SECURITY BOULEVARD

DevOps.com

BUILD A WORLD-CLASS SECURITY CHAMPION PROGRAM

By Ericka Chickowski

VERACODE

```
Confidently.secure
(your_0s_and_1s);
```

Putting you 01 step ahead.

Veracode is your partner for confidently reducing your risk of security breach. By increasing your security and development team's productivity, we help you achieve your business objectives. Accurate and reliable results mean fewer false positives and negatives, so you can react and respond efficiently and confidently knowing your software is protected by the industry's best solution.

Visit our table at **DevSecOps Days**
or at **RSA® Conference booth N-5553**

Security champions have grown to become a critical component to successful DevSecOps organizations. These embedded change agents can be developers, DevOps engineers, or other important stakeholders in the software delivery process. Trained and empowered by the security team, they take a special interest in cybersecurity best practices. Their role is to help advocate for security, answer questions from their peers, and take the lead on making their team or project more accountable to security requirements during the daily grind of delivering software.

Not only does this improve DevOps and security team relations, but it also helps the security team scale its efforts. There are only so many people a security team can hire, but if these experts design their champion

program effectively, they can lean on their embedded champions to give them a force multiplier in carrying out security tasks and strengthening security culture across the board.

In short, security champions provide a golden path to democratizing security and truly taking DevSecOps to the next level.

While it is possible for security advocates to organically bubble up within DevOps organizations, it usually takes systematic planning and investment to train and empower an army of security champions.

Here's what it takes to start building a world class program to do just that.

SECURITY CHAMPION PROGRAM: THE WIN-WIN SCENARIO

SECURITY GETS

Better collaboration with DevOps teams

Improved scale-out of security expertise across the organization

Better view into daily security practices

Strengthened security culture

DEVOPS TEAMS & CHAMPIONS GET

More say over how they meet security requirements

More peers to lean on for security questions and help

A path to gaining new security skills and improved career options

DESIGNING THE PROGRAM AND THE ROLE

The most successful security champions programs tend to be the ones that are designed with intent. In other words, they're built to meet specific, but realistic security goals.

"This (program design) process starts with selection of initial goals that will improve your security program but are scoped to something achievable by even those volunteers that have minimal previous experience with security," says Ryan O'Boyle, manager of product security for Veracode, a software security vendor.

From his experience some appropriate early goals can include adopting better processes for security reviews, facilitating the incorporation of security tools into build pipelines, improving response time to software test findings, or improving basic secure coding knowledge across the DevOps team. Then as the program matures, the corps of champions and the security team can start working together to heighten overall team goals to "require more security experience and make security champions mandatory for each project," O'Boyle explains.

Goals are crucial at the outset – they define the role of champion for your organization.

Goals are crucial at the outset because those will be what defines the role of

champion for your organization. Official responsibilities, training, and champion activities should all track back to them, says Christopher Emerson, a consultant with White Oak Security who helped build security champions programs at Best Buy and Target.

"The security team should provide each security champion with training, guidance and tools to be successful and meet the goals," says Emerson. "Teach the security champions how you perform security reviews, how your organization ranks risk, and how they can leverage existing security tools. Enable them to make decisions within their sphere of influence, and support those decisions."

"Make the champion role an official one with its own goals and objectives reflected in the individual's performance ratings as appropriate."

–Doug Graham, CSO, Lionbridge

From an org chart perspective, the champion should also be designated with an official role.

"Make the champion role an official one with its own goals and objectives reflected in the individual's performance ratings as appropriate. Invest in their training and development as part of the program," says Doug Graham, chief security officer for Lionbridge, a localization and AI training data company.

