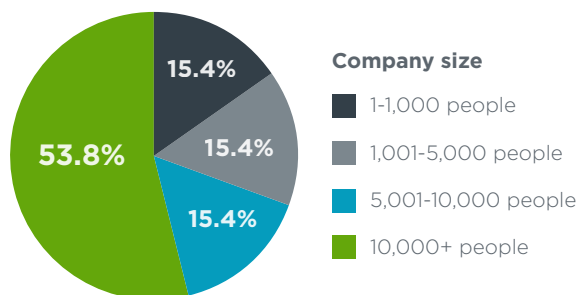
Some of these attributes were:

- *How many full-time team members are focused on application security?*
- *How long did it take to build an AppSec champions program and how long had it been in existence?*
- *How frequently do security leaders communicate with their AppSec champions and by what means?*
- *What type of managerial mandate do AppSec champions have?*

Survey parameters

Participants and organizational characteristics

- **26 companies** representing various industries, including pharma, banks, technology, telecommunications, financial technology, financial services, and entertainment
- **Companies of all sizes**, with the most participants from enterprise organizations with more than 10,000 employees
- **Private sector organizations**
 - Large-scale internal software production efforts
 - Full-time AppSec staff
 - AppSec champions program already in place or currently being built



Survey parameters CONTINUED

Questions were grouped into four areas

- 1** Common attributes of AppSec champions programs, including staffing ratios, construction, communication, interactions, governance, and mandates
- 2** Program timelines
- 3** Best practices for AppSec champions
- 4** Return on investment

With each survey participant, at least three calls were conducted – an overview, a data gathering, and an input validation call. The structured research approach also allowed for follow-on questions that provided substantially more context than might be gathered in a simplified format. This approach yielded relevant anecdotes and “war stories” that helped contribute to the overall understanding of AppSec champions programs.

To more deeply understand the common attributes of AppSec champions programs, we captured emerging

practices and common traits that AppSec managers believe will help build out the right program. Ensuring we captured a broad level of effort as reflected in the head count, we included software developers regardless of employment relationship to the survey participants. Along with full-time employees, temporary hires and contractors operating as an extension of the development team were also included.

The survey was conducted in 2020 and 2021 via live conversations with participants.

Overall key takeaways

1:50

AppSec programs identified as “mature” had a **1-to-50 ratio between full-time AppSec staff and developers.**



Most organizations built AppSec champions programs using volunteers, supplemented by developers who were “voluntold” or otherwise chosen by their managers to participate.

2/3

Two-thirds of organizations built AppSec champions programs without any organizational mandate or with only the blessing of the CISO.



Microsoft Teams

Most organizations use platforms like **Slack** and **Teams** to regularly communicate within AppSec champions programs, augmented with formal monthly newsletters or town hall meetings.

100%

There was a **100% correlation** between the existence of AppSec security tooling (SAST, DAST, and SCA) and the self-identified maturity of AppSec programs.



There is a **strong belief in AppSec champions programs**, but most are informal and immature.

6+ months

Most AppSec champions programs took **at least six months** to get off the ground.



Most organizations **have not captured ROI** for AppSec champions programs; if they have, it's mostly anecdotal.

Program approaches

Key takeaways

1:50

AppSec programs identified as “mature” had a 1-to-50 ratio between full-time AppSec staff and developers.

Insight: Security staff will likely be far outnumbered by developers (even in enterprises), and it is critical to identify security team members with the aptitude and desire to take part in the program.



Most organizations built an AppSec champions program using volunteers, supplemented by developers who were “voluntold” or otherwise chosen by their managers to participate.

Insight: Program success is dependent on finding participants who believe in the goals and have a voice in the evolution.

2/3

Two-thirds of respondents had no formal mandate or a CISO-only mandate, which is effectively a weak organizational mandate.

Insight: As with any cross-functional team, executive-level support and alignment among the managers of the program’s participants will drive long-term adoption and success.



slack



Microsoft Teams

Security teams were communicating directly with their champions through the platforms in which software developers operate daily, most notably Slack and Teams.

