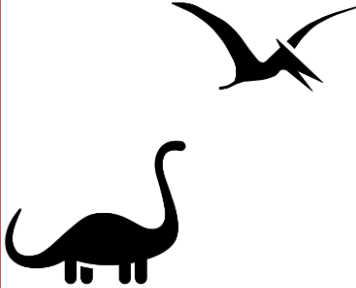




Starting the DevSecOps journey

Software Engineer

1994



Agile, Lean, Scrum

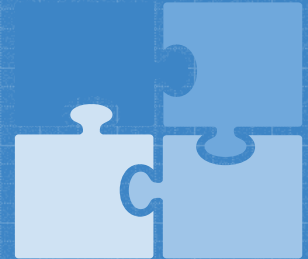
2008: process

2014:
ScrumMaster

Security

2011:
Secure
Development
2014:
Pen Testing

AppSec



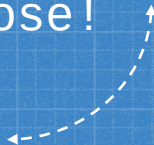
T: @IreneMichlin



1

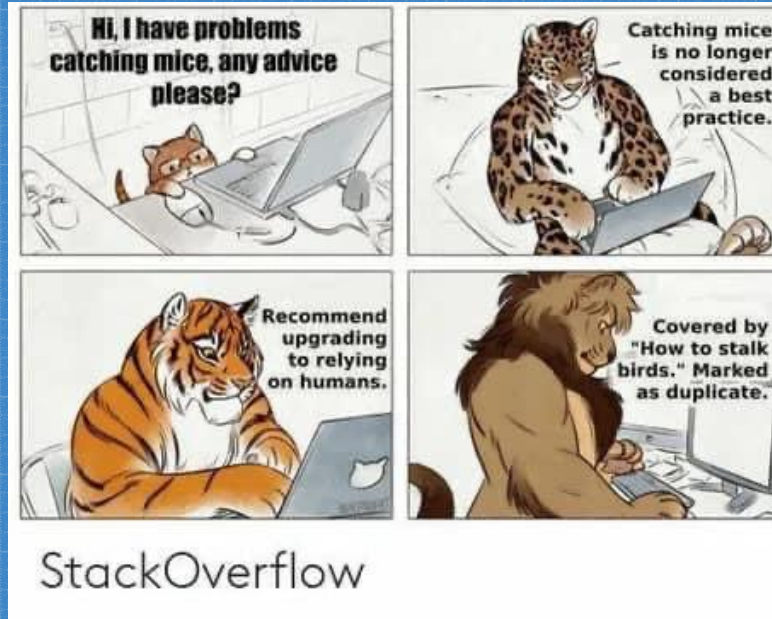
FAANG or MAMAA?

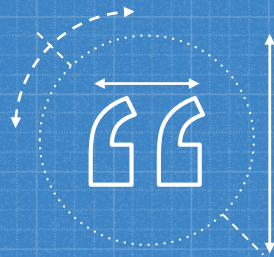
Most security engineers
don't work for those!



There is a lot of security advice available

Most of it goes like that:





**What hiring in security cannot help with
is engineering culture; culture is set by
the founders and early engineers.**

<https://devd.me/log/posts/startup-security/>

Principles of (security)-[:INTERACT]-(engineering)

- Security team **TRUSTS** that engineering teams **want to do the right thing**
- Security team **KNOWS** that engineering teams are closer to the business context and can make better **trade-off decisions** between security and other considerations of user success
- Security team **PLEDGES** to provide information and advice so that trade-off decisions are **more informed**
- Security team **AIMS** to lower the cost/effort side of introducing secure development tools or practices.
Practically speaking, we **PLEDGE** to make it easy **before** make it mandatory

Can't have a separate security culture

Aligned to company values

Neo4j's core values reflect how we connect with each other and to the world around us.

