

OWASP GLOBAL AppSec

ViE'26
NNA JUN
25-26

25

years
of open source security

SECURITY CHAMPIONS: LESSONS FROM OPPOSITE TRENCHES

BY LISI HOCKE & MIREIA CANO

Lessons from Building and Being a Champion



Mireia Cano

mee-re-yaa

AppSec Engineer @ PPRO



@m1r314@infosec.exchange



mireiacanopujol



Lisi Hocke

lee-see

Security Engineer @ DocuWare



@lisihocke@mastodon.social



@lisihocke.bsky.social



lisihocke



www.lisihocke.com



DISCLAIMER

What are Security Champions?

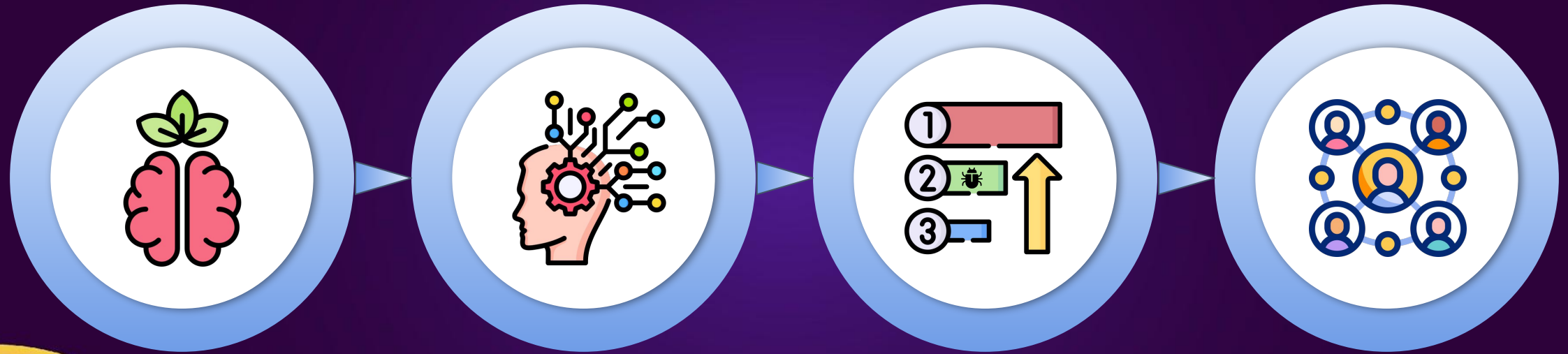
Someone not part of
the security team



Communicator between their
team and the security team

Advocating for security in their team

What you can expect



Starting point:

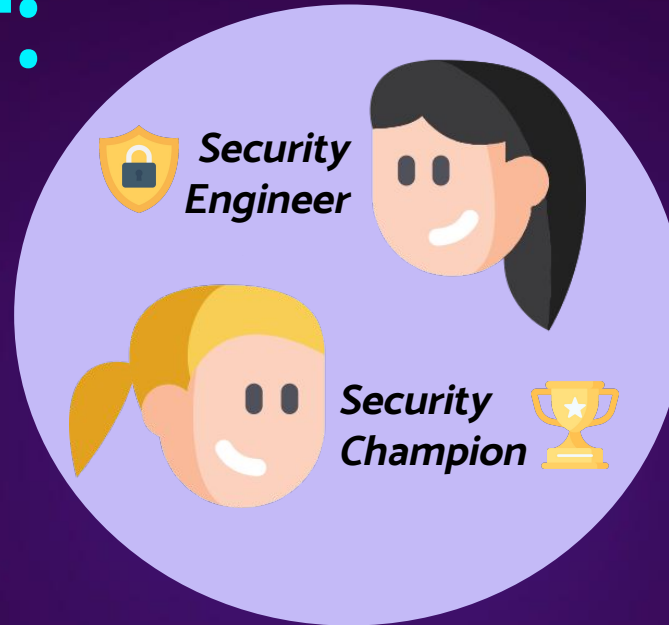
Program
already in place

Champions are
volunteers

SECURITY CHAMPIONS: LESSONS
FROM OPPOSITE TRENCHES

Running for
some time

Starting point:



Security and Champions in Opposite Trenches



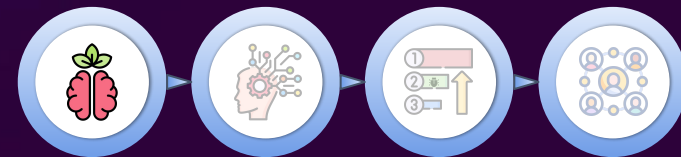
Psychological Safety

“Shared belief held by members of a team that the team is safe for interpersonal risk taking.”

