ZERONORTH™

Security Champions:
Empowering Heroes to Unite Security and DevOps

A ZeroNorth Survey | October 2020

Security Champions:

Empowering Heroes to Unite Security and DevOps

As companies embrace DevOps, the speed of software delivery increases dramatically. With development teams and pipelines spun up as necessary across an organization – and granted the autonomy to deliver capabilities aligned with business and product line objectives – the notion of centralized control fades away.

As greater focus turns to the security of applications, these DevOps teams are tasked with taking on associated security responsibilities. That said, developers often lack the knowledge, experience and security tools they need to make effective security decisions, which can create a rift across Security and DevOps teams. As a Ponemon Research report recently showed, the vast majority of developers find it difficult to work with AppSec, and vice versa. Even more troubling than the cultural conflict is evidence of deeper issues: 71% of AppSec professionals say security is undermined by developers who don't care about the need to secure applications early in the software development life cycle (SDLC).

If these are the realities of DevOps and AppSec today, the questions become:

- How can Chief Information Security Officers (CISOs) and Corporate Security teams help developers better understand the security, risk and compliance objectives of the organization?
- What is the role of Corporate Security in enabling developers to better address security across their pipelines?
- What programs can help unite the efforts of DevOps and Security to ensure software capabilities meet the velocity and quality goals of the business while still addressing the security, risk and compliance requirements of the CISO?

This is where the notion of a Security Champions program was born. In an effort to better prepare DevOps and shore up application security (AppSec), companies often enlist a team member to champion these initiatives, working to embed a culture of security across development. A bridge-building role if there every was one, these Security Champions focus intently on uniting groups who are often at odds, all for the betterment of secure software development.

As a company focused on uniting security, DevOps and business teams for the good of software, ZeroNorth® believes these programs have the potential to greatly improve the success of any AppSec initiative. With this in mind, we surveyed 99 security and development professionals to learn about the state of these programs and where success is being seen.

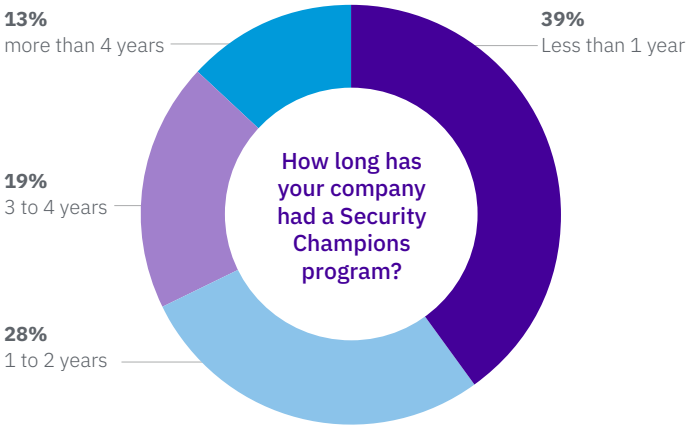
The report shares several significant takeaways, including:

- **Security Champions have the power to improve AppSec:** These professionals are viewed as successfully enabling the improvement of application security, with the unique ability to build better relationships between Security and DevOps organizations – 84% of those surveyed agree or strongly agree.
- **A passion for security gives strength to a Security Champion:** From Engineering to Security Architecture to Product Management, Security Champions originate from a broad range of positions. But the #1 characteristic of a successful Security Champion – named by 50% of those surveyed – was that these individuals have an interest in security.
- **Security Champions are a unifying force:** These individuals have the power to bring Security, DevOps and business/product teams together with the goal of improving software security. On that note, these programs must have top down support, across both the Security and Engineering leadership functions. Fifty-six percent of respondents said Corporate Security leadership was a top requirement for the success of a Security Champion; 47% said Engineering leadership support.
- **Corporate Security teams are vital to the success of Security Champions programs:** Active support by the CISO and other Corporate Security leaders is critical, and corporate teams also play an important enablement role, from defining security priorities (57%) to training on best practices (47%) to consulting on security issues (39%) to providing access to security tools, such as security scanning technologies (38%).

State of Security Champions

While the notion of a Security Champions program has been around for years, our survey illustrates how the majority of programs are relatively young. Thirty-nine percent have existed for less than a year; another 28% have been in place for 1-2 years.

The data tells us it's still early days for many companies looking to roll out these programs more broadly. While only about one quarter (27%) have a formalized plan across and products and/or teams, nearly half (46%) say they have seen initial implementation across select products and/or teams. And 26% say the program has been formalized across select products and/or teams.



Flexing their Muscle: Security Champions Bolster AppSec

Yes, frameworks for establishing a Security Champions program are important to understand, but the results are what really matter. Across the board, ZeroNorth's research highlights how these programs have improved the state of AppSec in a variety of categories.

First and foremost, Security Champions have the power to successfully strengthen relationships between Security and Development teams. In fact, 84% "agree" or "strongly agree." This role of uniting Security and DevOps is a critical one, as proper alignment ensures goals, frameworks and strategies for improving software security are commonly understood.

