Security Champions - case study

The story of 4 years of Security Champions development in a company with more than 15 development teams.

The environment before

Before setting up the Security Champions program, one of the biggest security problems was the lack of knowledge and low level of confidence among all company developers in the security area. Moreover, there was no possibility of having an application security specialist in each team.

As a leverage to solve those problems, I started the Security Champions initiative.

It had a lot of ups and downs. That’s how it worked over the time.

The first challenge

At the beginning of the Security Champions initiative, the biggest concerns were time and budget. It was challenging to convince the management to invest a particular amount of time in each development team to increase their security quality. Fortunately, the management was aware of the security importance as they worked closely with the main security department in the organization.

First stage - by the book

Starting the Security Champions, I decided to prepare it according to the many guidelines available on the internet.

I asked each team leader in the development department to designate a single person interested in the security area and able to take the responsibility of cultivating the security culture in their team.

The plan was to have one dedicated person in each team as an ambassador of security from the application security perspective and as a security consultant from the development team's perspective.

Common structure

When we set up the Security Champions community, it was time to think about the meeting structure and goals.

For simplicity and to make the preparation easier, I decided to keep the same structure for each meeting of the community.

In the beginning, we had 2 h meetings once a week. We needed it to make sure that all the community members are at least on the same level in the security area. Meetings were obligatory for all people designated by the team leaders.

Each meeting had the same structure.

We started with the current problems discussion to help Champions find solutions to streamline the development team's work. Then there was a lecture created by me to familiarize the Champions with the security topics. After each lecture, the community members had some small homework to do for the next week. It was discussed further at the next meeting.

Moreover, each training meeting had a written summary noted down.

At this stage, developers did not bring barely any security problems to the Security Champions meetings, so the first part of the meetings was usually short. They were not aware enough of the security of important areas to notice the potential problems.

Furthermore, that level of intensity did not bring good results. After a few weeks, many people stop attending the meetings. It turns out that not all of them were really interested in security as much as I thought. They said that the amount of knowledge was overwhelming for them.

The large amount of work needed to prepare the training did not pay off. Instead of increasing the level of security, it discouraged the community members.

Second stage - loosening of requirements

The first try to fix that problem was to change the way of choosing the Security

Champions. Instead of the team lead's designation, it was announced that this community is only for volunteers. It was not necessary for each team to have its representative in the Security Champions.

As a result, only about half of the original Security Champions members get back to the meetings. It means that not all development teams were having their own people specialized in application security. That was a big problem, but the main goal for that time was to build strong competency first.

Instead of the simple lecture, I started to conduct workshops at each meeting to engage the community and share the knowledge not only between me and them, but also (which was very beneficial) between them each other.

The meeting frequency was changed to 2h bi-weekly in order to not overwhelm them.

It worked quite well. That structure built a strong application security core in the organization. Moreover, people were a bit more engaged during the meetings and were noticing more security problems during the development.

Adding incentive

Still, the problem was that not all development teams were represented in the Security Champions community. It was due to the voluntary character of this community. That led to a grey area in the application security governance in the development department.

To facilitate it, we added an incentive to have a Security Champion in the team.

During the development of each project, there were moments when some kind of formal assessment, verification, or audit was required for the projects. Each of the development artifacts needed to be verified from many different perspectives. Each of those kinds of verification needed acceptance from the company application security team. Sometimes it led to delays in development.

We decided that we could delegate some acceptance work to the Security Champions. That way they could take more responsibility, and the development team didn't have a risk of delays.

It was a great incentive for each team to have their own Security Champion. It was not obligatory, but now, most of the teams wanted to have it.

At that time, the awareness of application security in important areas was

growing, and more and more Champions started to think about security in everyday work. It resulted in great discussions during the community meetings.

Inside marketing

To encourage people to join this community, each new employee was introduced to the Security Champions submission's terms and concepts. Meanwhile, they were invited to the Security Champions community.

Moreover, we started to talk wider about this initiative inside company communication channels. We published results of the meetings and summaries of security problems resolutions.

Building engagement

I noticed that people were engaged during the workshops, but they were still not willing to share the security knowledge enough with their teams.

Then, the next step was to invite the Champions to a more engaging activity - to start teaching. We selected a list of security vulnerabilities, and each of the Champions had to prepare a short (about 15 minutes) introduction about a few of vulnerabilities.

At the beginning, I was a bit afraid if requiring something more from them was a good idea. But finally, it turned out to be a great choice. Champions put a lot of heart and effort into preparing those topics. Most of the micro-training was well-prepared and organized. It gave a lot of knowledge to the whole community, and was presented in a really interesting form. That brought a bit of a different perspective to the known vulnerabilities.

But most importantly, it encouraged Security Champions to talk about security and even repeat their presentations with their development teams.

From that moment something has changed. It was visible that Champions took much more responsibility for the security during the development than before teaching experience.

Collaboration space

That set of changes and engaging activities encouraged champions to bring their own day-to-day security problems to the meeting more freely.
Like at the beginning, each meeting starts with a discussion on the current problems. Sometimes the discussion took the whole meeting time, but the current problem resolution was always more important than learning about the new risk.

Conclusion

After a few years of development, the Security Champions program works so well that it brings together more people than the teams count. Finally, it meets the original objectives: to increase the security level and to lighten the load on the security team.