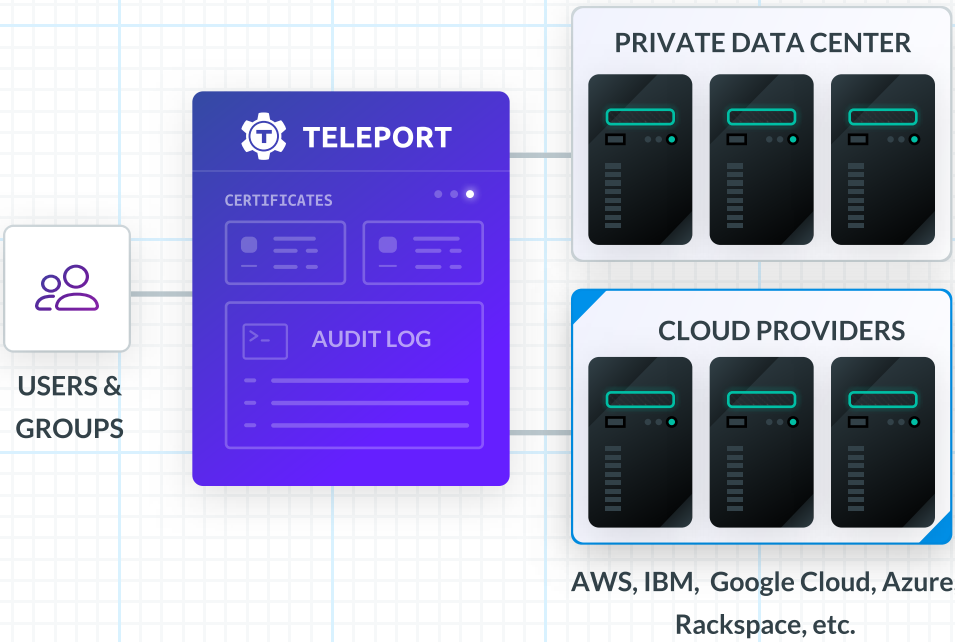
While the champions should be embraced as participating collaborators with the security team and included in security department meetings, Graham believes they need to be fully embedded into DevOps teams. He and other experts make it clear that organizations must take pains so that champions aren't seen as 'spies' for security, but instead as equal DevOps colleagues who have an especial interest and knowledge in security matters.

GRAVITATIONAL

Multi-Cloud Privileged Access Management

Teleport makes it easy for users to securely access infrastructure, while **meeting the toughest compliance requirements**.

Securing Infrastructure with Teleport



Learn more at **gravitational.com/teleport**

We're Open Source

"A dotted line or similar reporting path back to security helps with governance, but it does very little to make the champion a seamless part of the organization, which has to happen in order for them to effect positive change," he says.

All of this early program planning presupposes one important prerequisite: a solid secure development lifecycle (SDLC) with formalized best practices for champions–and everyone else–to draw upon. Without practices laid out in an SDLC backbone, security champions won't know what they're supposed to deliver, says Brook Schoenfield, master security architect for security firm IOActive, and a security practitioner who has built out champion programs at four different organizations.

"Clearly defining what 'secure' means in the context of the software to be delivered must be done in parallel with any champion program."

– Brook Schoenfield, Master Security Architect, IOActive

"Adopting a clear set of activities and expectations for the delivery of 'secure' software – and clearly defining what 'secure' means in the context of the software to be delivered must be done in parallel with any champion program," Schoenfield says. "Otherwise, what are these empowered people actually delivering? What are their responsibilities? To what are they being held accountable?"

PRO-TIP:

CLEARLY DEFINE THE ROLE

"A security champion is fundamentally an enabler and promoter of application security best practices. Defining a list of responsibilities and expectations helps organizations maintain alignment with the objectives of the security champion program. Don't forget about appropriate separation of duties. For example, the security champion may not be the role entitled to make fix/no-fix decisions."

–Shawn Asmus, Optiv

Want to Accelerate Cloud Adoption and Reduce Risk?

Security Policy Automation is the Key.

Cloud-native technology, containers, microservices, and the widespread dependency on APIs and third-party code are driving today's digital transformation efforts – often leaving security teams in a fog with no visibility or control of cloud activities. Balancing security without getting in the way of agile development is not an easy task.

Forge the DevSecOps partnership with security policy automaton to gain visibility and control of your security posture across hybrid cloud environments – without compromise. Ensure your hyper agile and automated environment is secure with Tufin SecureCloud.

Tufin SecureCloud

Balance Hybrid Cloud Security **and** Agility with Automatic Policy Generation

- ✓ Gain visibility and control
- ✓ Shift left security – integrate with CI/CD
- ✓ Generate, test and enforce microsegmentation
- ✓ Zero Trust security for cloud-native
- ✓ Ensure continuous compliance
- ✓ Unify security policy orchestration across hybrid cloud
- ✓ Accelerate cloud adoption without risk or compromise

Start your free trial of Tufin SecureCloud today to gain visibility and control of your security posture across hybrid cloud environments – without compromise.

tufin.com/contact-us

tufin The Security Policy Company.

