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...
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
## 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
### 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

**OWASP FRANKFURT #62**
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 are using Excel!

We track our tickets in JIRA.

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

<table>
<thead>
<tr>
<th>Plan</th>
<th>Design</th>
<th>Implement</th>
<th>Build &amp; Deploy</th>
<th>Test</th>
<th>Operate &amp; Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource planning</td>
<td>Architecture design and review</td>
<td>Coding standards</td>
<td>Build app</td>
<td>Integration tests</td>
<td>Bug fixing</td>
</tr>
<tr>
<td>Requirements gathering</td>
<td>Technology and framework decisions</td>
<td>Unit tests &amp; end-to-end tests</td>
<td>Run unit tests &amp; end-to-end tests</td>
<td>Functional tests</td>
<td>Continuous feedback cycles</td>
</tr>
<tr>
<td>Functional &amp; non-functional requirements</td>
<td>Threat modeling</td>
<td>Branching strategy and pull requests</td>
<td>Conf.mgmt</td>
<td>Non-functional tests</td>
<td>System monitoring</td>
</tr>
<tr>
<td>Security issues</td>
<td></td>
<td>Secrets management</td>
<td>Artifact mgmt</td>
<td>Dynamic application</td>
<td>Runtime monitoring</td>
</tr>
<tr>
<td>Application profiling</td>
<td></td>
<td>Security libraries</td>
<td>Provision env</td>
<td>security testing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Software composition analysis</td>
<td>Penetration testing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>application security testing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**OWASP FRANKFURT #62**
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
THANK YOU

Jasmin Mair
jasmin.mair@owasp.org