Is there room for SecArch in DevSecOps?
(or can old dogs perform new tricks?)

Dimitrios Petropoulos

26 April 2018

$ cut -f5 -d: /etc/passwd | grep -i petropoulos

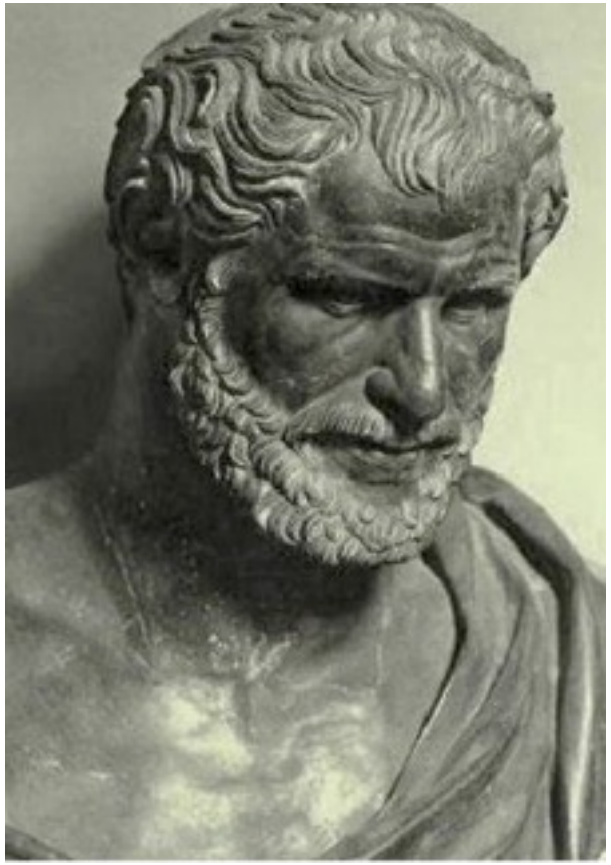
- Dimitrios Petropoulos
- Cryptographer by education (nobody's perfect)
- Security Architect (& past security developer) by trade
- Have been breaking & mending things for over a third of a century

this.Presentation

- …contains questions – not answers…
- Majority of points in this presentation are
  - Personal conclusions after having worked with numerous organisations and tried to extract common patterns of behaviour and trends
  - conjectures (in the mathematical sense of the word, i.e. unproven propositions which appear correct)
  - Based on relatively recent mindset
- Might be controversial…
- Don’t expect you to agree with me

<Rant>

Constant change & unity of opposites



“Τα πάντα ρεί” *

(everything flows)

“Πόλεμος πατήρ πάντων”

(war/struggle is the father of all)

Heraclitus

(c.535 – c.475 BC)

* - and Francesco Gabbani in Occidentali’s Karma

The brave new world

The opportunity:

- Cloud
- *aaS
- Automation
- AI
- Big Data
- …

The requirements (& benefits):

- Agility (↑)
- Speed (↑)
- Scalability (↑)
- Cost (↓)

