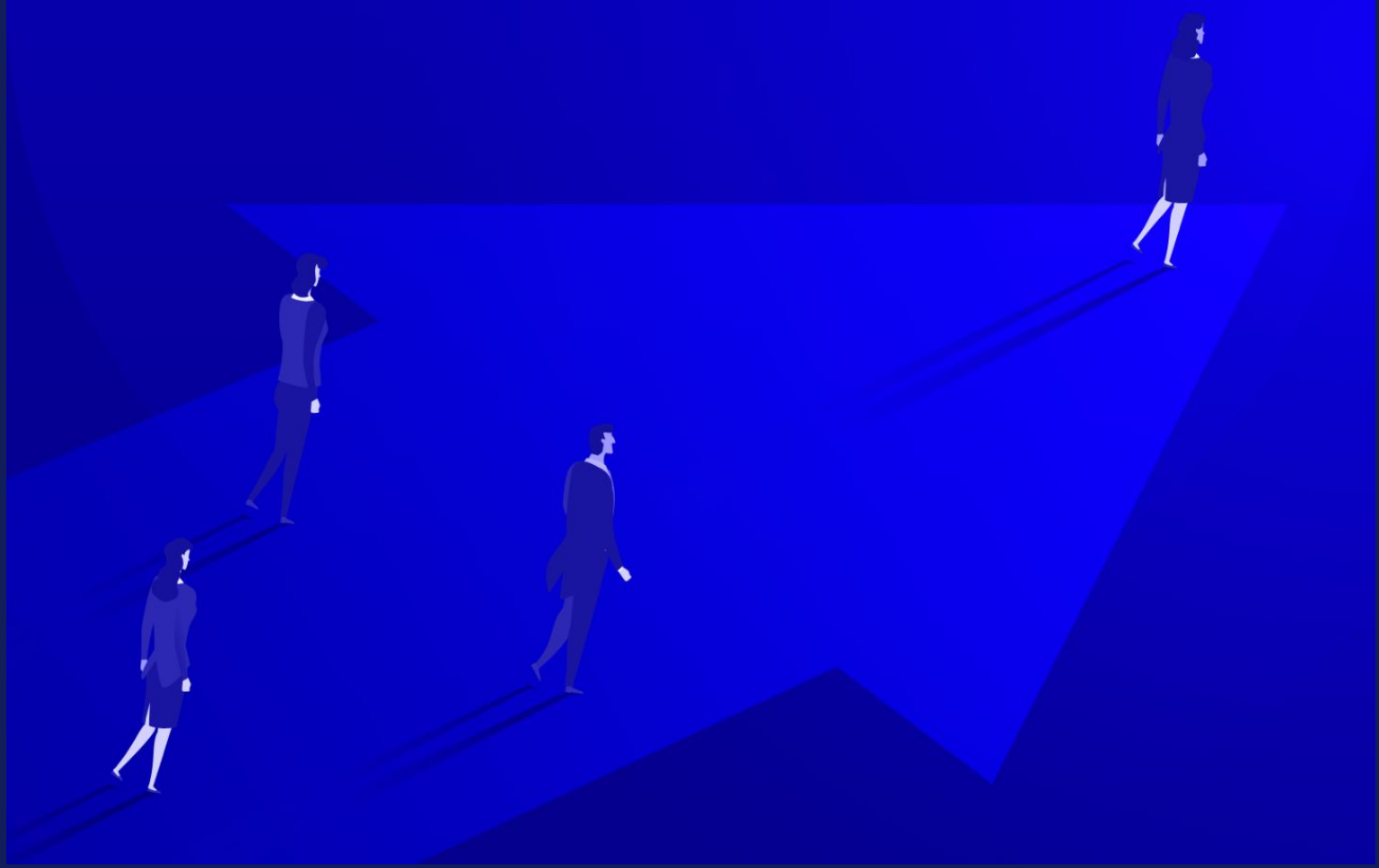
APPSEC engineer

by

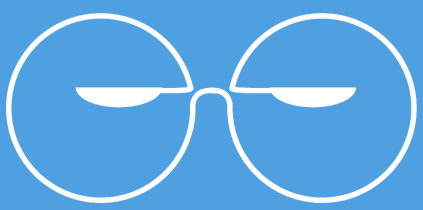
THE ULTIMATE GUIDE TO

Building Security Champions



CONTENTS

Introduction



For years now, companies have grown accustomed to the idea of siloed teams performing tasks independent of each other. It's a comfortable, familiar idea: the assembly line method was the backbone of the Industrial Revolution, and makes sense for a lot of manufacturing businesses. Each part of the assembly line is responsible for one thing, and one thing only. As long as they did their job on time, the next section could continue the job seamlessly, over and over until the product was fully assembled.