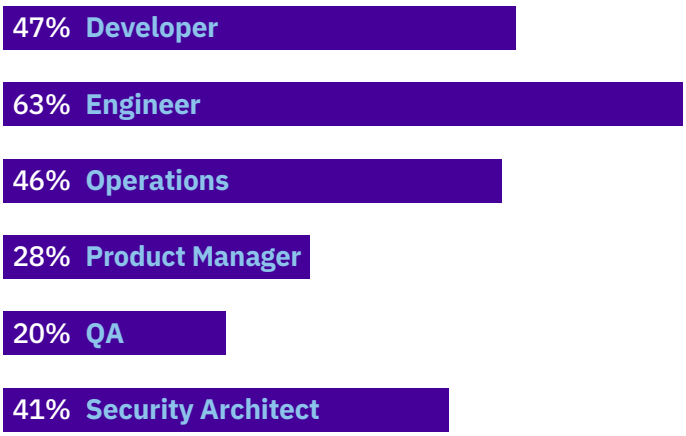
Beyond this, 78% said such security programs have strengthened the related skills and knowledge of developers, while 77% felt the company's overall AppSec posture actually improved. The most significant unknown – where time will tell – revolves around how well Security Champions programs can help organizations successfully scale their AppSec initiatives. Here, 32% were undecided, while 61% already believed this to be true.

	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
My company's Security Champions program has improved our AppSec posture	24%	53%	19%	2%	1%
My company's Security Champions program has strengthened our developers' security skills and knowledge	20%	58%	19%	1%	1%
My company's Security Champions program has strengthened relationships between Security and Dev teams	26%	58%	13%	1%	1%
My company's Security Champions program has enabled us to effectively scale AppSec	20%	41%	32%	5%	1%
My company's Security Champions program has improved our security culture	32%	49%	17%	0%	1%

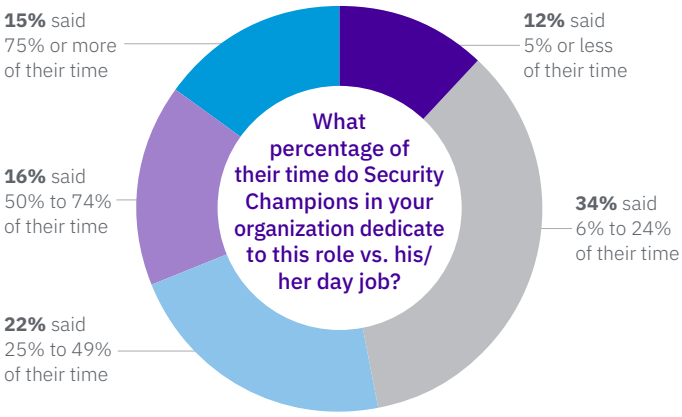
Recruiting a Roster of AppSec Heroes

It's generally understood that individuals coming from a wide variety of roles may be selected as a Security Champion, and ZeroNorth's survey supports this position. While those in development or engineering roles were most often designated as a Security Champion (47% and 63% respectively), those in Operations and Security Architecture roles were each named more than 40% of the time.

Which of the following roles have been designated a Security Champion in your organization?
(multiple answers accepted)



Security Champions are rarely assigned full-time responsibility for this role, which means it's a part-time effort on top of one's day job. Our survey demonstrates great disparities in the amount of time allotted to this security role:



Under the Cape: What Makes a Great Security Champion

Given the diverse set of roles and experiences that may lead someone down the path of becoming a Security Champion, we thought it important to take a step back and ask, "What skills and characteristics set up a Security Champion for success?"

The survey uncovered an interesting insight: softer skills lead the pack in terms of what creates a framework for success, as 50% said "interest in security" was tops, while 45% said "communication skills." About one third named "collaboration," "proactive" or "diverse set of engineering and security skills." Twenty-four percent of respondents indicated hands-on experience with security scanning tools, leadership skills and threat modeling skills as important.

Motivating Your Heroes: Keeping Your Security Champions Engaged

Once you've brought Security Champions on board, the question of continued motivation is key. Remember, this is a part-time role on top of regular work responsibilities, so finding ways to keep these committed professionals engaged will also be critical to the program's long term success.

As part of this study, we investigated the actions companies take to motivate Security Champions and found, interestingly enough, that benefits focusing on the long-term growth and development of an employee far outweighed compensation-related benefits.

Specifically, 76% of respondents said training and development was the motivator, while 55% cited career growth—and 50% named professional certifications. On the other hand, only 21%, 12%, 7% and 5% said their motivations were based performance bonuses, salary increases, stock awards and paid time off, respectively.

The Devil's in the Details: The Role of the Security Champion

Like any job or role, Security Champions need to understand the scope and responsibilities of their unique position. Otherwise, these individuals are flying blind and establishing a focus based on guesswork.

What are the Top Three Responsibilities of a Security Champion in Your Organization?