– Amy Edmondson (1999)
Psychological Safety and Learning Behavior in Work Teams

https://web.mit.edu/curhan/www/docs/Articles/15341_Readings/Group_Performance/Edmondson%20Psychological%20safety.pdf

1



Myths about Psychological Safety

~~“It’s about being nice and
feeling comfortable”~~

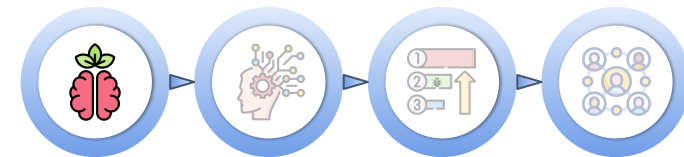
It’s about creating the space so everyone can take the risk to bring up deeply uncomfortable topics

~~“It’s static”~~

It does not arise from a single measure but from repeated experience

~~“It’s an individual trait”~~

It’s a shared belief



How can we create a psychologically safe space for security champions?



Vulnerability

- Having the courage to show up when you can't control the outcome
- It's always hard to be the first one, but you need to show up without an armor



Empathy

- Understand the position Champions are in
- Seek context before jumping to conclusions
- Empathy builds allies

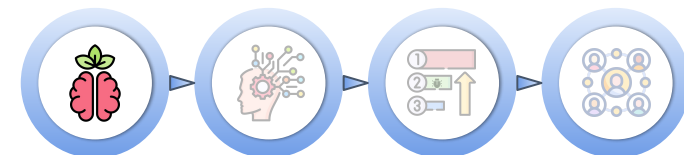


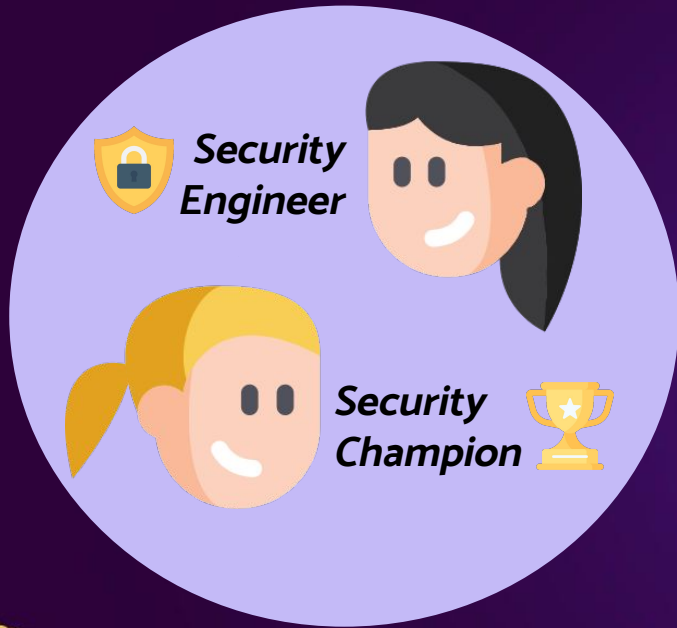
Environment

Co-create rules to foster safety

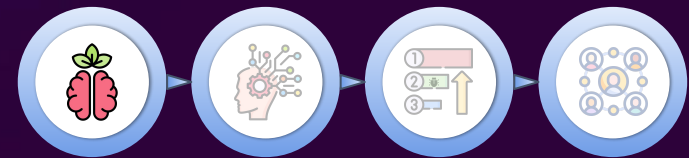
- No recordings
- What happens among us, stays among us
- No managers
- Level playing field so background is irrelevant

Psychological safety is a prerequisite for success





Security and champions feel safe enough to get out of the trenches



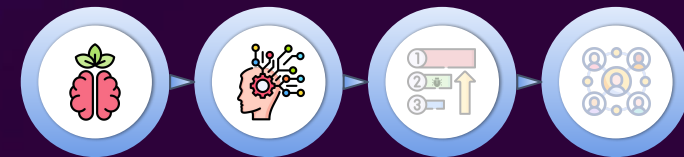


Beware of the Champions' Cognitive Load

Cognitive load: effort being used in the working memory

– John Sweller (1988)
*Cognitive Load During Problem Solving:
Effects on Learning*

https://en.wikipedia.org/wiki/Cognitive_load



Types of Cognitive Load and How We Can Help



Intrinsic

Related to the inherent complexity of a topic

- We cannot change this
- We can break tasks and topics up into smaller pieces to reduce the load



Extraneous

Related to how information or tasks are presented or handled

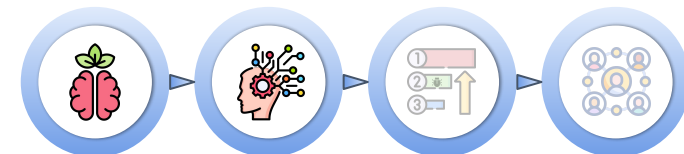
- Controllable
- Can and should be reduced as much as possible



