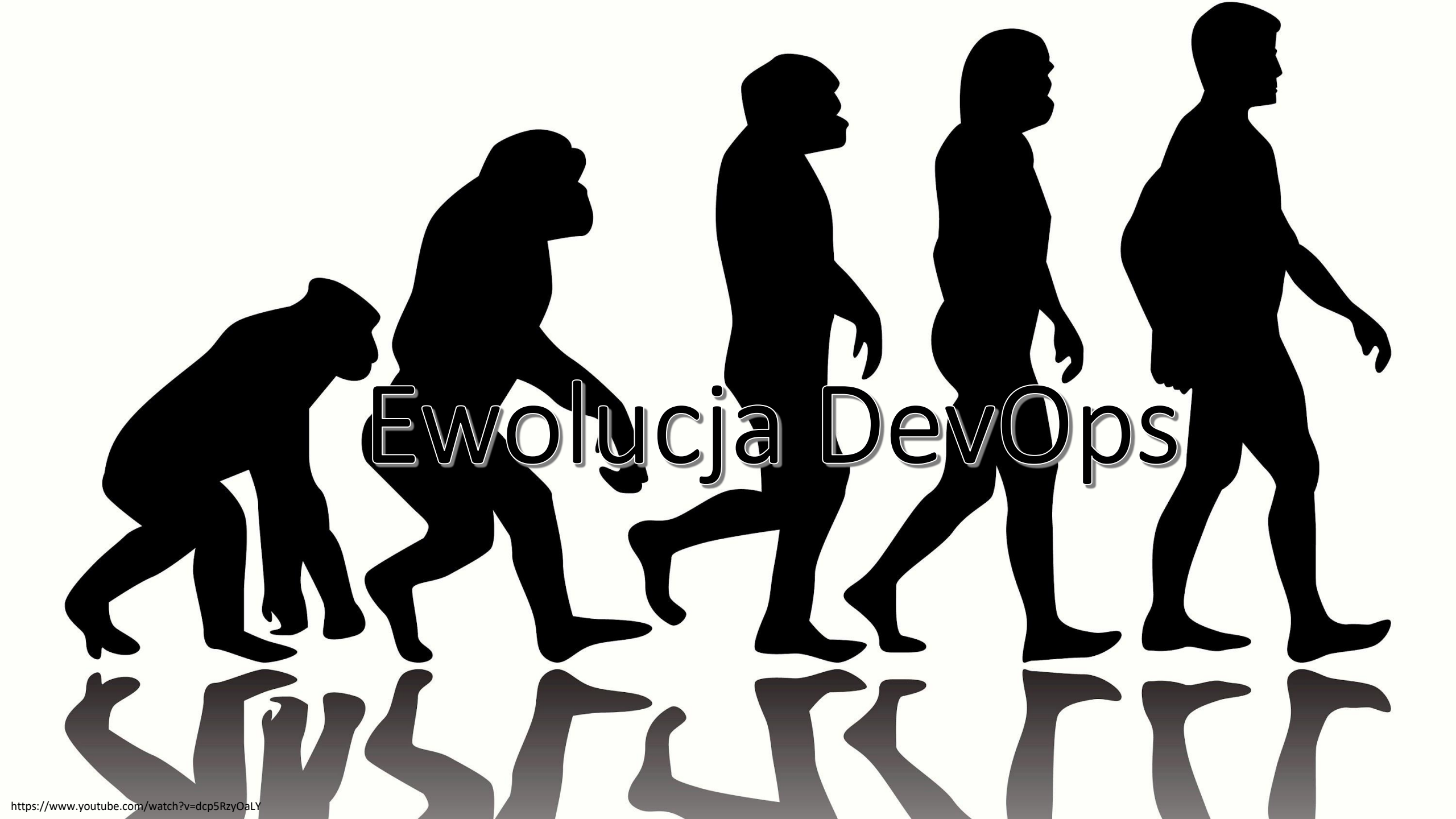
DevOps For Application Security

Krzysztof Kopera
Agile DevOps Consultant
krzysztof.kopera@insc.pl

INTELLIGENT SERVICES

apod.nasa.gov



https://www.youtube.com/watch?v=dcp5RzyOaLY

Equifax a błąd w Apache Struts2

- Wyciek maja’17 – 29 lipca’17
- Publiczna informacja 7 września’17
- 143M kont, 323M osób, 44% populacji USA
- 10 Marca’17 CVE-2017-5638
- 23 marca’17 GA Fix

https://techcrunch.com/2017/09/11/equifax-shares-tumble-another-8-after-credit-score-hack/

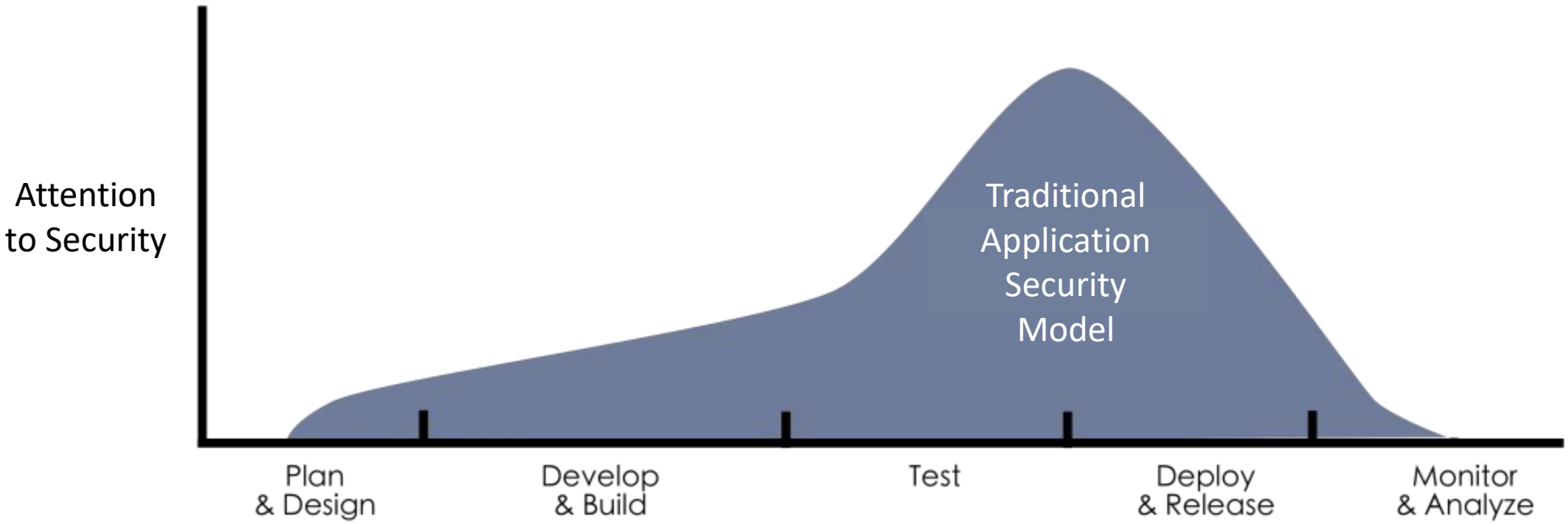
Dostarczać!

Automatyzować!

Bezpiecznie?

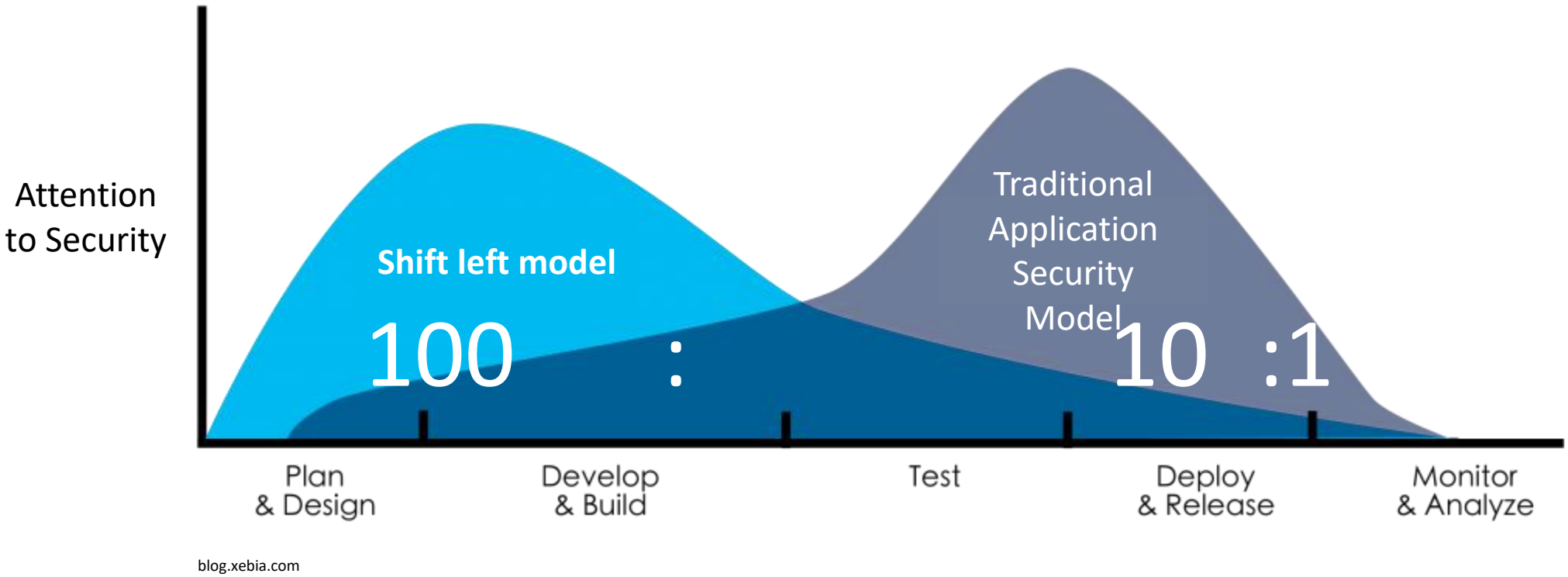
https://magnet.me
wall.alphacoders.com

Tradycyjne bezpieczeństwo aplikacji



blog.xebia.com

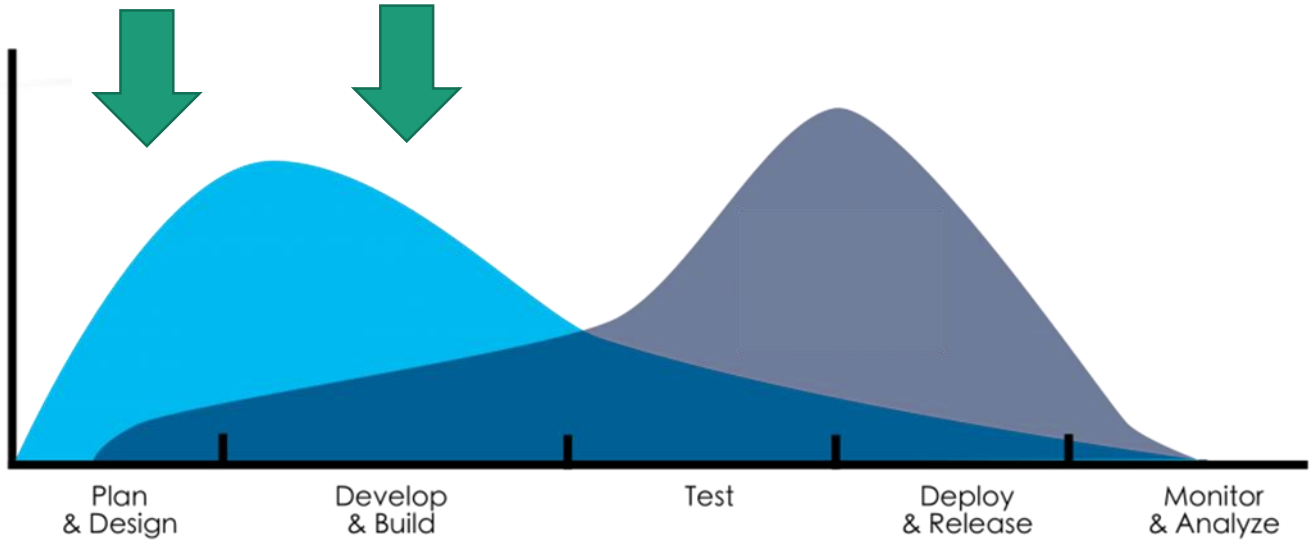
Shift it left!



blog.xebia.com

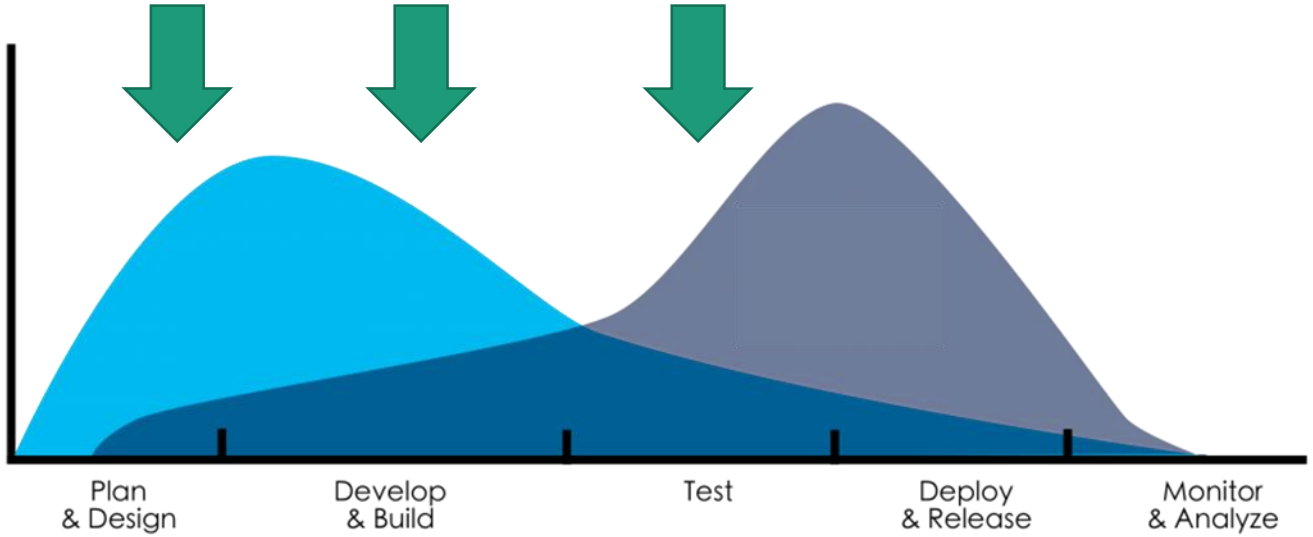
Rozmawiaj o bezpieczeństwie jak najwcześniej

- Planowanie projektu
- Praca nad wymaganiami
- Product show/demo



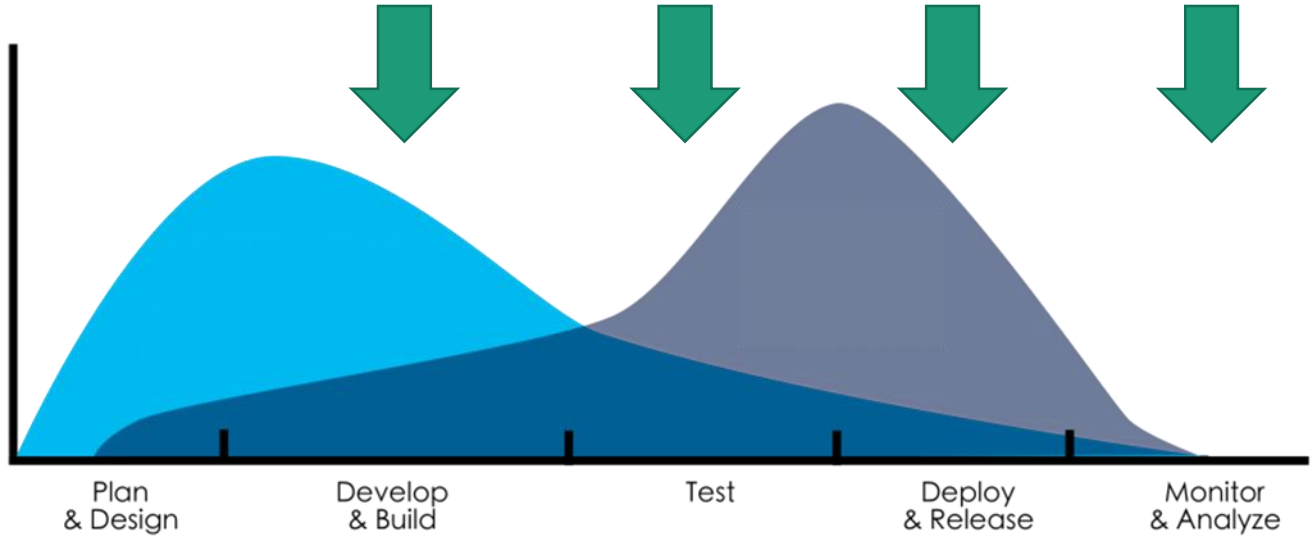
Wspólne repozytorium jako baza zdrowych praktyk

- Kod, biblioteki, testy, środowiska
- Zweryfikowane biblioteki/frameworki
- Standardy aplikacyjne
  - PIN Auth, bcrypt/scrypt, OWASP Sec. Loggi
  - NTP, filesystem, OpenSSL
- Tokeny API, klucze, certyfikaty



Śledź luki bezpieczeństwa

- Luki bezpieczeństwa traktowane jak błędy
- Planowanie napraw i monitorowanie
- Edukacja i zrozumienie zagrożeń

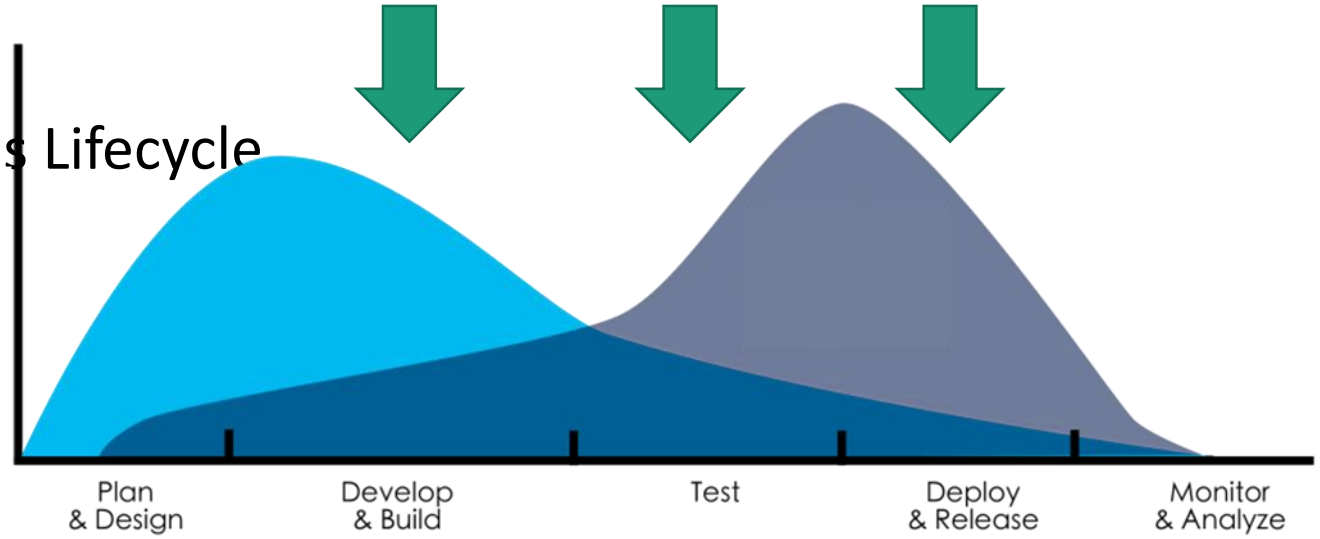


Bezpieczeństwo a strumień CI/CD

https://www.propublica.org
https://bsnscb.com

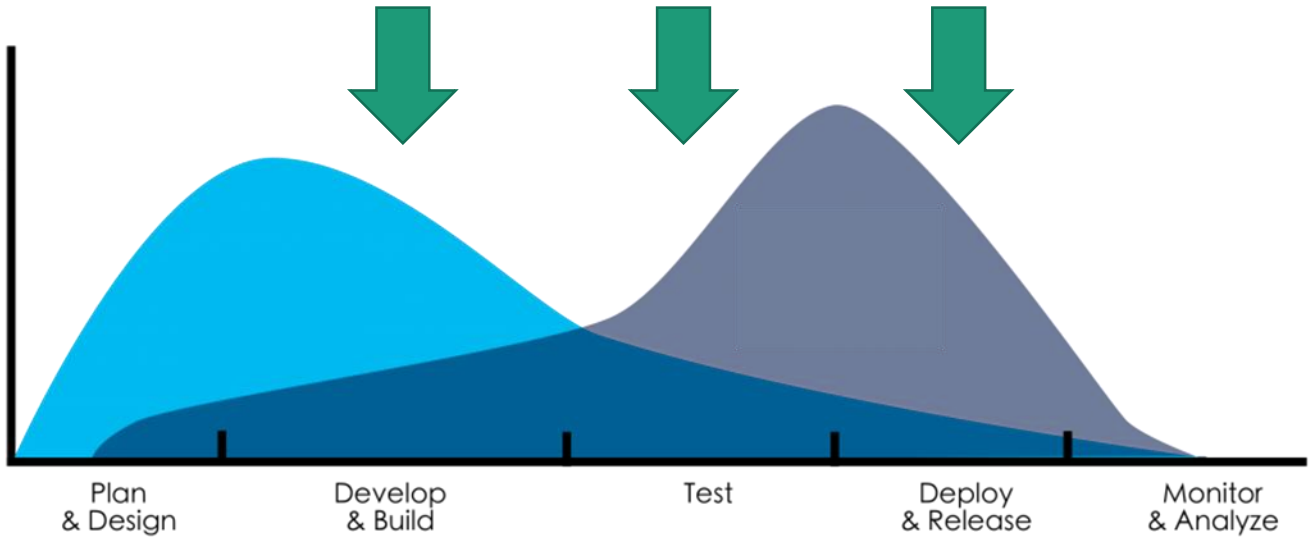
Zabezpieczenie aplikacji

- Dobre praktyki
  - OWASP Cheat Sheet
- Statyczne testy
  - SonarQube, Nexus Lifecycle, Checker framework
- Dynamiczne testy
  - OWASP ZAP, Nmap, Metasploit
- Analiza zależności
  - OWASP Dependency Check, Nexus Lifecycle
- Podpisywanie źródeł
  - Keybase.io



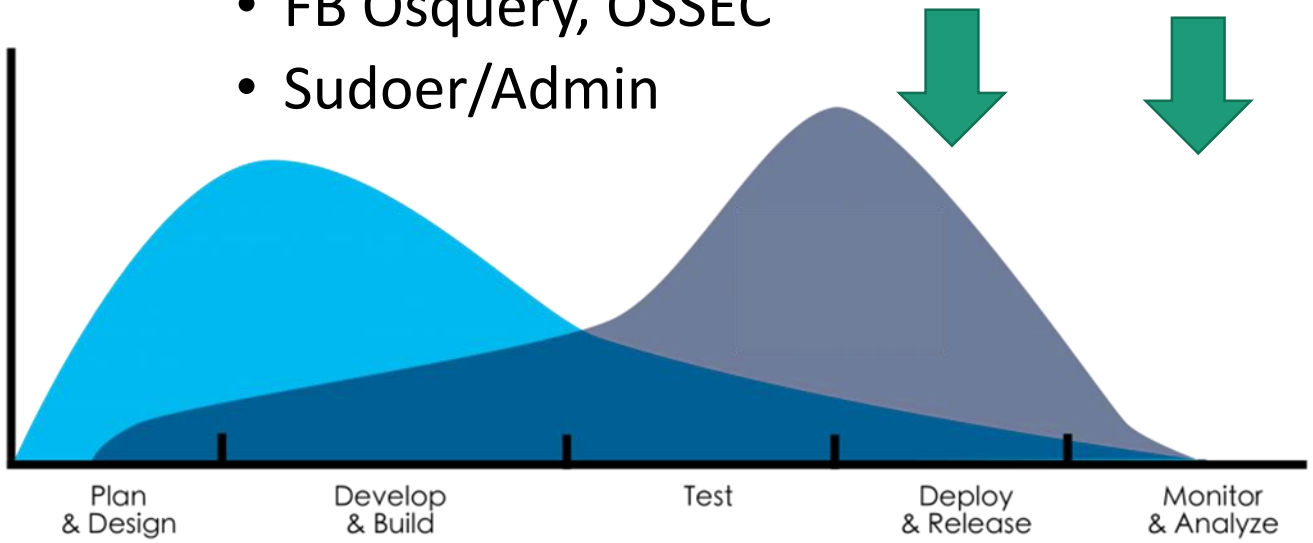
Zabezpieczanie środowisk

- IaaC
  - ChefSpec, Test-kitchen, Serverspec
- Skanowanie środowisk uruchomieniowych
  - Metasploit, Nmap
- Dane i środowiska testowe



Monitorowanie produkcji

- Monitoring aplikacji
  - OpenTSDB, ELK Stack, Grafana
  - Udanie vs. Nieudane logowania
  - Błędy SQL, HTTP 4xx, 5xx
- Zmiany w konfiguracji środowiska
  - FB Osquery, OSSEC
  - Sudoer/Admin



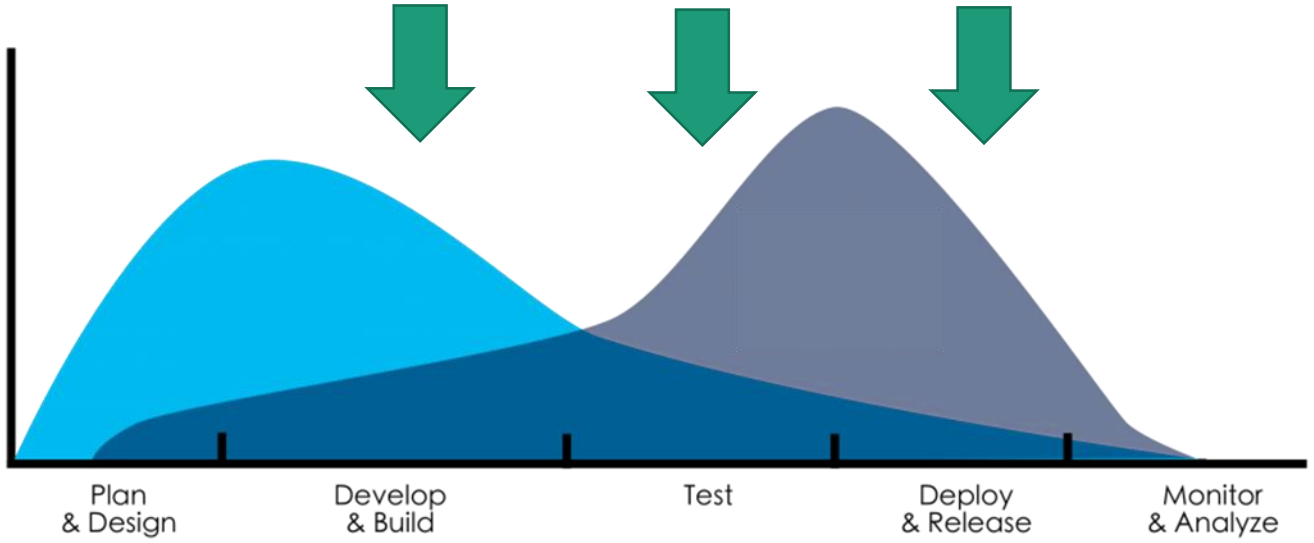
OSSEC

syslog-ng

OpenTSDB

Bezpieczeństwo infrastruktury CI/CD

- Zabezpieczanie konfiguracji środowisk
- Zabezpieczenie narzędzi IaaC oraz CI
- Kontrola dostępu do repozytoriów



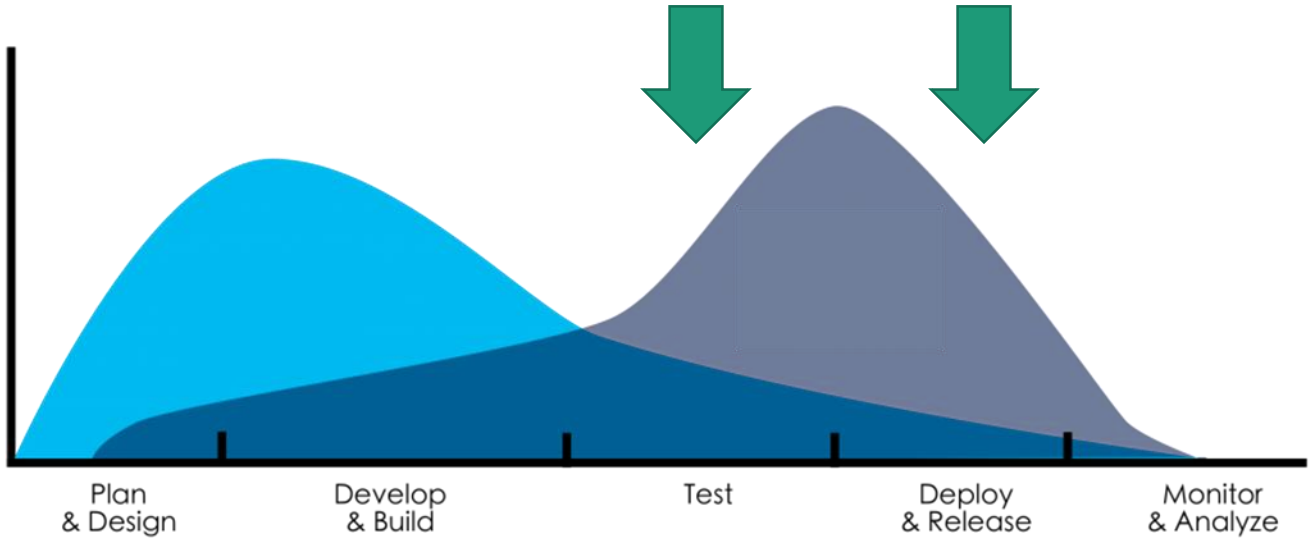
Wdrażanie zmian na produkcję

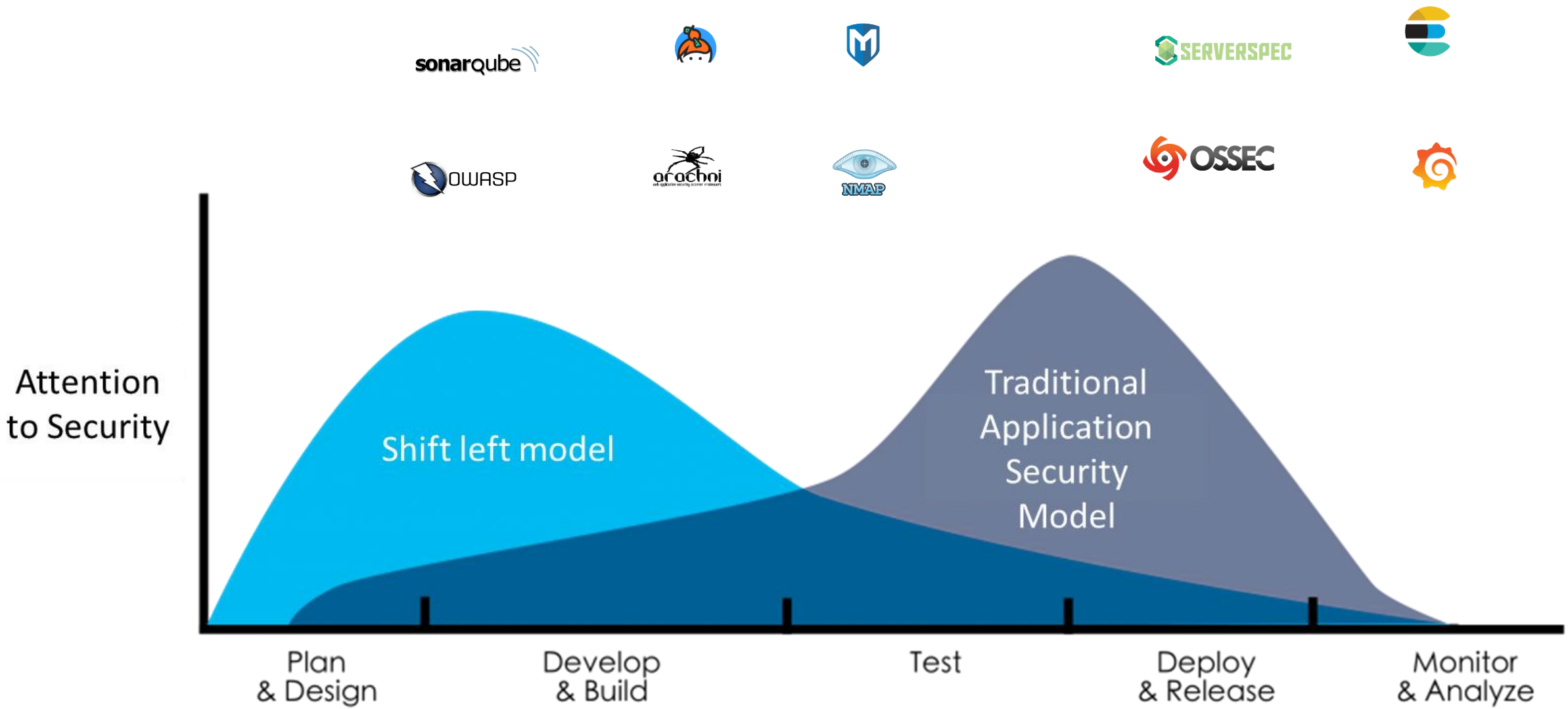
- Wdrożenia zmian:
  - Standardowych
  - Wyższego ryzyka
  - Krytyczne np. przywracające działanie

Electric Cloud

XebiaLabs

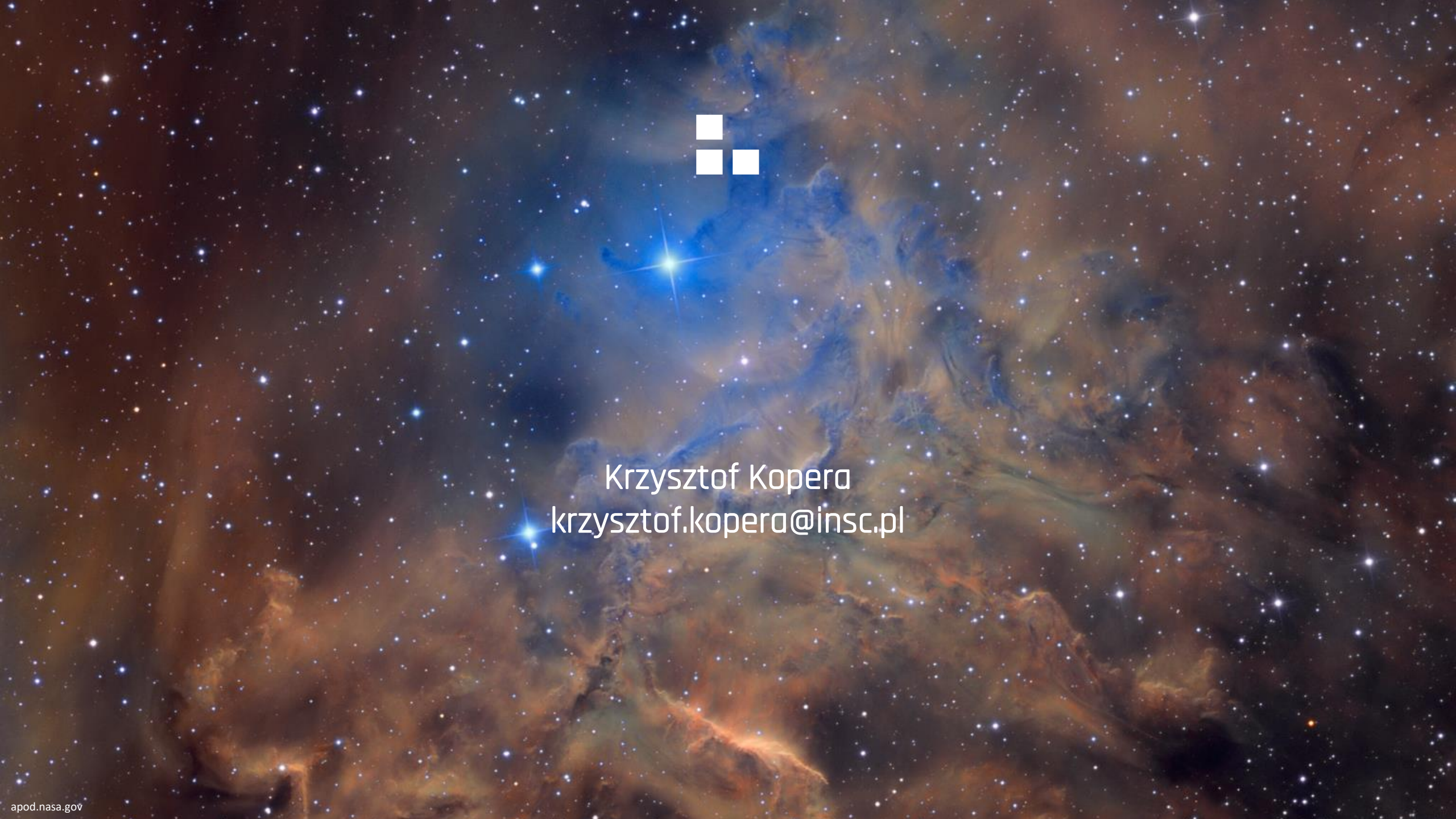
TC




sonarqube
SERVERSPEC
OWASP
arachni
NMAP
OSSEC
Attention to Security
Shift left model
Traditional Application Security Model
Plan & Design
Develop & Build
Test
Deploy & Release
Monitor & Analyze

Kluczowe obszary

- Management buy-in
- Planowanie bezpieczeństwa aplikacji
- Zaangażowanie Zespołu
- Koncentracja zabezpieczeń w procesie



Krzysztof Kopera
krzysztof.kopera@insc.pl

apod.nasa.gov