OWASP
The Open Web Application Security Project

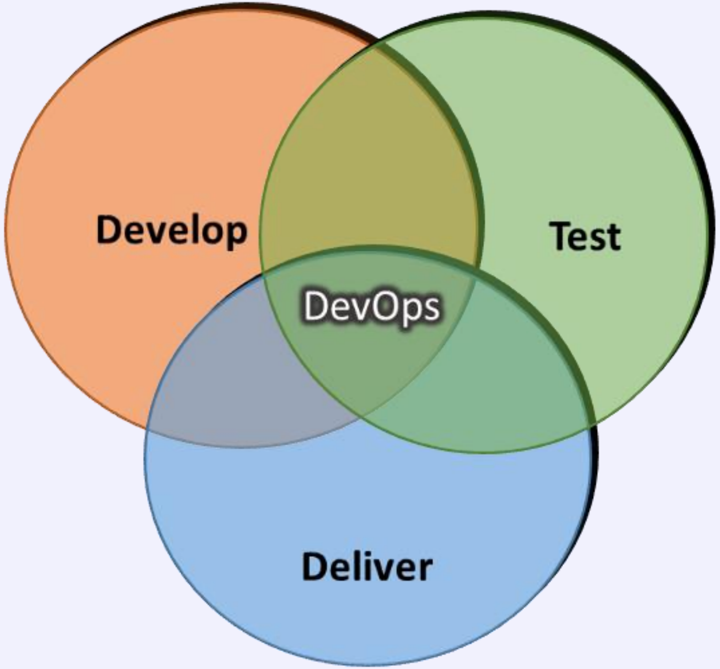
Putting the Sec in DevOps

Helen Bravo
Checkmarx

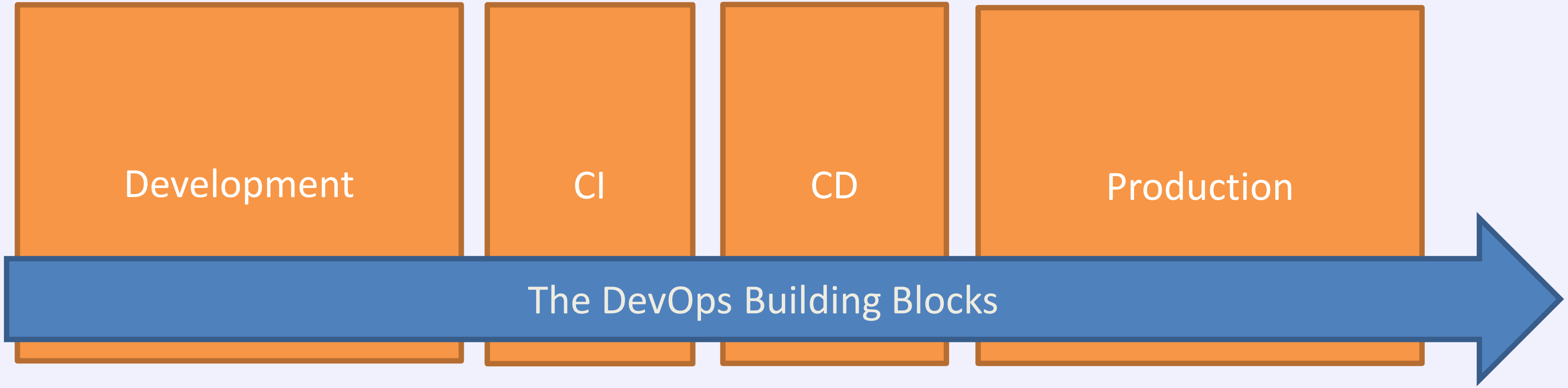
What is DevOps About?

