MY CI/CD PIPELINE CONTAINS ALL SECURITY TOOLS AVAILABLE! NOW WHAT...?

Just adding more tools won‘t make your products more secure

JASMIN MAIR

Global Product Security Manager @

Leica Microsystems

Connect with me:

jasmin.mair@owasp.org

linkedin.com/in/jasminmair

AGENDA

What is wrong with my tools?

Where is the problem?

Let’s figure a way out…

Credits: Ilya Pavlov on Unsplash

DANGER ZONE!

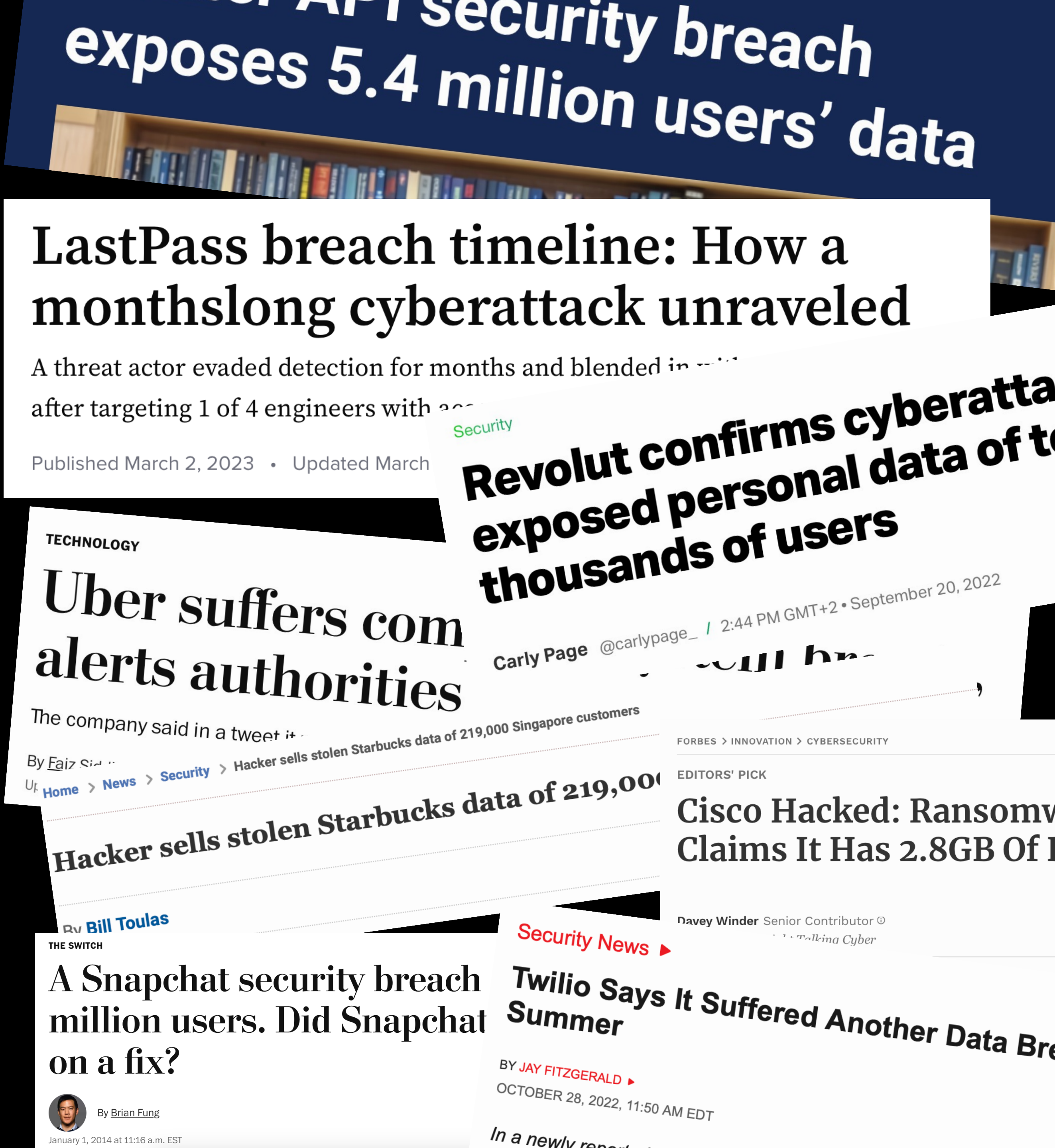
74% of all breaches include the human element[1]