Germane

Connecting new information to existing knowledge, and into long-term memory

- Good kind of load
- Effort that goes into actual learning, so optimize for it



Applying Cognitive Load Theory to Security Champions

Consider cognitive load in all your actions

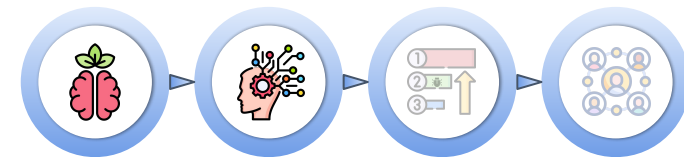
Trainings

Design of the champion's
program itself

Documentation and
processes

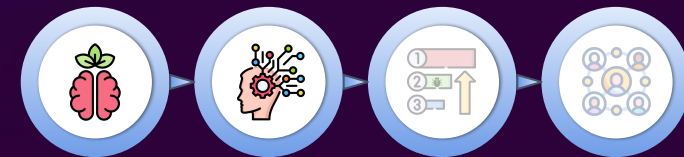
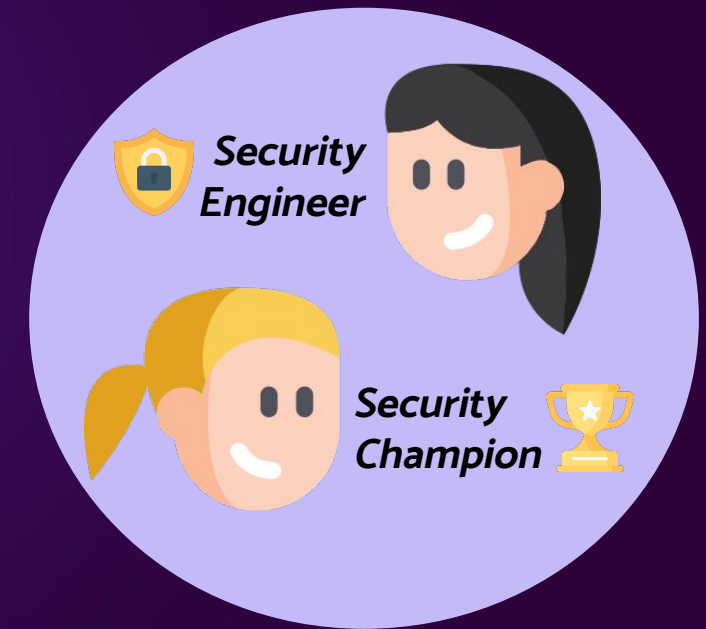


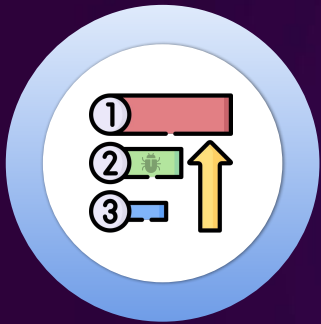
Both as security and as champions!



Security and champions collaborate and prevent mental overload

SECURITY CHAMPIONS: LESSONS
FROM OPPOSITE TRENCHES



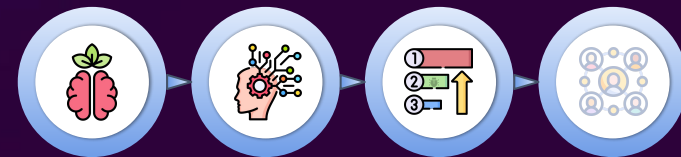


Leading Without Formal Authority

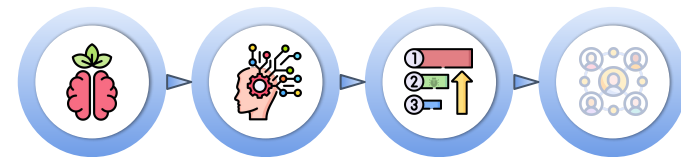
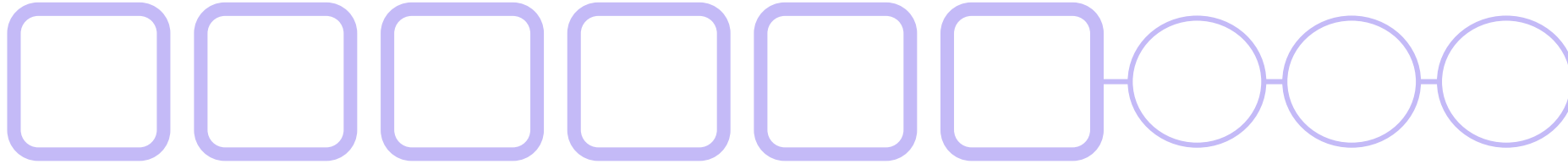
Security: champions are not their direct reports