DevOps is about

- Processes
- Connections
- Automation
- … and Tools



DevOps building blocks



Development

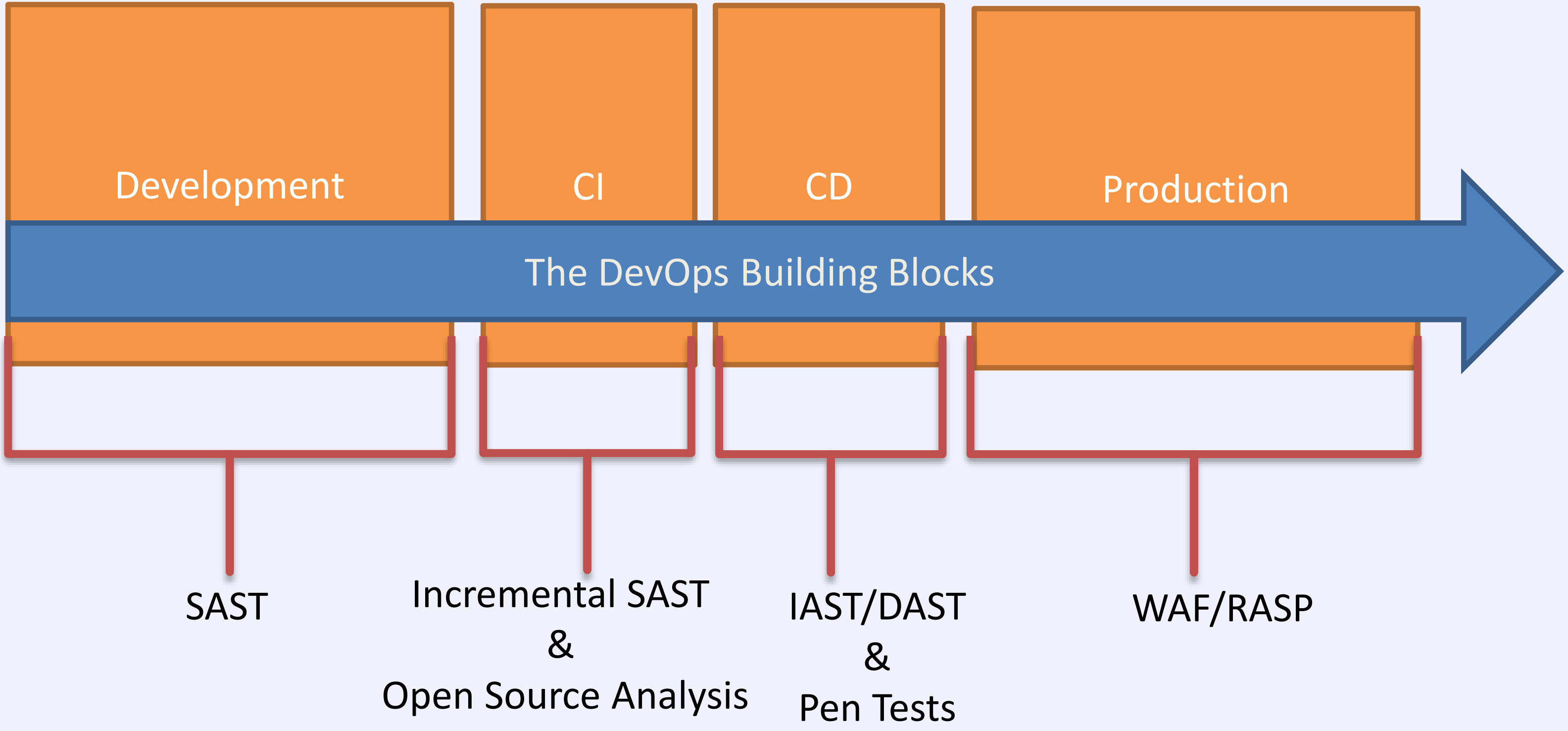
CI

CD

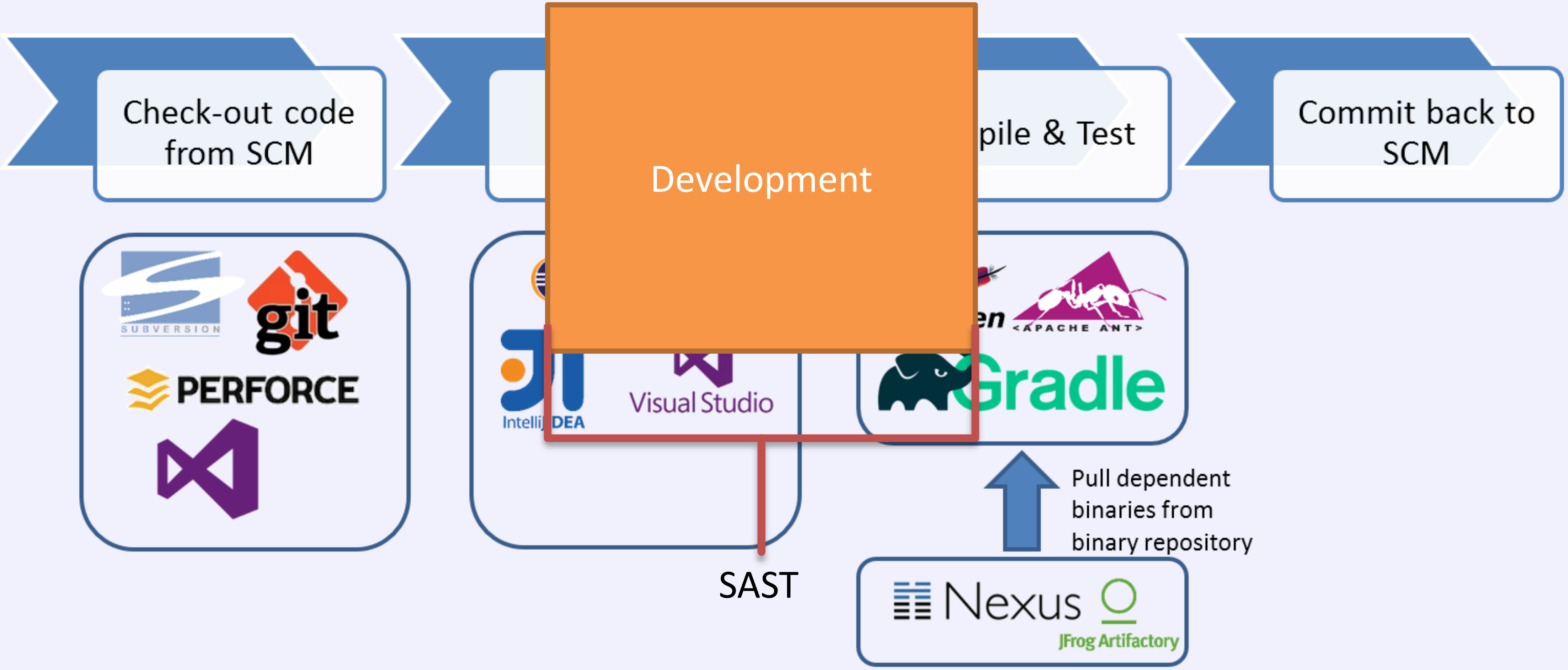