ATTRACTING CANDIDATES

Identifying and attracting suitable candidates to become your security champions throughout the DevOps organization is an obvious early step for setting up the program. There are two schools of thought here about whether it should be the very first step. Some organizations take an 'if you build it, they will come' approach by designing the program first and then attracting appropriate people to fill it out. Others prefer a more organic approach of identifying early, strong champions who can help pitch in to design the program to suit the culture and mission of the DevOps tribe while still meeting security goals.
Wherever your approach lands between these two philosophies, recruiting will be crucial to building initial momentum for the security champion program. One of the key ingredients of the best candidates is desire, Schoenfield says.

"Draw champions from among engineers and architects who express a desire to learn security, who have at least a glancing exposure to architecture and design in any form and level–this is going to be taught, anyway–and who demonstrate at least the beginnings of technical leadership," he says.

That leadership doesn't need to be formally demonstrated by title or senior role, but the program should ideally be seeded with engineers who have enough technical experience to lend them credibility amongst their peers to "hold their own in technical debates," says Dan Cornell, CTO of Denim Group. And

they should be able to conduct these debates and discussions with respect and openness.

"Security champions are going to be the local representatives of your application security program and need to be able to act the part," says Cornell, explaining that it's more than just technical ability that will make someone successful in the role. "Asking for help often isn't easy, so security champions also need to be approachable."

"Accepting all offers of help works towards a social tipping point of a 'culture of security.'"

– Brook Schoenfield, Master Security Architect, IOActive

Because so many stakeholders have a hand in security across an integrated DevOps teams, be sure not to limit recruiting to developers.

"If you're missing representation anywhere among teams, solicit some volunteers from managers to help fill in those gaps," O'Boyle says.

As organizations look out for the ideal traits in a perfect candidate, they should take care not get caught up in checking off all the boxes. They should remember that if the champion program is designed right it will naturally refine the pool of candidates as they progress in training.

"The program will determine who sticks and who doesn't," says Schoenfield. "Find a use for every offer of help, even from the most junior person, though these may not fulfill the requirements of a champion. Accepting all offers of help works towards a social tipping point of a 'culture of security.'"

VERICA

CONTINUOUS VERIFICATION

Use the principles of
Chaos Engineering
to proactively uncover
system weaknesses
& security flaws.

more at VERICA.io

PRO-TIP:

SOME WAYS TO GENERATE INTEREST

"You can generate interest in a variety of ways. I recommend activities that build security into your cultural fabric, such as lunch and learns on security topics, post-conference summary sessions, and capture the flag events. These are a great way to find those interested in learning more about security."

–Ryan O'Boyle, Veracode

World's First IAST for Mobile Apps

NowSecure

Deliver Secure Mobile Apps Faster

Purpose-built for mobile DevSecOps, get fully automated mobile app security and privacy testing that:

- ✓ Plugs directly into your CI/CD toolchain
- ✓ Runs SAST, DAST & IAST in minutes
- ✓ Eliminates false positives & wasted time
- ✓ Maps results to GDPR, CCPA, NIAP, HIPAA & more

Build security into your mobile dev pipeline today!

Stop by our table or visit **www.nowsecure.com**

TRAINING CHAMPIONS

Fundamentally, training will always be one of the most important core components of a security champion program. In many ways the champion program is actually a component itself–of a broader security awareness training program that seeks to bring security knowledge and insight to everyone involved in delivering software and IT services. The champions are simply the ones who take the initiative to move furthest along in the formal and informal learning paths.

"We have had success identifying security champions when they go through instructor-led training courses," says Cornell. "Keep an eye out for the students who really take an interest in the subject matter and keep themselves ahead of the class."

So, one of the best ways to identify and get the most out of champions is to actively recruit anyone who expresses interest and offer them as much security-oriented training as your organization can afford to provide, says Larry LeBlanc, chief engineer of security for Sierra Wireless, an IoT firm.

"It almost doesn't matter what the subject matter is – secure coding, threat

"The more people you can sensitize to security issues, the more champions you will find."

– Larry LeBlanc, Chief Engineer of Security, Sierra Wireless

assessment, network security, penetration testing, ethical hacking," LeBlanc says. "The more people you can sensitize to security issues, the more champions you will find, and you will also accelerate your security initiatives because the organization as a whole will be more receptive."

