



A SECURITY CHAMPION'S JOURNEY – HOW TO MAKE THINGS A BIT MORE SECURE THAN YESTERDAY EVERY DAY

LISI HOCKE

@lisihocke@mastodon.social

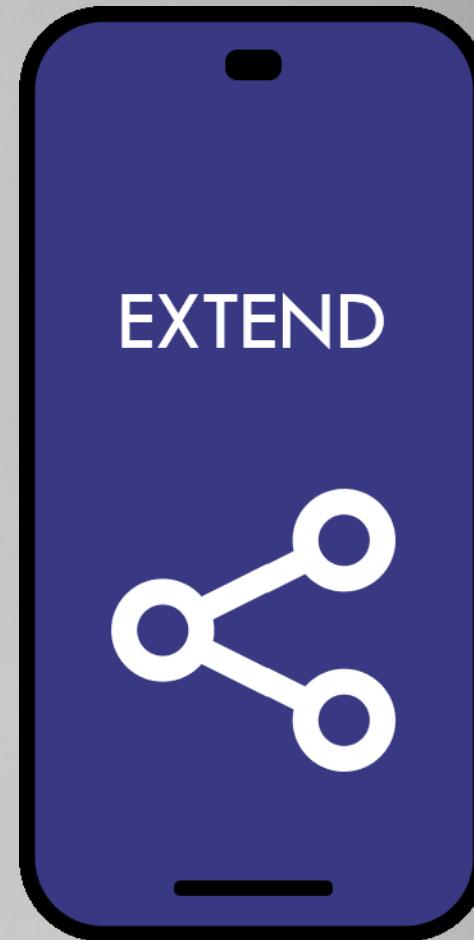


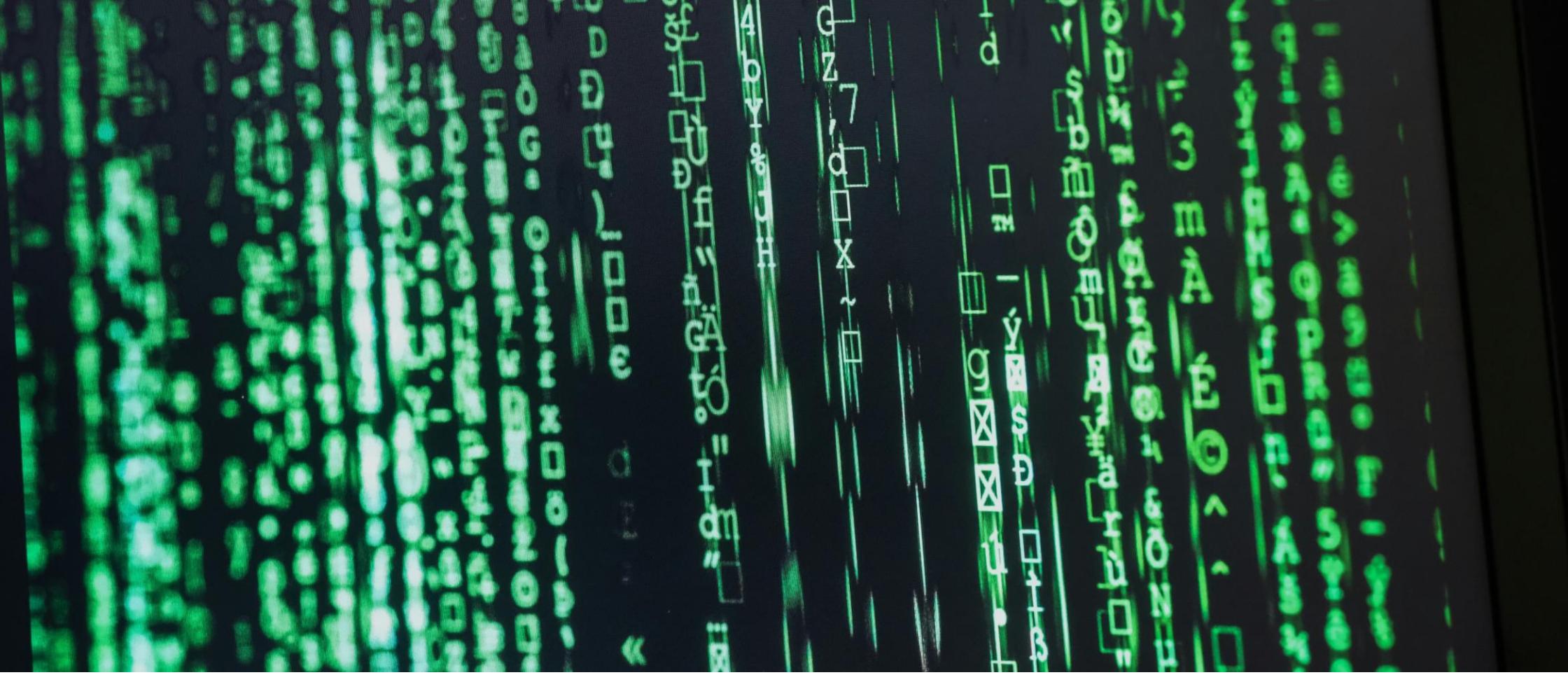
@lisihocke@mastodon.social



@lisihocke@mastodon.social







WAIT, I HAVE THE OPTION TO
SKILL UP IN SECURITY?

