- OH MY - H@CH

Jak wspierać deweloperów w bezpiecznym kodowaniu

Adrian Sroka, Software Security Architect

Jak zazwyczaj dbamy o bezpieczeństwo?

Kto najlepiej zadba o bezpieczeństwo aplikacji?

Deweloper

Dlaczego?

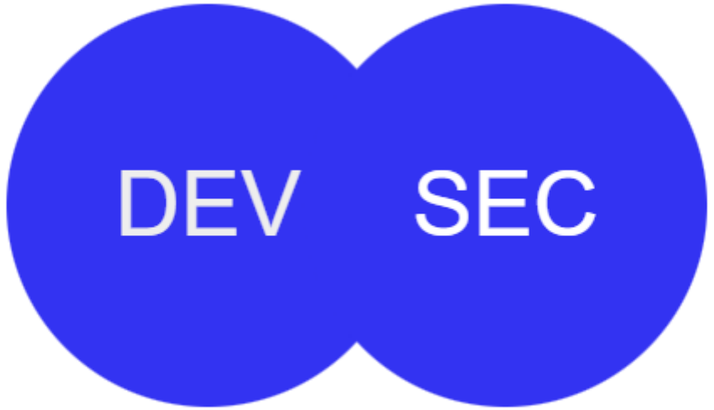
Ma największą wiedzę domenową i techniczną

Ale

Nie jest specjalistą od bezpieczeństwa

Dev + Sec – gdzie zaczynamy

Dev + Sec – gdzie dążymy



Jak wdrażać bezpieczeństwo?

Ludzie

Procesy

Narzędzia

W tej kolejności

Jak możemy pomóc deweloperom?

Szkolenie

Czy to brzmi znajomo?

1. Codzienna praca
2. Szkolenie bezpieczeństwa
3. Ekscytacja
4. Niewiele z tego pamięta

Automatyzacja

- DAST – mała wiedza o aplikacji
- SAST – wąski zakres zagrożeń
- SCA – wartościowe, ale nie sprawdza naszego kodu

Nie jest idealnie

Jaki deweloperzy mają problem z bezpieczeństwem?

- Deweloperzy nie czują się swobodnie
- Brak czasu, żeby poczuć bezpieczeństwo
- W konsekwencji nie stosują się do zasad

Jak więc pomóc developerom?

- Sprawmy, żeby bezpieczeństwo weszło im w krew

Ale…

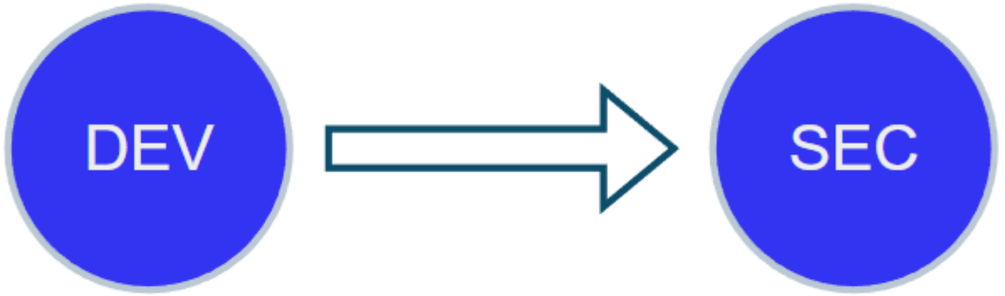
- Łatwo powiedzieć trudniej zrobić

5 metod jak pomóc deweloperom

To może być proste

Ostrzeżenie

- Bazuje to na doświadczeniu i eksperymentach
- Subiektywne



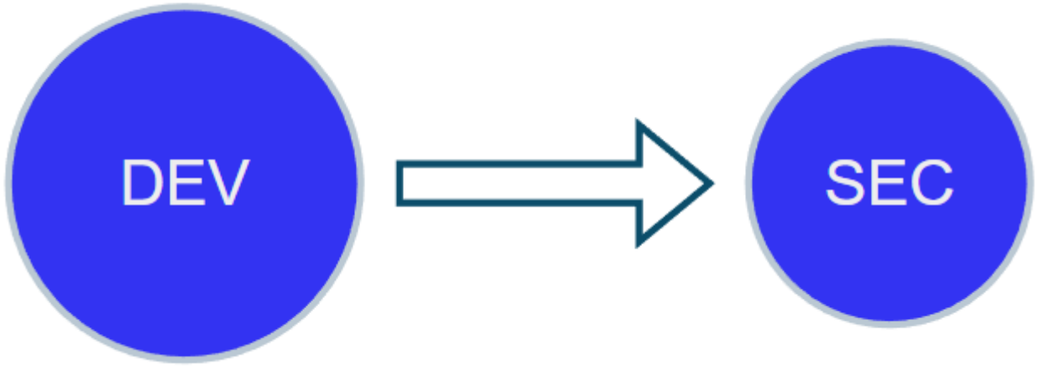
1. Zbudowanie świadomości ważnych obszarów