The basic training can be a mix of internal and external classes, as well as traditional instructor-led training and student-led learning experiences. As everyone advances beyond security fundamentals, budding champions need to be taught how these principles apply to your environment and be given a learning path to competency.

"You'll need to get them some training in how you do security," explains Jeff Williams, CTO of application security firm Contrast Security. "A 'ninja belt' system is often used to provide structure."

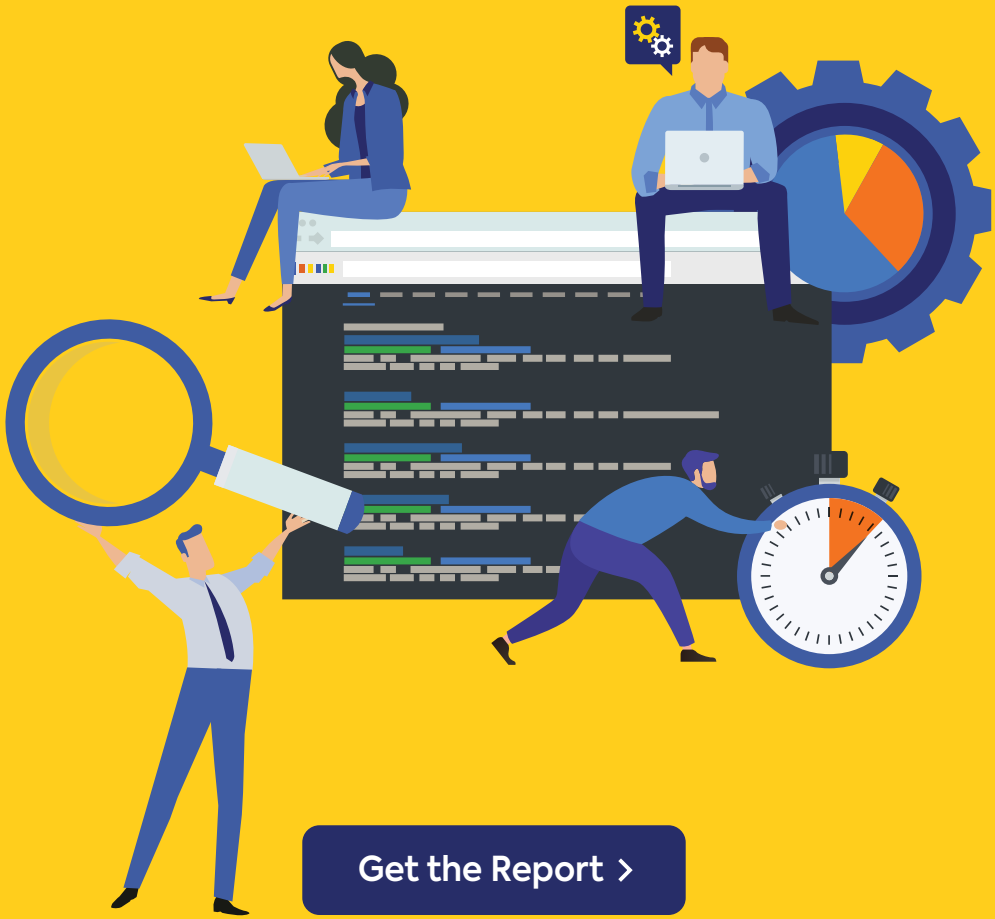
Some companies bring in instructional design experts to help them create a path to competency, others may engage with security training companies or security consultants, but the key lesson is that a champion program needs some formalized method for training and for acknowledging champions' growing expertise in security as they progress. This is good for the organization and provides a big motivator for champions seeking to bolster their resumes.

"We worked with a large bank to craft a matrix of the skills they wanted their security champions to build over time and the level of knowledge they were expected to have at each level of advancement," says Cornell. "This provided their security champion candidates with a solid understanding of how they could expect their career to progress over time and gave them specific goals for professional development."

Formal training should be just the start to boosting security champion competency. The most successful programs also

WhiteSource

Developers Are Taking Over AppSec



Get the Report >

establish mentoring relationships. According to Jim Hamilton, senior manager in the information security program office at LinkedIn and a leader of LinkedIn's security champions program, mentorship is a core component to his company's champion program.

"Champions are assigned a 'buddy' from LinkedIn's Information Security team based on their interests, the project they work on, and their area of expertise," Hamilton says. "Having this kind of specialized support is especially valuable for customizing the program, since the goal for champions is that they become security resources on their own teams."

