

# OSINT – czyli co internet wie o Tobie

0 mnie



Security Architect



Consultant



Microsoft Certified Trainer



AI & Cybersecurity Practitioner



Developer



Freelancer



Azure @ ❤️



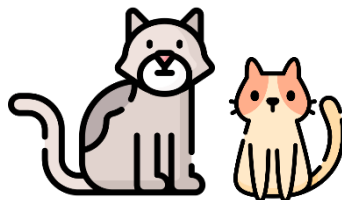
Google Cloud



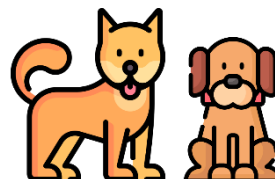
1 Maż



1 Córka



2 Koty



2 Psy



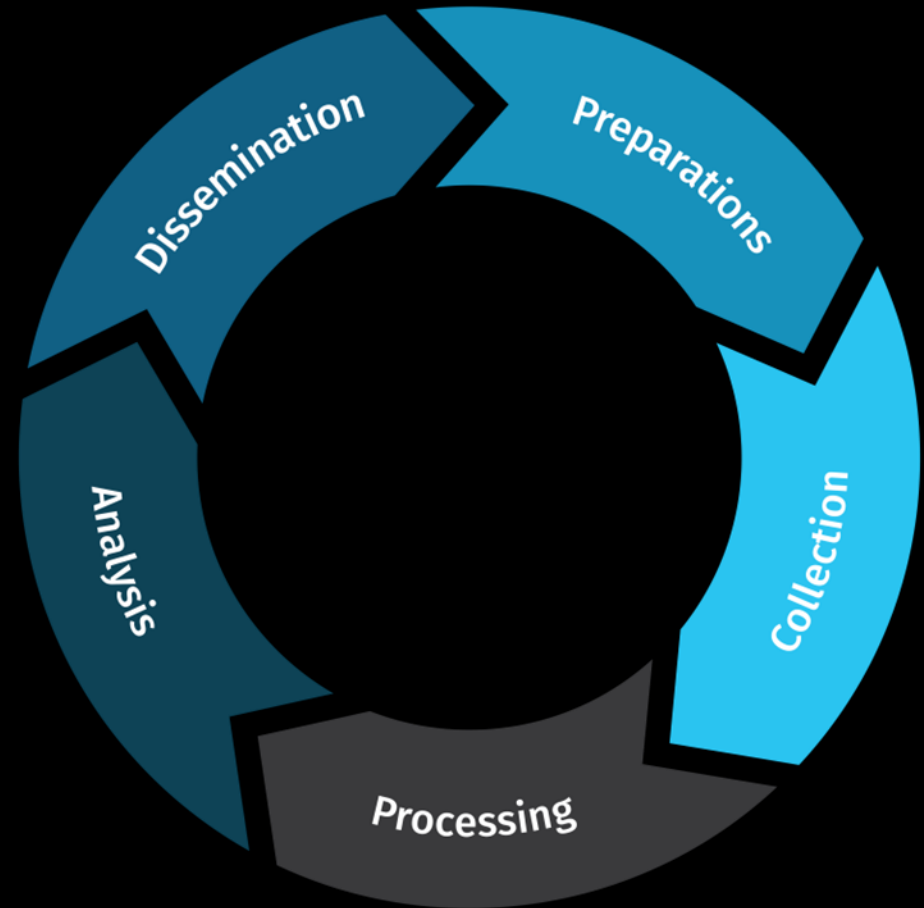
Kryminały



Fotografia

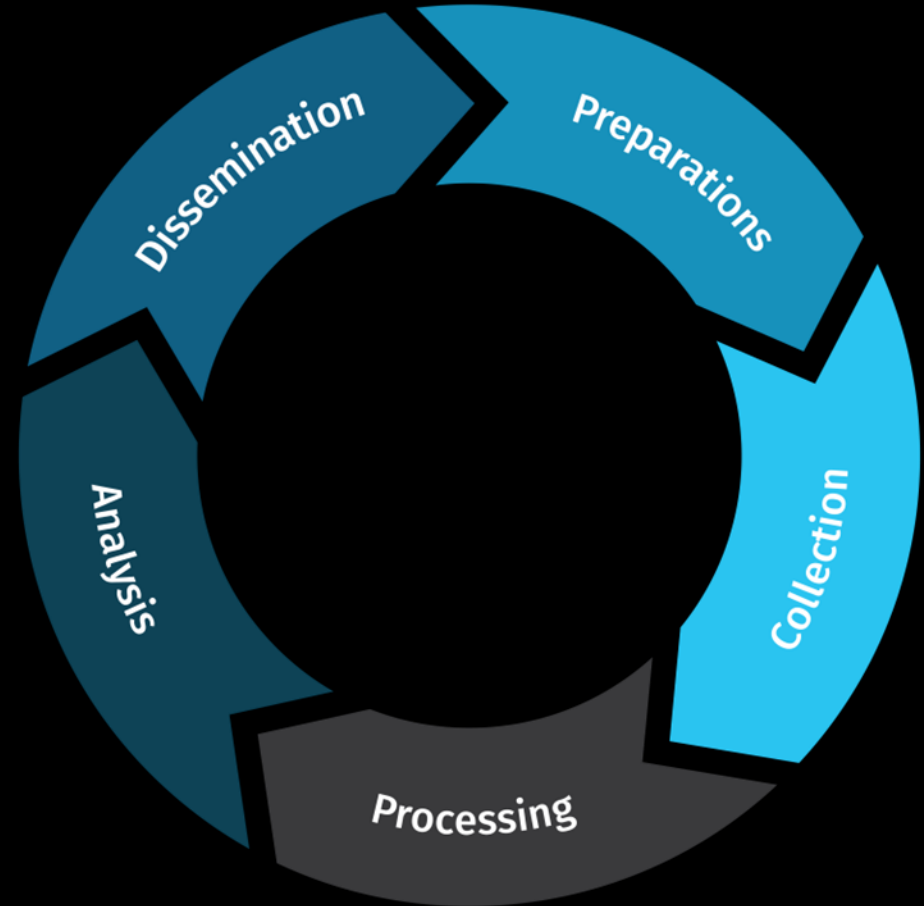
# OSINT – co to jest?

- Definicja OSINT (Open Source Intelligence)
- Narzędzia OSINT do monitorowania



# OSINT – co to jest?

- OSINT oznacza Open Source Intelligence
- OSINT odnosi się do wywiadu opartego na jawnych źródłach informacji.
- Obejmuje zbieranie, analizowanie i wykorzystywanie danych dostępnych publicznie
- OSINT nie polega na uzyskiwaniu dostępu do informacji chronionych czy nielegalnych, lecz na analizie danych, które są otwarcie dostępne dla każdego.



# OSINT (**ang.** *Open-Source INTelligence; OSINT*)

Biały wywiad, rozpoznanie z ogólnodostępnych źródeł

## Krótką historia

OSINT, czyli wywiad oparty na jawnych źródłach, narodził się w Stanach Zjednoczonych w latach 40. XX wieku, podczas II Wojny Światowej.

W tamtym czasie zauważono, że wiele informacji **uznawanych za tajne** można **znaleźć w publicznie dostępnych** materiałach, takich jak dokumenty, prasa czy inne otwarte źródła.

Zamiast angażować szpiegów, wystarczyło te dane zebrać i odpowiednio przeanalizować.

# OSINT (**ang.** *Open-Source INTelligence; OSINT*)

Biały wywiad, rozpoznanie z ogólnodostępnych źródeł

## Krótką historia

Powołano więc specjalną jednostkę działającą w ramach amerykańskiej marynarki wojennej.

Warto podkreślić, że **OSINT nie polega na hakowaniu ani na uzyskiwaniu dostępu do zakazanych miejsc** – opiera się wyłącznie na analizie informacji dostępnych publicznie.

# OSINT (**ang.** *Open-Source INTelligence*; OSINT)

Biały wywiad, rozpoznanie z ogólnodostępnych źródeł

- Pamiętaj, że w OSINT każde źródło informacji może być **wartościowe**.
- Mimo to, zawsze **weryfikuj dane** i podchodź do nich z odpowiednią dawką sceptycyzmu.
- Prawdziwy wywiad opiera się głównie na **analizie zebranych informacji**, a nie tylko na ich gromadzeniu.
- **A co z danymi pochodzącymi z wycieków znalezionych w Darknecie?**  
To pytanie nie jest takie proste i wymaga szczególnego podejścia do tematu i rozwagi, zanim zaczniemy rozpowszechniać treści.

# CELE OSINT

- **Wywiad dotyczący bezpieczeństwa i zagrożeń** - identyfikacja zagrożeń bezpieczeństwa poprzez analizę publicznych informacji o osobach i organizacjach.
- **Śledztwa** - prowadzenie śledztw w różnych sprawach poprzez zbieranie odpowiednich informacji.
- **Wywiad konkurencyjny** - gromadzenie informacji o konkurencji, trendach rynkowych, preferencjach.

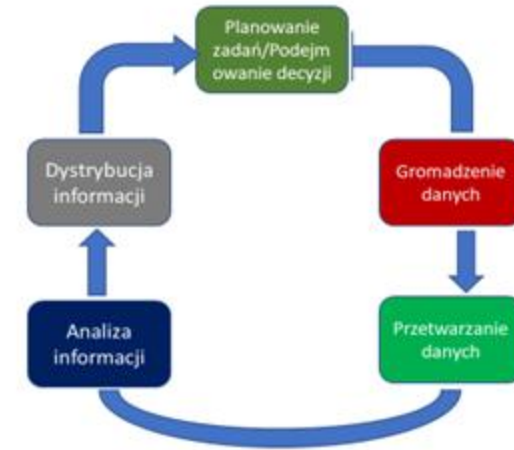


# CELE OSINT cd.

- **Zarządzanie reputacją** - monitorowanie i zarządzanie reputacją online osób, organizacji i marek.
- **Dziennikarstwo i badania** - wspieranie badań poprzez gromadzenie danych w celu odkrywania faktów, weryfikowania twierdzeń i dostarczania kontekstu.
- **Reagowanie na katastrofy i kryzysy** - ocena wpływu katastrof naturalnych, konfliktów lub kryzysów, aby ułatwić .

