Integrating Security and Compliance into CI/CD Pipeline

Fauzi Ramadhan

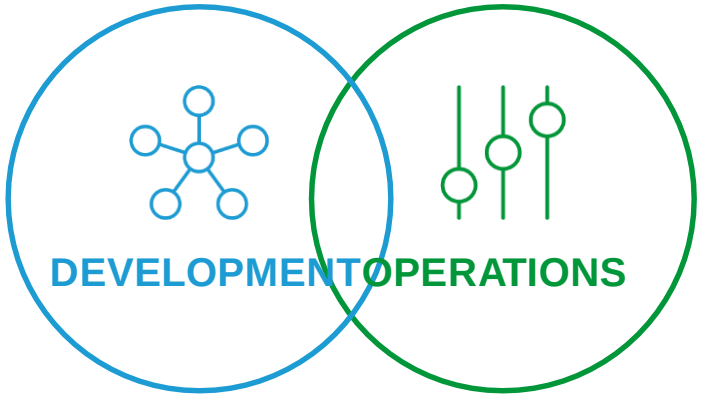
DevOps Community in Indonesia

Jakarta, 18 Desember 2019


NGINX
Part of F5
Integrating Security and Compliance into CI/CD Pipeline
JAKARTA • DECEMBER 18

Agenda

- Intro
- DevOps & Automation
- Waterfall vs DevOps
- DevSecOps Principle
- Security in the Pipeline Stage
- Advanced Web Application Firewall Instrumentation for CI/CD Pipeline
- F5 Advanced Web Application Firewall & Automation
- Demo


DEVELOPMENT
OPERATIONS

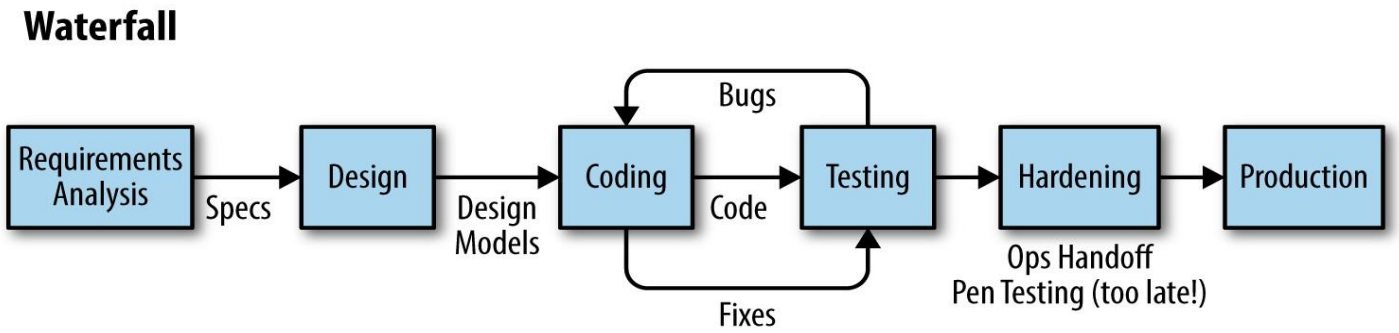
DevOps and Automation

- Automation is the ultimate need for DevOps practice and **'Automate everything'** is the key principle of DevOps.
- **Automation** speeds up and simplifies provisioning and configuring systems, especially at scale way

Security Should Be No Different

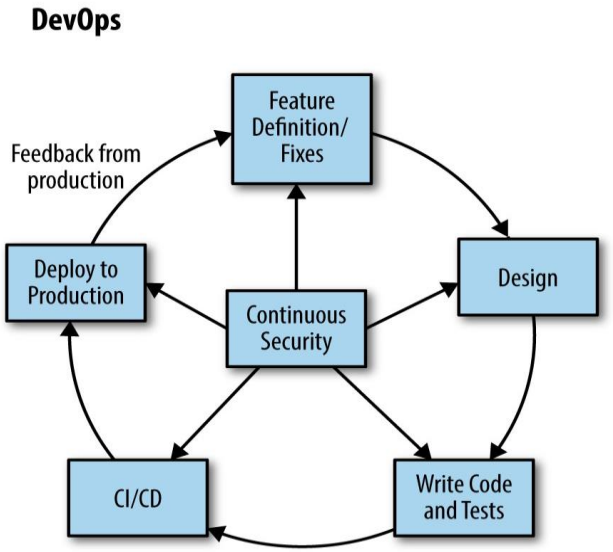
- DevOps adoption is increasing, but **Security** and **Compliance** typically remain afterthoughts.
- Time is the essence in a continuous environment and manual process of security can means preventing business

Waterfall Approach



- Waiting until the system is designed and built
- Then trying to fit some security checks just before release

DevOps Approach



“Shift Security Left”

Security ToolChain must be :

- Automated
- Efficient
- Repeatable
- Easy to Use

OWASP Proactive Controls

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

DevSecOps Principles

Breaking Down the Silos

Shifting Left

Nurturing Security Champions

Continuous Testing/ Test Automation

Making the Secure Path the Easy Path

Security in the Pipeline Stages

DEVELOP

INHERIT& BUILD

DEPLOY

OPERATION

DevSecOps Pipeline : Development

DEVELOP

- Threat Modeling
- Development Standard
- Static Code Analysis

Threat Modeling

- OWASP App Threat Modeling Cheat Sheet
- OWASP App Sec Verification Standard
- Mozilla Rapid Risk Assessment

Development Standard

- Secure coding practice
- Git-secret
- Git-hound

Static Code Analysis

Commercial option

VERACODE

RIPSTECH

kiuwan

raxis information security

Open Source option

CODE WARRIOR

Language/Framework	Tool
Ruby	Brakeman
Java Web Apps	Find Security Bugs
PHP	Phan
Node	NodeJsScan
Golang/Go	GoSec

DevSecOps Pipeline : Inherit & Build

INHERIT & BUILD

- Software Composition Analysis (SCA)
- Dependency Check
- Unit Test

Software Composition Analysis

OWASP Dependency-Check

Sonatype Nexus

VERACODE

BLACKDUCK

WhiteSource

Container Security

Open Source option

clair

Commercial option

aqua

Twistlock

DevSecOps Pipeline : Deploy

DEPLOY

- Performance & Load Testing
- Dynamic Analysis Security Testing (DAST) & Interactive Application Security Testing (IAST)
- Compliance Check
- WAF Shielding

Web Application Firewall

DAST & IAST

Open Source DAST Option

arachni
web application security scanner framework

Nikto

OWASP Zed Attack Proxy

BURPSUITE

sqlmap

Commercial DAST Option

WhiteHat SECURITY

FORTIFY

acunetix

Automation Integration

GAUNTLT

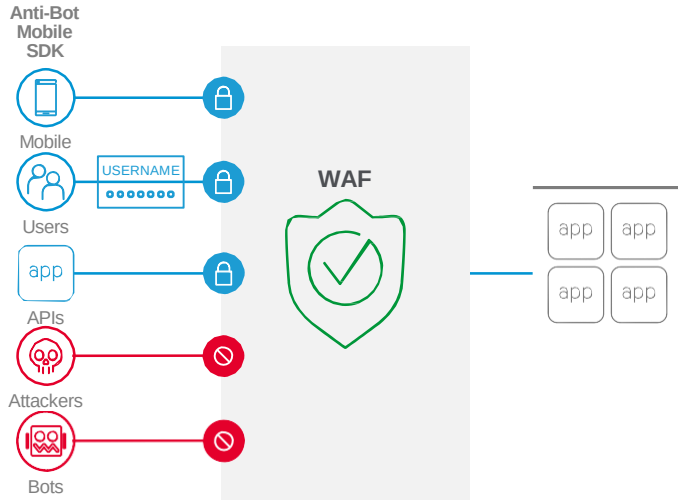
Open Source tool for Compliance Check

CHEF INSPEC™

DevSecOps Pipeline : Operation

OPERATION

- Web Application Firewall WAF Shielding
- Security Orchestration



Common Business Perception

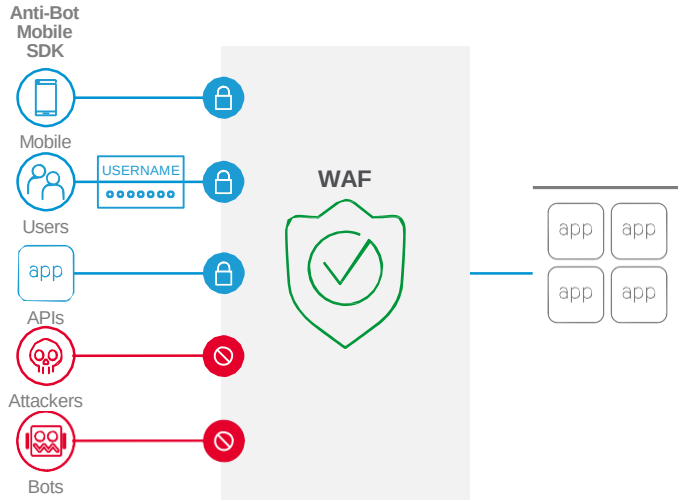
Security is preventing business, breaking the app

IT Security
(Traditional)

- Something got blocked – inconsistency between development and production
- Delays in resolution awaiting SecOps response – no rollback

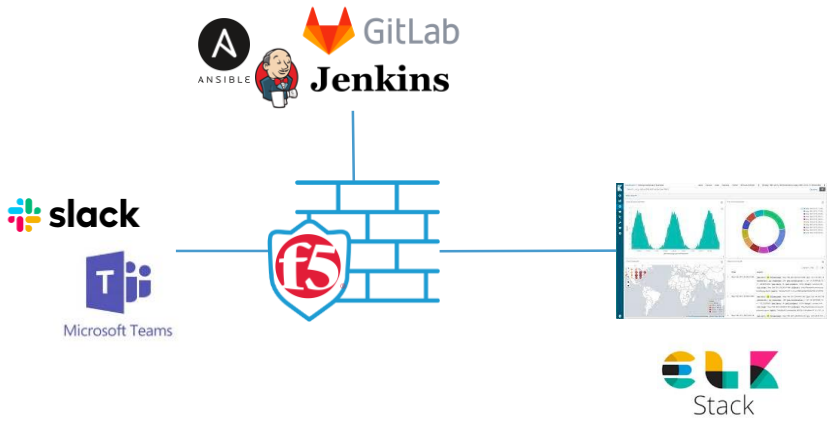
Advanced Web Application Firewall Instrumentation

- Provides Automation
- Visibility (Metric Based): Attack Events, Attack Logs
- Provides API
- Promotes Learning
- Advanced Application Attacks (Bot/Scraper, DoS)



F5 Advanced Web Application Firewall and Automation

Inserting Automation of WAF in CI/CD Pipeline



- Faster and easier to deploy WAF with frictionless security controls & Automation
- Speed app WAF Policy deployment consistently and repeatability in declarative manner
- Integration with CI/CD ToolChains (ChatOps, SCM, Automation & Orchestration Tools, ELK)

Summary

Breaking Down the Silos

Shifting Left

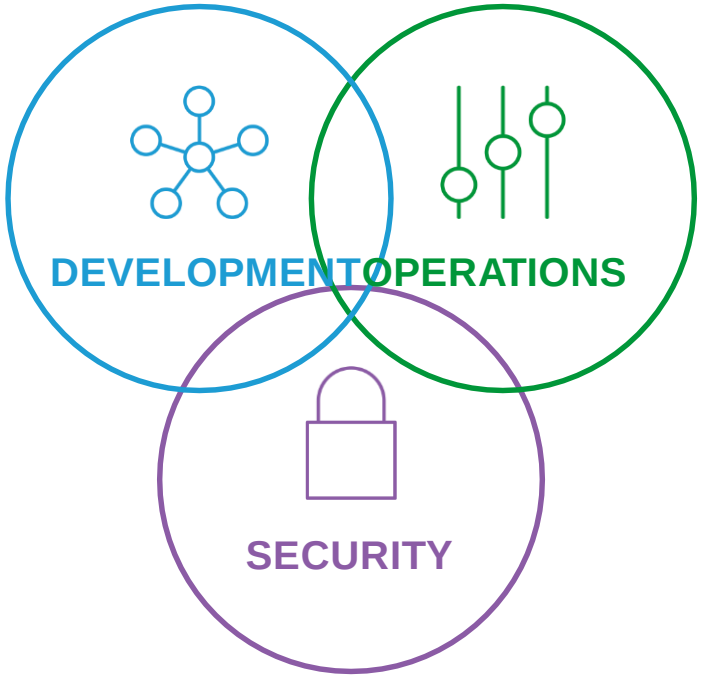
Nurturing Security Champions

Continuous Testing/ Test Automation

Making the Secure Path the Easy Path

Building Collaboration

Increasing Collaboration and Feedback Between SecOps and DevOps



Stay Connected

@IDDevOps

http://www.devopsindonesia.com

@IDDevOps

DevOps Indonesia

@devopsindonesia

Alone We are smart, together We are brilliant

DEVOPS INDONESIA

THANK YOU !

Quote by Steve Anderson