Champion: no formal authority over their teammates or team priorities

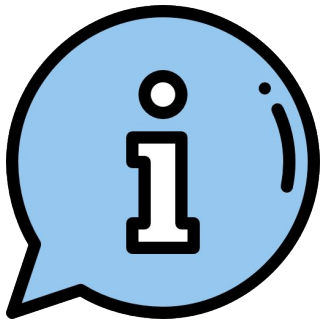
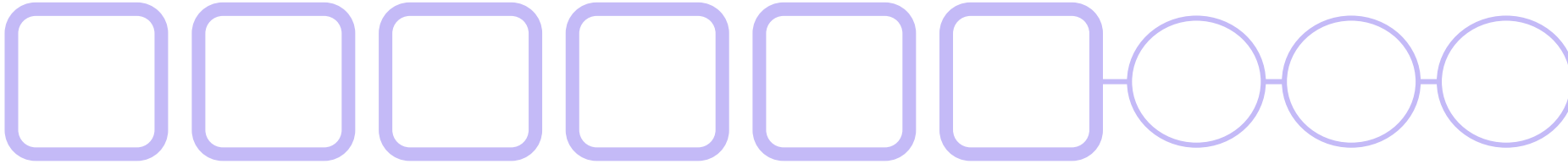
3



Power Bases according to French & Raven

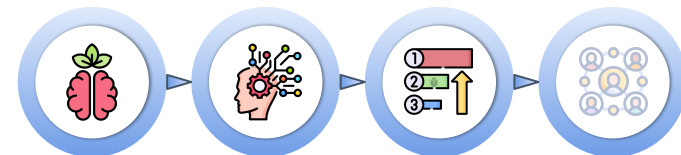


Power Bases according to French & Raven

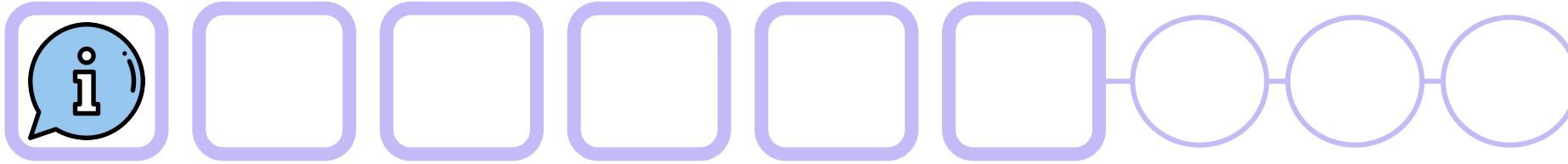


The information you provide then results in cognitive change and acceptance by the other person

Information Power

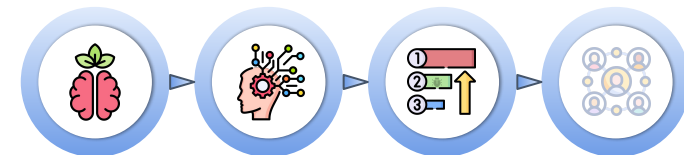


Power Bases according to French & Raven

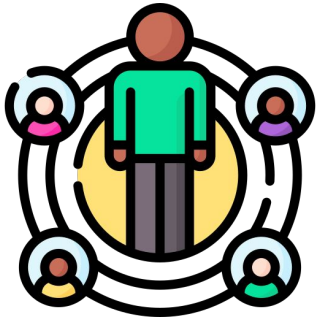
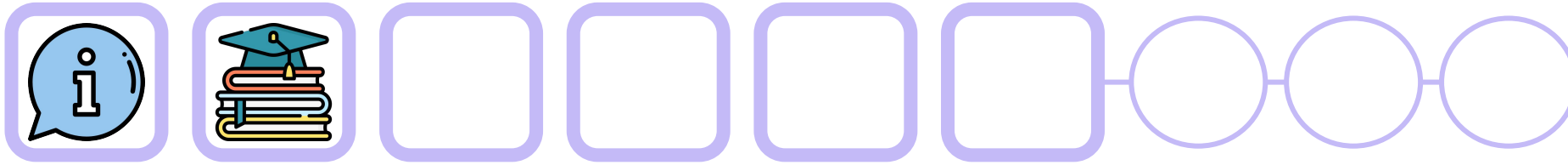


Expert Power

Expert power results from the other person's faith that you have some superior insight or knowledge about what behavior is best under the circumstances