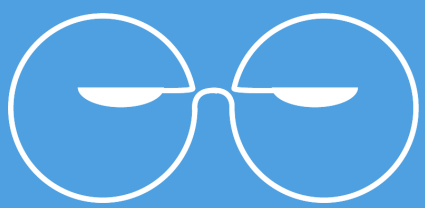
Except, that concept doesn't really work with modern-day software pipelines. It's not just that every new build of the application need to be tested for bugs and fixed before release. Engineering teams have now realised that, rather than mindlessly fixing security bugs reported by the security team, it's far more efficient in the long run to make systemic changes to the way they build software.

This means taking a preventive (rather than curative) approach that combines several security activities—DevSecOps, Threat Modeling, Security Architecture, etc.—to build *systems* that address the problem of AppSec as a whole, not just individual vulnerabilities. Therein lies the challenge: how do you align multiple teams, each with different roles and priorities, to the same goal? More importantly, how do you get them to collaborate in a way that doesn't end up slowing down the software development cycle?

In recent years, companies have found an innovative solution to this problem: Security Champions. But who exactly are champions? How are they valuable to your engineering teams? And crucially, how do you nurture security champions at your own organisation?

These are the questions we'll be answering in the *Ultimate Guide to Building Security Champions*. At the end of this ebook, you'll come away with solid, actionable steps on how to plan and execute your very own security champions program.

Why do we need Security Champions?



To really understand why security champions are needed, it's important to recognise a fundamental truth of most engineering teams — security isn't a top priority for developers. This isn't a knock on developers; most organisations simply haven't built a culture that places much importance on securing their software.

Security isn't about checking off items on a vulnerability
checklist. It's a conscious, ongoing effort to observe the behaviour of your application, understand how users interact with it, and create strategies to deal with unwanted outcomes. Everything from access control, to network security, to automated testing form part of this overarching playbook to build a higher quality software product.

A security champion plays a key role in enabling all of these activities. A well-functioning champions program is one of the best signs of a mature AppSec posture because it means the developers have the skills to build software that's secure by default.

What does a Security Champion do?

Security Champions are members of the engineering team who take a special interest in security. They're typically a developer who has significant experience working on their current product, and is familiar with the technical aspects of the project. But a potential champion isn't just any old developer on the team — they need to be specifically motivated with an interest in security.

It's a champion's responsibility to push AppSec initiatives within the engineering team, teach security principles to their fellow devs, and bridge the communication gap between the engineering and security teams. They help both teams collaborate, share knowledge, and advocate for security with their developer colleagues.

Why can't a security engineer do this?

It would seem like a member of the security is ideally suited to the role of security champion, given their skills in AppSec. But it's not quite so simple.

It's relatively straightforward to train developers in the principles of security — they're the ones who built the software, so they know best where the bugs, deficiencies, and loopholes lie. They can directly implement security knowledge while coding the software.

Teaching a security engineer how the app is built, on the other hand, is much more difficult, since they're never actually interacting with the code. They won't be able to offer any useful insight into what parts of the development process need to change.

Moreover, a security engineer doesn't speak the same language as a developer, so collaborating and sharing knowledge with the engineering team would be exponentially harder

A potential champion isn't just any old developer on the team — they need to be specifically motivated with an interest in security.

Benefits of having a Security Champion

The biggest incentive to build security champions is to level the playing field between engineering and security. For context, the ratio of developers to security professionals is roughly 135 to 1. To say that there's a shortage of security talent out there is a tragic understatement.

But having a security champion (or *champions*) on your team confers several tangible benefits on your development process:

Central point of contact for security issues

Engineering and security teams sometimes struggle to communicate because of knowledge barriers — developers don't know security, and security folks don't understand software dev. Champions who are trained in AppSec can serve as the security team's point of contact with engineering, and explain security issues to developers in a way they can easily understand.

Reduced demand on security experts

Security teams are already facing a talent shortage as it is, stretching thin their existing time and resources to complete basic security tasks. Champions help bolster efforts from the developers' side by cultivating a pro-security mindset within the engineering team. This reduces the overall burden on the security folks, who can spend more time planning long-term security strategy and not be stuck in daily firefighting.

