kod szkolenia: GH-500 / PL DL 1d

GitHub Advanced Security

Szkolenie zapewnia kompleksowy przegląd GitHub Advanced Security (GHAS), koncentrując się na jego integralnych funkcjach, takich jak skanowanie sekretów, skanowanie kodu i Dependabot. Obejmuje kluczowe aspekty wdrażania i zarządzania środkami bezpieczeństwa w organizacjach, podkreślając rolę GHAS w identyfikowaniu i łagodzeniu luk w zabezpieczeniach na wczesnym etapie cyklu życia oprogramowania. Kurs jest autoryzowany przez Microsoft.

Odbiorcy szkolenia

- Specjaliści ds. bezpieczeństwa odpowiedzialni za wdrażanie i zarządzanie środkami bezpieczeństwa w swojej organizacji
- Programiści chcący pogłębić swoją wiedzę na temat zaawansowanych funkcji bezpieczeństwa w GitHub
- Specjaliści IT, którzy chcą efektywnie wykorzystywać GitHub Advanced Security do zwiększenia bezpieczeństwa kodu i procesu rozwoju
- Osoby przygotowujące się do certyfikacji GitHub Advanced Security

Korzyści

- Kompleksowa wiedza o bezpieczeństwie – Zdobędziesz głębokie zrozumienie funkcji GitHub Advanced Security i ich praktycznego zastosowania
- Ulepszone wykrywanie podatności – Nauczysz się efektywnie wykorzystywać skanowanie sekretów, skanowanie kodu i Dependabot do wczesnego wykrywania problemów bezpieczeństwa
- Praktyczne wdrażanie zabezpieczeń – Poprzez ćwiczenia praktyczne zdobędziesz doświadczenie w konfigurowaniu i zarządzaniu funkcjami bezpieczeństwa.
- Zastosowanie w praktyce – Poznasz najlepsze praktyki i przepływy pracy, które można natychmiast zastosować w celu poprawy poziomu bezpieczeństwa 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

- 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

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