ACTIVE BUSINESS TRAINING
ul. Zakątek 19 D, 44-203 Rybnik
tel. +48 601 16 80 20

www.ab-training.pl
biuro@ab-training.pl

ACTIVE BUSINESS TRAINING

wiedza, innowacyjność i praktyka zarządzania

PROGRAM SZKOLENIA
„Cyberbezpieczeństwo: normy, analiza i monitoring”

dla

Sieć Badawcza Łukasiewicz - Instytut Technik Innowacyjnych EMAG

Rybnik, 28.10.2024

Dzień 1: Normy i standardy bezpieczeństwa

Sesja 1: Wprowadzenie do norm serii IEC 62443
- Opis: Omówienie historii, zakresu i celu norm IEC 62443.
- Case Study: Analiza wdrożenia IEC 62443 w fabryce produkującej komponenty elektroniczne

Sesja 2: Przegląd Standardu NIST
- Opis: Zrozumienie kluczowych elementów standardu NIST i ich znaczenia dla cyberbezpieczeństwa.
- Case Study: Porównanie wymagań NIST i IEC 62443 na przykładzie firmy telekomunikacyjnej.

Sesja 3: Znaczenie norm i standardów w praktyce
- Opis: Dyskusja na temat integracji standardów w istniejące systemy zarządzania.
- Przykład: Implementacja NIST w środowisku IT korporacyjnym.

Sesja 4: Dyskusja i studium przypadku
- Przykład: Nieudane wdrożenie standardu bezpieczeństwa i jego konsekwencje.
- Ćwiczenie: Analiza błędów i proponowanie poprawek.

Dzień 2: Systemy ochrony i monitorowania

Sesja 1: Wprowadzenie do systemów IDS i SOC
- Opis:Definicja, rodzaje oraz rola IDS i SOC w ochronie przed zagrożeniami.
- Przykład: Konfiguracja i optymalizacja IDS w średniej wielkości przedsiębiorstwie.

Sesja 2: Rola i konfiguracja systemów SIEM i SOAR
- Opis: Jak SIEM i SOAR pracują razem w celu poprawy reakcji na incydenty.
- Case Study: Wdrożenie SOAR dla automatyzacji odpowiedzi na incydenty w banku.

Sesja 3: Koncepcja zbudowania SOC w organizacji
- Opis: Praktyczne podejście do planowania, projektowania i implementacji SOC wewnątrz organizacji.
- Ćwiczenie: Projektowanie SOC dla fikcyjnej organizacji, z uwzględnieniem rozmiaru, branży i specyficznych potrzeb bezpieczeństwa.

Sesja 4: Wprowadzenie do NSM
- Opis: Jak monitoring sieci może być używany do wykrywania subtelnych anomalii.
- Przykład: Użycie NSM do identyfikacji nieautoryzowanego ruchu w sieci korporacyjnej.

Dzień 3: Polityki bezpieczeństwa i analiza ryzyka

Sesja 1: Tworzenie i wdrażanie polityk bezpieczeństwa
- Opis: Proces tworzenia efektywnych polityk bezpieczeństwa.
- Case Study: Rewizja polityk bezpieczeństwa po naruszeniu danych w firmie technologicznej.

Sesja 2: Wprowadzenie do analizy ryzyka - metodyka CIARA
- Opis: Metodyka CIARA - kompleksowe podejście do analizy ryzyka.
- Przykład: Użycie CIARA do oceny ryzyka w projekcie IT.

Sesja 3: Automatyzacja analizy ryzyka - narzędzia i techniki
- Opis: Narzędzia służące do automatyzacji analizy ryzyka.

- Ćwiczenie: Praktyczne zastosowanie narzędzi do automatyzacji w scenariuszu biznesowym.

Sesja 4: Przypadki zastosowania analizy ryzyka
- Przykład: Ocena ryzyka dla nowego produktu cyfrowego.

Dzień 4: Analiza zdarzeń i inwentaryzacja zasobów

Sesja 1: Techniki analizy różnych przypadków zdarzeń bezpieczeństwa sieci
- Opis: Różne metody analizy zdarzeń i ich zastosowanie w praktyce.
- Ćwiczenie: Analiza symulowanych zdarzeń bezpieczeństwa.

Sesja 2: Narzędzia do inwentaryzacji zasobów
- Opis: Przegląd narzędzi do inwentaryzacji i zarządzania zasobami IT.
- Przykład: Inwentaryzacja zasobów w środowisku wieloplatformowym.

Sesja 3: Ćwiczenia praktyczne z analizy zdarzeń i inwentaryzacji
- Ćwiczenie: Praktyczne zadanie polegające na wykonaniu pełnej inwentaryzacji zasobów i analizy potencjalnych luk.

Dzień 5: Protokoły przemysłowe i narzędzia do analizy

Sesja 1: Analiza protokołów przemysłowych
- Opis: Omówienie najważniejszych protokołów przemysłowych i ich zabezpieczeń.
- Case Study: Analiza luk w zabezpieczeniach protokołów przemysłowych.

Sesja 2: Wykorzystanie Wireshark do analizy ruchu sieciowego
- Opis: Podstawy pracy z Wireshark.
- Ćwiczenie: Przechwytywanie i analiza pakietów w symulowanej sieci.

Sesja 3: Zastosowanie reguł i sygnatur – Snort
- Opis: Konfiguracja i zastosowanie Snort jako systemu IDS/IPS.
- Ćwiczenie: Tworzenie własnych reguł dla Snort.

Sesja 4: Ćwiczenia praktyczne z Wireshark i Snort
- Przykład: Wykorzystanie Wireshark i Snort do identyfikacji i neutralizacji ataku DDoS.

DODATKOWE INFORMACJE

- Termin szkolenia: **18-22.11.2024**
- Lokalizacja: siedziba Zamawiającego

Z poważaniem:

dr Piotr Pinoczek

T: +48 601 16 80 20

M: piotr.pinoczek@ab-training.pl

PODPIS ZAUFANY
PIOTR
PINOCZEK
28.10.2024 09:25:54 [GMT+1]
Dokument podpisany elektronicznie
podpisem zaufanym