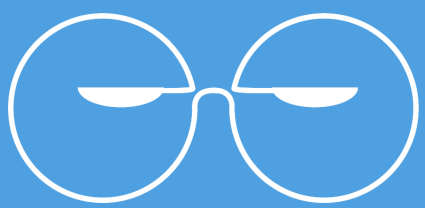
Faster identification and remediation of vulnerabilities

Developers typically have to rely on security testing in order to find vulnerabilities in their product, which can take time. A champion trained in security is capable of spotting some of the more obvious or serious security issues very early on, ensuring the vulnerability doesn't become widespread or cause serious damage to the product.

Training other developers in secure coding practices

Even if a security engineer were to train developers in security, secure coding probably isn't something they'll have the expertise to teach. In such cases, a security champion can take over. With their combined knowledge of security principles and code, they can teach their fellow developers to write code that's secure by default.

How to Get Management Approval for a Champions Program?



Before we get into how you can start your own security champion program, we need to address the elephant in the room — management. It's not always easy to get company executives to see the value in an initiative that doesn't have an immediate business impact. But it's also extremely important to get executive approval for a champion program for two reasons: time and resources.

A security champion needs to have the time to take security training and implement new practices in their role as developer. This means taking time away from their primary role — otherwise, the champion will burn out from too much extra work.

Your organisation will also need to provide resources for you to conduct security training, plan events like CTFs and hackathons, and even build an internal security champion 'brand' (more on that later). Without a formal thumbs-up from management, champions will be doing all this work as extra in their own time, and won't be compensated for it. Not a good situation if you want your champion program to last more than 2 months.

A champions program will increase the overall security skill level of your whole product team, making it possible for them to take on complex new projects with advanced security requirements. Not only that, security assurance helps build trust with your customers, which allows you to land bigger, multi-year contracts with them.

Beyond that, security champions will help your company grow their resources without increasing headcount. A developer will be far more valuable if they're also able to perform crucial security tasks, avoiding the need to hire a dedicated security expert.

If you can get upper management to see the potential return on investment of supporting this new initiative, they'll be more likely to take an active interest in helping you build your security champion program.

How to pitch your Security Champion program

If you don't clearly communicate the *what* and *why* of your champion program, management won't feel incentivised to greenlight the project. Here are some things you can do to get executive buy-in at your organisation:

Make the business case

Many companies—particularly the larger ones—have strict requirements for software security. In 2021, the White House released an order mandating that all vendors who work with the US Government need to have thoroughly secured their software supply chain. If your team doesn't have the resources or skills to meet security demands like this, they're losing out on massive contracts and business deals.

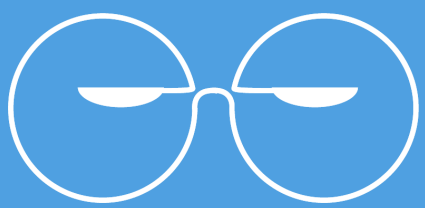
Ask a higher-up to be the Executive Sponsor for the program

Not everyone in management may be as excited about security champions as you are. That's why it can help to seek out an individual who's showing more interest and ask them to partner with you as an executive sponsor for the new program. This person can be someone who helps you get the resources or approvals you need, helps with decision-making, and is your point of contact within management at your company.

It's useful to have a dedicated sponsor to look out for the interests of the champion program, since they can act as an advocate for your efforts and help channel resources to things that need the most attention.

Security assurance helps build trust with your customers, which allows you to land bigger, multi-year contracts with them.

What Skills does a Security Champion need?



As a member of the engineering team, a security champion needs to have skills that directly complement their primary role as developer. They don't need to be an encyclopaedic source of security knowledge — rather, they have a highly focused set of skills that pertain to security issues that affect their team's work.

If your organisation has multiple teams in charge of different products or aspects of development, they each need to have champions who are trained in the security skills relevant to their work. If a team is working on cloud-native infrastructure, your champions' training needs to focus on cloud-native security, containers, APIs, etc.

But simply assigning courses to your champion isn't enough — you need to guide them through their learning so they can graduate from AppSec novice to guru over time. This requires looking at their learning progress as 'levels' of security proficiency.

4 levels of skill for Security Champions

Level 1: Completed awareness training

This is where a champion begins their journey — awareness. At this level, they're still learning about the potential threats to an application and how vulnerabilities impact software.