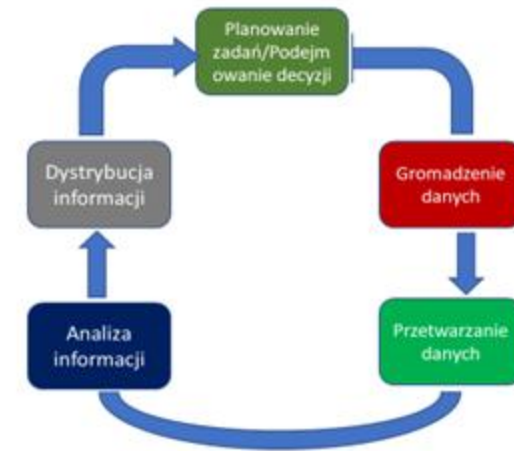
# 1. Planowanie i ukierunkowywanie

- Określenie celu
- Identyfikacja źródeł informacji
- Zdefiniowanie zakresu działań
- Dobór narzędzi i metod
- Ocena ryzyka i zgodności z prawem
- Przydzielenie zasobów
- Opracowywanie strategii badania i planu działania
- Dyskusje



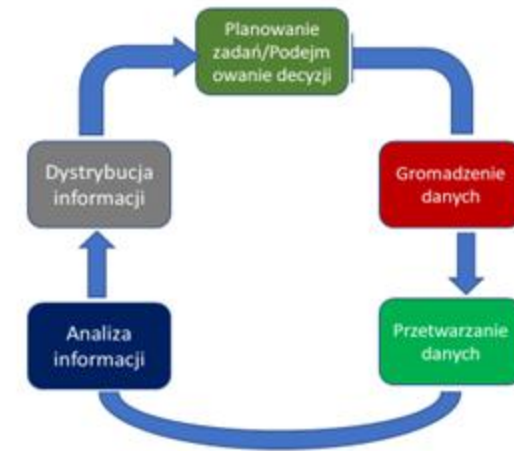
## 2. Zbieranie / gromadzenie danych

- Identyfikacja dostępnych źródeł
- Wykorzystanie narzędzi OSINT
- Zbieranie danych z mediów społecznościowych
- Analiza domen i infrastruktury sieciowej
- Zbieranie danych multimedialnych
- Monitorowanie Darknetu i forów
- Weryfikacja i filtrowanie danych



### 3. Przetwarzanie danych

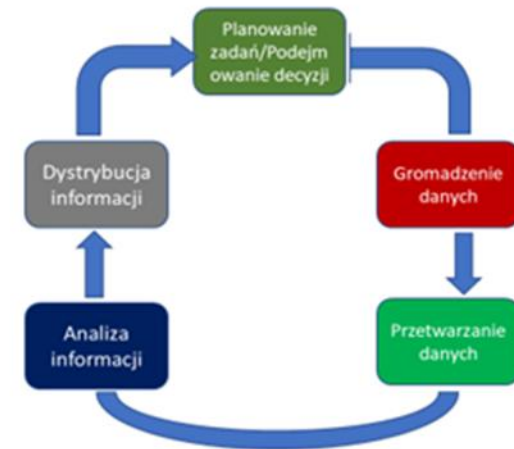
- Organizacja zebranych danych
- Konwersja danych do użytecznego formatu
- Analiza metadanych
- Filtrowanie i weryfikacja danych
- Łączenie danych z różnych źródeł
- Automatyzacja przetwarzania
- Identyfikacja wzorców i anomalii
- Tworzenie raportów i wizualizacji
- Zabezpieczenie przetworzonych danych



Skompilowanie zebranych danych w raporty wywiadowcze.

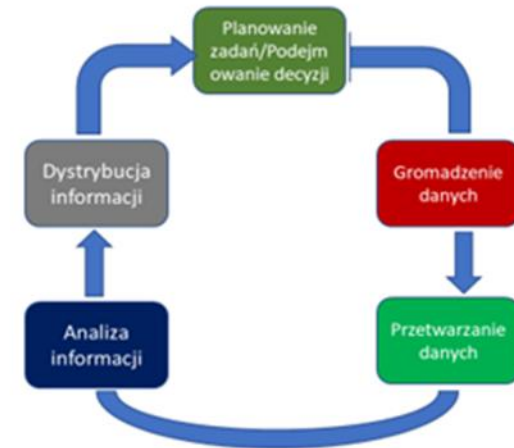
## 4. Analiza informacji

- Zrozumienie kontekstu
- Łączenie danych
- Identyfikacja wzorców i trendów
- Ocena wiarygodności informacji
- Priorytetyzacja danych
- Tworzenie hipotez
- Wizualizacja wyników
- Dokumentowanie wyników
- Ocena ryzyka i potencjalnych działań



## 5. Rozpowszechnianie/ dystrybucja informacji

- Przygotowanie raportu końcowego
- Dostosowanie formatu do odbiorcy
- Zabezpieczenie informacji
- Wybór kanałów dystrybucji
- Przekazanie informacji
- Zapewnienie możliwości dalszej analizy
- Zbieranie informacji zwrotnej
- Monitorowanie dalszego wykorzystania informacji



- Przekazanie analizy decydentowi
- Czekanie na opinię
- W razie potrzeby powtórzenie



# Główni odbiorcy OSINT

- Służby wywiadowcze i agencje rządowe
- Prywatni detektywi
- Kancelarie prawne
- Pentesterzy
- Analitycy finansowi
- Ubezpieczyciele
- Firmy konsultingowe
- Dziennikarze śledczy itd.



# Rządy

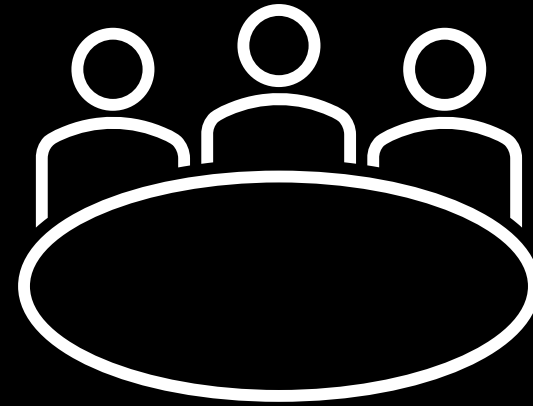
- Nastawienie społeczności
- Ryzyko i zagrożenia dla bezpieczeństwa publicznego
- Pogoda i klęski żywiołowe
- Popularne działania
- Krytyczne informacje





# Korporacje

- Ochrona i kontrola personelu
- Należyta staranność
- Śledztwa w sprawie oszustw
- Ryzyko łańcucha dostaw
- Ochrona aktywów
- Monitorowanie marki



# Organy ścigania

- Reagowanie kryzysowe
- Zwalczanie brutalnego ekstremizmu
- Świadomość sytuacyjna
- Bezpieczeństwo publiczne
- Głębokie dochodzenia



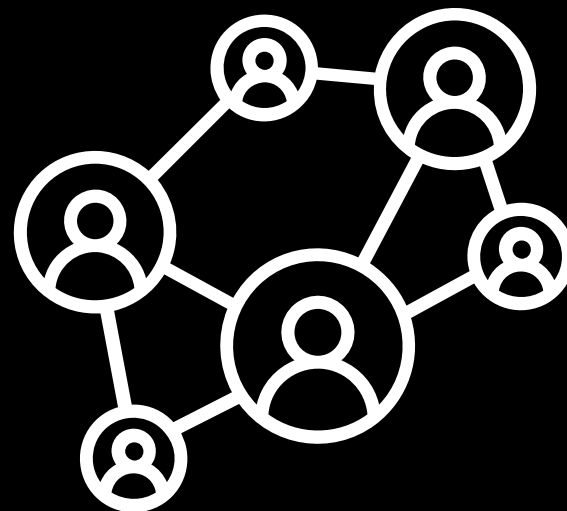
# Śledczy i dziennikarze

- Weryfikacja informacji
- Dziennikarstwo śledcze
- Śledztwo prywatne
- Odkrywanie faktów
- Dostęp do danych



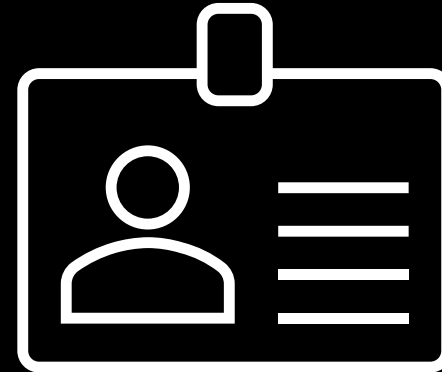
# Główne źródła OSINTu

- Identyfikatory osób
- Social media
- Artykuły informacyjne
- Raporty
- Witryny
- Blogi i fora internetowe



# Identyfikatory osób

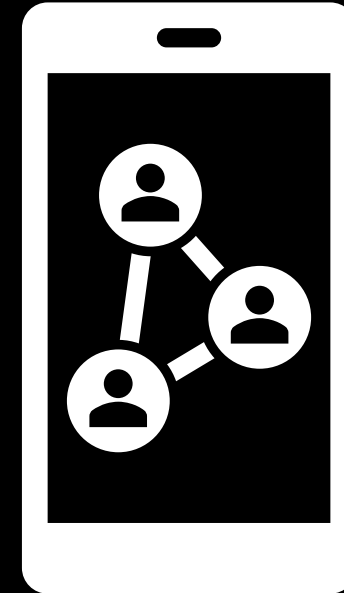
- Imiona
- Pseudonimy
- Adresy e-mail
- Numery telefonów
- Historia zatrudnienia
- Wykształcenie



# Social media

Pozyskiwanie informacji z takich platform jak:

- Facebook
- X (dawny Twitter)
- Instagram
- LinkedIn
- TikTok
- inne



# Artykuły informacyjne

Może to obejmować:

- tradycyjne serwisy informacyjne
- gazety internetowe
- inne źródła, w których relacjonowane są wiadomości i bieżące wydarzenia



# Raporty

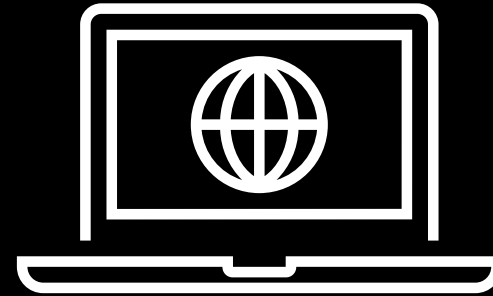
- Dokumenty
- Publikacje
- Dokumenty informacyjne
- Dane statystyczne
- Inne informacje publikowane przez agencje rządowe





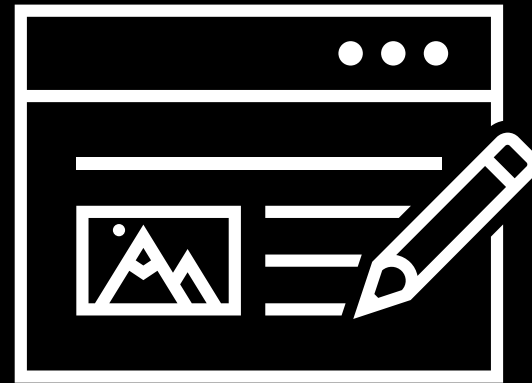
# Witryny

- Tekst
- Obrazy
- Filmy
- Dokumenty
- Metadane
- Inne treści multimedialne



# Blogi i fora internetowe

- Cenne spostrzeżenia
- Opinie
- Dyskusje i treści tworzone przez użytkowników na szeroki zakres tematów



# Techniki OSINT

- Wyszukiwanie informacji np. o autorach hejtu
- Analiza metadanych i geolokalizacji
- Wykorzystanie wyszukiwania obrazem do identyfikacji źródeł

<https://verificators.com/wyszukiwanie-informacji-osint-case-study/>

<https://rynekinformacji.pl/>

<https://www.support-online.pl/blog/bialy-wywiad-jak-osint-zmienia-i-analizuje-informacji-z-ogolnodostepnych-zrodel/>



źr. wydawnictwo.securitum.pl/

# Darmowe narzędzia OSINT

- Web Archive wykorzystuje technologię zwaną web crawlingiem, która polega na automatycznym przeszukiwaniu i zbieraniu danych z Internetu.
- W praktyce oznacza to, że zawartość archiwum jest regularnie aktualizowana przez boty skanujące sieć, a także przez pracowników, partnerów organizacji, takich jak biblioteki czy uczelnie, oraz zwykłych użytkowników Internetu.
- W archiwum gromadzone są różnorodne treści, w tym strony internetowe, blogi, fora, multimedia, gry online, nagrania audio i wiele innych materiałów.