UNLOCKING
SECURITY



UNLOCK



HI, I'M A SPECIALIZED GENERALIST



@lisihocke@mastodon.social

UNLOCK



HI, I'M A SPECIALIZED GENERALIST

Testing & quality



@lisihocke@mastodon.social



HI, I'M A SPECIALIZED GENERALIST

Testing & quality

Product development teams





HI, I'M A SPECIALIZED GENERALIST

Testing & quality

Cross-functional

Product development teams





HI, I'M A SPECIALIZED GENERALIST

Testing & quality

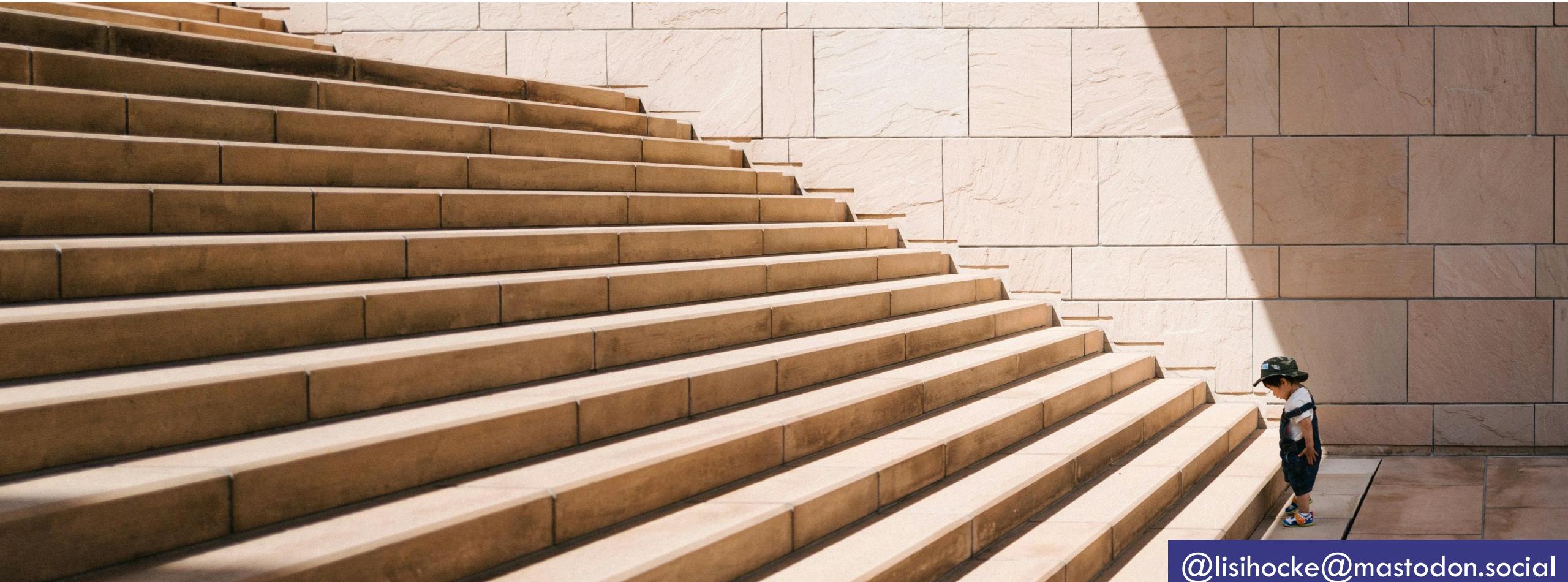
Cross-functional

Product development teams

Embedded hands-on



STEP BY STEP INTO SECURITY



@lisihocke@mastodon.social

STEP BY STEP INTO SECURITY



It all started with OWASP Juice Shop





STEP BY STEP INTO SECURITY

A photograph of a large set of light-colored stone steps leading up to a wall made of large rectangular stones. A small child wearing a cap and a backpack is walking up the steps from the bottom right. The sun is shining, creating strong shadows on the wall. Two dark blue rectangular boxes with white text are overlaid on the image: one in the middle left and one at the bottom left.