Level 1 is where champions learn the 'what' and 'why' of security, but not the 'how'. Awareness training covers all the essentials of AppSec, from terminologies to basic concepts, common vulnerabilities, and more.

Level 2: Completed training in general topics

Now that your champion is more familiar with security, it's time to up the ante. In Level 2, champions will start to learn topics they can actively implement in their real-world workflows. 'General' security topics for champions include:

- Secure coding practices
- Code review
- Common classes of vulnerability
- Offensive security assessments
- Threat modeling
- Incident response
- How to fix bugs they find

Note that it's not recommended to train your champions in all of these topics all at once, as that will almost certainly overwhelm them. Training should be staggered over a period of months so they can assimilate what they're learning and develop a baseline of knowledge, regardless of what product they're developing.

Level 3: Completed platform-specific training

This is where training for champions will need to be differentiated. Teams working on different projects are likely using a variety of platforms, languages, cloud providers, etc. Each champion needs to have skills relevant to their specific tech stack — skills which go way deeper than any general training.

For example, a developer using Python to build containers in AWS needs security skills that reflect all three: secure coding in Python, container security, and AWS security.

To cover the full breadth of skills you need, the training has to offer a diverse library of courses and labs. Learn more by checking out the course catalogue for AppSecEngineer.

Level 4: 6+ months of being a Security Champion

The only way to evaluate the skills of a security champion is to have them *just be* a champion for the better part of a year and execute on their security goals. They need to gain experience and meet their KPI targets. They need to work with the security team, understand where the weaknesses in their product lie, and actively work towards fixing them. Over time, you should be able to see a champions' positive influence within the engineering team, and ultimately, the software they develop.

Champions need defensive security

Most security training and knowledge we encounter comes from an offensive perspective: how can we find vulnerabilities? How does a hacker compromise the system? How do we break the application?

This is important, of course — you can't build secure apps without first identifying the weak points.

But focusing purely on the 'Attack' point of view ignores the entire other half of the equation: defensive security.

Once you find out where the vulnerabilities come from, your developers need to know how to fix these vulnerabilities. There are 3 lines of defence in defensive security:

- Prevention
- Detection
- Mitigation & incident response

If you can stop the attack from ever happening, that's the best option. For example, writing secure code, or testing your app and fixing bugs before it goes into production can entirely prevent certain attacks.

But it's not possible to eliminate 100% of bugs. Which is why you need to set up logging and monitoring systems that can detect suspicious or malicious activity and report it. If an attack is underway, your team will be alerted.

Which brings us to the final line of defence: incident response. Using the information from the alert, your team can find the source of the attack and shut it down, stopping it from doing any further damage.

Combining all 3 of these skills is essential for your team of security champions, especially at a high level. Not every champion will get training in all of these skills, of course, but it's important to ensure your teams have a balanced distribution of defensive and offensive security skills to tackle any challenge that comes their way.

What should training for your Champions look like?

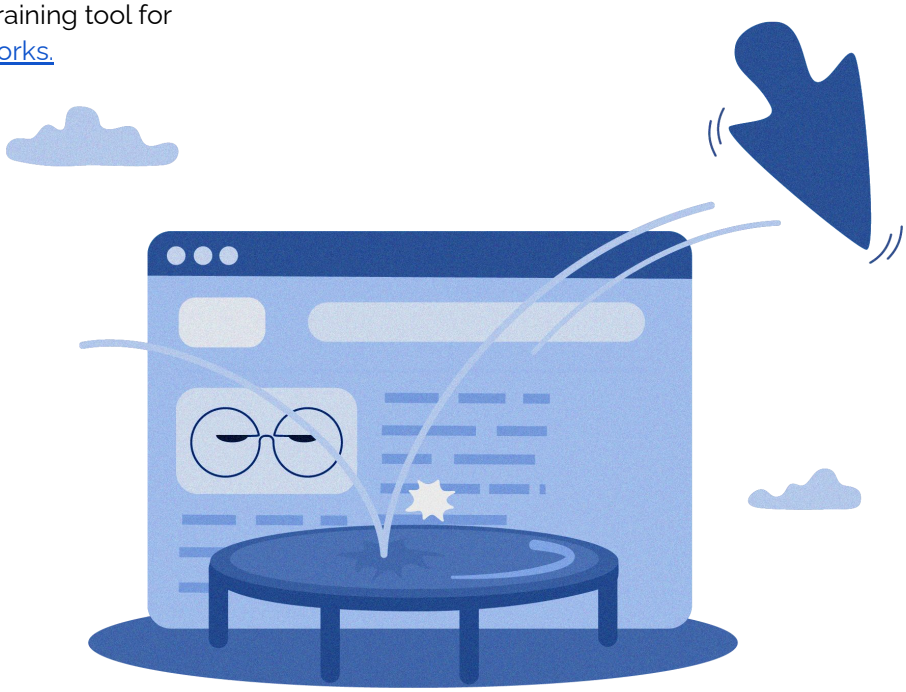
When considering training for anyone on your team—not just security champions—it's important to note that learning is always a continuous process. No matter how well-trained your team is today, innovations in tech are so rapid that you're almost certainly lagging behind if you're not updating your skills every few months.