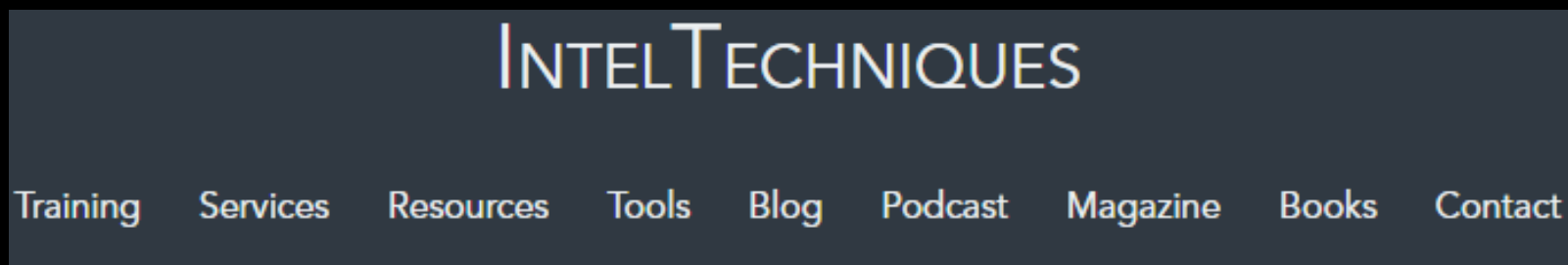
<https://web.archive.org/>



# Darmowe narzędzia OSINT

Firma **IntelTechniques** od dwóch dekad jest uznawana za lidera w dziedzinie szkoleń z zakresu wywiadu opartego na otwartym oprogramowaniu (OSINT).

<https://inteltechniques.com/>



# Darmowe narzędzia OSINT

- EPICOS jest wiodącą globalną platformą informacyjną B2B (Business-to-Business) dla przemysłu lotniczego, obronnego i zaawansowanych technologii, a także jedyną globalną firmą konsultingową i usługodawcą offsetu i współpracy przemysłowej.
- EPICOS oferuje informacje, rozwiązania i usługi wsparcia w zakresie współpracy przemysłowej i offsetów na całym świecie.

<https://www.epicos.com/>



# Darmowe narzędzia OSINT

- Rozszerzenie Chrome Forensic OSINT jest niezawodnym partnerem, starannie opracowanym, aby sprostać wysokim wymaganiom gromadzenia dowodów cyfrowych.
- Mająca siedzibę w Kanadzie firma Forensic OSINT gwarantuje integralność i dokładność, rewolucjonizując sposób, w jaki podchodzi się do wywiadu open source.

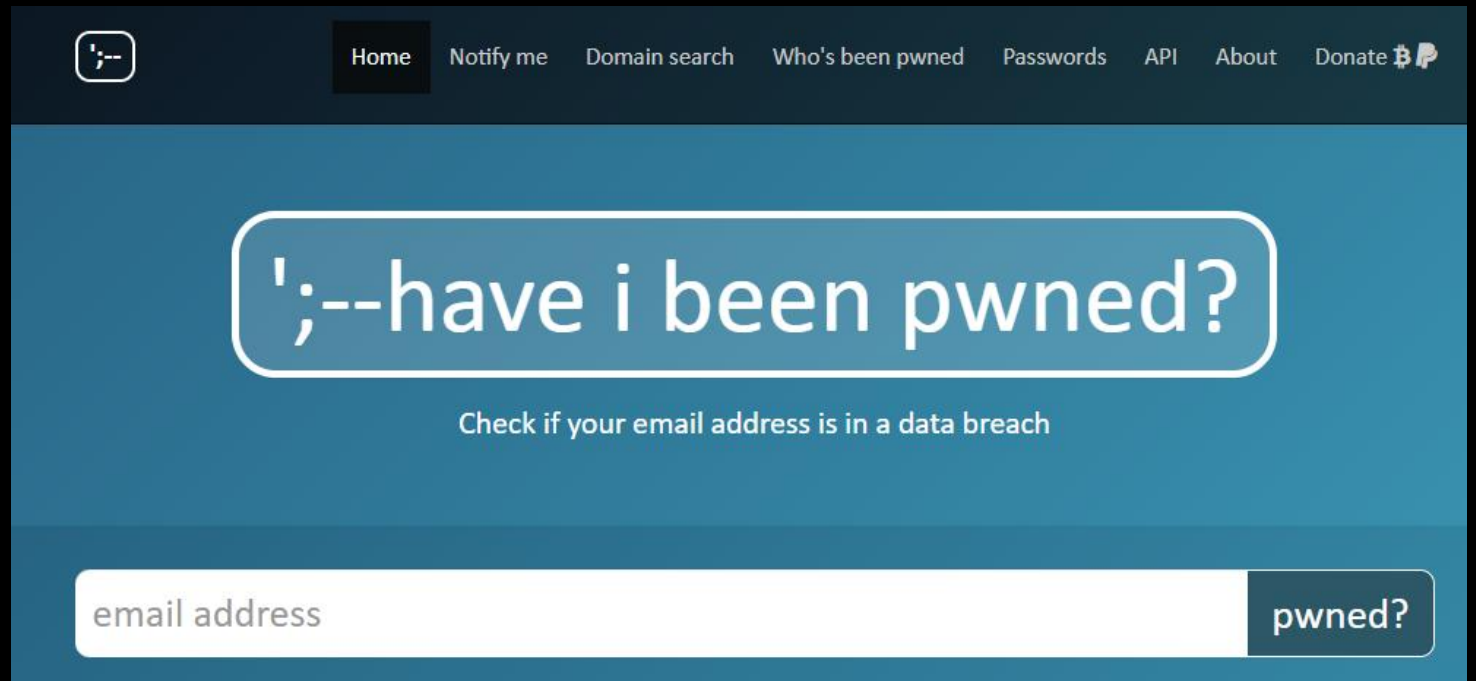
<https://www.forensicosint.com/>



# Darmowe narzędzia OSINT

**Have I Been Pwned** umożliwia przeszukanie wielu naruszeń danych, aby sprawdzić, czy Twój adres e-mail lub numer telefonu został naruszony.

<https://haveibeenpwned.com/>



The screenshot shows the homepage of the 'Have I Been Pwned' website. The header is dark blue with a navigation menu containing links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate (with a Bitcoin icon). The main content area has a light blue background. In the center, there is a large white rounded rectangle containing the text 'have i been pwned?' in a large, white, sans-serif font. Below this, in a smaller white font, it says 'Check if your email address is in a data breach'. At the bottom, there is a white input field with the placeholder text 'email address' and a dark blue button with the text 'pwned?' in white.



# Darmowe narzędzia OSINT

- FOCA to pakiet oprogramowania typu open source, który umożliwia użytkownikom wykonywanie podstawowych analiz metadanych w celu określenia, czy określona witryna internetowa może zawierać uszkodzone dokumenty.
- Niektóre powszechnie obsługiwane formaty to DOC, ODT, ODS, SVG i PPT.
- Wyniki są zestawiane w formacie przyjaznym dla użytkownika, dzięki czemu łatwo jest wykryć ewentualne problemy.

<https://github.com/ElevenPaths/FOCA>



źr. offsec.tools

# Narzędzia OSINT

- **Maltego** - graficzna analiza linków. Wszechstronna platforma wywiadowcza typu open source, która może uprościć i przyspieszyć dochodzenia.
- Zapewnia dostęp do 58 źródeł danych i możliwości ręcznego przesyłania, a także baz danych obejmujących do 1 miliona podmiotów, co pomaga w przeprowadzaniu lepszych analiz.
- Jego potężne narzędzia do wizualizacji umożliwiają także wybór różnych układów, takich jak bloki, wykresy hierarchiczne lub kołowe z wagami i notatkami w celu dalszego udoskonalenia.

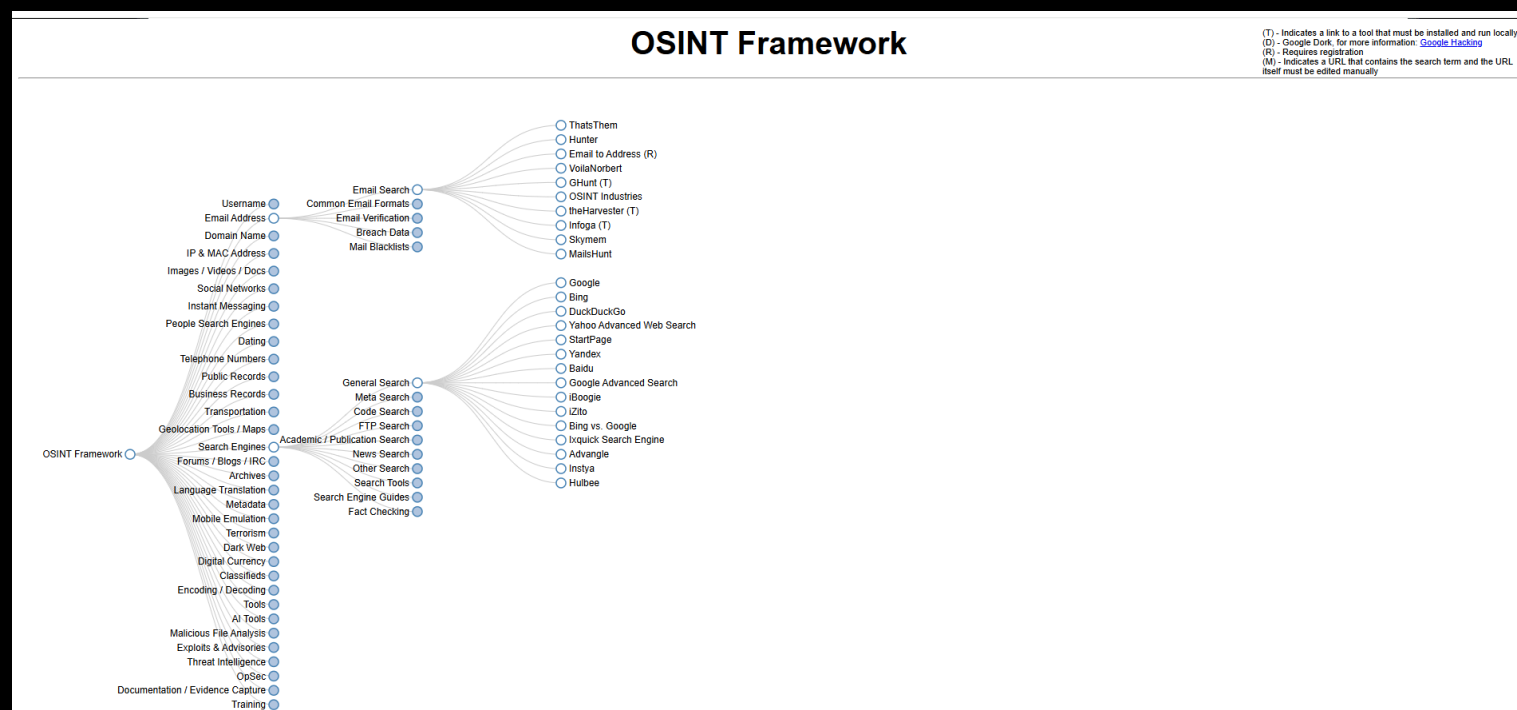


<https://www.maltego.com/>

# Narzędzia OSINT

OSINT Framework jest doskonałym źródłem informacji o otwartym kodzie źródłowym. Zawiera wszystko, od źródeł danych po przydatne linki do skutecznych narzędzi, dzięki czemu jest to znacznie łatwiejsze niż indywidualne badanie każdego dostępnego programu i narzędzia.