Bringing security mindset into the team

It all started with OWASP Juice Shop



STEP BY STEP INTO SECURITY

Continued learning in my personal time

Bringing security mindset into the team

It all started with OWASP Juice Shop



UNLOCK



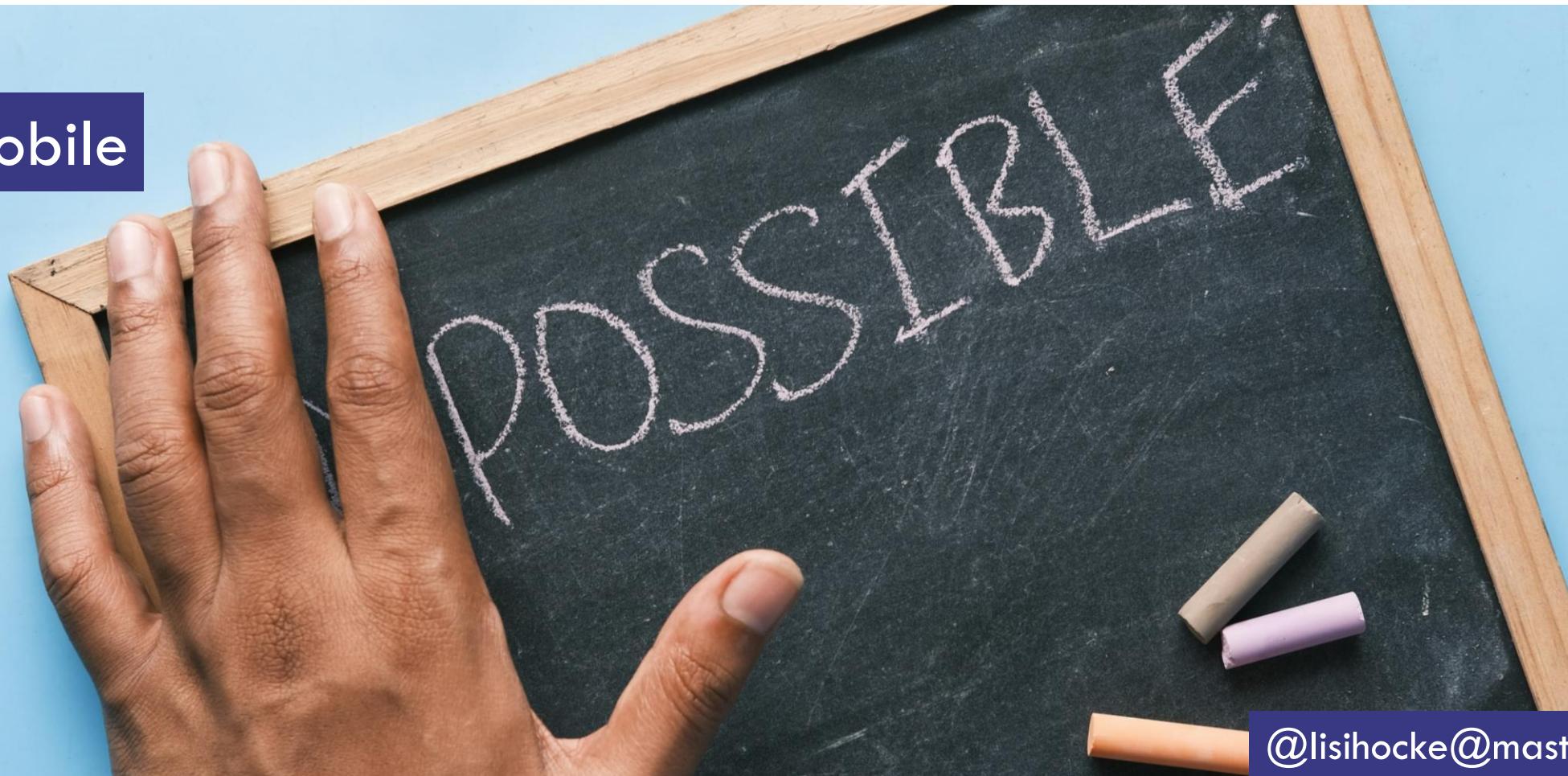
NEW COMPANY, NEW PRODUCT, NEW CHALLENGE





NEW COMPANY, NEW PRODUCT, NEW CHALLENGE

Mobile



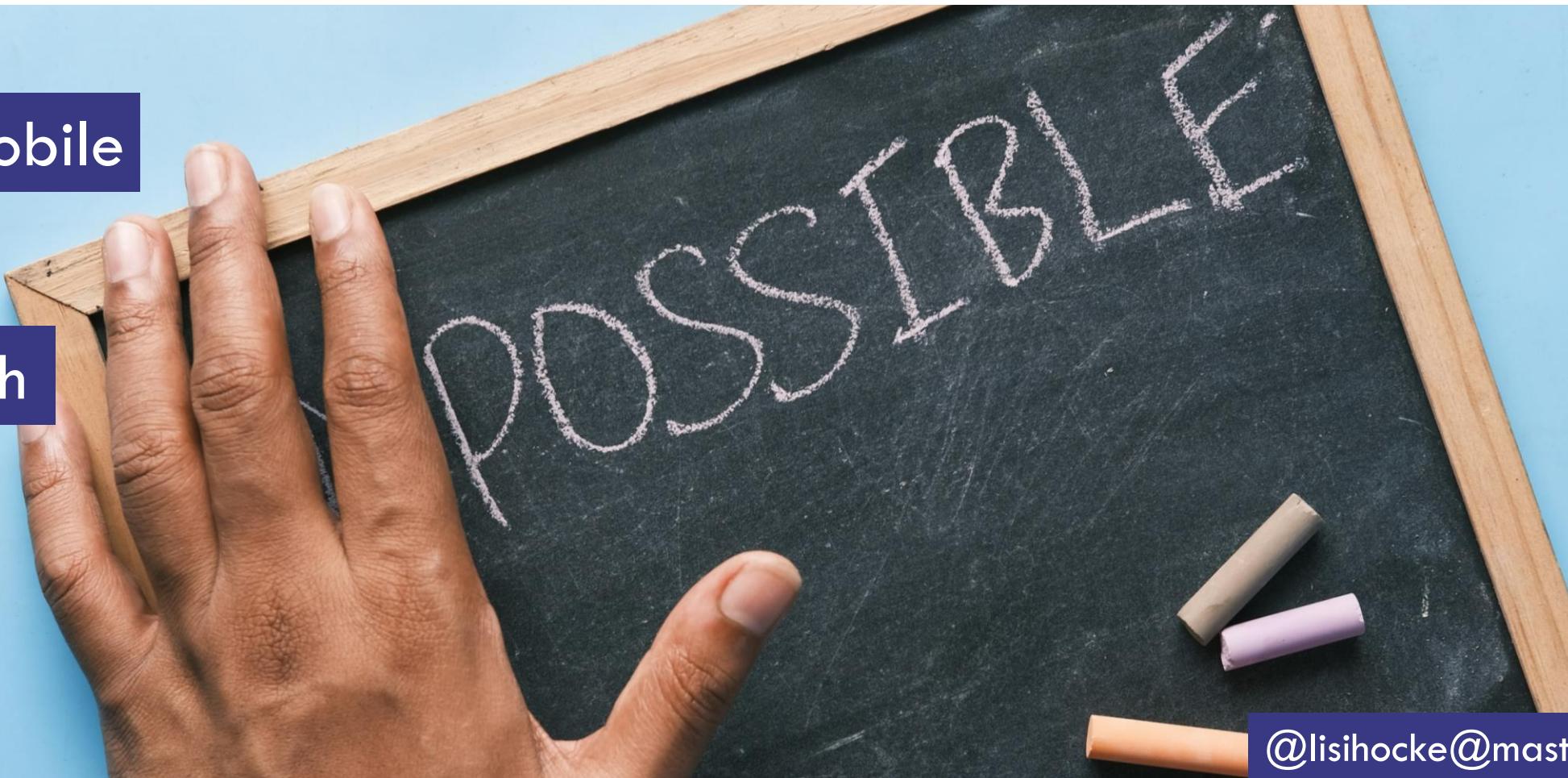
@lisihocke@mastodon.social



NEW COMPANY, NEW PRODUCT, NEW CHALLENGE

Mobile

Health



@lisihocke@mastodon.social

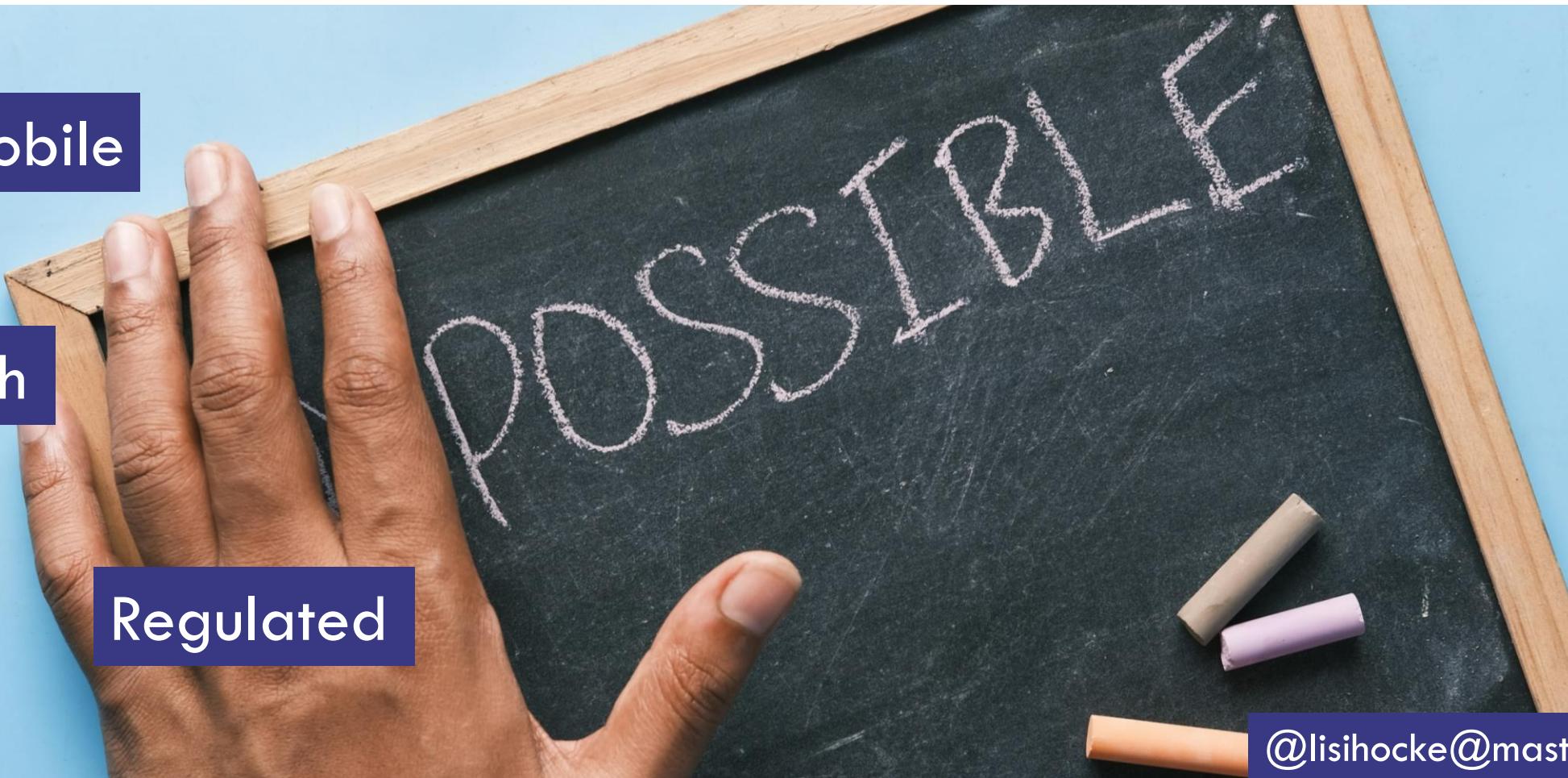


NEW COMPANY, NEW PRODUCT, NEW CHALLENGE

Mobile

Health

Regulated



@lisihocke@mastodon.social



NEW COMPANY, NEW PRODUCT, NEW CHALLENGE

Mobile

Health

Regulated

Security team





NEW COMPANY, NEW PRODUCT, NEW CHALLENGE

Mobile

Health

Regulated

A close-up photograph of a person's hands holding a piece of chalk and writing the word "POSSIBLE" in white chalk on a dark green chalkboard. The chalkboard has a wooden frame and sits against a light blue background. The hand is positioned as if it just finished writing the last letter of the word.

POSSIBLE

Security team

Security champions program

ACTING LIKE A CHAMPION WITHOUT BEING THE APPOINTED CHAMPION



@lisihocke@mastodon.social

ACTING LIKE A CHAMPION WITHOUT BEING THE APPOINTED CHAMPION



What is a security champion in a nutshell?



ACTING LIKE A CHAMPION WITHOUT BEING THE APPOINTED CHAMPION



What is a security champion in a nutshell?

A member of a
non-security team



ACTING LIKE A CHAMPION WITHOUT BEING THE APPOINTED CHAMPION

A photograph of a volleyball game. In the foreground, a player in a dark green jersey with a ponytail is shouting with arms raised. Behind her, another player in a maroon jersey is also at the net. The background shows the volleyball net and other players. Three blue callout boxes with white text are overlaid on the image.

What is a security champion in a nutshell?

A member of a
non-security team

Acting as communicator between
their team and the security team

ACTING LIKE A CHAMPION WITHOUT BEING THE APPOINTED CHAMPION



What is a security champion in a nutshell?

