

CYBER, BEZPIECZEŃSTWO W SMARTCITY



BEZPIECZNE PLANOWANIE I PROJEKTOWANIE

- Stosowanie zasady najmniejszych uprawnień
- Wymuszanie uwierzytelniania wieloskładnikowego
- Wdrożenie architektury zerowego zaufania
- Zarządzanie zmianami ryzyka związanego z architekturą wewnętrzną
- Bezpieczne zarządzanie zasobami inteligentnego miasta
- Ochrona usług internetowych
- Terminowe instalowanie aktualizacji systemów i aplikacji
- Analiza zagrożeń prawnych, bezpieczeństwa i prywatności związanych z wdrożeniami

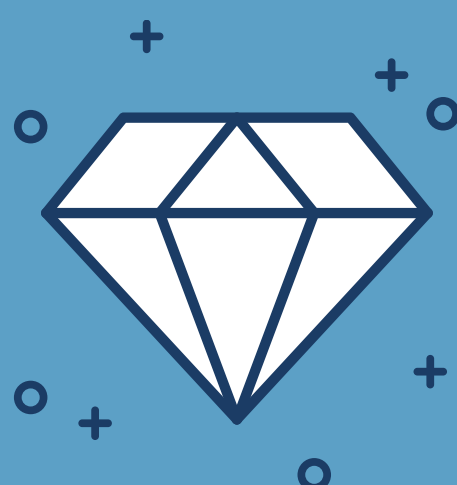


PROAKTYWNE ZARZĄDZANIE RYZYKIEM W ŁAŃCUCHU DOSTAW

- Łańcuch dostaw oprogramowania
- Łańcuch dostaw sprzętu i urządzeń IoT
- Dostawcy usług zarządzanych i dostawcy usług w chmurze

ODPORNÓŚĆ OPERACYJNA

- Tworzenie kopii zapasowych systemów i danych
- Przeprowadzanie szkoleń pracowników
- Opracowanie i ćwiczenie planów reagowania na incydenty i odzyskiwania danych



ŹRÓDŁO: CYBERSECURITY BEST PRACTICES
FOR SMART CITIES, WWW.CISA.GOV, 2023

AUTOR: JOANNA WZIĄTEK

Czytaj więcej na
www.purecybersec.pl