|  |  |
| --- | --- |
| **Detekcja i monitorowanie zagrożeń** | |
| Zespół: | Damian Linek  Wojciech Minner |
| Grupa: | 1IZ22B |
| **Projekt** | |

**Wybrana organizacja: Służba Ochrony Zdrowia**

**Koncept**

Zidentyfikowanie zagrożeń cybernetycznych, które mogą stanowić ryzyko dla bezpieczeństwa pacjentów i funkcjonowania infrastruktury IT. Wskazanie potencjalnie słabych punktów systemu, znalezienie potencjalnych wektorów ataków które mogło by być użyte do realizacji ataku, a następnie zasugerowanie działań zabezpieczających przed takim atakiem.

**Plan pracy Projektowej**

1. Wybranie informacji które mamy analizować.
2. Wypisanie krytycznych zasobów IT (np. serwery, bazy danych)

Analiza architektury sieciowej.

1. Wykorzystanie platformy MITRE ATT&CK do stworzenia modelu zagrożeń.
2. Określenie środków zapobiegawczych