Production

The DevOps Building Blocks

What security fits where?

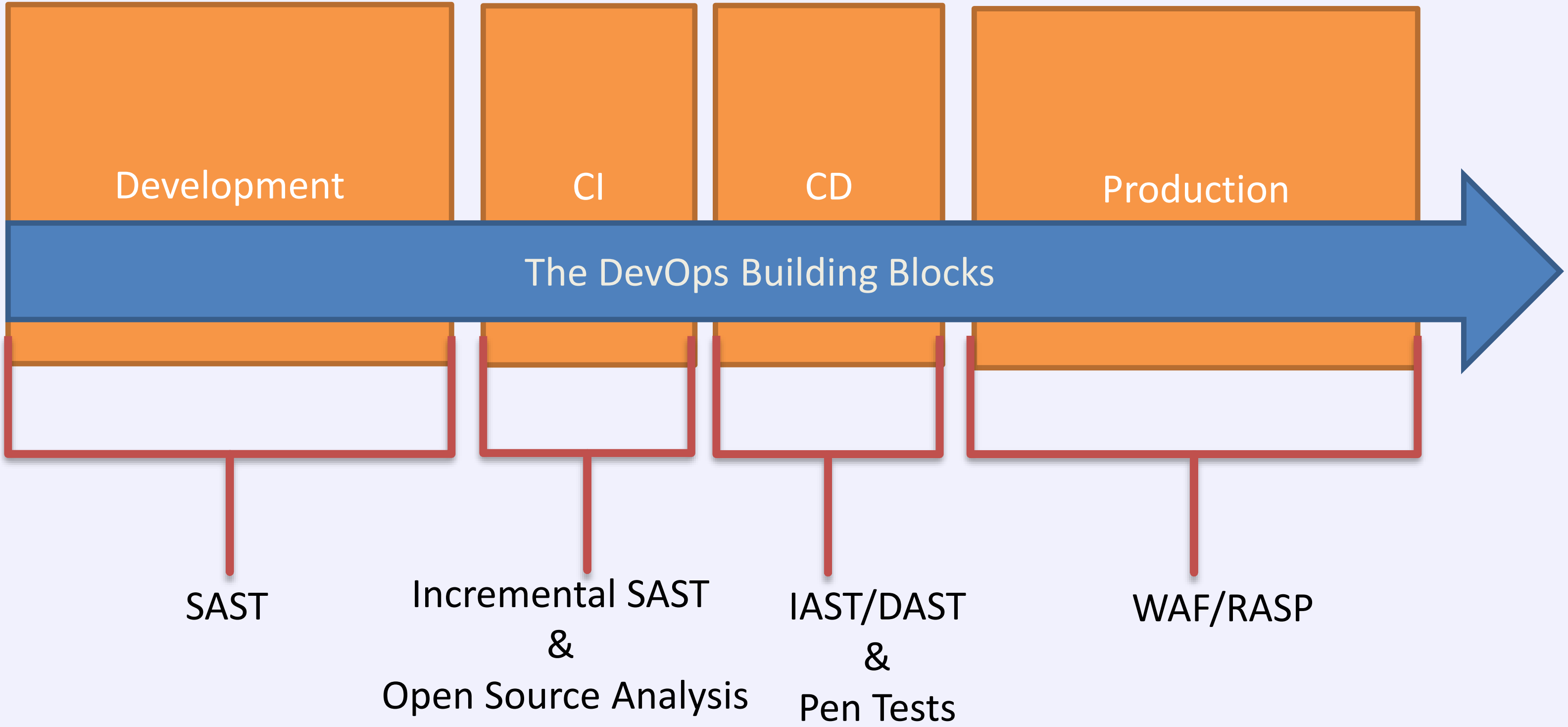


The Developer's Process



What security fits where?

OWASP
The Open Web Application Security Project



What CI is about?

CI is the process of integrating code into a mainline code base.

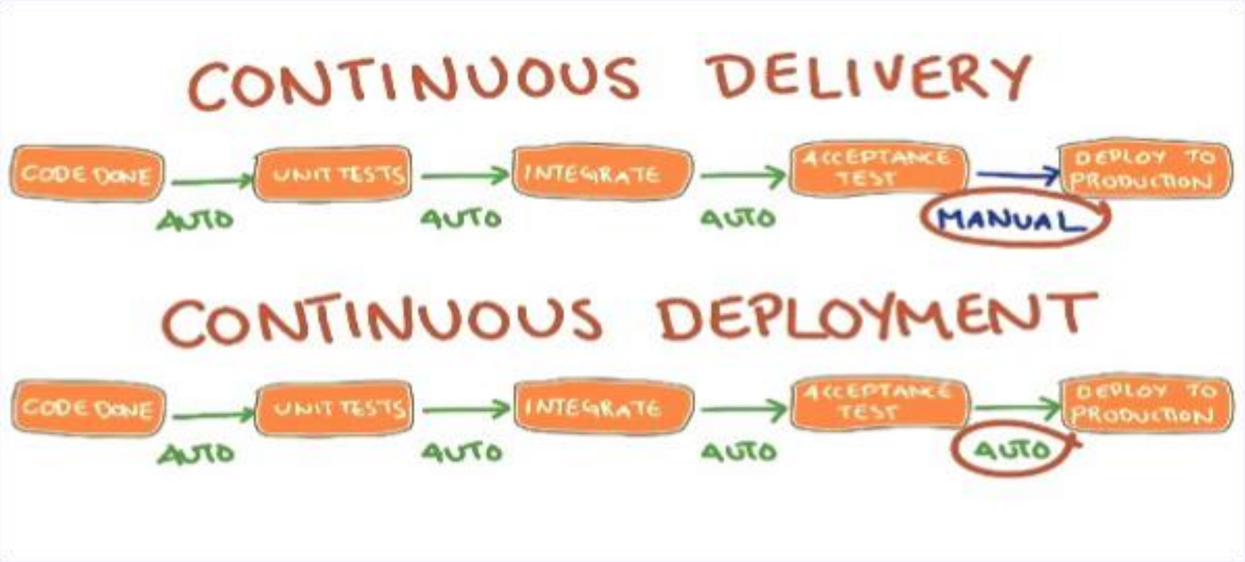
Implementing CI is, therefore, as simple as using the right tools.

What CD is about?

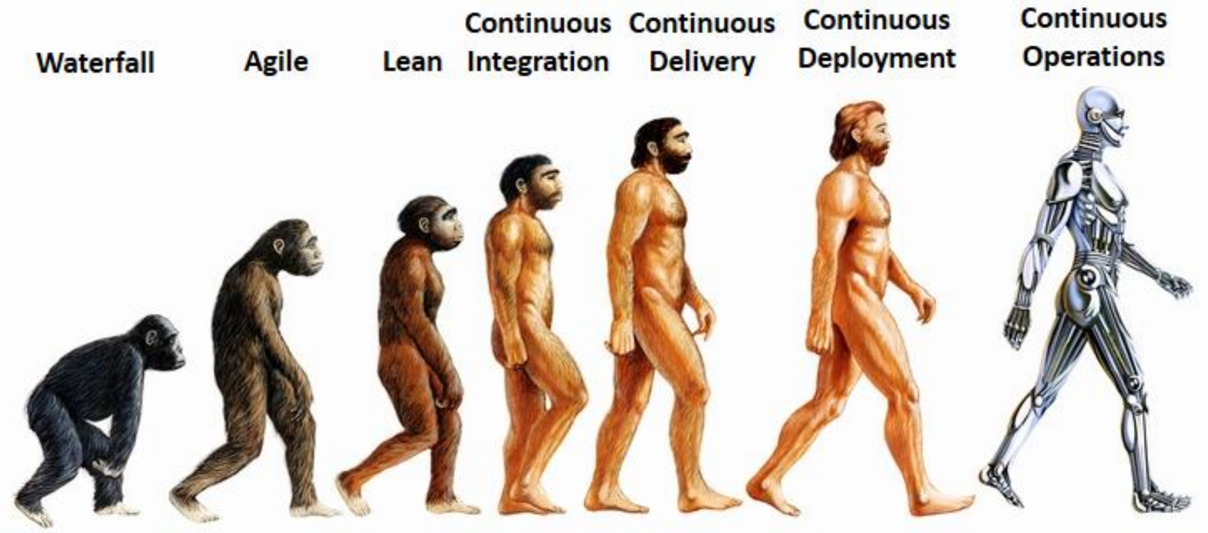
CD is a software development practice in which every code change goes through the entire pipeline toward the end user.

- To achieve CD, you have to organize your software testing, staging and deployment processes in a way that **automates** them as much as possible and makes them **continuous**.
- These processes take different forms, depending on the culture of the team and the type of app it is creating.

Continuous Delivery vs. Continuous Deployment



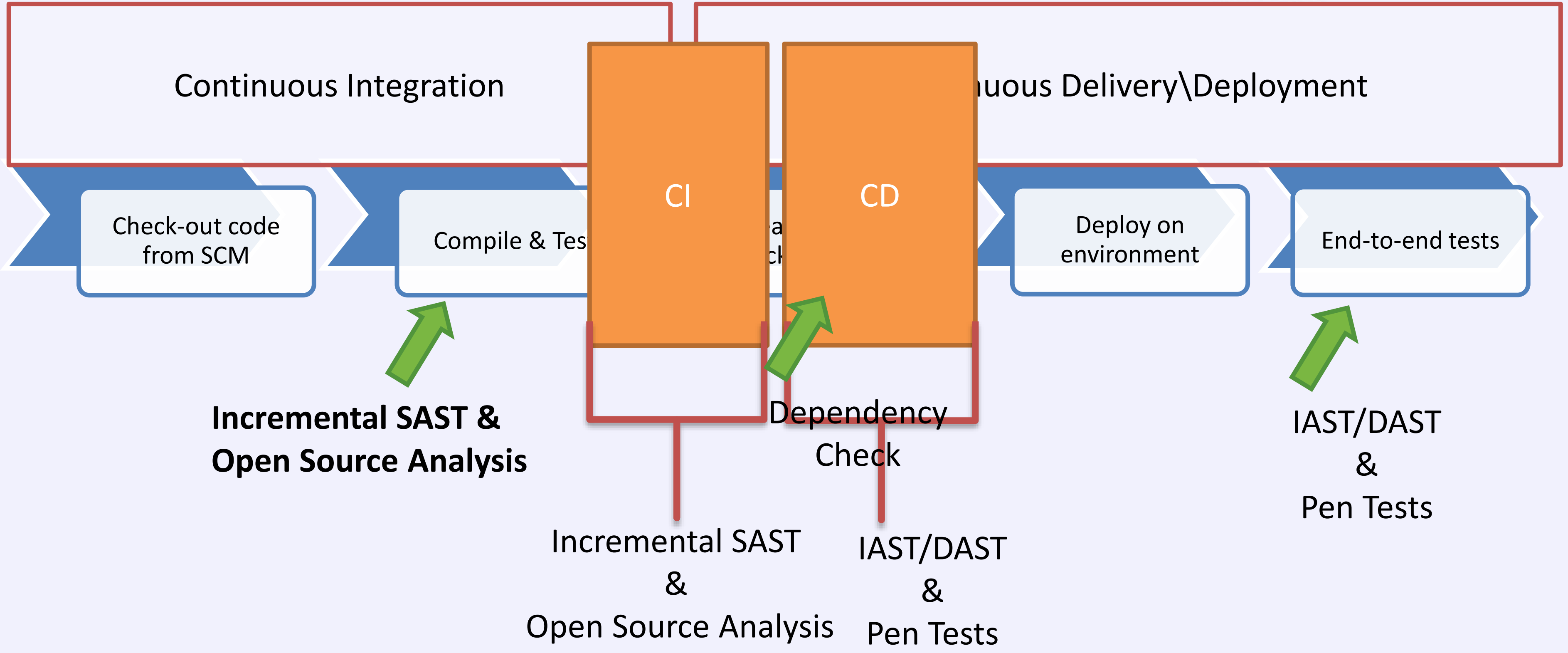
DevOps Movement



Shift Left

The further right the project is on the DevOps scale the further left it should start implementing security checks

Full Build/ Nightly Build



Incremental SAST & Open Source Analysis

Dependency Check

Incremental SAST
&
Open Source Analysis

IAST/DAST
&
Pen Tests

IAST/DAST
&
Pen Tests

Build Break is a sensitive issue

490 × 409 - quickmeme.com

tps://www.google.co.il/imgres?imgurl=http%3A%2F%2Fs.quickmeme.com...

Don’t let security be the build breaker

- When CI breaks (and it breaks) it impacts everyone and everything in the process. Creating a significant delay in the release cycle.
- In order to avoid build breaks you should start implementing security before the CI stage.

If you have 365 developers and each developer breaks only a single build once a year (usually much more), you have an average of one build break per day.

- DevOps would work best if there were no developers

- As security professionals we need to ensure DevOps can maintain a constant flow of deliveries. Blocking these flows is unacceptable.

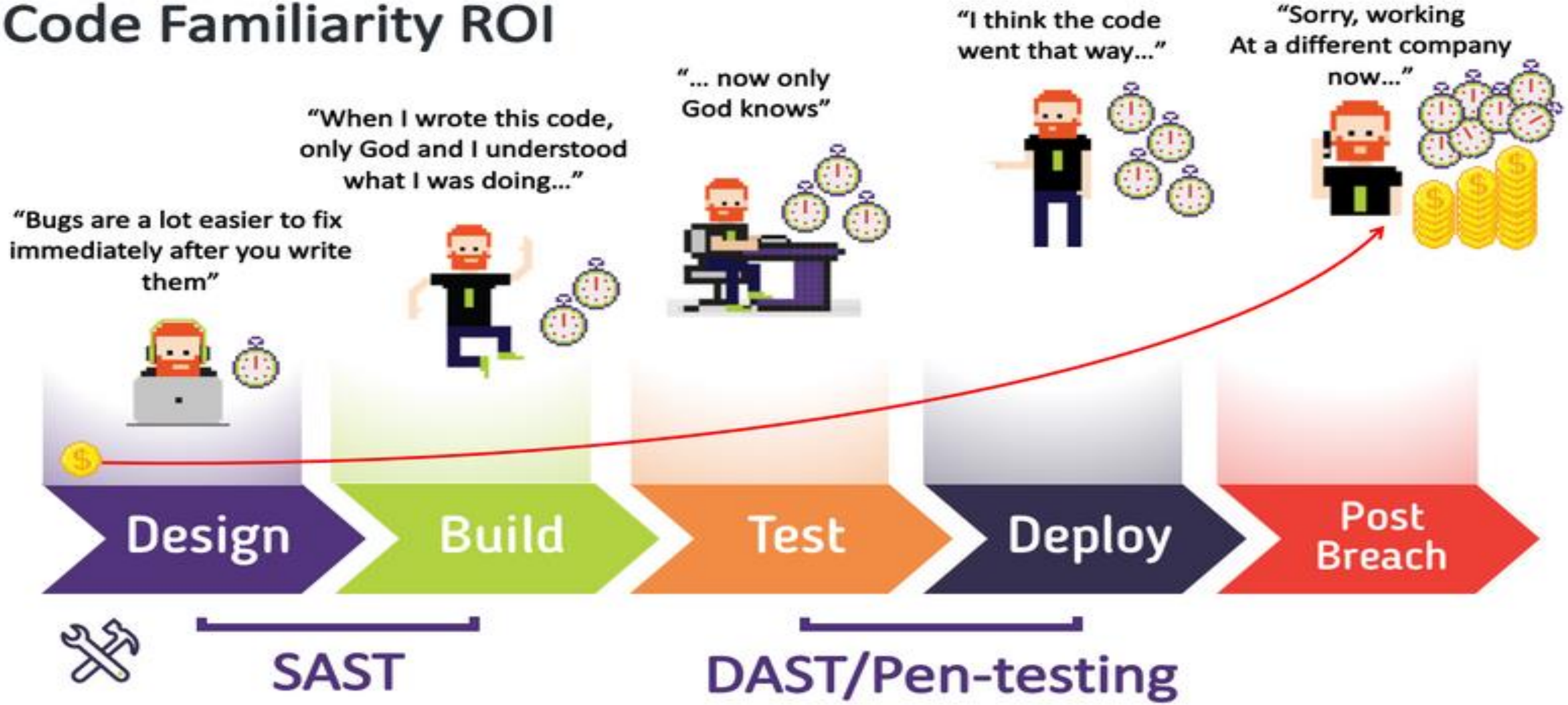
- Where does security clash with the DevOps key requirements
  - Speed
    - Full code scans too long
    - Special requirements to initiate scans are time consuming
  - Stability
    - Build breaks have to be justifiable therefore accuracy is key.

Security Policy

OWASP
The Open Web Application Security Project

- Policy for
  - Legacy code security findings
  - New code security findings
- Evolving policy
- Segregated policy based on vulnerability type or age
- Open Source vulnerabilities policy

Code Familiarity ROI



"Bugs are a lot easier to fix immediately after you write them"

"When I wrote this code, only God and I understood what I was doing…"

"… now only God knows"

"I think the code went that way…"

"Sorry, working At a different company now…"

Design

Build

Test

Deploy

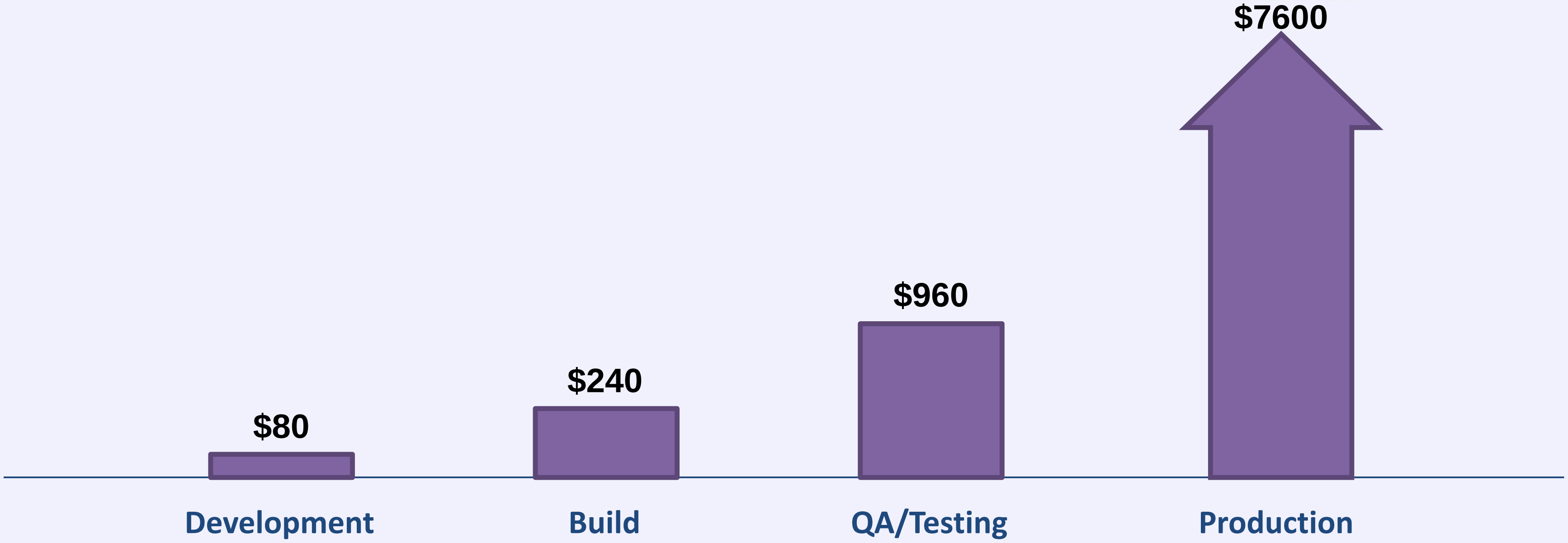
Post Breach

SAST

DAST/Pen-testing

EARLIER SCANNING. LESS COSTS. MORE SECURE

OWASP
The Open Web Application Security Project

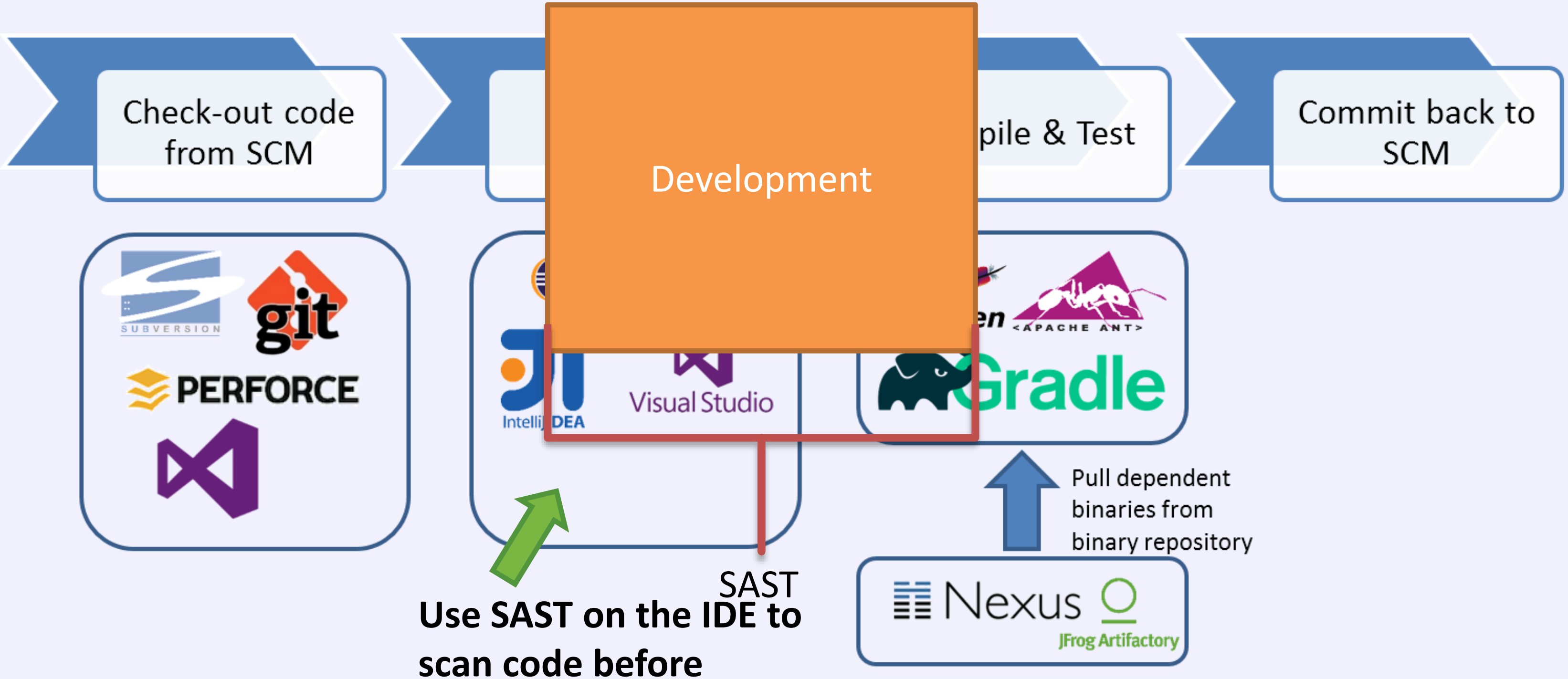


COST OF A SECURITY BUG AT EACH DEVELOPMENT STAGE

Source: Ponemon Institute: National Institute of Standards and Technology

