BO·TT·EGA
IT minds

Program szkolenia:

Kubernetes - bezpieczeństwo platformy i kontenerów

Informacje:

Nazwa:	**Kubernetes - bezpieczeństwo platformy i kontenerów**
Kod:	**sec-kuber**
Kategoria:	DevOps i narzędzia
Odbiorcy:	architekci, developerzy, 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 patformy 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 linuksie)

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

BOTTEGA IT minds

Szczegółowy program:

1. Analiza ryzyk środowiska Kubernetes i aplikacji na nim uruchomionych

2. RBAC i zasada jego działania

3. Konta serwisowe dla aplikacji i użytkowników

4. Nadawanie ról użytkownikom i grupom

5. Workload Identity

6. Domyślne mechanizmy zabezpieczeń kontenerów w Kubernetes

7. Ograniczenie uprawnień kontenerów (gVisor, appArmor)

8. Wymuszanie stosowania dobrych praktyk bezpieczeństwa na klastrze

9. Przechwytywanie i analiza zagrożeń z Falco

10. Ograniczanie ruchu sieciowego podów za pomocą Network Policy

11. Bezpieczne udostępnianie aplikacji na zewnątrz klastra

12. Zabezpieczanie współdzielonych środowisk (multitenancy)