26% of incidents were caused by exploiting public facing applications[2]

13% of attack vectors were vulnerabilities in third-party software[2]

[1] Verizon 2023 Data Breach Investigation Report

[2] 2023 IBM X-Force Threat Intelligence Report



API security breach exposes 5.4 million users' data

LastPass breach timeline: How a monthslong cyberattack unraveled

A threat actor evaded detection for months and blended in

after targeting 1 of 4 engineers with

Published March 2, 2023 • Updated March

Security

Revolut confirms cyberatta exposed personal data of t thousands of users

Carly Page @carlypage_ / 2:44 PM GMT+2 • September 20, 2022

TECHNOLOGY

Uber suffers com alerts authorities

The company said in a tweet

By Faiz Si

Home > News > Security > Hacker sells stolen Starbucks data of 219,000 Singapore customers

Hacker sells stolen Starbucks data of 219,00

By Bill Toulas

FORBES > INNOVATION > CYBERSECURITY

EDITORS' PICK

Cisco Hacked: Ransomw Claims It Has 2.8GB Of I

Davey Winder Senior Contributor

Talking Cyber

THE SWITCH

A Snapchat security breach million users. Did Snapchat on a fix?

By Brian Fung

January 1, 2014 at 11:16 a.m. EST

Security News

Twilio Says It Suffered Another Data Bre Summer

BY JAY FITZGERALD

OCTOBER 28, 2022, 11:50 AM EDT

In a newly rep

LET‘S BUY SOME MORE TOOLS

Plan

- Resource planning
- Requirements gathering
- Functional & non-functional requirements
- Security issues

Design

- Architecture design and review
- Technology and framework decisions

Implement

- Coding standards
- Unit tests & end-to-end tests
- Branching strategy and pull requests

Build & Deploy

- Build application
- Run unit tests & end-to-end tests
- Configuration management
- Artifact management
- Provision environment

Test

- Integration tests
- Functional tests
- Non-functional tests

Operate & Monitor

- Bug fixing
- Continuous feedback cycles
- System monitoring

IriusRisk snyk VERACODE BLACKDUCK clair OWASP Zed Attack Proxy aqua StackRox DATADOG

SECURE CODE WARRIOR trivy WhiteSource HashiCorp Vault sonarqube DEPENDENCY-CHECK SYNOPSYS® Checkmarx intruder sysdig SECURE tenable

...THE MORE THE MERRIER

Plan

- Resource planning
- Requirements gathering
- Functional & non-functional requirements
- Security issues

Design

- Architecture design and review
- Technology and framework decisions

Implement

- Coding standards
- Unit tests & end-to-end tests
- Branching strategy and pull requests

Build & Deploy

- Build application
- Run unit tests & end-to-end tests
- Configuration management
- Artifact management
- Provision environment

