Security Champions

Sikkerhetsfestivalen 2023


Improving the Chances of Success in Secure Software Development

Operationalising security work in DNB

Introduksjon til «Security Champions» – Hva, hvorfor, og hvordan?


OBOS S-SDLC og veien til et Security Champions program


Sikkerhet for utviklere med Security Champions i NAV


Oslo Origo og sikkerhetstesting - hvorfor og hvordan gjør vi det?


Improving the Chances of Success in Secure Software Development

Operationalising security work in DNB

Introduksjon til «Security Champions» – Hva, hvorfor, og hvordan?


OBOS S-SDLC og veien til et Security Champions program


Sikkerhet for utviklere med Security Champions i NAV


Oslo Origo og sikkerhetstesting - hvorfor og hvordan gjør vi det?

Introduksjon til «Security Champions»

– Hva

Sikkerhetsfestivalen 2023

Julian Ravn Thrap-Meyer

Introduksjon til «Security Champions»

– Hva, hvorfor

Sikkerhetsfestivalen 2023

Julian Ravn Thrap-Meyer

Introduksjon til «Security Champions»

– Hva, hvorfor, og hvordan?

Sikkerhetsfestivalen 2023

Julian Ravn Thrap-Meyer

Julian Ravn Thrap-Meyer

Utvikler og Security Champion

Utvikler i 12 år // USIT/UiO, Tripletex/Visma, **NAV IT**

Sikkerhetsentusiast

Fritidshacker

Security Champions Norge

Julian Ravn Thrap-Meyer

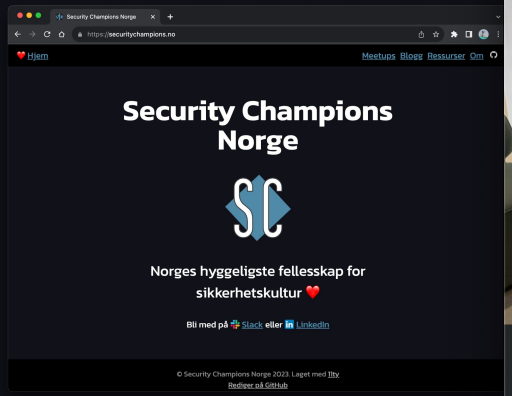
Utvikler og Security Champion

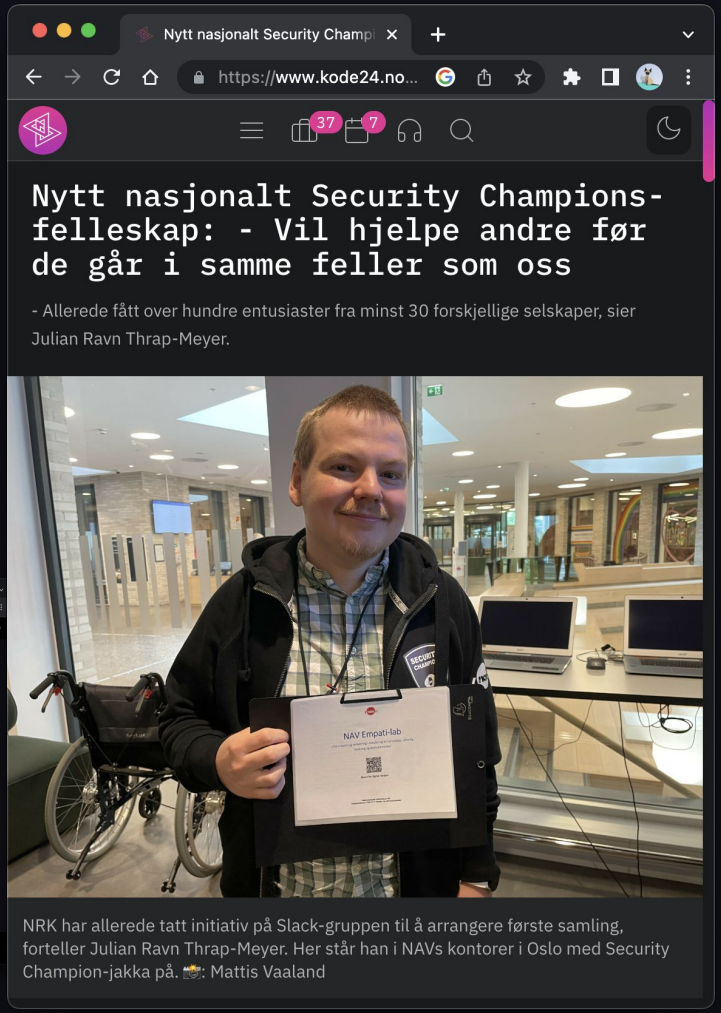
Utvikler i 12 år // USIT/UiO, Tripletex/Visma, **NAV IT**

Sikkerhetsentusiast

Fritidshacker

Security Champions Norge





Julian Ravn Thrap-Meyer

Utvikler og Security Champion

Utvikler i 12 år // USIT/UiO, Tripletex/Visma, NAV IT

Sikkerhetsentusiast

Fritidshacker

Security Champions Norge

Hva er Security Champions?