A member of a non-security team

Advocating for security in their team

Acting as communicator between their team and the security team



UNLOCK



FIRST AUDIT – BUILDING OUR ASSET INVENTORY



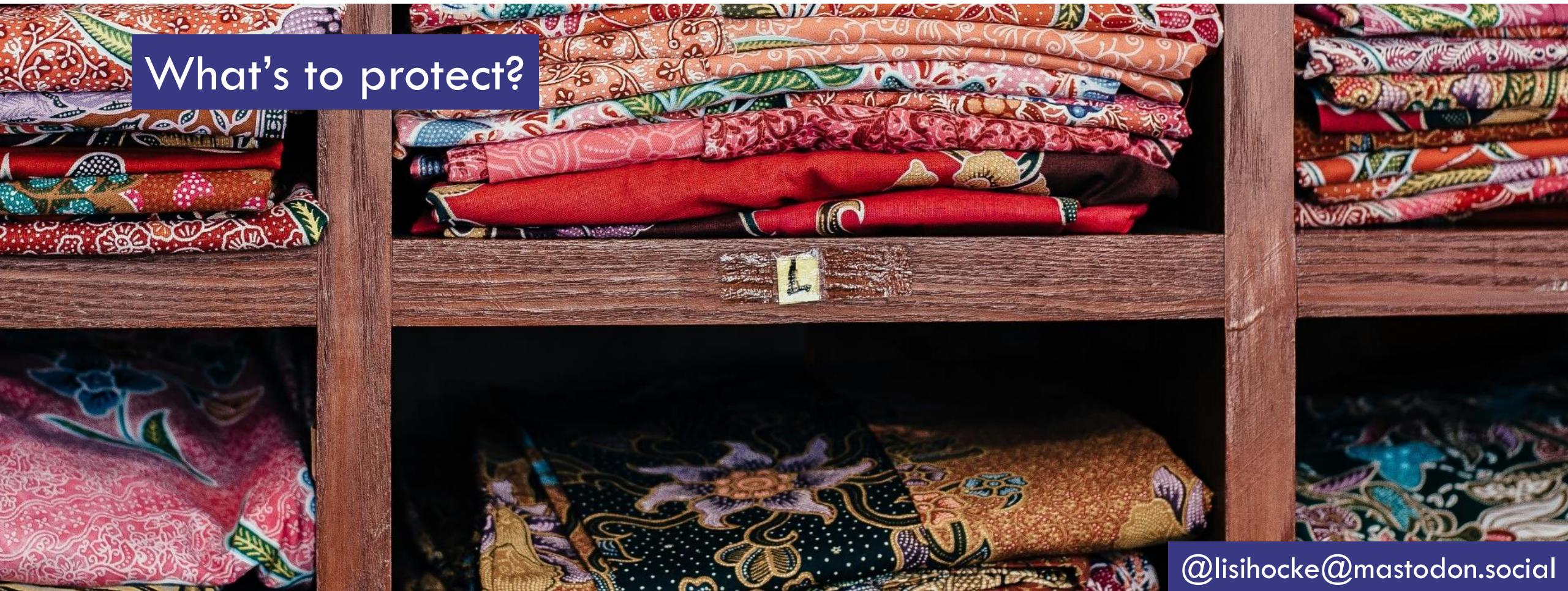
@lisihocke@mastodon.social

UNLOCK



FIRST AUDIT – BUILDING OUR ASSET INVENTORY

What's to protect?



@lisihocke@mastodon.social

UNLOCK



FIRST AUDIT – BUILDING OUR ASSET INVENTORY

What's to protect?

What's public facing?



FIRST AUDIT – BUILDING OUR ASSET INVENTORY



What's to protect?

What's public facing?

How confidential is it?

UNLOCK



FIRST AUDIT – BUILDING OUR ASSET INVENTORY

What's to protect?

What's public facing?

How confidential is it?

What's the business risk if breached?



FIRST AUDIT – BUILDING OUR ASSET INVENTORY

What's to protect?

What's public facing?

How confidential is it?

What's the business risk if breached?

Which security controls are in place?



YAY, I'M THE OFFICIAL MOBILE
SECURITY CHAMPION!

ADVOCATING
HANDS-ON

@lisihocke@mastodon.social



A MOBILE APPSEC STRATEGY TO RULE THEM ALL



@lisihocke@mastodon.social



A MOBILE APPSEC STRATEGY TO RULE THEM ALL

Helps align on a common goal





A MOBILE APPSEC STRATEGY TO RULE THEM ALL

Helps align on a common goal

Serves as reference





A MOBILE APPSEC STRATEGY TO RULE THEM ALL



Helps align on a common goal

Serves as reference

Provides focus on the most valuable topic



A MOBILE APPSEC STRATEGY TO RULE THEM ALL



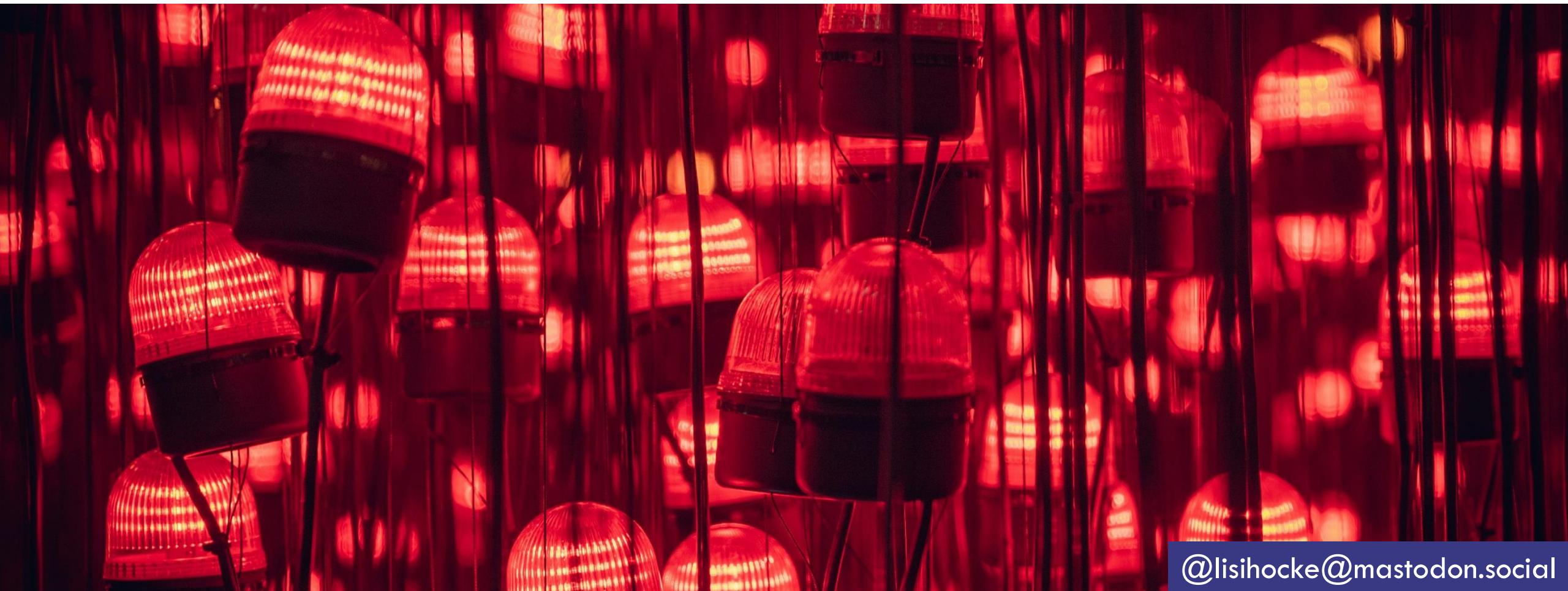
Helps align on a common goal

Serves as reference

Provides focus on the most valuable topic

Allows measuring progress

ALERT FATIGUE... DON'T TELL US WHAT WE ALREADY KNOW



@lisihocke@mastodon.social

ALERT FATIGUE... DON'T TELL US WHAT WE ALREADY KNOW



Throwing more tools
on it won't fix it



ALERT FATIGUE... DON'T TELL US WHAT WE ALREADY KNOW

A dense grid of numerous red emergency or warning lights, likely from police cars or ambulances, creating a pattern of red and yellow light streaks against a dark background.

