

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

Just adding more tools won't
make your products more
secure



OWASP FRANKFURT #62

JASMIN MAIR

Global Product Security Manager @
Leica Microsystems

Connect with me:

jasmin.mair@owasp.org

[linkedin.com/in/jasminmair](https://www.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 element¹

26% of incidents were caused by exploiting public facing applications²

13% of attack vectors were vulnerabilities in third-party software²

¹ Verizon 2023 Data Breach Investigation Report

² 2023 IBM X-Force Threat Intelligence Report

AI 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 with employees after targeting 1 of 4 engineers with access to the company's security database.

Published March 2, 2023 • Updated March 2, 2023

Revolut confirms cyberattack exposed personal data of thousands of users

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

Uber suffers compliance alerts authorities

The company said in a tweet it is investigating a data breach that exposed the personal information of 219,000 Singapore customers.

By Faiz Siddiqui

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

Hacker sells stolen Starbucks data of 219,000

By Bill Toulas

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 Breach

BY JAY FITZGERALD ▶

OCTOBER 28, 2022, 11:50 AM EDT

In a newly reported...

FORBES > INNOVATION > CYBERSECURITY

EDITORS' PICK

Cisco Hacked: Ransomware Claims It Has 2.8GB Of Data

Navey Winder Senior Contributor @naveywinder

Talking Cyber

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



...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



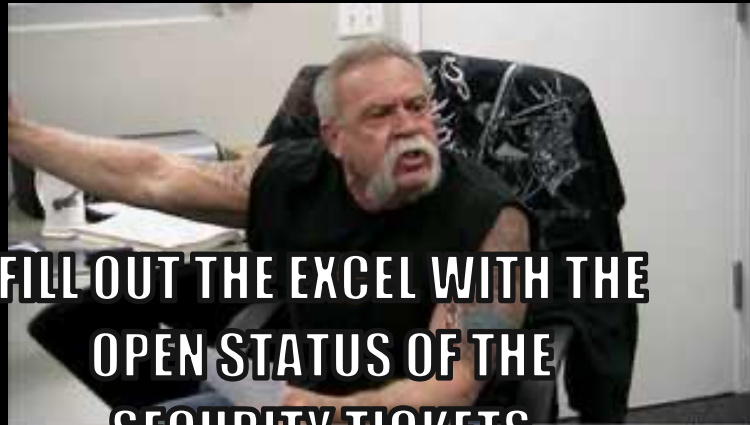




**DEVELOPERS MUST COMPLY WITH ALL
SECURITY POLICIES I ASSIGNED THEM**



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

A painting of two muscular men wrestling. The man on the left is wearing a white shirt and has his arm around the neck of the man on the right. The man on the right is wearing a red shirt and is being held. The background is a dark, textured grey. The text 'SECURE PRODUCTS' is overlaid in the upper center, 'DEVELOPMENT' is overlaid on the right side, and 'SECURITY' is overlaid on the left side.

**SECURE
PRODUCTS**

DEVELOPMENT

SECURITY



THANK YOU

Jasmin Mair

jasmin.mair@owasp.org