Szkolenie: Microsoft
# GH-500T00: GitHub Advanced Security

Gold Microsoft Partner

## DOSTĘPNE TERMINY

2025-11-14 | 1 dzień | Kraków / Wirtualna sala
2025-12-12 | 1 dzień | Warszawa / Wirtualna sala

## Cel szkolenia:

Kurs "GH-500T00: GitHub Advanced Security" oferuje dogłębną eksplorację funkcji bezpieczeństwa GitHub, w tym skanowania sekretów, skanowania kodu za pomocą CodeQL oraz zarządzania zależnościami. Uczestnicy nauczą się konfigurować i wykorzystywać te narzędzia, aby zwiększyć bezpieczeństwo swojego oprogramowania. Kurs GH-500 obejmuje również aspekty administracyjne, takie jak ustalanie polityk bezpieczeństwa i zarządzanie danymi wrażliwymi w GitHub.

Cele kursu GitHub Advanced Security – GH-500

- Zrozumieć i skonfigurować funkcje GitHub Advanced Security.
- Wdrożyć Dependabot do automatycznych aktualizacji zależności.
- Skonfigurować i zarządzać skanowaniem sekretów w celu ochrony informacji wrażliwych.
- Skonfigurować skanowanie kodu za pomocą CodeQL do wykrywania podatności.
- Analizować i interpretować wyniki skanowania CodeQL.
- Administrować politykami bezpieczeństwa i zarządzać danymi wrażliwymi w GitHub**.**

## Plan szkolenia:

- Wprowadzenie do GitHub Advanced Security
  - Definiowanie GHAS i znaczenie integralnych funkcji, takich jak skanowanie sekretów, skanowanie kodu i Dependabot
  - Wiedza, jak wykorzystać GHAS, aby zmaksymalizować wpływ na bezpieczeństwo
  - Zrozumienie GHAS i jego roli w ekosystemie bezpieczeństwa
  - Konfiguracja aktualizacji bezpieczeństwa Dependabot w repozytorium GitHub
  - Opis dostępnych narzędzi do zarządzania podatnymi zależnościami w GitHub
  - Włączanie i konfigurowanie alertów Dependabot



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

    - Identyfikacja uprawnień i ról wymaganych do przeglądania i włączania alertów Dependabot
    - Włączanie i konfigurowanie aktualizacji bezpieczeństwa Dependabot
    - Identyfikacja, przegląd i rozwiązywanie podatnych zależności
    - Wyjaśnienie, jak używać GraphQL API do pobierania informacji o podatnościach
    - Wyjaśnienie, jak konfigurować powiadomienia o podatnościach
    - Laboratorium: Konfiguracja aktualizacji bezpieczeństwa Dependabot
- Konfiguracja i używanie skanowania sekretów w repozytorium GitHub
    - Opis skanowania sekretów
    - Konfiguracja skanowania sekretów
    - Używanie skanowania sekretów
- Konfiguracja skanowania kodu na GitHub
    - Opis skanowania kodu
    - Lista kroków umożliwiających włączenie skanowania kodu w repozytorium
    - Lista kroków umożliwiających włączenie skanowania kodu za pomocą analizy zewnętrznej
    - Kontrastowanie implementacji analizy CodeQL w przepływie pracy GitHub Actions w porównaniu do narzędzia CI zewnętrznego
    - Wyjaśnienie, jak skonfigurować skanowanie kodu w repozytorium za pomocą zdarzeń wyzwalających
    - Kontrastowanie częstotliwości przepływów pracy skanowania kodu (zaplanowane vs wyzwalane przez zdarzenia)
- Identyfikacja podatności bezpieczeństwa w kodzie za pomocą CodeQL
    - Tworzenie bazy danych za pomocą CodeQL w celu wyodrębnienia pojedynczej reprezentacji relacyjnej każdego pliku źródłowego w kodzie
    - Uruchamianie CodeQL w bazie danych w celu znalezienia problemów w kodzie źródłowym i potencjalnych podatności bezpieczeństwa
    - Zrozumienie wyników skanowania CodeQL za pomocą zapytań stworzonych przez GitHub lub własnych zapytań niestandardowych
- Skanowanie kodu za pomocą GitHub CodeQL
    - Zrozumienie CodeQL i jak analizuje kod
    - Zrozumienie QL, unikalnego języka programowania logicznego
    - Konfiguracja skanowania kodu opartego na CodeQL w repozytorium GitHub
    - Odwoływanie się do niestandardowego zapytania CodeQL
    - Konfiguracja macierzy językowej w przepływie pracy CodeQL
    - Nauka korzystania z CodeQL CLI do generowania wyników skanowania kodu i przesyłania ich do GitHub
    - Implementacja niestandardowych kroków budowania
    - Laboratorium: Odwoływanie się do zapytania CodeQL



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Laboratorium: Konfiguracja macierzy językowej CodeQL
- Administracja GitHub dla GitHub Advanced Security
  - Zrozumienie, czym jest GitHub Advanced Security i jak go używać w cyklu życia oprogramowania
  - Identyfikacja, które funkcje GitHub Advanced Security są dostępne dla projektów open-source, a które dla produktów enterprise
  - Włączanie różnych funkcji GitHub Advanced Security na różnych produktach enterprise
  - Określenie, kto powinien mieć dostęp do funkcji GitHub Advanced Security w organizacji i przyznawanie odpowiednich uprawnień
  - Ustalanie polityk bezpieczeństwa na poziomie organizacji i repozytorium
  - Zrozumienie, jak reagować na alert bezpieczeństwa
  - Korzystanie z Security Overview do monitorowania alertów bezpieczeństwa
  - Korzystanie z punktów końcowych API GitHub Advanced Security do zarządzania funkcjami i alertami GitHub Advanced Security
  - Zarządzanie danymi wrażliwymi i politykami bezpieczeństwa w GitHub
  - Tworzenie dokumentacji zawierającej wytyczne dotyczące bezpieczeństwa i przydatne informacje dla współpracowników
  - Ustalanie uprawnień i innych zasad
  - Automatyzacja procesów zapobiegających naruszeniom bezpieczeństwa
  - Reagowanie na naruszenia bezpieczeństwa

## Wymagania:

- Podstawowa znajomość programowania: Uczestnicy powinni mieć podstawowe umiejętności programowania w dowolnym języku, aby móc efektywnie korzystać z funkcji GitHub Advanced Security.
- Podstawowa znajomość systemów kontroli wersji: Wskazane jest, aby uczestnicy mieli podstawową wiedzę na temat systemów kontroli wersji, takich jak Git, aby lepiej zrozumieć i wykorzystać funkcje kursu.

## Poziom trudności

## Certyfikaty:

Certyfikat ukończenia autoryzowanego kursu Microsoft.



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

## Prowadzący:

Microsoft Certified Trainer.



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001