<https://osintframework.com/>



# Narzędzia OSINT

**Recon-ng** to potężne narzędzie służące do wyszukiwania informacji związanych z domenami stron internetowych. Pierwotnie zaczął się jako skrypt, ale teraz przekształcił się w pełną platformę

<https://github.com/lanmaster53/recon-ng>

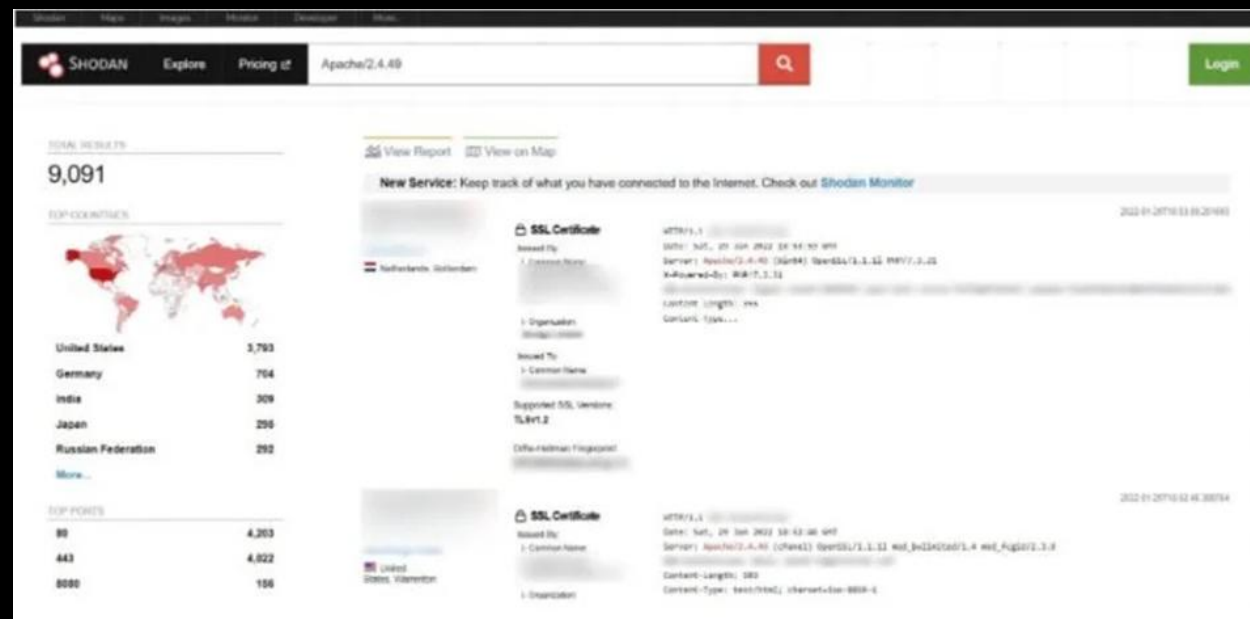


źr. WirePost

# Narzędzia OSINT

**Shodan** to zaawansowana wyszukiwarka, która pozwala użytkownikom szybko zidentyfikować i uzyskać dostęp do informacji na temat technologii wykorzystywanej przez dowolną firmę. Wpisując nazwę firmy, można uzyskać szczegółowy wgląd w jej urządzenia IoT – takie jak lokalizacja, szczegóły konfiguracji i luki w zabezpieczeniach – pogrupowane według sieci lub adresu IP.

<https://www.shodan.io/>



# Narzędzia OSINT

**Open Corporates** to świeże, standaryzowane, audytowalne informacje bezpośrednio z oficjalnych źródeł podstawowych w ponad 140 jurysdykcjach — wszystko oparte na naszych zasadach danych podmiotów prawnych i wiodącej na świecie wiedzy specjalistycznej w zakresie danych podmiotów prawnych. To dane, którym możesz zaufać.

<https://opencorporates.com/>

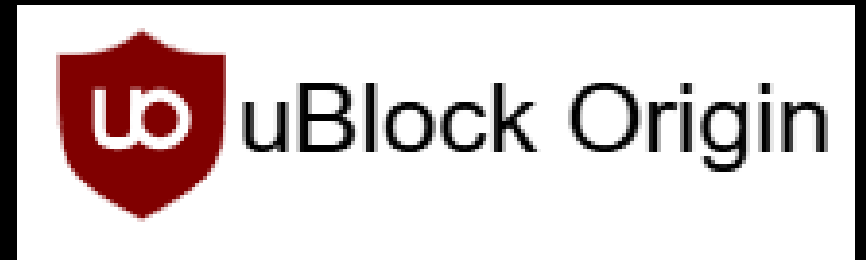


# Rozszerzenia do przeglądarek

uBlock Origin to darmowe i otwarte rozszerzenie przeglądarki do filtrowania treści, w tym blokowania reklam.

Rozszerzenie jest dostępne dla Chrome, Chromium, Edge, Firefox, Brave, Opera, Pale Moon, a także wersji Safari przed 13.

<https://ublockorigin.com/>

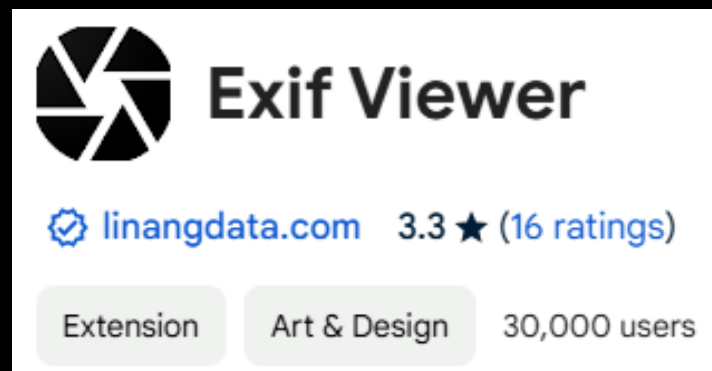


# Rozszerzenia do przeglądarek

**Exif Viewer** to bezpłatne narzędzie pozwala otworzyć obraz z urządzenia lub z adresu URL i wyświetlić jego dane Exif.

Dane Exif obrazu można wyświetlić na dowolnej stronie internetowej.

<https://chromewebstore.google.com/detail/exif-viewer/kbnpbnmjmgabkfemdehelbgdppngihhg>





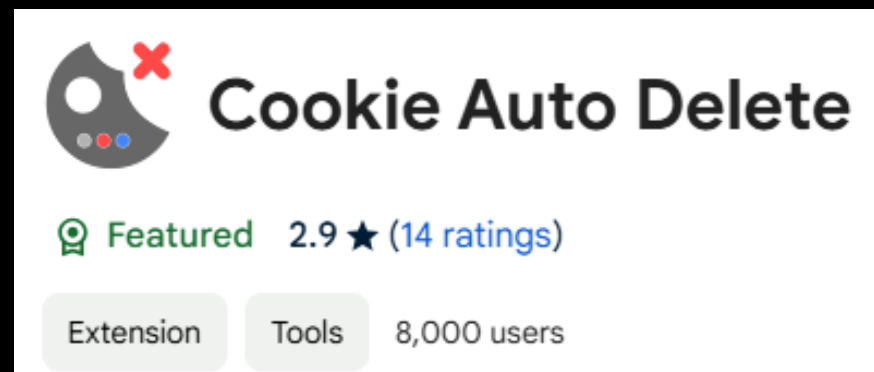
# Rozszerzenia do przeglądarek

**Cookie Auto Delete** to rozszerzenie, które pomaga szybko usuwać pliki cookie dla karty po jej zamknięciu (tryb „Tab-Only”).

Ponadto możesz ustawić dodatek tak, aby usuwał pliki cookie dla wszystkich kart po zamknięciu przeglądarki (tryb „Session-Only”).

Ikona paska narzędzi służy jako przełącznik WŁ./WYŁ., aby szybko włączyć lub wyłączyć dodatek.

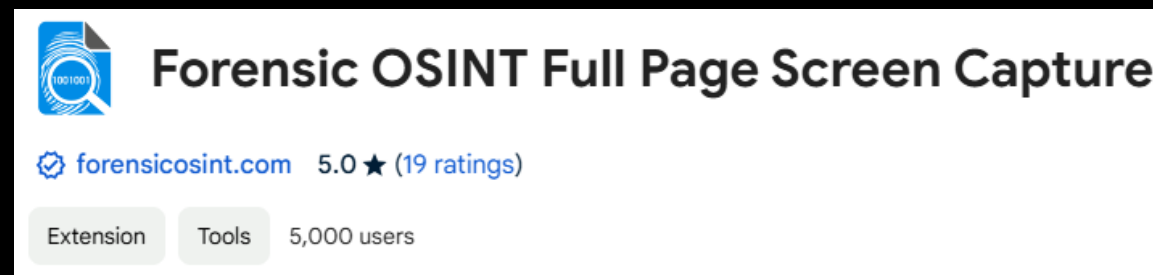
<https://chromewebstore.google.com/detail/cookie-auto-delete/>



# Rozszerzenia do przeglądarek

Forensic OSINT Full Page Screen Capture to możliwość wzbogacenia swojego dochodzenia OSINT o intuicyjne narzędzia do przechwytywania danych, łatwe pobieranie filmów i bezpieczne przetwarzanie danych.

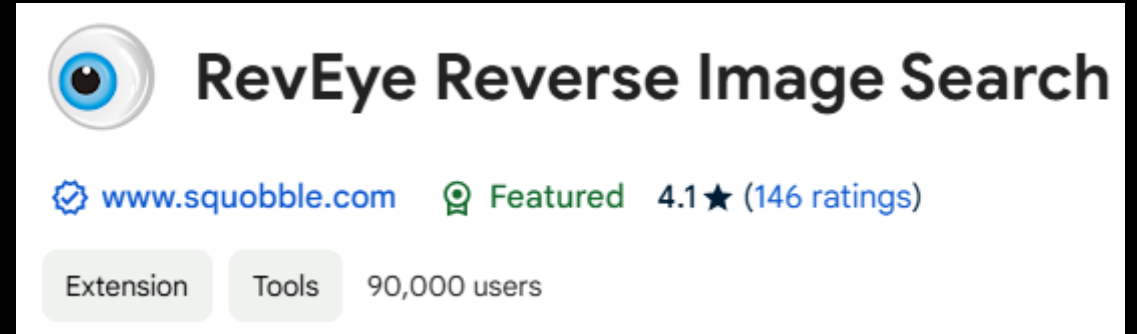
<https://chromewebstore.google.com/detail/forensic-osint-full-page/>



# Rozszerzenia do przeglądarek

**RevEye Reverse Image Search** to rozszerzenie umożliwiające wykonywanie odwrotnego wyszukiwania obrazów poprzez kliknięcie prawym przyciskiem myszy na dowolnym obrazie na stronie internetowej.

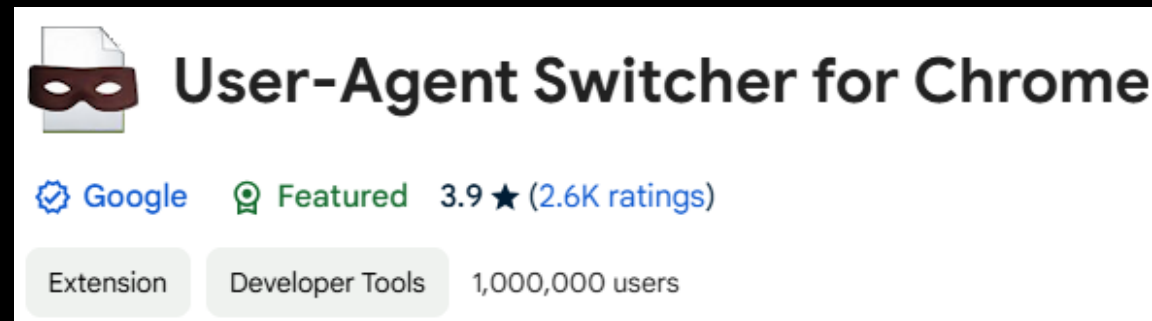
<https://chromewebstore.google.com/detail/reveye-reverse-image-sear/>



# Rozszerzenia do przeglądarek

User-Agent Switcher for Chrome to rozszerzenie, dzięki temu rozszerzeniu możesz szybko i łatwo przełączać się między ciągami user-agent. Możesz również skonfigurować określone adresy URL, które chcesz podszywać za każdym razem.

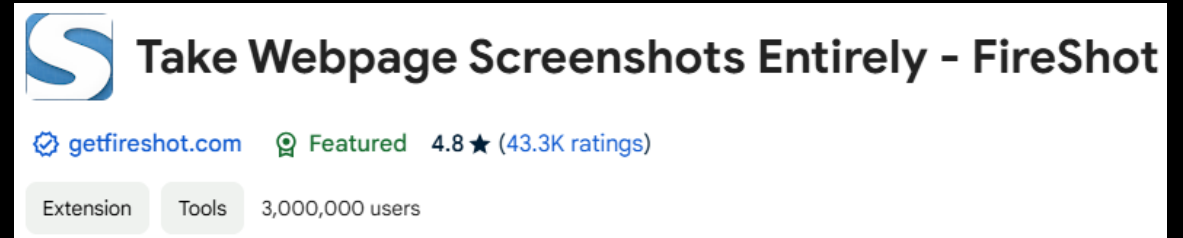
<https://chromewebstore.google.com/detail/reveye-reverse-image-sear/>



# Rozszerzenia do przeglądarek

**Take Webpage Screenshots Entirely – FireShot** robi pełny zrzut ekranu całej strony internetowej. Przechwytuje, edytuje i zapisuje go do formatu PDF/JPG/GIF/PNG, wgrywanie, drukowanie. Można edytować i opisywać zrzuty. Można przechwytywać strony internetowe w całości do plików PDF (z linkami) / JPEG / PNG, drukować lub kopiować do schowka.

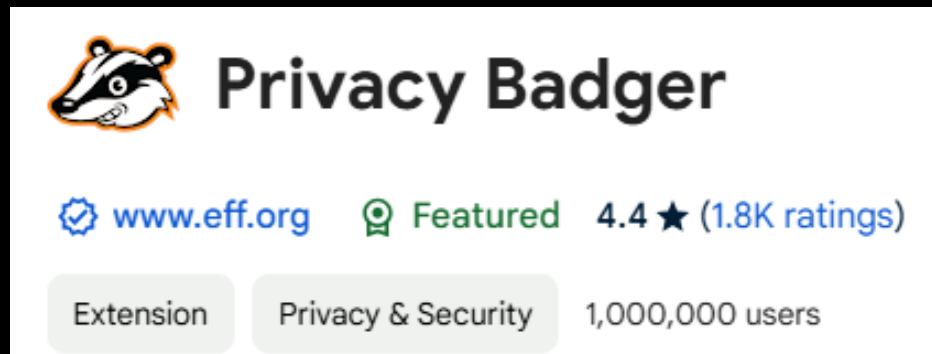
<https://chromewebstore.google.com/detail/take-webpage-screenshots/>



# Rozszerzenia do przeglądarek

**Privacy Badger** automatycznie uczy się blokować niewidoczne trackery. Zamiast przechowywać listy blokowanych elementów, Privacy Badger automatycznie odkrywa trackery na podstawie ich zachowania. Privacy Badger wysyła sygnał Global Privacy Control, aby zrezygnować z udostępniania i sprzedaży danych, oraz sygnał Do Not Track, aby poinformować firmy, aby Cię nie śledziły. Jeśli trackery ignorują Twoje życzenia, Privacy Badger nauczy się je blokować.

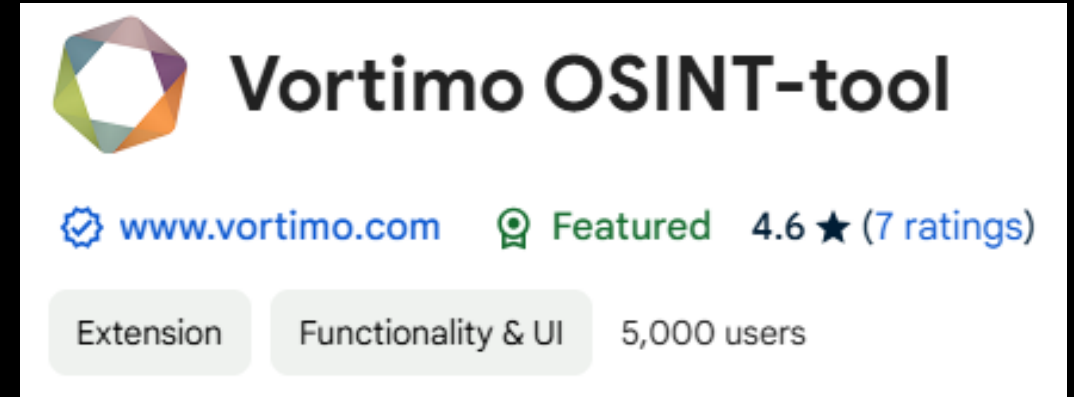
<https://chromewebstore.google.com/detail/privacy-badger/>



# Rozszerzenia do przeglądarek

**Vortimo OSINT-tool** to szwajcarski scyzoryk OSINTu: zakładki/zapis stron, przechowywanie zrzutów ekranu, usuwanie i wzbogacanie. Znajduje tekst na każdej stronie + podświetlanie. Wszystkie dane są przechowywane lokalnie i nie opuszczają komputera.

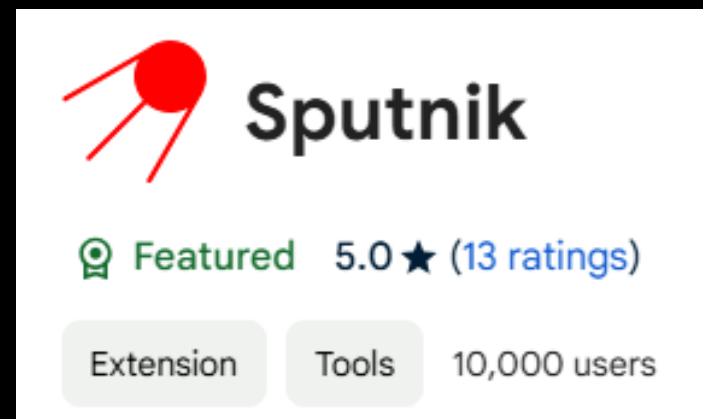
<https://chromewebstore.google.com/detail/vortimo-osint-tool/>



# Rozszerzenia do przeglądarek

**Sputnik** to rozszerzenie umożliwiające szybkie i łatwe wyszukiwanie adresów IP, domen, skrótów plików i adresów URL przy użyciu bezpłatnych zasobów Open Source Intelligence (OSINT).

<https://chromewebstore.google.com/detail/sputnik/>



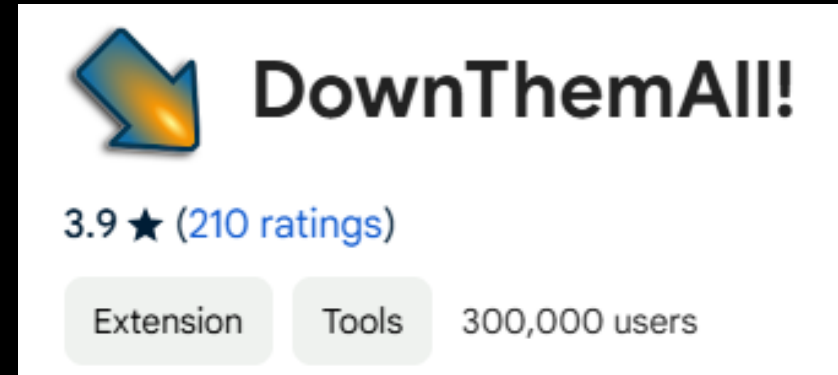


# Rozszerzenia do przeglądarek

**DownThemAll** pomaga wybierać, kolejkować, sortować i uruchamiać pobieranie szybciej.

Zawiera zaawansowane sposoby wybierania linków do pobrania i zapamiętuje poprzednie decyzje użytkownika, dzięki czemu można kolejkować więcej pobrań za pomocą jednego kliknięcia!

<https://chromewebstore.google.com/detail/downthemall/>



# Optymalizacja komputera

1. **Program antywirusowy** - oprogramowanie antywirusowe to rodzaj aplikacji, która służy do wykrywania, zapobiegania i usuwania złośliwego oprogramowania, znanego jako malware, z komputerów i sieci (Windows Defender, ESET, Avast itp.)
2. **VPN (wirtualna sieć prywatna)** - technologia umożliwiająca utworzenie bezpiecznego połączenia przez Internet między urządzeniem a zdalnym serwerem. Sieci VPN szyfrują ruch internetowy (MullvadVPN itp.)
3. **Maszyny wirtualne (VM)** - emulacje komputerów fizycznych oparte na oprogramowaniu, które pozwalają na jednoczesne działanie wielu systemów operacyjnych (OS) na jednej maszynie fizycznej (Kali Linux, Trace Labs, Silo, Tsurugi itp.)
4. **Przeglądarki internetowe** - przeglądarki internetowe są podstawowym narzędziem do przeprowadzania wyszukiwań i odgrywają kluczową rolę w prowadzeniu dochodzeń OSINT, zapewniając dostęp do szerokiej gamy źródeł i narzędzi online (Brave, Firefox, Tor itp.)
5. **Marionetki (Sock Puppets)** - marionetki odnoszą się do fałszywych tożsamości lub osób online tworzonych i obsługiwanych przez osoby lub grupy w celach dochodzeniowych (FakePersonGenerator, ThisPersonDoesNotExist, ChatGPT).

# Książki

1. OSINT Techniques - Michael Bazzell
2. Deep Dive - Rae Baker
3. Hunting Cyber Criminals - Vinny Troia
4. OSINT Methods and Tools - Nihad A. Hassan & Rami Hijazi
5. We are bellingcat: An Intelligence Agency for the People - Eliot Higgins
6. How to Find Out Anything - Don MacLeod
7. Operator Handbook - Joshua Picolet
8. OSINT: The Art of Collecting Open

# Podcasts

1. Darknet diaries - <https://darknetdiaries.com/>
2. NeedleStack - [https://www.youtube.com/playlist?list=PLgC1X8zH-TyLA8qTApjxEL\\_b0eyJSvLzM](https://www.youtube.com/playlist?list=PLgC1X8zH-TyLA8qTApjxEL_b0eyJSvLzM)  
Spotify - <https://open.spotify.com/episode/4PlwCRImn1m9oBLxFDd3iE>
3. ShadowDragon - <https://podcast.shadowdragon.io/>
4. The Pivot - <https://www.maltego.com/categories/the-pivot-podcast/>
5. The OSINT Bunker News Snapshot - <https://open.spotify.com/show/0MdC1XeHAZycXvBBaPxtzy>
6. Layer 8 - <https://creators.spotify.com/pod/show/layer-8-podcast>
7. The World of Intelligence - <https://open.spotify.com/show/00YnC7VESPyjXWUDafDnvP>

# Blogi

1. Zaufana Trzecia Strona - <https://zaufanatrzeciastrona.pl/post/tag/osint/>
2. CQure - <https://cquireacademy.com/blog/>
3. Sekurak - <https://sekurak.pl/tag/osint/>
4. Niebezpiecznik - <https://niebezpiecznik.pl/?s=OSINT>
5. Cyber Detective's website - <https://cybdetective.com/>
6. Secjuice - <https://www.secjuice.com/>
7. Sector035 - <https://sector035.nl/>
8. IntelTechniques- <https://inteltechniques.com/blog/>
9. OffensiveOSINT - <https://www.offensiveosint.io/>
10. OSINT Combine - <https://www.osintcombine.com/blog>
11. SocialLinks - <https://blog.sociallinks.io/>
12. WebBreacher - <https://webbreacher.com/>
13. SANS Institute - <https://www.sans.org/>
14. OSINTME - <https://www.osintme.com/>
15. OH SHINT! - <https://ohshint.gitbook.io/oh-shint-its-a-blog>
16. OSINTCurio.us - <https://www.osintcurio.us/>
17. Bellingcat - <https://www.bellingcat.com/>

