SHIFT LEFT W ORGANIZACJI

Kategoria	Czas trwania	Termin	Cena
Security	2-4 dni/16-32 h*	ustalamy indywidualnie	ustalamy indywidualnie

Program szkolenia:

Poniżej przedstawiamy przykładowy program szkolenia, który może zostać zmodyfikowany zgodnie z oczekiwaniami oraz poziomem grupy szkoleniowej. Przed przygotowaniem docelowego programu szkolenia, przeprowadzamy rozmowę techniczną, w której bierze udział trener oraz osoba techniczna lub cały zespół developerów reprezentujący klienta, w celu ustalenia szczegółów szkolenia.

Czas trwania szkolenia zależy od zaawansowania grupy i wyniku ankiety przedszkoleniowej.

Program

1. Podstawy koncepcji Shift Left i Shift Left Security

- Wprowadzenie do Shift Left: Wyjaśnienie, na czym polega koncepcja przesuwania testów oraz praktyk bezpieczeństwa na wcześniejsze etapy rozwoju oprogramowania
- Korzyści z Shift Left i Shift Left Security: Omówienie zalet wczesnego wykrywania błędów i luk bezpieczeństwa, takich jak obniżenie kosztów napraw, zmniejszenie ryzyka cyberataków oraz zwiększenie jakości i zgodności z przepisami.

2. Praktyki i techniki Shift Left oraz Shift Left Security

- Testowanie wczesne i częste (Early Testing): Wprowadzenie technik, takich jak testowanie na etapie planowania i projektowania oraz przeprowadzanie testów statycznych kodu.
- Test-Driven Development (TDD) i Behavior-Driven Development (BDD): Przedstawienie podejść wymuszających tworzenie testów przed implementacją funkcji, co umożliwia wczesne wykrywanie problemów zarówno jakościowych, jak i związanych z bezpieczeństwem.

Program c.d.

- Automatyzacja testów i bezpieczeństwa: Nauka implementacji automatyzacji testów jednostkowych, integracyjnych i bezpieczeństwa przy użyciu narzędzi takich jak Jenkins, Selenium, JUnit oraz narzędzi do analizy bezpieczeństwa (np. SonarQube, Snyk, Fortify).
- Continuous Integration/Continuous Deployment (CI/CD) i automatyzacja bezpieczeństwa: Omówienie, jak zintegrować testy i kontrole bezpieczeństwa w procesie CI/CD, aby zapewnić ciągłe testowanie i weryfikację kodu, uwzględniając aspekty bezpieczeństwa na każdym kroku.

3. Bezpieczeństwo na wczesnych etapach procesu (Shift Left Security)

- Bezpieczne projektowanie (Security by Design): Jak uwzględniać zasady bezpieczeństwa na etapie projektowania systemu, aby minimalizować ryzyko ataków.
- Testy bezpieczeństwa na każdym etapie: Jak integrować testy bezpieczeństwa, takie jak analiza statyczna i dynamiczna kodu, oraz testy penetracyjne w procesie rozwoju.
- Threat Modeling: Modelowanie zagrożeń na etapie projektowania, aby identyfikować potencjalne wektory ataku i wdrażać odpowiednie zabezpieczenia.

4. Wykorzystanie narzędzi wspierających Shift Left oraz Shift Left Security

- Narzędzia do analizy statycznej i dynamicznej kodu: Przedstawienie narzędzi, takich jak SonarQube, Checkstyle, ESLint do analizy jakości kodu oraz Snyk, Veracode i Fortify do analizy bezpieczeństwa.
- Automatyzacja testów i skanowanie zależności: Jak stosować narzędzia do automatyzacji testów oraz skanowania obrazów kontenerów i zależności (np. Docker, Aqua Security), aby wykrywać błędy i luki bezpieczeństwa

Program c.d.

5. Zmiana kultury organizacyjnej na „Quality & Security First"

- Współpraca zespołowa DevSecOps: Podkreślenie znaczenia współpracy między zespołami deweloperskimi, testerami, operacjami i zespołem bezpieczeństwa, aby zarówno jakość, jak i bezpieczeństwo były wspólną odpowiedzialnością
- Kultura jakości i bezpieczeństwa: Wprowadzenie praktyk, które promują odpowiedzialność każdego członka zespołu za jakość i bezpieczeństwo od samego początku cyklu rozwoju.
- Mentoring i coaching: Jak promować praktyki Shift Left i Shift Left Security w codziennej pracy oraz wspierać rozwój zespołu w tych obszarach.

6. Testowanie, monitorowanie i zarządzanie ryzykiem

- Metryki jakości i bezpieczeństwa: Nauka identyfikowania i mierzenia kluczowych wskaźników, takich jak czas wykrycia błędu, czas naprawy, pokrycie testów oraz zarządzanie podatnościami (Vulnerability Management).
- Ciągłe monitorowanie i analiza ryzyka: Wykorzystanie narzędzi do monitorowania infrastruktury i aplikacji pod kątem nowych zagrożeń i podatności (np. AWS Security Hub, Splunk).

7. Case study i praktyczne warsztaty

- Praktyczne przykłady wdrożeń Shift Left i Shift Left Security: Omówienie przypadków firm, które wdrożyły te strategie z sukcesem, oraz jakie korzyści osiągnęły.
- Warsztaty i symulacje: Symulacje i ćwiczenia praktyczne, które pozwalają uczestnikom na zastosowanie zdobytej wiedzy w realistycznych scenariuszach

8. Dostosowanie Shift Left i Shift Left Security do kontekstu organizacyjnego

- Analiza obecnych procesów w firmie: Ocena, w którym momencie cyklu życia produktu najlepiej wprowadzać elementy Shift Left i Shift Left Security, aby miało to największy sens.
- Plan wdrożenia i dostosowanie strategii: Opracowanie spersonalizowanej strategii, która stopniowo wdraża te praktyki w sposób dostosowany do unikalnych procesów i narzędzi używanych w organizacji

KONTAKT

Jesteś zainteresowany dedykowanym szkoleniem dla Twojej firmy?

Skontaktuj się z Przemkiem!

PRZEMYSŁAW WOŁOSZ

Key Account Manager

(+48) 730 830 801

przemyslaw.wolosz@infoShareAcademy.com