Test

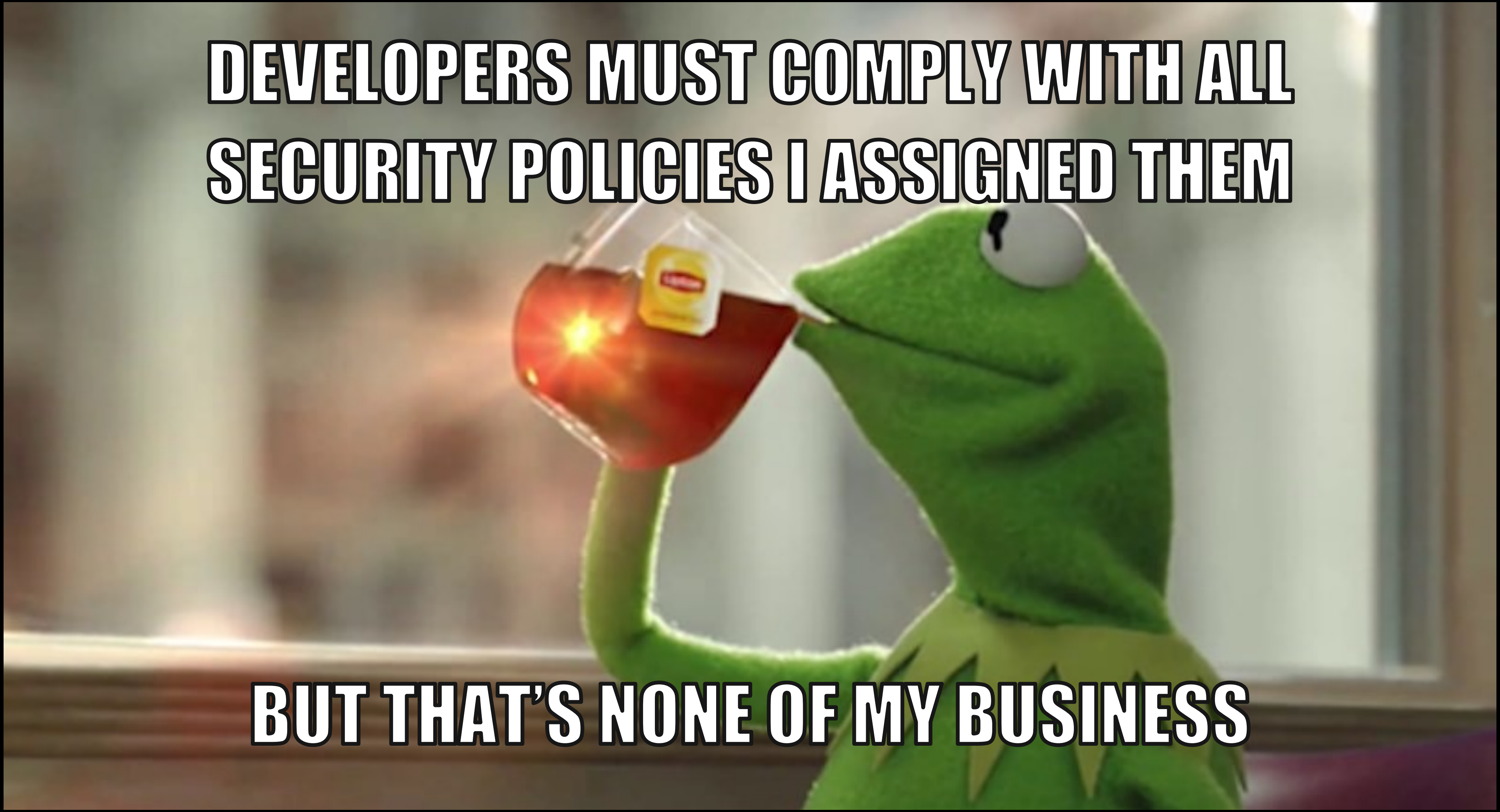
- Integration tests
- Functional tests
- Non-functional tests