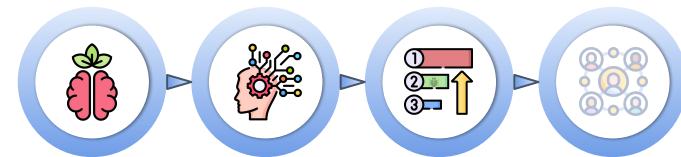


Power Bases according to French & Raven

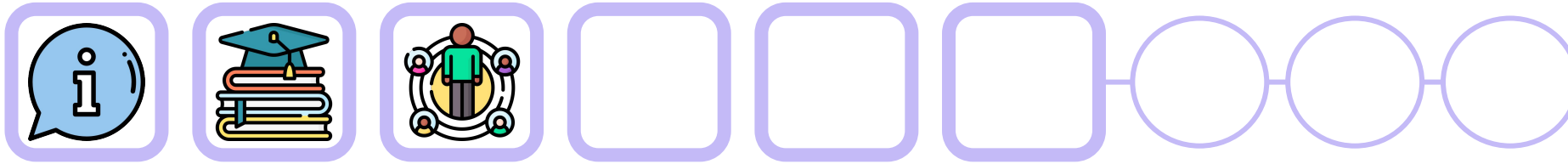


Referent Power

Referent power stems from the other person identifying with us, or seeing us as a role model that they would want to emulate



Power Bases according to French & Raven

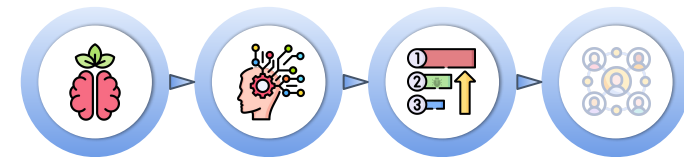


Reward Power

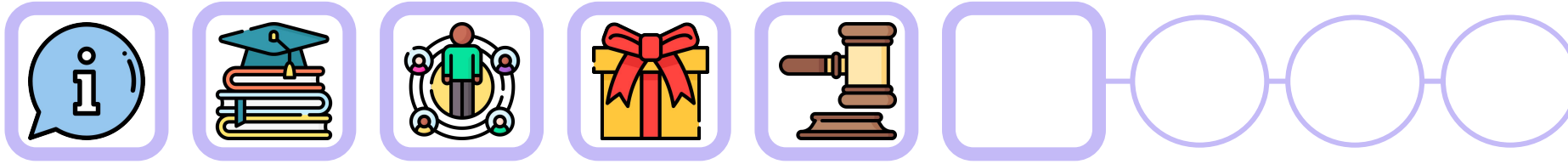


Coercive Power

Comes from the ability to offer a positive incentive if the other person complies, or punish if they don't

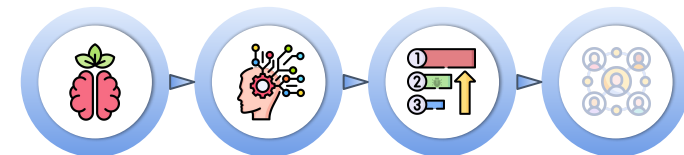


Power Bases according to French & Raven

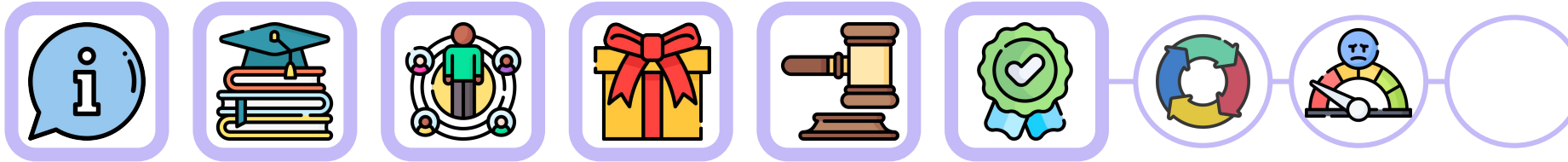


Legitimate Power

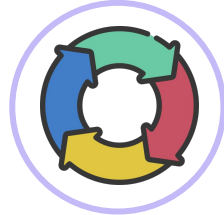
Legitimate power stems from the person accepting that you have the right to require the changed behavior, and the person is obliged to comply



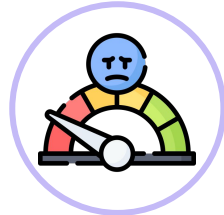
Power Bases according to French & Raven



Legitimate Power



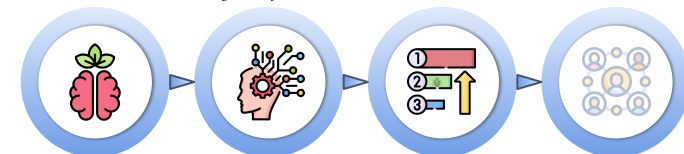
Power of reciprocity: you do someone a favor, they feel an obligation to reciprocate



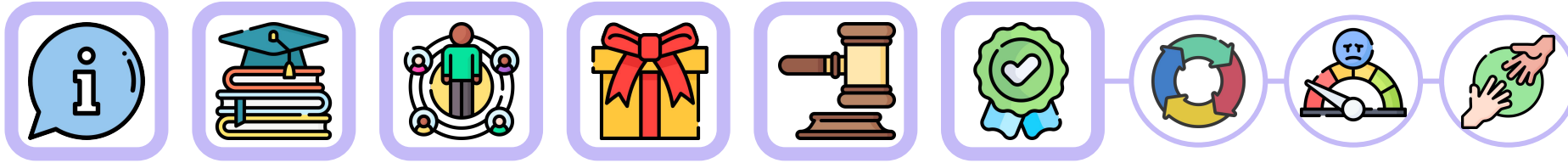
Power of equity: people believe you've experience unfair things and have a right to compensation