Throwing more tools
on it won't fix it

Focus on cleaning up the noise

ALERT FATIGUE... DON'T TELL US WHAT WE ALREADY KNOW

A background image showing multiple red emergency lights, possibly from a police car or fire truck, creating a blurred, glowing effect.

Throwing more tools
on it won't fix it

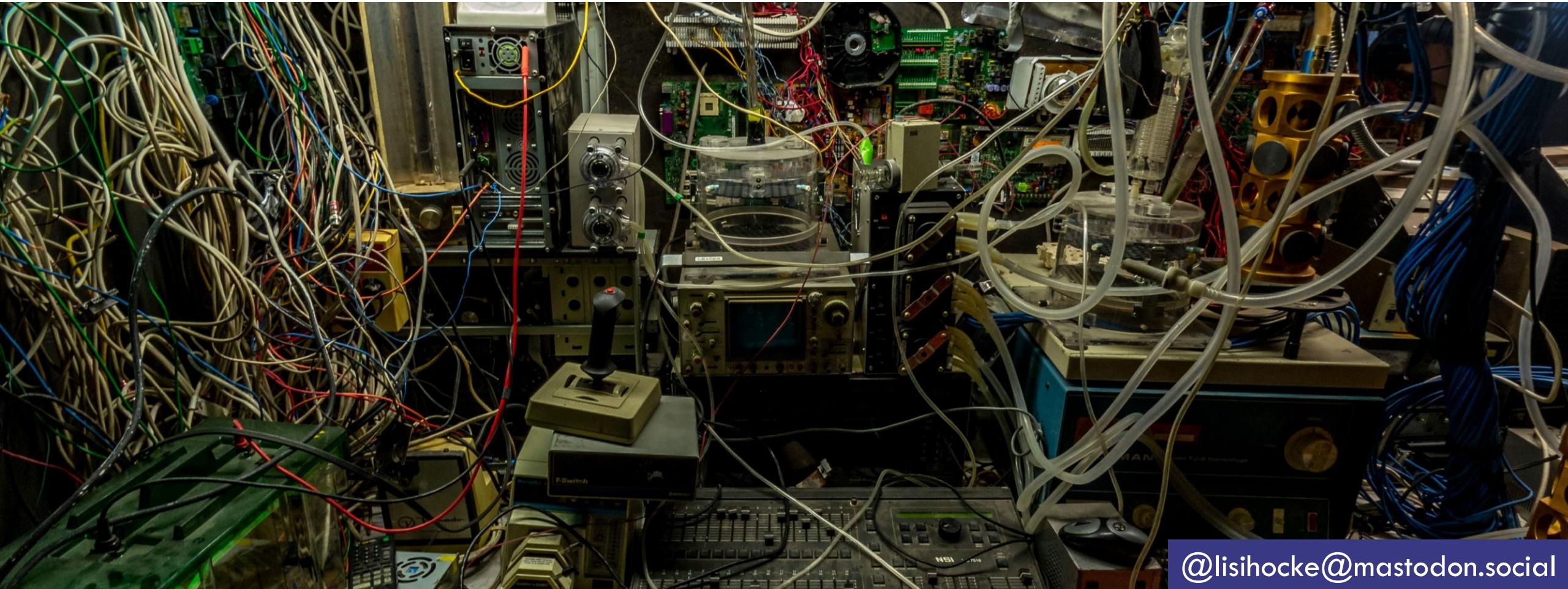
Focus on cleaning up the noise

Be intentional about the tools you
use and what value they bring

ADVOCATE



OH MY, ALL THESE DEPENDENCIES...



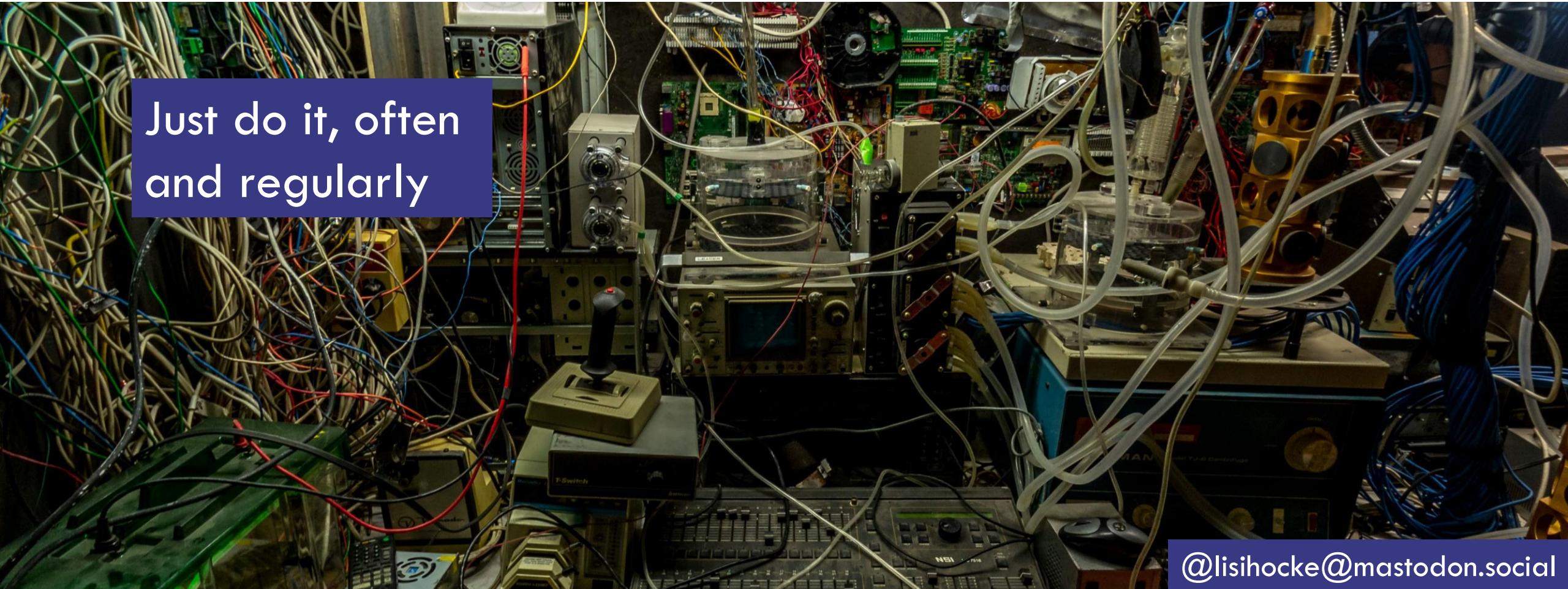
@lisihocke@mastodon.social

ADVOCATE



OH MY, ALL THESE DEPENDENCIES...

Just do it, often
and regularly





OH MY, ALL THESE DEPENDENCIES...



Just do it, often
and regularly



Start where the
risk is highest



OH MY, ALL THESE DEPENDENCIES...

Just do it, often
and regularly

Start where the
risk is highest

Tackle quick
wins first



OH MY, ALL THESE DEPENDENCIES...



Just do it, often
and regularly

Start where the
risk is highest

Tackle quick
wins first

Write out steps
for big upgrades



OH MY, ALL THESE DEPENDENCIES...