Insight: Program teams need to determine primary communication channels in their charter. The ideal channels will be collaborative and part of the members’ existing workflows.

Security leaders want to know how they are doing relative to their peers. We wanted to uncover core common practices that are fundamental to any AppSec champions program.

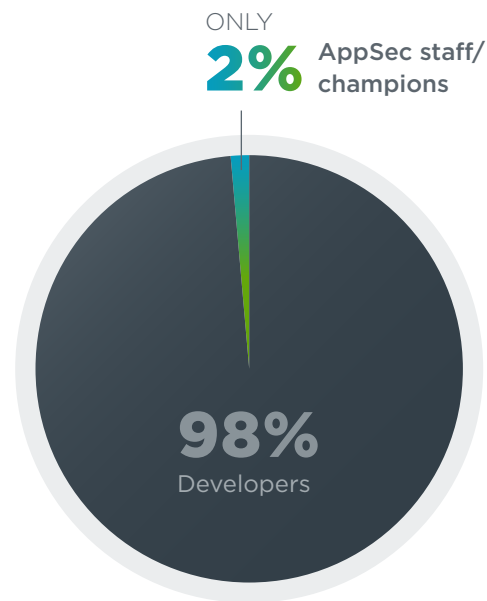
On average, we found that organizations had 1,657 developers, 13 full-time AppSec staff, and 8 AppSec champions.

Comparing the average number of AppSec staff to the average number of developers within each organization resulted in a ratio of 1-to-50 for mature AppSec programs. This is impactful and relevant to anyone seeking to build a sophisticated AppSec program. **In short, mature AppSec programs are likely to have a ratio of 1 AppSec staff member for every 50 developers.**

Constant communication and engagement appear to be central to any successful AppSec champions program. Although this might seem obvious, given the lack of managerial control and formal mandate, AppSec leaders should nurture AppSec champions programs to ensure long-term impact.

Several survey respondents communicated the importance of regular, formalized communication in addition to daily and weekly communication via platforms like **Slack** and **Teams**. Town halls and monthly email newsletters highlighting successes and positive behaviors provided a cadence of regular “official” program communication that supplemented the regular program chatter in Slack and Teams.

The promising aspect was that security teams were communicating directly with their



65%

communicate “constantly to weekly” – nearly all communicated at least monthly.



64%

of survey respondents use **Slack** and **Teams**.

champions in the platforms where software developers operate daily, most notably Slack and Teams. Other communication tools include email and SharePoint. The more sophisticated teams used dashboards or application vulnerability management systems to measure and communicate progress.

One final approach we wanted to understand was around the governance, mandates, and program structures that were in place. The result was in line with our original hypothesis that survey respondents had either no formal mandate or a CISO-only mandate. **Without the approval and support of the CISO, any AppSec champions program would not get off the ground.** Only a handful of responses cited support from the CTO or VP of software development; nobody cited the CFO or COO.

“When I was hired in 2016 as CISO at Q2 Software, we had multiple engineering teams developing software in multiple languages. We decided to update our software development lifecycle program to include periodic static and dynamic scanning across all teams. The best way to implement the new requirements was to develop an AppSec champions program to utilize everyone's input and knowledge in developing best practices. The best part is the knowledge we share each week on secure coding.”

Bob Michaud

SVP, Chief Security Officer, Q2 Software

Best practices for adoption

Key takeaways

2/3

Nearly two out of three organizations did not have defined roles, formal training, or a reward program for their AppSec champion program.

Insight: Establishing best practices is critical to achieving a successful program that will scale across the organization.

100%

There was a 100% correlation between the existence of AppSec security tooling (SAST, DAST, and SCA) and the self-identified maturity of AppSec programs.

Insight: Programs are successful when there is alignment around the importance of having the right security tools in place.

To many of our survey participants, understanding emerging best practices for AppSec champions programs was of the most interest. Given that AppSec champions programs typically involve a small number of AppSec staff trying to influence a larger number of their development colleagues, we wanted to understand how programs are formalized, scaled, and what, if any, best practices are implemented.

62%

of respondents have defined roles and standards.

62%

of respondents do not have a formal AppSec champions training program.