He explains that mentors make it much easier to customize training and projects to tailor the experience to each champion. Mentoring also gives champions an opportunity for applying new principles with a safety net and solidifying knowledge gained in the classroom or online.

"Truly, the most novel thing I've observed this year at a large national insurance company, both profound and simple, was a series of training sessions where application developers and security professionals were paired up to better understand each other's roles," says Dave Klein, senior director of architecture and engineering for cloud security firm Guardicore. "The developers were given a series of coding exercises while the security professionals watched and commented on security hygiene throughout the process."

Not only did that exercise teach the developer, but it also proved to be a learning experience for the security mentors themselves.

"The result was that the security expert learned just as much about coding as the developer learned about better security practices," Klein says. "Truly, if done right, this kind of training could be a trend that leads to true DevSecOps."

Rapidly Scale Application and Infrastructure Security

Did you know...

You can spend up to 150% of scanning tool license costs annually just managing and maintaining these tools. This doesn't even include selecting and onboarding.

The ZeroNorth platform provides risk-based vulnerability orchestration across applications and infrastructure so you can:

- Securely embrace digital transformation
- Integrate security across the entire software lifecycle
- Gain continuous visibility of vulnerabilities from AppSec to SecOps
- Reduce the costs and burden of managing disparate scanning tools

Learn more. Download the eBook "The Essential Guide to Risk-Based Vulnerability Orchestration Across the Software Lifecycle."

