Modelowanie Zagrożeń w Praktyce

Odbiorcy: Programiści, Architekci, Projektanci, Testerzy, Administratorzy, DevOps, Bezpiecznicy
Forma: Warsztat (70% praktyki, 30% teorii)
Czas trwania: 1-2 dni
Wymagania: Laptop, tablica

Przewidywanie i rozwiązywanie problemów bezpieczeństwa przed ich powstaniem znacząco zmniejsza koszt związany z utrzymaniem systemu IT. Celem tego szkolenia jest nauczenie Twojego zespołu procesu modelowania zagrożeń, czyli identyfikacji problemów bezpieczeństwa na etapie projektowania po to, aby uniknąć ich na etapie implementacji oraz potwierdzić ich brak w fazie weryfikacji.

Agenda

1. Bezpieczeństwo w procesie wytwórczym (Secure SDLC, SSDLC)
1.1. Zarządzanie bezpieczeństwem aplikacji
1.2. Zarządzanie podatnościami
1.3. Budowanie wymagań bezpieczeństwa
1.4. Sposoby oceny bezpieczeństwa systemów IT
2. Modelowanie zagrożeń: teoria
2.1. Poziomy modelowania zagrożeń
2.2. Podejście oparte o Attack Trees
2.3. Podejście oparte o model STRIDE
2.4. Rozszerzenie modelu STRIDE o model TRIM
2.5. Metodyka Agile Threat Modeling
2.6. Przegląd dostępnych narzędzi (TMT, Deciduous, Elevation of Privilege & Privacy, Cornucopia i inne)
3. Modelowanie zagrożeń: praktyka
3.1. Modelowanie zagrożeń na poziomie infrastruktury - ćwiczenia
3.2. Modelowanie zagrożeń na poziomie aplikacji - ćwiczenia

3.3. Modelowanie zagrożeń na poziomie konkretnej funkcjonalności - ćwiczenia
3.4. *Modelowanie zagrożeń na przypadkach klienta - ćwiczenia

*** Tylko w przypadku wariantu 2-dniowego. W tym wariancie drugi dzień poświęcony jest w większości na zajęcia praktyczne pod kątem realnych systemów, aplikacji i funkcjonalności klienta. Wypadkowe modele zagrożeń wnoszą dodatkową wartość dla klienta.**