<https://neo4j.com/culture/>

Other sources of inspiration

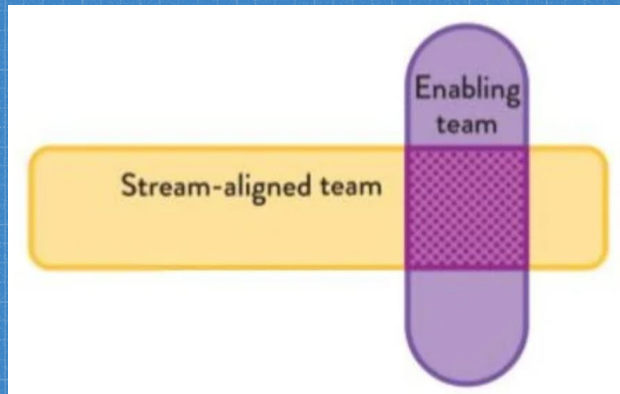
<https://www.rsaconference.com/library/presentation/the-impact-of-software-security-practice-adoption-quantified>

[Application Security | GitLab](#)

Tangent - team topologies

4 fundamental topologies

- Stream-aligned team
- Enabling team
- Complicated Subsystem team
- Platform team



<https://teamtopologies.com/videos-slides/team-topologies-for-security-by-mario-platt-amp-manuel-pais>



2

You promised actionable!

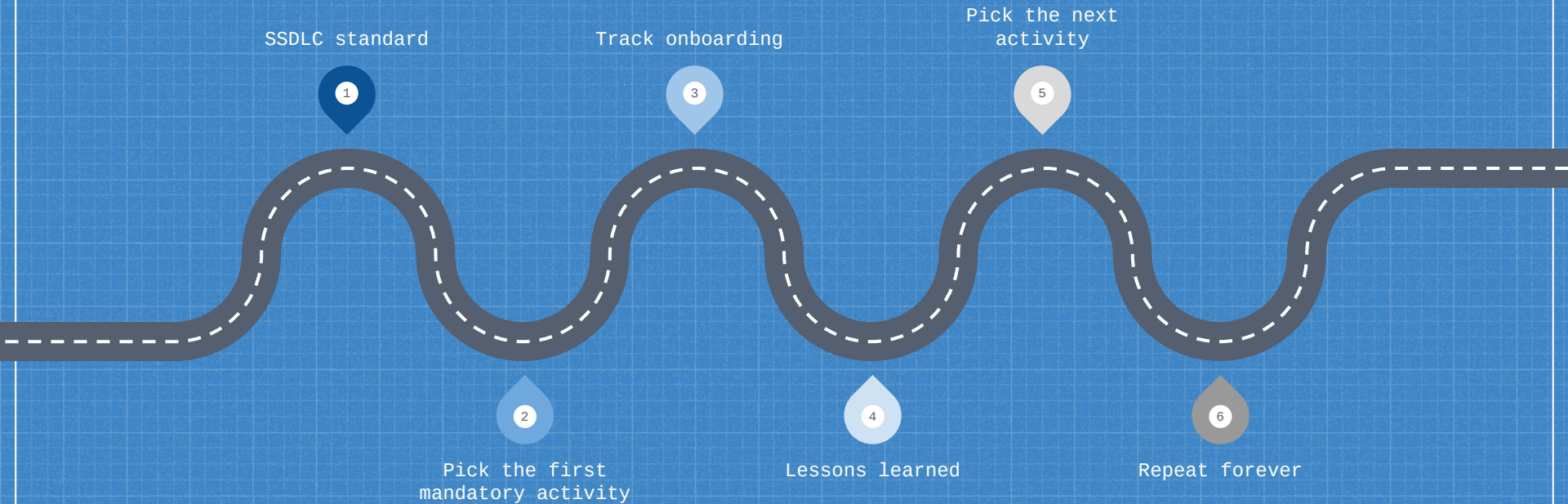
Where is my action plan?

