



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

LISI HOCKE

[@lisihocke@mastodon.social](https://mastodon.social/@lisihocke)

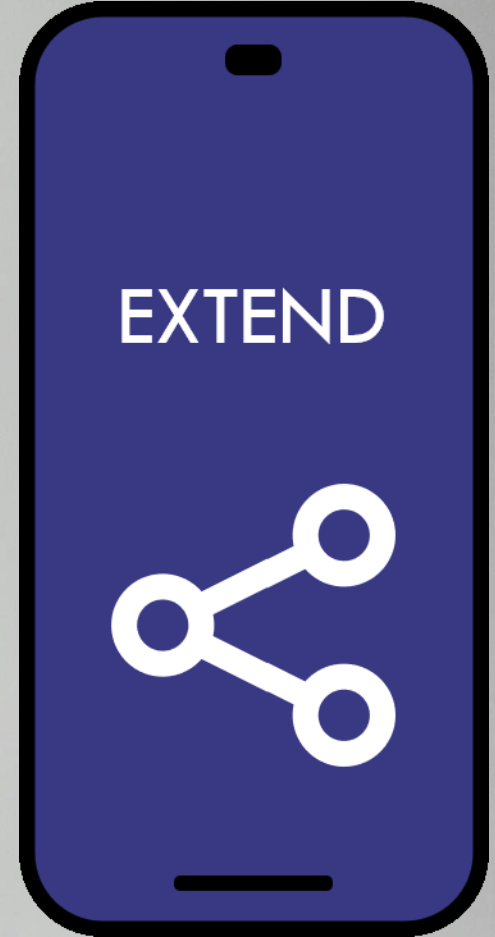














WAIT, I HAVE THE OPTION TO  
SKILL UP IN SECURITY?

UNLOCKING  
SECURITY

UNLOCK



@lisihocke@mastodon.social



# HI, I'M A SPECIALIZED GENERALIST



[@lisihocke@mastodon.social](https://mastodon.social/@lisihocke)



