

AGENDA

16.06.2024

- Przyjazd w godz. 15.00 - 18.00 - dla chętnych
- 19.30 - kolacja integracyjna w restauracji w formie bufetu

17.06.2024

- 08.30-09.30 – śniadanie
- 9:30 - **Sesja I: Tenable - Nowoczesne podejście do zarządzania ryzykiem**
- Portfolio Tenable: Przegląd kompleksowych rozwiązań zapewniających pełną ochronę Twojej infrastruktury.
- Tenable Attack Surface Management: Poznaj narzędzia i strategię identyfikacji oraz minimalizacji zewnętrznej powierzchni ataku.
- Przerwa kawowa
- Tenable Web Application Scanner: Dowiedz się, jak skutecznie analizować aplikacje webowe w celu wykrywania luk w zabezpieczeniach.
- Tenable Security Center: Klasyczne zarządzanie podatnościami "on-premise"
- 13:00-14:00 - Obiad
- 14:00 - **Sesja II: Tenable - Chmura i Tożsamość**
- Tenable Cloud Security: Odkryj strategię i narzędzia zapewniające bezpieczeństwo Twojej infrastruktury chmurowej.
- Przerwa kawowa
- Tenable Identity Management: Zrozum zagrożenia związane z narażeniem tożsamości/Active Directory i dowiedz się, jak się przed nimi bronić.
- 15:30 – zakończenie
- 17.00 – rejs statkiem
- 19.00 – kolacja w formie grilla

18.06.2024

- 08.30-09.30 – śniadanie
- 09.30 – 10.40 - **Po drugiej stronie decepcji. Prezentacja kilku praktycznych przypadków z perspektywy atakującego - Labyrinth**
- Wprowadzenie, definicje głównej terminologii, omówienie interakcji między komponentami
- Konfiguracja: konfiguracja Labyrinth (dodanie listy słów, honeynety itp.). Konfiguracja dwukierunkowa z integracją ze Splunk.
- Przypadki testowe
- część 1: interaktywna część. Uczestnicy wykonają ataki na przygotowane punkty i zobaczą wyniki w czasie rzeczywistym.
- 10:35 - 10:40 - Przerwa

AGENDA

10:40 - 11:20 - Przypadki testowe

- część 2: **kontynuacja badania różnych przypadków. Omówienie bardziej złożonych scenariuszy.**
- Sesja pytań i odpowiedzi
- 11.30 – 12.00 - Przerwa
- 12.00 – 15.00 - **Rodzina Energy**
- Koncepcja kontroli infrastruktury w rodzinie produktów Energy Logserver / Soar / Monitor
- Energy Logserver quick lab
 - praktyczne zapoznanie się z platformą
 - praca z danymi
 - wizualizacje, zadania search, alerty
- Zastosowania Energy Logserver w bezpieczeństwie i nadzorze
 - Typowe realizacje SIEM
- Przerwa kawowa
- Analityka i ocena bezpieczeństwa ruchu sieciowego
- Przerwa kawowa
- Omówienie projektów niestandardowych i innowacyjnych w Energy Logserver
 - Helicopter View
 - CMDB
 - Splunk Connector
- Algorytmy AI zastosowane w praktyce
 - Detekcja anomalii liczbowych
 - Budowa słowników technologicznych
 - Nienadzorowane grupowanie danych
 - AI Community
- Przerwa kawowa
- SIEM i co dalej - automatyka zdarzeń w Energy SOAR
 - Sprawy i procedury
 - Integracje
 - Procesy automatyzacji
- Energy Monitor
 - Geneza
 - Cel realizacji
 - Funkcje

15.00 – 16.00 – obiad

16.00 – wyjazd z ośrodka