Skalering av sikkerhetsarbeid

i større organisasjoner

Skalering av sikkerhetsarbeid

på tvers av uavhengige team

Skalering av sikkerhetsarbeid

i det daglige

Skalering av sikkerhetsarbeid

for utviklere i det daglige

Bevissthet
om sikkerhet

for utviklere i det daglige
for produkteiere i det daglige
for QA i det daglige
for ... i det daglige

Bevissthet
om sikkerhet

for teamet i det daglige

Hva er ikke Security Champions?

en dedikert stilling

en sikkerhetsekspert*

den eneste som jobber med sikkerhet

sikkerhetsansvarlig

Hva er en Security Champion?

en utvikler
som får sikkerhet inn
i de daglige diskusjonene
og beslutningene

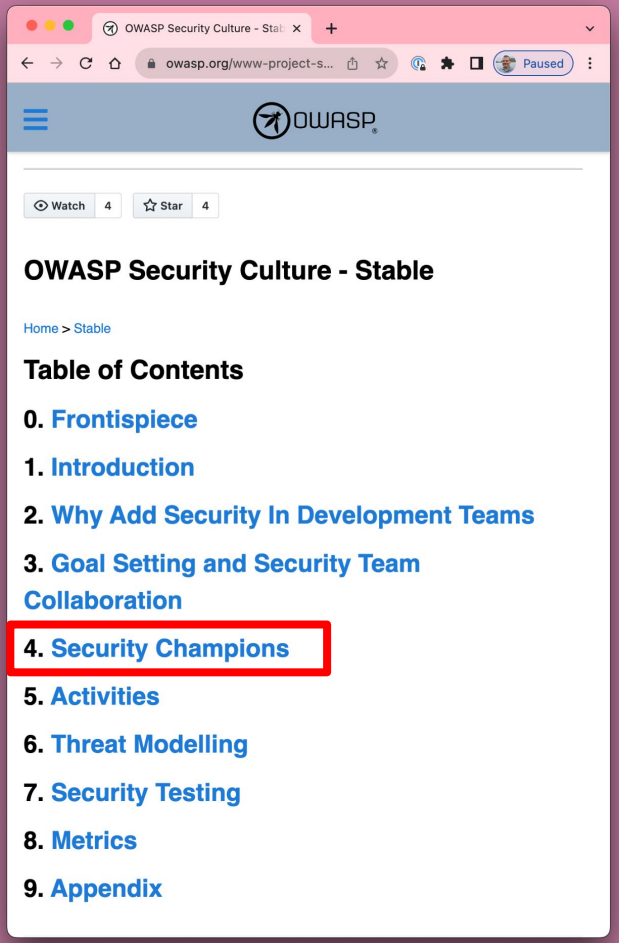
Hvorfor ha Security Champion?

skalere sikkerhet ut til teamene

enklere å nå ut med informasjon

sikkerhetskultur er viktig ❤️

Hvordan få Security Champions?



OWASP Security Champions Playbook

Security Champions playbook

Identify teams

- Enumerate products and services
- List teams per each product
- Identify Product manager (responsible for product) and team manager (working directly with developers)
- Write down technologies (programming languages) used by each team

Define the role

- Measure current security state among the teams and define security goals you plan to achieve in mid-term (e.g. by using OWASP SAMM)
- Identify the places where champions could help (such as verifying security reviews, raising issues for risks in existing code, conducting automated scans etc.)
- Write down clearly defined roles, as these will be the primary tasks for newly nominated champions to work on

Nominate champions

- Introduce the idea and role descriptions and get approvals on all levels - both from product and engineering managers, as well as from top management
- Together with team leader identify potentially interested candidates
- Officially nominate them as part of your security meta-team

Comm channels

- Make sure to have an easy way to spread information and get feedback
- While differing from company to company, this usually includes chats (Slack/IRC channel, Yammer group, ...) and separate mailing lists
- Set up periodic sync ups - bi-weekly should be fine to start with

Knowledge base

- Build a solid internal security knowledge base, which would become the main source of inspiration for the champions
- It should include security meta-team page with defined roles, secure development best practices, descriptions of risks and vulnerabilities and any other relevant info
- Pay special attention to clear and easy-to-follow checklists, as it's usually the simplest way to get the things going

Maintain interest

- Develop your ways or choose one of the below to keep in touch and maintain the interest of the champions
- Conduct periodic workshops and encourage participation in security conferences
- Share recent appsec news (e.g. Ezine) via communication channels
- Send internal monthly security newsletters with updates, plans and recognitions for the good work
- Create champions corner with security library, conference calendar, and other interesting materials

https://owasp.org/www-project-security-culture/v10/4-Security_Champions/


Identify teams
Define the role
Nominate champions
Comm channels
Knowledge base
Maintain interest

Identify teams

dagens sikkerhetstilstand

Define the role

hva trenger dere?

