SEKURAK.ACADEMY

CERTYFIKAT

UCZESTNICTWA W SZKOLENIU SEKURAK.ACADEMY 2024

MIAŁEM INCYDENT!
ANALIZA POWŁAMANIOWA W WINDOWSIE

2024 — semestr_02

DLA:

Rafał Szponarski

DATA: 4.11.2024 r. **TRENER:** Tomasz Turba **CZAS TRWANIA:** 3 godziny

AGENDA

1. Przygotowanie „pola bitwy" – pokazy praktyczne:
   - Wykonanie ataków na infrastrukturę:
     - *brute-force*
     - MiTM
     - eksploit
2. Wprowadzenie do analizy incydentów bezpieczeństwa:
   - Omówienie faz Cyber Kill Chain i zagrożenia APT
   - Potencjalne architektury dla monitoringu i reagowania na incydenty
   - Zabezpieczanie materiałów, normy, procedury, dokumentacja
   - Monitoring ruchu sieciowego (logi i onelinery)
3. Techniki analizy powłamaniowej – pokazy praktyczne:
   - Analiza hosta i obrazu dysku twardego:
     - pokaz narzędzi wspierających poza systemowymi
   - Analiza pamięci ulotnej RAM:
     - wykorzystanie Volatility + narzędzi wspierających
   - Analiza ruchu sieciowego na podstawie zrzutu PCAP:
     - wykrywanie stealera z SSL
     - wykrywanie malware'u
   - Analiza dużych porcji danych – logów:
     - narzędzia a rzeczywistość
4. Dobre rady administratora w formie sesji Q&A

PUNKTY CPE/ECE: 3

SZKOLENIA.SECURITUM.PL

securitum