ZERONORTH™

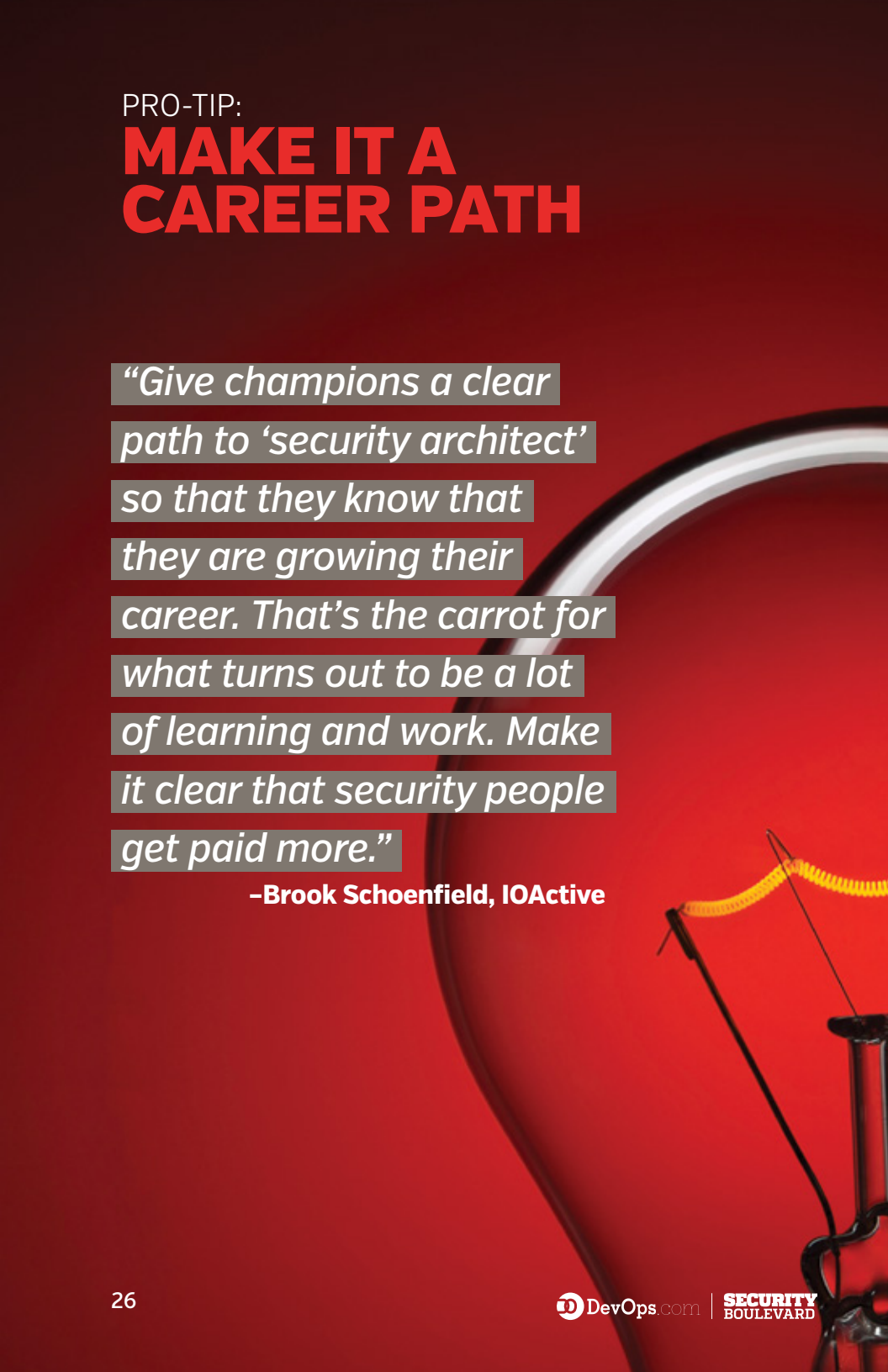
zeronorth.io

PRO-TIP:

MAKE IT A CAREER PATH

"Give champions a clear path to 'security architect' so that they know that they are growing their career. That's the carrot for what turns out to be a lot of learning and work. Make it clear that security people get paid more."

–Brook Schoenfield, IOActive



sysdig

Ship applications faster

Embed security, compliance and performance into your secure DevOps workflow.

Scan images and block threats at runtime with Kubernetes-native controls. Speed incident response and forensics using granular data with cloud and Kubernetes context. Unified platform for monitoring and security reduces tool sprawl. Open by design, with the scale and usability you need.

Embed Security

Maximize Availability

Validate Compliance

LEARN MORE AT
sysdig.com

MAKE THE PROGRAM SUSTAINABLE

Don't make that investment in security champion training and program development all for naught by letting the program stall out. It's crucial to take steps out of the gate to make the program sustainable–and a big part of that is ensuring that you don't leave these embedded advocates out in the cold once you've identified and trained them. Carving out a role is just the start. It takes political support and leadership from security and line-of-business executives in order to empower champions to affect change.

"Support your champions. Security initiatives will inevitably conflict with business realities and it is easy for security champions to be seen as roadblocks," says LeBlanc. "Make sure issues raised are promptly reviewed by the security team and that there is a clear escalation path for resolving conflicts."

According to Schoenfield, this is one of the hardest lessons he's learned in building out champion programs.

"Don't leave your champions hanging when their own management is resisting their advice," he says. "At that point, a central, empowered [strong] team has to pick up escalations in order to protect champions from conflict with the people who are also responsible for their bonuses and promotions."

It's not easy to provide that kind of support, says Schoenfield, explaining that it takes a lot of modeling behavior, community building, servant leadership, and at least a little bit of political

acumen to pull off properly.

It's not just moral support or political backing that these champions need, either. They'll also need the time and mental space to carry out their additional duties.

According to Hamilton, at LinkedIn security champions are allocated approximately 25% of their time to work on program related tasks. This gives them time to learn and practice security techniques.

"Since this time is taken from their typical workload, it's critical to have buy-in from a champion's manager at the outset," he says. "In fact, one of our program requirements is manager pre-approval–this helps make sure that everyone is on the same page about the adjusted workload and that any temporary changes can be made accordingly."

At the same time, this is where both C-suite leaders and the security team needs to manage their own expectations. Security champions can't be all things to all people, even when they have time appropriated for their security duties.

"Companies struggling with the overwhelming amount of work involved with security often want a security champion program to help scale their efforts," says Williams, explaining that this will be a natural result of building a program, but that you've got to be realistic about how much any one champion can do. "Because champions aren't full time security experts and almost certainly have other responsibilities, you can't expect them to do the heavy lifting."

To that end, don't make the security activities that champions are deputized to carry out or any harder than they have to be. One of the most important buttresses to a champion program is security tooling and automation that's seamlessly embedded into the DevOps toolchain. That makes it so much easier for champions to advocate to their colleagues to take meaningful

RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

EXPLORE THE HUMAN ELEMENT OF CYBERSECURITY.

What's the most important weapon in the fight against cyberthreats? New software? Faster equipment? Smarter computers? At RSA Conference, we believe it's people.