Power of responsibility: you're perceived as helpless and people feel the need to help you

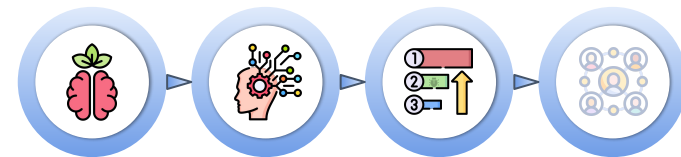


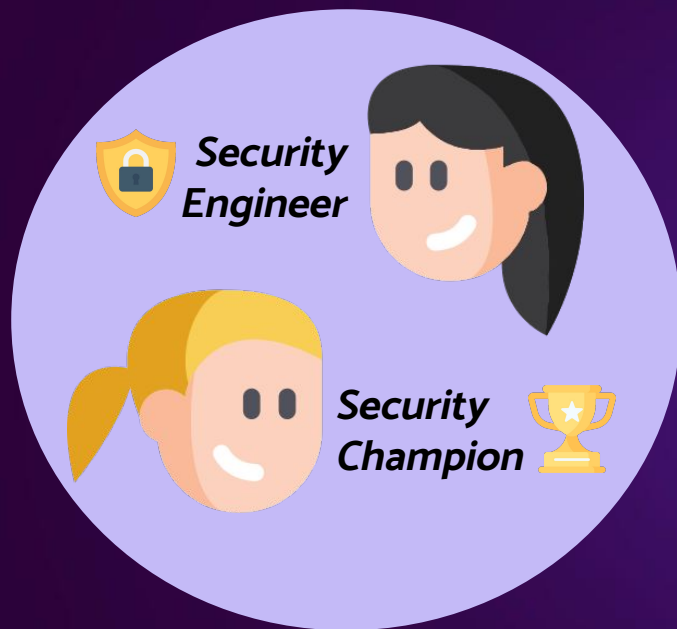
Power Bases according to French & Raven



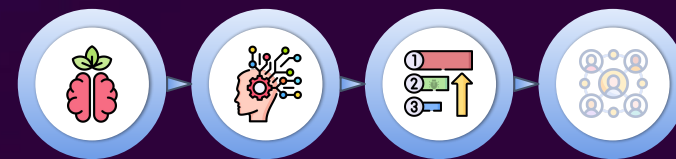
You might not use all of them yet, but you can cultivate each of these power bases

Tap into more power sources to effect change





Security and champions use their power to drive change together





Champions Community

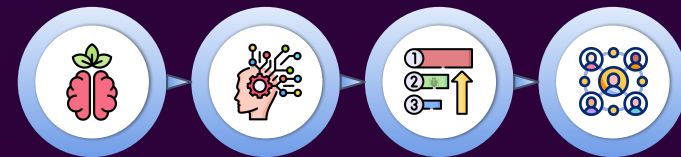
Security will always be the bottleneck unless the security champions build a strong and resilient network

Community of Practice: A group of people connected by a shared passion for something they practice, who collectively improve as they interact regularly.

– Emily Webber (2025)

<https://emilywebber.co.uk/building-communities-of-practice-that-amplify-the-flow-of-learning-across-organisations/>

4



How do we build a community?

Incentivize knowledge sharing among champions

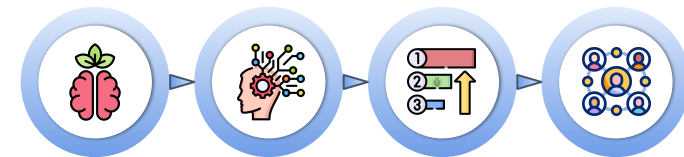
- Reinforce eager champions
- Give a little push to ones who only share with you
- Connect them!