The challenge is: *'security'*

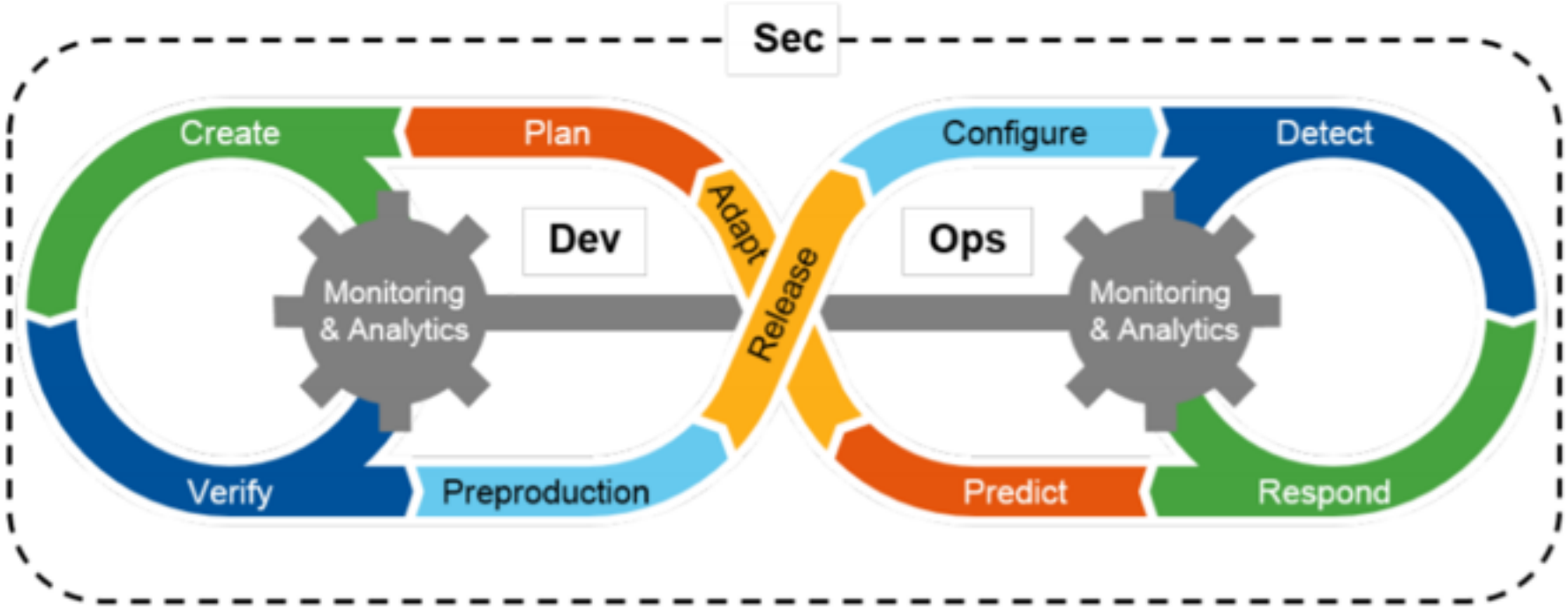
Source: https://www.sumologic.com

The birth of DevSecOps

- In times where speed and agility are the name of the game, security:
  - cannot slow down business…
  - …but cannot be overlooked

- The answer (allegedly) comes from *automation*

It all started here…

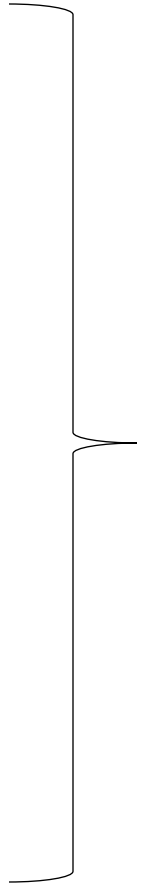


Source: Gartner (September 2016)

What does this ‘Sec’ mean?

The ‘Sec’ in ‘DevSecOps’

- Application Security Testing
  - SAST
  - DAST
  - IAST
- Infrastructure/Platform Vulnerability Scanning
- Platform configuration & compliance
- Deployment of controls
  - Firewalling, micro-segmentation
  - WAFs, DBSGs, etc.
  - RASP
- Identity & Access Management
- …



Automated & programmatically provisioned

Where does ‘SecArch’ fit in all this?