Nie muszę wiedzieć jak sobie z tym poradzić, wystarczy wiedzieć w jakich przypadkach mam dopytać

Zbudowanie świadomości ważnych obszarów

Budowa mapy tego co ważne:

- obszary
- dane
- funkcjonalności



2. Ułatwienie decyzji

Nawet gdy nie wiem, co będzie najlepsze, wiem gdzie znajdę pomoc

Ułatwienie decyzji

Rodzaje decyzji

- wybór technologii
- biblioteki
- algorytmy
- dobre praktyki

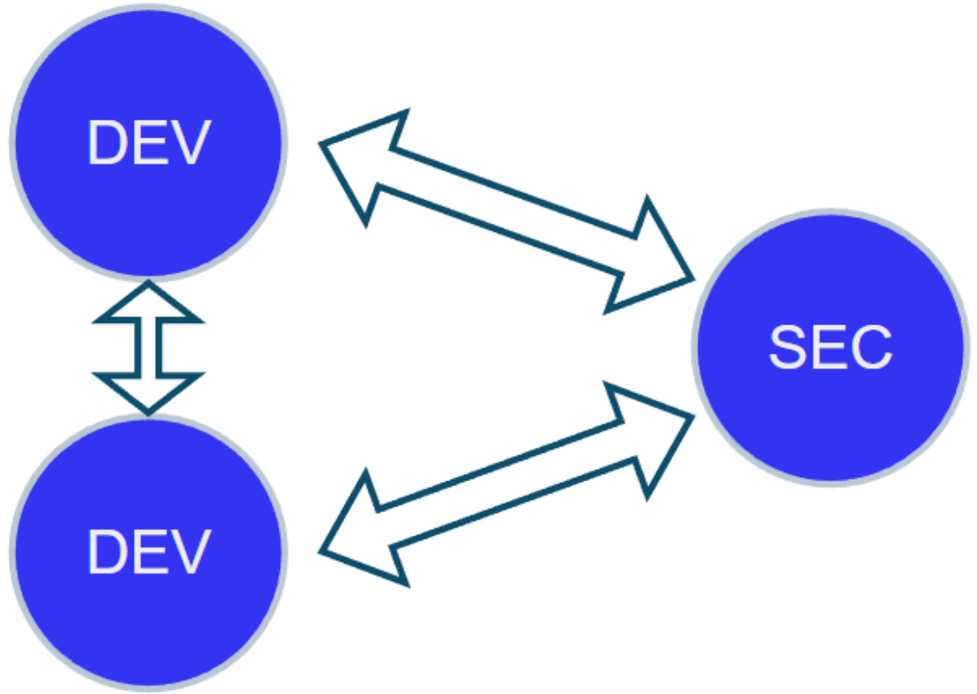
Ułatwienie decyzji

Automatyzuj decyzje tak samo jak automatyzujesz testy

Narzędzia:

- checklisty
- bazy wiedzy
- modele myślowe
- polityki – krótkie

Jeżeli funkcjonalność dotyczy...	... oraz ...	... zadaj następujące pytania
Backend	Pliki	• Czy walidujemy pliki podczas uploadu? ◦ Czy sprawdzamy wielkość, rozszerzenie, content type? • Czy pliki podlegają skanowaniu antywirusowemu? File Upload Cheatsheet



