

Program szkolenia:

Kubernetes - bezpieczeństwo platformy i kontenerów

Informacje:

Nazwa:	Kubernetes - bezpieczeństwo platformy i kontenerów
Kod:	sec-kuber
Kategoria:	Narzędzia
Odbiorcy:	developerzy, architektki, DevOps
Czas trwania:	2 dni
Forma:	50% wykłady / 50% warsztaty

Kubernetes doskonale sprawdza się jako docelowe miejsce do uruchamiania mikroserwisów, ale często też służy jako uniwersalna platforma do budowania złożonych systemów. To szkolenie porusza najważniejsze tematy związane z bezpieczeństwem samej platformy oraz aplikacji na niej uruchamianych. Uczestnicy zapoznają się z modelem RBAC, możliwościami związanymi z ograniczeniami działania kontenerów, wewnętrznego firewalla (NetworkPolicy) do zapewnienia bezpiecznego dostępu do danych poufnych aplikacji. Szkolenie ma charakter warsztatu, gdzie uczestnicy w praktyce wdrożą zdobytą wiedzę na praktycznych przykładach.

Ze względu na charakter praktyczny wymagane jest, aby uczestnicy:

- znali podstawy działania Kubernetesa
- poruszali się swobodnie w linuksowym środowisku linii poleceń
- byli zaznajomieni z typowymi narzędziami typu ssh, vim (lub inny edytor tekstu dostępny w linuxie)

Zalety szkolenia:

Uczestnicy po szkoleniu będą:

- potrafili zwiększyć bezpieczeństwo obrazów kontenerów uruchamianych na platformie
- znali zasadę działania kontroli dostępu do zasobów klastra na podstawie ról (RBAC - Role Based Access Control)
- potrafili utworzyć własną rolę dla użytkownika i aplikacji
- potrafili ograniczyć ruch między aplikacjami wewnątrz klastra oraz ruch wchodzący i wychodzący poza

Szczegółowy program:

1. Jak działają "pod spodem" kontenery w Kubernetes
2. Hardening obrazów (container image)
3. Least privilege - ograniczenie uprawnień kontenerów
4. Wymuszanie stosowania dobrych praktyk bezpieczeństwa na klastrze
5. Skanowanie pod kątem bezpieczeństwa obrazów i plików konfiguracyjnych
6. Wymuszanie stosowania bezpiecznych obrazów
7. Przechwytywanie i analiza zagrożeń (threat detection)
8. RBAC i zasada jego działania
9. Nadawanie ról użytkownikom i kontom serwisowym
10. Tworzenie własnych ról RBAC
11. Ograniczanie ruchu sieciowego Podów za pomocą Network Policy
12. Podejście Multi-tenant
13. Jak bezpiecznie opublikować aplikację na zewnątrz klastra