BOTTEGA IT minds

Program szkolenia:

Świadomość problemów bezpieczeństwa (OWASP, Cloud, CD) dla programistów Java, .Net, Node.js

Informacje:

Nazwa:	**Świadomość problemów bezpieczeństwa (OWASP, Cloud, CD) dla programistów Java, .Net, Node.js**
Kod:	**sec-OWASP**
Kategoria:	Bezpieczeństwo
Grupa docelowa:	architekci developerzy testerzy
Czas trwania:	3 dni
Forma:	50% wykłady / 50% praktyczne demonstracje

Niniejsze szkolenie stanowi wprowadzenie do tematyki bezpieczeństwa aplikacji Webowych. W trakcie szkolenie wyjdziemy daleko poza OWASP.

Dla każdego z zagrożeń przedstawimy:

- Mechanizm działania
- Sposoby wykrycia
- Sposoby przeciwdziałania
- Przykładowy scenariusz ataku

Wybrane zagrożenia zostanę zilustrowane studiami konkretnych przypadków firm i instytucji, które padły ofiarą ataków.

Warsztaty praktyczne będą przeprowadzone w zależności od potrzeb grupy w Javie, C#, Node.js.

Zalety szkolenia:

- Wychodzimy poza OWASP w kierunku Cloud i Continous Delivery
- Praktyczne demonstracje ataków zależne od wybranego stosu technologicznego
- Trener pracujący na codzień w ogólnoświatowej organizacji zajmującej się rozwiązaniami z zakresu bezpieczeństwa

BOTTEGA IT minds

Szczegółowy program:

1. OWASP Top 10

- 1.1. Wstrzyknięcia
- 1.2. Błędy w uwierzytelnianiu
- 1.3. Wyciek danych wrażliwych
- 1.4. XML External Entities
- 1.5. Błędy w kontroli dostępu
- 1.6. Błędna konfiguracja zabezpieczeń
- 1.7. Cross-site Scripting (XSS)
- 1.8. Błędy deserializacji
- 1.9. Komponenty ze znanymi podatnościami
- 1.10. Brak logowania i monitoringu

2. OWASP - co dalej?

- 2.1. Proactive controls
- 2.2. ASVS
- 2.3. Testing Guide

3. OWASP Top 10 w praktyce programisty Java/.NET/Node.js

- 3.1. Obrona przed wstrzyknięciami
- 3.2. Uwierzytelnianie z OAuth 2.0 i OpenID Connect
- 3.3. Ochrona danych wrażliwych z Azure Key Vault
- 3.4. Ochrona przed XSS

4. Bezpieczeństwo w Continuous Delivery

- 4.1. Monitoring podatności za pomocą Dependency Check i Dependency Track
- 4.2. Statyczna analiza kodu za pomocą find-sec-bugs

BOTTEGA IT minds

4.3. Skanowanie za pomocą OWASP ZAP

5. Bezpieczeństwo w chmurze

5.1. HTTPS i nagłówki HTTP dot. Bezpieczeństwa

5.2. Web Application Firewalls i OWASP Core Rule Set

5.3. Kontrola dostępu do klastra Kubernetesa

5.4. Kontrola dostępu do środowiska CI/CD

5.5. Logowanie i monitoring za pomocą systemu klasy SIEM na przykładzie SumoLogic

6. API Security

6.1. Użycie OAuth 2.0 oraz tokenów JWT w celu zabezpieczenia dostępu do API

6.2. Wprowadzenie do Azure Active Directory

6.3. Wprowadzenie do Azure API Management and policies

6.4. API access control z wykorzystaniem Azure API Management

6.4.1. Network access control i IP restrictions

6.4.2. Ochrona przed atakami DoS z wykorzystaniem throttling and caching

6.4.3. Wykorzystanie OAuth 2.0 i tokenów JWT z Azure API Management