

How to Run a Great **Security Champion** Program



True success is overcoming the fear of being unsuccessful ~ Paul Sweeney



Raphael Schaffo (29)

IT Software Engineer & Security Champion by the Swisspost

- Living in Fleurier (Switzerland)
- Still not married
- Many hobbies (Soccer, Uni-Hockey, White Hacking, Volunteer Firefighter, Youth coach)

Who am I

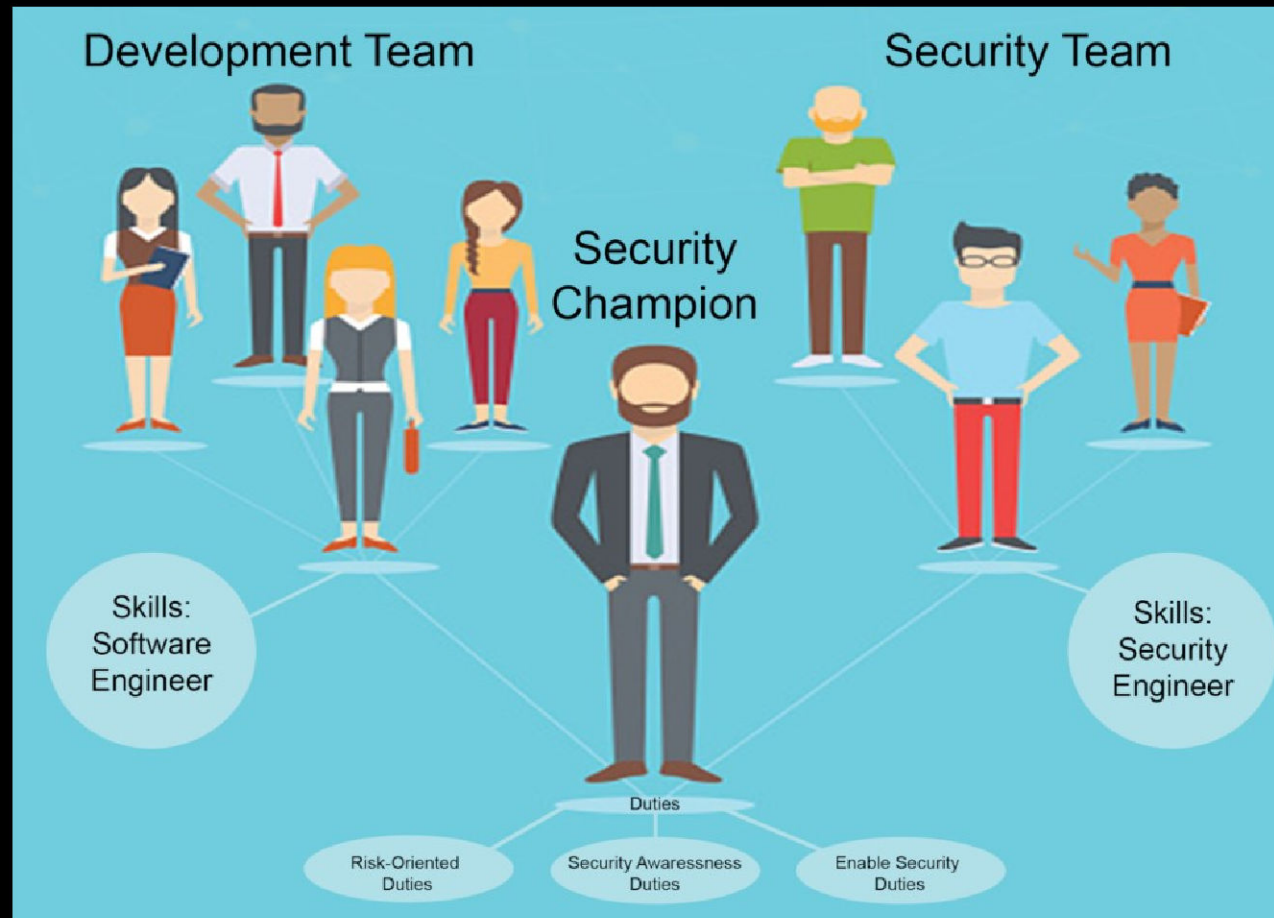
- What is a “Security Champions Program”?
- OWASP Security Champions Guide
- Story Telling “Swisspost’s adventure”
- Swisspost’s Manifesto
- Conclusion
- Question?



Red Line



What is the Security Champion Program



What is the Security Champion Program



Define guiding principles that are crucial to run a **successful** program

OWASP Security Champions Guide

- Be passionate about security.
- Start with a clear vision for your program.
- Secure management support.
- Nominate a dedicated captain.
- Trust your champions.
- Create a community.
- Promote knowledge sharing.
- Reward responsibility.
- Invest in your champions.
- Anticipate personnel changes.



The Ten **Key** Principles

OWASP Security Champions Manifesto



What made Swisspost's Security Champion Program so successful?