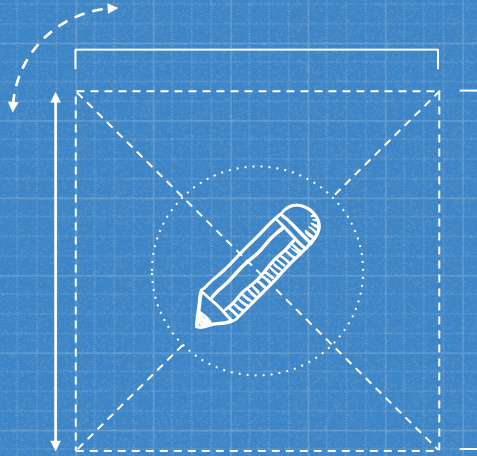


High level list

- Secure development standard
- One (at most two!) mandatory activities
- Track onboarding
- Security champions

ROADMAP

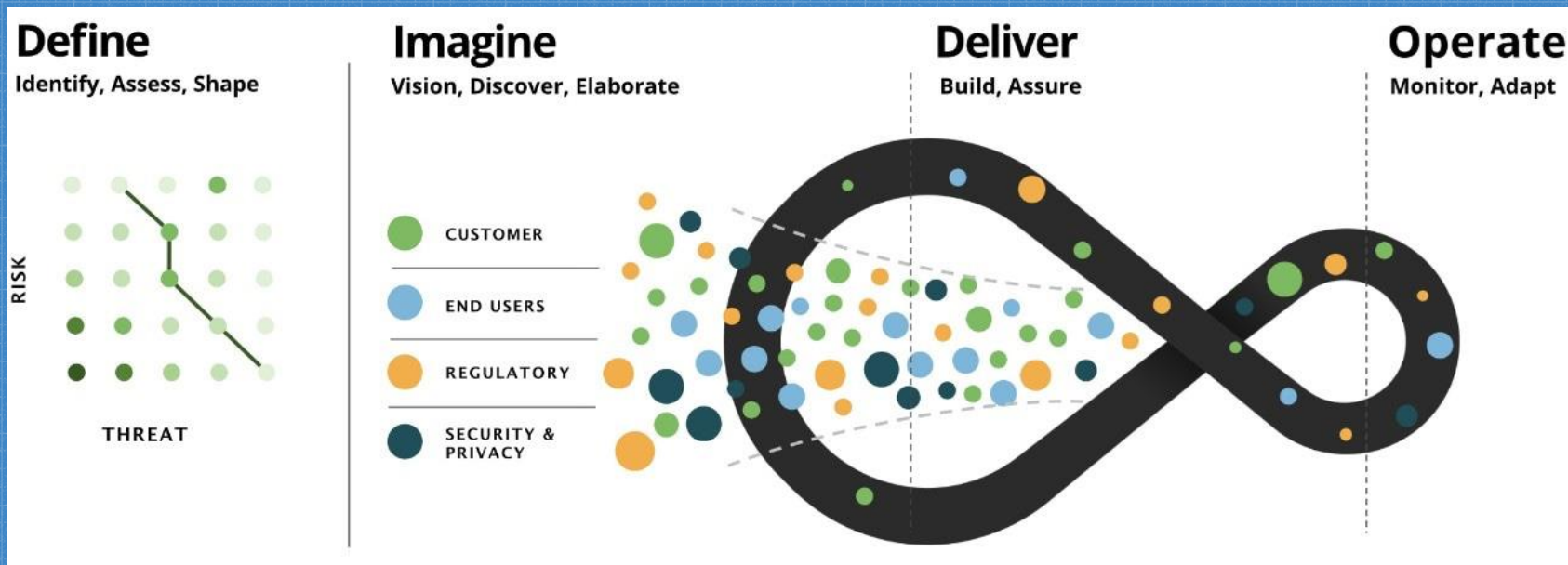




DevSecOps

Where is my infinity loop?

Maybe a better infinity loop?



