BO·TT·EGA
IT minds

Program szkolenia:

Modelowanie zagrożeń - projektowanie wymagań bezpieczeństwa systemów

Informacje:

Nazwa:	**Modelowanie zagrożeń - projektowanie wymagań bezpieczeństwa systemów**
Kod:	**sec-model**
Kategoria:	Bezpieczeństwo
Odbiorcy:	developerzy, analitycy, admini, architekci
Czas trwania:	1 dzień
Forma:	30% wykłady, 70% warsztaty

Autorski program szkolenia oparty o wieloletnie doświadczenie w testowaniu bezpieczeństwa, dobieraniu zaleceń i projektowaniu wymagań bezpieczeństwa systemów. Modelowanie zagrożeń to część podejścia "Shift Left" i kompleksowa metodyka unikania podatności w aplikacjach i systemach zanim powstanie dane rozwiązanie, a także komunikowania ryzyk bezpieczeństwa do zarządu.

Modelowanie zagrożeń to testy bezpieczeństwa na kartce - burza mózgów, której efektem jest zwiększenie świadomości ryzyka bezpieczeństwa i opracowanie zabezpieczeń adekwatnych do ryzyka. Obecne metodyki modelowania zagrożeń są szalenie skomplikowane, pracochłonne i wymagają zgromadzenia dużej ilości informacji na wejściu. W naszym podejściu „light weight" staramy się uprościć ten proces, tak żeby mógł być on wpleciony w cykl rozwojowy każdej aplikacji. Metoda ta polega na odpowiedzeniu sobie na trzy pytania: KTO chciałby zaatakować nasz system? CO – jest jego celem? Oraz – JAK atakujący może to osiągnąć? W końcowej fazie analizy do potencjalnych metod ataku dobieramy zabezpieczenia i to jest produkt modelowania zagrożeń. Podczas warsztatów uczestnicy nauczą się samodzielnie przeprowadzać analizę na przykładzie kilku aplikacji i systemów. Dzięki szkoleniu uczestnicy nauczą się również świadomie podejmować decyzje na temat architektury rozwiązania, sposobów uwierzytelnienia i przetwarzania danych.

KORZYŚCI WYNIKAJĄCE Z MODELOWANIA ZAGROŻEŃ

- Architekci - biorąc pod uwagę potencjalne zagrożenia, wprowadzają zmiany w projekcie na etapie planowania
- Developerzy i administratorzy - pisząc kod lub konfigurując systemy, biorą pod uwagę wymagania bezpieczeństwa i implementują bezpieczne rozwiązania
- Dział bezpieczeństwa - otrzymuje metrykę bezpieczeństwa i może oceniać jakość oprogramowania pod kątem bezpieczeństwa
- Testerzy QA i bezpieczeństwa - weryfikują przypadki testowe wynikające z modelu zagrożeń, efektywniej pokrywają zakres testów
- Właściciel produktu - podejmuje świadome decyzje bazujące na znanym ryzyku, może przekazywać wymagania bezpieczeństwa do firm trzecich
- Klienci - klienci rozwiązań klasy enterprise oczekują wyników testów bezpieczeństwa, a model zagrożeń to coś znacznie więcej - świadczy o świadomym podejściu firmy do ryzyk związanych z bezpieczeństwem

Zalety szkolenia:

- Uświadomisz sobie kompetencje miękkie pozwalające na biznesowe wytłumaczenie technicznych ryzyk

- Dowiesz się jak aplikacje i systemy postrzegają testerzy bezpieczeństwa
- Uświadomisz sobie, że pewne decyzje architektoniczne podejmowane na wczesnych etapach mają wpływ na koszt łatania potencjalnych podatności
- Poznasz różne podejścia do modelowania zagrożeń - a przede wszystkim jak je zastosować w praktyce
- Nauczysz się technik rozmowy o bezpieczeństwie systemu w taki sposób, żeby zrozumiał je zarząd

BOTTEGA IT minds

Szczegółowy program:

1. Wstęp do modelowania zagrożeń

- 1.1. Skutki projektowania aplikacji i systemów bez wymagań bezpieczeństwa
- 1.2. Korzyści płynące z modelowania zagrożeń
- 1.3. Metodologie modelowania zagrożeń - ich wady i zalety

2. Wdrażanie modelowania zagrożeń w SDLC

- 2.1. Jak wdrożyć program modelowania zagrożeń?
- 2.2. Jak przekonać do tego zarząd?
- 2.3. Ile czasu zajmuje modelowanie zagrożeń?

3. Przykładowe modelowanie zagrożeń

- 3.1. Określanie potencjalnych atakujących - ćwiczenie
- 3.2. Definiowanie kluczowych zasobów - ćwiczenie
- 3.3. Podejście abuser stories - ćwiczenie
- 3.4. Definiowanie wymagań bezpieczeństwa na podstawie zagrożeń - ćwiczenie
- 3.5. Definiowanie przypadków testowych na podstawie wymagań - ćwiczenie

4. Optymalizacja zadań

- 4.1. Bazowe modele zagrożeń - wprowadzenie
- 4.2. Dobieranie bazowych modeli zagrożeń dla danego rozwiązania - ćwiczenie
- 4.3. Definiowanie bazowego modelu zagrożeń - ćwiczenie
- 4.4. Automatyzacja przypadków testowych

5. Procesowanie wyników

- 5.1. Sposób zapisywania zagrożeń - PDF, diagramy UML/DFD, Jira
- 5.2. Podejmowanie decyzji dla zagrożeń i projektowanie akcji

6. Sesja modelowania zagrożeń

BOTTEGA IT minds

6.1. Pełna sesja modelowania zagrożeń małej aplikacji korzystającej z prostego serwera i bazy danych - ćwiczenie

6.2. Dyskusja na temat typowych pułapek - ograniczenia czasowe, problematyczni dyskutanci

7. Podsumowanie i dyskusja

7.1. Podsumowanie wiedzy i technik modelowania zagrożeń

7.2. Dyskusja z ekspertem