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


UNLOCK

@lisihocke@mastodon.social

@lisihocke@mastodon.social

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

UNLOCKING SECURITY

@lisihocke@mastodon.social

HI, I'M A SPECIALIZED GENERALIST

@lisihocke@mastodon.social

HI, I'M A SPECIALIZED GENERALIST

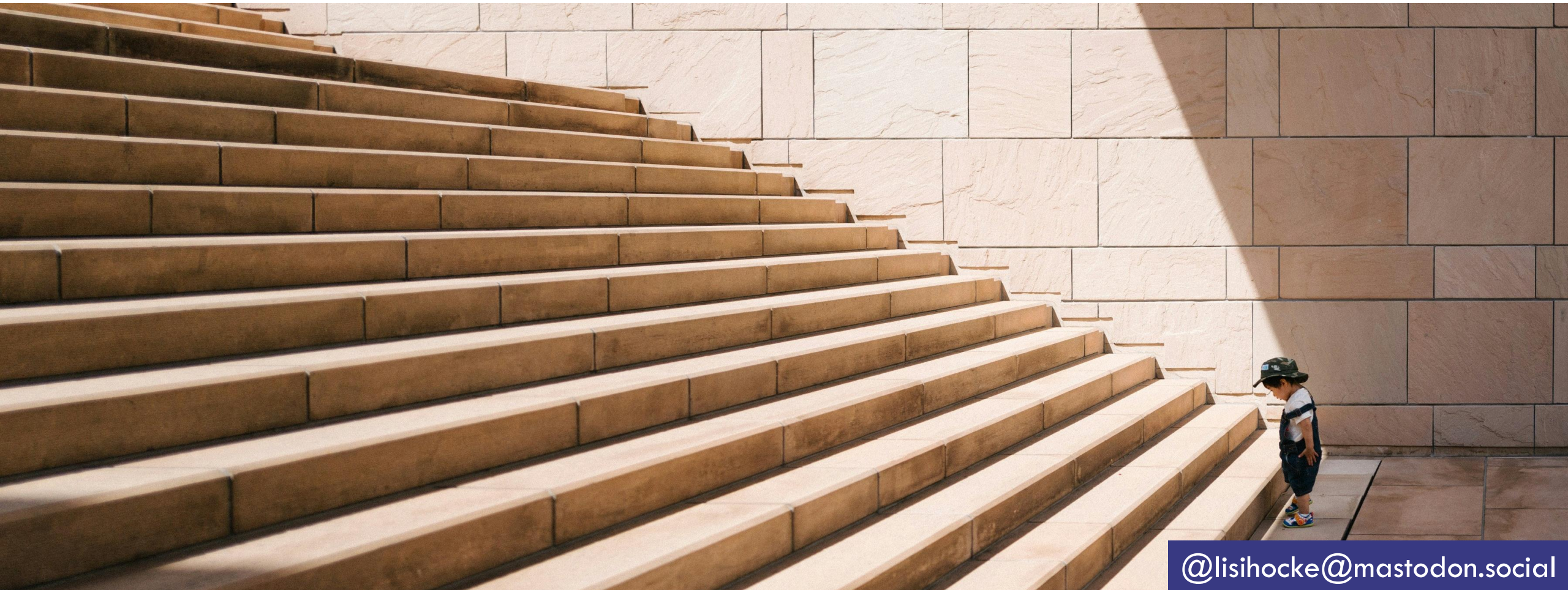
@lisihocke@mastodon.social

HI, I'M A SPECIALIZED GENERALIST

HI, I'M A SPECIALIZED GENERALIST

HI, I'M A SPECIALIZED GENERALIST

STEP BY STEP INTO SECURITY



@lisihocke@mastodon.social

STEP BY STEP INTO SECURITY

It all started with OWASP Juice Shop

@lisihocke@mastodon.social

STEP BY STEP INTO SECURITY

Bringing security mindset into the team

It all started with OWASP Juice Shop

@lisihocke@mastodon.social

STEP BY STEP INTO SECURITY

Continued learning in my personal time

Bringing security mindset into the team

It all started with OWASP Juice Shop

@lisihocke@mastodon.social

NEW COMPANY, NEW PRODUCT, NEW CHALLENGE

@lisihocke@mastodon.social

NEW COMPANY, NEW PRODUCT, NEW CHALLENGE

@lisihocke@mastodon.social

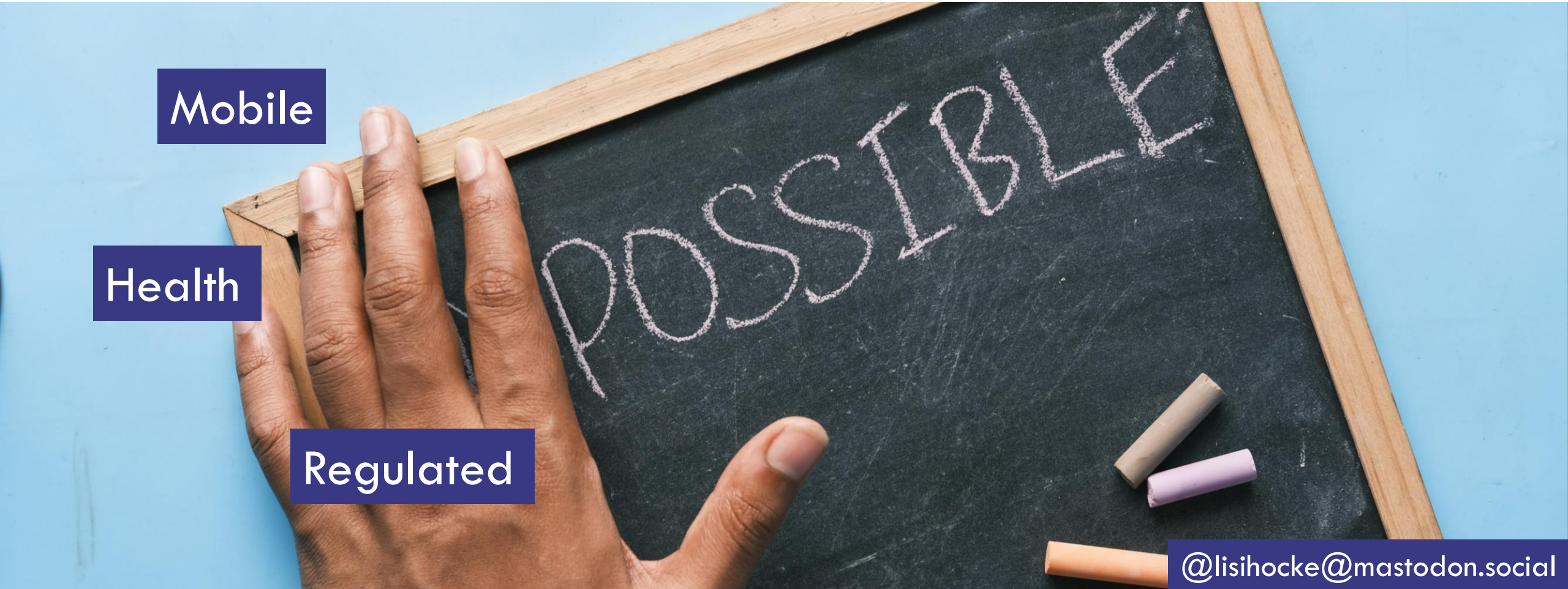
NEW COMPANY, NEW PRODUCT, NEW CHALLENGE

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

@lisihocke@mastodon.social

NEW COMPANY, NEW PRODUCT, NEW CHALLENGE

Mobile

Health

Regulated

Security team

Security champions program

@lisihocke@mastodon.social

ACTING LIKE A CHAMPION WITHOUT BEING THE APPOINTED CHAMPION

@lisihocke@mastodon.social

ACTING LIKE A CHAMPION WITHOUT BEING THE APPOINTED CHAMPION

ACTING LIKE A CHAMPION WITHOUT BEING THE APPOINTED CHAMPION

What is a security champion in a nutshell?

A member of a non-security team

@lisihocke@mastodon.social

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 as communicator between their team and the security team

@lisihocke@mastodon.social

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 as communicator between their team and the security team

Advocating for security in their team

@lisihocke@mastodon.social

FIRST AUDIT – BUILDING OUR ASSET INVENTORY

@lisihocke@mastodon.social

FIRST AUDIT – BUILDING OUR ASSET INVENTORY

What's to protect?

@lisihocke@mastodon.social

FIRST AUDIT – BUILDING OUR ASSET INVENTORY

@lisihocke@mastodon.social

FIRST AUDIT – BUILDING OUR ASSET INVENTORY

@lisihocke@mastodon.social

FIRST AUDIT – BUILDING OUR ASSET INVENTORY

@lisihocke@mastodon.social

FIRST AUDIT – BUILDING OUR ASSET INVENTORY

@lisihocke@mastodon.social

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

@lisihocke@mastodon.social

A MOBILE APPSEC STRATEGY TO RULE THEM ALL

Helps align on a common goal

Serves as reference

@lisihocke@mastodon.social

A MOBILE APPSEC STRATEGY TO RULE THEM ALL

Helps align on a common goal

Serves as reference

Provides focus on the most valuable topic

@lisihocke@mastodon.social

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

@lisihocke@mastodon.social

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

@lisihocke@mastodon.social

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

@lisihocke@mastodon.social

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

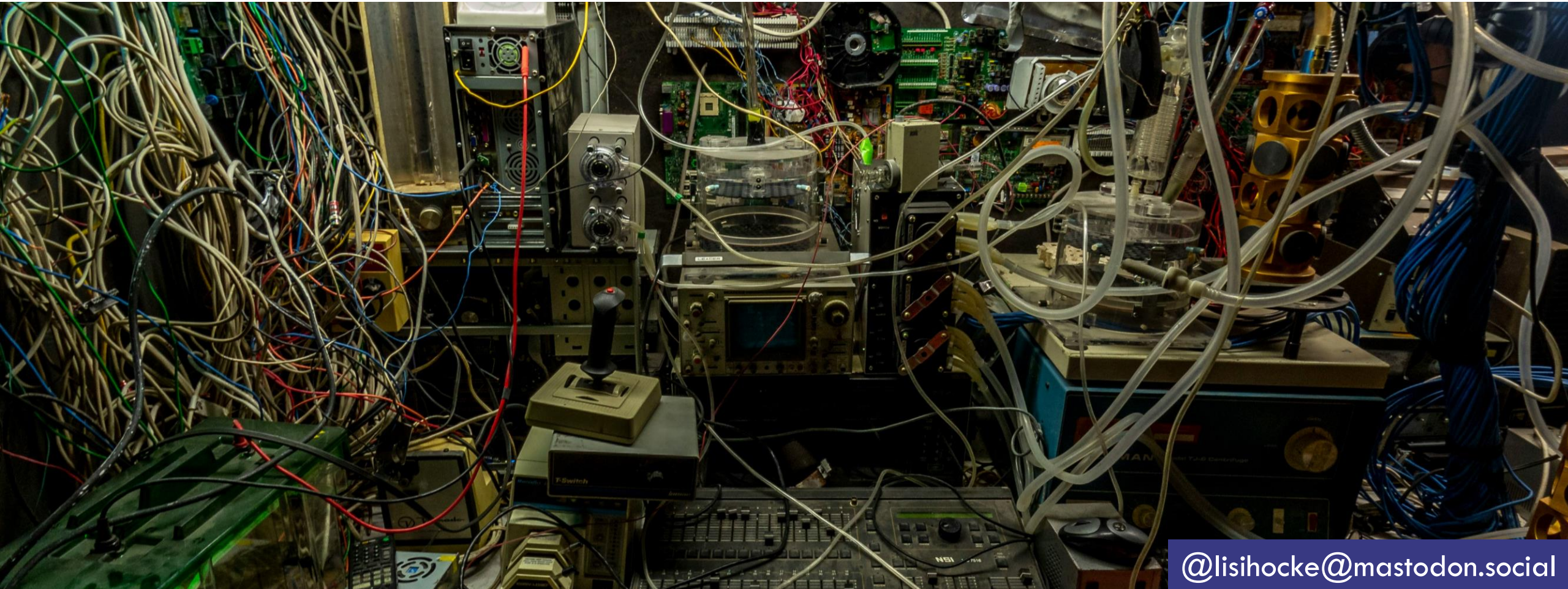
Throwing more tools on it won't fix it

Focus on cleaning up the noise

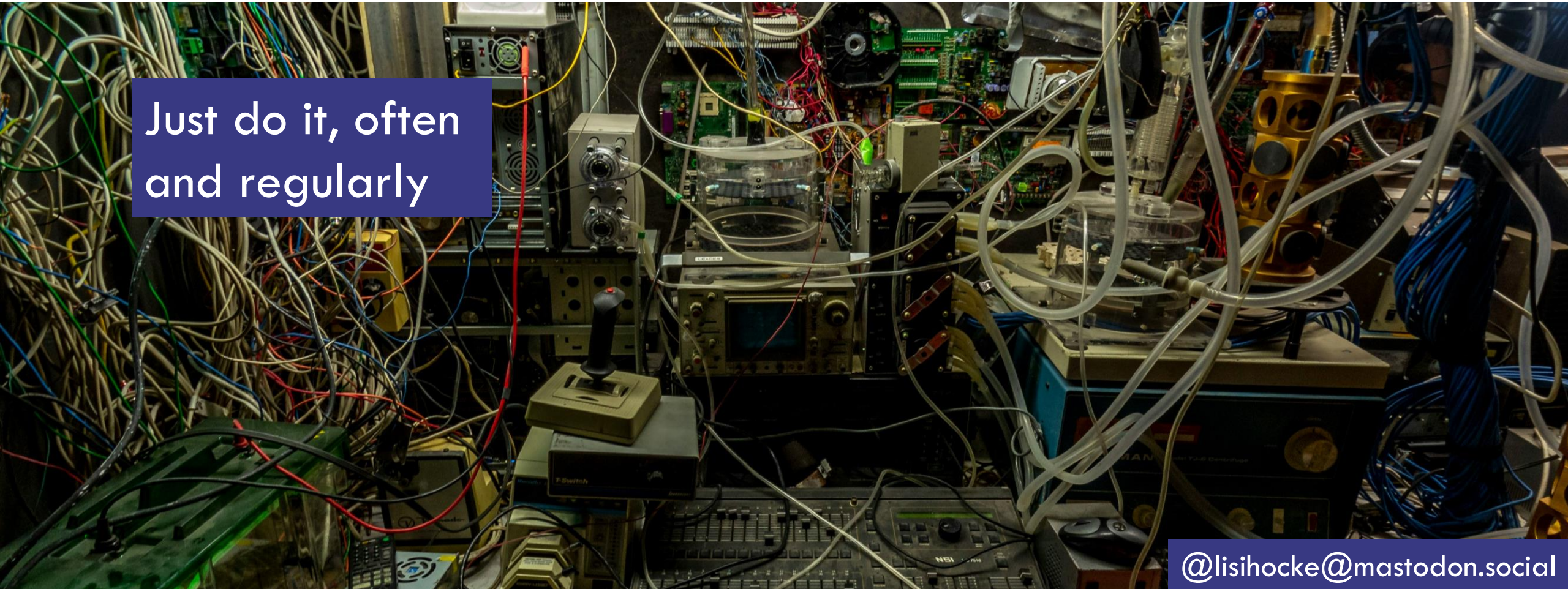
Be intentional about the tools you use and what value they bring

@lisihocke@mastodon.social

OH MY, ALL THESE DEPENDENCIES...



OH MY, ALL THESE DEPENDENCIES…



OH MY, ALL THESE DEPENDENCIES…

OH MY, ALL THESE DEPENDENCIES…

@lisihocke@mastodon.social

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

@lisihocke@mastodon.social

OH MY, ALL THESE DEPENDENCIES…

CLEANUPS REDUCE THE ATTACK SURFACE

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-debacle/

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-debacle/

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-debacle/

Outdated implementation offers opportunities for attackers

Make cleanup non-negotiable

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

@lisihocke@mastodon.social

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

@lisihocke@mastodon.social

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

Get insecure implementations out right away

Think of risks early on

@lisihocke@mastodon.social

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

Get insecure implementations out right away

Think of risks early on

Educate, educate, educate

@lisihocke@mastodon.social

WOW, SO MANY FOLKS ARE PROBING OUR SYSTEM – CONSTANTLY

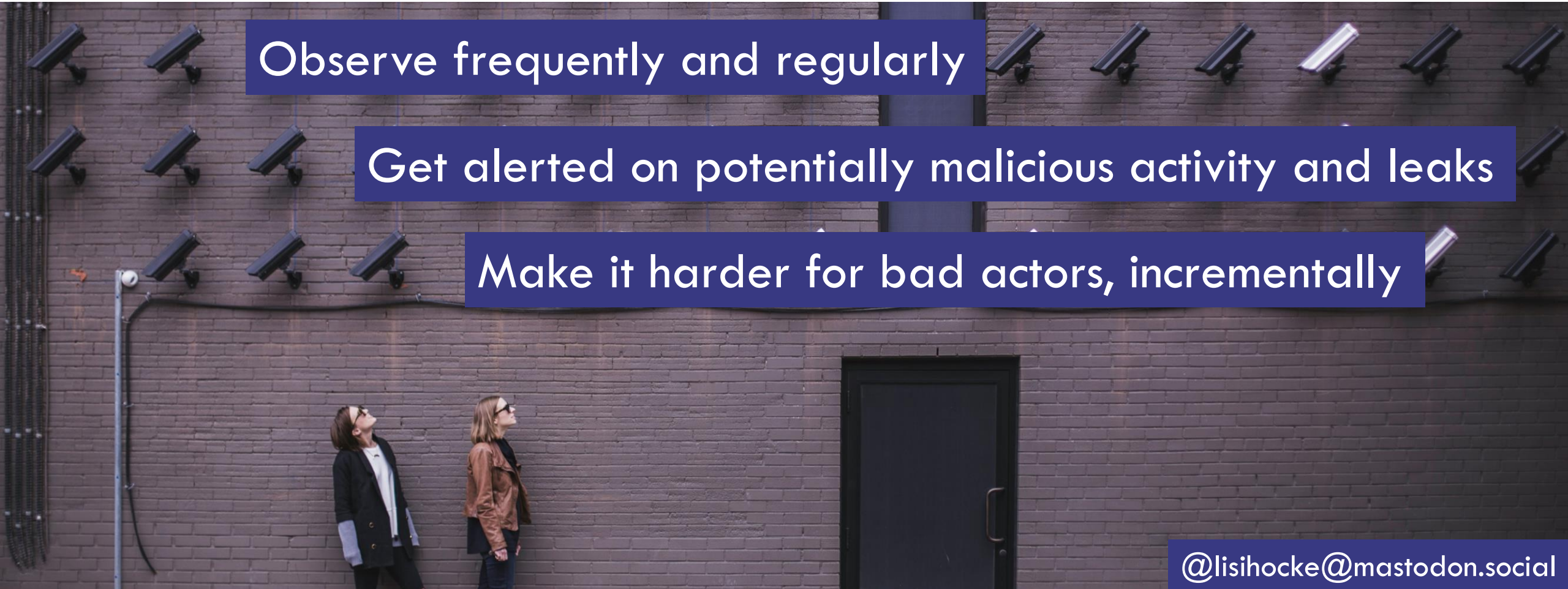
WOW, SO MANY FOLKS ARE PROBING OUR SYSTEM – CONSTANTLY

@lisihocke@mastodon.social

WOW, SO MANY FOLKS ARE PROBING OUR SYSTEM – CONSTANTLY

@lisihocke@mastodon.social

WOW, SO MANY FOLKS ARE PROBING OUR SYSTEM – CONSTANTLY



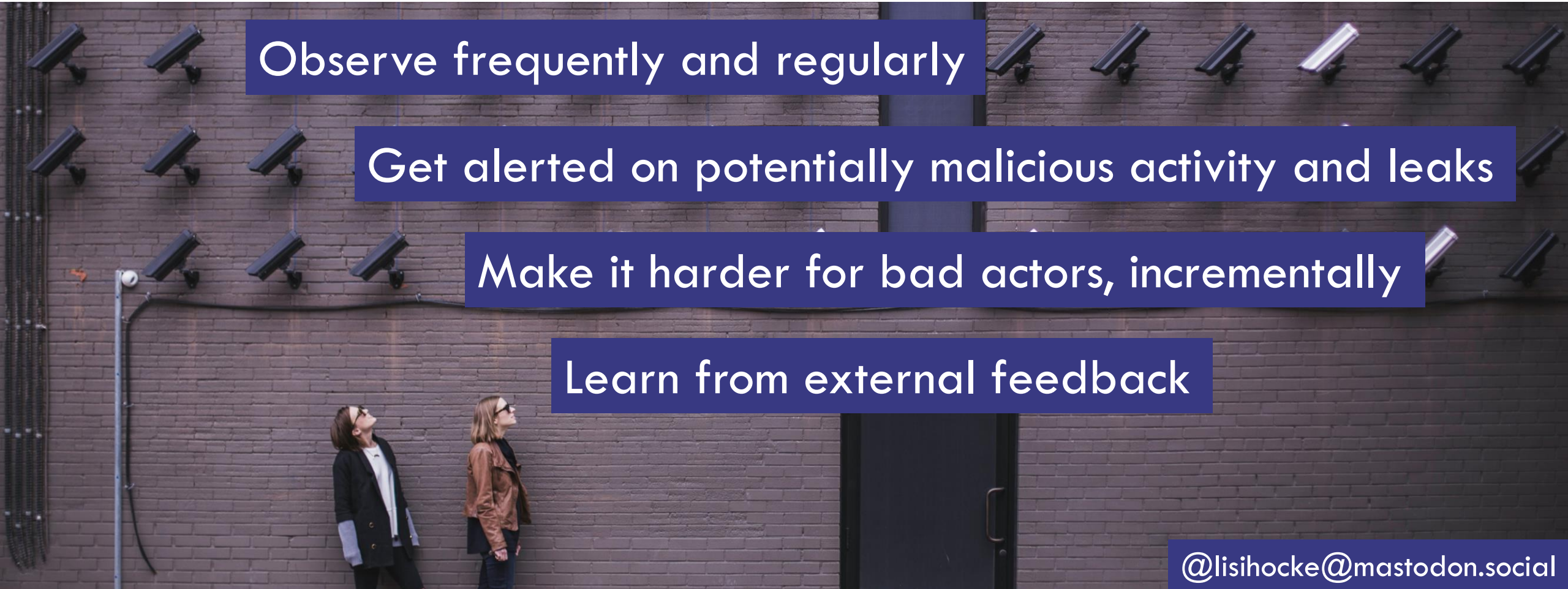
Observe frequently and regularly

Get alerted on potentially malicious activity and leaks

Make it harder for bad actors, incrementally

@lisihocke@mastodon.social

WOW, SO MANY FOLKS ARE PROBING OUR SYSTEM – CONSTANTLY



Observe frequently and regularly

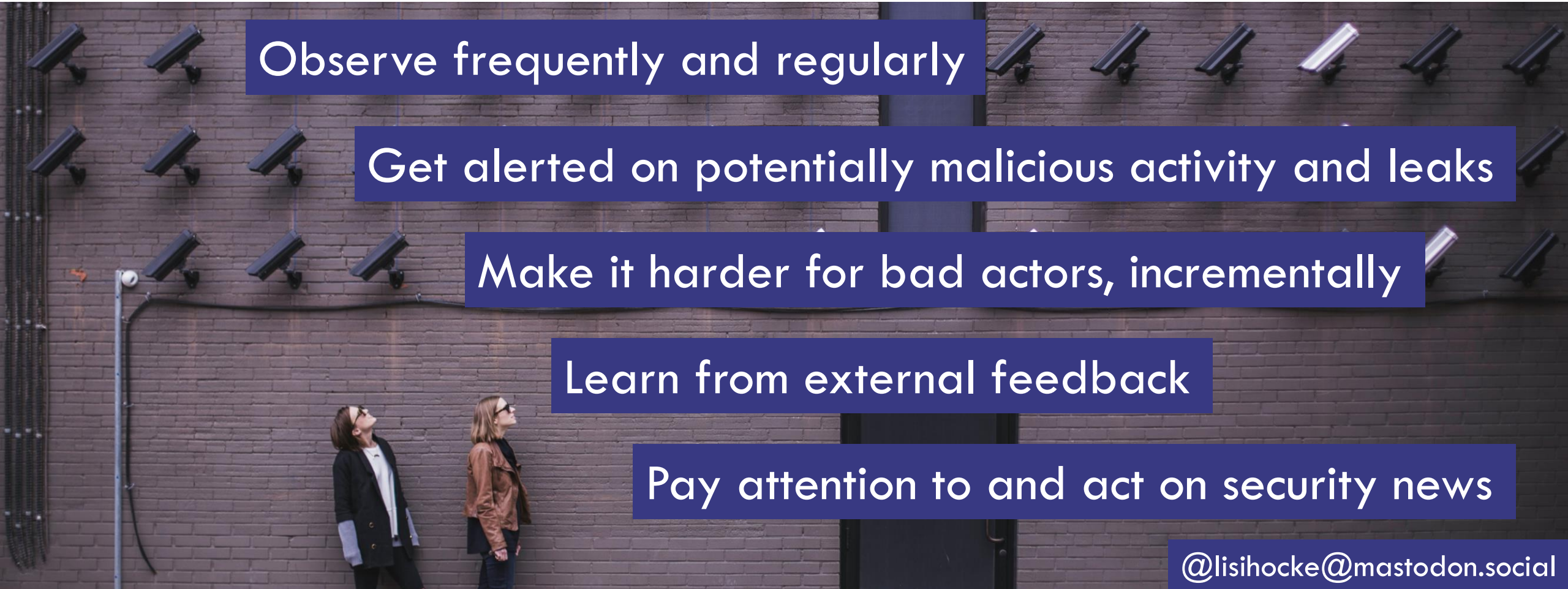
Get alerted on potentially malicious activity and leaks

Make it harder for bad actors, incrementally

Learn from external feedback

@lisihocke@mastodon.social

WOW, SO MANY FOLKS ARE PROBING OUR SYSTEM – CONSTANTLY



@lisihocke@mastodon.social

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

@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

Register risks officially

@lisihocke@mastodon.social

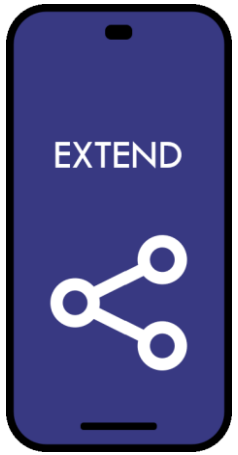
THE PROBLEM OF "LATER" – WHY WE NEED EXPLICIT PRODUCT DECISIONS

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

Register risks officially

Make a decision with stakeholders how to handle them

@lisihocke@mastodon.social



WHAT'S THE SECRET INGREDIENT TO CHAMPIONING SECURITY?