# HI, I'M A SPECIALIZED GENERALIST

UNLOCK



Testing & quality

@lisihocke@mastodon.social



# HI, I'M A SPECIALIZED GENERALIST

UNLOCK



Testing & quality

Product development teams

@lisihocke@mastodon.social



# HI, I'M A SPECIALIZED GENERALIST

UNLOCK



Testing & quality

Product development teams

Cross-functional

@lisihocke@mastodon.social



# HI, I'M A SPECIALIZED GENERALIST

UNLOCK



Testing & quality

Product development teams

Cross-functional

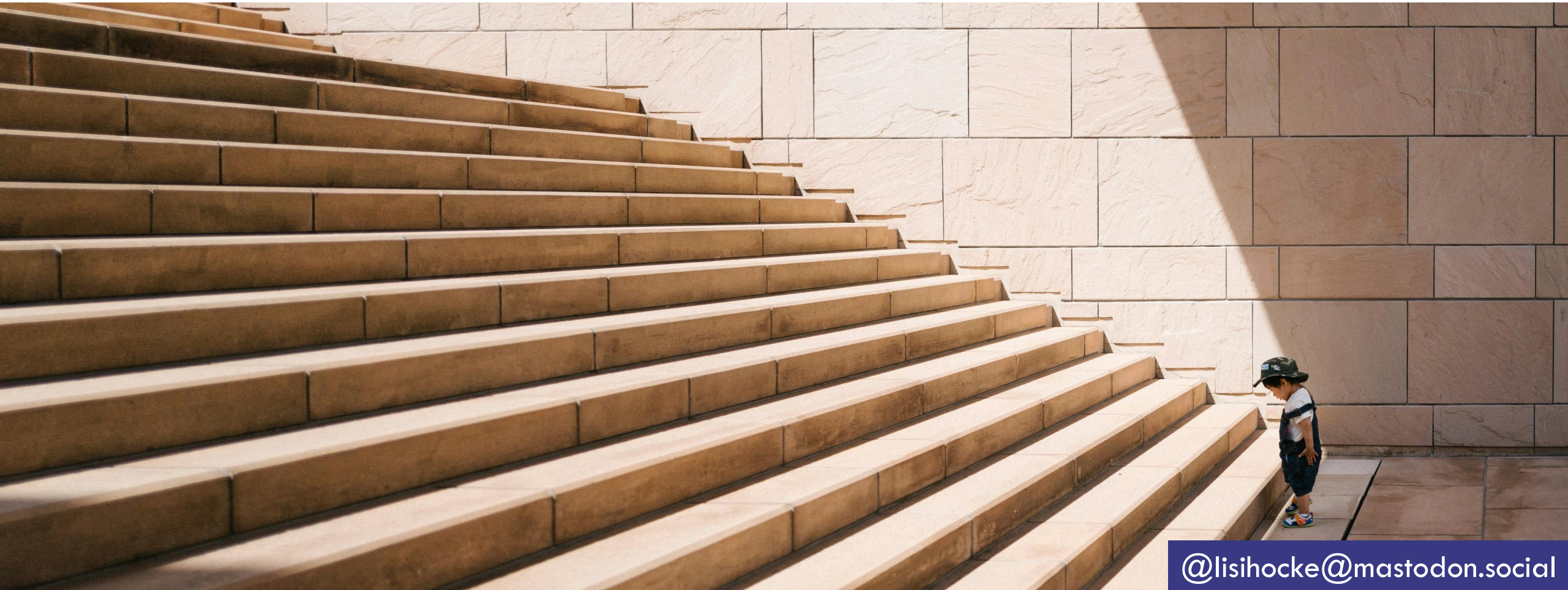
Embedded hands-on

@lisihocke@mastodon.social



# STEP BY STEP INTO SECURITY

UNLOCK



@lisihocke@mastodon.social



# STEP BY STEP INTO SECURITY

UNLOCK



It all started with OWASP Juice Shop

@lisihocke@mastodon.social



# STEP BY STEP INTO SECURITY

UNLOCK



Bringing security mindset into the team

It all started with OWASP Juice Shop

@lisihocke@mastodon.social



# STEP BY STEP INTO SECURITY

UNLOCK



Continued learning in my personal time

Bringing security mindset into the team

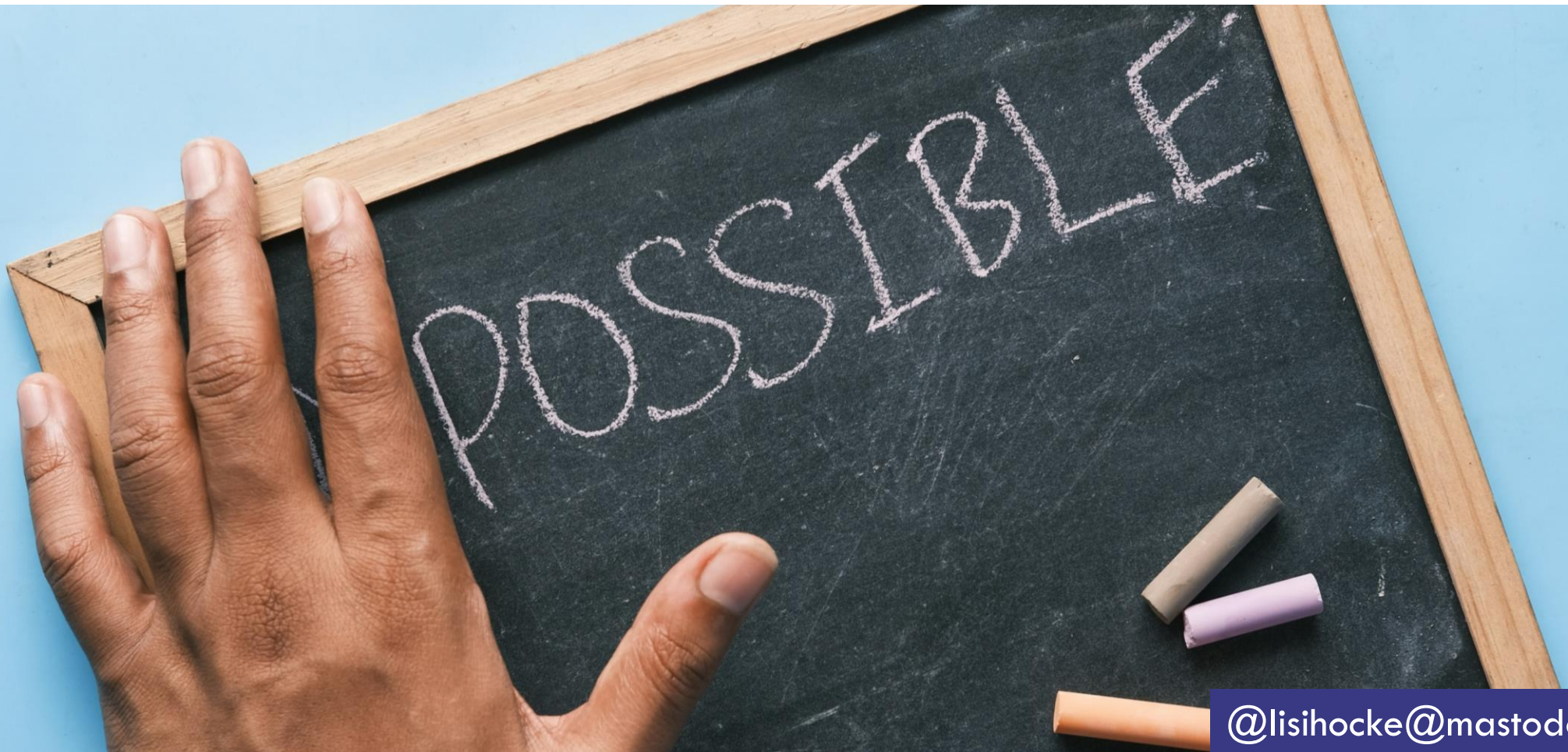
It all started with OWASP Juice Shop

@lisihocke@mastodon.social



# NEW COMPANY, NEW PRODUCT, NEW CHALLENGE

UNLOCK



@lisihocke@mastodon.social



# NEW COMPANY, NEW PRODUCT, NEW CHALLENGE

UNLOCK



Mobile

POSSIBLE

@lisihocke@mastodon.social



# NEW COMPANY, NEW PRODUCT, NEW CHALLENGE

UNLOCK



Mobile

Health

POSSIBLE

@lisihocke@mastodon.social



# NEW COMPANY, NEW PRODUCT, NEW CHALLENGE

UNLOCK



Mobile

Health

Regulated

POSSIBLE

@lisihocke@mastodon.social



# NEW COMPANY, NEW PRODUCT, NEW CHALLENGE

UNLOCK



Mobile

Health

Regulated

Security team

POSSIBLE

@lisihocke@mastodon.social



# NEW COMPANY, NEW PRODUCT, NEW CHALLENGE

UNLOCK



Mobile

Health

Security team

Regulated

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

UNLOCK



What is a security champion in a nutshell?



@lisihocke@mastodon.social



# ACTING LIKE A CHAMPION WITHOUT BEING THE APPOINTED CHAMPION

UNLOCK



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

UNLOCK



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

UNLOCK



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

UNLOCK



@lisihocke@mastodon.social



# FIRST AUDIT — BUILDING OUR ASSET INVENTORY

UNLOCK



What's to protect?

@lisihocke@mastodon.social



# FIRST AUDIT — BUILDING OUR ASSET INVENTORY

UNLOCK



What's to protect?

What's public facing?

@lisihocke@mastodon.social



# FIRST AUDIT — BUILDING OUR ASSET INVENTORY

UNLOCK



What's to protect?

What's public facing?

How confidential is it?

@lisihocke@mastodon.social



# FIRST AUDIT — BUILDING OUR ASSET INVENTORY

UNLOCK



What's to protect?

What's public facing?

How confidential is it?

What's the business risk if breached?

@lisihocke@mastodon.social



# FIRST AUDIT — BUILDING OUR ASSET INVENTORY

UNLOCK



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?

@lisihocke@mastodon.social





**YAY, I'M THE OFFICIAL MOBILE  
SECURITY CHAMPION!**

**ADVOCATING  
HANDS-ON**

[@lisihocke@mastodon.social](https://mastodon.social/@lisihocke)



# A MOBILE APPSEC STRATEGY TO RULE THEM ALL

ADVOCATE



[@lisihocke@mastodon.social](https://mstdn.social/@lisihocke)



# A MOBILE APPSEC STRATEGY TO RULE THEM ALL

ADVOCATE



Helps align on a common goal



@lisihocke@mastodon.social



# A MOBILE APPSEC STRATEGY TO RULE THEM ALL

ADVOCATE



Helps align on a common goal

Serves as reference



@lisihocke@mastodon.social



# A MOBILE APPSEC STRATEGY TO RULE THEM ALL

ADVOCATE



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

ADVOCATE



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

ADVOCATE



@lisihocke@mastodon.social



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

ADVOCATE



Throwing more tools  
on it won't fix it

@lisihocke@mastodon.social



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

ADVOCATE



Throwing more tools  
on it won't fix it

Focus on cleaning up the noise

@lisihocke@mastodon.social



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

ADVOCATE



Throwing more tools  
on it won't fix it

Focus on cleaning up the noise

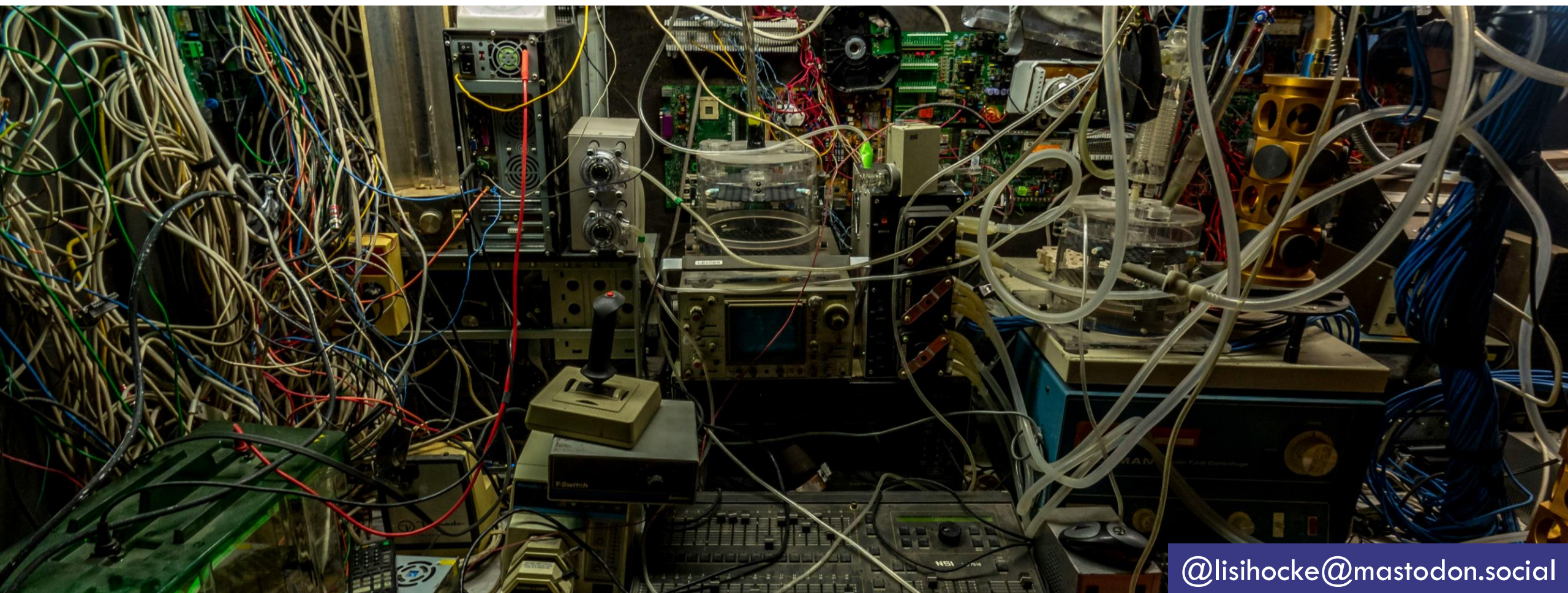
Be intentional about the tools you  
use and what value they bring

@lisihocke@mastodon.social



# OH MY, ALL THESE DEPENDENCIES...

ADVOCATE



@lisihocke@mastodon.social



# OH MY, ALL THESE DEPENDENCIES...

ADVOCATE



Just do it, often  
and regularly

@lisihocke@mastodon.social



# OH MY, ALL THESE DEPENDENCIES...

ADVOCATE



Just do it, often  
and regularly

Start where the  
risk is highest

@lisihocke@mastodon.social



# OH MY, ALL THESE DEPENDENCIES...

ADVOCATE



Just do it, often  
and regularly

Start where the  
risk is highest

Tackle quick  
wins first

@lisihocke@mastodon.social



# OH MY, ALL THESE DEPENDENCIES...

ADVOCATE



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...

ADVOCATE



Just do it, often  
and regularly

Start where the  
risk is highest

Tackle quick  
wins first

Write out steps  
for big upgrades

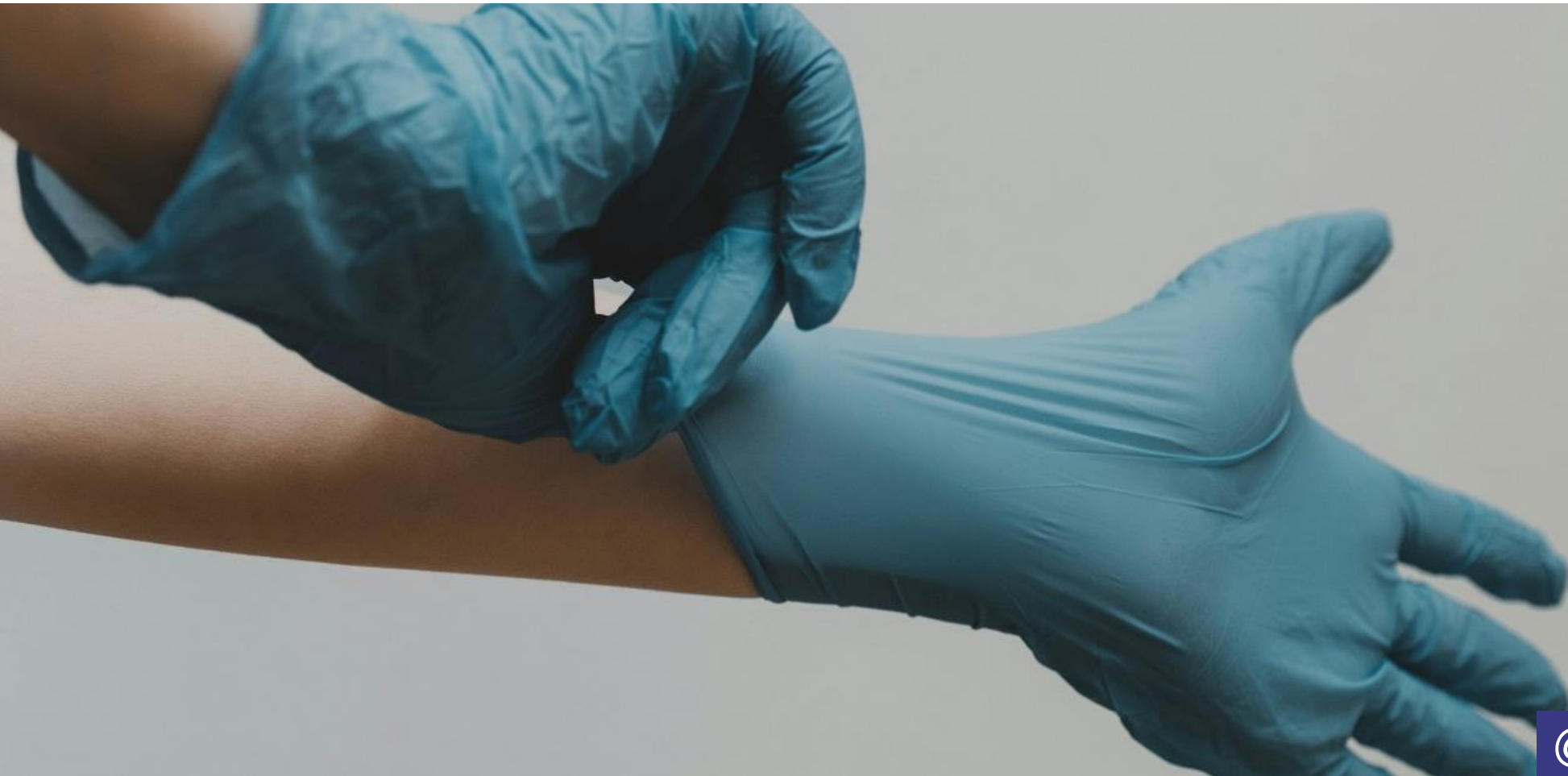
Cling to a working  
update strategy

@lisihocke@mastodon.social



# CLEANUPS REDUCE THE ATTACK SURFACE

ADVOCATE



[@lisihocke@mastodon.social](https://mastodon.social/@lisihocke)



