SECURITY INNOVATION

Five Ways to Train Security Champions in Cross-Functional DevOps Teams

As organizations seek to better embed security into DevOps and Agile software development, they're going to need to find better ways of scaling security knowledge across cross-functional teams.

Gone are the days where the security team can hold all the relevant knowledge for an IT organization and personally enact all the security checks on software code or infrastructure hosting applications. There are too many new applications and features being deployed, too much infrastructure spun up and down daily.

Everyone needs to chip in, and the only way they can do that is if companies properly train members of cross-functional teams on what it means to build and deploy secure software.

Cross-functional DevOps teams—and even non-DevOps teams moving toward continuous delivery of software—need all their members to skill up with both generalized and specific security training. From developers to DevOps engineers to site reliability specialists to database professionals, while each role has shared responsibility for security, how they accomplish it will vary significantly.

The following pages outline five ways to up-level your team's skills:

1.

RAISE THE BAR ON SECURITY AWARENESS ACROSS THE TEAM

The goal for modern security training in the DevOps era should be two-fold. First, organizations should seek to generally elevate security awareness across all IT functions. Second, they should seek to train up an elite cadre of security champions with deeper levels of security knowledge who work in various capacities for the team.

The first objective of awareness isn't to make everyone deep security experts, but instead to raise the overall bar for awareness about security from anyone that touches the continuous delivery/continuous integration (CI/CD) software pipeline. This includes developers, but also QA engineers, operations professionals, DBAs and more.

The second objective recognizes that in a DevOps environment that deputizes technologists of all types to execute on security strategy, there are going to be times where the organization risks watering down deep technical security competence in the trenches. Seeding teams with at least a handful of security champions with deeper levels of security knowledge as it applies to their specialty ensures that things don't get overlooked.

DevOps depends on an increased collaboration between IT roles and self-service. The challenge is as roles start to bleed into one another through deeper collaboration, individuals start to need a wider breadth of knowledge than ever before about how their actions impact the organization's threat posture. Take developers, for example: so much of application security (APPSEC) training today is focused solely on secure coding techniques, without accounting for the reality that developers today are using open-source libraries, spinning up servers, containers, and otherwise self-provisioning the infrastructure their software is running on.

Even when developers take the best secure coding training available, they may be missing a lot of knowledge about the dangers of security misconfiguration when they're setting up their infrastructure.

There should be a core set of common knowledge that everyone needs to know about security principles: things like regulatory concerns, infrastructure issues commonly used tools, and so on.

This is would give your architects, developers, database administrators, and anyone else in the CI/CD world a common foundation of awareness. In this scenario, ideally they would all be asking themselves, "Is this the most secure way to do this task?"

At the same time, security champions who are more interested in the technical details of these issues should also have the opportunity to extend their learning path beyond the basics so they can bring greater technical knowledge to bear and act as a security resource for the rest of their team.

YOUR TEAM SHOULD BE ASKING THEMSELVES: *IS THIS THE MOST SECURE WAY TO DO THIS TASK?*

2.

BALANCE TRADITIONAL TRAINING WITH HANDS-ON LEARNING METHODS

Traditional training is still the best starting point for disseminating security knowledge across teams. Continuing professional education (CPE) classes and overviews are all relevant and help build a foundation of introductory awareness. They're not always the most exciting method of learning, but they are incredibly effective when paired with more advanced training.

At the same time, that traditional training is more likely to stick with employees when supplemented with additional hands-on reinforcement. Security leaders hoping to build out security knowledge across the DevOps contingent should start exploring the benefits of gamification and simulation and how it can improve performance on the job.

Software engineers/developers, IT operators, and architects are much more likely to appreciate the nuances of security risks when their "book" knowledge is paired with hands-on training in simulated environments, or some kind of area where they can appreciate what they're defending against. Rather than just academically saying, "Here's what SQL injection is, here's how to defensively code against it," it's better to allow security champions to exploit those issues so they really understand them from all angles. This "learn by doing" approach is proven in its efficacy to transform knowledge into permanent skills

3.

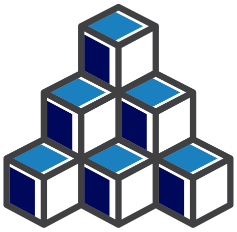
TACKLE ROLE-BASED SECURITY TRAINING

Even with a sophisticated blended learning experience, generic security training should only be the foundation for developing security champions within DevOps teams. A security champion program depends on training that's tailored to specific roles. Not only that, this training needs to be designed for the new reality of collaborative DevOps roles, rather than the limited and siloed IT functions of years past.