Training shouldn't be a gruelling, multi-day slog where you burn through years' worth of material in a matter of days. Self-paced learning is often the best option, where employees can take lessons at their own pace — especially since not everyone learns at the same rate.

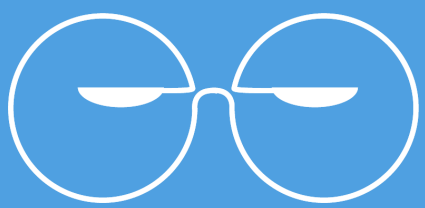
This strategy should be coupled with hands-on learning, which is by far the most effective way of training your team. Not only do hands-on learners retain more information, they also gain real-world skills that they can use at work.

This combined strategy is what makes AppSecEngineer such a compelling training tool for security champions. Learn how this works.

Training shouldn't be a gruelling, multi-day slog where you burn through years' worth of material in a matter of days.



How to Recruit Security Champions?



Recruiting for the position of security champion isn't as straightforward as hiring for a regular job. Your champions will mostly be volunteers, so unless upper management is agreeing to offer monetary compensation (which they likely won't until they see results), you need to be able to convince key members of the engineering team to take up the mantle.

Note that a security champion's responsibilities will NOT be in addition to their usual tasks as a developer. They will have to devote 20 - 30% of their normal work-hours to security activities and training. This is why it's so important to get corporate approval for the security champions program — you don't want to either burn out your champions, or have management shut it down because it's taking up too much of your developers' time.

When you start your brand-new champions program, you're very likely not going to get a lot of enthusiastic responses from the team. You'll need to find and persuade the right people for the job, and that may take some work. Here are 3 important things you need to do:

- Find developers who are interested in security
- Clearly communicate the specifics of the role
- Persuade them with rewards and growth opportunities

Let's go over these three steps in detail.

How to find developers who are passionate about security

Your security champions are going to be volunteers, so don't go in expecting people to line up for the role. You'll need to identify specific individuals who show a marked interest in security activities, and approach them to be your next champion.

Host security talks and events

This kills two birds with one stone — you not only educate your developers on security, but you also get a chance to see who's most involved. Who's asking the most questions? Who's trying to implement what they've learned, or being extra proactive about security? These people might just be potential champion material.

Send out emails to the team

Tell them what a security champion is, what they'll need to do, and show them how they stand to benefit through opportunities and training. Make sure they understand this isn't an extra burden they'd have to bear apart from their main job.

Just approach them and ask

Perhaps a more appropriate word would be...beg? But seriously, sometimes the most effective route is the most direct. Ask your developers if they'd like to be a part of the new program, explain the details to them, and try to persuade them on the benefits. At this early stage, finding your first few champions is bound to be a difficult exercise, but don't give up!

Persuade them with rewards and opportunities

Security champions are, of course, volunteers, and you need to keep your volunteers interested in sticking around with useful rewards. Here are some of the biggest ways champions will see immediate benefits:

Champions get security training

Employees place immense value in quality training and professional development. In fact, the two biggest barriers to training are that employees have too little time, and companies have budget constraints. But if the program is approved, your security champions will have both. They're getting a golden opportunity to upskill and advance their careers.

Champions get to attend and speak at events

Security champions (once fully trained) are in the unique position of having skills in both security and software development, which just so happens to be a killer combo. Their perspective will be highly valued at security events, where an experienced champion might even get the chance to deliver talks and be recognised for their work.

Champions can advance their career quickly

As we noted earlier, security champions have a unique set of skills. This means they have more options to advance their career, either vertically in software development or horizontally, switching to a full-time role in application security. They'll also get recognition from upper management.

Bonus tip #1: Build a brand for your Security Champions

Here's a fun idea that you can use to spice up your champions program, courtesy of Christopher Romeo, CEO of Security Journey. This may not be something you can do at the start of the program, but can help give your crack-team of champions a sense of team camaraderie.

And that idea is: build a brand around your security champions. Design a logo or mascot to represent the program and distribute swag to all your champions. It could be t-shirts featuring your new mascot, or a coffee mug with a cheesy tagline, or even colourful stickers.

The idea behind building a brand is to give the champions program a sense of identity within the company (since champions may come from different teams). The program's successes and achievement can be attributed to the brand, and it serves as a reward mechanism for your champions. It also acts as an advertisement to attract new people interested in joining your little 'club'.

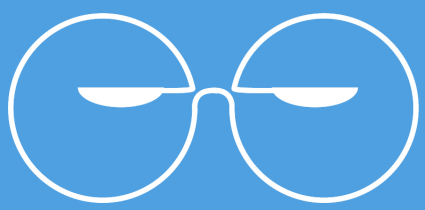
Bonus tip #2: Ask them to opt-in for a full year, every year

Rather than asking your new recruits to volunteer for some unspecified period of time, ask them to opt-in for a full year. This means that once they're in, they have to complete the full year of being security champion.

This stops a non-serious applicant dropping out of the program after a few months, and they get to experience one full year of training and security activities. After the first year, they're automatically 'out' of the program, and have to opt back in if they want to continue as champion.

Your champions will take their role more seriously as a result, but also not feel pressured to keep going after a year if they're not interested.

How to Train Security Champions?



This is it. This, right here, is the fiery crucible from whence true masters are forged. Where mere 'developers' become 'Security Champions'. Once you cross the Rubicon, there's no turning back.
Unless of course your devs decide the training sucks and they're done with your program.

The problem with training your team is that you can't just make them follow any old training program and expect results. There are a few roadblocks you need to cross in order to achieve a learning cycle that sticks, and yields positive results over time. That means answering these 3 questions:

- Is the training relevant to what your developers are doing?
- How is the training going to be designed and delivered?
- Will you be able to evaluate a learner's progress?

These questions, in broad strokes, cover each stage of your champions' learning process. Depending on how you answer them, you can determine whether they will stick with the training, gain something useful from it, and demonstrate their skills. Let's look at the ideal answers for all 3 questions.

Only teach security champions what they need to know

A lot of trainings tend to make this common mistake: creating a general-purpose, 'one size fits all' program that has a moderate level of utility for all learners on the team.

Imagine trying to market a lawn mower to literally everyone: suburban homeowners, city apartment residents, college students, artists, tech professionals, lawyers, etc. Sure, you might technically be reaching a lot more people than ever, but if most of them are going to ignore your product, what's the point? You want to specifically target your ideal market — those suburban homeowners

Security training for your champions needs to be like targeted advertising: narrow and deep, not wide and shallow. Ask yourself this question — will your learners have a real-world use for their new skills in the next month or so? If the answer is no, they might not need to learn it at all.

This helps you focus your training efforts on skills that actually matter, not waste your champions' time on skills they'll never have use for. Moreover, irrelevant training only serves to bore the learner, making them less engaged and receptive for trainings in the future. But if they find the training genuinely useful, they'll be more motivated to continue learning.

Training is best done hands-on

It's no secret that most people don't like corporate training. It's not that they don't want it — surveys have shown that 84% of workers are willing to change jobs if their new employers offer learning opportunities.

The simple fact is that most company training programs suck. They tend to take the form of boring lectures where learners stare at Powerpoints and take notes for 3 hours.

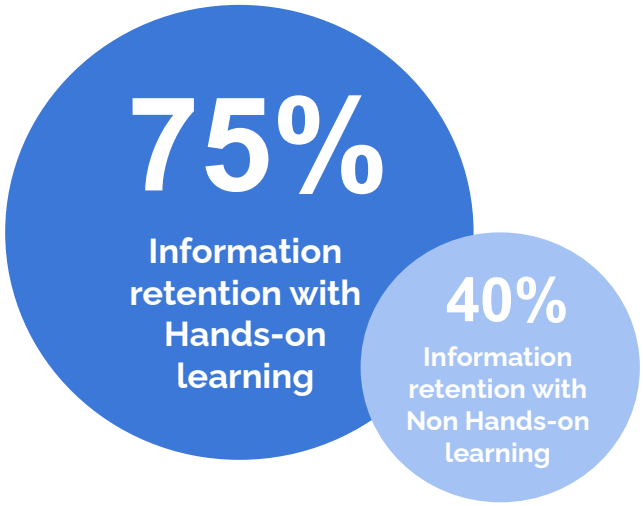
There's very little engagement or interaction going on, and learners don't actually absorb or retain 50-60% of what they're taught. It's a waste of time for both the employees and your company.

Contrast that with hands-on training: learners need to solve problems using practical lab exercises. They need to actually implement their newly learned skills by hand, thereby getting a feel for how the skill will translate to a real-world setting.

This makes learning much more fun, mentally engaging, and has been shown to increase information retention by as much as 75%. In a field like application security, hands-on experience is vital to understand how, for example, you should configure access management policies in AWS to minimise the risk of privilege escalation.

For security champions, the most important requirement is to acquire new security skills as quickly and efficiently as possible, and put those skills to use right away. No academic mumbo-jumbo, no unnecessary theoretical knowledge required (at least at first).

Find out how AppSecEngineer uses world-class hands-on labs to train teams in everything from DevSecOps, to Cloud Security, to Secure Coding, and more.



Champions need to be regularly evaluated

You can have your champions take all the training programs you want, but how can you be totally sure they're actually learning something? With evaluations, of course!

Evaluations can take many forms, but they essentially boil down to the same thing: providing solid proof that the champions have learned crucial security skills. There are 2 main ways you can conduct an evaluation:

Solving CTF-style challenges

This type of challenge is useful for testing your champions on highly specific skills by making them solve various problems in the style of a CTF or hackathon. For example, you could show them the source code of deliberately insecure application, and ask them to find all the vulnerabilities and fix them.

These challenges can work like standardised testing: whenever your champions have finished a particular set of courses or training programs, you can test their knowledge before they get to the next 'level'.

AppSecEngineer has a new Challenges feature, with hundreds of CTF-style test scenarios where you have to go hands-on to solve real-world problems in AWS, Kubernetes, Python, Java, Go, and more.

Secure code reviews

This is an important one to do on a regular basis. A champion's primary skill will be in secure coding, so it's important to ensure they're following through on that in their role as developer.

Perform regular secure code reviews to determine the flaw density in their code, ie., number of confirmed bugs found in an application during the period of development, divided by the size of the software.

These code reviews can be part of specified milestones or KPI targets you set for your team. Champions who get positive results in these evaluations can even be rewarded for their efforts with certificates, encouraging emails, public recognition, etc.

Divide your champions into 4 skill levels

As we discussed in the third chapter of this ebook, OWASP recommends dividing your security champions program into 4 levels of security competency. Here are the 4 levels, as a quick reminder:

- Level 1: Completed mandatory awareness training
- Level 2: Completed general topics training
- Level 3: Completed platform-specific training
- Level 4: 6+ months of being a Security Champion

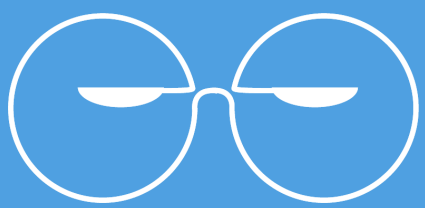
Each new champion who enters your program will have to go through this 'gauntlet' of training and performing security tasks, growing their skill levels gradually.

Formalise the training curriculum for each level, and make sure to keep it up-to-date with new advancements and changes at your company. At Levels 2 or 3, you might need to give different trainings to champions from different teams — they won't all be working on the same project, after all.

To formally advance a champion from one level to the next, you should evaluate their skills through hands-on challenges. A champion who successfully graduates to the next level can be rewarded with certificates, swag (t-shirts, stickers, coffee mugs), and commendations.

Evaluate champions' learning levels with [Assessments on AppSecEngineer.]

How to Motivate & Engage Security Champions?



Read the title of this chapter as 'How to Keep Your Champions Program Alive'.

Of all the aspects of a security champions program, the most deceptively hard things to do is keep the whole thing running smoothly. This might not sound like a challenge once you've gotten your recruitment and training in order, but consistent implementation is what can make or break your shiny new program.

No matter how carefully you plan every little detail, you still can't account for the biggest source of unpredictability in all this: the security champions themselves.