3. Miejsce do dyskusji

Zawsze mam się do kogo odezwać z moim problemem

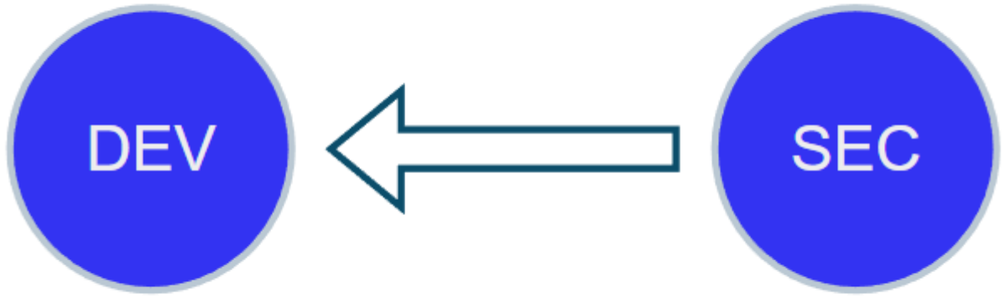
Miejsce do dyskusji

Tworzenie społeczności

- w ramach zespołu
- w ramach firmy

Dobrze, że identyfikuje problemy

i chce o nich mówić



4. Regularna ekspozycja

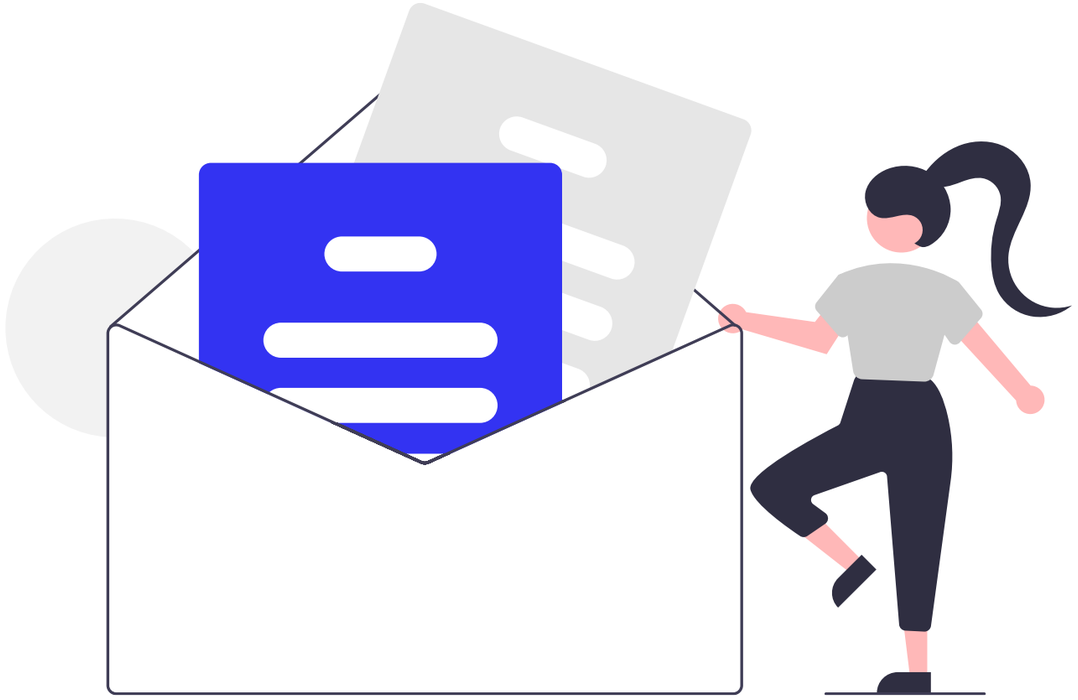
Systematycznie słyszę o bezpieczeństwie i o tym, co się dzieje w tym temacie w firmie