Have events to bring champions together

- Conferences
- Security news review
- Lean coffee sessions

Co-create the community with the champions

Members are more invested and engaged if they helped shape the program



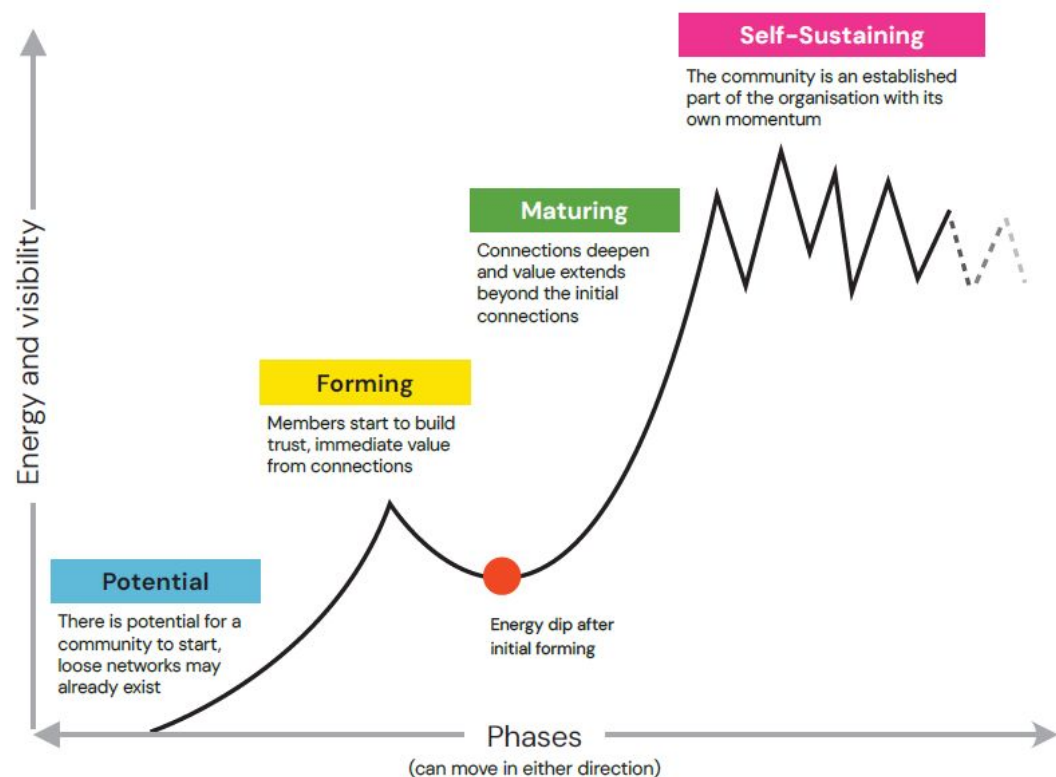
A Community Evolves over Time



Tacit's Community of Practice Maturity Model

<https://hellotacit.com/community-of-practice-maturity-model/>

V 4.9



About this model

The Tacit Community of Practice Maturity Model identifies the different phases of a community of practice and highlights areas that can help it progress towards self-sustaining.

The content is based on research and experience across different organisations over several years. But is generic and you may need to review and adapt it to your own situation.

Version 1 of the model appeared in the book *Building Successful Communities of Practice: Discover How Connecting People Makes Better Organisations*

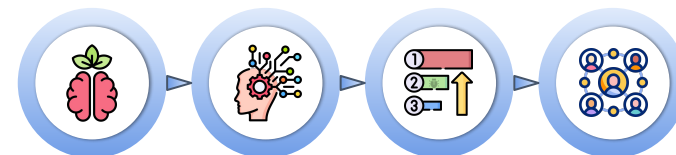
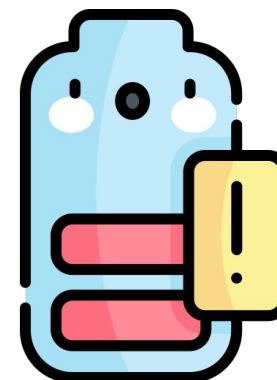
Find out more at hellotacit.com/publications

The latest version of this model is available at tacit.pub/copmaturitymodel

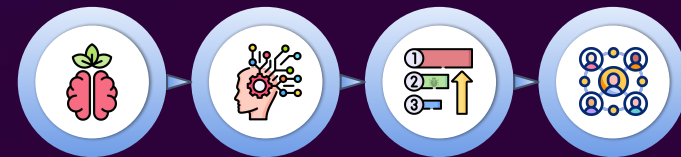
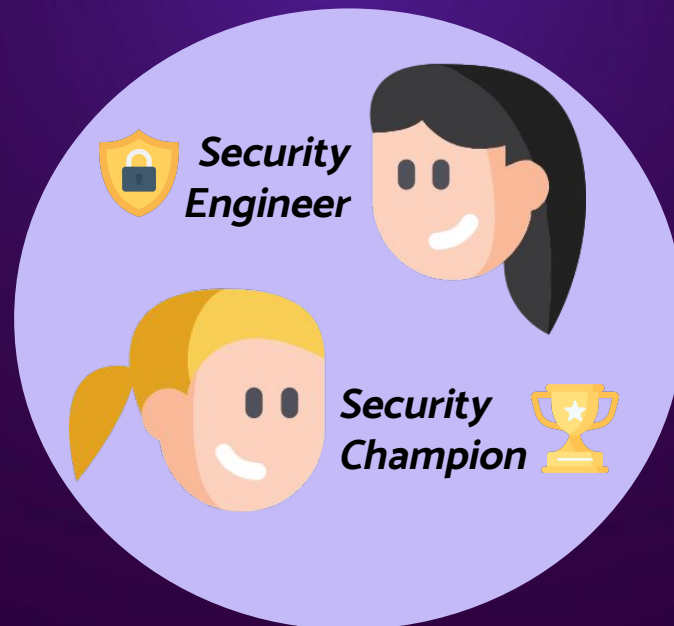
Looking for support to embed, train or supercharge your communities of practice? Get in touch at hellotacit.com