<https://www.securityjourney.com/post/devops-security-culture-12-fails-your-team-can-learn-from>
<https://www2.deloitte.com/uk/en/blog/cyber-risk/2022/devsecops.html>

Secure Development Lifecycle Standard

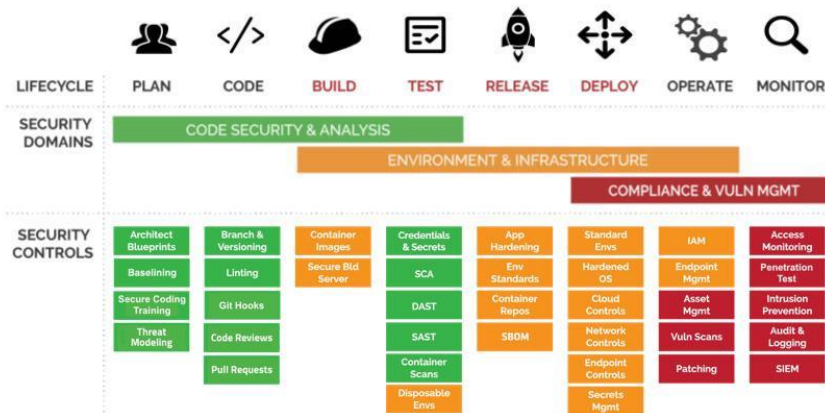
Why? Business will likely ask for it

Structure: align to your actual development process

Depth: keep mandatory bits short, and allow in depth reading

Which security activity to do first?

Framework/ Maturity model	Activities
<u>BSIMM</u>	122
<u>OpenSamm</u>	30? * 3 levels
<u>DSOMM</u>	16 * 4 levels
<u>Playbook</u>	~50 controls



Which security activity to do first?

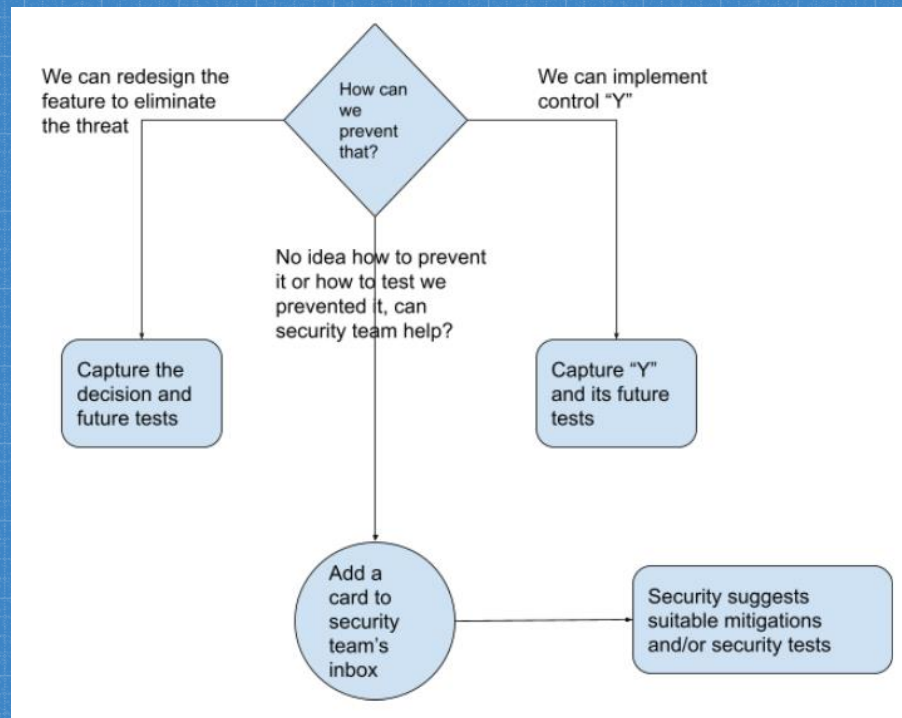
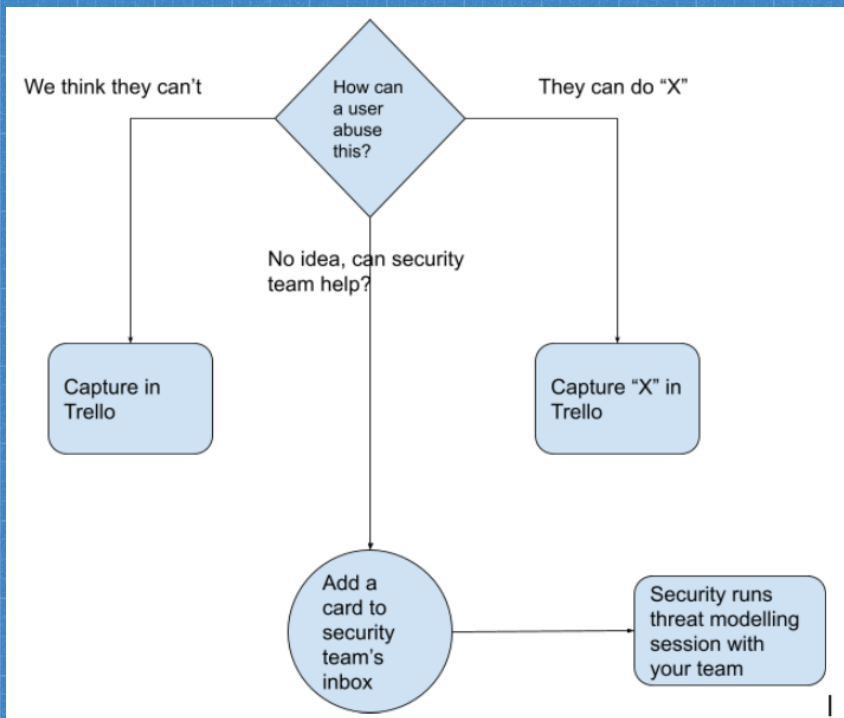
Security prompt:

For each story/backlog item, ask:

How can a malicious user intentionally abuse this functionality? How can we prevent that?

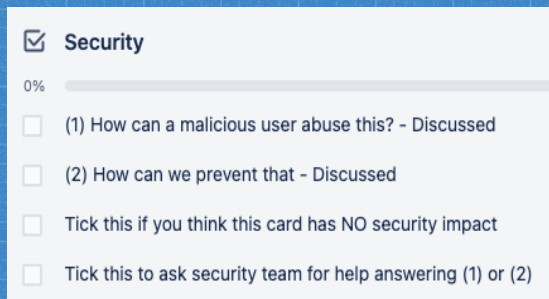
<https://tldrsec.com/blog/insecure-development-why-some-product-teams-are-great-and-others-arent/#the-one-security-prompt>

Example (specific to us!)



Automation (specific to us!)

Checklist appears in the card



☒ **Security**

0%

- ☐ (1) How can a malicious user abuse this? - Discussed
- ☐ (2) How can we prevent that - Discussed
- ☐ Tick this if you think this card has NO security impact
- ☐ Tick this to ask security team for help answering (1) or (2)

For “No Impact” Security team is alerted

when the "Tick this if you think this card has NO security impact" item is checked in a checklist named "Security" by anyone, create a unique card with title "{cardname}" has no security impact? Check {cardlink}" and description "{boardname}" in list "Look at Me" on board "Neo4j Security", and add link "{triggercardlink}"

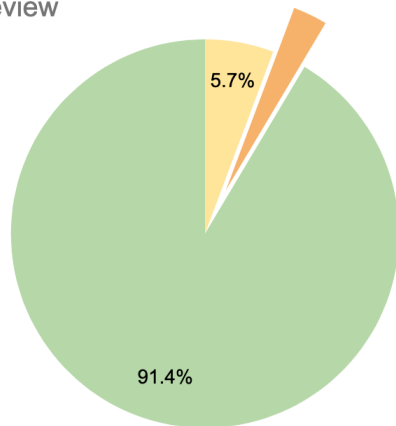
For “Ask for help”

when the "Tick this to ask security team for help answering (1) or (2)" item is checked in a checklist named "Security" by anyone, create a unique card with title "Security Review Request: {triggercardname}" in list "Inbox for security team" on board "Neo4j Security", add the blue "SDLC/AppSec" label to the card, set the card's description to "{boardname}", and add link "{triggercardlink}"