The Developer's Process

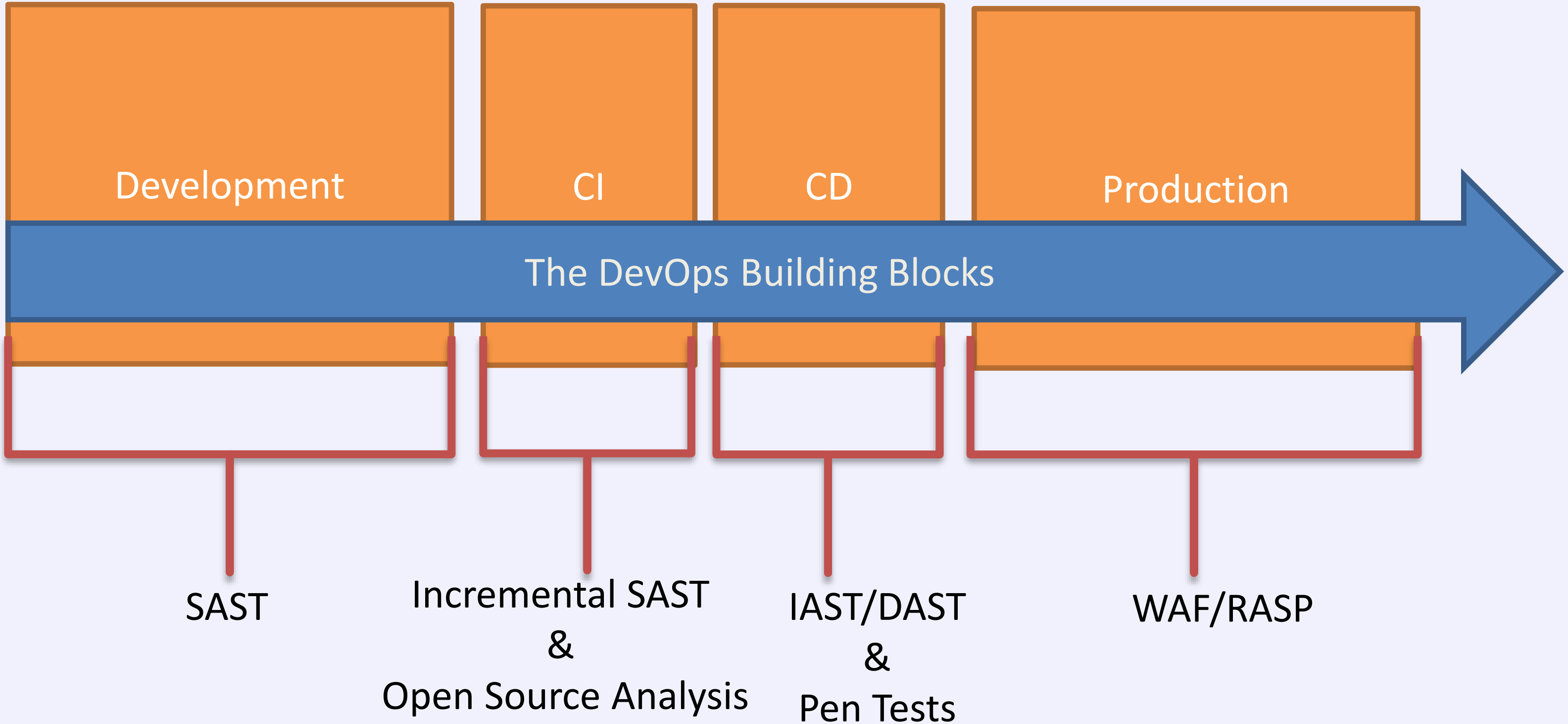
OWASP
The Open Web Application Security Project



Use SAST on the IDE to scan code before commit

What security fits where?

OWASP
The Open Web Application Security Project



SUMMARY

- Develop security policy that fits the DevOps flow
- Shift Security Left
- Mind Open Source

Thank You