Ministerstwo Cyfryzacji

PWCyber

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Departament Cyberbezpieczeństwa

SZKOLENIE ONLINE DLA PODMIOTÓW KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

3 grudnia 2025 r.
Typ 300
Automatyzacja i orkiestracja reakcji na incydenty (SOAR)
Fortinet

9.45 – 10.00	**Logowanie**
10.00 – 10.05	**Zasady organizacyjne przebiegu szkolenia** *Przedstawiciel Departamentu Cyberbezpieczeństwa MC*
10.05 – 12.00	**Automatyzacja i orkiestracja reakcji na incydenty (SOAR)** 1. Wprowadzenie do narzędzia SOAR a. Wprowadzenie do tematyki SOAR: czym jest automatyzacja i orkiestracja reakcji na incydenty, znaczenie dla bezpieczeństwa IT b. Krótkie omówienie wyzwań zespołów SOC bez automatyzacji 2. Kluczowe funkcje SOAR a. Automatyczne importowanie i klasyfikacja incydentów b. Korzyści orkiestracji i integracji z różnymi systemami bezpieczeństwa (SIEM, EDR, zdarzenia losowe) c. Przykłady gotowych scenariuszy (playbook'ów) reakcji na różne zdarzenia 3. Demonstracja a. Pokaz działania automatycznych procedur (playbook'ów) na incydentach b. Omówienie efektów: skrócenie czasu reakcji, zwiększenie efektywności zespołu 4. Zaawansowane możliwości i trendy a. Wykorzystanie sztucznej inteligencji i uczenia maszynowego w SOAR b. Integracja z Threat Intelligence 5. Wyzwania wdrożeniowe i ROI a. Typowe problemy podczas implementacji b. Metryki sukcesu i zwrot z inwestycji c. Rekomendacje dla organizacji planujących wdrożenie 6. Podsumowanie a. Kluczowe wnioski i rekomendacje dot. SOAR b. Informacje o materiałach dodatkowych i szkoleniach Ekspert Fortinet: Grzegorz Cebula
12.00 – 12.10	**Sesja pytań i odpowiedzi do ekspertów**