Teams quickly learn to get it right

End of February

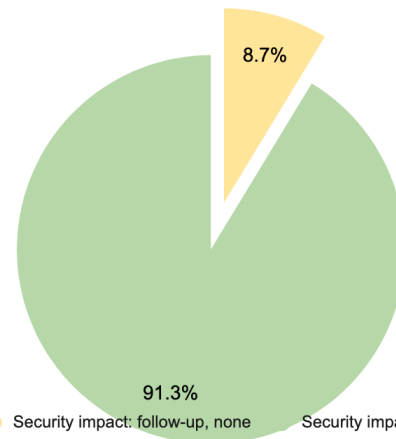
Outcomes of review



● Security impact: follow-up, none ● Security impact: follow-up, found ● Security impact: none

End of March

Outcomes of review



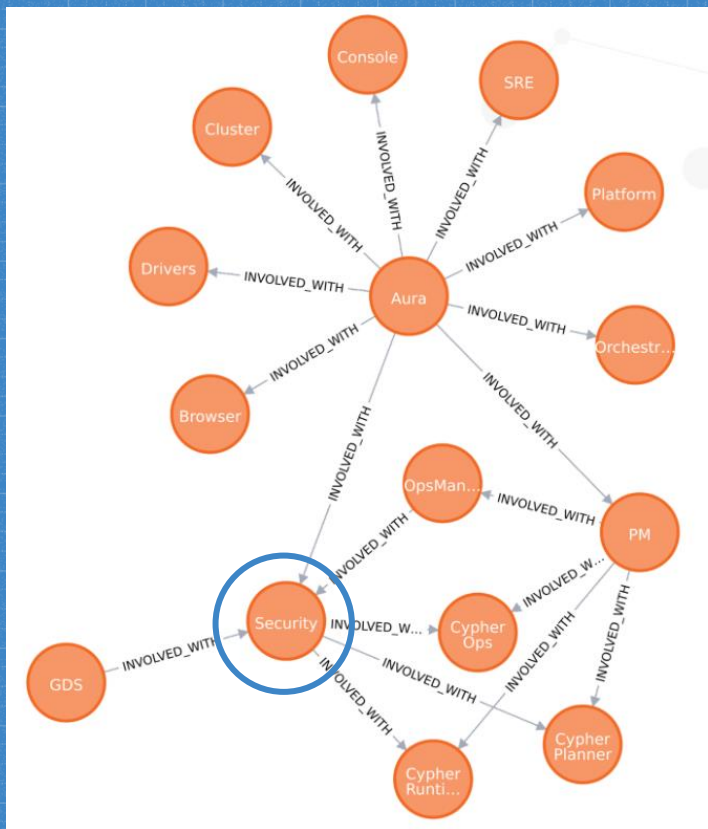
● Security impact: follow-up, none ● Security impact: none

I am preaching bad practice?

- Everybody says “Centralised security reviews do not work”
- Yes, but I am in learning mode. The “secure patterns” phase will come
- Also, I am not a gate

<https://r2c.dev/blog/2021/appsec-development-keeping-it-all-together-at-scale/>

Well-connected team



- We are a graph database company
- “Help the world make sense of data”
- Couldn’t resist making sense of Trello data

Track onboarding

	Security Prompt	SAST	ASVS
Team A			
Team B			
Team C			

<https://www.rsaconference.com/library/presentation/the-impact-of-software-security-practice-adoption-quantified>

Security Champions

- SSDLC - be aware of that's required and encourage the team to follow
- Adapt tools to the team's need
- Share knowledge
- Think about issues proactively
- Drill procedures (incident response, critical update etc)
- Contribute to the newsletter

High level list

- Secure development standard
- One (at most two!) mandatory activities
- Track onboarding
- Security champions

Useful resources

- <https://tldrsec.com/> ← My number one resource
- [Security Champions Playbook v 2.1](#)
- [How to Turn Your Developers into Security Champions](#)
- [DevSecOps Series: Shifting Security Left | by Lucas Kauffman | Medium](#)
- [Security Programs - CloudSecDocs](#)
- [Team Topologies for Security by Mario Platt & Manuel Pais](#)
- <https://www.threatmodelingmanifesto.org>

Thanks !

ANY QUESTIONS?

You can find me at:

@IreneMichlin

irene221b@gmail.com

CREDITS

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash