Security is everybody's job….
Literally!

Changing DevOps into DevSecOps

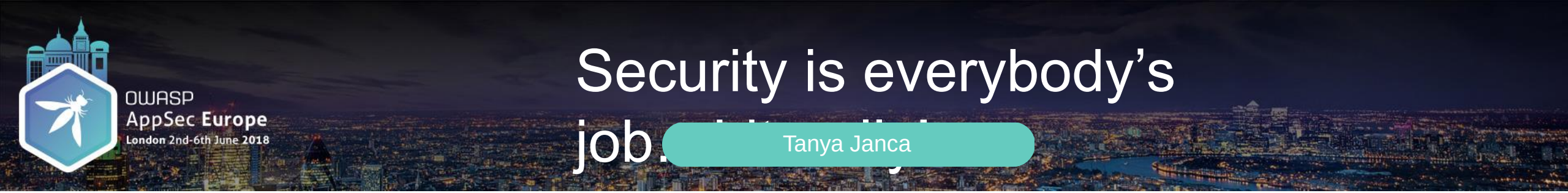
Tanya Janca

Security is everybody's job.

Tanya Janca

Security is everybody's job.

Tanya Janca



@SheHacksPurple

Security is everybody's job.

Tanya Janca

Security is everybody's job.

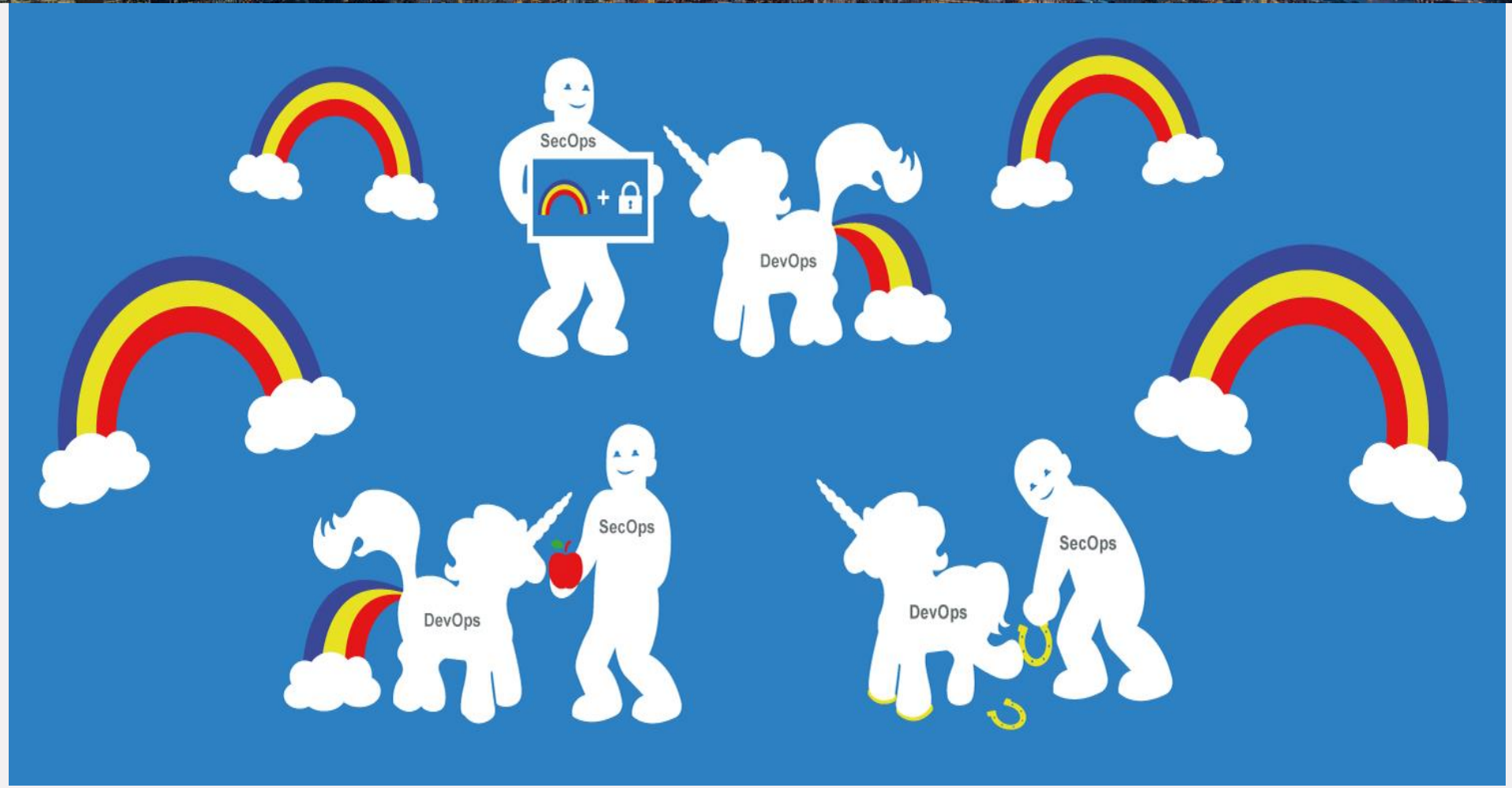
Tanya Janca

How some security people see DevOps

Slide Credit: Pete Cheslock

Security is everybody's job.

Tanya Janca

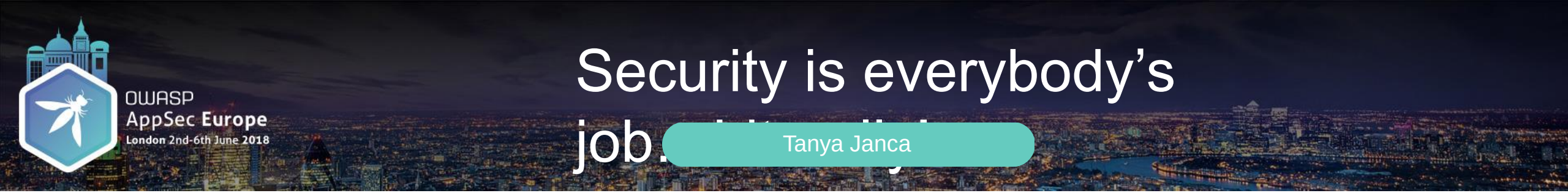


How I see DevOps: DevSecOps

Slide Credit:
DevSecCon

Security is everybody's job.

Tanya Janca



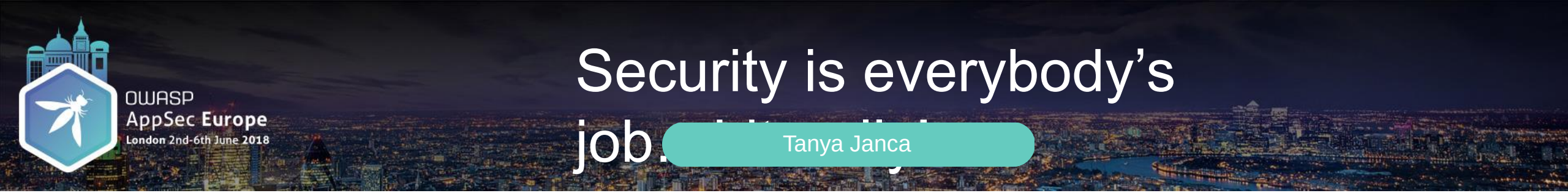
Security is everybody's job.

Tanya Janca

This is me.

I'm Tanya Janca.

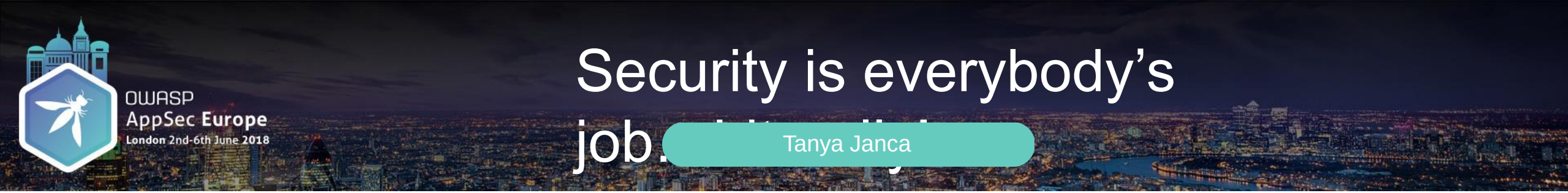
@SheHacksPurple



This is me.

I'm a Senior Cloud Developer Advocate at:

What does **THAT** mean?



Security is everybody's job.

Tanya Janca

This is me.

I'm a Senior Cloud Developer Advocate at:

It means I help developers use our products more securely.

I provide feedback to make our products more secure.

I do security research and share it with the community.

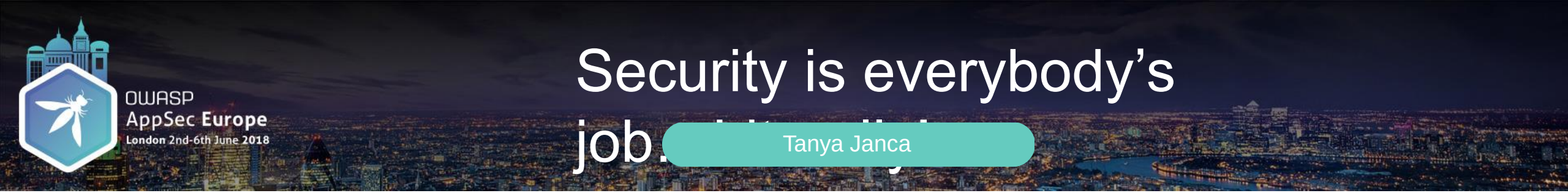
I work to make security features easier to use.

Security research, such as this presentation, OWASP DevSlop, and much more.

Security is everybody's job.

Tanya Janca

This is me. AppSec Evangelist.



Security is everybody's job.

Tanya Janca

This is me. AppSec Evangelist.

@SheHacksPurple

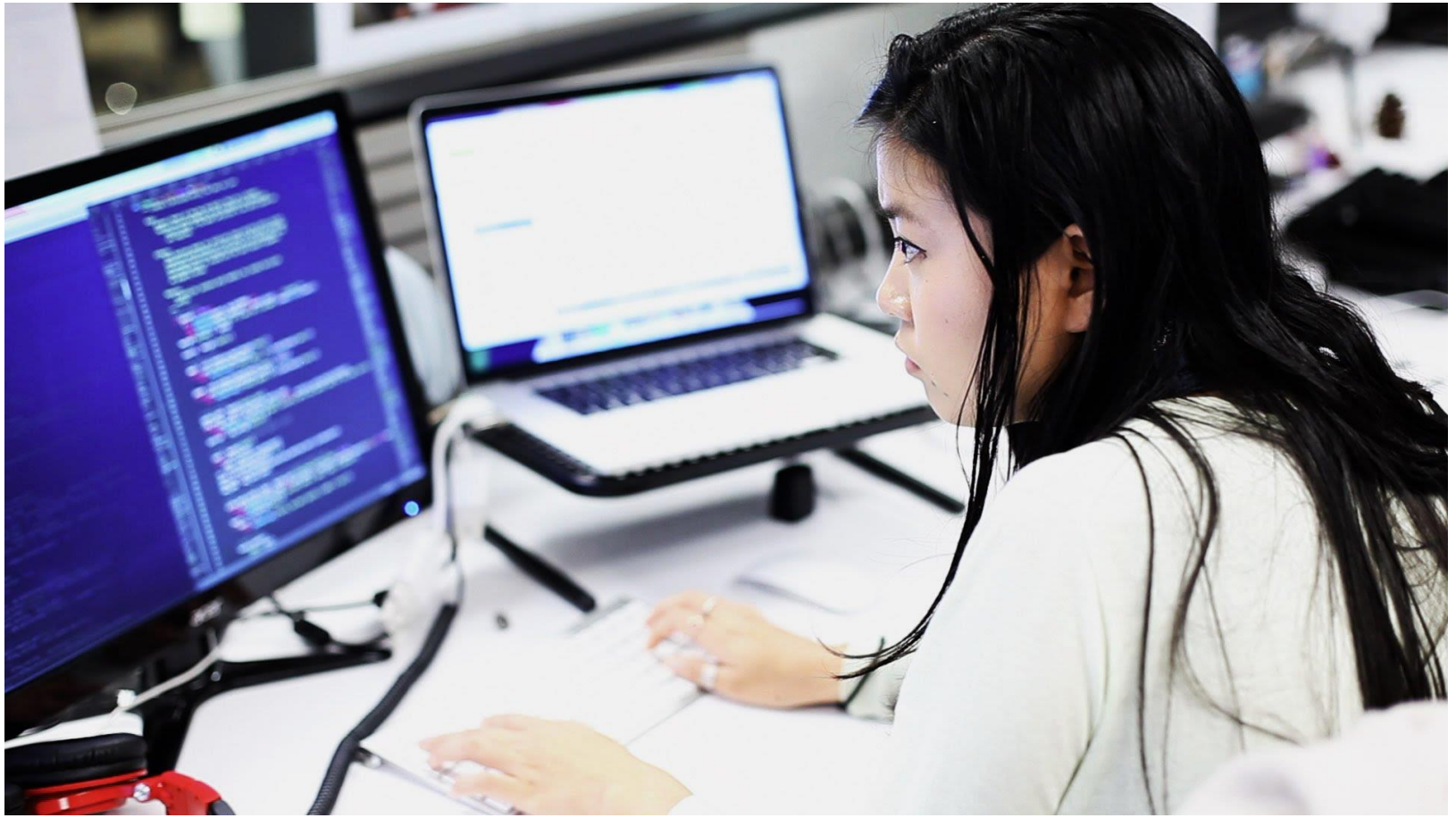
Security is everybody's job.

Tanya Janca

I want to know how things work.

This is me.

Ethical hacker



Security is everybody's job.

Tanya Janca

This is me.

I **LOVE** OWASP!

Open Web Application Security Project

An international non-profit that operates chapters, projects and conferences all over the globe, in efforts to help everyone create more secure software.

Security is everybody's job.

Tanya Janca

This is me.

OWASP Ottawa
Chapter Leader

@SheHacksPurple

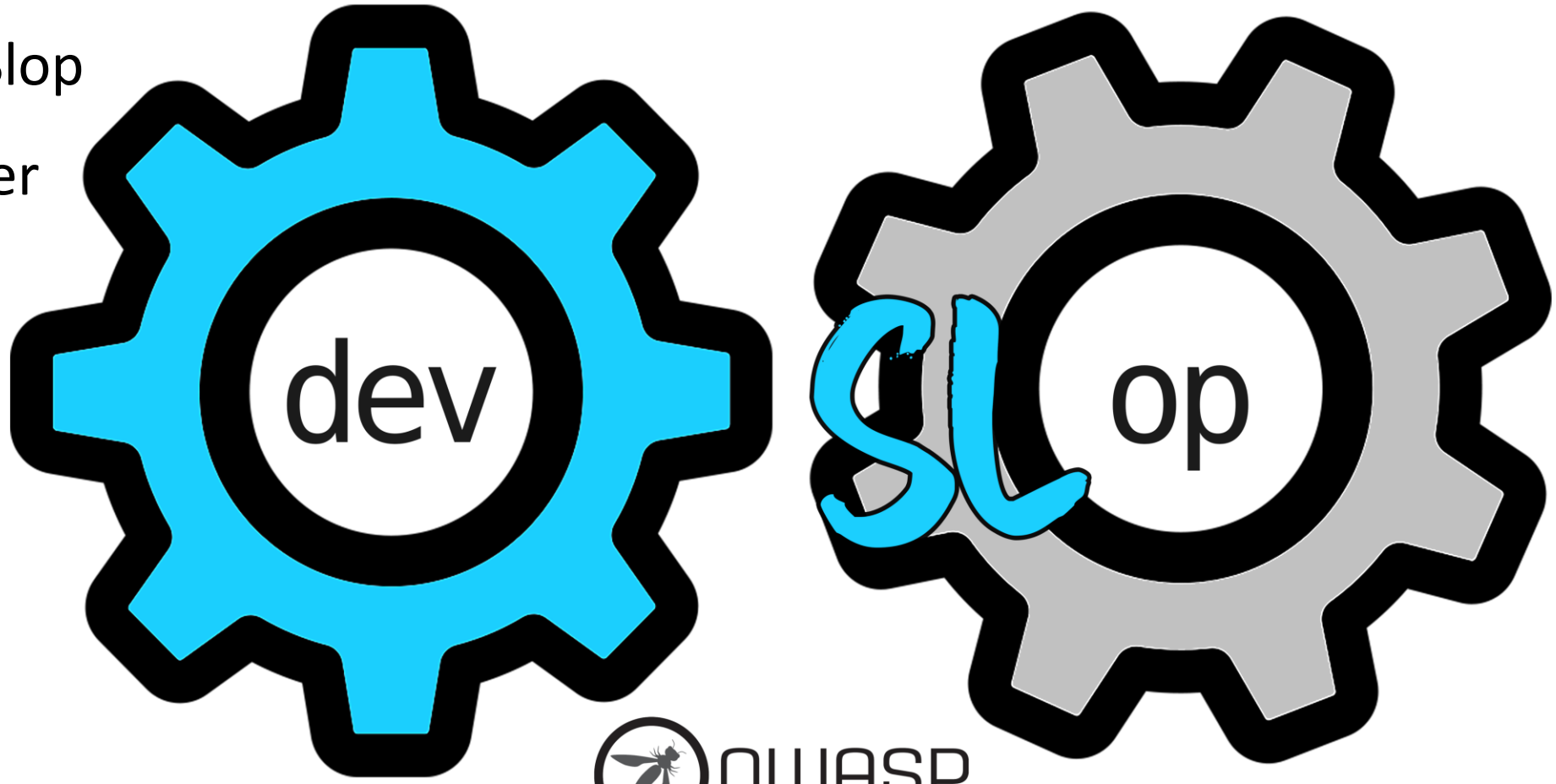
Security is everybody's job.

Tanya Janca

This is me.

OWASP DevSlop

Project Leader



Security is everybody's job.

Tanya Janca

This is me.

Software Developer

(since the late 90's)

That's over 20 years!

AHHHHHHHHHHHH!

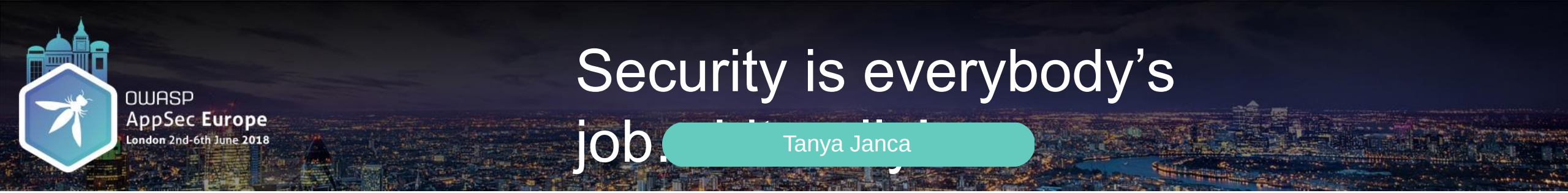
Security is everybody's job.

Tanya Janca

Photo: Belfast, Ireland, AppSec EU 2017

This is me.

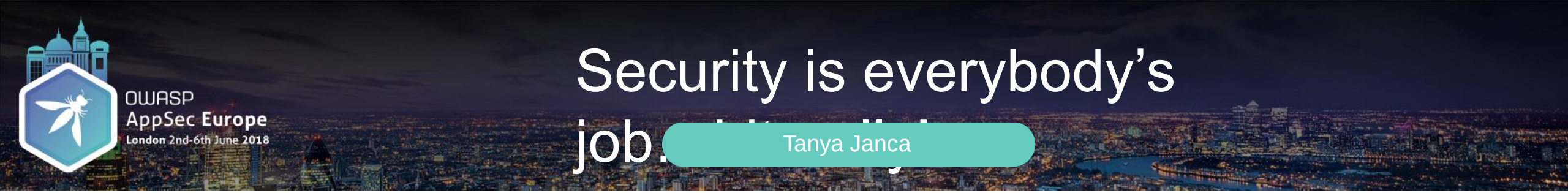
Goal: to change the way we make software so that the easiest way to do something is also the most secure way.


OWASP
AppSec Europe
London 2nd-6th June 2018
Security is everybody's
job.
Tanya Janca

Let's do this.

Introduction

Application Security



What IS AppSec?

"It's any and every activity that you perform to ensure that your software is secure."

-Me

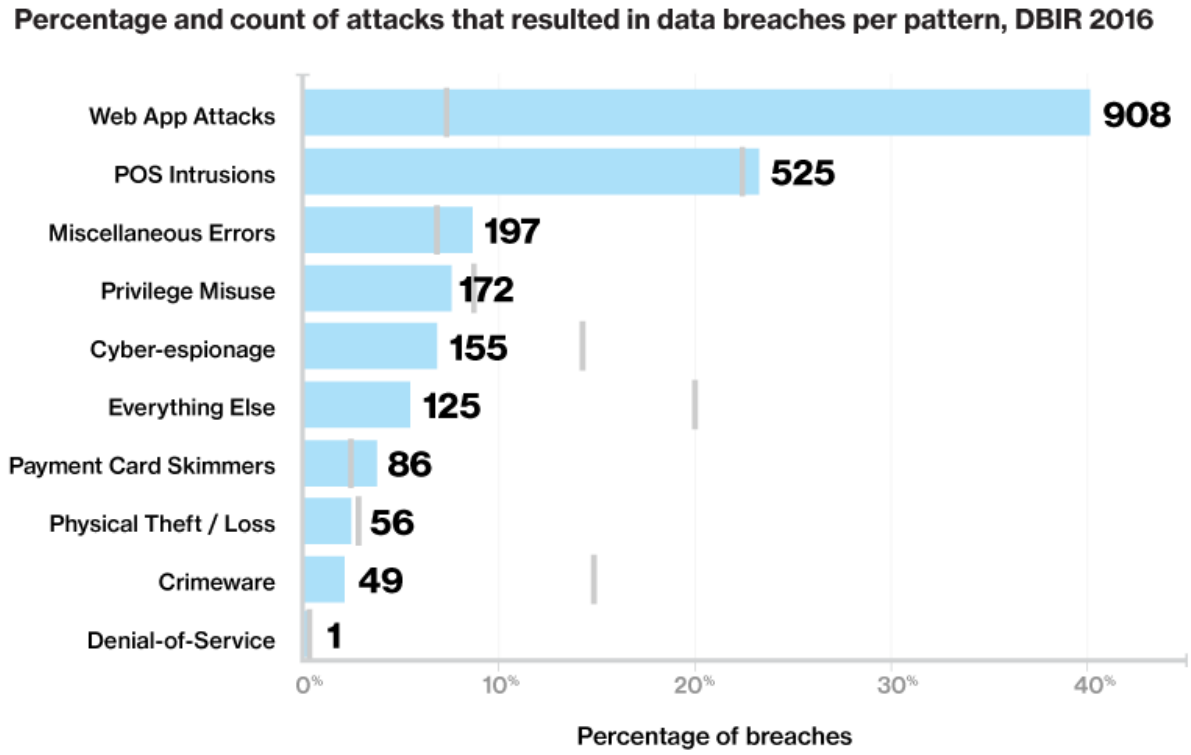
Security is everybody's job.

Tanya Janca

Poor AppSec is a Problem!

Poor AppSec Causes 29-40%~ of Breaches!

Verizon Data Breach Investigation Report (DBIR) for 2017 and 2016.



Security is everybody's job.

Tanya Janca

Application Security Missing!

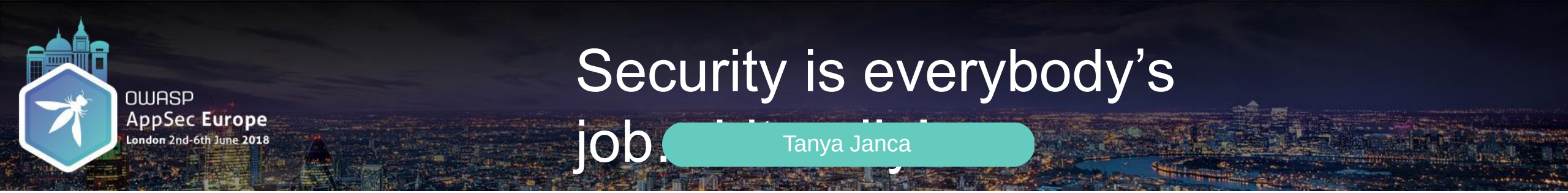
AppSec is not covered in most post-secondary Comp-Sci and Soft-Eng programs

And when it is, it's often an after thought.

Security is everybody's job.

Tanya Janca

Photo: #WOCTechChat



Security is Outnumbered!

Dev / Ops / Sec

100 / 10 / 1

Security is everybody's job.

Tanya Janca

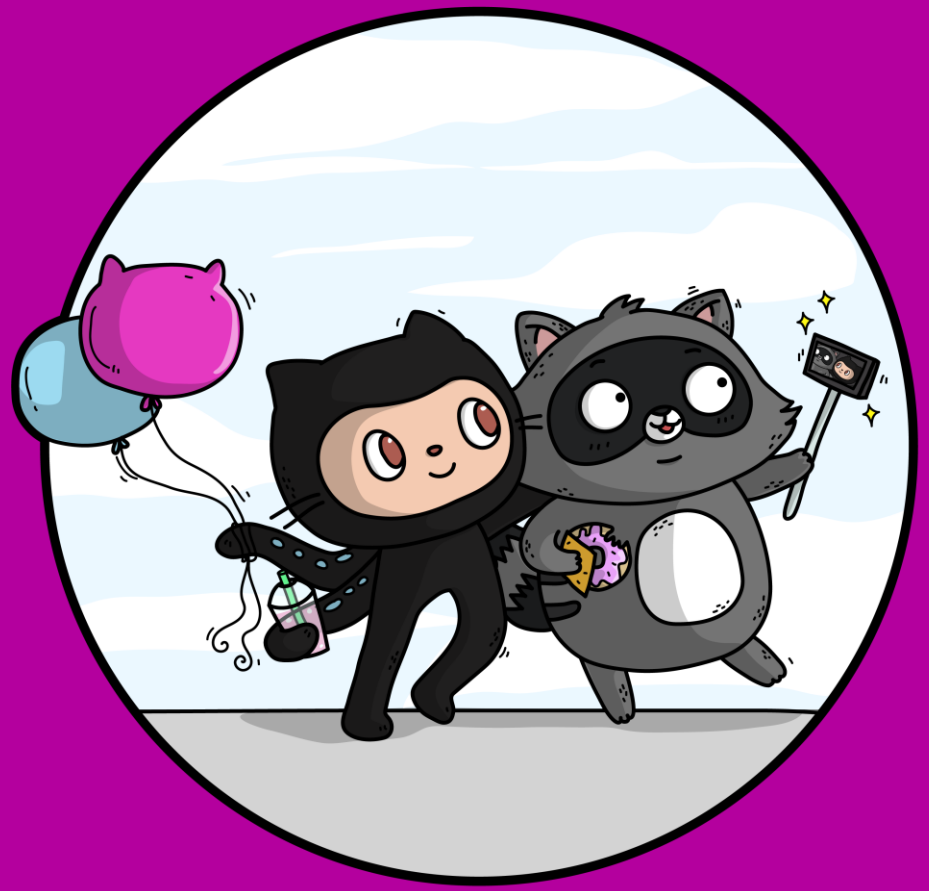
Waterfall Never Worked Well

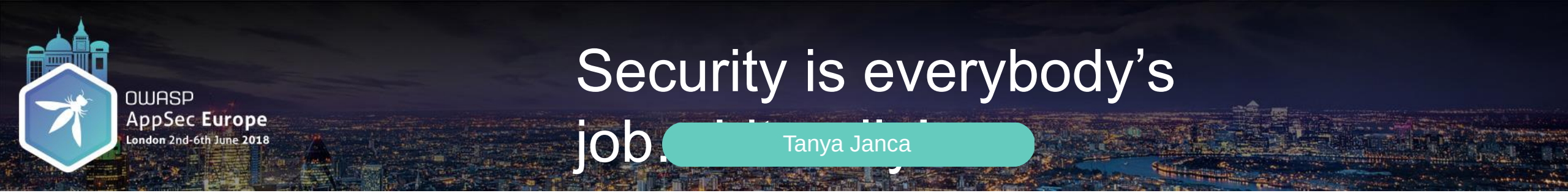
And the accompanying security model was much, much worse.

Image: Winged Beast

DevOps

Main Goals





Improved Deployment Frequency

Security emergencies can be fixed NOW.

Security is everybody's job.

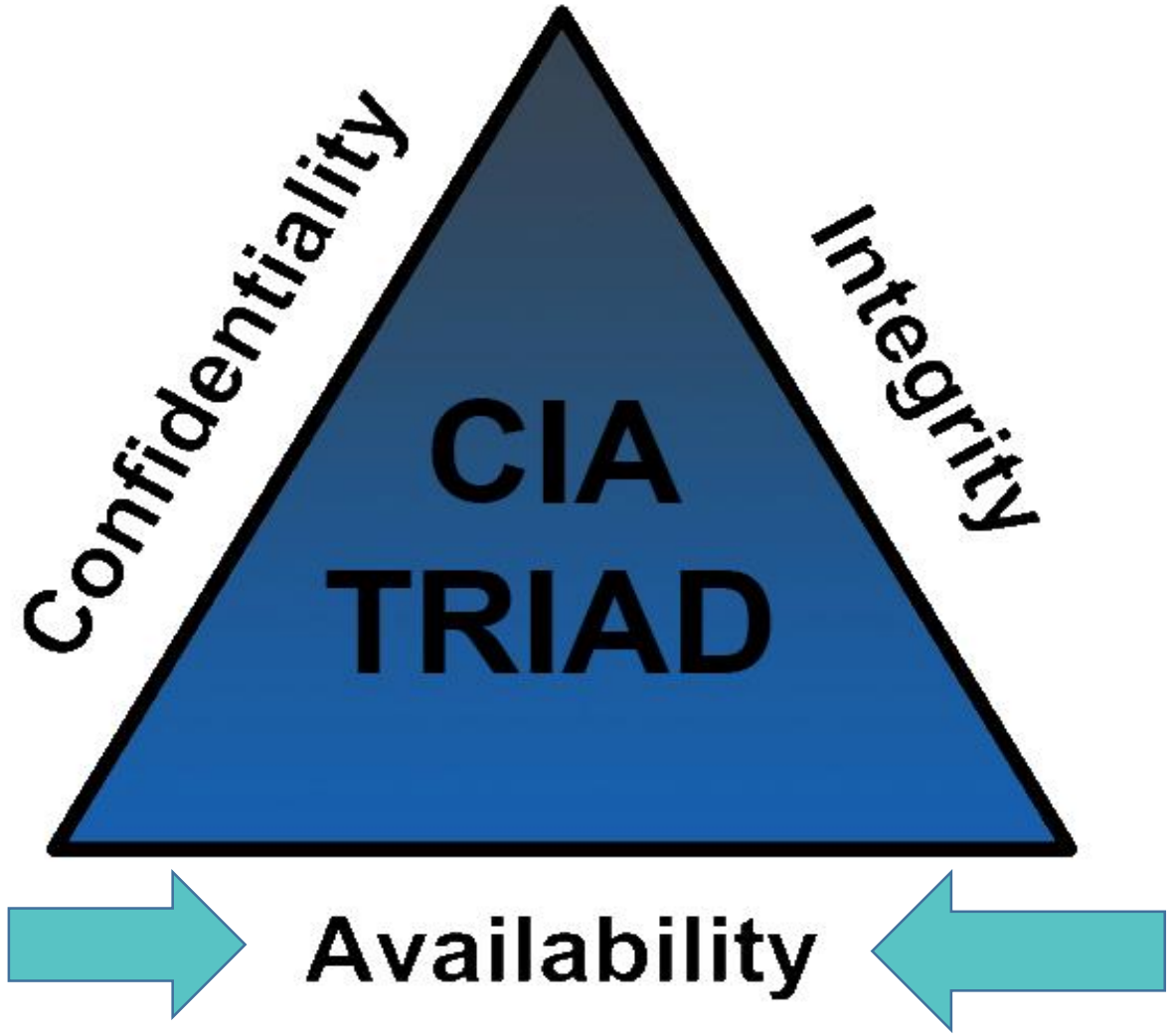
Tanya Janca

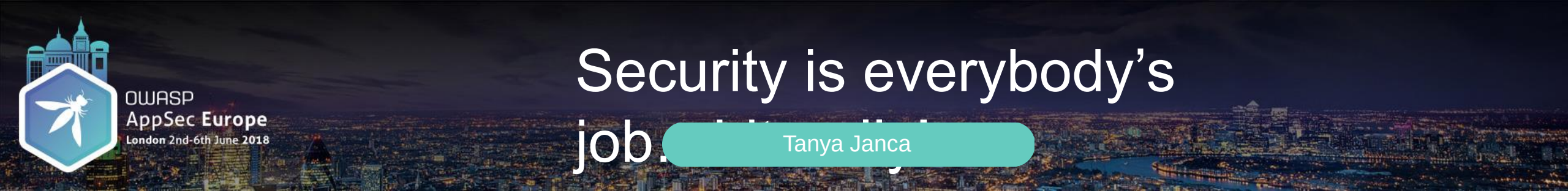
Lower Failure Rates

Resiliency

Security is everybody's job.

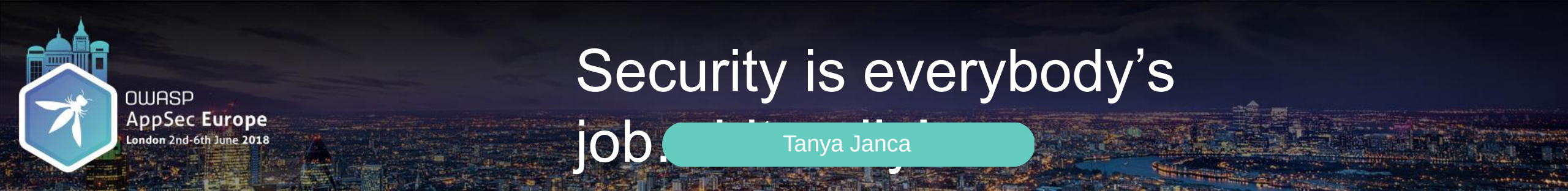
Tanya Janca





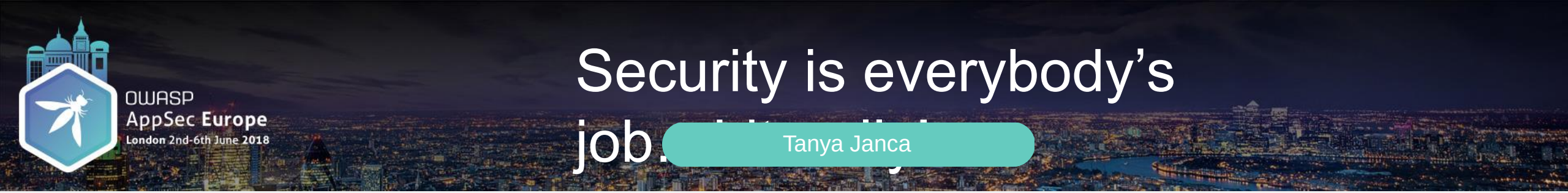
Lower Failure Rates

Resiliency = Confidentiality
Integrity
Availability



Faster Time to Market

Security doesn't win if the business doesn't also win.

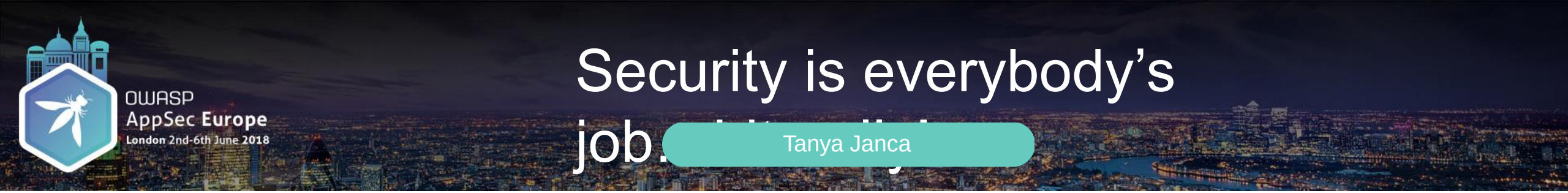


"DevOps is the best thing to happen to Application Security since OWASP. "

-Tanya Janca

DevOps

The Three Ways



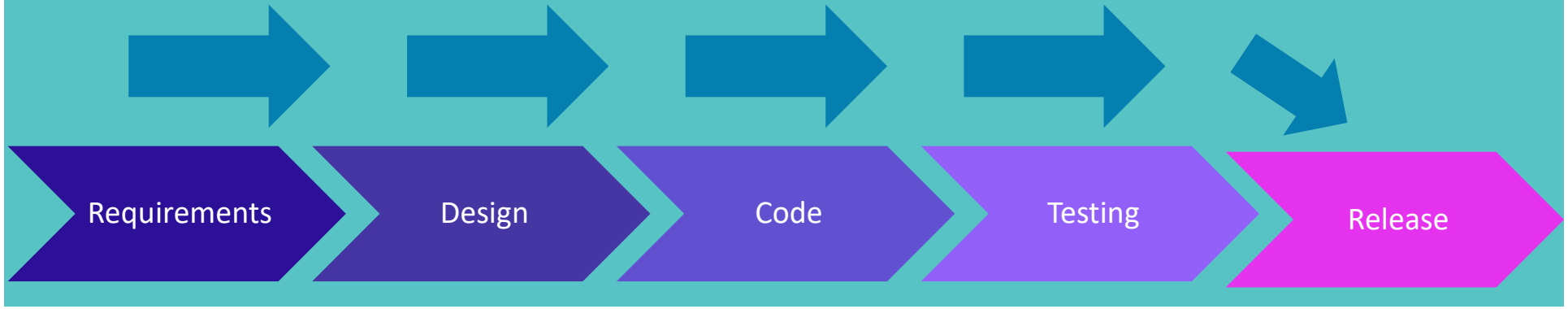
Emphasize the efficiency of the *entire* system.

Left -> Right = speed

Security is everybody's job.

Tanya Janca

Emphasize the efficiency of the *entire* system.



Security is everybody's job.

Tanya Janca

What does this mean for Security?

Photo: #WOCTechChat

Security is everybody's job.

Tanya Janca

What does this mean for dev & ops?

Photo: #WOCTechChat

Security is everybody's job.

Tanya Janca

What does this mean for dev & ops?

Only deploy up-to-date images and containers.

Photo: #WOCTechChat

Security is everybody's job.

Tanya Janca

What does this mean for dev & ops?

The "Photo" Slide, #1

- Helping the AppSec team tune static code analysis tools
- Add security bugs to the defect tracker
- Using templates and code samples that a known-secure (sec code library)
- Using freshly scanned images that are up to date/fully patched
- Setup regular, automated scans for VMs and containers

Security is everybody's job.

Tanya Janca

Help the AppSec Team tune their tools.

For their sake, and yours.

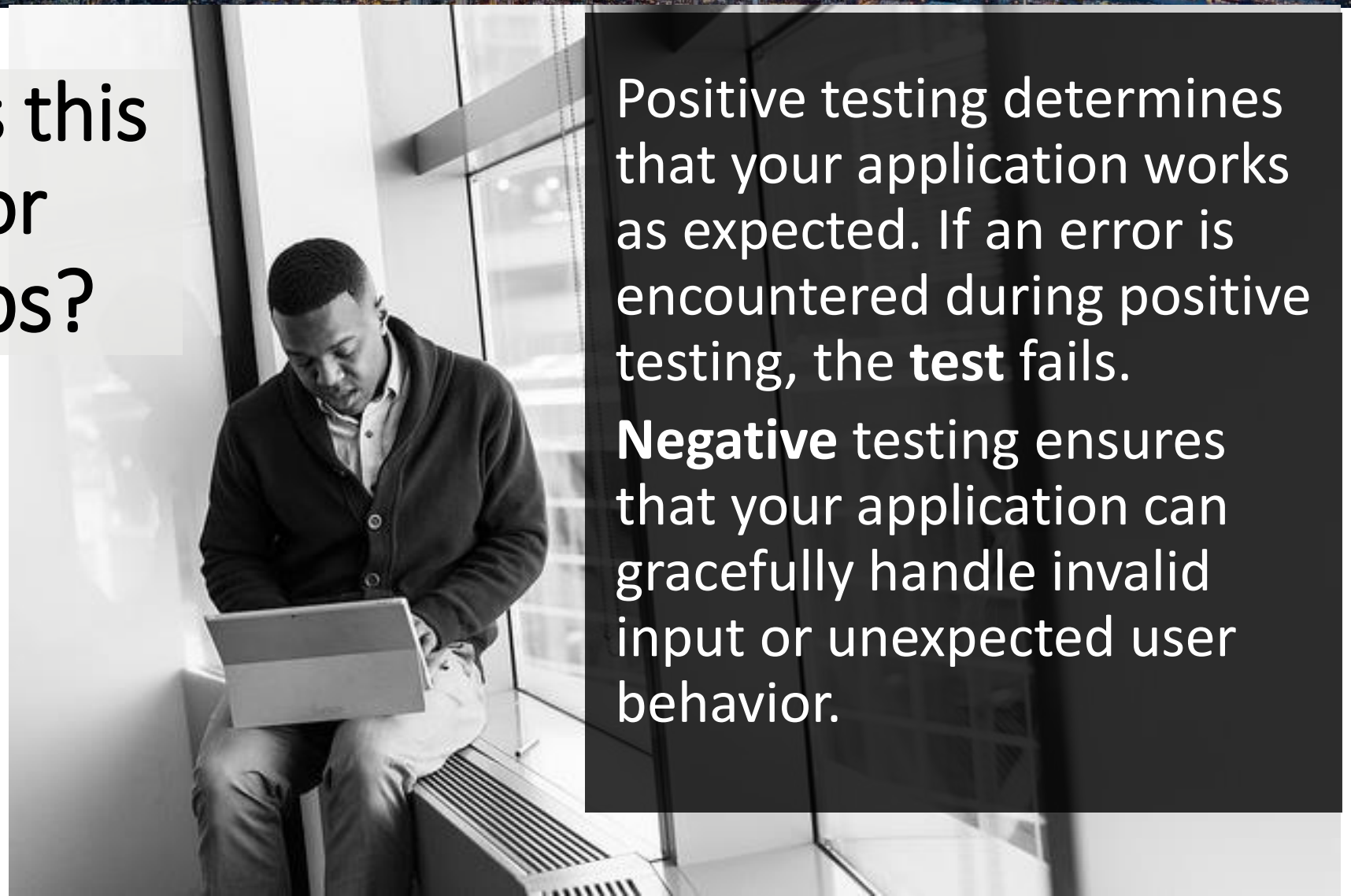
What does this mean for dev & ops?

Photo: #WOCTechChat

Security is everybody's job.

Tanya Janca

What does this mean for dev & ops?



Positive testing determines that your application works as expected. If an error is encountered during positive testing, the **test** fails.

Negative testing ensures that your application can gracefully handle invalid input or unexpected user behavior.

Photo: #WOCTechChat

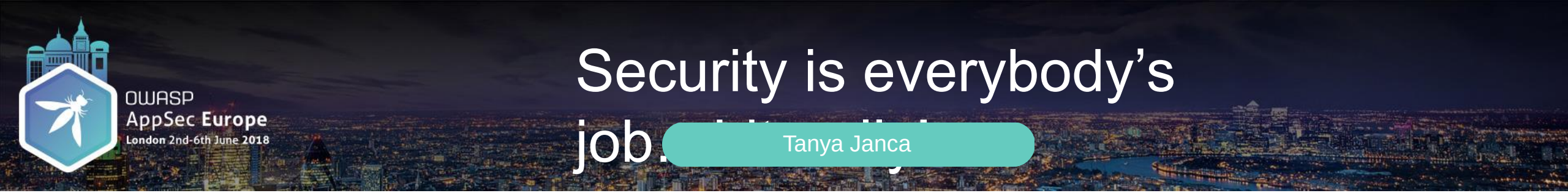
Security is everybody's job.

Tanya Janca

What does this mean for dev & ops?

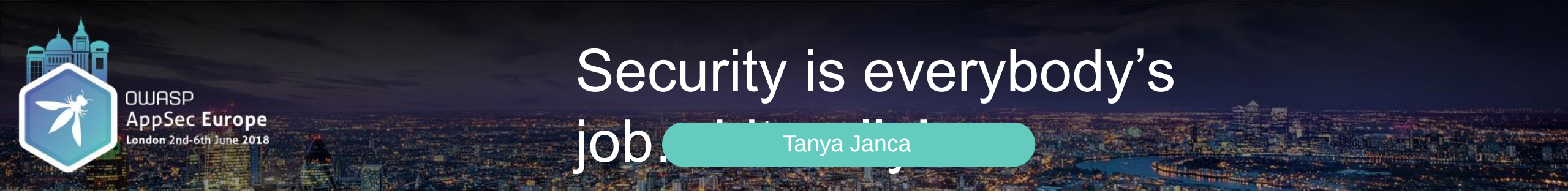
The "Photo" Slide, #2

- Add negative use cases as unit tests, not just positive use cases (Morgan Roman, **@Hackimedes**)
- Helping AppSec team tune web proxy scanners (DAST)
- If the AppSec team creates a security pipeline for testing for you, use it!
- OWASP Dependency check, Retire.js, Synk, Black Duck, etc. Tools to remove known vulnerable code/ libraries/ components



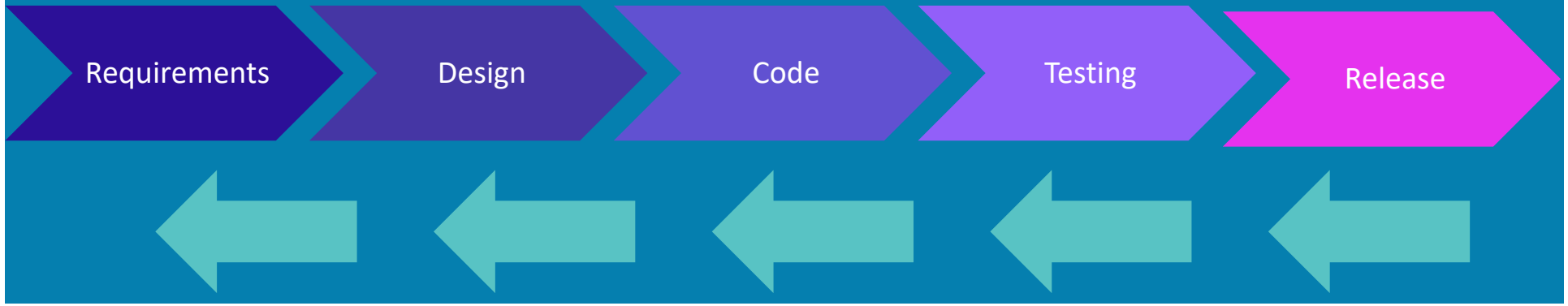
Faster Feedback

Right -> Left = Feedback



Faster Feedback = Pushing Left!

Right -> Left = Feedback

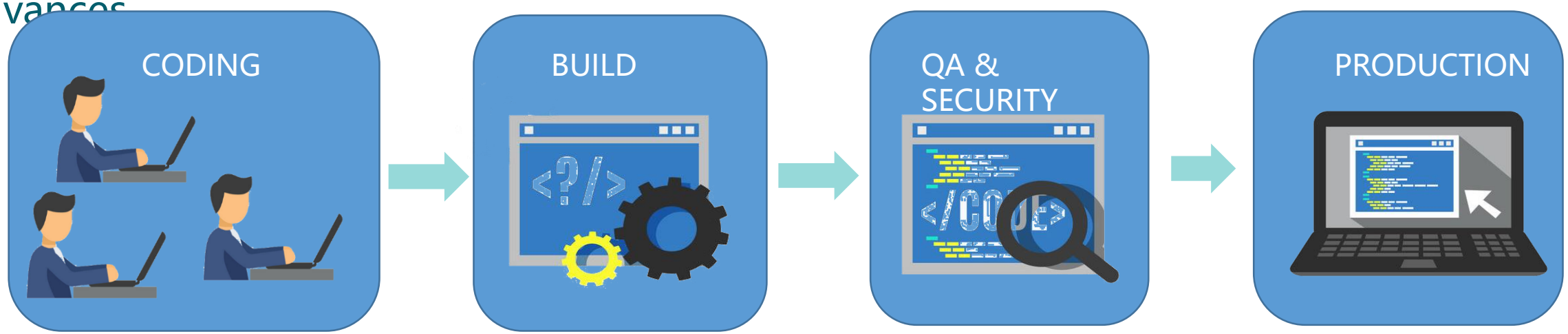


Security is everybody's job.

Tanya Janca

DevOps and the "Shift Left" principal

Fixing costs of quality & security issues rises significantly as the development cycle advances



Source: Ponemon Institute Research

Security is everybody's job.

Tanya Janca

What does this mean for Security?

Photo: #WOCTechChat

Security is everybody's job.

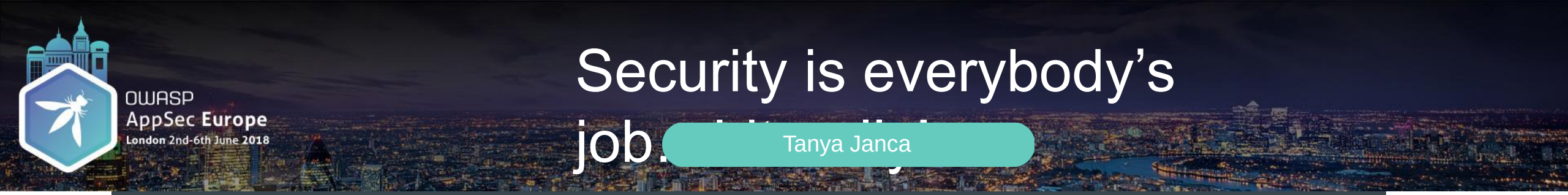
Tanya Janca

What does this mean for dev & ops?

Telling the security team what you are concerned about.

Feedback goes both ways.

Photo: #WOCTechChat



High ROI Security Engineering Tasks

Side Tangent: The SecDevOpronomicon

- Build libraries / tools that are secure by default for dev teams
- E.g. Today, many web frameworks handle output encoding by default
  - Before that, devs had to manually add it everywhere, `h()` in Rails
- Potential areas to consider:
  - Managing secrets
  - Anything related to crypto
  - Authentication / authorization
  - SQL, file system access, shell exec()
  - E.g. `nonCryptographicallySecureMd5()`

Clint Gibler - @clintgibler

Security is everybody's job.

Tanya Janca

What does this mean for dev & ops?

Participating in Security Activities

- Incidents
- Threat Modelling
- Security Sprints
- Etc.

Photo: #WOCTechChat

Security is everybody's job.

Tanya Janca

What does this mean for dev & ops?

The "Photo" Slide, #3

- Faster feedback loops = fixing bugs sooner
- Breaking the build if you introduce security issues
- Adding security sprints to your project timeline
- Participating in Threat modelling activities
- Participating in incident response, if need be
- Learning to use security tools
- Security becomes part of the definition of quality

Security is everybody's job.

Tanya Janca

Continuous Learning

Full Circle

Security is everybody's job.

Tanya Janca

What does this mean for Security?

Photo: #WOCTechChat

Security is everybody's job.

Tanya Janca

What does this mean for dev & ops?

Photo: #WOCTechChat

Security is everybody's job.

Tanya Janca

Photo: #WOCTechChat

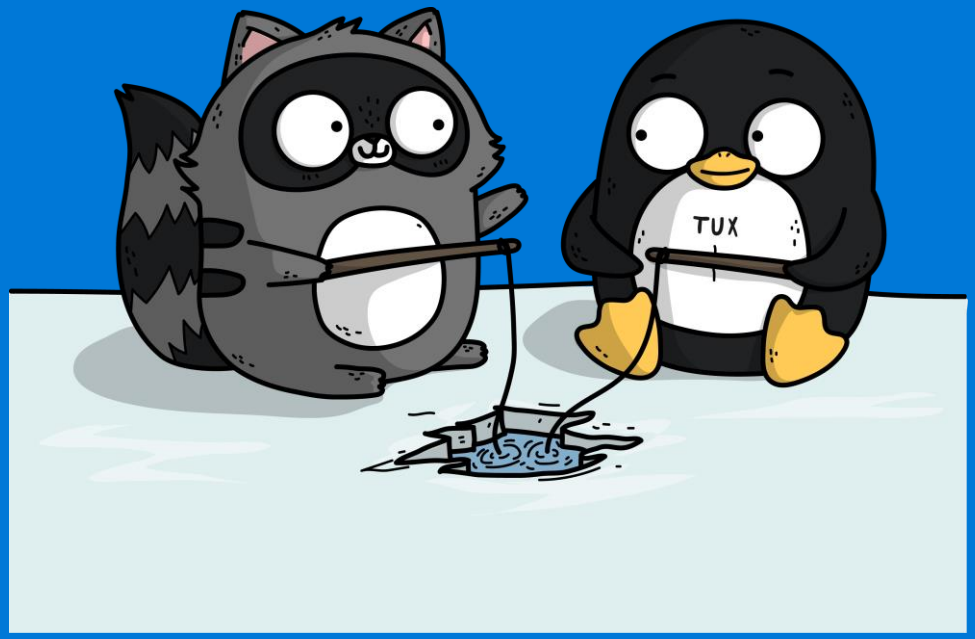
Security is everybody's job.

What does this mean for dev & ops?

The "Photo" Slide, #4

- Accept security training if offered
- Train yourself
- Share information widely when you fix security issues
- Participate in Security Simulations
- Ask for and analyze metrics from security testing, look for patterns or systemic issues
- Ensure you perform blameless introspection

Security is Everybody's Job



Culture Change

Security is everybody's job.

Tanya Janca

Reinforce Culture Change

Photo: #WOCTechChat

Security is everybody's job.

Tanya Janca

Reinforce Culture Change

Photo: #WOCTechChat

Security is everybody's job.

Tanya Janca

Reinforce Culture Change

Photo: #WOCTechChat

Security is everybody's job.

Tanya Janca

Reinforce Culture Change

Photo: #WOCTechChat

Security is everybody's job.

Tanya Janca

Call To Action

Security is everybody's job.

Tanya Janca

Call To Action

The definition of quality must include "secure".

Resilience
Learning
Speed
Feedback

Conclusion

Security is everybody's job.

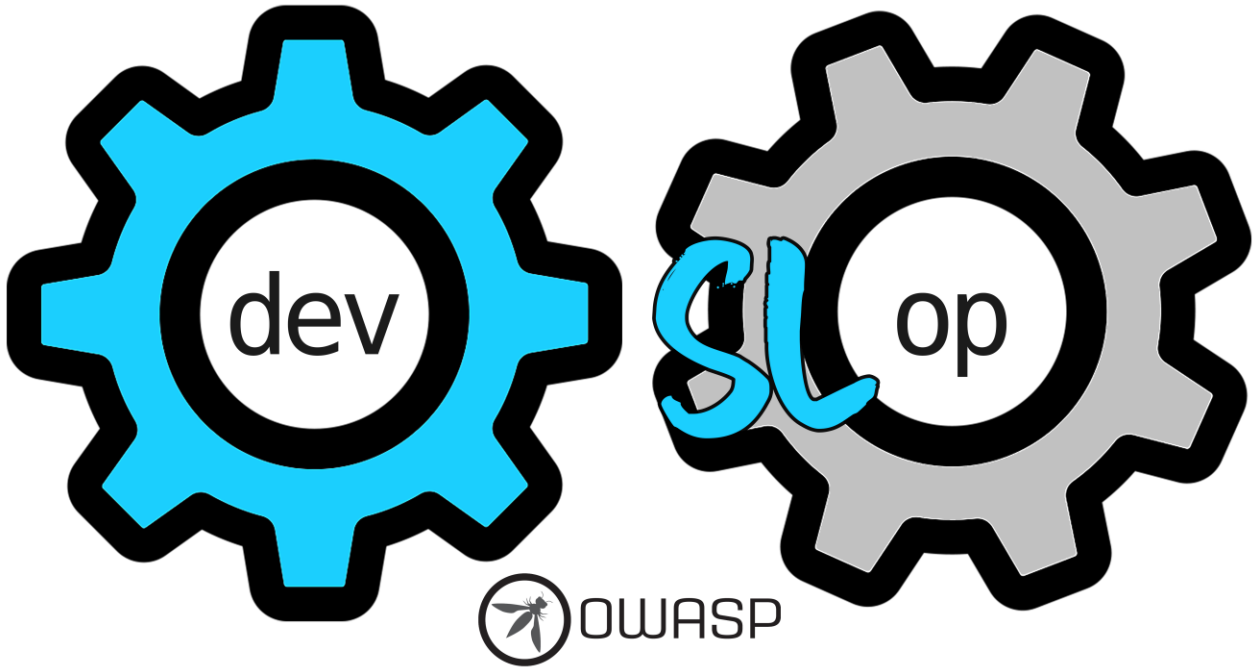
Tanya Janca

Resources

Security is everybody's job.

Tanya Janca

OWASP DevSlop Has Your Back

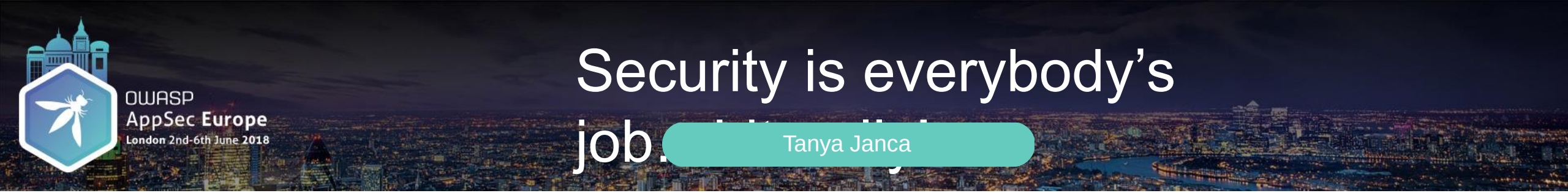


DevSlop.co

https://www.owasp.org/index.php/OWASP_DevSlop_Project

Resources


Links for Getting Started in Application Security
https://aka.ms/GettingStartedWithAppSec



Security Learns To Sprint

Learn Security's View of DevSecOps in the Companion Talk

@SheHacksPurple

Resources


Follow me?
Twitter: @SheHacksPurple
https://medium.com/@shehackspurple
https://DevSlop.co

Security is everybody's job.

Tanya Janca

Resources

Thank You

http://aka.ms/AppSecEU

Tanya.Janca@Microsoft.com

Tanya.Janca@owasp.org

@SheHacksPurple