(limit of three answers)

Promote AppSec best practices	41%
Advocate for security within the development team	40%
Promote adoption of security standards	35%
Promote adoption of AppSec tools by Developers (e.g., security scanning)	32%
Elevate priority issues to Corporate Security	25%
Consult on security scan test results	20%
Communicate with Corporate Security on AppSec program status	20%
Provide formal developer training	17%
Execute threat modeling	15%
Mentor developers	15%
Consult on proposed remediation	14%
Execute security scans	14%
Assist with QA & testing	6%

As part of this study, we asked respondents to identify the top three responsibilities of a Security Champion in the organization. Promoting AppSec best practices and advocating for security within development were most often named (by 41 and 40%, respectively). Thirty-five percent believed promoting the adoption of security standards was a leading responsibility, followed by 32% who said promotion of AppSec tools by developers, such as security scanning technology.

Arming our Heroes: Paving the Way for Success

Given the diverse nature of a Security Champion's work, including the varying attitudes among team members, it's important to understand what will create the greatest likelihood of success.

Fifty-six percent of respondents felt "active support by Corporate Security leadership" was the main priority when setting up a Security Champion for success. Forty-seven percent said "active support by Engineering" leadership was a top requirement. Where Champions are concerned, these data show the criticality of alignment across Security and Engineering, including the opportunity to help build bridges across the divide.

What are the Top Three Requirements for Ensuring the Success of a Security Champion?

(limit of three answers)

Active support by Corporate Security leadership	56%
Active support by Engineering leadership	47%
Key success metrics defined	41%
Active support of Business Unit/ Product Line leadership	40%
Responsibilities defined	39%
Buy-in from the Security Champion's direct manager	37%
Protect Security Champion against potential conflicts-of-interest	31%

Often, corporate security teams are the driving forces behind establishing a Security Champions program. These are the people and teams focused on helping to drive a culture of security, and building the bridges that enable secure DevOps. This means the responsibilities of Corporate Security must be clear.

What are the Top Three Responsibilities of the Corporate Security Team in Enabling Security Champions?

(limit of three answers)

Defining security priorities	57%
Training on best practices	47%
Ongoing consulting on security issues	39%
Access to security tools (e.g., scan tools)	38%
Evangelizing the Security Champion program	35%
Training on how security reviews are conducted	28%
Training on how the company assesses risk	28%
Ongoing mentorship	24%

The number one responsibility for Corporate Security in enabling Security Champions is defining security priorities (57%), according to our survey. Forty-seven percent said, "training on best practices," while 39% said "ongoing consulting on security issues." And 38% of respondents believe it's Corporate Security's responsibility to provide access to security tools (e.g., security scanning tools).

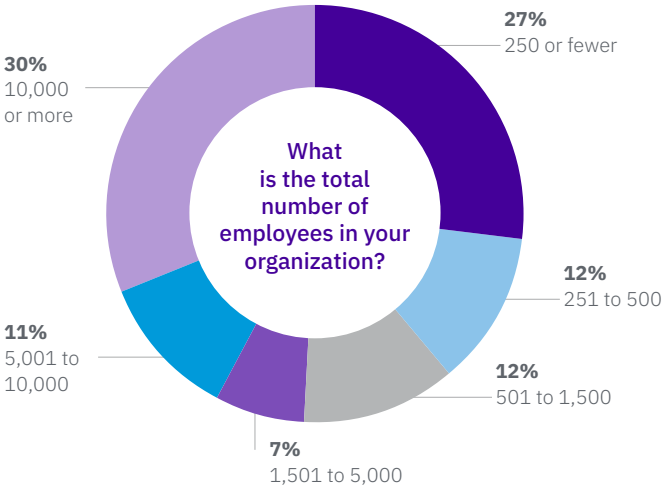
What's Next? Security Champions – Activate!

It is clear from this study that there is a need to better unite security, DevOps and business/product lines in order to bolster application security. Security Champions have a key role in furthering these objectives. With sponsorship and support from the CISO – and armed by Corporate Security with the training, best practices and security tools necessary – Security Champions can be the hero our business and product lines need, and help developers meet their goals while supporting the security, risk and compliance requirements of the organization.

Survey Methodology

ZeroNorth's study was conducted via an online survey fielded between September 11-25, 2020. All survey respondents were aware of the status of a Security Champions program, and all were knowledgeable about the program itself.

Ninety-nine individuals participated in the study; 23 were in AppSec roles; 39 in Corporate/IT Security roles. Others represented included consultants (11), Developers and Engineers (8), IT Operations (6), Software Architects (7) and Product Security (5). Twenty-seven percent came from organizations with fewer than 250 employees; 24% were between 251-1500 employees; 48% were from companies with more than 1500 employees.



ZERONORTH™ ZeroNorth brings security, DevOps and the business together to improve application security performance and reduce organizational risk. The company's application security automation and orchestration platform unites enterprises to rapidly identify, prioritize and remove the vulnerabilities standing in the way of software excellence. In an age where the security of applications needs to be everyone's responsibility, ZeroNorth is where organizations come together for the good of software. For more information, follow ZeroNorth on Twitter (@ ZeroNorthSec), or LinkedIn—or visit www.zeronorth.io