Nominate champions

frivillig > tvang

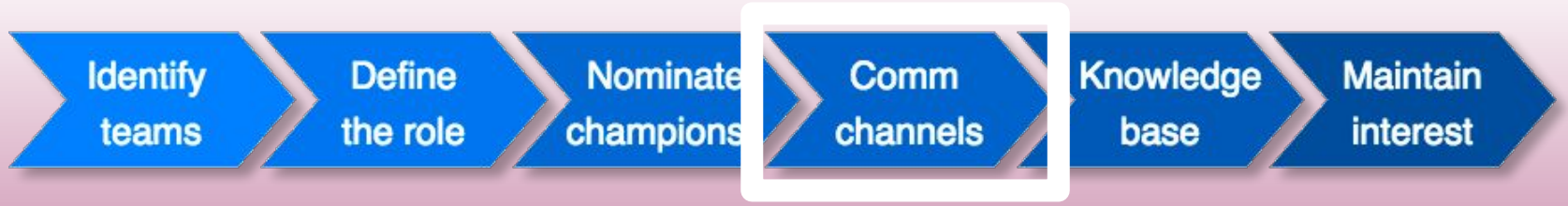
kvalitet > kvantitet

Nominate champions

frivillig > tvang

kvalitet > kvantitet

snakk høyt om det!

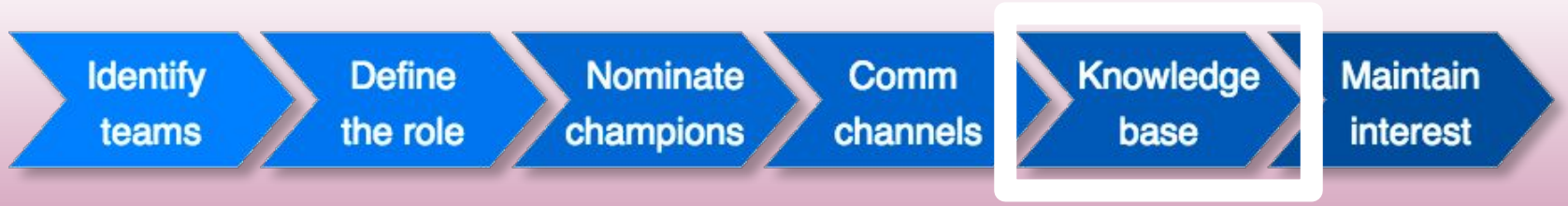


Comm channels

vær tydelig

Comm channels

vær tydelig
båndbredde



Knowledge base

felles hukommelse

ett sted å huske

kurateterte ressurser

Knowledge base

felles hukommelse

ett sted å huske

kurateterte ressurser

enkelt å redigere!

✅ Del 1

«Den lette biten»

Maintain interest

… den vanskelige biten

Maintain interest

Gøy!

CTF

Kurs

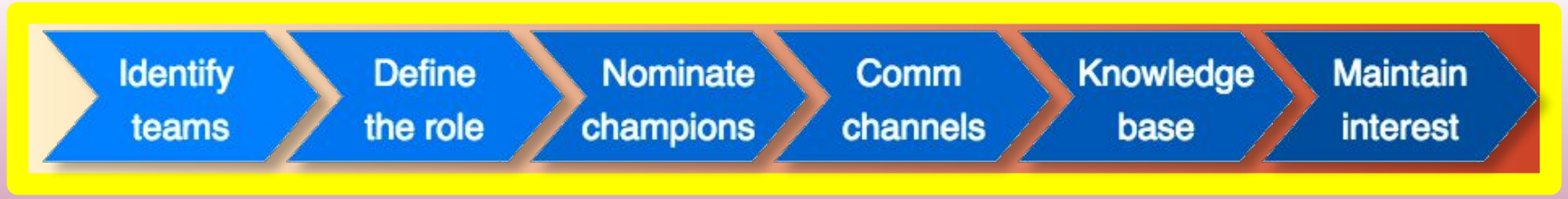
Workshops

Heder og ære

Meetups

Gamification

Måling



Gratulerer! 🎉

Du har nå Security Champions

Bør du ha Security Champions?

Ja!

Så lenge du har …

… sikkerhetsfolk

… flere team

… tid og kapasitet

Lykke til! 🚀

securitychampions.no

Takk!

securitychampions.no

Lillehammer kino sal 2, kl. 10.45: