Bezpieczeństwo oprogramowania w firmie
krok po kroku

Adrian Sroka

Security Architect – British Council/DCG

Twoja firma

- Zatrudnia ludzi
- Posiada procesy
- Przetwarza dane
- Oferuje Klientom swoje systemy

- Jest cenna

Dlaczego hakerzy wolą atakować aplikacje zamiast ich użytkowników?

Czy jesteś pewien bezpieczeństwa swoich systemów?

Co się stanie, gdy zostaną skompromitowane?

Sprawdźmy to. Czy możesz czuć się bezpiecznie?

- Wymuszasz MFA w swoich systemach
- Dbasz o bezpieczeństwo pracowników (w tym szczególnie o deweloperów)
- Dbasz i weryfikujesz bezpieczeństwo procesu wytwarzania
- Dbasz i weryfikujesz bezpieczeństwo infrastruktury
- Dbasz i weryfikujesz bezpieczeństwo aplikacji
- Dbasz o bezpieczeństwo w relacjach z dostawcami

Sprawdźmy to. Czy możesz czuć się bezpiecznie?

6 x TAK - 👍

<6 x TAK - 👉

Jak więc najlepiej zadbać o bezpieczeństwo?

Krok po kroku

Analiza

Co może pójść „nie tak”?

aplikacja

(OWASP TOP 10, OWASP ASVS)

proces wytwórczy

(OWAS SAMM, BSIMM)

łańcuch dostawczy

(CIS Software Supply Chain Security Guide)

infrastruktura

(CIS Benchmarks)

Czemu ataki na łańcuch dostawczy zyskały ostatnio na popularności?

Co interesuje atakujących?

aplikacja

proces wytwórczy

łańcuch dostawczy

infrastruktura

Wymagania zewnętrzne

- GDPR (RODO)
- ISO
- PCI-DSS
- HIPPA
- inne zależne od domeny

https://www.datprof.com/test-data-compliance/

Czynniki ryzyka

- jakie dane przetwarzamy
- kto jest naszym Klientem
- hosting model (chmura, własna infrastruktura, infrastruktura Klienta)

Definiujemy, co jest dla nas ważne z punktu widzenia bezpieczeństwa.
Określamy, gdzie widzimy największe ryzyko.

Realizacja

Główne zasady

- Dbaj o najsłabsze ogniwo
- Nie ufaj nikomu
- Nie komplikuj życia użytkownikom
- Nie dawaj więcej uprawnień niż potrzeba
- Jeden użytkownik nie powinien mieć za dużo uprawnień

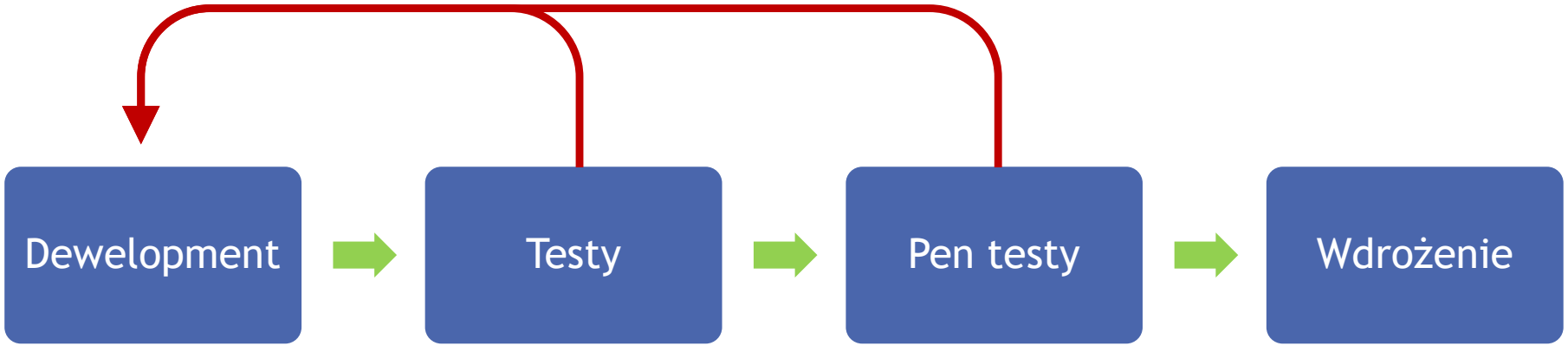
Samodzielny dewelopment

Jest trudniej – więcej do zaadresowania

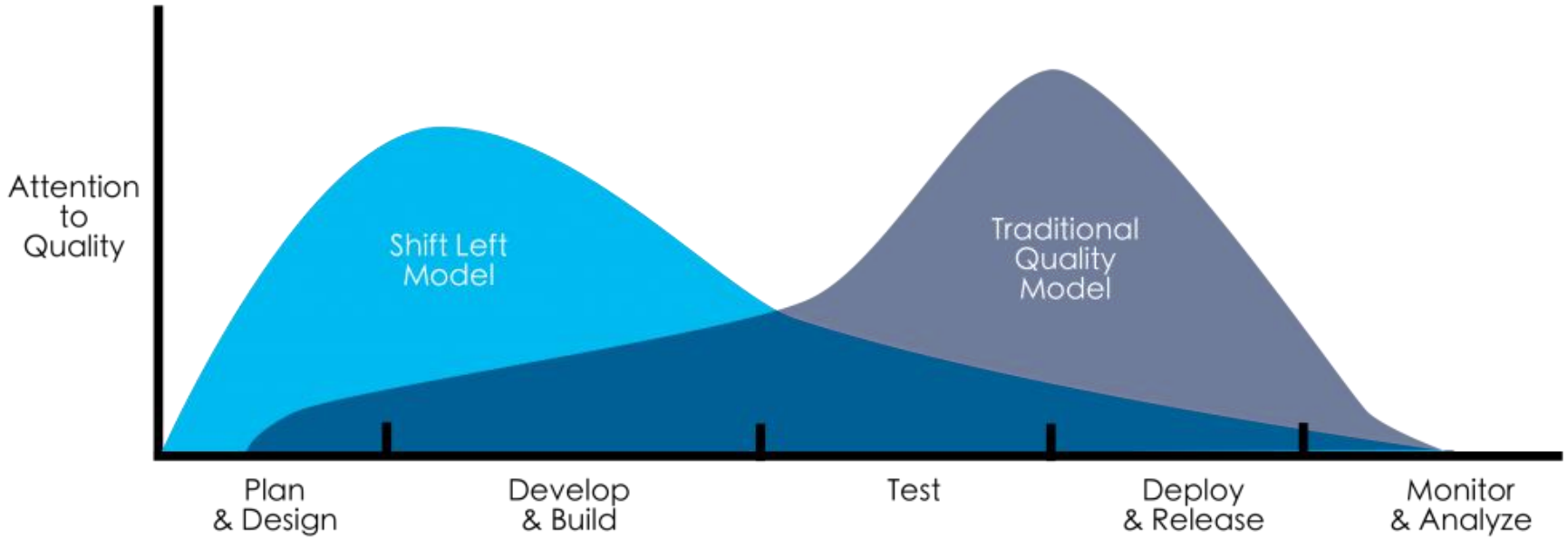
Kilka opcji:

1. Testy i weryfikacja na koniec
2. Wdrożenie bezpieczeństwa w proces wytwarzania
    1. Shift left
    2. DevSecOps

Jak zazwyczaj firmy dbają o bezpieczeństwo oprogramowania?



Shift Left

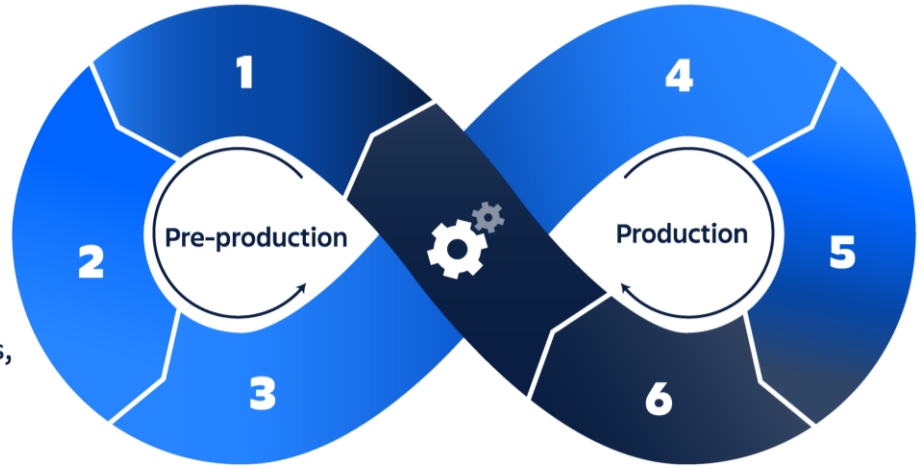


https://devopedia.org/shift-left

DevSecOps

Plan
(PRE-PRODUCTION)
Threat modeling, change impact analysis

Deploy
(PRODUCTION)
Access and configuration management, chaos engineering, pen testing



Build
(PRE-PRODUCTION)
Pre-commit hooks, software composition analysis, SAST, code review, container security, vulnerability scanning, DAST

Operate
(PRODUCTION)
Log collection, RASP, Patching, WAF

Test
(PRE-PRODUCTION)
DAST

Monitor
(PRODUCTION)
SIEM, vulnerability monitoring, access control

https://medium.com/@cloud_tips/devsecops-definition-best-practices-and-tools-1789587d165a

Software Bill of Material

https://www.replicated.com/blog/how-to-validate-the-sboms-on-replicated-releases

Outsourcing dewelopmentu

Czy warto w pełni zaufać dostawcy?

- Są profesjonalistami
- Pracujemy z nimi od dawna
- Ufamy im

Ale

- Czy dbają o bezpieczeństwo?
- Czy robią to tak jak potrzebujemy?

Adwokat interesów naszej firmy

Warto mieć po swojej kogoś, kto zweryfikuje prace zewnętrznych dostawców.

Tak samo jak odbieramy funkcjonalności, powinniśmy odbierać niefunkcjonalne aspekty systemu (np. bezpieczeństwo)

Bezpieczeństwo w aplikacjach

Analiza

- Obszary dewelopmentu
- Zewnętrzne regulacje
- Klasyfikacja danych
- Czynniki ryzyka

Wykonanie

Wewnętrznie

Proces

Łańcuch dostawczy

Aplikacja

Infrastruktura

Outsourcing

Weryfikacja rezultatów

Dziękuję za uwagę

https://securitychampions.pl/