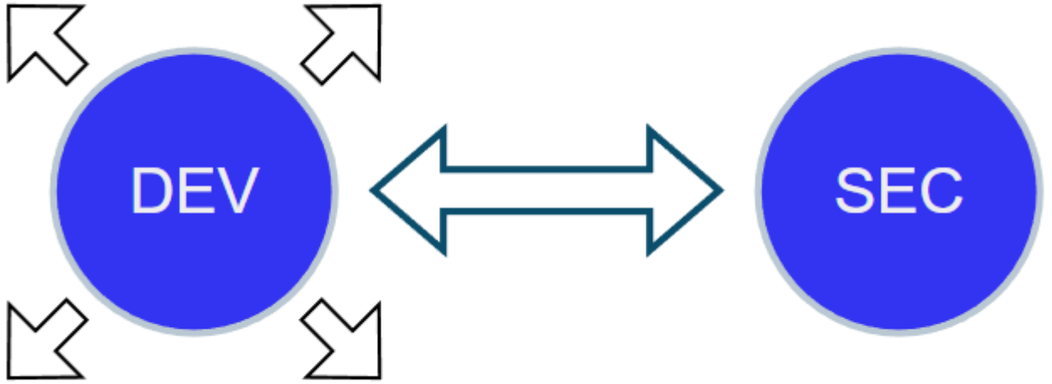
Regularna ekspozycja

Przypomnienia

Newslettery

Transparencja działań



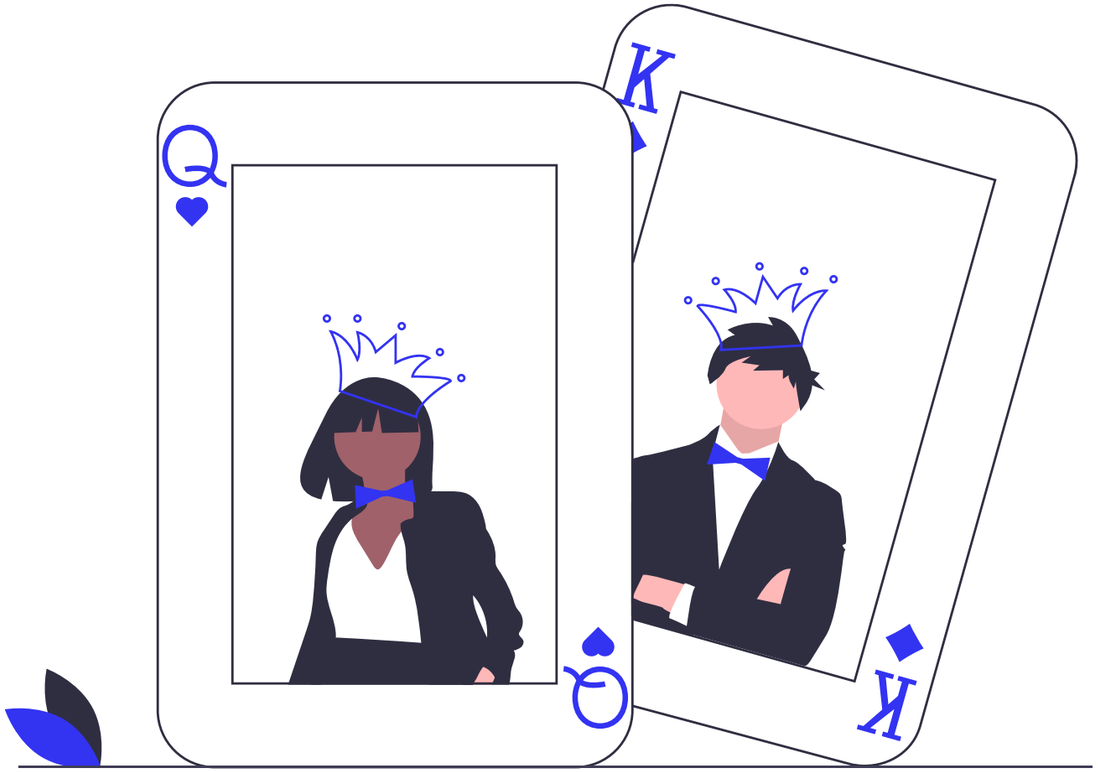


5. Zaangażowanie

Regularnie mogę zweryfikować moją wiedzę i testować nowe pomysły

Zaangażowanie

- Możliwości sprawdzenia się
- Wspólne wyzwania
- Hackatony
- Ćwiczenia
- Włączenie w decyzje



5 kluczowych aspektów

1. Zbudowanie świadomości ważnych obszarów
2. Ułatwienie decyzji
3. Miejsce do dyskusji
4. Regularna ekspozycja
5. Zaangażowanie

Wspólny mianownik

- Komunikacja
- Security Champions

Security Champions

Społeczność ludzi zainteresowanych bezpieczeństwem

Jakie problemy rozwiązuje?

- Skalowanie - Specjaliści bezpieczeństwa nie mogą być w każdym zespole
- Eliminuje dystans – zbliża deweloperów i bezpieczeństwo

Security Champions – jak to zrobić dobrze

Security Champions – jak to zrobić dobrze

Jak utrzymać zainteresowanie?

- Są na bieżąco z tym, co się dzieje w firmie
- Wiedzą więcej niż inni
- Mają większe możliwości

- OH MY - H@CH

Oceń mój wykład
w aplikacji Eventory

1 WEJDŹ W AGENDĘ

2 WYBIERZ MÓJ WYKŁAD

3 OCEŃ I SKOMENTUJ

Dla tych, którzy mnie uważnie słuchali - konkurs:
https://www.diwebsity.com/omh22

3.12.2022