Just do it, often
and regularly

Start where the
risk is highest

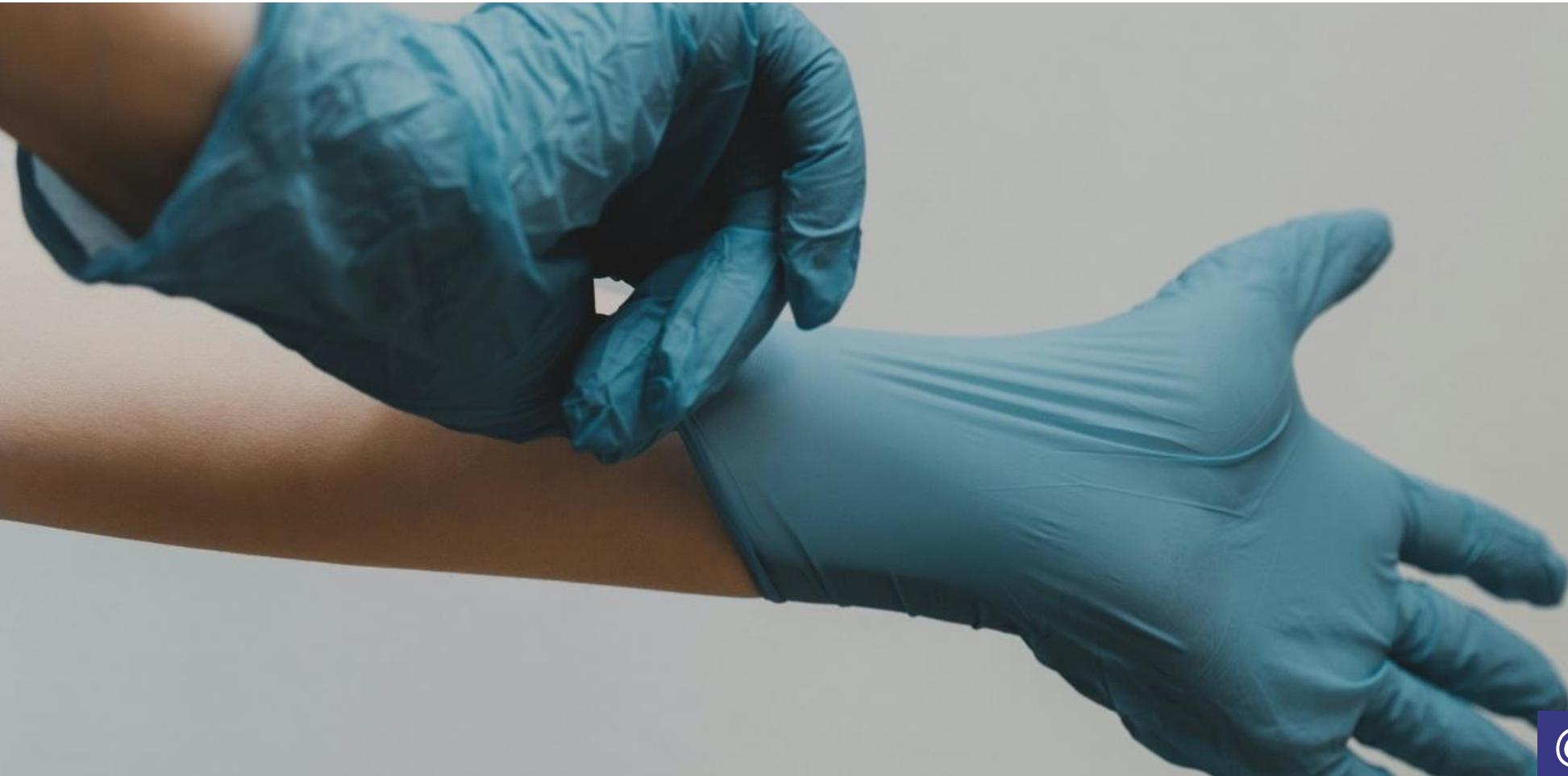
Tackle quick
wins first

Write out steps
for big upgrades

Cling to a working
update strategy



CLEANUPS REDUCE THE ATTACK SURFACE



@lisihocke@mastodon.social



CLEANUPS REDUCE THE ATTACK SURFACE

“Technical debt is security debt.”
— Tanya Janca

<https://shehackspurple.ca/2021/12/23/discoveries-as-a-result-of-the-log4j-debaacle/>



CLEANUPS REDUCE THE ATTACK SURFACE



“Technical debt is security debt.”
— Tanya Janca

<https://shehackspurple.ca/2021/12/23/discoveries-as-a-result-of-the-log4j-debaacle/>

Outdated implementation offers
opportunities for attackers



CLEANUPS REDUCE THE ATTACK SURFACE



“Technical debt is security debt.”
— Tanya Janca

<https://shehackspurple.ca/2021/12/23/discoveries-as-a-result-of-the-log4j-debaacle/>

Outdated implementation offers opportunities for attackers

Make cleanup non-negotiable

ADVOCATE



AAARGH, WE LET IT IN AND IT'S HERE TO STAY





AAARGH, WE LET IT IN AND IT'S HERE TO STAY

Get insecure
implementations
out right away





AAARGH, WE LET IT IN AND IT'S HERE TO STAY

Get insecure
implementations
out right away



DO NOT
ENTER

Think of risks early on



AAARGH, WE LET IT IN AND IT'S HERE TO STAY

Get insecure
implementations
out right away



DO NOT
ENTER

Think of risks early on

Educate,
educate,
educate

WOW, SO MANY FOLKS ARE PROBING OUR SYSTEM – CONSTANTLY



WOW, SO MANY FOLKS ARE PROBING OUR SYSTEM – CONSTANTLY



Observe frequently and regularly





WOW, SO MANY FOLKS ARE PROBING OUR SYSTEM – CONSTANTLY

Observe frequently and regularly

Get alerted on potentially malicious activity and leaks





WOW, SO MANY FOLKS ARE PROBING OUR SYSTEM – CONSTANTLY

Observe frequently and regularly

Get alerted on potentially malicious activity and leaks

Make it harder for bad actors, incrementally

WOW, SO MANY FOLKS ARE PROBING OUR SYSTEM – CONSTANTLY



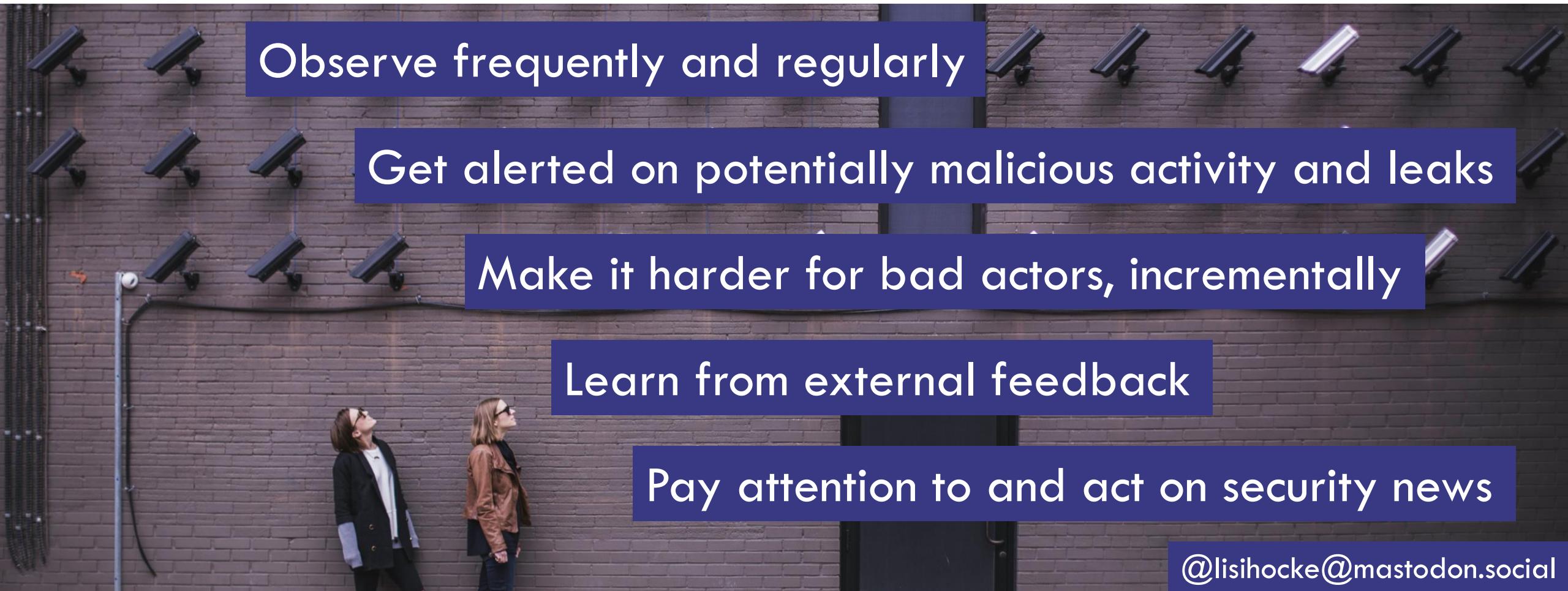
Observe frequently and regularly

Get alerted on potentially malicious activity and leaks

Make it harder for bad actors, incrementally

Learn from external feedback

WOW, SO MANY FOLKS ARE PROBING OUR SYSTEM – CONSTANTLY

A photograph of a brick wall covered in numerous surveillance cameras. Two women are standing at the bottom left, looking up at the wall.

