securITum

CERTYFIKAT

UCZESTNICTWA

POZNAJ BEZPIECZEŃSTWO WINDOWS

CZĘŚĆ 1

USŁUGI SYSTEMOWE

Tomasz Nienałtowski

TRENER Grzegorz Tworek | **DATA** 20.03.2023 | **CZAS TRWANIA** 3 GODZINY

AGENDA

- Idea usług (serwisów) systemowych
- Architektura
  - Service Manager
  - Baza danych
  - Komunikacja sieciowa
  - Komunikacja z usługami
  - Uprawnienia
- Usługi oparte o svchost
- Procesy chronione
- Usługi uruchamiane przez ETW i WNF
- Blokowanie komunikacji sieciowej
- Ukrywanie usług przed administratorami
- Wykrywanie ukrytych usług
- Wykrywanie niebezpiecznych uprawnień do usług
- Wykrywanie niebezpiecznych uprawnień do bazy danych
- Wykrywanie niebezpiecznych uprawnień do binariów
- Wykrywanie niechcianych binariów
- Przykładowa złośliwa usługa. Projekt, kod, implementacja

sekurak.pl