OWASP Security Champions Guide

Waypoints and Pitfalls for R&D Organizations

Scenario

You are a R&D engineering leader for a product or service company. Security is one big challenging area of your organization that you are trying to tackle - because a lot of workstreams and initiatives at your organization are cutting edge R&D (move very fast), and some conclude very fast (fail fast + lessons learned), you know that security approach at your organization has to navigate this unique nature. Company leadership is bugging you to take control of the situation, fast.

You had previously heard of the concept of “Security Champions” - organically building security know-how and culture from within the organization with promised returns on accelerated improvements of security posture. You pitched it as a solution approach to leadership for the situation at hand. To your surprise, it was received very well!

Leadership gave you their sincere words of support, and asked you to roll out the “Security Champions” program with undue delay. You were given some budget to leverage tools or R&D associates’ working time as you see fit, but with expectations of concrete Return-on-Investment (ROI). You are also expected to report the progress with the leadership at the next quarterly review, and are told that the leadership is expecting “great things from you!”

You thought to yourself, “Now, what!?” A fiscal quarter is not a lot of time, and you only have a very high-level concept of the program with a lot of “unknowns”.

If the above scenario sounds familiar to you, and are seeking for the answers, you are at the right place! The author had lived the scenario, and he would like to share the journey with you so that you could navigate the program rollout efficiently, and look out for the pitfalls!

Author

The author currently works for an innovative R&D organization within a multi-national enterprise as an engineering leader. He started his career as a software engineer at another similarly sized organization, and got a start in the security profession through sheer curiosity and pure chance - as a “Security Champion” program being rolled out at that company.

Having been both a “Security Champion” himself as well as having been the one to bootstrap a “Security Champion” program, the author would like to share his learnings so that you can be more effective at bootstrapping the program at your company, and avoid his fumbles.

The Journey

The author would like to reflect his journey of “Security Champion” program operations of 5 years in two distinct perspectives: waypoints and pitfalls. Waypoints are the approaches that the author found particularly helpful through the years to get the program moving where it needs to go. Pitfalls are the “unexpected” challenges arising from otherwise well-intentioned activities and interactions which the author had to resolve.

Even after 5 years, the program operations is far from “feature” complete: every new endeavors and changes in business will bring new challenges, and the program is in the state of continuous improvements and optimizations. This is the aspect of the “Security Champion” program for which the author finds very fascinating, and hope that you, as reader, do too!

Now, without further ado ….

Waypoints

- “Keeping the regular social connection with leadership / executives who gave you support, and sponsored the program.”

  Company leadership / executives have a lot on their plate, and sometimes, the “Security Champion” program roll out might slip their minds. It really helps to have a regular social connection outside of project / program business review so that they remain informed through informal exchanges on how the program roll-out and operation is coming along. This is a challenging task, and having yourself heard by the leadership / executive sponsors regularly also boosts your morale.

- “Be a transparent and crisp communicator. Sometimes, a little bit of candor goes a long way, especially with leadership / executives.”

  Regular program progress reporting does not have to always be “happy” paths. This is especially important in communicating with the leadership / executives: you would be surprised to find out that leadership is usually willing to help if you can articulate the kinds of support you need from them for the challenges you are trying to tackle.

- “Be friends with the stakeholders in the frontlines, and be empathetic to their perspectives.”

  It is great that you have the buy-in and blessing from the company leadership / executives, but you should not forget about the other stakeholders in the frontlines: project managers, people managers, product owners. Always try to see what you can bring to the table for what is important for them: reciprocity goes a long way!

- “The Security Champion program that works for your organization is a unique one.”

  There is no one-size fits all “Security Champion” program. There will be approaches which have been successful elsewhere, but they would not necessarily be successful out-of-the-box at your organization. Every organization has uniqueness in how it ticks. Recognize the uniqueness, embrace it, and adapt the approaches accordingly. Or even better, craft new ones of your own!

- “Lean-in to what is already there and universally understood organizationally when initiating the roll out of the Security Champion program.”

  Are there standardized processes for quality management at your organization? Are you aware of organizational guidelines regarding how projects are to be structured and executed? Great! Try to see if there are synergies to security champion activities, and align them to tried and true organizational processes.

  Find the associates who can iterate / amend these organizational practices, and integrate the security champion activities into them.

- “Concretely showing what is in it for the Security Champions goes a long way, keeping motivation and engagement high.”

  For most “Security Champion” program roll outs, the title of “Security Champion” will be a role served by associates who hold other formal duties. So, being able to articulate and show what is in it for these great folks for their contributions is crucial.

  There are many ways of giving back to the “Security Champions” - organizational recognition being the most common one. But be mindful of the fact that the reason for keeping engaged will vary across individual champions: some might have found their passion for security with the opportunity to become a champion like the author did, but some might keep on engaging because of the social aspects. Understand and know your own security champions so that you can be balanced when articulating why the program matters for the champions themselves.

- “Start from a very simple set of responsibilities for the Security Champions, aligned with what is needed for the organization at the moment. Then, evolve!”

  When the roll out started at the author’s organization, it only started with champions building dataflow diagrams and data sensitivity classification for their teams without requiring in-depth analysis of threats and risks.

  At the time, getting a wide, general coverage of the landscape was the first priority. Only after the champions had become familiar with the process, and the coverage became reasonable, additional security knowledge training were introduced, which enabled the

champions to start sharing more advanced technical security topic duties: such as implementing software security features, performing some baseline security testing in proper manner as part of quality management processes, and monitoring for security relevant events for the teams' assets.

A side benefit of having the completed data flow diagrams and accurate data inventory was that it helped the teams in their activities as well, so "Security Champion" activities got appreciation by the teams.

Pitfalls

- "Recognize that different teams or departments in your organization require different kinds of security champion activities."

  Some companies are unique in that there are software development departments as well as departments which work with technology outside of software, e.g., physical sciences or hardware, etc.

  Be mindful of the fact that even if departments or teams do not work on software, they could still be working with software and connected technologies, and proper security care should be given.

  The concrete example was that there is a department performing R&D on chemicals at the author's company, and it appeared as if it would not be important to recruit security champions from that department. However, upon closer look, it turned out that the lab equipment in use required sophisticated software and network setup, and as such, security champions were recruited from the department, and were trained on network security.

- "Recognize that some security champions could be very eager."

  Be on the look out that some security champions could go above and beyond in the ways you never thought they would, even though it was well intentioned.

  The concrete example was that the author works with a champion who went ahead, and helped "penetration test" another team's application without proper training or permission from the team. Even though there was no significant damage done, the author had to give impromptu explanations to multiple concerned stakeholders. The author also took it as a feedback opportunity to integrate proper processes of security testing training into the "Security Champion" program.

- "Recognize that not all stakeholders are up-to-date on security champion activities and efforts they require."

Be transparent and precise with frontline stakeholders: project managers, people managers, and product owners about the responsibilities of a security champion, and efforts required to fulfill them. Always aim to proactively reach out, and inform the front line stakeholders because they are the primary partners to the program rollout.

As a concrete example, the author had to learn this hard lesson of being complained by a discontented project manager who had an impression that security champion activities were hampering the project goals due to not understanding the responsibilities of the security champion in the project team.

It is important to set the expectations of responsibilities straight not only with the security champions but also with the frontline stakeholders who are expecting work output from the associates with the security champion role.

- "Be mindful about social tensions that could arise within security champions community"

  "Security Champions" are people, and each will bring their personality to the security champion community at large. Be mindful of the dynamics within the community, anticipate and diffuse the social tensions before they become issues, and impact the program operation.

- "Be mindful about the business side of things as you scale up the security champion program."

  Not being able to align the security champion activities with business incentives / goals / benefits can lead to losing support from many different stakeholders. This is especially true as the program is scaling up, and the scope of the activities expands.

  This was especially true for the author when he was starting to expand the security champion activities to include implementing security features for the software, which was met with lukewarm reception from frontline stakeholders who were fully supportive before. The author had to pivot by aligning the commonalities in the security features and tie them to the business outcomes for the teams to regain full buy-in again.

Closing

The author is glad that he was able to share some of his learnings over the years. He hopes that you find them useful or spark ideas for your own.

He believes that all the stories are worth telling, and insists you share yours at OWASP Security Champions Guide project!