Graph adapted from Cultivating Communities of Practice Wenger, McDermott and Snyder (2002)

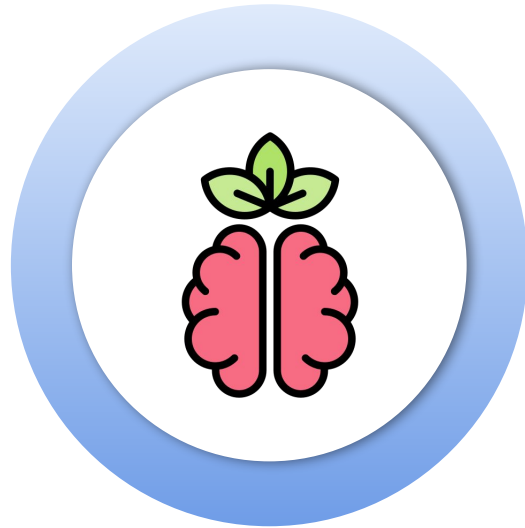
Energy dips are real – watch out for them and find ways to move beyond them



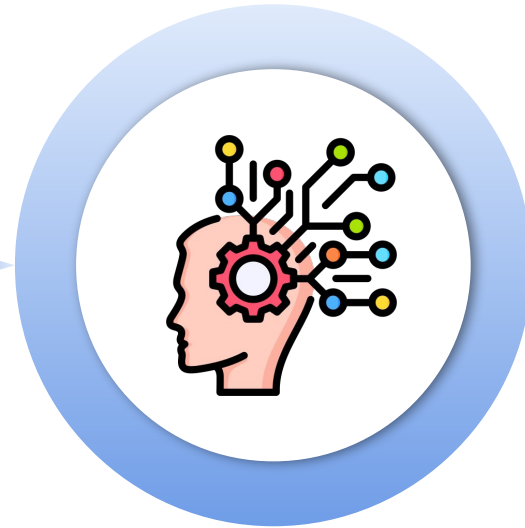
We co-created a strong and resilient champions community



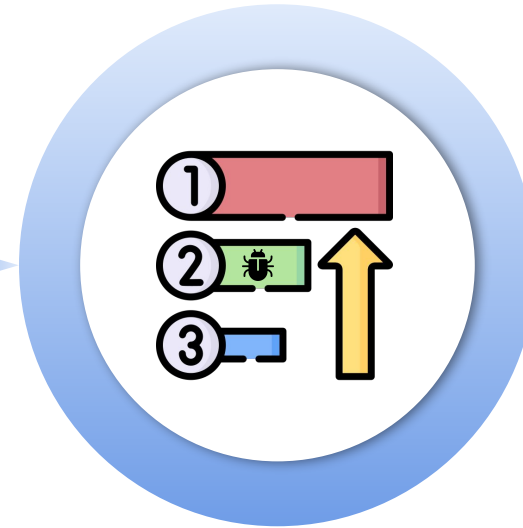
Takeaways



**Foster
Psychological
Safety**



**Consider
Cognitive Load**



**Tap Into More
Power Sources**



**Build
Champions
Community**

Recommended Resources

Security champions: <https://www.lisihocke.com/p/security.html#champions>

Psychological safety:

- <https://www.lisihocke.com/p/inclusion.html#psychological-safety>
- Book “The Fearless Organisation” by Amy Edmondson:
<https://fearlessorganizationscan.com/the-fearless-organization>

Cognitive load: Talk “Human Buffer Overflow: How To Deal With Cognitive Load In High-Performing Teams - Juliane Reimann”: <https://www.youtube.com/watch?v=5Lp5lut7uVs>

Leadership, power, and influence:

- <https://www.lisihocke.com/p/leadership.html#influence>
- Book “Dare to Lead” by Brené Brown: <https://brenebrown.com/book/dare-to-lead/>

Communities of practice: Book “Building Successful Communities of Practice” by Emily Webber:
<https://hellotacit.com/building-successful-communities-of-practice-second-edition/>



VIENNA'26 JUN
25-26



THANK YOU!

Icons in this presentation are made by [Dewi Sari](#), [Freepik](#), [HAJICON](#), [Iconjam](#), [juicy_fish](#), [Three musketeers](#), [Wichai.wi](#), [vectors-market](#) from Flaticon.com