Attend RSA Conference 2020, February 24-28, and join thousands of security professionals, forward-thinking innovators and solution providers for five days of actionable learning, inspiring conversation and breakthrough ideas.

Register today to save your spot at the world's most comprehensive cybersecurity event.

FOLLOW US

#RSAC

rsaconference.com/devops20

*$900 discount applied to the on-site price.

action in their workflows without causing painful disruptions.

"When your security team architects and builds security solutions, they need to be consumable by every team. Good security solutions will do you no good if developers can't use them," says Sean Lutner, infrastructure architect at Edgewise Networks. "So make sure you have good documentation and a central repository for all software packages and libraries."

For example, Lutner points to an artifact storage tool that his team uses that automatically scans every artifact for security vulnerabilities. When one is found, the team has created a remediation process that can help developers address it as quickly as possible.

A truly successful program is built around the concept that security champions aren't meant to just be isolated security workhorses. Instead, they should also be security teachers and mentors for colleagues to lean on about security-related technical problems. By emphasizing this important component of the champion role, organizations can design a sustainable security champion program that can weather staff churn when the most experienced champions inevitably take their newfound skills to more senior, specialized positions.

"The secret is to make training and mentoring a part of each champion's role. Training will go viral, as each generation of champions turns around and starts training/mentoring the next," says Schoenfield. "The moment champions begin to become self-sufficient, encourage and empower them to train others."

Not only does this ensure the long-term viability of the champion program but it also provides a force multiplier on any training or mentorship offered directly by security team, bolstering the security culture of the organization without bringing on more security staff to make it happen.

accelerated strategies

WE ARE TO ANALYSIS WHAT OPEN SOURCE IS TO SOFTWARE

ACCELERATED STRATEGIES GROUP

is out to democratize access of industry expertise and knowledge.

We offer insightful, intelligent, useful information in a variety of formats relevant to the IT community on cybersecurity and DevSecOps.

"Knowledge wants to be free"

ACCELST.COM

TONS OF FREE CONTENT

FREE 20-MIN CONSULTATION

PRO-TIP:

SOME WAYS TO GENERATE INTEREST

"Support your champions. Security initiatives will inevitably conflict with business realities and it is easy for security champions to be seen as roadblocks. Make sure issues raised are promptly reviewed by the security team and that there is a clear escalation path for resolving conflicts."

–Larry LeBlanc, Sierra Wireless















PROVING BUSINESS RELEVANCE

Make no mistake, setting up a fully functional security champion program will take considerable investment and executive support. Which means that program designers should be thinking out of the gate about how they can prove the business relevance of the investment in order to scale out the program and maintain long-term funding and support.

This is why it is important to not only pick initial goals that will drive the program, but also establish metrics around those goals to track how the program is moving the needle on these issues over time.

"Measure as you go," recommends Shawn Asmus, director of threat management at Optiv. "Define measures of success that relate to the program's effectiveness. For example, the number of vulnerabilities found should shift earlier in the lifecycle, a reduction of high-severity / overall findings, faster times to remediate, and improved program maturity assessment scores."

Don't forget to measure sentiment, too. Technical indicators are important but

"Measure as you go. Define measures of success that relate to the program's effectiveness."

– Shawn Asmus, Director of Threat Management, Optiv

management will also be interested to hear how the program is helping them professionally develop and hang onto key developer and security talent. This can be done both anecdotally and formally through surveys that measure opinions over time on topics like security awareness and satisfaction with the security team relationship on the developer side of the house, or burnout and risk comfort levels on the security side.

It's not good enough to simply measure the program's performance, but also to tell stories about these measurements that increase visibility of security champion successes. Always be looking for ways to help everyone recognize what is working in order to not only maintain support from the business but also as feedback to improve the program long-term.

"Leverage the 'wins' you see from this program ... it will help to raise awareness of security within the organization and potentially increase interest in the program itself."