Observe frequently and regularly

Get alerted on potentially malicious activity and leaks

Make it harder for bad actors, incrementally

Learn from external feedback

Pay attention to and act on security news

THE PROBLEM OF “LATER” – WHY WE NEED EXPLICIT PRODUCT DECISIONS



@lisihocke@mastodon.social

THE PROBLEM OF “LATER” – WHY WE NEED EXPLICIT PRODUCT DECISIONS



Letting security topics rot in the backlog means we're implicitly accepting the respective risk

THE PROBLEM OF “LATER” – WHY WE NEED EXPLICIT PRODUCT DECISIONS



Letting security topics rot in the backlog means we're implicitly accepting the respective risk

Register risks officially



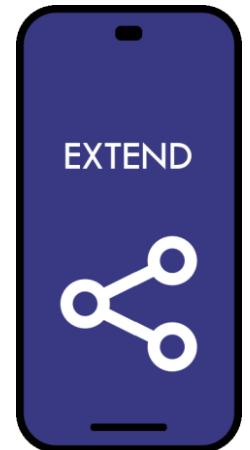
THE PROBLEM OF “LATER” – WHY WE NEED EXPLICIT PRODUCT DECISIONS

A close-up photograph of several apples that are severely rotten, showing brown, mushy flesh and dark spots. They are arranged in a cluster, with some in sharp focus in the foreground and others blurred in the background.

Letting security topics rot in the backlog means we're implicitly accepting the respective risk

Register risks officially

Make a decision with stakeholders how to handle them



WHAT'S THE SECRET INGREDIENT
TO CHAMPIONING SECURITY?

EXTENDING
REACH

@lisihocke@mastodon.social

EXTEND



FOSTER RELATIONSHIPS, GROW ALLIES



@lisihocke@mastodon.social

EXTEND



FOSTER RELATIONSHIPS, GROW ALLIES

A close-up photograph of several hands of different skin tones and wearing various colored knitted cuffs (brown, red, green, blue).

Close collaboration with
your security team

EXTEND

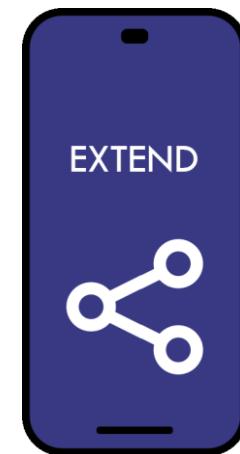


FOSTER RELATIONSHIPS, GROW ALLIES

A close-up photograph of several hands of different skin tones and clothing colors (red, blue, green) coming together in a group hug or handshake. One hand in the center wears a gold ring with a small blue stone. A second ring is visible on another hand. The hands are resting on a dark, textured surface.

Close collaboration with
your security team

Take your own
team with you



FOSTER RELATIONSHIPS, GROW ALLIES

Close collaboration with
your security team

Take your own
team with you

Experiment with
different approaches to
figure out what works

EXTEND



ANYONE OUT THERE TO LEARN TOGETHER WITH?



@lisihocke@mastodon.social

EXTEND



ANYONE OUT THERE TO LEARN TOGETHER WITH?

Engage exchange
among security
champions

I'm

not

Alone



@lisihocke@mastodon.social

EXTEND



ANYONE OUT THERE TO LEARN TOGETHER WITH?

Engage exchange
among security
champions

I'm

not

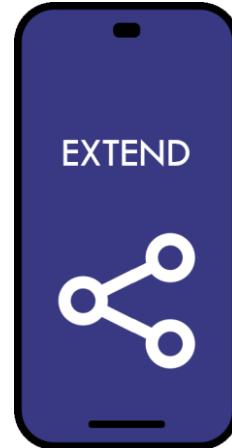
Alone

Connect with security communities



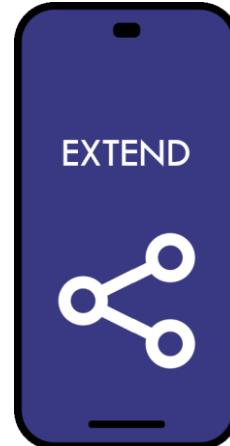
@lisihocke@mastodon.social

SECURITY IS EVERYONE'S RESPONSIBILITY, AND WE NEED EVERYONE TO SECURE OUR PRODUCTS



@lisihocke@mastodon.social

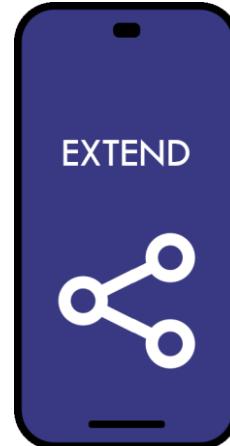
SECURITY IS EVERYONE'S RESPONSIBILITY, AND WE NEED EVERYONE TO SECURE OUR PRODUCTS



There's strength in diversity – given we foster inclusion and equity

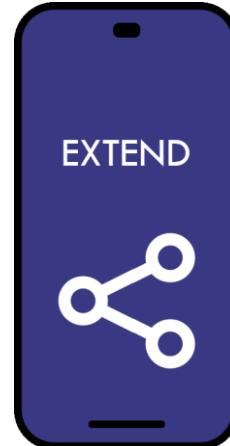


WHAT WORKED, WHAT DIDN'T, WHAT WE REALLY SHOULDN'T HAVE DONE IN THE FIRST PLACE



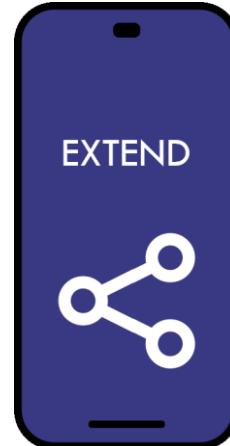
@lisihocke@mastodon.social

WHAT WORKED, WHAT DIDN'T, WHAT WE REALLY SHOULDN'T HAVE DONE IN THE FIRST PLACE

A photograph of a woman with short, dark, curly hair and large black-rimmed glasses. She is wearing a black top with a red floral pattern. Her right hand is resting against her chin, and she is looking upwards and to the left with a thoughtful expression. The background is a rustic wooden wall.