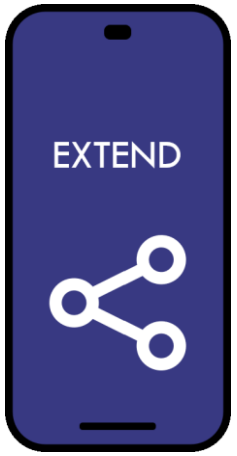
EXTENDING REACH

@lisihocke@mastodon.social

FOSTER RELATIONSHIPS, GROW ALLIES

@lisihocke@mastodon.social

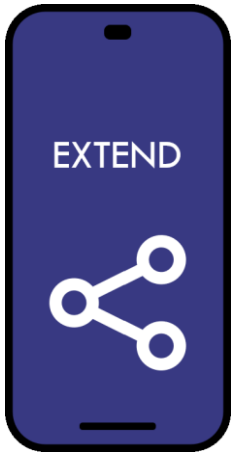
FOSTER RELATIONSHIPS, GROW ALLIES



FOSTER RELATIONSHIPS, GROW ALLIES

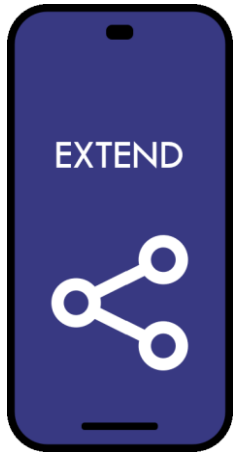
FOSTER RELATIONSHIPS, GROW ALLIES

ANYONE OUT THERE TO LEARN TOGETHER WITH?



@lisihocke@mastodon.social

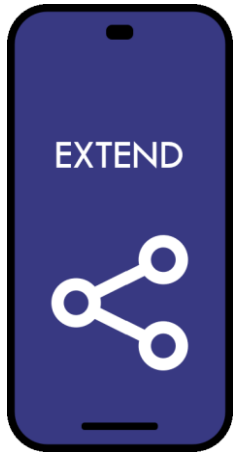
ANYONE OUT THERE TO LEARN TOGETHER WITH?



Engage exchange among security champions

@lisihocke@mastodon.social

ANYONE OUT THERE TO LEARN TOGETHER WITH?



Engage exchange among security champions

Connect with security communities

@lisihocke@mastodon.social

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

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

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

@lisihocke@mastodon.social

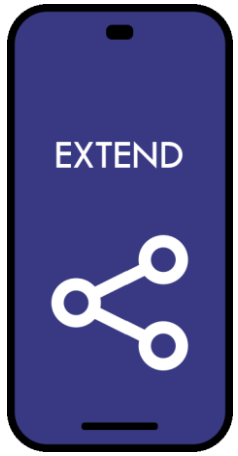
WHAT WORKED, WHAT DIDN‘T, WHAT WE REALLY SHOULDN‘T HAVE DONE IN THE FIRST PLACE

@lisihocke@mastodon.social

WHAT WORKED, WHAT DIDN‘T, WHAT WE REALLY SHOULDN‘T HAVE DONE IN THE FIRST PLACE

WHAT WORKED, WHAT DIDN‘T, WHAT WE REALLY SHOULDN‘T HAVE DONE IN THE FIRST PLACE

WHAT WORKED, WHAT DIDN‘T, WHAT WE REALLY SHOULDN‘T HAVE DONE IN THE FIRST PLACE



Worked: investing in a security culture

Did not work: not using our veto

Don’t even consider: inaction

@lisihocke@mastodon.social

KEEP GOING, SMALL STEPS CUMULATE!

@lisihocke@mastodon.social

KEEP GOING, SMALL STEPS CUMULATE!

@lisihocke@mastodon.social

bit.ly/lisihocke-security-resources

@lisihocke@mastodon.social

bit.ly/lisihocke-security-resources

Make things a bit more secure than yesterday every day

@lisihocke@mastodon.social

bit.ly/lisihocke-security-resources

Make things a bit more secure than yesterday every day

THANK YOU!

www.lisihocke.com

@lisihocke@mastodon.social