# Maszyny wirtualne i spółka

1. Sherlock Linux VM - <https://github.com/sherlock-project/sherlock>
2. Silo (platform for isolated online investigations) - <https://www.authentic8.com/products/silo-for-research>
3. Kali Linux VM - <https://www.kali.org/get-kali/#kali-platforms>
4. Trace Labs OSINT VM - <https://www.tracelabs.org/initiatives/osint-vm>
5. CSI Linux VM - <https://downloads.csilinux.com/>
6. Tsurugi VM - <https://tsurugi-linux.org/>
7. Tails (privacy centered OS) - <https://tails.net/>
8. Debian (optimal Linux OS) - <https://www.debian.org/distrib/>

# Toolkits

- Bellingcat's Investigation

<https://bellingcat.gitbook.io/toolkit>

- OSINT For Finding

[https://docs.google.com/spreadsheets/d/1JxBbMt4JvGr--G0Pkl3jP9VDTBunR2uD3\\_faZXDvhxc](https://docs.google.com/spreadsheets/d/1JxBbMt4JvGr--G0Pkl3jP9VDTBunR2uD3_faZXDvhxc)

- Aaron CTI's OSINT Collection

<https://docs.google.com/spreadsheets/d/1klugQqw6POlBtuzon8S0b18-gpsDwX-5OYRrB7TyNEw>

# Pliki do pobrania

1. Awesome Cybersecurity Handbooks - <https://github.com/0xsyr0/Awesome-Cybersecurity-Handbooks/tree/main/handbooks>
2. Toddington - <https://www.toddington.com/resources/cheat-sheets/>
3. I-Intelligence OSINT Handbook – [https://i-intelligence.eu/uploads/public-documents/OSINT\\_Handbook\\_2020.pdf](https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf)
4. Blackdot Solutions – [https://blackdotsolutions.com/wp-content/uploads/2021/11/The-OSINT-Handbook\\_.pdf](https://blackdotsolutions.com/wp-content/uploads/2021/11/The-OSINT-Handbook_.pdf)
5. The Intelligence Handbook - <https://go.recordedfuture.com/the-intelligence-handbook-fourth-edition>



# Github

1. Cyber Detective - <https://github.com/cipher387>
2. Daniel Durnea FBI Tools - <https://github.com/danieldurnea/FBI-tools>
3. OSINT Team Links - [https://github.com/IVMachiavelli/OSINT Team Links](https://github.com/IVMachiavelli/OSINT_Team_Links)
4. Awesome OSINT - <https://github.com/jivoi/awesome-osint>
5. OSINT Encyclopedia - [https://github.com/optiv/OSINT Encyclopedia](https://github.com/optiv/OSINT_Encyclopedia)
6. OH SHINT! - <https://github.com/ohshint>
7. OSINTDojo - <https://github.com/OsintDojo>
8. OSINT Resources by Country - <https://github.com/wddadk/OSINT-for-countries>
9. Ph055a - <https://github.com/ph055a>
10. Datajournalism resources - <https://github.com/r3mlab/datajournalism-resources>
11. Non-typical OSINT guide - <https://github.com/OffcierCia/non-typical-OSINT-guide>
12. Soxoj - <https://github.com/soxoj>
13. Offensive-OSINT-Tools - <https://github.com/wddadk/Offensive-OSINT-Tools>
14. Awesome Soc Analyst - <https://github.com/LetsDefend/awesome-soc-analyst>

# Not The Hidden Wiki

Największe repozytorium linków powiązanych z cybersecurity:

<https://github.com/notthehiddenwiki/NTHW>



# Polski OSINT

Osintown: <https://start.me/p/rx4q8r/polski-osint>

Osintown

POLSKI OSINT

startme

Osintown

**Rejestry Publiczne**

- Otwarte Dane
- Bank Danych
- Urząd Patentowy
- Wyszukiarka Publiczna RWDZ
- Rejestr Zbiórek Publicznych
- Rejestr Decyzji Środowiskowych
- Fedrowanie Sieć Obywatelska
- Wyszukiwanie ogłoszeń BZP
- Rejestr kościołów i innych związków wyznaniowych
- Analizy i raporty antykorupcyjne
- Wykaz podatników VAT
- SUDOP - Wyszukiwanie Środków Pomocowych
- Mapa Dotacji UE
- Przetargi - Zamówienia Publiczne
- Pressinfo - Dostęp Do Przetargu
- Przetargi Publiczne, Zamówienia
- Placówki NFZ
- Wykaz Podmiotów Leczniczych
- Rejestr Podmiotów Wykonujących Działalność Leczniczą

**Archiwa**

- Archiwa Państwowe
- Szukaj w Archiwach
- Repozytorium Cyfrowe Instytutów Naukowych
- Polona - Biblioteka Cyfrowa
- Zbiory NAC (Archiwa Państwowe)
- Inwentarz IPN
- Wojskowe Biuro Historyczne

**Serwisy Społecznościowe**

- Albicla
- Cebulka (TOR)
- Fotka
- GG
- Golden Line
- Hejto
- Gloria
- Karab
- Lurker
- Mastodon
- Moblo
- Osobie
- Szmer
- Queery
- Wykop

**Serwisy Randkowe**

- Ipon - Dla Osób Niepełnosprawnych
- Zapisaniosobie - Dla Osób Religijnych
- Przeznaczeni - Dla ludzi z Wartościami
- Randki w Sympatii

**Osoby i Identyfikacja**

- Lista Imion Występujących w Rejestrze PESEL
- Otwarte Dane - Nazwiska w rejestrze PESEL
- Rozkład występowania nazwisk
- Nazwiska-polskie - Wyszukaj Osoby Po Nazwiskach
- Biuletyn Informacji Publicznej
- Zaginieni
- Zaginieni.policja.pl
- Poszukiwani.policja.pl
- Indeks Represjonowanych
- Rejestr Sprawców Przestępstw na Tle Seksualnym
- Grobonet - Wyszukiwarka Osób Pochowanych
- Mogiły - Internetowa Baza Pochowanych
- Webcmentarz - Wyszukiwarka Zmarłych
- Księgarnie - Internetowa Wyszukiwarka Zmarłych
- Genealogia - Wyszukiwarka Nazwisk
- Informacja o więźniach / Muzeum / Auschwitz-Birkenau
- JRI - Genealogia
- Pgsa - Branch Geneologiczny w USA
- Genealodzy - Serwis
- Ornatowski - Pochodzenie Nazwisk

**Rejestry Osób**

- Rejestr Tłumaczy Przysięgłych
- Rejestr Biegłych
- Rejestr Detektywów
- Rejestr Radców
- Rejestr Komorników Sądowych
- Wykaz Księży
- Rejestr Adwokatów i Aplikantów Adwokackich
- Aktualni Senatorowie
- Aktualni posłowie
- Rejestr Diagnostów Laboratoryjnych
- Rejestr Doktorów
- Rejestr Profesorów
- Krajowy Rejestr Fizjoterapeutów
- Rejestr Farmaceutów
- Rejestr Inżynierów i Architektów
- Polska Izba Architektów

**Firmy**

- GoWork - Opinie z Gowork.pl
- Pracodawcy - Opinie z Pracuj.pl
- Opracodawcach
- Panorama Firm
- Absolvent
- Informacje o Spółkach, Fundacjach i Stowarzyszeniach
- Wyszukiwarka KRS - IMSIG
- System EKRS
- Krajowy Rejestr Zadłużonych
- CEIDG - Baza Przedsiębiorców
- Aleo - Baza Firm
- Gielda długów - Vindix

**Książki Telefoniczne oraz Numery Telefonów**

- Dostawca Usług
- Rejestr Premium
- Kto Dzwonił - Wyszukiwarka numerów
- Kto to? - Wyszukiwarka nieznanych numerów
- Nieznany numer.pl - najnowsze oceny numerów
- Nieznany-numer.pl - baza nieznanych numerów
- Baza Firm Pkt
- Biznesfinder - Baza B2B
- Aleranking
- Książka telefoniczna Plus
- Książka telefoniczna Vectra
- Książka Telefoniczna Play

**Wyszukiwarki plików**

- Chomikuj.pl - Wyszukiwarka Chomikuj
- Docer - Wyszukiwarka Dokumentów
- Slideplayer - Wyszukiwarka Prezentacji
- Wyszukiwarka Pastebin.pl (Google Dorks)
- Fotosik - Wyszukiwarka Zdjęć
- Polska na fotografii z wyszukiwarką

**Domeny**

- Krajowy rejestr domen
- Lista domen usuniętych
- Rejestr Domen Zakazanych

**Skracacze Linków**

- Shortener.pl
- linkd
- Utn.pl
- Tiny.pl
- Cutt.ly
- Ujeb.se

**Fora Dyskusyjne**

- Forum Gazeta
- Forum Racjonalista
- Forum Joemonster
- Forum.bytomsk.pl
- M-forum.pl
- Forum Ostrowiec Świętokrzyski
- Ateista.pl
- Goldenline Grupy
  - Forum Alfa Romeo - Alfaholicy
  - Forum Nissan Klub Polska
  - Forum Satkurier
  - Forum DBNAO
  - Najlepsze forum dla Polaków w Niemczech
  - Forum Radom
  - Forum Łowców Gier

**Mapy i Lokalizacja**

- Geoportal Otwartych Danych Przestrzennych
- Mapy - Targeo
- Ukośne - Przestrzeń 360 Polskich Miast
- Stacje Paliw
- Mapa Sieci Elektroenergetycznej
- Mapa Skrzynek Pocztowych
- Mapa przejeżdż i obiektów Straży Granicznej
- Mapa informacji drogowej
- Morskie Mapy Nawigacyjne
- Mapa Lotnisk Cywilnych
- Mapa Ograniczeń Emisji Laserów
- Bank Danych o Lasach
- Policyjna Mapa Zagrożeń Przestępczami Na Tle Seksualnym
- Krajowa Mapa Zagrożeń Bezpieczeństwa
- iMPA - Menedżer Punktów Adresowych
- Betasearch - Mapa Nadajników Radiowych
- BTS - Lokalizacja Nadajników Radiowych
- Wyszukiwarka UKE
- Mapa Pogodowa METEO
- Mapa Burzowo-opadowa
- Radar Opadów
- Mapa Obiektów Fortyfikacyjnych
- Retro Mapy
- Archiwum Map Zachodniej Polski
- Baza Miejscowości Kresowych
- Inne Mapy Archiwalne Polski

**Transport Morski**

- Rejestr Statków, Jachtów oraz Łodzi
- Gospodarka Morska
- Komisja Badań Wypadków Morskich
- Shipspotting Trójmiasto
- Fotografie Archiwalne - Statki i Okręty

**Transport Lotniczy**

- Radar Iotów
- Wyszukiwarka Samolotów
- Urząd Lotnictwa Cywilnego - Publikacje
- Lista zdarzeń - Raporty Wypadków Lotniczych
- Łądowiska w Polsce
- Forum Lotnictwa

**Transport Lądowy**

- Sprawdź OC Pojazdu
- Dekoder VIN
- Autobaza - Sprawdzenie Numeru VIN
- Data Rejestracji
- Raport z Centralnej Ewidencji Pojazdów
- Numer Rejestracyjny oraz Raport
- Wyszukiwarka Numerów Rejestracyjnych
- Truck-spotters - Forum / Firmv