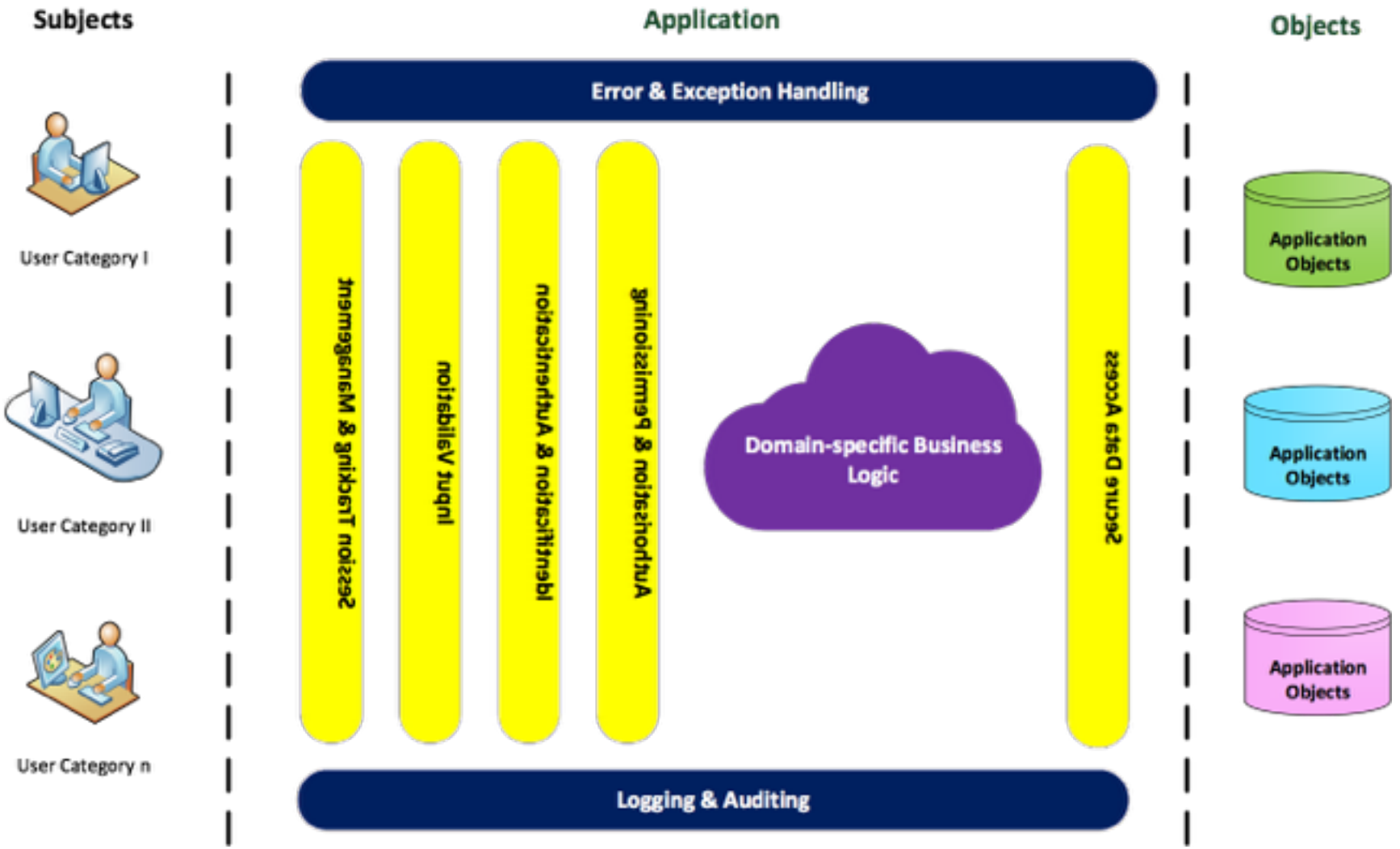
Is SecArch superfluous?

- We didn’t get software ‘right’ in the era of rigider (stricter?) SDLC paradigms – do we stand a better chance in these agile times?
  - Can DevOps make a difference?
  - Can DevSecOps make a difference?

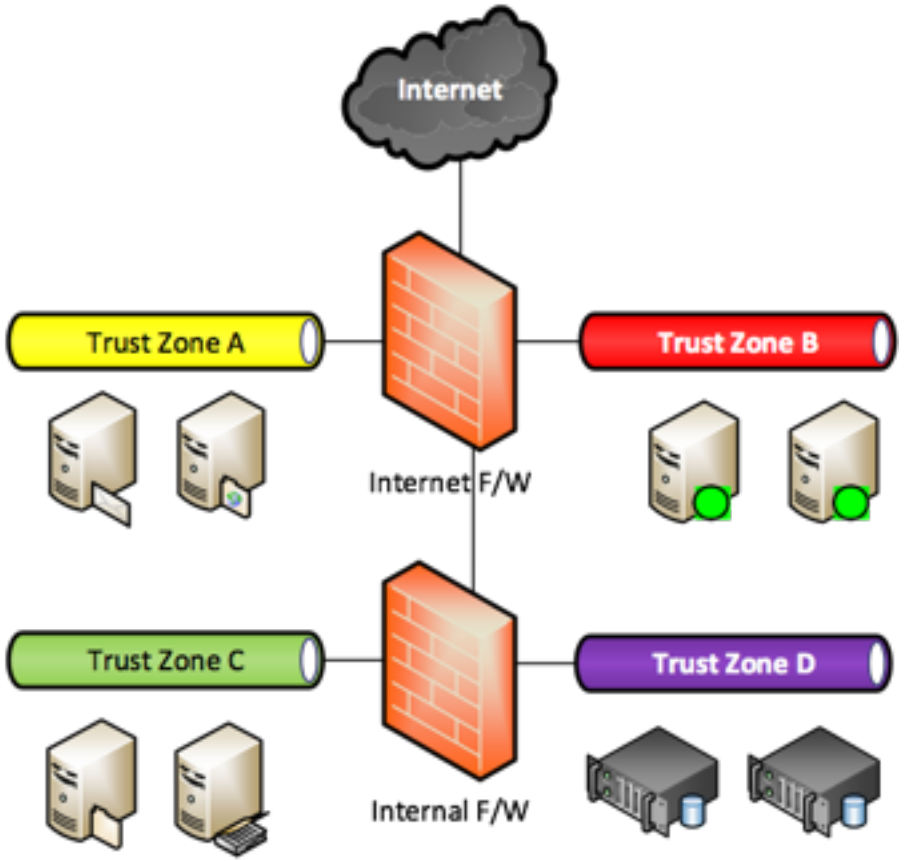
- They are a *step* in the right direction
  - Facilitating (i.e. automating) unwanted (i.e. security) tasks can only help

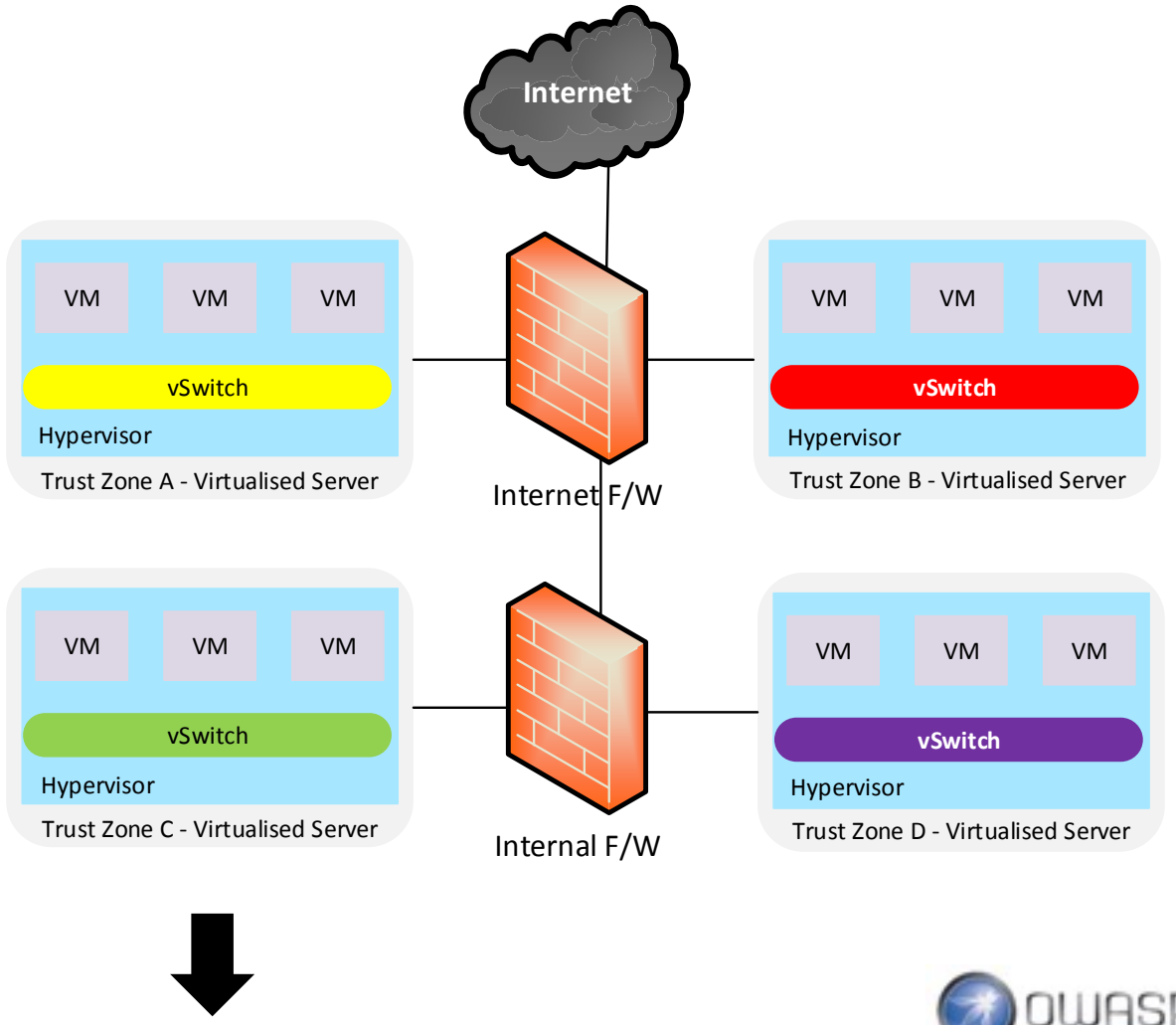
- But they cannot *replace* SecArch

WebApp SecArch (example)

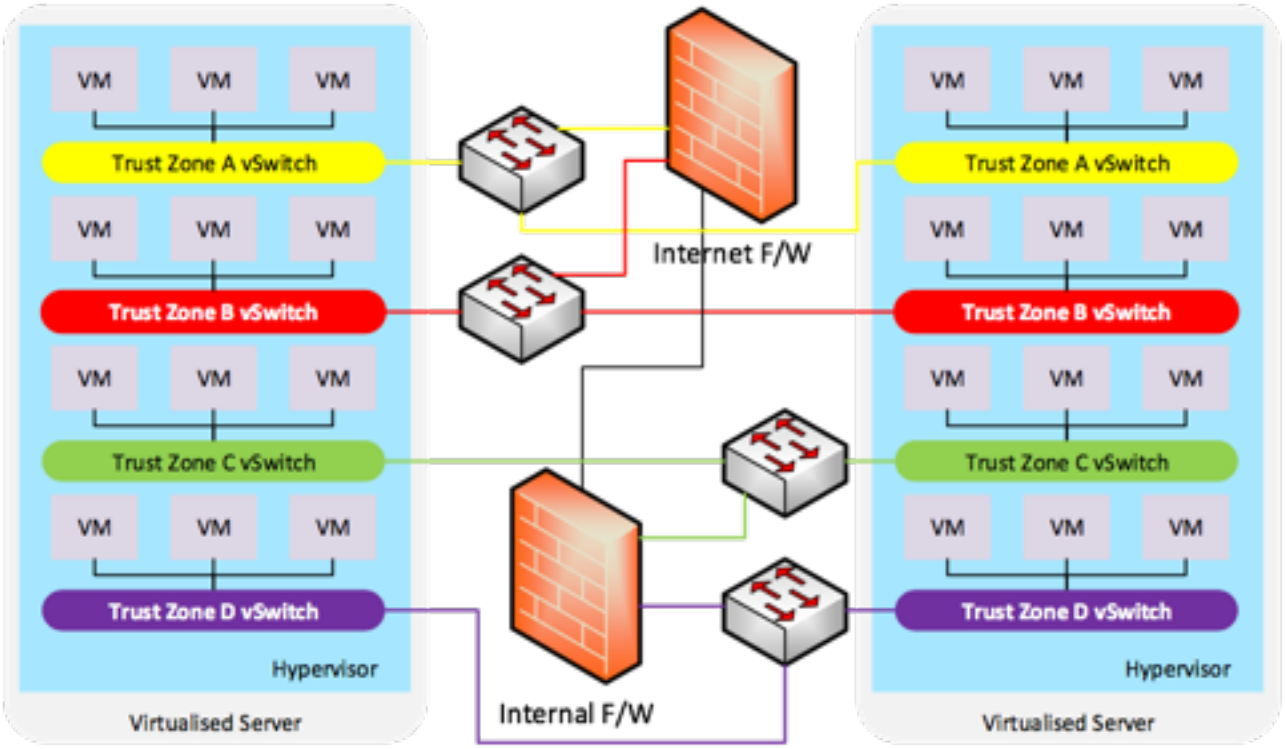


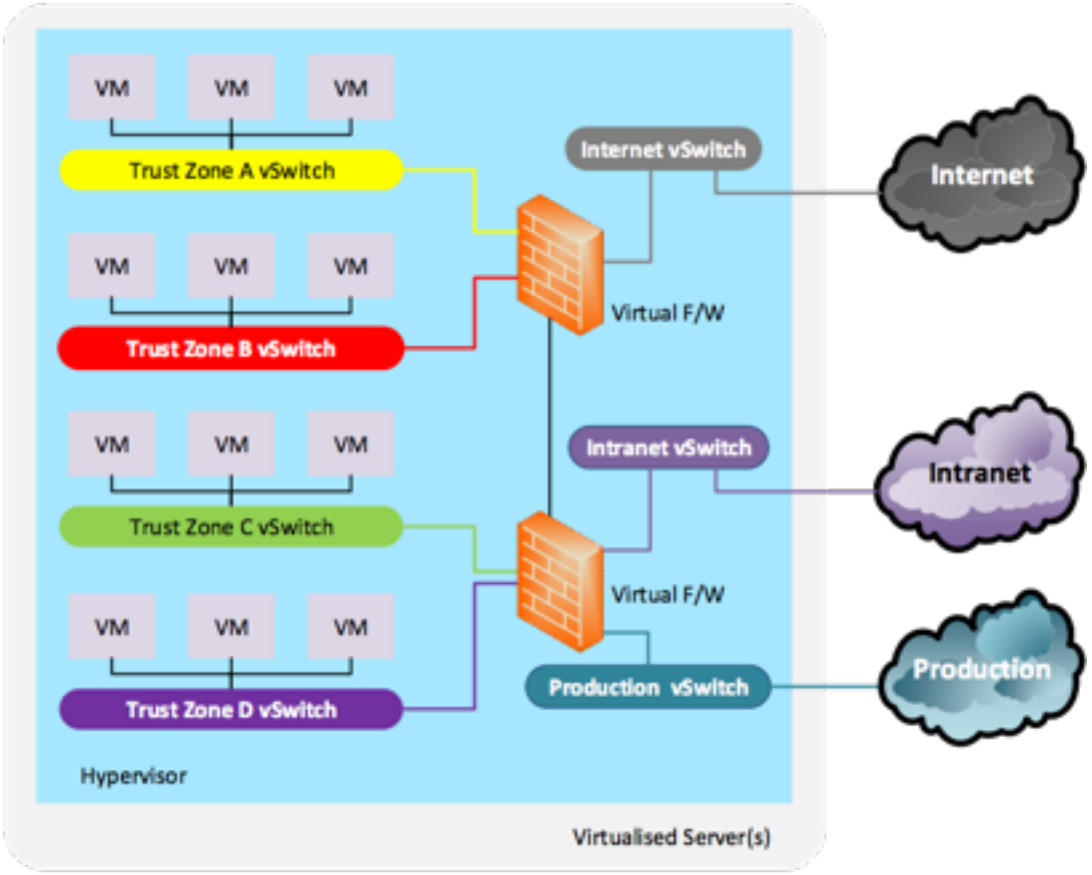
InfraSecArch evolution (example) [1]





InfraSecArch evolution (example) [2]