It all began at the end of 2019



Knock on the right door

- Analysis of the benefits
- Challenges
- Costs
- Goals
- Timeline
- Playbook

APPROVED

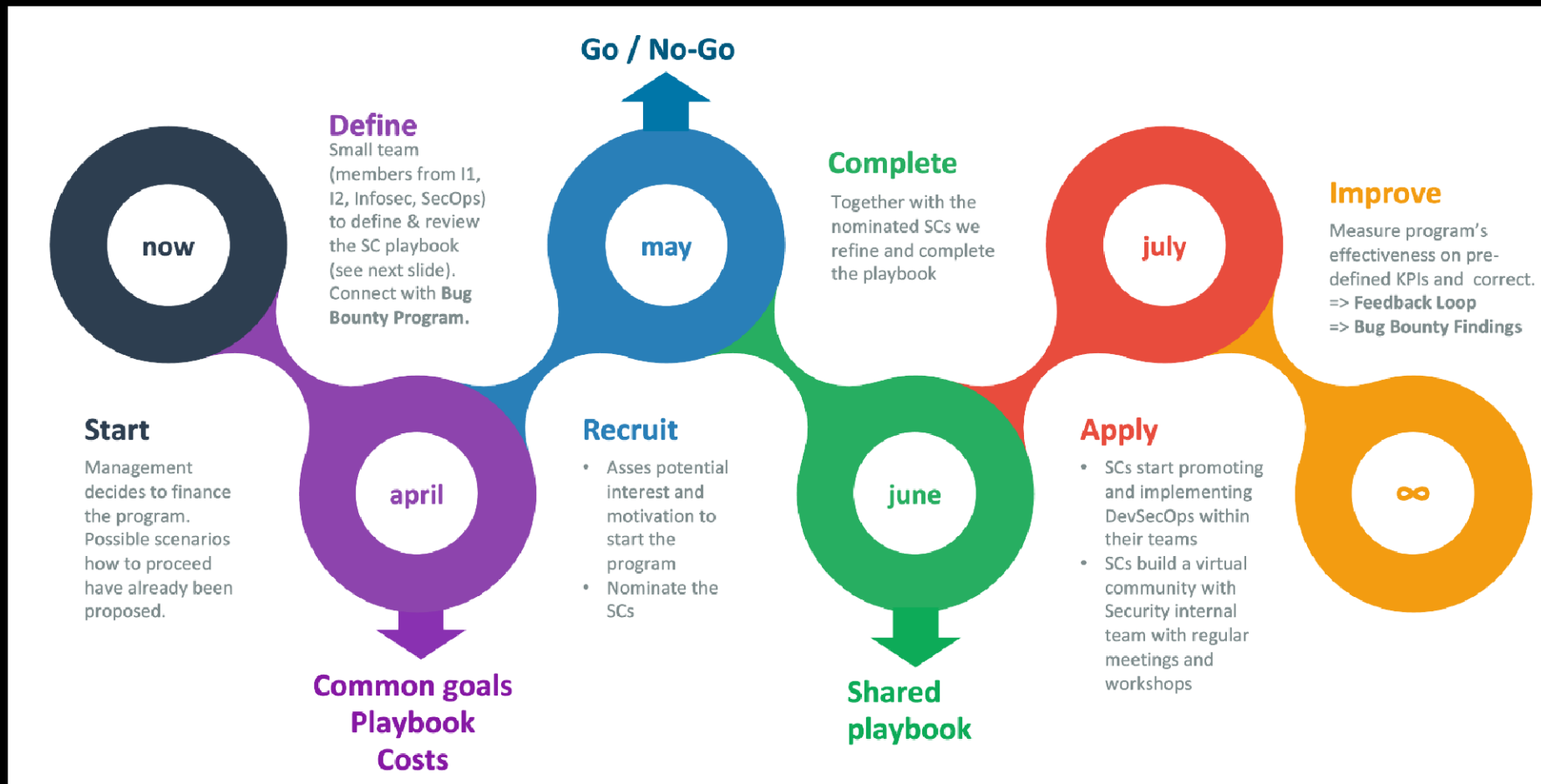
**This proposal has been presented at end of
February 2020**

The proposal



We didn't reinvent the wheel!

Playbook



Timeline 2020

Goals:

- Personal training
- Promote the community
- Follow the playbook
 - BugBounty cases
 - Improve toolchain for secure development

More information:

- Activity rate from 10 to 20% for the SCP.
- SC Team should grow with the time (~10)
- Embedded core team will guide the program.
- The SCs meet regularly (every two weeks for a 2-hours).



I've **joined** the program at end of 2020

Insights 2020

Goals:

- BugBounties
- Trainings
- Recruit (~20)

More information:

- During 2021, the Security Champions gained visibility.
- SCs could add annual objectives linked to Cybersecurity.
- Trainings has been organized for the newbies.
- SCs were invited to take part in Security Day.
- A presentation slot has been reserved for SCP in the INFORM.
- The first Security Champion Day has been organized.



24 November 2021

(or the 9 December 2021)

Insights 2021

Goals:

- One Voice! (SC Community publicity)
- DevSecOps Toolchain
- Threat Modeling Introduction
- Promote Coding best practices (Hitchhiker's Guide)
- Recruit (~30)

More information:

- Promote the program (LeHack, Hacktober, TechTalks).
- Working closely with different teams (WAF / ISO).