Even if you find developers who seem perfect for the role, even if you get them the best possible security training money can buy, you still need to motivated and engage them. After all, they're volunteering to be champions, which makes it hard to enforce anything on them.

Instead, the best way to keep your champions from burning out or growing bored is to encourage, reward, and actively support them in their journey. Let's understand how we can go about doing that in the workplace.

Keep your champions engaged

Training is just one aspect of your interactions with security champions. But you're not always trying to get them to learn new skills — that just leads to monotony and boredom. It's important to nurture your champions' passion for security in other ways, and keep the momentum of the program. Here are some ideas to get your champions more engaged and motivated.

Tournaments & contests

Host a hackathon or capture-the-flag (CTF) event in your company and have your champions take part. You can involve people from all teams and projects, giving the champions a chance to get to know many more of their colleagues and perhaps even build contacts or friendships.

For a champion, enabling collaboration is everything, so expanding their social circle is a great way to help them do their job better. Besides, a little friendly competition is always good for team morale.

Workshops & talks

If it's possible, invite an industry expert to give your security champions a talk on some pertinent area of AppSec, or run a hands-on workshop. Teams tend to become echo chambers without some exposure to outside influences, and this could be the perfect opportunity to broaden their horizons.

Interactive quizzes, bug bounties

You'll find that most employees won't say no to a fun activity that involves something related to their work. Having them participate in teamwide quizzes or bug bounties where you offer the winner an attractive prize could be just the thing to rejuvenate teams that are stuck in a rut.

Security conferences

Another good way to expose your security champions to the wide, exciting world of security out there is to have them attend security conferences like Black Hat, Def Con, OWASP, and more. These are weird and wonderful melting pots of highly accomplished security professionals from across the world.

Your champions could attend trainings and talks, or go to the show floor where they can get to see large and small companies showing off their latest and greatest AppSec innovations. If you don't quite have the budget to send your entire cohort of champions, you could even offer conference tickets as a prize for meeting certain milestones or exceptional performance.

It's important to nurture your champions' passion for security in other ways, and keep the momentum of the program.

Maintain strong lines of communication

Your security champions are your tribe, your community, so you should treat them as such. Keep in constant communication with them either in person, or over an exclusive Slack channel where you can share information and chat.

Newsletters are a great way to constantly keep your champions in the loop. Whether it's about something cool happening in the industry in general or within the company itself (or both), send out a regular email blast to help them catch up with interesting new trends.

If possible, have your champions be the first ones to know about new security tools or processes being implemented in the company. Let them in on your security activities and ask for their inputs on what could be improved or changed. As developers, they might see something the security team totally missed, and it will give them a sense of ownership over the overarching security initiatives at your organisation.

Motivate your champions with rewards

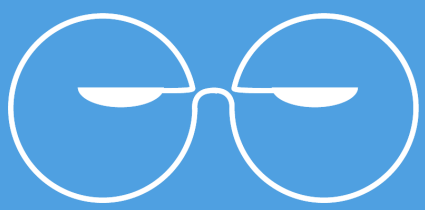
Rewards are a fun way to thank your security champions for volunteering to be part of the program and doing a good job. Depending on how flexible upper management is on this, you can prepare all kinds of exciting rewards for when your champions advance in their training levels, achieve the KPIs and milestones, and have shown exceptional performance over time.

The simplest way to reward a champion is giving them a physical certificate, or acknowledging their achievements among their peers. Never underestimate the positive boost a solid pat on the back can give a budding champion.

If you've created a 'brand' for your security champions program, you can give out fun swag — everything from t-shirts, to water bottles, to keychains, to stickers. This is where that mascot you designed will really come in handy.

Specifically commending a high-performing champion to upper management is an excellent way of getting them noticed among the higher-ups at your organisation. It's also a way to let the champion know you're invested in supporting the advancement of their career.

Build a Security Champions Program with AppSecEngineer



The path to transforming your software with security champions begins with training. And AppSecEngineer offers the best training money can buy.

Your team can leverage our massive growing library of 100% hands-on content, with new cutting-edge courses, Challenges, and Playgrounds released every week.

Track your team's progress with analytics, challenge them to solve hands-on security problems, and support them every step of the way to mastering security.

Give it a try, your champions will be hooked.

Manufacturing

Retail

Technology

Finance

Defense

Government

Healthcare

AppSecEngineer for Businesses