Worked: investing
in a security culture

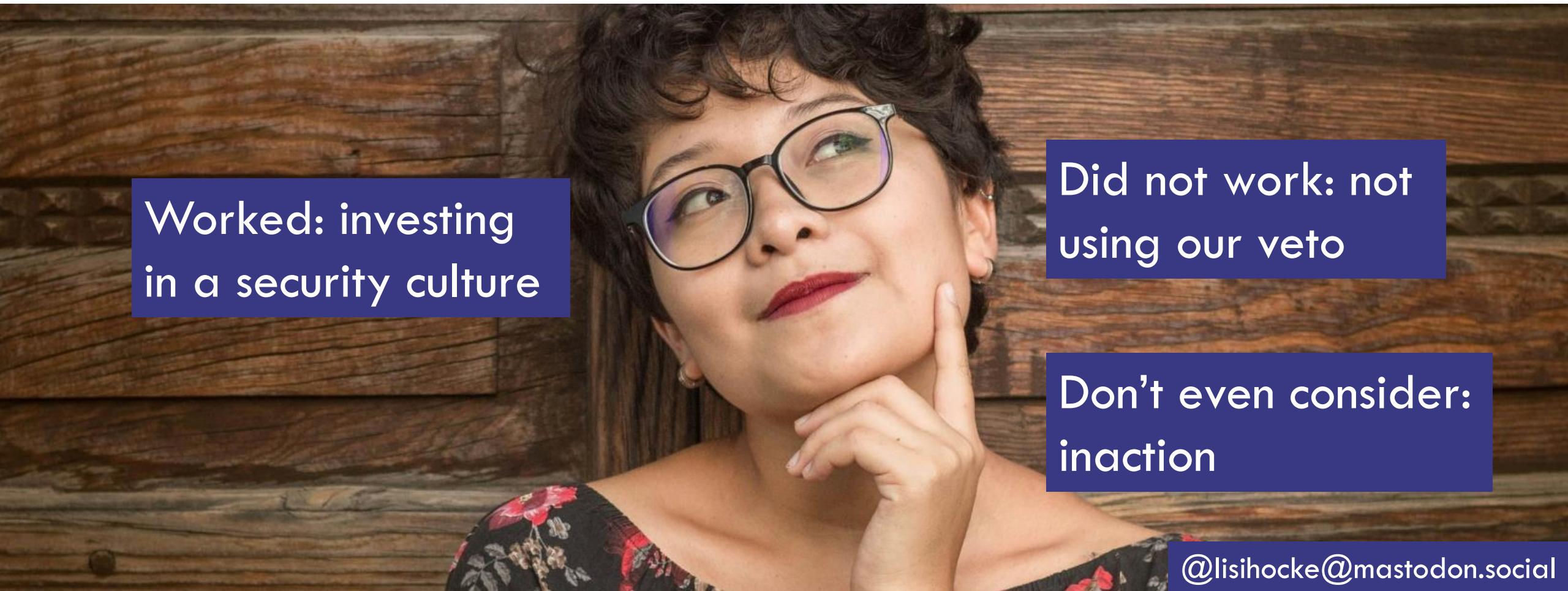
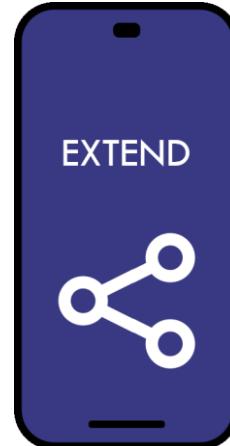
WHAT WORKED, WHAT DIDN'T, WHAT WE REALLY SHOULDN'T HAVE DONE IN THE FIRST PLACE

A woman with short dark hair and glasses, resting her chin on her hand and looking thoughtful.

Worked: investing
in a security culture

Did not work: not
using our veto

WHAT WORKED, WHAT DIDN'T, WHAT WE REALLY SHOULDN'T HAVE DONE IN THE FIRST PLACE

A photograph of a woman with short, dark, curly hair and large black-rimmed glasses. She is wearing a black top with a red floral pattern. Her right hand is resting against her chin, and she is looking upwards and to the left with a thoughtful expression. The background is a rustic wooden wall.

Worked: investing
in a security culture

Did not work: not
using our veto

Don't even consider:
inaction

EXTEND



KEEP GOING, SMALL STEPS CUMULATE!



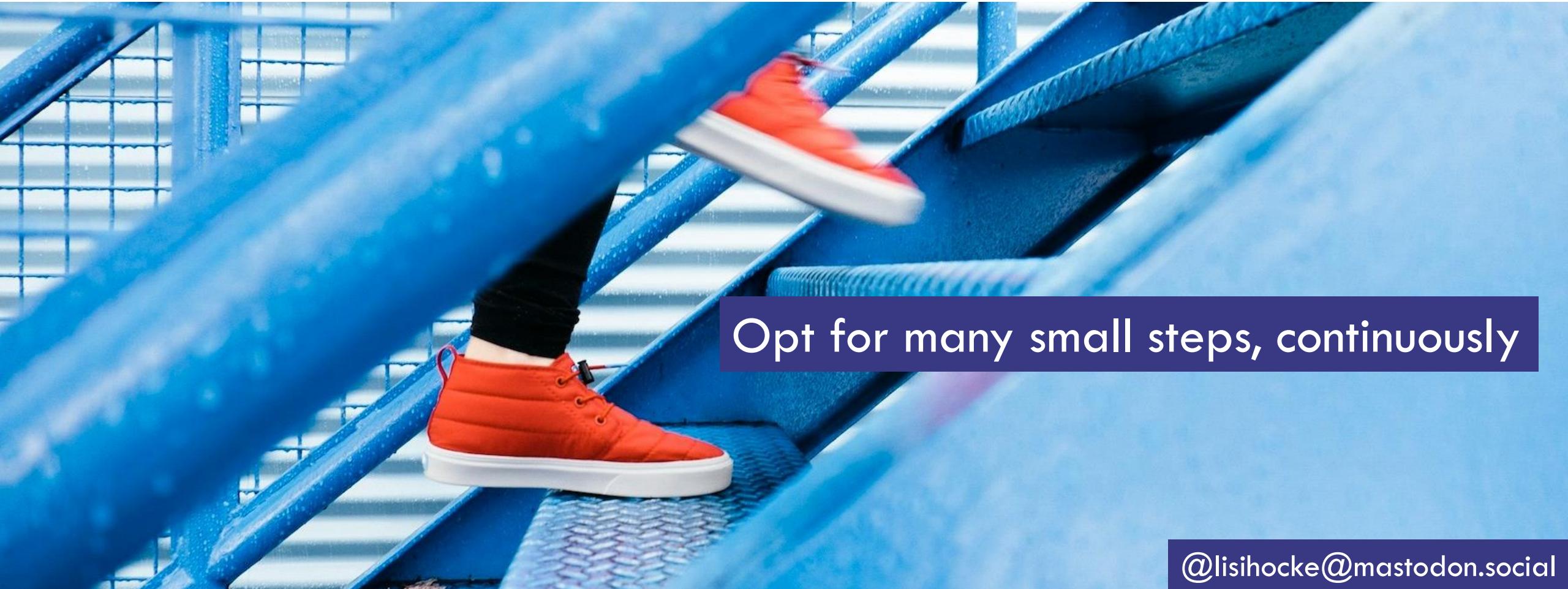
@lisihocke@mastodon.social

EXTEND



KEEP GOING, SMALL STEPS CUMULATE!

Opt for many small steps, continuously



@lisihocke@mastodon.social

**WISH FOR IT
HOPE FOR IT
DREAM OF IT**



bit.ly/lisihocke-security-resources



**BUT BY
ALL MEANS
DO IT □□□**

@lisihocke@mastodon.social

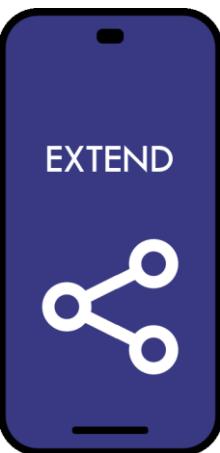
**WISH FOR IT
HOPE FOR IT
DREAM OF IT**

**BUT BY
ALL MEANS
DO IT**

Make things a bit more secure than yesterday every day



bit.ly/lisihocke-security-resources



@lisihocke@mastodon.social

**WISH FOR IT
HOPE FOR IT
DREAM OF IT**

**BUT BY
ALL MEANS
DO IT**

Make things a bit more secure than yesterday every day



bit.ly/lisihocke-security-resources



THANK YOU!

www.lisihocke.com

@lisihocke@mastodon.social