**Źródła Informacji**

- Counterintelligence
- #osintquest
- Zlotuszpaka
- Sekurak - Osint
- Rynek Informacji
- Internet. Czas działa!
- Ciennastrona.com.pl
- Otwarte Źródła
- WizCase - Bezpieczne Strony TOR
- ITContent - Aktywne Strony TOR

**OPSEC**

- PAYLOAD
- Blog DimensioX (TOR)
- Niepodam.pl (tymczasowy e-mail)
- Adrestymczasowy.pl (tymczasowy e-mail)
- Generatory.it (PESEL, NIP, REGON itd.)
- Testerzy - Multum generatorów

**Symbole, Język i Slang**

- Elektroniczny Słownik Języka Polskiego
- PWN - Słownik Języka Polskiego
- Słownik Śląski
- Słownik Kaszubski
- Dialekty i Gwary Polskie
- Grażdanka
- Polski Slang
- Słownik Slangu
- Słownik Slangu - Miejski
- Słownik gwary
- Wszystkie Symbole
- Polskie symbole narodowe

**Subkultura - Kibice**

- Kibice.net
- Stylkibica - Serwis Dla Kiboli
- Pozaboiskowe spotkania — Stadionowi Oprawcy
- Ekipy — zgody, układy, kosi, grupy, grill i inne.
- Forumgiekasy.pl
- Forumniebiescy.pl
- Forum Kibiców Legii Warszawa
- Forum Kibiców Wisły Kraków
- Forum.kibicelecha.pl
- Forum Dyskusyjne Kibiców Cracovii
- Forum kibiców Śląska Wrocław
- Forum-jagiellonii.pl
- Forum.sociosgornik.org
- Forum lechia.gda.pl
- Forum.arkowcy.pl
- Forum Kibiców Wisłoki
- Forum.uniataromow.net

# Pozyskiwanie danych z wycieków znalezionych w Darknecie

Jeśli dane te są wykorzystywane do celów mających na celu wyrządzenie szkody danej osobie, może to stanowić **przestępstwo**.

Nie należy wykorzystywać danych zdobytych przy użyciu OSINT do:

- Do celów szantażu lub zastraszania.
- Do celów kradzieży tożsamości.
- Do celów rozpowszechniania informacji poufnych lub wrażliwych.



Kiedy może być legalne ?

- Do celów dziennikarskich lub edukacyjnych (anonimizacja).
- Do celów bezpieczeństwa, takich jak wykrywanie i zapobieganie cyberprzestępczości.
- Do celów biznesowych, takich jak badania rynku lub analiza konkurencji.

Ważne jest, aby pamiętać, że prawo w tym zakresie może się różnić w zależności od kraju lub regionu. Dlatego przed pozyskaniem danych z wycieków w Darknecie należy sprawdzić, czy jest to legalne w danym miejscu.

# Pozyskiwanie danych z wycieków znalezionych w Darknecie

Pozyskiwanie danych z wycieków w Darknecie w kontekście OSINT wymaga szczególnej ostrożności i przestrzegania zasad etycznych oraz prawnych.

1. **Zachowaj zgodność z prawem:** Upewnij się, że działania są zgodne z obowiązującymi przepisami w Twoim kraju. Pozyskiwanie danych w sposób nielegalny może prowadzić do poważnych konsekwencji prawnych.
2. **Korzystaj z bezpiecznego środowiska:** Używaj systemów operacyjnych przeznaczonych do analizy, takich jak Tails lub Qubes OS, aby chronić swoją tożsamość i dane.
3. **Anonimowość:** Korzystaj z sieci Tor i VPN, aby ukryć swoją lokalizację i tożsamość.
4. **Unikaj korzystania z nielegalnych treści:** Nawet jeśli dane są dostępne, nie korzystaj z nich, jeśli nie jesteś do tego uprawniony. Dane mogą być nielegalne lub naruszać prawa innych osób.
5. **Weryfikuj źródła:** Dane z Darknetu mogą być zmanipulowane lub fałszywe. Zawsze weryfikuj ich autentyczność z innymi źródłami.

# Pozyskiwanie danych z wycieków znalezionych w Darknecie

Pozyskiwanie danych z wycieków w Darknecie w kontekście OSINT wymaga szczególnej ostrożności i przestrzegania zasad etycznych oraz prawnych.

6. **Używaj narzędzi OSINT:** Wykorzystuj narzędzia przeznaczone do analizy danych, takie jak Maltego, Spiderfoot czy recon-ng, które mogą pomóc w bezpiecznym przetwarzaniu informacji.

7. **Zachowaj etykę:** Pamiętaj, że OSINT opiera się na analizie jawnych źródeł. Dane z wycieków mogą być wątpliwe etycznie, dlatego zawsze rozważ, czy ich użycie jest uzasadnione.

8. **Zabezpiecz swoje urządzenie:** Upewnij się, że Twoje urządzenie jest odpowiednio zabezpieczone przed złośliwym oprogramowaniem, które może być obecne w plikach z Darknetu.

**Podsumowując**, pozyskiwanie danych z Darknetu w OSINT wymaga dużej ostrożności, świadomości prawnej i etycznej oraz odpowiednich narzędzi i zabezpieczeń.

# Zalety i wady OSINT

## Zalety OSINT

- jest to metoda legalna i etyczna
- jest to metoda stosunkowo tania
- jest to metoda, która może być zastosowana w wielu różnych dziedzinach

## Wady OSINT

- informacje dostępne publicznie mogą być **niepełne lub nieaktualne**
- może być **trudne i czasochłonne** zebranie wszystkich niezbędnych informacji

## Podsumowanie

OSINT to potężne narzędzie, które może być wykorzystywane do pozyskiwania informacji o szerokim zakresie tematów. Jest to metoda, która jest dostępna dla każdego, kto chce się jej nauczyć.

## Art. 267. [Bezprawne uzyskanie informacji]

§1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.

§5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego.



## Art. 269a. [Zakłócenie systemu komputerowego]

Kto, **nie będąc do tego uprawnionym**, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, **podlega karze pozbawienia wolności od 3 miesięcy do lat 5.**

## Art. 269b. [Wytwarzanie programów komputerowych]

§1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 lub 2, art. 269a, art. 270 § 1 albo art. 270a § 1, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej, **podlega karze pozbawienia wolności od 3 miesięcy do lat 5.**

§1a. **Nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia** systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia.

§2. W razie skazania za przestępstwo określone w § 1, **sąd orzeka przepadek** określonych w nim **przedmiotów**, a może orzec ich przepadek, **jeżeli nie stanowiły własności sprawcy.**

## Art. 269c. [Kontratyp działania w celu wykrycia błędów w zabezpieczeniach systemów informatycznych]

Nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

## Czy zgodnie z polskim prawem można przeglądać dane z wycieku z baz danych zawierające hasła i loginy do serwisów internetowych ?

W przypadku przeglądania danych z wycieku z baz danych zawierających hasła i loginy do serwisów internetowych, sprawca uzyskuje dostęp do informacji, do której nie jest uprawniony. Informacje te są wrażliwe, ponieważ mogą zostać wykorzystane do nieuprawnionego dostępu do kont użytkowników w serwisach internetowych.

Zatem przeglądanie danych z wycieku z baz danych zawierających hasła i loginy do serwisów internetowych jest czynem zabronionym i może skutkować odpowiedzialnością karną.

Wyjątki:

Istnieją jednak pewne wyjątki od tej zasady. Dostęp do danych z wycieku z baz danych może być legalny w przypadku, gdy:

- Osoba uzyskująca dostęp jest uprawniona do tego na podstawie przepisów prawa (np. pracownik organu ścigania prowadzący śledztwo).
- Osoba uzyskująca dostęp uzyskała dostęp do danych w wyniku błędu lub zaniedbania podmiotu przetwarzającego dane.
- Osoba uzyskująca dostęp uzyskała dostęp do danych w celu ochrony swoich praw lub dóbr osobistych.

**Podsumowanie:**

Ogólnie rzecz biorąc, **przeglądanie danych z wycieku z baz danych** zawierających hasła i loginy do serwisów internetowych **jest czynem zabronionym** i może skutkować odpowiedzialnością karną.

Istnieją jednak pewne wyjątki od tej zasady, które należy wziąć pod uwagę.

# Narzędzia pracy – odizoluj prywatne środowisko od zadań OSINT !

## Środowisko pracy

- Windows Sandbox <https://learn.microsoft.com/en-us/windows/security/application-security/application-isolation/windows-sandbox/windows-sandbox-install>
- VirtualBOX <https://www.virtualbox.org/wiki/Downloads>
- Ubuntu <https://ubuntu.com/>
- KaliLinux <https://kali.org>

## Który Klient VPN?:

<https://thatoneprivacysite.xyz/>

## Przeglądarka Tor:

<https://www.torproject.org/download/>



# Windows Sandbox - wykorzystanie

- **Testowanie plików pobranych z Internetu:** Zanim otworzysz plik pobrany z Internetu, możesz uruchomić go w Sandbox, aby sprawdzić, czy nie zawiera złośliwego oprogramowania.
- **Testowanie aplikacji lub oprogramowania beta:** Jeśli chcesz wypróbować nową aplikację lub oprogramowanie, które nie jest jeszcze gotowe do użycia w głównym systemie operacyjnym, możesz uruchomić je w Sandbox, aby sprawdzić, czy działa poprawnie i czy nie zawiera błędów.
- **Testowanie nowych ustawień lub konfiguracji systemu:** Jeśli chcesz wypróbować nowe ustawienia lub konfiguracje systemu, możesz uruchomić je w Sandbox, aby sprawdzić, jak wpływają na system.

Aby uruchomić **Windows Sandbox**, otwórz menu **Start** i wyszukaj **Windows Sandbox**.

Następnie kliknij przycisk **Uruchom**.




Microsoft

# Windows Sandbox - korzystanie

Windows Sandbox

Ransomware.live - Group : Hellcat

https://www.ransomware.live/group/hellcat



RANSOMWARE.LIVE

Search...

