BO·TT·EGA
IT minds

Program szkolenia:

Praktyczne Bezpieczeństwo AWS

Informacje:

Nazwa:	**Praktyczne Bezpieczeństwo AWS**
Kod:	**sec-AWS**
Kategoria:	AWS
Odbiorcy:	DevOps, admini, architekci, developerzy
Czas trwania:	2 dni
Forma:	30% wykładów, 70% warsztatów

Rosnąca liczba włamań do środowisk chmurowych pokazuje, że zabezpieczenie danych oraz zasobów w chmurze wymaga odpowiednich kompetencji. Oferujemy szkolenie dla zespołów projektowych dedykowane bezpieczeństwu AWS.

Główne cele szkolenia Praktyczne Bezpieczeństwo AWS są następujące:

- dostarczyć dogłębne zrozumienie aspektów bezpieczeństwa w kontekście AWS
- pokazać popularne błędy oraz ich konsekwencje
- nauczyć, jak krok po kroku wykonywać testy bezpieczeństwa chmury
- dać instrukcje jak logować i monitorować potencjalne incydenty bezpieczeństwa
- zapewnić świetną zabawę podczas laboratoriów opartych o historię, w której wcielisz się w rolę specjalisty zabezpieczającego firmę E-Corp przed atakiem grupy hakerów fsociety

Szkolenie jest dedykowane wszystkim osobom, pracującym z technologią AWS, w tym deweloperów, administratorów i specjalistów ds. bezpieczeństwa.

Zalety szkolenia:

- Szkolenie skupione na praktycznych aspektach bezpieczeństwa AWS, czyli na tym, jak rozwiązywać konkretne problemy przy pomocy narzędzi AWS oraz open-source
- Wszystkie warsztaty prowadzone są na specjalnie przygotowanym do tego środowisku dostępnego z poziomu przeglądarki
- Dla uatrakcyjnienia nauki, scenariusze warsztatów oparte są o historię, w której to uczestnicy zabezpieczają infrastrukturę firmy E-Corp przed atakami grupy hakerów fsociety

BOTTEGA IT minds

Szczegółowy program:

1. Wprowadzenie

1.1. założenia i cele szkolenia

1.2. komunikacja z usługami AWS poprzez CLI

2. Podstawy bezpieczeństwa w AWS

2.1. model współodpowiedzialności

2.2. planowanie ciągłości działania

3. IAM

3.1. zrozumienie wszystkich typów polityk oraz jak one ze sobą współdziałają

3.2. różne podejście do zarządzania uprawnieniami

3.3. analiza popularnych błędów

4. Bezpieczeństwo S3

4.1. analiza potencjalnych zagrożeń

4.2. wbudowane mechanizmy bezpieczeństwa

4.3. wdrożenie najlepszych praktyk bezpieczeństwa

5. Bezpieczeństwo aplikacji

5.1. zagrożenia w aplikacjach w chmurze,

5.2. zabezpieczanie infrastruktury aplikacji

6. Bezpieczeństwo danych

6.1. szyfrowanie danych "w spoczynku" oraz danych "w przepływie"

7. Logowanie i monitorowanie

7.1. usługi odpowiedzialne za logowanie i monitorowanie

7.2. analiza logów

8. Audyt infrastruktury AWS

8.1. proces audytu infrastruktury AWS

8.2. narzędzia open-source do wyszukiwania błędów bezpieczeństwa

8.3. przeprowadzenie audytu bezpieczeństwa w formie ćwiczenia CTF