69%

of respondents do not have a rewards program for their AppSec champions.

The results point toward further across-the-board areas for improvement of AppSec champions programs. We expected to see organizations with more structure – defined roles, standards, and formalized training programs. The lack of rewards programs seems to be an opportunity missed as well. The assumption is that with more structure – e.g., training, roles, and rewards – organizations might be able to scale their AppSec champions program across all their software development teams.

Interestingly, when focusing exclusively on respondents who identified their AppSec program as “mature,” the results vastly improved. Given that security teams are trying to win the “hearts and minds” of software developers, the use of rewards, training, and other attractive incentives strikes us as table stakes for any AppSec champions program.

To round out common program practices, we wanted to understand organizations’ technology stacks (security tooling, cloud, and pipelines) and identify whether any relationship existed between the environment and AppSec champions program maturity.

Overall, results confirmed the gap between developers and AppSec staff and that there was a direct correlation with AppSec programs that had tooling technologies in place. **Sixty-one percent of companies said they were using pipelines to build and deliver software**, while the remainder said they were planning on putting pipeline evaluation into production within the next two calendar years. In addition, **most programs (94%) had penetration testing**, and a third have implemented or were planning on implementing bug bounties.

“Many developers and development teams lack sufficient incentives for pursuing security initiatives. Performance is typically measured on delivery of business features, not quality or security. A successful security culture shift requires offering the right rewards and incentives to your security champions, as well as the broader organization.”

Dustin Lehr, director, application security, Fivetran

Program timing and timelines

Key takeaways

6+ months

AppSec champions programs took six months to one year to get off the ground.

Insight: Clear charters and deployment roadmaps are needed at the start of the program and will help decrease the time to establish an effective AppSec program.



AppSec champions programs might fade away without consistent management attention and leadership.

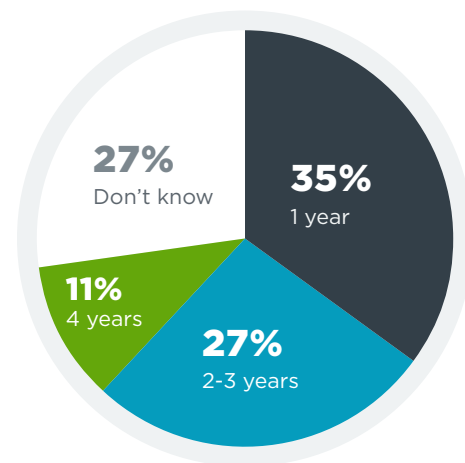
Insight: Organizations must ensure that AppSec programs are part of the team's foundation to ensure longevity and success.

Most of the champions programs take **six months to a year** to become fully functioning within development teams. This includes all aspects of program definition, recruitment, and engagement on platforms like Slack. As previously stated, the common denominator of these programs is that they originated in the centralized information security organization. Variables such as strength of organizational mandate, strategies for recruiting, and other factors likely influenced the length of time it took programs to become fully operational.

For the companies that had programs already in place, the results varied immensely from only a year (35%) to 2 to 3 years (27%), with a small group of respondents saying their program existed for more than 4 years (11%). Of note, 27% responded that they did not know. This was likely a function of staff turnover. The people who answered “don’t know” did so because the AppSec champions program was running when they arrived at their organizations.

Many respondents noted that their AppSec champions program had incurred “restarts” when key AppSec leaders departed their organizations. This was interesting as an implied pre-survey assumption was that most AppSec champions programs would always be expanding and creating deeper impacts with software development teams. So despite their organic creation, AppSec champions might go away without consistent management attention and leadership. This is an important point for managers of AppSec programs to remember.

How long has your AppSec champions program been in place?



Many respondents noted that their AppSec champions program had **incurred “restarts”** when key AppSec leaders departed their organizations.

Return on investment

Key takeaway

62%

62% of survey respondents replied that they have not been able to quantify success for their AppSec champions program.

Insight: Organizations need to establish AppSec program KPIs upfront that can be tracked and communicated to showcase clear ROI.