– Christopher Emerson, White Oak Security

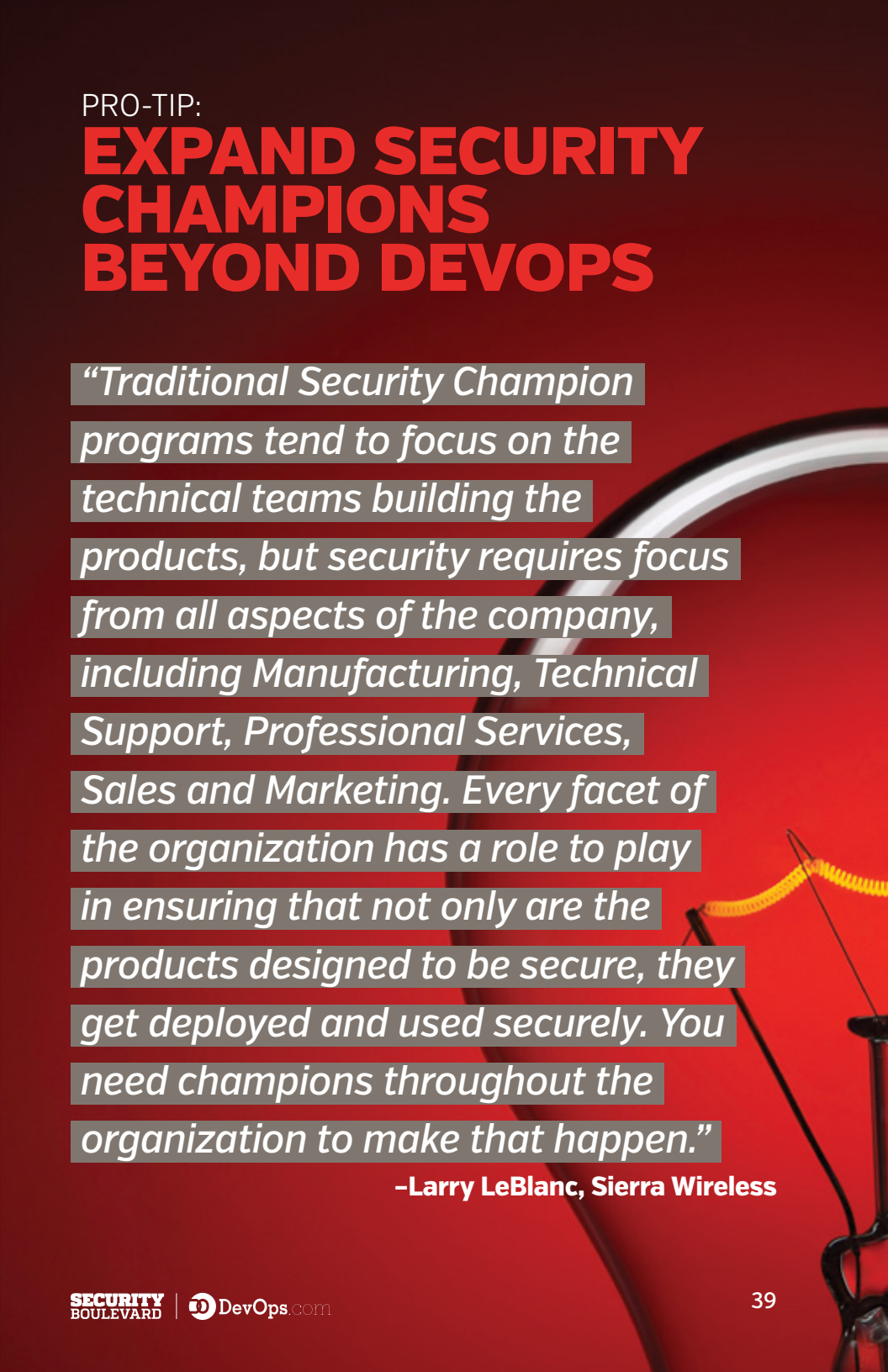
"Leverage the 'wins' you see from this program for both internal workshops or external presentations," Emerson says. "It will help to raise awareness of security within the organization and potentially increase interest in the program itself along with educating development and product teams about ways in which they can continue to provide secure solutions and products."

PRO-TIP:

EXPAND SECURITY CHAMPIONS BEYOND DEVOPS

"Traditional Security Champion programs tend to focus on the technical teams building the products, but security requires focus from all aspects of the company, including Manufacturing, Technical Support, Professional Services, Sales and Marketing. Every facet of the organization has a role to play in ensuring that not only are the products designed to be secure, they get deployed and used securely. You need champions throughout the organization to make that happen."

–Larry LeBlanc, Sierra Wireless




SECURITY
BOULEVARD
securityboulevard.com
twitter.com/securityblvd
facebook.com/secboulevard
DevOps.com
devops.com
twitter.com/devopsdotcom
facebook.com/devopscom