Szkolenie

OSINT – techniki pozyskiwania informacji

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

OSINT– Inteligentne pozyskiwanie informacji w nowej erze zagrożeń

W świecie, w którym każdy ślad cyfrowy może stać się informacją operacyjną, umiejętność wyszukiwania, analizowania i weryfikacji danych stała się kompetencją kluczową. Nowoczesny OSINT nie polega już tylko na ręcznym przeszukiwaniu internetu , dziś wymaga znajomości narzędzi, korelacji, środowisk operacyjnych, a także umiejętnego wykorzystania sztucznej inteligencji jako wsparcia analitycznego.

To szkolenie pokazuje OSINT takim, jakim naprawdę jest: połączeniem analityki, bezpieczeństwa operacyjnego, technologii i krytycznego myślenia.

Korzyści

- **Bezpieczna praca operacyjna (OPSEC)** - uczestnik uczy się chronić swoją tożsamość, przygotowywać konta operacyjne i unikać błędów spalających śledztwo.
- **Profesjonalne stanowisko OSINT** - poznaje konfigurację narzędzi, przeglądarek i środowisk pracy (Linux/VM), dzięki czemu może działać skutecznie i anonimowo.
- **Scraping, harvesting i korelacja danych** – zdobywa praktyczne umiejętności techniczne pozwalające pozyskiwać i łączyć informacje z wielu źródeł.
- **Analiza social media (SOCMINT)** - potrafi identyfikować powiązania, fałszywe konta, boty i ślady cyfrowe użytkowników.
- **Darknet bez mitów** - rozumie, jak działa TOR, jak bezpiecznie analizować dane z ukrytych sieci i jak ocenić wiarygodność znalezionych treści.
- **AI jako wsparcie analityczne** - umie wykorzystać sztuczną inteligencję do filtrowania danych, generowania hipotez i porządkowania informacji.

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

- **Praktyczna umiejętność prowadzenia mini-śledztwa** - zna cały proces: pozyskanie danych → analiza → korelacja → wnioski.
- **Gotowy zestaw narzędzi OSINT 2026** - otrzymuje listę aktualnych, sprawdzonych narzędzi i metod działania w realnych scenariuszach.
- **Zwiększenie kompetencji zawodowych** - zdobyta wiedza wzmacnia profil zawodowy związany z cyberbezpieczeństwem, IT, śledztwami i administracją.
- **Świadomość zagrożeń i dezinformacji** - potrafi rozpoznawać manipulacje, fejki i szum informacyjny.

Wymagania

Uczestnik powinien posiadać podstawową umiejętność pracy w systemach Windows lub Linux, w tym korzystania z różnych przeglądarek i ustawień prywatności. Wymagana jest orientacja w podstawowych pojęciach sieciowych, takich jak adresacja IP, DNS, VPN, proxy i routing ruchu. Przydatna jest umiejętność analizowania struktury stron internetowych, rozpoznawania elementów HTML oraz korzystania z narzędzi deweloperskich przeglądarki. Oczekuje się, że uczestnik potrafi wyszukiwać i weryfikować informacje w wielu źródłach oraz rozumie podstawy bezpieczeństwa informacji. Mile widziana jest wstępna znajomość narzędzi OSINT, takich jak wyszukiwarki niestandardowe, przeszukiwarki wycieków i podstawy pracy z danymi z social media. Dodatkowym atutem będzie swoboda w używaniu narzędzi AI jako wsparcia analitycznego, zwłaszcza do korelacji i filtrowania danych.

Program szkolenia

Moduł 1: Fundamenty bezpieczeństwa operacyjnego (OPSEC).

1. Modele zagrożeń OSINT-owca
    1. kto może nas obserwować
    2. analiza ekspozycji cyfrowej
2. OPSEC techniczny i behawioralny
    1. błędy najczęściej popełniane przez początkujących
    2. jak „przecieki informacyjne” psują śledztwo
3. Konta operacyjne
    1. separacja środowisk
    2. tworzenie, utrzymywanie, „starzenie” kont
    3. zarządzanie tożsamością

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

4. Przeglądarki i izolacja
    1. Firefox hardened, LibreWolf, Mullvad Browser
    2. fingerprinting → jak go minimalizować

Moduł 2: Przygotowanie stanowiska OSINT. Kompletna konfiguracja narzędziowa.

1. Środowiska pracy
    1. systemy: Linux (preferowany), Windows z izolacją (VM)
    2. VM vs Bare metal vs Live USB
2. Narzędzia bazowe
    1. przeglądarki hardened
    2. VPN vs proxy vs TOR → bez mitów
    3. rozszerzenia ochronne
3. Agregacja i organizacja danych
    1. sposób gromadzenia: Obsidian / Notion / lokale bazy danych
    2. standardy nazewnictwa artefaktów OSINT

Moduł 3: Narzędzia OSINT klasyczne + AI jako wsparcie

AI nie zastępuje OSINT - AI przyspiesza jego etapy: filtrowanie, korelacja, analiza.

1. Scraping i harvesting - legalne techniki
    1. scraper-box narzędzia GUI
    2. monitoring zmian stron
2. Korelacja danych
    1. Maltego (case study)
    2. SpiderFoot
    3. Gathid / OpenCTI (light overview)
3. Rola AI w korelacji i analizie
    1. wykrywanie sprzeczności
    2. tworzenie hipotez śledczych
    3. porządkowanie danych, redukcja szumu

Moduł 4: Media społecznościowe (SOCMINT) oraz automatyzacja

1. Analiza profili
    1. taktyki identyfikacji użytkownika
    2. łączenie kont poprzez metadane

2. Narzędzia do harvestingu danych
    1. OSINTTools, WhatsMyName, Sherlock
    2. Geolokalizacja treści (analizy zdjęć, wideo)
3. AI do wspomagania SOCMINT
    1. generowanie hipotez po przeglądzie profilu
    2. wyszukiwanie wzorców zachowań

Moduł 5: Darknet OSINT (bez mitów)

1. Czym darknet NIE jest (najczęstsze mity)
2. TOR architektura, limity, błędy 90% użytkowników
3. Jak znaleźć rzeczy, które „nie są w Google”
    1. katalogi, wyszukiwarki TOR
    2. fora, wycieki danych
4. Analiza informacji z darknetu
    1. jak odróżnić realny dump od fejku
    2. korelacja z surface web
5. AI w darknet OSINT
    1. klasyfikacja treści
    2. filtrowanie szumu informacyjnego
    3. pomoc przy analizie językowej (slangi, szyfry, akronimy)

Moduł 6: Praktyczne mini case study 2025/2026

Uczestnicy dostają: dane, wpisy, zdjęcia, listingi. Twoje zadanie: krok po kroku. Przykładowe scenariusze:

1. Fake profil + korelacja
2. Identyfikacja sprzedawcy na darknetowym forum (bez wchodzenia w nielegalne treści)
3. Ustalenie powiązań między dwoma kontami na IG/TikTok

Tagi:

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.