Operate & Monitor

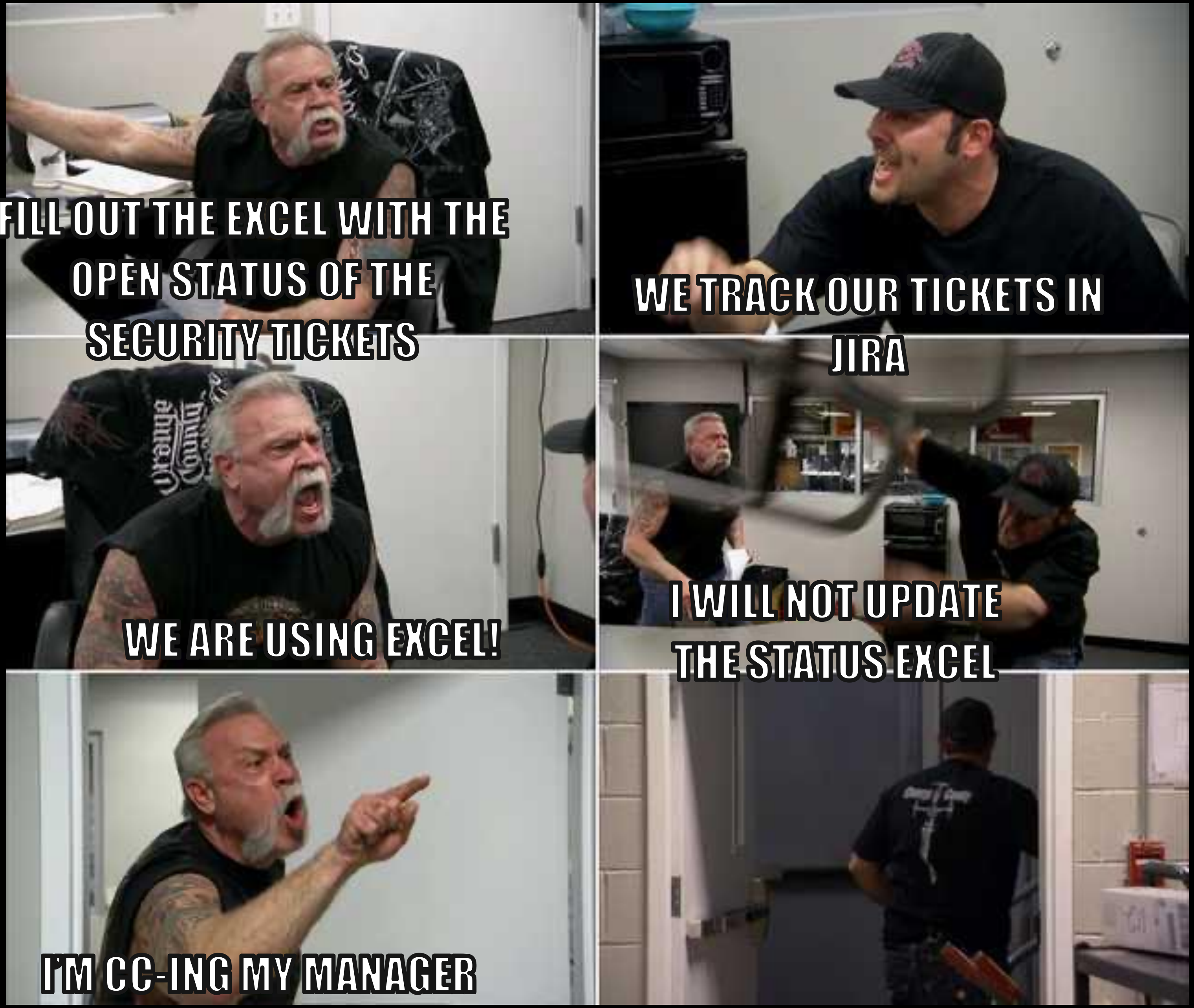
- Bug fixing
- Continuous feedback cycles
- System monitoring

SECURITY
DEVELOPMENT

I SEE CYBER RISKS
EVERYWHERE



DEVELOPERS MUST COMPLY WITH ALL SECURITY POLICIES I ASSIGNED THEM
BUT THAT’S NONE OF MY BUSINESS


FILL OUT THE EXCEL WITH THE OPEN STATUS OF THE SECURITY TICKETS
WE TRACK OUR TICKETS IN JIRA
WE ARE USING EXCEL!
I WILL NOT UPDATE THE STATUS EXCEL
I'M CC-ING MY MANAGER

YOU CANNOT BUY DEVSECOPS

COLLABORATION CULTURE

- Security experts embedded in development team
- Clarification of success metrics
- Align on security priorities

AWARENESS & TRAINING

- Foster a security mindset among stakeholders
- Establish security champion program
- Train developers on security

SECURE THE SDLC

- Take security into consideration in each step of the SDLC
- Act on priorities and define security activities

WHERE TO GET STARTED

Plan

- Resource planning
- Requirements gathering
- Functional & non-functional requirements
- Security issues
- **Application profiling**

Design

- Architecture design and review
- Technology and framework decisions
- **Threat modeling**

Implement

- Coding standards
- Unit tests & end-to-end tests
- Branching strategy and pull requests
- **Secrets management**
- Security libraries

Build & Deploy

- Build app
- Run unit tests & end-to-end tests
- Conf.mgmt
- Artifact mgmt
- Provision env
- **Software composition analysis**
- **Static application security testing**

Test

- Integration tests
- Functional tests
- Non-functional tests
- Dynamic application security testing
- Penetration testing

Operate & Monitor

- Bug fixing
- Continuous feedback cycles
- System monitoring
- Runtime protection

ADDING ONE TOOL AT A TIME

TRAIN DEVELOPERS

- Clarify scope and goal of the tool
- Enable developers to manage findings
- Align on security priorities

SET BASELINE

- Scan existing code base
- Finetune scans
- Create meaningful quality gates
- Continuously improve

MANAGE FINDINGS

- Integrate tools with existing ticketing system
- Prioritize findings
- Visualize necessary work

SECURE PRODUCTS
DEVELOPMENT
SECURITY

THANK YOU

Jasmin Mair jasmin.mair@owasp.org