Recent victims

Cyberattacks in the press

Ransomware Groups

Negotiation Chats


Ransom Notes

Statistics

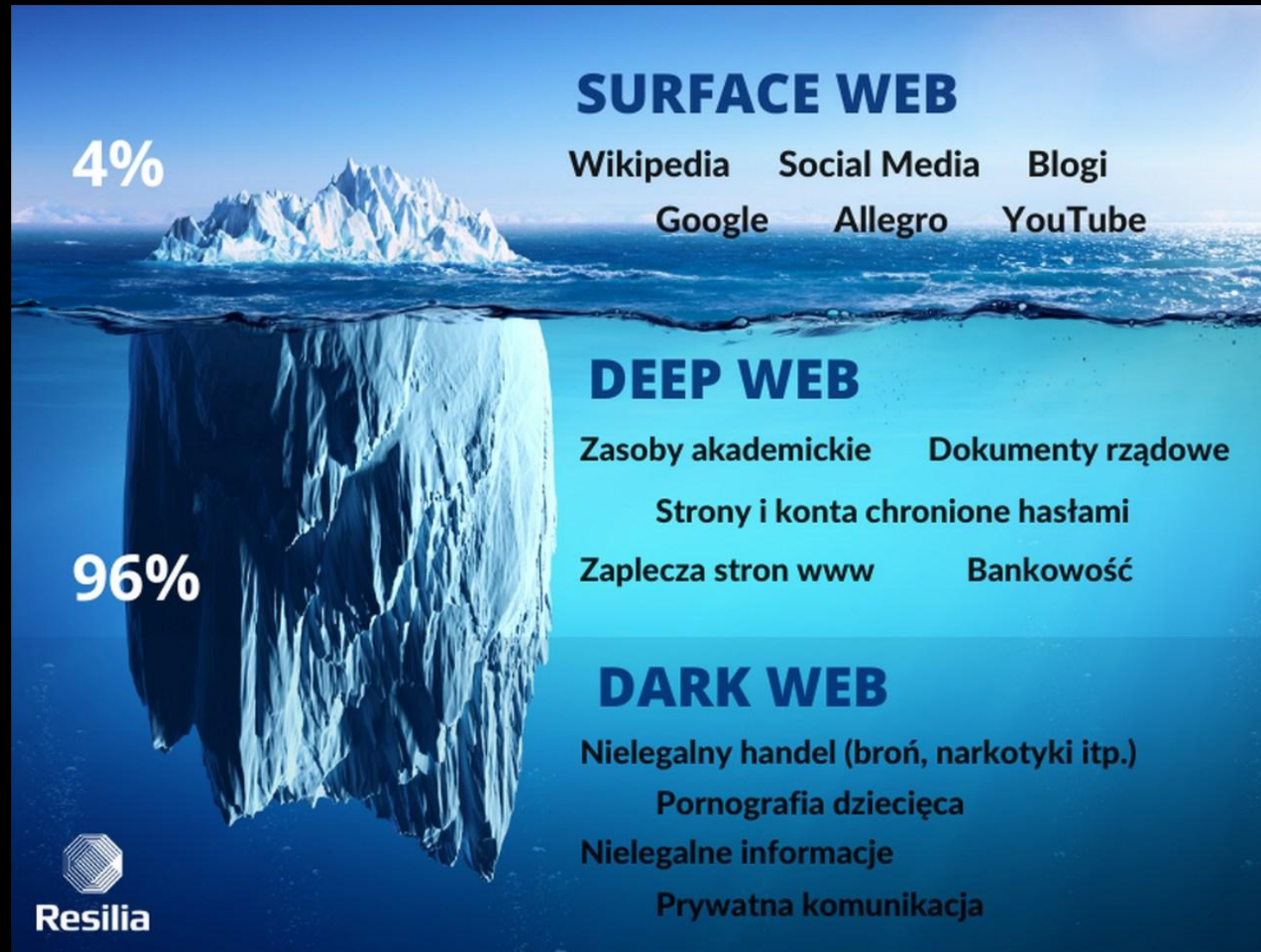
Sponsored by **Hudson Rock** – [Use Hudson Rock's free cybercrime intelligence tools to learn how Infostealer infections are impacting your business](#)

Sites | Ransom Note(s) | Activity | Worldmap | Victims (20)

Sites

FAVICON	TITLE	TYPE	AVAILABLE	LAST VISIT	FQDN
		🎯	●	2025-05-07 09:00:43.271372	hellcakbszllztlyqbjzwcdbhfrodx55wq77kmftp4bhnhsnn5r3odac
	404 Not	⚙️	●	2025-05-07 00:00:54.070570	hellcakbszllztlyqbjzwcdbhfrodx55wq77kmftp4bhnhsnn5r3odac

# Kategorie internetu





# Kategorie Intelligence

OSINT - Open Source Intelligence

SOCMINT - Social Media Intelligence

HUMINT - Human Intelligence

GEOINT - Geospatial Intelligence

IMINT - Imagery Intelligence

SIGINT - Signals Intelligence

# SOCMINT

- **SOCMINT** jest procesem gromadzenia i analizowania zebranych informacji z różnych portali społecznościowych, kanałów i grup komunikacyjnych w celu namierzenia obiektu, zebraniu o nim jak najwięcej danych cząstkowych oraz potencjalnie w celu zrozumienia jego działania.
- Wszystko po to, by analizując zebrane informacje – osiągnąć założony cel poprzez podjęcie właściwych decyzji operując jak największą liczbą zebranych i zwalidowanych danych.
- Tak wygląda ta definicja według gałęzi białe wywiadowczej.
- Jednak SOCMINT jest także wykorzystywany jako narzędzie analizy marketingowej i społecznej – w celu zrozumienia wpływu tzw. influencerów na środowisko danego portalu lub całe społeczeństwo obserwatorów (tzw. “followersów”).

<https://sekurak.pl/socmint-czyli-osint-mediow-spoecznosciowych/>

# HUMINT

- HUMINT (ang. Human Intelligence, pol. rozpoznanie osobowe) to kategoria danych rozpoznawczych lub wywiadowczych, opracowanych na podstawie informacji zbieranych i dostarczanych przez źródła osobowe.
- Podstawowym sposobem zdobywania danych wywiadowczych w ramach HUMINT są czynności związane z przeprowadzaniem rozmów z osobami mającymi dostęp do pożądanых informacji.
- HUMINT może dostarczać różne rodzaje informacji – nie tylko dotyczące operacji wojskowych, czy planów technicznych sprzętów bojowych, ale też relacji interpersonalnych i sieci interesów.
- W ścisłym rozumieniu definicji HUMINT – ze względu na swoją specyfikę – pozostaje domeną wojska, służb specjalnych i policji.

[https://rynekinformacji.pl/humint-czlowiek-jako-zrodlo-w-erze-nowych-technologii/#google\\_vignette](https://rynekinformacji.pl/humint-czlowiek-jako-zrodlo-w-erze-nowych-technologii/#google_vignette)

# GEOINT

- **Geospatial Intelligence (GEOINT)**, czyli wywiad geoprzestrzenny to wykorzystanie i analiza obrazów i informacji geoprzestrzennej do opisu, oceny i wizualizacji cech fizycznych, a także zlokalizowanych działalności na Ziemi.
- GEOINT może obejmować także gromadzenie danych z wykorzystaniem innych technik wywiadowczych – IMINT (rozpoznanie obrazowe, ang. Imaginery Intelligence), SIGINT (rozpoznanie elektromagnetyczne, ang. Signals Intelligence), MASINT (rozpoznanie pomiarowo-badawcze, ang. Measurement and Signature Intelligence) i HUMINT (rozpoznanie osobowe, ang. Human Intelligence).

<https://rynekinformacji.pl/geospatial-intelligence>

# IMINT

- **IMINT (Imagery Intelligence)** to jedna z głównych dziedzin wywiadu wojskowego, która wykorzystuje obrazy i zdjęcia satelitarne do pozyskiwania informacji o obiektach na Ziemi.
- Umożliwia zbieranie danych o terenie, obiektach wojskowych, infrastrukturze czy też ruchach wojskowych przeciwnika.
- Jest to niezwykle istotna gałąź wywiadu, która umożliwia zbieranie danych o terenie, obiektach wojskowych, infrastrukturze czy też ruchach wojskowych przeciwnika.

<https://quantico.pl/imint-imagery-intelligence-co-to-jest/>

# SIGINT

- **SIGINT**, czyli Signals Intelligence, to jeden z działów wywiadu, który specjalizuje się w zbieraniu, analizie i interpretacji sygnałów radiowych oraz elektronicznych.
- W skrócie, SIGINT zajmuje się wywiadem związanym z elektronicznymi komunikacjami, w tym z przechwytywaniem, dekodowaniem i interpretacją komunikatów radiowych, telefonicznych, internetowych oraz innych form transmisji danych.
- Głównym celem SIGINT jest pozyskiwanie informacji wywiadowczych poprzez analizę komunikacji przekazywanej za pomocą sygnałów radiowych i elektronicznych.
- Ta dziedzina wywiadu odgrywa rolę w identyfikacji, lokalizacji oraz monitorowaniu celów wywiadowczych, w tym potencjalnych zagrożeń dla bezpieczeństwa narodowego, grup terrorystycznych, czy też innych państwowych i niepaństwowych aktorów.

<https://quantico.pl/sigint-co-to-jest/>

# Facebook - Załóż profil operacyjny

Wyhoduj konto, dojrzewanie trwa około 6 miesięcy.

Zanotuj szczegóły profilu.

- zainteresowania
- spójna tożsamość e-mail z profilem (imię, nazwisko)
- udzielaj się na grupach zainteresowań
- rozbuduj sieć znajomych

<https://this-person-does-not-exist.com/en>

## Random Face Generator (This Person Does Not Exist)

Generate random human face in 1 click and download it! AI generated fake person photos: man, woman or child.

Gender:

Female

Age:

35-50 years old

Ethnicity:

White

Refresh Image





# Facebook

## - This Person Does Not Exist

Facebook i LinkedIn rozpoznają wygenerowane sztucznie zdjęcia osób.

Wygenerowane zdjęcie osoby ma układ oczu i ust w tym samym miejscu.

Należy zmodyfikować paletę barw, skorygować ułożenie twarzy.

<https://this-person-does-not-exist.com/en>





## Wyszukiwarki

<https://google.pl>

<https://yandex.com>

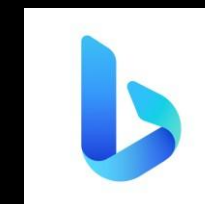
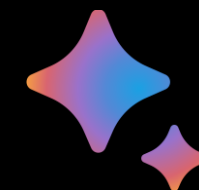


## Wsparcie AI

<https://bard.google.com/chat>

<https://chat.openai.com/>

<https://www.bing.com/?/ai=>



# Używanie operatorów w Google

Proste: „” - | OR () \*

Zaawansowane: site, filetype, inurl, intitle, intext, ext, related

Proste można łączyć: *filetype: xls | xlsx | doc*

[https://www.google.com/advanced\\_search](https://www.google.com/advanced_search)

[https://www.google.com/advanced\\_image\\_search](https://www.google.com/advanced_image_search)

<https://www.google.com/intl/pl/help/operators.html>

<https://www.exploit-db.com/google-hacking-database>





[https://www.google.com/advanced\\_search](https://www.google.com/advanced_search)

Advanced Search

Find pages with...

all these words:

this exact word or phrase:

any of these words:

none of these words:

numbers ranging from:  to

To do this in the search box.

Type the important words: tri-colour rat terrier

Put exact words in quotes: "rat terrier"

Type OR between all the words you want: miniature OR standard

Put a minus sign just before words that you don't want:  
-rodent, -"Jack Russell"

Put two full stops between the numbers and add a unit of measurement:  
10..35 kg, £300..£500, 2010..2011

Then narrow your results by...

language:

region:

last update:

site or domain:

terms appearing:

file type:

usage rights:

Find pages in the language that you select.

Find pages published in a particular region.

Find pages updated within the time that you specify.

Search one site (like wikipedia.org ) or limit your results to a domain like .edu, .org or .gov

Search for terms in the whole page, page title or web address, or links to the page you're looking for.

Find pages in the format that you prefer.

Find pages that you are free to use yourself.

Advanced Search



## Advanced Image Search

Find images with...

all these words:

this exact word or phrase:

any of these words:

none of these words:

To do this in the search box.

Type the important words: winter hoarfrost

Put exact words in quotes: "frost flower"

Type OR between all the words you want:  
trees OR weeds OR grasses

Put a minus sign just before words that you don't want:

Then narrow your  
results by...


image size:

Find images in any size you need.

aspect ratio:

Specify the shape of images.

colours in the image:

☒ any colour ☐ full colour ☐ black & white ☐ transparent ☐ this colour 

Find images in your preferred colours.

type of image:

Limit the kind of images that you find.

region:

Find images published in a particular region.

site or domain:

Search one site (like sfmoma.org ) or limit your results  
like .edu, .org or .gov

file type:

Find images in the format that you prefer.

usage rights:

Find images that you are free to use.

[Advanced Search](#)

Stale poszukuję nowych możliwości i ekscytujących wyzwań. Jeśli chcesz się ze mną skontaktować, proszę, skorzystaj z poniższych kanałów:

Email: [beata@zalnet.pl](mailto:beata@zalnet.pl)

LinkedIn: <https://www.linkedin.com/in/beatazalewa/>

Blog: <https://zalnet.pl/blog/>

X: <https://x.com/beatazalewa>

GitHub: <https://github.com/beatazalewa/Conferences/>

