kod szkolenia: GH-500 / PL DL 1d

GitHub Advanced Security

Szkolenie pokazuje, jak wykorzystać GitHub Advanced Security do wcześniejszego wykrywania podatności, ujawnionych sekretów i zagrożeń wynikających z zależności.

Uczestnicy poznają najważniejsze funkcje GHAS, w tym skanowanie kodu, skanowanie sekretów, Dependabot oraz CodeQL. Dowiedzą się również, jak konfigurować mechanizmy bezpieczeństwa, zarządzać alertami i dostępem, tworzyć polityki oraz włączać ochronę kodu do codziennego procesu wytwarzania oprogramowania.

Odbiorcy szkolenia

Szkolenie jest przeznaczone dla osób odpowiedzialnych za bezpieczeństwo kodu, repozytoriów i procesów wytwarzania oprogramowania, które chcą praktycznie wykorzystywać GitHub Advanced Security.
W szczególności szkolenie jest skierowane do:

- specjalistów ds. bezpieczeństwa,
- programistów,
- inżynierów DevSecOps i DevOps,
- administratorów GitHub,
- specjalistów IT odpowiedzialnych za bezpieczeństwo środowisk programistycznych,
- osób wdrażających polityki i mechanizmy ochrony kodu,
- osób przygotowujących się do certyfikacji GitHub Advanced Security.

Korzyści

- GitHub Advanced Security – poznasz najważniejsze funkcje GHAS i dowiesz się, jak wykorzystywać je do ochrony kodu i repozytoriów.
- Wykrywanie ujawnionych sekretów – nauczysz się konfigurować skanowanie sekretów i reagować na

przypadki ujawnienia danych wrażliwych.
- Skanowanie podatności w kodzie – poznasz sposoby konfigurowania skanowania kodu i analizowania wykrytych problemów bezpieczeństwa.
- Analiza kodu z CodeQL – dowiesz się, jak CodeQL identyfikuje podatności oraz jak dostosowywać zapytania i przepływy skanowania.
- Bezpieczeństwo zależności z Dependabot – nauczysz się korzystać z alertów, aktualizacji bezpieczeństwa i przeglądu zależności.
- Administracja i zarządzanie GHAS – poznasz zasady włączania funkcji, zarządzania dostępem, alertami i konfiguracją zabezpieczeń.
- Polityki i reguły bezpieczeństwa – nauczysz się tworzyć zestawy reguł repozytoriów, zarządzać danymi wrażliwymi i wzmacniać standardy bezpieczeństwa w organizacji.

Program szkolenia

1. Wprowadzenie do GitHub Advanced Security
   - Wprowadzenie
   - Definicja GHAS i znaczenie jego integralnych funkcji
   - Jak wykorzystać GHAS, aby uzyskać największy wpływ
   - Zrozumienie GHAS i jego roli w ekosystemie bezpieczeństwa
2. Konfiguracja aktualizacji bezpieczeństwa Dependabot w repozytorium GitHub
   - Wprowadzenie
   - Zarządzanie zależnościami w GitHub
   - Alerty Dependabot
   - Aktualizacje bezpieczeństwa Dependabot
   - Zarządzanie powiadomieniami i raportami Dependabot
   - Przegląd zależności
   - Ćwiczenie – Konfiguracja aktualizacji bezpieczeństwa Dependabot
3. Konfiguracja i używanie skanowania sekretów w repozytorium GitHub
   - Wprowadzenie
   - Czym jest skanowanie sekretów?
   - Konfiguracja skanowania sekretów
   - Używanie skanowania sekretów
   - Ćwiczenie – Wprowadzenie do skanowania sekretów
4. Konfiguracja skanowania kodu w GitHub
   - Wprowadzenie
   - Czym jest skanowanie kodu?
   - Włączanie skanowania kodu z narzędziami innych firm
   - Konfiguracja skanowania kodu
   - Ćwiczenie – Konfiguracja skanowania kodu

5. Identyfikacja luk w zabezpieczeniach w kodzie przy użyciu CodeQL
   - Wprowadzenie
   - Przygotowanie bazy danych dla CodeQL
   - Uruchamianie CodeQL w bazie danych
   - Zrozumienie wyników CodeQL
   - Rozwiązywanie problemów z wynikami CodeQL
6. Skanowanie kodu z GitHub CodeQL
   - Wprowadzenie
   - Czym jest CodeQL?
   - Jak CodeQL analizuje kod?
   - Czym jest QL?
   - Skanowanie kodu i CodeQL
   - Dostosowywanie przepływu pracy skanowania kodu z CodeQL – Część 1
   - Ćwiczenie – Odniesienie do zapytania CodeQL
   - Dostosowywanie przepływu pracy skanowania kodu z CodeQL – Część 2
   - Używanie CodeQL CLI
   - Dostosowywanie języków i kompilacji do skanowania kodu
   - Ćwiczenie – Konfiguracja macierzy języków CodeQL
7. Administracja GitHub dla GitHub Advanced Security
   - Wprowadzenie
   - Czym jest GitHub Advanced Security?
   - Włączanie GitHub Advanced Security
   - Zarządzanie dostępem do GitHub Advanced Security
   - Zarządzanie funkcjami i alertami GitHub Advanced Security
8. Zarządzanie danymi wrażliwymi i politykami bezpieczeństwa w GitHub
   - Wprowadzenie
   - Ustawianie polityk bezpieczeństwa
   - Tworzenie i zarządzanie zestawami reguł repozytorium
   - Raportowanie i rejestrowanie
   - Ćwiczenie – Usuwanie commita z historii git

Oczekiwane przygotowanie uczestnika

- uczestnik musi posiadać założone konto na GitHub
- Doświadczenie w używaniu i administrowaniu repozytoriami GitHub
- Doświadczenie w pracy z usługami Microsoft Azure
- Umiejętności techniczne w zakresie skanowania kodu, zarządzania zależnościami i skanowania sekretów
- Znajomość narzędzi takich jak CodeQL i Dependabot

- Średniozaawansowana znajomość funkcji i możliwości Git i GitHub

Dla zwiększenia komfortu pracy oraz efektywności szkolenia zalecamy skorzystanie z dodatkowego ekranu. Brak dodatkowego ekranu nie jest przeciwwskazaniem do udziału w szkoleniu, ale w znaczący sposób wpływa na komfort pracy podczas zajęć
Informacje oraz wymagania dotyczące uczestniczenia w szkoleniach w formule zdalnej dostępne na: https://www.altkomakademia.pl/jak-dzialamy/o-szkoleniach/?distance-learning

Szkolenie obejmuje

* podręcznik w formie elektronicznej dostępny na platformie: https://learn.microsoft.com/pl-pl/training/
* dostęp do portalu słuchacza Altkom Akademii

Produkt zawiera:

- Wykład (60%)
- ćwiczenia (40%)

Język

- Szkolenie: polski
- Materiały: angielski

Metoda egzaminacyjna

Egzamin w formie on-line. Zapis na stronie https://home.pearsonvue.com/Clients/Microsoft.aspx

Czas trwania

1 dni / 7 godzin

Opis egzaminu

GitHub Advanced Security

Exam

URL:https://learn.microsoft.com/en-us/credentials/certifications/github-advanced-security/?practice-assessment-type=certification