# CLEANUPS REDUCE THE ATTACK SURFACE

ADVOCATE



“Technical debt is security debt.”  
— Tanya Janca

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

@lisihocke@mastodon.social



# CLEANUPS REDUCE THE ATTACK SURFACE

ADVOCATE



“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

@lisihocke@mastodon.social



# CLEANUPS REDUCE THE ATTACK SURFACE

ADVOCATE



“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

@lisihocke@mastodon.social



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

ADVOCATE



@lisihocke@mastodon.social



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

ADVOCATE



Get insecure  
implementations  
out right away



@lisihocke@mastodon.social



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

ADVOCATE



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

ADVOCATE



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

ADVOCATE



@lisihocke@mastodon.social



# WOW, SO MANY FOLKS ARE PROBING OUR SYSTEM — CONSTANTLY

ADVOCATE



Observe frequently and regularly



@lisihocke@mastodon.social



# WOW, SO MANY FOLKS ARE PROBING OUR SYSTEM — CONSTANTLY

ADVOCATE



Observe frequently and regularly

Get alerted on potentially malicious activity and leaks

@lisihocke@mastodon.social



# WOW, SO MANY FOLKS ARE PROBING OUR SYSTEM — CONSTANTLY

ADVOCATE



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

ADVOCATE



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

ADVOCATE



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

@lisihocke@mastodon.social



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

ADVOCATE



[@lisihocke@mastodon.social](https://social.mastodon.social/@lisihocke)



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

ADVOCATE



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

ADVOCATE



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

ADVOCATE



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





EXTEND



# WHAT'S THE SECRET INGREDIENT TO CHAMPIONING SECURITY?

EXTENDING  
REACH

@lisihocke@mastodon.social



# FOSTER RELATIONSHIPS, GROW ALLIES

EXTEND



@lisihocke@mastodon.social



# FOSTER RELATIONSHIPS, GROW ALLIES

EXTEND



Close collaboration with  
your security team

@lisihocke@mastodon.social



# FOSTER RELATIONSHIPS, GROW ALLIES

EXTEND



Close collaboration with  
your security team

Take your own  
team with you

@lisihocke@mastodon.social



# FOSTER RELATIONSHIPS, GROW ALLIES

EXTEND



Close collaboration with  
your security team

Take your own  
team with you

Experiment with  
different approaches to  
figure out what works

@lisihocke@mastodon.social



# ANYONE OUT THERE TO LEARN TOGETHER WITH?

EXTEND



@lisihocke@mastodon.social



# ANYONE OUT THERE TO LEARN TOGETHER WITH?

EXTEND



Engage exchange  
among security  
champions

I'm  
not  
Alone



@lisihocke@mastodon.social



# ANYONE OUT THERE TO LEARN TOGETHER WITH?

EXTEND



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

EXTEND



@lisihocke@mastodon.social



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

EXTEND



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

EXTEND



[@lisihocke@mastodon.social](https://mastodon.social/@lisihocke)



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

EXTEND



Worked: investing  
in a security culture

@lisihocke@mastodon.social



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

EXTEND



Worked: investing  
in a security culture

Did not work: not  
using our veto

@lisihocke@mastodon.social



# 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!

EXTEND



@lisihocke@mastodon.social



# KEEP GOING, SMALL STEPS CUMULATE!

EXTEND

A person wearing bright orange sneakers and black socks is climbing a blue metal staircase. The stairs are wet, and the person's legs are in motion, with one foot on a higher step and the other on a lower one. A dark blue text box is overlaid on the right side of the image.

Opt for many small steps, continuously

[@lisihocke@mastodon.social](https://mastodon.social/@lisihocke)



WISH FOR IT  
HOPE FOR IT  
DREAM OF IT

BUT BY  
ALL MEANS  
DO IT



[bit.ly/lisihocke-security-resources](https://bit.ly/lisihocke-security-resources)

UNLOCK



ADVOCATE



EXTEND



[@lisihocke@mastodon.social](https://mastodon.social/@lisihocke)



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](https://bit.ly/lisihocke-security-resources)

UNLOCK



ADVOCATE



EXTEND



[@lisihocke@mastodon.social](https://mastodon.social/@lisihocke)



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](https://bit.ly/lisihocke-security-resources)

UNLOCK



ADVOCATE



EXTEND



THANK YOU!

[www.lisihocke.com](https://www.lisihocke.com)

[@lisihocke@mastodon.social](https://@lisihocke@mastodon.social)