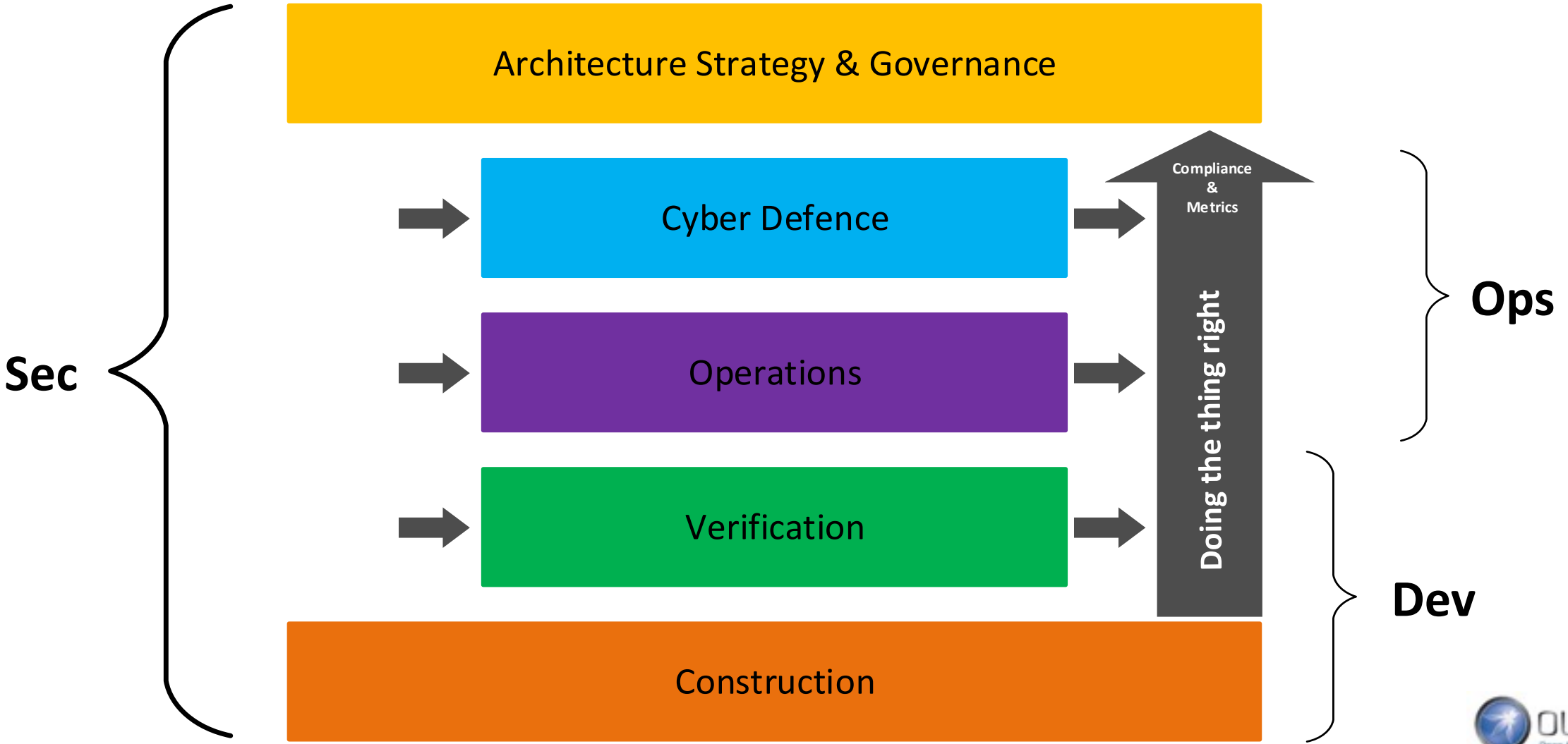
‘* as Code’

- Infrastructure as Code
- Security as Code
- …

- Can we determine (let alone achieve) the objectives without sound SecArch?
  - Manifestos alone (rugged as they may be) are not enough…
  - God help us…

- SecDevOps’ reach is not broad or deep enough…
- It’s not early enough in the lifecycle…

Architecture comes first...



Don’t say I didn’t warn you…

- XY + XZ = X(Y + Z)
- SecDev + SecOps = Sec(Dev + Ops)

Now that σ(Dev, Sec, Ops) has freed us from the *chains of the mundane*, can we focus and spend more time on something that **really matters**?

</Rant>

Thank you for your attention!

Time for questions…

https://www.linkedin.com/in/dpetropoulos/

OWASP
Open Web Application Security Project