Ministerstwo Cyfryzacji

PWCyber

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Departament Cyberbezpieczeństwa

SZKOLENIE ONLINE DLA PODMIOTÓW KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

12 grudnia 2024 r.
Typ 300
Sztuczna Inteligencja w SIEM i SOAR: Nowe Podejście do identyfikacji Cyberzagrożeń
Energy Logserver (EMCA Software)

9.45 – 10.00	**Logowanie**
10.00 – 10.05	**Zasady organizacyjne przebiegu szkolenia** *Przedstawiciel Departamentu Cyberbezpieczeństwa MC*
10.05 – 10:30	**Sztuczna Inteligencja w SIEM i SOAR** • Przedstawienie środowiska pracy w koncepcji Energy SIEM oraz Energy Logserver • Omówienie źródeł danych i typów wiadomości logowania • Wyzwania stojące przed SOC w obszarze identyfikacji zagrożeń • Gdzie AI może pomóc? *Artur Bicki Energy Logserver*
10.30 – 11:00	**Sztuczna Inteligencja w SIEM i SOAR** • Zastosowanie metod AI w praktyce • Detekcja anomalii w logach tekstowych syslog serwerów i aplikacji • Detekcja anomalii w logach liczbowych na bazie ruchu sieciowego • Analityka AI dla zachowań użytkownika • Automatyczna kategoryzacja zdarzeń • Związki przyczynowo-skutkowe *Artur Bicki Energy Logserver*

11.00 – 12:00	**Sztuczna Inteligencja w SIEM i SOAR** • Przetwarzanie wsadowe oraz w czasie rzeczywistym • Połączenie alertowania w decyzjami AI • Współpraca AI z SOAR, rozpoznanie incydentu • Wzbogacanie wiedzy o incydencie • Praca z incydentem • Automatyzacja workflow, bloki moduły • Reakcje SOAR na incydent AI • Zaawansowane procesy obsługi *Artur Bicki Energy Logserver*
12.00 – 12.10	**Sesja pytań i odpowiedzi do ekspertów**