Hacktober
Hacktober
Hacktober



Insights 2022

Goals:

- Collaboration with ISOs and Clusters
- Threat Modeling
- Continue promote Coding best practices (Hitchhiker's Guide)
- Provide a cybersecurity training program
- Represent the Swisspost at cyber security conferences
- Recruit (~60)

More information:

- Redefinition of the role of the Security Champion according to the company's needs.
- Improved onboarding process for Security Champions.
- Improved documentation for the Security Champion program.



We've laid a good **foundation, which allows us to add easily the next stones.**

Insights 2023



Six key principles to run a **Great
Security Champion Program**

Swisspost's Manifesto



Be passionate about security

Thank you Marcel!



Start with a clear vision for your program



Secure management support / Trust your champions (team)



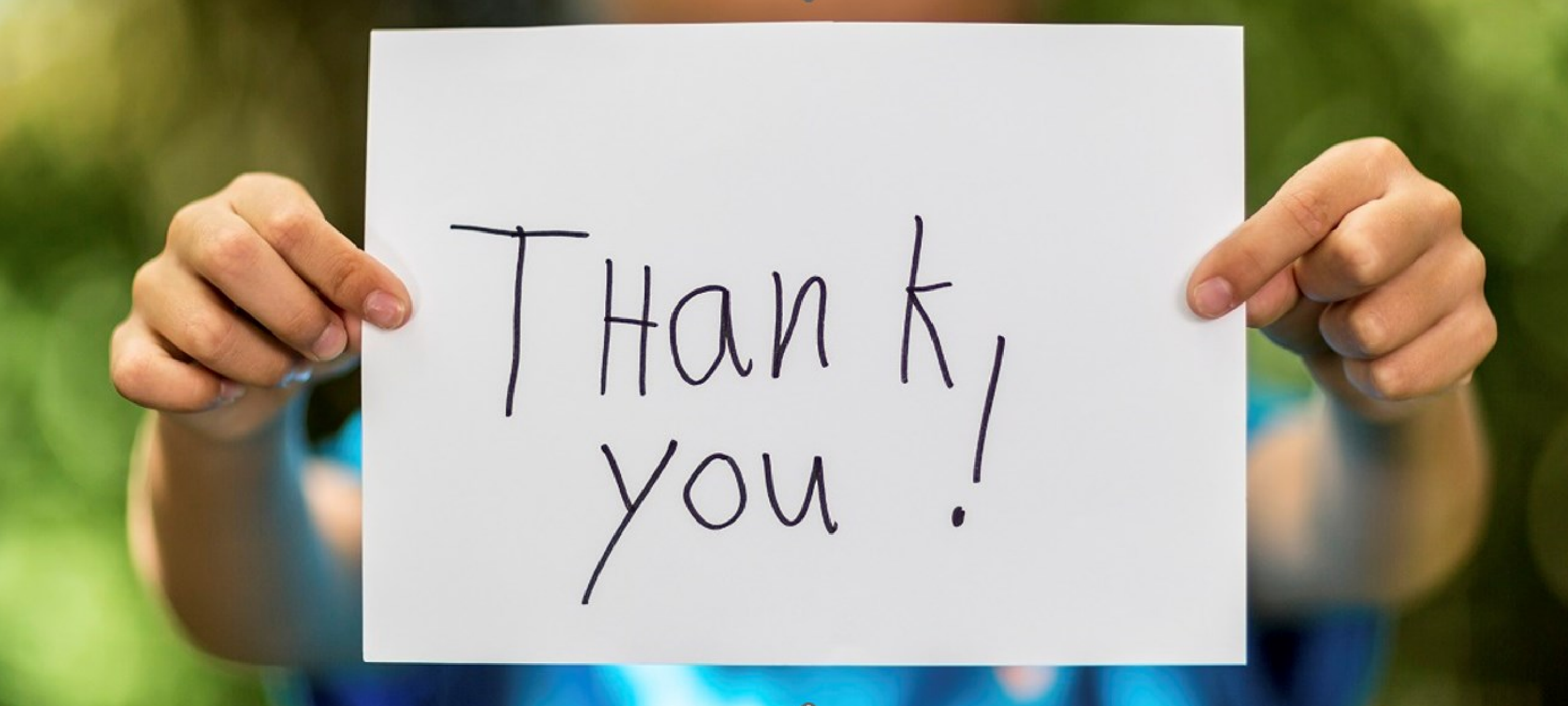
Create a community



Create a community



Promote knowledge sharing

A close-up photograph of a person's hands holding a white rectangular sign. The sign has the words "Thank you!" written in a dark blue, handwritten cursive font. The background is a blurred green and blue, suggesting an outdoor setting. The person's hands are visible on the left and right sides of the sign, gripping the edges.

Thank
you!

Reward responsibility

It's important to...

- Find motivated people.
- Clearly define the vision (and regularly checks).
- Give your trust to your Champions.
- Promote the Community.
- Encourage information sharing and trainings.
- Say Thank you!



Conclusion



Any questions?