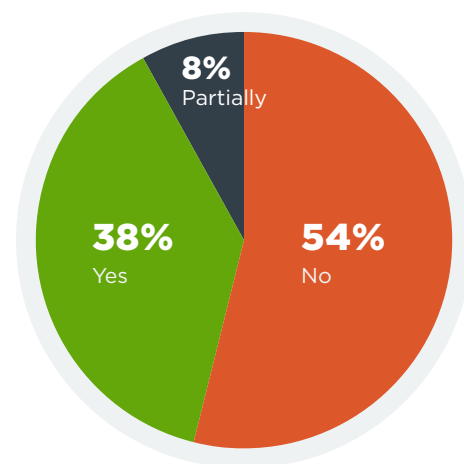
While the ROI of any security activity is highly debated, it's safe to say that at some point there will be organizational pressure to quantify successes of AppSec champions programs. Given this fact and our hypothesis surrounding the ROI of AppSec champions programs, we wanted to understand if the programs were achieving their desired outcome and if they were able to quantify success.

Forty-two percent of the survey respondents claimed they had achieved their desired outcome. The question was broad enough to encompass a variety of responses, including anecdotes shared by security leaders who participated in the survey. This response, in isolation, is mildly surprising and worthy of further analysis. On one hand, AppSec champions programs remain a relatively new phenomena within many organizations. On the other hand, in corporate environments where expenses are scrutinized, one might expect more thought would be put into explicit outcomes for AppSec champions programs.

When focused on any efforts to quantify and measure things, such as mean time to fix for application vulnerabilities or software security defect counts, most respondents replied that they had not been able to quantify the success of their program.

Although AppSec champions programs have been widely adopted, survey respondents indicate that efforts to quantify their impact within their organizations are early stage and not widely adopted. This is an area of obvious improvement, and our strong recommendation is to capture and quantify your success with an ROI model.

Are you able to quantify and measure the success of your AppSec program?



42%

of survey respondents claimed they had **met their desired outcomes** from their AppSec champions programs.

Conclusions and recommendations

This report provides interesting numbers to widely adopted security programs designed to improve development practices. Although these programs exist across multiple industries, efforts to capture emerging practices and common quantitative information have yet to occur. This report helps address that problem and encourages further quantification of a practice that continues to drive positive behaviors within software development teams.

Based on the great input from survey participants, a series of observations stood out.

Is your program built for long-term success?

- ☒ AppSec champions programs are proven to flourish with approval and support of the senior leadership team.
- ☒ Ongoing governance and clarification of roles is essential to successful AppSec programs.
- ☒ Organizations need to establish clear program objectives and measurement.
- ☒ Rewards and communication platform utilization are keys to success.
- ☒ AppSec tooling (SAST, DAST, and SCA) is a benchmark of a mature AppSec program.
- ☒ AppSec programs are found to be useful, and to ensure further growth, measuring tools must be implemented to demonstrate ROI.

More importantly, we are led to believe that these programs are having an impact in the organizations they serve. Armed with data about application security, managers can better manage software risk and further

influence software developers to write more resilient code on a recurring basis. If this occurs, then our efforts to capture data around AppSec champions will not have been in vain.



About Coalfire

The world's leading organizations – the top 5 cloud service providers; 8 of the top 10 SaaS businesses; and 3 of the top 5 in financial services, healthcare, and retail – trust Coalfire to elevate their cyber programs and secure the future of their business. As the largest global firm dedicated to cybersecurity, Coalfire delivers a full lifecycle of solutions through professional services, managed services, and technology platforms to help our clients solve their toughest cyber challenges. With more than 20 years of proven cybersecurity leadership, Coalfire combines extensive cloud expertise, industry knowledge, and innovative approaches to fuel success.

Get started building your AppSec champion program today.

877-224-8077 | [Coalfire.com](https://coalfire.com)



Copyright © 2022 Coalfire. All rights reserved. The information in this document is subject to change at any time based on revisions to applicable regulations and standards. Any forward looking statements are not predictions and are subject to change without notice. Coalfire is not responsible for any errors or omissions.

RR_AppSecChampions_03292022