Organizations can take a team's security knowledge to the next level with tailored, prescriptive training based on specific roles and skills. Once individuals have the basic education and some hands-on experience, it pays to take the information about how they performed in these trainings and direct the trainee where they should focus next based on their job duties. So developers would get one suggested learning path, QAs another, infrastructure specialists a different one, and so on. By doing that, it'll give every security champion a much deeper level of training applicable to his or her daily workflows.

The training needs to offer people the path to not necessarily turn into security staff, but to learn at an elite level how security applies to their specific role. If teams can pepper even just a percentage of these elite security champions across each common role, these highly trained individuals can help their peers level up their skills organically as they work together on a daily basis..

4.



LEVERAGE MODULARIZED TRAINING

Many of the security principles taught to different roles will overlap so there's no reason to reinvent the wheel with brand new curriculum for every unique role. One way to do this is to develop a modularized training approach.

Modularized training breaks down certain principles into individual components of a curriculum library. From there an organization can then mix and match these components for each person's appropriate path—based on their role and depth of knowledge they need. Not only does this make it more elegant to shift to role-based security training, but it also adheres to the latest research in education that favors shorter, more consumable modules. Additionally, it offers a greater degree of curriculum flexibility and customization without reinventing learning content for every role-based training path.

5.

ESTABLISH A SECURITY TRAINING PLAN FOR DEVOPS TEAMS

Gartner analysts predict that DevSecOps practices will become embedded into 80% of rapid development teams by 2021. In this day and age where every company is a software company, IT leaders need to develop a security training roadmap to help their teams keep up with cybersecurity best practices to ensure that applications don't add unnecessary risk to the business.

Without detailed, prescriptive learning paths based on roles, organizations risk wasting their training dollars on generic knowledge. Many times companies simply require a number of hours for professional development in security, without offering any guidance or prescriptions of what the course matter should include. As a result, employees often choose the easiest path to racking up those hours without gaining many appreciable skills or knowledge along the way.

Because there are so many moving pieces to building out training that grooms security champions across so many IT functions, security and IT leaders need to actually lay out a detailed plan for how they're going to develop security skills relevant to every function of a DevOps team. While each role needs to understand the fundamentals of secure DevOps, privacy protection, the OWASP Top Ten, and other core topics, additional job specific training is needed to do their specific tasks:

ABOUT THE AUTHOR

Ed Adams is the President and CEO of Security Innovation, the independent authority on application security risk assessment, risk mitigation, and education. He is a seasoned software executive with successful business experience in various-sized organizations that serve the IT security and quality assurance industries.

As CEO, Mr. Adams applies his technical and business skills, as well as his pervasive industry experience in the Application Quality space to direct world-renowned application security experts and deliver world-class professional services to many of the most recognizable companies in the world including Microsoft, IBM, Visa, FedEx, ING, Symantec, SAP, and HP.

Mr. Adams is the founder and business owner of the Application Security Industry Consortium, Inc. (AppSIC), an association of industry technologists and leaders focused on establishing and defining cross-industry application security guidance and metrics. He is on the board of the National Association of Information Security Groups (NAISG).

No stranger to the podium, Mr. Adams has presented to thousands at numerous seminars, software industry conferences, and private companies. He has contributed written and oral commentary for business and technology media outlets such as New England Cable News, CSO Magazine, SC Magazine, CIO Update, Investor's Business Daily, Optimize, and CFO Magazine.

ABOUT SECURITY INNOVATION

Security Innovation is a pioneer in software security and trusted advisor to its clients. Since 2002, organizations have relied on our assessment and training solutions to make the use of software systems safer in the most challenging environments – whether in Web applications, IoT devices, or the cloud. The company's flagship product, CMD+CTRL Cyber Range, is the industry's only authentic environment to build the skills teams need to protect the enterprise where it is most vulnerable – at the software layer. Security Innovation is privately held and headquartered in Wilmington, MA USA. For more information, visit **www.securityinnovation.com** or connect with us on **LinkedIn** or **Twitter**.

Get in **Touch** |

✉ 187 Ballardvale Road, suite A195
Wilmington, MA 01887

☎ 887.839.7598 x1
www.securityinnovation.com