PRAWDZIWA GŁĘBIA OSINT

ODKRYJ WARTOŚĆ DANYCH OPEN SOURCE INTELLIGENCE

Rae Baker

Przedmowa: Micah Hoffman

WILEY

Helion

Tytuł oryginału: Deep Dive: Exploring the Real-world Value of Open Source Intelligence

Tłumaczenie: Piotr Rakowski

ISBN: 978-83-289-0590-0

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/pragle
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

Rozdział

2

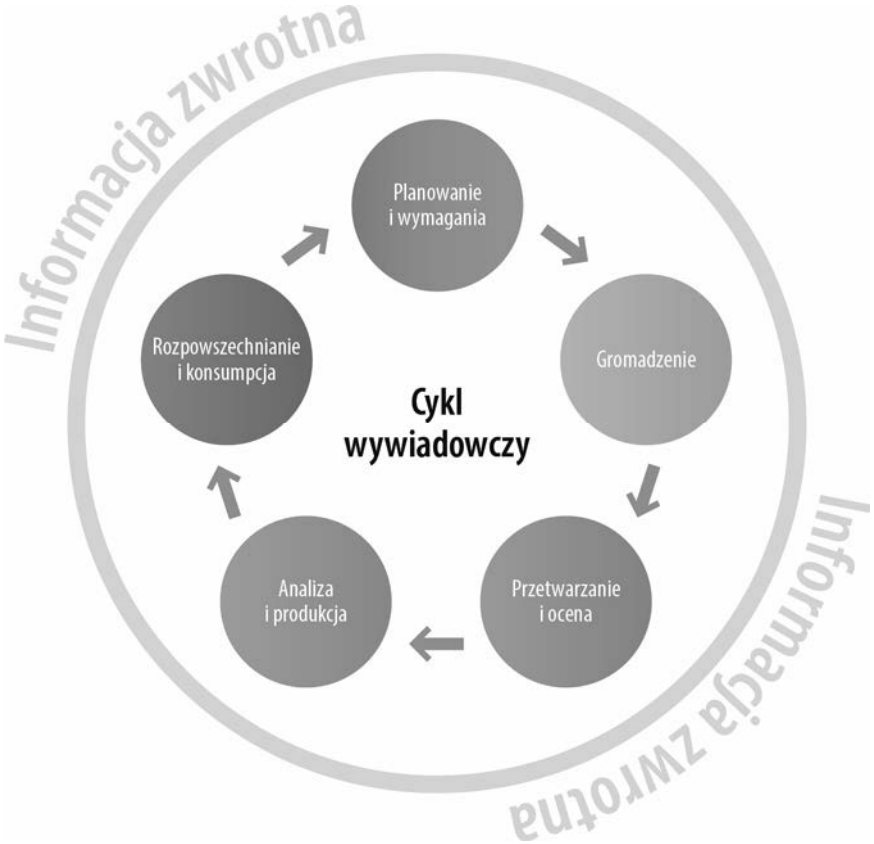
Cykl wywiadowczy

2.1. Czym jest cykl wywiadowczy?

Wywodzący się ze społeczności wywiadowczej **cykl wywiadowczy**, praktykowany w Stanach Zjednoczonych, jest wykorzystywany jako zestaw wytycznych wykorzystywany do gromadzenia i przetwarzania informacji w niezawodny i powtarzalny sposób. Cykl ten zazwyczaj składa się z pięciu kluczowych faz, począwszy od planowania, a skończywszy na rozpowszechnianiu (patrz rysunek 2.1). Jednak były wiceprzewodniczący Narodowej Rady Wywiadu (ang. *National Intelligence Council*), Mark Lowenthal, proponuje w swojej książce połączenie fazy rozpowszechniania z konsumpcją i wstawienie fazy informacji zwrotnej[1]. Sugeruje on, że kluczowi decydenci lub interesariusze nie zawsze byliby zainspirowani do tego, aby konsumować i działać na podstawie dostarczonych danych wywiadowczych, a dodanie fazy informacji zwrotnej do cyklu zmotywowałoby interesariuszy do czytania i przekazywania informacji zwrotnych analitykom.

Cykl rozpoczyna się od ustalenia potrzeb i wymagań kluczowych interesariuszy lub konsumentów danych wywiadowczych. Gdy wymagania zostaną opracowane, wymienione i uszeregowane pod względem ważności, są one wykorzystywane do inicjowania gromadzenia danych. Cykl kończy się informacją zwrotną i ponownym uruchomieniem cyklu z nowymi pytaniami uzyskanymi na końcu procesu.

[1] Mark M. Lowenthal, *Intelligence: from secrets to policy*.



Rysunek 2.1. Cykl wywiadowczy

Według Lowenthala cykl ten składa się z tych sześciu kluczowych faz:

1. Planowanie i wymagania.
2. Gromadzenie.
3. Przetwarzanie i ocena.
4. Analiza i produkcja.
5. Rozpowszechnianie i konsumpcja.
6. Informacja zwrotna.

2.2. Faza planowania i wymagań

Planowanie strategii skutecznego badania i tworzenia produktu końcowego, identyfikacja wymagań interesariuszy oraz definiowanie pytań wywiadowczych, na które chcemy odpowiedzieć poprzez gromadzenie i analizę danych, są kluczowymi elementami **fazy planowania i wymagań**. Wymagania powinny być określone przez kluczowych interesariuszy i konsumentów, którzy mają otrzymać nasze ostateczne raporty. Mówiąc prościej, musimy wiedzieć, „kto, co, dlaczego i jak"

przed rozpoczęciem procesu śledczego, i potrzebujemy, aby informacje te zostały określone przez osoby wnioskujące o dane wywiadowcze. Jako analitycy możemy być skłonni do bezpośredniego rozpoczęcia gromadzenia danych bez zebrania tych kluczowych pytań, ale może to skutkować stratą czasu w postaci gonienia za niepotrzebnymi tropami i słabymi danymi wywiadowczymi, na które nie da się zareagować.

Po jasnym zdefiniowaniu pytań otrzymanych od kluczowych interesariuszy musimy opracować plan, który obejmuje czas od fazy gromadzenia do fazy informacji zwrotnej. Plan ten wymaga odpowiedzi na kilka podstawowych pytań, w tym na następujące:

- Ilu analityków jest potrzebnych do tego projektu?
- Czy potrzebujemy wyspecjalizowanych analityków?
- Ile czasu zostanie poświęcone na proces?
- Jakie źródła danych zostaną wykorzystane?
- Czy będziemy potrzebować narzędzi do masowego gromadzenia danych, takich jak API?
- Czy są jakieś kwestie prawne lub drażliwe kwestie, o których należy pamiętać?
- Gdzie będą przechowywane dane?
- Kto będzie miał dostęp do danych?
- Jakie zagrożenia bezpieczeństwa napotkają analitycy?
- Jak będziemy współpracować?
- W jakim formacie będziemy przechowywać notatki (mapa myślowa, plik Worda itp.)?
- Jak będzie wyglądał raport końcowy?
- Czy raport będzie prezentacją, czy dokumentem?
- W jaki sposób interesariusze będą przekazywać informacje zwrotne po zapoznaniu się z raportem?

Łatwo zauważyć, w jaki sposób faza planowania i wymagań zapewnia sukces pozostałej części procesu. Jeśli ta faza jest słabo rozwinięta i wykonywana bez zaangażowania interesariuszy, następuje efekt wodospadu prowadzący do niepotrzebnego gromadzenia danych, bezproduktywnej analizy i ostatecznie przekazywania w raporcie informacji, które są bezużyteczne i nie nadają się do wykorzystania.

Na tym etapie ważne jest określenie dyscypliny wywiadowczej, której używamy do zbierania danych (HUMINT, OSINT, IMINT, SIGINT, MASINT), ponieważ często określa to sposób oceny informacji przez analityka. To rozróżnienie pomaga również określić, czy wykorzystywane są dane wywiadowcze ze wszystkich źródeł, czy z jednego źródła, co wpłynie na wiarygodność i klasyfikację produktów. Po upewnieniu się, że planowanie i wymagania zostały ustalone dla tego konkretnego dochodzenia, można przejść do następnej fazy.

2.3. Faza gromadzenia

Na tym etapie procesu powinniśmy pomyślnie zebrać pytania wywiadowcze i wymagania od interesariuszy oraz opracować i dopracować plan radzenia sobie z pozostałymi fazami. Możemy teraz przejść do prawdopodobnie najbardziej ekscytującej fazy cyklu, **fazy gromadzenia**. Jest to miejsce, w którym wcześniej ustalony plan gromadzenia danych jest wprowadzany w życie, a my, jako analitycy, mamy zwykle tendencję do odnoszenia sukcesów. Zidentyfikowane źródła danych powinny być teraz aktywne i gromadzić informacje, interfejsy API powinny być aktywne, a analitycy powinni przeszukiwać publiczne źródła danych w poszukiwaniu odpowiednich informacji. Ilość danych zebranych w tej fazie, jak również wszelkie ograniczenia prawne powinny być w całości określone przez wcześniej ustalone wymagania z pierwszej fazy i być zgodne z potrzebami kluczowych interesariuszy.

W zależności od lokalizacji, w której gromadzone są dane, możemy napotkać ograniczenia wynikające z konieczności zachowania zgodności z przepisami prawnymi i konieczne jest, abyśmy byli świadomi przepisów dotyczących gromadzenia danych osobowych w kraju, a nawet stanie, w którym działamy. W Unii Europejskiej przepisy i regulacje, takie jak *Ogólne Rozporządzenie o Ochronie Danych* (RODO), mogą być mylące. Na przykład gromadzenie danych osobowych i dziennikarskich jest w większości wyłączone z RODO, a gromadzenie danych osobowych związane z egzekwowaniem prawa podlega zasadom innym niż te, które obowiązują podmioty gromadzące dane komercyjnie[2]. Ponadto konkretne przepisy mogą być różne w poszczególnych krajach UE, co utrudnia ustalenie, co dokładnie jest legalne. RODO zawiera pewne wytyczne dotyczące gromadzenia danych, ale przed rozpoczęciem gromadzenia danych konieczne jest uzyskanie porady prawnej, aby upewnić się, że żadne przepisy nie są łamane.

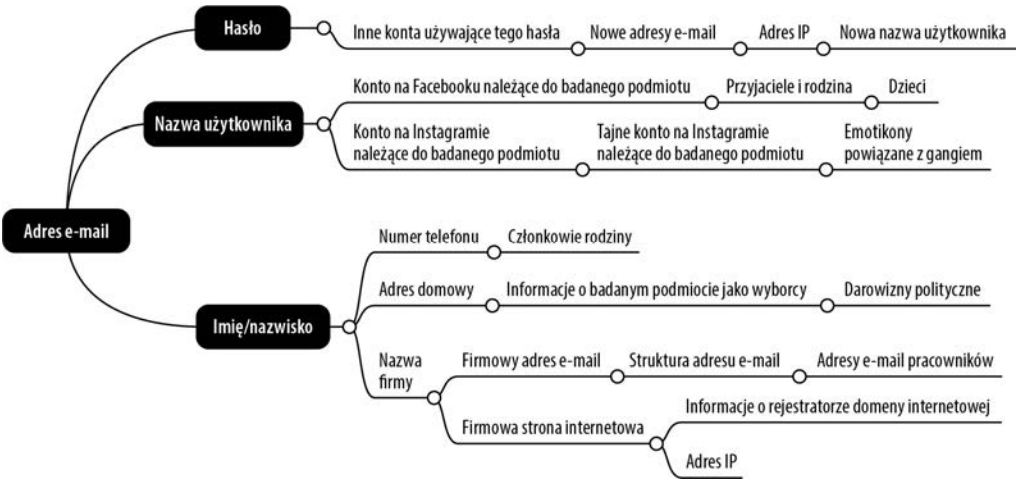
- Wymagana jest podstawa prawna przetwarzania danych osobowych.
- Podczas przetwarzania danych osobowych należy stosować pewne zasady określone w RODO.
  - Zgodność z prawem, uczciwość i przejrzystość.
  - Ograniczenie celu.
  - Minimalizacja danych.
  - Dokładność.
  - Ograniczenie przechowywania.
  - Integralność i poufność.
  - Odpowiedzialność.
- Prawa podmiotu, którego dane są przetwarzane, muszą być przewidywane, rozumiane i respektowane.
- Należy określić, czy jesteśmy administratorem danych, czy podmiotem przetwarzającym dane.

[2] *https://eur-lex.europa.eu/eli/dir/2016/680/oj.*

Metodologia gromadzenia danych może różnić się w zależności od analityków i zespołów w oparciu o ich osobiste preferencje i wymagania. Analitycy mogą zdecydować się na rozpoczęcie badań od różnych punktów wyjścia, w tym gromadzenia big data, wyników wyszukiwarek i kont w mediach społecznościowych. Bez względu na to, z jakiej metodologii korzystamy, główna technika zbierania danych, określana jako piwotowanie (ang. *pivoting*), musi być rozumiana i zintegrowana, aby śledztwo zakończyło się sukcesem.

Sztuka piwotowania

W *fazie gromadzenia* napotkamy dane, które zaprowadzą nas bezpośrednio do innych danych, które z kolei mogą wiązać ze sobą ustalenia i konta użytkowników. Ten proces podążania za śladami (dosłownie okruszkami chleba; ang. *breadcrumbs*) nazywany jest *piwotowaniem*. Umiejętność dostrzegania i wykorzystywania potencjalnych powiązań w informacjach jest nieocenioną umiejętnością, a także podstawą całego gromadzenia danych w białym wywiadzie. Ogólny przykład procesu *piwotowania* może rozpocząć się od informacji, takiej jak adres e-mail. Wprowadzając adres e-mail do narzędzi lub wyszukiwarki, możemy skorelować go z dodatkowymi danymi, takimi jak nazwa użytkownika, hasło, numer telefonu, adres, imię i nazwisko lub adres IP. Po zebraniu wszystkich tych punktów danych każdy z nich staje się teraz własnym punktem wyjścia, który doprowadzi do dalszego rozszerzenia naszego dochodzenia. W rzeczywistości każda nowa informacja jest zbudowana na poprzedniej, a po skompilowaniu opowiada nam historię. Znalezienie punktów zwrotnych wymaga jednak praktyki. Rysunek 2.2 pokazuje kilka przykładów tego, jak może wyglądać poprzednio wspomniany scenariusz e-mailowy.



Rysunek 2.2. Przykład diagramu stosowanego w piwotowaniu

Dodatkowe punkty zwrotne obejmują następujące elementy:

- Imię i nazwisko.
- Alias.
- Zagraniczne imię i nazwisko.
- Data urodzenia.
- Zdjęcie profilowe.
- Adresy e-mail.
- Hasła.
- Numery telefonów.
- Adresy.
- Zdjęcia miejsca zamieszkania.
- Nazwy użytkowników.
- Firmy.
- Współpracownicy.
- Adresy IP.
- Współmałżonek.
- Krewni.
- Dzieci.
- Informacje o pojeździe.
- Wi-fi/Bluetooth.
- Konta w mediach społecznościowych.
- Portfele walut cyfrowych.
- Szczegóły podróży.
- Zastosowana technologia.
- Domeny internetowe.
- Hobby.
- Imiona zwierząt domowych.
- Grupy w mediach społecznościowych/członkostwo.

Nauka szybkiego i skutecznego piwotowania może być formą sztuki i wymaga treningu dla naszych mózgów, aby lepiej znajdować i interpretować to, co widzimy. W swojej książce *Visual Intelligence* Amy E. Herman pisze: „Nauka dostrzegania tego, co ważne, może zmienić Twój świat". Używając dzieł sztuki jako narzędzia, Herman uczy agentów FBI, analityków wywiadu i firmy z listy Fortune 500, jak analizować i ponownie rozpatrywać sposób, w jaki wcześniej patrzyliśmy na świat. Sugerując, że musimy spojrzeć na rzeczy dwa razy, aby w pełni je zrozumieć, Herman uważa, że można to bezpośrednio zastosować do sztuki piwotowania. Korzystanie z jej metody może pomóc nam najpierw spojrzeć na coś bez wpływu z zewnątrz, a następnie ponownie w oparciu o nowe dane[3].

[3] A.E. Herman, *Visual intelligence sharpen your perception, change your life*, Mariner Books, 2017, s. 55 – 56.

1. Spójrz po raz pierwszy.
2. Zapoznaj się z innymi wcześniejszymi informacjami lub opiniami.
3. Spójrz jeszcze raz.

Herman wierzy, że często ważne szczegóły są ukryte w widocznych miejscach, a jeśli nadmiernie skupimy się na większych szczegółach, możemy przegapić to, co jest tuż przed nami. Aby zwalczyć naszą skłonność do przeoczania tego, co zwyczajne, i pomóc nam odkryć ukryte szczegóły w naszej pracy, opracowała metodę COBRA[4].

Metoda COBRA	
C (ang. *concentrate*)	*Skoncentruj* się na zamaskowanych szczegółach.
O (ang. *one*)	Rób *jedną* rzecz w danym czasie.
B (ang. *break*)	Zrób sobie *przerwę*.
R (ang. *realign*)	*Ponownie określ* swoje oczekiwania.
A (ang. *ask*)	*Poproś* kogoś, aby spojrzał na analizowany obiekt razem z Tobą.

Skoncentruj się na zamaskowanych szczegółach. Nasze mózgi są zaprogramowane tak, aby dostrzegać rzeczy, które wyróżniają się na tle innych lub nie znajdują się na swoim właściwym miejscu, co stanowi mechanizm przetrwania. Aby dostrzec rzeczy ukryte, musimy zmusić się do zwolnienia tempa i ponownego spojrzenia, rozważając to, co widzimy, bez uprzedzeń.

Rób jedną rzecz w danym czasie. Unikaj wielozadaniowości i skup się tylko na jednym zadaniu, aby uniknąć przeciążenia poznawczego. Wielozadaniowość sprawia, że jesteśmy mniej wydajni i mniej skuteczni, pozwalając informacjom umknąć naszej uwadze.

Zrób sobie przerwę. Aby zachować długoterminową koncentrację na zadaniu, musimy robić przerwy. Przeciążenie sensoryczne może prowadzić do stresu, a często oderwanie się na chwilę przed ponownym skupieniem uwagi prowadzi do przełomów.

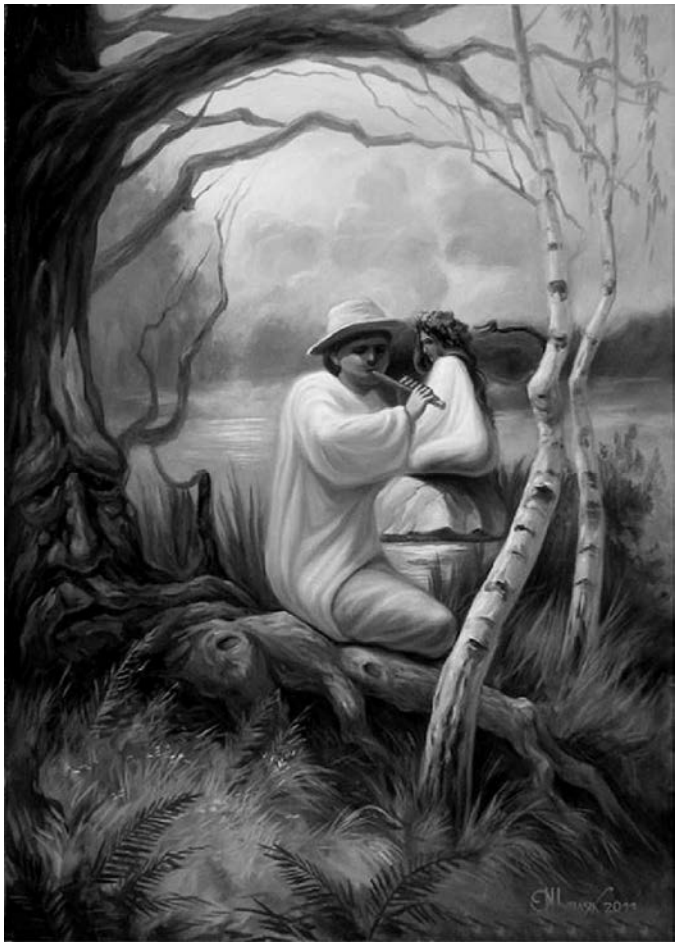
Ponownie określ swoje oczekiwania. Szukając czegoś konkretnego w naszych badaniach, narażamy się na ryzyko pominięcia informacji, które nasz mózg uważa za nieistotne. Nasza osobista stronniczość odgrywa ogromną rolę w naszych oczekiwaniach dotyczących sprawy, a korzystnie jest rozpoznać tę tendencyjność i starać się ją ominąć.

Poproś inną osobę, aby spojrzała na analizowany obiekt razem z Tobą. Ponieważ każdy patrzy na świat przez inny pryzmat, pomocne może być uzyskanie różnych opinii i punktów widzenia na naszą pracę. Szukaj wglądu w sprawę ze strony kogoś o innym pochodzeniu, opiniach i perspektywie niż Twoja własna, bo to może doprowadzić do przełomu.

[4] *Ibid.*, s. 97 – 102.

Ciągła nauka jest niezbędna dla analityków OSINT. Powinniśmy trenować nasze umysły, aby pozostały bystre i otwarte nie tylko na małe, skomplikowane szczegóły w danej sytuacji, ale także na większe, bardziej oczywiste rzeczy. Jeśli na przykład spojrzymy na mały fragment jednego z obrazów iluzji optycznej ukraińskiego malarza Olega Szuplaka[5], zobaczymy coś, co wydaje się być mężczyzną siedzącym na kłodzie i grającym na instrumencie, podczas gdy kobieta siedzi obok i słucha.

Powiększenie obrazu w celu spojrzenia na całość ujawnia jednak coś ekscytującego, ponieważ wszystkie elementy obrazu zaczynają się wizualnie łączyć. Gdybyśmy spojrzeli tylko na jedną małą część obrazu, przegapilibyśmy, że mężczyzna i kobieta są częścią większej iluzji optycznej tworzącej twarz:



[5] *https://www.tuttartpitturasculturapoesiamusica.com/2012/04/oleg-shuplyak-1967-mighty-optical.html.*

Nie ruszajmy się jeszcze! Ten obraz ma jeszcze jeden ukryty element do znalezienia. Chociaż skupiliśmy się na dwóch głównych obiektach na obrazie, a także na szerszym złudzeniu optycznym twarzy osoby ukrytej w elementach, wciąż jest jeszcze jedna twarz do znalezienia. Przyglądając się bliżej drzewu na obrazie, można zobaczyć ukrytą twarz w korze drzewa.

Celem tego ćwiczenia jest pomoc w zrozumieniu, że podczas śledztwa nie zawsze musimy skupiać uwagę na drobnych szczegółach lub szerszym obrazie, ale raczej ważyć te dwa elementy w równym stopniu, aby zapobiec przeoczeniu kluczowych szczegółów, które mogą znajdować się tuż przed naszymi oczami. Nauka identyfikowania ważnych danych i poruszania się po nich może być bardzo pracochłonna. Warto zauważyć, że praca nad piwotowaniem może być zautomatyzowana i zlecona na zewnątrz narzędziom, które mogą gromadzić duże ilości danych z wielu źródeł i korelować je za pomocą algorytmów lub technologii sztucznej inteligencji. Drogie narzędzia do automatyzacji mogą oferować wiele nowych punktów danych do zbadania; jednak bez żywych analityków, którzy nadadzą sens korelacjom i stworzą produkt wywiadowczy z informacji, gromadzenie danych jest bezużyteczne.

Jako instruktor na kilku profesjonalnych kursach OSINT i bootcampach nauczyłam się, że koncepcja piwotowania danych jest najtrudniejszą, ale najważniejszą umiejętnością dla nowych adeptów białego wywiadu. Często szkolenie studenta w zakresie korzystania ze złożonych narzędzi do gromadzenia danych może być łatwiejsze niż nauczenie kogoś, jak być dociekliwym i myśleć krytycznie. Podczas gdy umiejętności techniczne są oczywiście poszukiwane, często pomijamy wartość umiejętności miękkich, kreatywnego myślenia i innowacyjności. Niektórym analitykom myślenie analityczne przychodzi naturalnie, ale pocieszające powinno być to, że umiejętności tych można się nauczyć poprzez praktykę. Poniżej znajduje się kilka ćwiczeń, które pomogą Ci wzmocnić umiejętności analitycznego myślenia i piwotowania.

Opracuj raport na swój temat. W tym ćwiczeniu wykorzystaj własne informacje, aby sprawdzić, ile Twoich danych osobowych jest dostępnych w ogólnodostępnych źródłach.

- Ile informacji na swój temat można znaleźć, korzystając jedynie ze swego osobistego adresu e-mail i wyszukiwarki internetowej?
- Czy znalazłeś jakieś swoje osobiste nazwy użytkownika lub konta w mediach społecznościowych?
- Czy można znaleźć jakieś oficjalne dane, takie jak informacje o głosowaniu lub zakupie domu? Co te dane ujawniły na Twój temat i jak można było je wykorzystać?

Opracowanie raportu na temat firmy. Wybierz dowolną firmę do tego ćwiczenia i spróbuj odpowiedzieć na następujące pytania, które mogą pomóc w napisaniu raportu OSINT:

- Czy możesz określić firmową strukturę nazewnictwa adresów e-mail, taką jak *imię.nazwisko@email.com* lub *inicjałimienia.nazwisko@email.com*?
- Czy korzystając ze struktury nazewnictwa z ostatniego pytania, potrafisz użyć wyszukiwarki do zlokalizowania dodatkowych firmowych adresów e-mail?
- Jakie inne informacje na temat tej firmy i jej pracowników możesz znaleźć na portalach społecznościowych, takich jak LinkedIn?

Odkrywanie informacji o nazwie użytkownika. W tym ćwiczeniu użyj jednej ze swoich osobistych nazw użytkownika i spróbuj odpowiedzieć na poniższe pytania:

- Uruchom wyszukiwanie w narzędziu internetowym do tworzenia list wystąpień nazwy użytkownika, takim jak *whatsmyname.app*. Ile kont używa tej nazwy użytkownika?
- Czy wszystkie konta wymienione w *whatsmyname.app* należą do Ciebie?
- Czy używając prefiksu adresu e-mail jako nazwy użytkownika, możesz znaleźć dodatkowe konta należące do użytkownika? Na przykład, jeżeli mamy adres *Email123@example.com*, ***Email123*** jest prefiksem, który możesz wyszukać jako nazwę użytkownika.
- Jakie inne dane są dostępne na bazie każdego znalezionego konta w mediach społecznościowych? Czy możesz znaleźć datę urodzenia? Czy były tam jakieś aktualne zdjęcia? Czy były jakieś zdjęcia z numerem domu?

Pokonywanie wyzwań związanych z OSINT

Nawet najlepsi analitycy OSINT mogą natknąć się na blokady w przypadkach, w których po prostu nie mogą osiągnąć postępu lub znaleźć użytecznych punktów zwrotnych. Często przychodzi taki moment w dochodzeniu, gdy czujemy, że sprawdziliśmy wszystkie możliwe tropy lub że nasza normalna strategia poszukiwań nie działa. W takich przypadkach najlepszą lekcją, jakiej nauczyłam się, rozpoczynając pracę w tej branży, jest to, że *brak informacji jest nadal informacją*. Chodzi o to, że czasami po prostu nie ma danych i bez względu na to, jak bardzo będziemy szukać, nigdy ich nie znajdziemy, co czasami może być frustrujące, ale brak danych może być anomalią, którą należy zgłosić, gdy spojrzymy na cały obraz naszego dochodzenia.

Jeśli brak danych nie jest możliwy i wiesz, że z dochodzenia można wydobyć dalsze informacje, technika RESET i analiza luk są świetnymi metodami pomagającymi usunąć tzw. mgłę mózgową i utrzymać analityków na ścieżce postępu.

Technika RESET

Na blogu grupy non profit *The OSINT Curious Project* Nico Dekens opisuje, jak wykorzystać technikę RESET do „restartu" i oczyszczenia mózgu, co ma na celu ułatwienie przeprowadzania lepszych analiz[6]. Technika ta jest fantastycznym sposobem na wzięcie mentalnego „oddechu" i pozwolenie przeciążonemu umysłowi na otwarcie się na nowe możliwości i ścieżki eksploracji. Poniżej znajduje się pięć kroków, które mogą pomóc naszemu mózgowi ominąć blokady pojawiające się w trakcie śledztwa.

[6] *https://osintcurio.us/2021/02/09/using-reset-for-better-osint*.

Rutyna (***R**outine*)	Zamiast popadać w rutynę, wykonując te same procesy w ten sam sposób przy każdym śledztwie, prowadź listę i zapisuj nowe pomysły, gdy tylko się pojawią. Utrzymywanie stale ewoluującego sposobu pracy pomoże zachować świeżość pomysłów.
Emocje (***E**motions*)	Dobrą praktyką jest umiejętność radzenia sobie z własnymi emocjami, zwłaszcza podczas traumatycznych dochodzeń o wysokiej stawce. Zapisywanie naszych uczuć i myśli może pomóc w zapobieganiu stronniczości i tunelowemu widzeniu, które mogą mieć wpływ na rozwiązywaną sprawę.
Odcięcie (***S**ever*)	Zerwij mentalne powiązania z pracą i odsuń się od sprawy. Czas spędzony z dala od śledztwa i komputera sprawi, że umysł poczuje się odświeżony i będzie w stanie efektywniej przetwarzać dane.
Eksploruj (***E**xplore*)	Poświęć czas na odkrywanie i naukę poza bieżącymi obowiązkami. Sprawdź nowe narzędzie i spróbuj czegoś nowego!
Myśl (***T**hink*)	Staraj się nie budować murów wokół swojego umysłu i pozwól mu marzyć i szaleć. Często wolność do marzeń bez granic może inspirować nowe i odświeżające pomysły.

Analitycy powinni przechodzić przez etapy techniki RESET, gdy czują się zablokowani lub szukają nowego spojrzenia na sytuację. Jednym ze sposobów, w jaki wdrożyłam RESET, jest wstanie od biurka i odbycie 30-minutowego spaceru. Mentalne oderwanie się od pracy zazwyczaj pomaga w uzyskaniu nowej perspektywy. RESET to świetna metoda na zresetowanie umysłu, ale istnieje inna technika zwana analizą luk, której możemy użyć do analizy dużej ilości informacji i szybkiego nadania im sensu.

Analiza luk

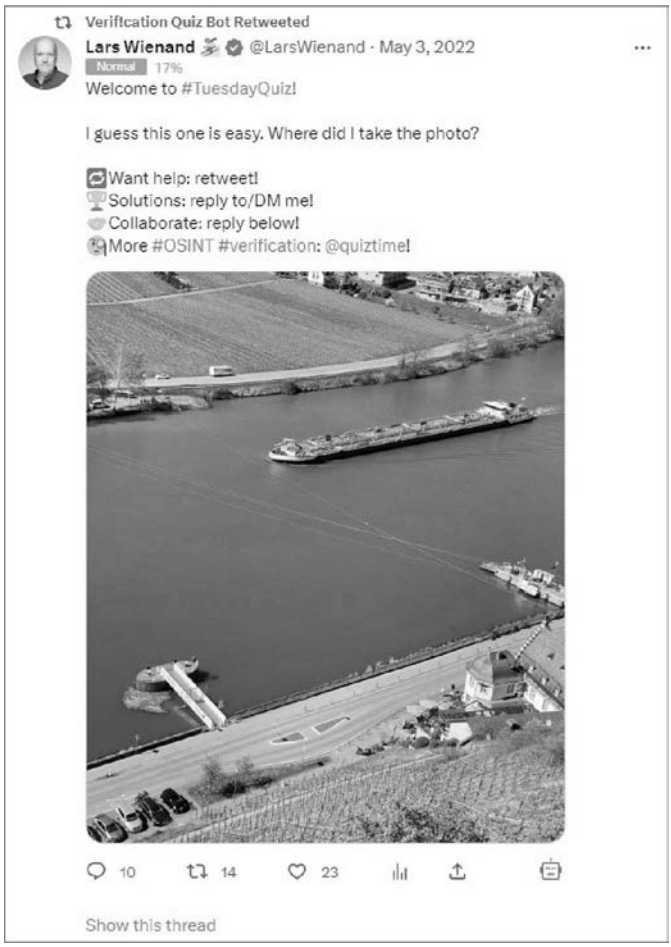
Analiza luk jest techniką, którą można zastosować do metodycznego rozbicia badania poprzez zadawanie pytań mających pomóc w ocenie całości informacji, a następnie zidentyfikowanie luk w naszej wiedzy[7]. Poniżej przedstawiłam cztery główne pytania stosowane w analizie luk:

1. Co już wiem?
2. Co to oznacza?
3. Co jeszcze muszę wiedzieć?
4. Jak mogę się tego dowiedzieć?

Zaletą stosowania metody analizy luk jest to, że pozwala nam ona szybko wyszczególnić dużą ilość informacji do postaci czegoś bardziej uporządkowanego i łatwiejszego w zarządzaniu.

[7] *https://nixintel.info/osint/using-gap-analysis-to-keep-osint-investigations-on-track*.

Przykład analizy luk. Korzystając z metodologii analizy luk opartej na czterech pytaniach, rozwiążmy quiz geolokalizacyjny opublikowany przez Larsa Wienanda[8] na koncie Quiztime na Twitterze[9]. Quiz jest obrazem statku znajdującego się na zbiorniku wodnym, a Lars prosi nas o odpowiedź na pytanie: „Gdzie zrobiłem to zdjęcie?". Możemy zacząć od rozbicia na czynniki pierwsze tego, co już wiemy o tym zdjęciu.



Co już wiem? Udostępniony obraz przedstawia wydłużoną łódź płynącą ze wschodu na zachód po spokojnym akwenie. Flaga Niemiec powiewa na molo w prawym dolnym rogu obrazu, a także na rufie statku. Statek ma nazwę *Temptation* widoczną na dziobie, wraz z nierozróżnialnym logo. Po obu stronach drogi wodnej znajdują się drogi lądowe; jedna wydaje się prowadzić przez miasto, a druga droga obejmuje ścieżkę rowerową. W dolnym rogu znajduje się konstrukcja ze szklanym sufitem, a na podstawie parasoli i miejsc do siedzenia na zewnątrz możemy wnioskować,

[8] *https://twitter.com/LarsWienand*.

[9] *https://twitter.com/quiztime*.

że może to być restauracja. Oba obszary roślinności na zdjęciu wydają się być polami uprawnymi; w oparciu o rozmieszczenie roślin możemy zakładać, że może to być winnica.

Co to oznacza? Dane, które znaleźliśmy, oznaczają, że zdjęcie najprawdopodobniej zostało wykonane w Niemczech, w pobliżu drogi wodnej używanej zarówno do podróży, jak i rekreacji. Drogi i winnica leżą po obu stronach wody, z restauracją w prawym dolnym rogu i czymś, co wydaje się być pasem drogowym przeznaczonym na ścieżkę rowerową. Wszystkie te informacje wskazują na to, że jest to prawdopodobnie miejsce turystyczne.

Co jeszcze muszę wiedzieć? Nadal musimy wiedzieć, jak nazywa się restauracja lub miasto.

Jak mogę się tego dowiedzieć? Możemy zacząć od wyszukania nazwy statku w bezpłatnych bazach danych służących do śledzenia statków morskich, takich jak VesselFinder[10], aby dowiedzieć się, dokąd dany statek zmierzał lub dokąd często pływa. Korzystając ze zdjęć satelitarnych uzyskanych z Google Earth[11], możemy metodycznie przeszukiwać Niemcy w poszukiwaniu dróg wodnych, które mają również drogę lądową i winnicę znajdujące się po obu stronach. Korzystanie z technik odwrotnego wyszukiwania obrazu na oryginalnym obrazie może potencjalnie prowadzić do podobnych zdjęć, które ujawniają miasto lub możliwe do zidentyfikowania cechy pod innym kątem.

[10] *https://www.vesselfinder.com*.

[11] *https://earth.google.com/web*.

Korzystając z techniki analizy luk, możemy ustalić, że lokalizacja oryginalnego zdjęcia Quiztime została ustalona dla miejscowości Beilstein i zamku Metternich nad rzeką Mozelą w Niemczech[12]. Podejście polegające na systematycznym dzieleniu wyzwania na małe, łatwo przyswajalne części, dzięki czemu możemy skupić się tylko na istotnych informacjach, jest nie tylko świetne w przypadku dużych, nadrzędnych pytań badawczych, ale może być również wykorzystane do odpowiedzi na każde pytanie, które pojawi się podczas naszej analizy.

Dlaczego mamy tak dużo danych

W 2009 roku, wraz z rozwojem smartfonów i portali społecznościowych, skoordynowana sieć dziennikarstwa obywatelskiego zaczęła koncentrować się na protestach przeciwko irańskiemu reżimowi[13]. Korzystając z mediów społecznościowych i forów, obywatele byli w stanie skutecznie ominąć nakazaną przez rząd blokadę komunikacji i protestować w otwartym internecie, gdzie reszta świata mogła być tego świadkiem. Ta sieć dziennikarzy obywatelskich zdolnych do manipulowania komunikacją doskonale ilustruje, w jaki sposób połączenie między technologią a komunikacją pozwoliło na szybką ekspansję internetu, z ogromną liczbą 64,2 zetabajtów danych tworzonych lub replikowanych w roku 2020[14] i szacowaną liczbą 175 ZB do roku 2025[15]. Ponieważ większość istniejących danych składa się z danych osobowych, które są przenoszone i przechowywane, stały się one źródłem otwartych informacji, które można pozyskiwać, analizować i przekształcać w dane wywiadowcze.

Sama ilość danych dostępnych w otwartych źródłach jest wyjątkowo przydatna do badań OSINT, ale jest także największą przeszkodą w ich gromadzeniu. Przydzielanie ludziom zadań ręcznego zbierania i analizowania zetabajtów informacji nie tylko przeciążyłoby nasze zbiory, ale także z mniejszym prawdopodobieństwem przyniosłoby użyteczne wskazówki. Ta bariera w gromadzeniu danych jest doskonałym przykładem sytuacji, w której użycie narzędzia może usprawnić pracę analityka. Aby zmniejszyć obciążenie związane z ręcznym zbieraniem użytecznych danych, możemy użyć narzędzi takich jak agregatory danych, interfejsy API i roboty indeksujące.

Agregator danych. *Agregator danych* gromadzi, przetwarza i tworzy pakiety danych pochodzących z jednego lub większej liczby źródeł i przedstawia je w użyteczny sposób do wykorzystania przez ludzi. Kilka popularnych agregatorów danych często używanych do wyszukiwania osób to Lexis Nexis[16], Tracers[17], i Pacer[18].

[12] One Million Places.com, *https://one-million-places.com/en/germany/beilstein-castle-metternich-sleeping-beauty-of-the-moselle/* [dostęp: 15 lutego 2023 r.].

[13] *https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence*.

[14] *https://www.idc.com/getdoc.jsp?containerId=US46410421*.

[15] *https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf*.

[16] *https://www.lexisnexis.com*.

[17] *https://www.tracers.com*.

[18] *https://pacer.uscourts.gov*.

Interfejs programowania aplikacji (API) to interfejs łączący dwa elementy oprogramowania (lub nawet dwa programy) i zapewniający programistom zestaw reguł pozwalający na łączenie się z docelowym oprogramowaniem i modyfikowanie jego działania na własny użytek. Poniżej znajduje się kilka przykładów popularnych usług, które są często integrowane z innymi narzędziami za pośrednictwem ich API:

- Shodan[19],
- VirusTotal[20],
- Dehashed[21],
- EmailRep[22],
- Greynoise[23],
- IntelligenceX[24].

Crawlery sieciowe w procesie znanym jako *crawling*, *crawlery sieciowe* przeszukują internet w poszukiwaniu danych publicznie dostępnych, takich jak linki, nazwy i e-maile. Gdy crawler zidentyfikuje nowe witryny lub zasoby, pobierze dane lub dosłownie „zeskrobie" (ang. *scrapping*) je z internetu, wzbogacając je o dane osobowe zebrane z witryn indeksujących. Poprzez techniki *crawlingu* i *scrappingu* internetu witryny indeksujące, takie jak witryna wyszukująca nieruchomości Zillow[25] i witryna wyszukująca osoby That'sThem[26], są w stanie łączyć wiele źródeł w celu budowania swoich baz danych. Niektóre popularne płatne narzędzia do „crawlowania" stron internetowych używane w OSINT to Pipl[27], Spiderfoot[28] i Skopenow[29].

Pozyskiwanie danych ze stron internetowych (ang. *Web scrapping*) jest kontrowersyjną kwestią i chociaż wiele zastosowań przypisuje się dziennikarzom, badaczom i archiwistom, firmy zajmujące się sztuczną inteligencją przyznały się do pozyskiwania miliardów zdjęć z mediów społecznościowych w celu wykorzystania ich w oprogramowaniu do rozpoznawania twarzy[30]. Pomimo oczywistych konsekwencji dla prywatności w kwietniu 2022 r. Sąd Najwyższy Stanów Zjednoczonych potwierdził, że *scrapping* publicznie dostępnych danych nie jest nadużyciem ustawy o oszustwach i nadużyciach komputerowych CFAA (ang. *Computer Fraud and Abuse Act*)[31].

[19] *https://www.shodan.io*.

[20] *https://www.virustotal.com*.

[21] *https://www.dehashed.com*.

[22] *https://emailrep.io*.

[23] *https://www.greynoise.io*.

[24] *https://intelx.io*.

[25] *https://www.zillow.com*.

[26] *https://thatsthem.com*.

[27] *https://pipl.com*.

[28] *https://www.spiderfoot.net*.

[29] *https://www.skopenow.com*.

[30] *https://www.theguardian.com/technology/2022/may/25/techscape-clearview-ai-facial-recognition-fine*.

[31] *https://techcrunch.com/2022/04/18/web-scraping-legal-court*.

Kolejnym ograniczeniem podczas korzystania z technologii big data w naszej analizie jest to, że mając tak wiele danych na wyciągnięcie ręki, ryzykujemy dostrzeżenie znaczących wzorców tam, gdzie ich nie ma[32]. Ten rodzaj błędu percepcji został zdefiniowany przez niemieckiego neurologa Klausa Conrada jako **apofenia** lub **iluzja klastrowania**. W badaniu opublikowanym w 2018 r. w „The European Journal of Social Psychology" stwierdzono, że apofenia może dokładnie wyjaśniać rozwój teorii spiskowych[33]. Aby uniknąć apofenii w naszej własnej pracy, możemy pozostać świadomi naszej potencjalnej stronniczości lub uprzedzeń i szukać informacji zwrotnych od współpracowników. Pomimo tych potencjalnych wyzwań związanych z big data jedną wielką zaletą tej technologii jest to, że dane można sortować, przeszukiwać i dostarczać szybko i spójnie do użytkownika końcowego.

Usprawniony proces pozyskiwania danych przy użyciu big data znacznie skraca czas gromadzenia danych, umożliwiając szybsze ich opracowywanie i analizę po stronie użytkownika. Dodatkowo poziom oceny ryzyka związanego z analizą zagrożeń i alerty dotyczące anomalii są często stosowane do zebranych punktów danych w wielu gotowych narzędziach do indeksowania stron internetowych, które wskażą analitykowi najważniejsze ustalenia do natychmiastowego zbadania. Możliwość wzbogacenia i połączenia wielu zbiorów danych w jeden jest tylko wisienką na torcie. Musimy jednak wziąć pod uwagę odpowiedzialność związaną z posiadaniem tak dużego zbioru danych osobowych.

Jako analitycy pracujący z dużymi ilościami danych osobowych ponosimy odpowiedzialność etyczną, a w przypadku RODO — odpowiedzialność prawną, nakazującą zawęzić nasz zbiór tylko do danych wymaganych do spełnienia wymagań interesariuszy. Zasada ograniczania gromadzenia danych tylko do tego, co jest konieczne i istotne dla pierwotnego żądania, znana jest jako **minimalizacja danych**. W praktyce oznacza to, że musimy być bardzo ukierunkowani w naszych strategiach gromadzenia i przechowywania danych. Na przykład, jeśli początkowym żądaniem jest ustalenie, czy nasz podmiot podróżował z punktu A do punktu B, nie powinniśmy mieć rzeczywistej potrzeby gromadzenia 10-letnich danych osobowych o naruszaniu przepisów przez podmiot. W przypadku, gdy nie jesteśmy w stanie zminimalizować gromadzenia danych, powinniśmy dążyć do usunięcia wszelkich niepotrzebnych danych osobowych z naszej dokumentacji i naszych systemów po udzieleniu odpowiedzi na zapytanie.

2.4. Metody dokumentacji

Dokumentacja odnosi się do procesu, w którym katalogujemy i przekazujemy informacje. Mówiąc prościej, jest to sposób, w jaki będziemy przechwytywać nasze notatki podczas dochodzenia. Notatki mogą być wykorzystywane wyłącznie do organizowania naszych myśli, a w przypadku organów ścigania lub prywatnych dochodzeń mogą być wykorzystywane jako dowód. Powinieneś zacząć dostrzegać, jak właściwe przygotowanie i organizacja są kluczem do spełnienia naszych wymagań dochodzeniowych.

[32] danah boyd, Kate Crawford, *Critical Questions For Big Data*, „Information, Communication & Society", 15, 5, 2012, s. 662 – 679, *doi: 10.1080/1369118X.2012.678878*.

[33] J.-W. van Prooijen, *The Psychology of Conspiracy Theories*, Taylor & Francis, 2018.

Skuteczna dokumentacja zaczyna się od uchwycenia potrzeb i wymagań interesariuszy. Bez znajomości pytań, na które musimy odpowiedzieć, lub danych, które interesariusz chce zobaczyć (i przedstawić jako dowód), poniesiemy porażkę, zanim jeszcze zaczniemy. Niezorganizowane notatki mogą okazać się kosztowne dla interesariusza, jeśli analitycy będą musieli powtórzyć badania z powodu utraty szczegółów. Ustalenie jasnych wymagań dotyczących sposobu kompilowania i organizowania danych z wyprzedzeniem może pomóc w organizacji; mogą również istnieć przepisy dotyczące gromadzenia danych w danym kraju lub stanie, których należy przestrzegać. Po otrzymaniu i zrozumieniu wymagań możemy przejść do najlepszych praktyk w zakresie sporządzania notatek.

Techniki sporządzania notatek przez osoby przechwytujące informacje są zwykle indywidualne. Na przykład osoba ucząca się wzrokowo może preferować zapisywanie zrzutów ekranu, podczas gdy osoba ucząca się słuchowo może używać cyfrowego dyktafonu do zbierania myśli. Niezależnie od tego, jak zdecydujemy się udokumentować nasze odkrycia, konieczne jest rozważenie poniższych kwestii.

Notatki muszą być:

- Jasne i łatwe do zrozumienia *przez nas*.
- Jasne i łatwe do zrozumienia *przez innych*.

Ponieważ łatwo jest dać się wciągnąć w ekscytujący proces przeglądania ustaleń OSINT, prawdopodobnie wszyscy jesteśmy winni wrzucania notatek do dokumentacji z całkowitym lekceważeniem organizacji i struktury. Pod koniec dochodzenia z pewnością przeoczymy coś ważnego i będziemy musieli podzielić się naszymi żenująco zwichrzonymi notatkami z naszym zespołem lub, co gorsza, z szefem. Wyobraźmy sobie następujący scenariusz dochodzenia:

Analityk ma za zadanie znaleźć konkretny zestaw szczegółów na z góry określony temat w ciągu miesiąca. Przechodzi przez wszystkie etapy cyklu wywiadowczego; gromadzi wymagania interesariuszy i odpowiednio planuje swoje śledztwo. Dobrze przeprowadzona faza gromadzenia pozwala zespołowi przetwarzać i analizować wszystkie dane oraz sfinalizować je ładnie napisanym raportem, który jest rozpowszechniany w FBI. Jednak podczas fazy informacji zwrotnej FBI wyraża zainteresowanie osobą wymienioną w raporcie i pyta, w jaki sposób analityk znalazł tę informację.

W panice analityk wraca, by przeszukać swoje notatki tylko po to, by zdać sobie sprawę, że nigdy dokładnie nie udokumentował kroków, które podjął w celu znalezienia osoby będącej przedmiotem zainteresowania. Teraz musi wrócić do FBI i albo przyznać, że nie ma notatek, albo poprosić o dodatkowe godziny na ponowne przeprowadzenie badań. Niestety, z powodu opóźnienia okno czasowe na złożenie dokumentów w sądzie zostało już zamknięte, a FBI nie może już prowadzić sprawy.

Przykład ten może wydawać się ekstremalny dla celów zilustrowania znaczenia organizacji, ale faktem jest, że taki scenariusz może być bardzo realną możliwością, gdy mamy do czynienia z dochodzeniami, w których szczególnie liczy się czas. Dokładność naszych notatek ma kluczowe znaczenie dla skutecznego prowadzenia dochodzenia, a staje się to bardziej widoczne podczas współpracy z innymi analitykami.

Mogą również wystąpić sytuacje, w których nasze notatki muszą być swobodnie udostępniane w zespole w czasie rzeczywistym za pomocą platformy do robienia notatek, takiej jak OneNote, lub po prostu poprzez udostępnianie dokumentu Worda. Zaletą tego rodzaju współpracy jest to, że może ona generować nowe leady ze względu na różne tła i perspektywy, które każdy analityk wnosi do zespołu. Każdy analityk patrzy na te same dane i powiązania przez inny pryzmat w oparciu o swoje doświadczenia życiowe. Dlatego też posiadanie zespołu, który może wspólnie analizować dane, zapewnia nowe możliwości piwotowania i może inspirować rozwój nowych podejść do gromadzenia danych.

Niestety, przy tak wielu „rękach w puli" notatki dotyczące współpracy szybko stają się chaotyczne i zdezorganizowane, co może powodować, że analitycy będą zmagać się ze zmęczeniem danymi, nie mając wyraźnego punktu zaczepienia, od którego mogliby rozpocząć pracę. W takim przypadku analitycy mogą gromadzić własny zestaw notatek i wchodzić w interakcje z notatkami zespołu tylko wtedy, gdy jest to konieczne, negując ogólne korzyści płynące ze współpracy zespołowej. Aby zapobiec dezorganizacji, należy z wyprzedzeniem uzgodnić styl lub grupa może wyznaczyć lidera, który nadzoruje koordynację wszelkich sporządzonych notatek. Ponadto, jeśli dochodzenie nie ma ograniczeń dotyczących automatycznych narzędzi do zbierania danych, mogą one oferować rozwiązanie dla organizacji.

Zautomatyzowane narzędzia przeglądarkowe oparte na Chromium, takie jak Hunchly i Vortimo, mogą być używane zarówno jako mechanizmy gromadzenia, jak i dokumentowania; dzięki temu analityk ma więcej czasu na analizę i mniej czasu na przekopywanie się przez setki otwartych kart przeglądarki, aby znaleźć to, czego potrzebuje. Zautomatyzowane narzędzia nie tylko ułatwiają zbieranie obrazów, wycinków i tekstu, ale także pomagają w oznaczaniu elementów i oferują miejsce do robienia szczegółowych notatek, podczas gdy my kontynuujemy przeglądanie. Po zakończeniu możemy po prostu przejrzeć nasze notatki, tagi i linki w tych narzędziach i wygenerować raport na podstawie zebranych szczegółów.

W zależności od złożoności naszej sprawy konieczne może być uwzględnienie wizualizacji w naszych notatkach, takich jak mapy myśli, diagramy i wykresy. Każdy rodzaj wizualizacji powinien służyć określonemu celowi, gdy przeglądamy naszą własną dokumentację. Zrozumienie jednostek, linków i atrybutów w trakcie dochodzenia jest znacznie łatwiejsze, gdy możemy je wyświetlić na diagramie analizy linków. Z drugiej strony mapy myśli mogą być używane do rozszyfrowania połączeń i zobaczenia punktów zwrotnych (ang. *pivotpoints*) między punktami danych.

Podczas gdy metody dokumentowania i przechwytywania danych zasadniczo podlegają osobistym preferencjom, rozsądnie byłoby przetestować kilka różnych podejść, aby zobaczyć, które z nich można zastosować najbardziej efektywnie. Musisz mieć na uwadze konkretny przypadek użycia, a także wziąć pod uwagę potencjalną współpracę, która może być konieczna między członkami zespołu lub zespołami. Poniżej przedstawiłam kilka ważnych wskazówek i technik dotyczących dokumentacji stosowanych przez społeczność OSINT:

- Zawsze zakładaj, że notatki będą udostępniane.
- Dołączaj zrzuty ekranu z opisami.
- Zapisuj adresy URL i źródła, które przechwytujesz.
- Używaj nieaktywnych lub wyłączonych linków do stron źródłowych.
- Dołączaj tabele, aby uporządkować selektory.

- Dokumentuj procesy i kroki piwotowania.
- Zapisuj daty i godziny.
- Wyjaśniaj, co zrobiłeś i jak to zrobiłeś.

Dokument edytora tekstu. Jest to dokument tekstowy, który wygląda tak samo na komputerze jak w druku. Istnieje wiele różnych rodzajów oprogramowania używanego do przetwarzania tekstu, w zależności od tego, czy korzystasz z komputera Mac, PC, czy systemu opartego na chmurze. Powszechnie używane edytory dokumentów tekstowych obejmują Microsoft Word, Google Docs i LibreOffice.

Zalety: łatwe w użyciu i dostępne.

Wady: uciążliwe w przypadku dużych dochodzeń, trudne do zorganizowania podczas udostępniania między zespołami.

Arkusze kalkulacyjne. Arkusze kalkulacyjne pozwalają analitykom na tabelaryzację, organizowanie, analizowanie i przeprowadzanie obliczeń na danych, oferując jednocześnie możliwość ich wizualizacji w postaci diagramów, histogramów i wykresów. Arkusze kalkulacyjne są wykorzystywane w zespołach współpracujących w ramach OSINT do skutecznego przechwytywania i weryfikowania danych w czasie rzeczywistym między analitykami i innymi zespołami. Najpopularniejsze programy do obsługi arkuszy kalkulacyjnych to LibreOffice Calc, Microsoft Excel i Google Sheets.

Zalety: łatwe tworzenie elementów wizualizacji, analitycy mogą uruchamiać formuły do szybkiego liczenia i analizowania danych, zorganizowany układ i możliwość przenoszenia plików.

Wada: krzywa uczenia się formuły.

Microsoft Teams. Oprogramowanie Teams jest wykorzystywane głównie jako platforma komunikacyjna; posiada jednak funkcję udostępniania plików, aby umożliwić współpracę nad dokumentami między członkami zespołu.

Zalety: łatwe w użyciu, często zatwierdzane w środowiskach korporacyjnych, dostęp do chmury z dowolnego miejsca.

Wady: nie jest przeznaczone do badań i może być trudne w przeprowadzaniu dużych analiz, może zawierać błędy, interfejs pozostawia wiele do życzenia.

Microsoft OneNote. OneNote to cyfrowa aplikacja do notowania, która umożliwia tworzenie wielu notatników, które zawierają karty treści i oddzielne strony. Jednocześnie płynnie integruje się z pakietem produktów Microsoft.

Zalety: łatwa w użyciu, świetna do pracy zespołowej, łatwe udostępnianie pełnych notatników, wykorzystuje standardy Microsoftu do przetwarzania tekstu, można importować dokumenty Microsoftu, łatwo wklejać zdjęcia, aby udostępniać je zespołowi, często zatwierdzana w środowiskach korporacyjnych, dostęp w chmurze z dowolnego miejsca.

Wady: może zawierać błędy, duże badania mogą stać się uciążliwe, jeśli standardy notowania nie zostaną wcześniej uzgodnione.

Google Workspace. Workspace to zbiór opartych na chmurze narzędzi do współpracy, w tym Google Docs, Sheets, Slides i Drive. Porównywalne do produktów Microsoft Office, narzędzia te pozwalają na płynne udostępnianie dokumentów między analitykami i ich zespołami przy oczekiwanej użyteczności produktów Google.

Zalety: łatwe w użyciu, współpraca jest prosta, dostęp z dowolnego miejsca.

Wady: pewne problemy z kopiowaniem i wklejaniem, mniejsze bezpieczeństwo w przypadku wrażliwych materiałów, hosting na serwerach Google, a nie na serwerach własnych, co umożliwia potencjalny dostęp do danych użytkownika.

Hunchly. Jest to płatne narzędzie śledcze opracowane przez kanadyjskiego konsultanta ds. bezpieczeństwa i autora książek Justina Seitza. Oprogramowanie działa jako rozszerzenie przeglądarki, dzięki czemu po utworzeniu dochodzenia Hunchly przechwytuje adresy URL i zrzuty ekranu, umożliwiając robienie notatek i płynne śledzenie procesu podczas pracy.

Zalety: Hunchly to dobrze opracowane narzędzie, które jest wysoko cenione w społeczności OSINT. Korzystając z oprogramowania, minimalizuje się liczbę otwartych kart w przeglądarce oraz gromadzi i dokumentuje proces, jednocześnie śledząc źródła.

Wady: narzędzie płatne, niezbyt stroma krzywa uczenia się.

Vortimo. Zostało opracowane w 2019 roku przez założyciela firmy Paterva (która stworzyła Maltego), Roelofa Temmingha. Vortimo to bezpłatne narzędzie zaprojektowane do działania jako rozszerzenie przeglądarki, podobnie jak Hunchly, przechwytujące procesy i dane w tle podczas pracy i ogólnie ułatwiające analizę poprzez przechowywanie listy źródeł.

Zalety: darmowe, dobrze przechwytuje dynamiczną zawartość i stale analizuje pod kątem nowych punktów piwotowania, minimalizuje liczbę otwartych kart w przeglądarce.

Wady: ograniczone wyłącznie do przeglądarek opartych na Chromium, a największą wadą jest to, że pływająca nakładka często przeszkadza podczas pracy.

Obsidian. Jest to oprogramowanie do tworzenia notatek i baz wiedzy, które wykorzystuje katalogi i pliki tekstowe wraz z mediami hostowanymi w systemie lokalnym do przechowywania notatek i generowania pokazów slajdów, map myśli i innych pomocy tego typu; pozwala na wizualizację notatek w różnych widokach, takich jak widok wykresów, widok linków przychodzących (zwrotnych) i widok linków wychodzących.

Zalety: łatwy w użyciu interfejs, a oprogramowanie jest darmowe do użytku osobistego. Obsidian wykorzystuje również lokalną pamięć masową (ang. *local storage*) dla lepszego bezpieczeństwa i trwałości danych. Fajną funkcją jest możliwość manipulowania danymi w celu automatycznego generowania pokazów slajdów i map myśli. Dostępnych jest wiele samouczków dla Obsidiana, aby dowiedzieć się, jak korzystać z tego narzędzia.

Wady: Obsidian nie posiada obecnie własnego rozwiązania do współpracy i najlepiej sprawdza się w projektach, które nie wymagają udostępniania notatek na żywo zespołowi. Obsidian nie jest również darmowy dla firm lub grup składających się z dwóch lub większej liczby osób.

Każde narzędzie do dokumentacji daje analitykowi unikalny sposób na zaoszczędzenie czasu i zminimalizowanie wysiłku podczas dokumentowania procesów. Niezależnie od tego, czy zdecydujemy się dokumentować naszą pracę ręcznie, czy przy użyciu automatycznych narzędzi, posiadanie jasnego, dobrze sformułowanego zapisu naszych ustaleń okaże się przydatne, gdy przejdziemy do fazy przetwarzania i oceny cyklu wywiadowczego.

2.5. Faza przetwarzania i oceny

Według Biura Dyrektora Wywiadu Narodowego w Stanach Zjednoczonych (ODNI) „wywiad to informacje zebrane w Stanach Zjednoczonych lub poza nimi, które dotyczą zagrożeń dla naszego narodu, jego obywateli, mienia lub interesów; rozwoju, rozprzestrzeniania lub użycia broni masowego rażenia; oraz wszelkich innych kwestii związanych z bezpieczeństwem narodowym lub wewnętrznym Stanów Zjednoczonych (indeks, 2022)". Posiadanie informacji nie czyni ich automatycznie informacjami wywiadowczymi; w rzeczywistości wszystkie dane zebrane w *fazie gromadzenia* to tylko surowe dane. Analitycy muszą wziąć te surowe dane, udoskonalić je i przekształcić w przydatne informacje wywiadowcze poprzez kroki wykonane w fazie przetwarzania i oceny.

W trakcie procesu udoskonalania danych możemy rozpocząć ich oczyszczanie za pomocą narzędzi takich jak CyberChef[34], które jest bezpłatnym narzędziem internetowym potrafiącym odszyfrowywać ciągi danych. Możemy również zacząć tłumaczyć tekst skompilowany w języku obcym i korzystając z kluczowych pytań interesariuszy opracowanych w pierwszej fazie, interpretować wszelkie powiązania danych, które zauważyliśmy w naszej dokumentacji. W tym momencie musimy również rozważyć, czy zebrane przez nas dane są dokładne i wiarygodne.

Ponieważ potrzeba weryfikacji informacji wzrosła wykładniczo w ciągu ostatniej dekady z powodu fałszywych wiadomości i manipulacji obrazami, poświęciłam jej cały rozdział w dalszej części książki; jest ona jednak również integralną częścią fazy przetwarzania i oceny cyklu wywiadowczego, więc omówię tutaj również kilka strategii weryfikacji. Istnieje kilka profesjonalnych systemów oceny stosowanych do weryfikacji danych w ramach społeczności wywiadowczej. Jedną z takich metod oceny jest System Admiralicji NATO (ang. *NATO Admiralty Code*) mający na celu ocenę rzetelności zebranych informacji oraz poziomu zaufania do prawdziwości danych (patrz rysunek 2.3)[35].

Źródło danych jest oceniane na podstawie jego rzetelności i otrzymuje literę od *A* do *F*. Następnie źródło jest oceniane na podstawie wiarygodności danych w oparciu o prawdopodobieństwo, że informacje mogą zostać potwierdzone, i otrzymuje liczbę od 1 do 6. Gdy tylko informacje zostaną odpowiednio ocenione, powinny zapewnić użytkownikowi wystarczającą ilość danych, aby mógł zdecydować, czy można je zweryfikować, co jest niezbędne do zapewnienia informacji wywiadowczych opartych na prawdzie. Po przetworzeniu i ocenie zebranych danych może być konieczne zadanie dalszych pytań stronom zainteresowanym, aby mieć pewność, że otrzymają udany produkt.

[34] *https://gchq.github.io/CyberChef*.

[35] FM 2-22, *https://fas.org/irp/doddir/army/fm2-22-3.pdf* .

Rysunek 2.3. Kod Admiralicji NATO

Ustalanie zakresu

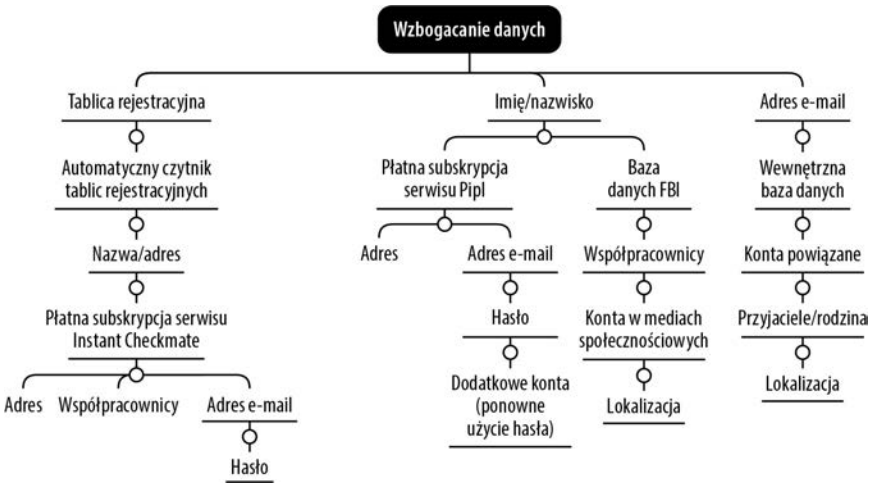
Czynność polegająca na ponownym ukierunkowaniu, przedefiniowaniu i zawężeniu wysiłków przy wzięciu pod uwagę wymagań interesariuszy w celu uniknięcia długotrwałych, błędnych wysiłków nazywana jest **ustalaniem zakresu** (ang. *scoping*). Ustalanie zakresu może mieć i będzie miało miejsce w dowolnym momencie cyklu wywiadowczego, jeśli interesariusze uznają to za konieczne. Często istnieje wstępny proces ustalania zakresu, nawet zanim wymagania wywiadowcze zostaną sfinalizowane i przekazane analitykom. Jeśli proces ustalania zakresu zmieni pytania i wymagania wywiadowcze, będziemy musieli przerwać przetwarzanie i ponownie rozpocząć cykl wywiadowczy, koncentrując się na nowych wymaganiach. Można sobie wyobrazić proces ustalania zakresu jako lejek, w którym dane wchodzą z jednego końca, a poprzez serię wyjaśniających pytań i wymagań wychodzą z drugiego końca tylko najbardziej istotne dane. Podczas procesu ustalania zakresu i udoskonalania naszej pracy możemy mieć dodatkową możliwość wzbogacenia naszych danych o inne zamknięte źródła danych.

Wzbogacanie danych

Oczywiście jesteśmy analitykami danych wywiadowczych o otwartym źródle, ale dzięki procesowi **wzbogacania danych** możemy dalej ulepszać nasze własne dane, łącząc je z wewnętrznymi i zewnętrznymi źródłami zatwierdzonymi przez interesariuszy, aby wypełnić luki w brakujących lub niekompletnych danych. Dzięki włączeniu źródeł wewnętrznych możemy uzyskać głębszy i dokładniejszy obraz z gromadzonych przez nas danych.

Oto kilka przykładów zastosowania wzbogacania danych:

- Korzystanie z wewnętrznej bazy danych organów ścigania w celu wyszukania informacji o pojeździe danej osoby.
- Odpytanie płatnej bazy danych marketingowych należącej do firmy zewnętrznej (strony trzeciej) w celu znalezienia informacji o podmiocie.
- Odwoływanie się do wewnętrznego podręcznika analizy zagrożeń w celu zebrania informacji o osobie stwarzającej zagrożenie.



Prawidłowo wdrożone wzbogacanie danych może pomóc w tworzeniu korelacji między punktami danych. Załóżmy na przykład, że analityk ds. oszustw finansowych bada potencjalnego oszusta, a jedynym tropem, jaki posiada, jest adres e-mail, który został użyty do popełnienia oszustwa. Po pierwsze analityk może sprawdzić istnienie tego adresu e-mail w wewnętrznych bazach danych popełnionych oszustw, a także w zewnętrznych modułach wyszukiwania OSINT w celu wyszukania dopasowań. Jednym ze sposobów na osiągnięcie tego celu jest użycie narzędzi takich jak Spiderfoot[36], które pomagają zautomatyzować wykrywanie połączonych kont. Wyszukiwanie analityka ujawnia następujące szczegóły dotyczące docelowego konta e-mail:

- Jest połączone z aktywnymi kontami w mediach społecznościowych.
- Jest obecnie aktywne i używane.
- Można je znaleźć w kilku przypadkach naruszenia danych uwierzytelniających.
- Zostało powiązane z postami na forum hakerskim.

Teraz w oparciu o nowe informacje znalezione w wyniku wzbogacenia naszego początkowego selektora — adresu e-mail — o dane własne i dane osób trzecich, możemy ustalić w oparciu o znaczniki czasu użytkowania, że adres e-mail jest aktywny i używany. Korzystając z kont w mediach społecznościowych, danych pochodzących z naruszeń i postów w mediach społecznościowych powiązanych z adresem e-mail, możemy zbudować sprawę przeciwko osobie kryjącej się za tym adresem.

2.6. Faza analizy i produkcji

W **fazie analizy** cyklu wywiadowczego oceniamy przetworzone dane, które zostały już przetłumaczone, odszyfrowane i zinterpretowane w celu wygenerowania produktów wywiadowczych. Wnioski są wyciągane na podstawie naszych ustaleń, a następnie, w zależności od wymagań, potencjalnie łączone z informacjami zidentyfikowanymi w dodatkowych źródłach niejawnych

[36] *https://www.spiderfoot.net.*

i jawnych. Innymi słowy, powinniśmy zadać sobie pytanie: „Co mówią nam zebrane dane i dlaczego nas to obchodzi?". Po określeniu danych możemy zacząć myśleć o sposobach rozpowszechniania tych informacji wśród naszych interesariuszy.

W zależności od pilności produkty wywiadowcze mogą mieć formę natychmiastowych raportów z działań lub oceny długoterminowej przy użyciu produktów o charakterze ciągłym. Ważne jest, aby w ramach tych raportów odpowiedzieć na pytania zidentyfikowane w **fazie planowania i wymagań** oraz stworzyć raporty w formacie opartym na potrzebach interesariuszy. Chociaż prawdopodobnie jest to najmniej ekscytująca faza dla wielu analityków, jest ona kluczową częścią całego procesu dochodzeniowego. Cały cykl wywiadowczy jest niczym bez zrozumiałego raportowania, a jeśli nie możemy zapewnić interesariuszom spójnej i kompleksowej oceny naszych ustaleń, to niezależnie od ich wiedzy technicznej zawiedliśmy jako analitycy. Podczas konstruowania raportu wywiadowczego ważne jest, aby zawarte w nim informacje zostały sprawdzone i przeanalizowane pod kątem dokładności i były zgodne z pięcioma głównymi zasadami wywiadu[37].

- Raport musi być dostarczony na czas.
- Musi istnieć wyraźne poczucie pewności w zestawieniu z niepewnością.
- Raporty muszą być dostosowane do potrzeb czytelnika.
- Raporty muszą być łatwe do przyswojenia.
- Raporty muszą odpowiadać na pytania wywiadowcze.

Wizualizacje

Istnieje wiele sposobów na uporządkowanie danych, abyśmy mogli je zinterpretować i zrozumieć na głębszym poziomie, nie tylko podczas analizy, ale także w celu pracy zespołowej i ostatecznego raportowania. Sposób, w jaki wizualizujemy rzeczy do analizy, zależy od osobistych preferencji, chyba że grafika jest umieszczana w raporcie rozpowszechnianym wśród interesariuszy. W takim przypadku chcemy opracować grafikę w najlepszym formacie, aby czytelnik mógł zrozumieć nasze kluczowe punkty. Poniżej przedstawiłam kilka metod wizualizacji danych:

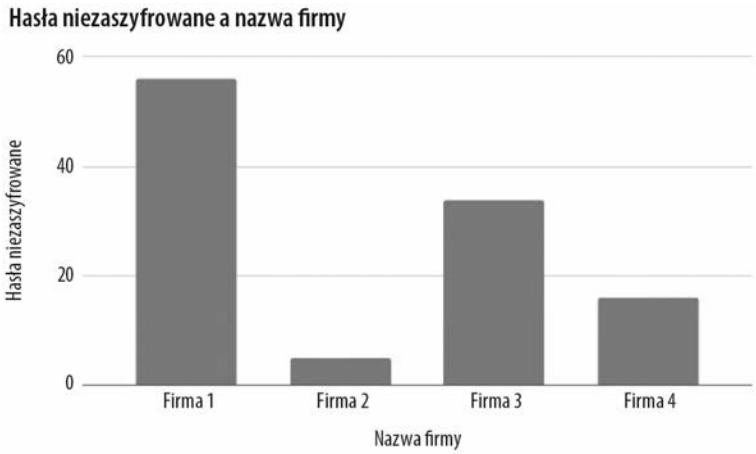
Mapy myśli. Mapa myśli, używana do organizowania pomysłów, wyświetla dane wizualnie, aby zobrazować relacje między elementami. Ta forma wizualizacji najlepiej nadaje się do użytku wewnętrznego dla członków zespołu współpracujących ze sobą i jest często używana do zilustrowania punktów zwrotnych lub połączeń między punktami danych.

[37] *https://www.chds.us/coursefiles/NS4156/lectures/intel_7_step_intel_cycle/script.pdf.*

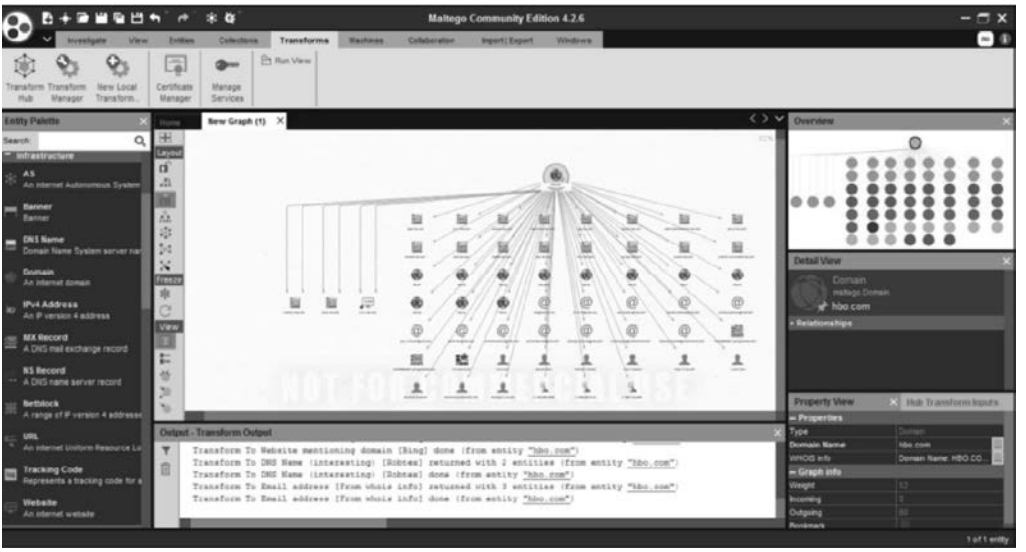
Tabele. Tabela to wizualizacja, która ma być łatwym do odczytania podsumowaniem informacji, często używanym do wizualnego sortowania danych. Przykład jest pokazany tutaj:

TYP SELEKTORA	SELEKTOR	DODATKOWE SZCZEGÓŁY
Adres e-mail	*fałszywy_email@fałszywa_domena.com*	Hasła: *password123*, *bestengineer123*, *qwerty321*
Data urodzenia	28.01.1979	Znaleziona w wyniku naruszeniu bezpieczeństwa aplikacji Birthdayapp
Stanowisko w pracy	Główny inżynier, *Fałszywa_Korporacja*	Wcześniej zatrudniony jako geodeta dla *Fałszywa_Firma*

Wykresy. Wykresy słupkowe i histogramy mogą być używane do wyświetlania wymiernych ilości danych. Wykresy można tworzyć zarówno za pomocą bezpłatnego, jak i płatnego oprogramowania, takiego jak Microsoft Excel, Open Office Calc i Arkusze Google.



Diagramy analizy powiązań. Tego typu diagramy są używane jako graficzne reprezentacje danych i pokazują relacje między dwoma lub większą liczbą punktów danych. Istnieje wiele różnych programów do tworzenia diagramów, a ich koszt zależy od oferowanych możliwości; istnieją jednak firmy, które zapewniają bezpłatne wersje swojego oprogramowania do tworzenia diagramów z ograniczeniami. Jedną z takich firm jest Maltego[38]. Oferuje ona bezpłatną edycję społecznościową, która może być używana do gromadzenia informacji i tworzenia diagramów służących do analizy połączeń opartych na węzłach w celu analizy powiązań między nimi (patrz rysunek 2.4).



Rysunek 2.4. Diagram analizy powiązań w programie Maltego CE

2.7. Raportowanie

W raporcie OSINT przekazujemy wszystkie nasze ustalenia interesariuszom. Celem raportu jest poinformowanie czytelnika o naszych ustaleniach w celu dostarczenia zaleceń dotyczących podejmowania decyzji i wiedzy kontekstowej. Raport ten powinien być dostosowany do konsumentów i należy założyć, że raport będzie rozpowszechniany poza nimi, więc wszelkie szczegóły muszą być oczywiste dla czytelnika bez dalszej prezentacji przez analityka. Style raportowania będą się różnić w zależności od firmy, analityka i celu, ale istnieje kilka kluczowych wskazówek, o których musisz pamiętać podczas tworzenia raportu.

Po pierwsze powinieneś zastanowić się, kto będzie odbiorcą raportu. Czy czytelnik będzie osobą skoncentrowaną na technologii, czy też będzie prezesem zarządu, który może nie być zainteresowany szczegółami technicznymi? Dostosuj swój raport do różnych typów osobowości; pamiętaj, że niektórzy ludzie kierują się danymi, podczas gdy inni są bardziej wzrokowcami.

[38] *https://www.maltego.com*.

Postaraj się uwzględnić obie te koncepcje w jednym raporcie. Zawsze skupiaj się na pytaniu „i co z tego wynika?" i pisz w krótkich i zwięzłych akapitach. Bez względu na to, kim jest czytelnik, powinien on zrozumieć przesłanie i wszystkie kluczowe punkty. Używaj bardzo przemyślanego i precyzyjnego języka, aby uniknąć nieporozumień. Starannie dobieraj słowa, które przekażą Twoje myśli i wynik analizy bez żargonu, nadmiarowości, retoryki lub niejasności. Staraj się wyeliminować wszelkie możliwości, że czytelnik może źle zinterpretować lub źle zrozumieć to, co czyta.

Być może słyszałeś kiedyś angielską frazę *If it bleeds, it leads!* („jeśli jest krew, przyciąga uwagę"), spopularyzowaną przez słynnego dziennikarza Williama Randolpha Hearsta pod koniec lat 90. XIX wieku. Wyrażenie to sugeruje, że najbardziej szokujące i makabryczne nagłówki wiadomości przyciągają największą uwagę. Format pisania tzw. *leadów* zawierających najważniejsze lub szokujące informacje można zobaczyć w przewodniku pisania dla dziennikarzy, znanym jako odwrócona piramida[39].

Odwrócona piramida zaczyna się w najszerszym punkcie, to znaczy podaje w *leadzie* najważniejsze informacje. W raporcie OSINT ta sekcja mogłaby być naszym streszczeniem, w którym zwięźle podsumowujemy to, co znaleźliśmy. Środkowa część odwróconej piramidy to miejsce, w którym umieszczamy wszystkie ważne szczegóły, które wspierają nasze streszczenie; mogłoby to być uważane za treść raportu i mogłoby się składać z podziału na to, co znaleźliśmy i jak to znaleźliśmy, a także mogłoby zawierać wszelkie sugestie dotyczące środków zaradczych. Na końcu piramidy znajdują się najmniej ważne informacje, takie jak indeks lub załącznik.

[39] *https://ohiostate.pressbooks.pub/stratcommwriting/chapter/inverted-pyramid-style.*

Ton raportu

Podczas opracowywania raportu OSINT ton pisania powinien być przekonujący i mieć przekaz analityczny. Sposób, w jaki formułujemy zdania w raporcie, może wpływać na to, jak czytelnik interpretuje wiadomość, którą próbujemy przekazać. Jednym ze sposobów, w jaki możemy sprawić, że nasze teksty będą wywierać większy wpływ, jest użycie tonu aktywnego, perswazyjnego i analitycznego.

Lead *bez* analitycznego przesłania:

„Badamy ogólną skuteczność białego wywiadu w strukturach władz USA".

Lead *z* analitycznym przesłaniem:

„Władze USA zmagają się z wdrożeniem białego wywiadu".

Projekt raportu

Projekt i układ naszych raportów, jeśli są wykonane prawidłowo, powinny być przejrzyste, uporządkowane i łatwe do odczytania. Jeśli interesariusz otrzyma zdezorganizowany raport z różnymi rozmiarami czcionek, kolorami i odstępami, ryzykujemy, że kluczowe punkty, które staramy się przedstawić, zostaną pominięte, co może wstrzymać dochodzenie lub źle świadczyć o nas jako analitykach.

Po pierwsze zastanów się, kto jest odbiorcą raportu; prezes zarządu powinien otrzymać inny raport niż FBI lub prywatny obywatel. Pamiętaj, aby dostosować format i terminologię tylko z myślą o czytelniku końcowym. Powinniśmy wybrać kolory, które są łatwe do odczytania i spójne (pomyśl o odcieniach niebieskiego, zielonego i czarnego) oraz pary czcionek, które są czytelne zarówno pod względem kroju, jak i rozmiaru.

Dobrą praktyką jest dzielenie znaczących sekcji pogrubionymi nagłówkami lub separatorem w postaci poziomej linii. Nagłówek powinien zwięźle definiować informacje zawarte w akapicie pod nim, aby czytelnik mógł szybko przeskanować stronę w poszukiwaniu tego, co jest dla niego najbardziej istotne.

Obrazy takie jak zdjęcia, wykresy i zrzuty ekranu powinny zawierać numer rysunku, a wszystkie tabele powinny zawierać numer tabeli. Adresy URL stron internetowych i odniesienia powinny być odpowiednio cytowane przy użyciu standardów Amerykańskiego Towarzystwa Psychologicznego (APA — ang. *American Psychological Association*), Towarzystwa Języka Współczesnego (MLA — ang. *Modern Language Association*) lub przypisów.

Rozmiar obrazów i tabel powinien być spójny, aby uniknąć wątpliwości lub dezorientacji u czytelnika. Dobrym pomysłem jest też ujednolicenie nazewnictwa plików raportów, jeśli to możliwe.

Tytuł i data

Pamiętaj, aby nadać raportowi krótki, ale opisowy tytuł i w razie potrzeby podać numer raportu. Może się to wydawać oczywiste, ale powinniśmy zawsze datować raport, aby śledzić, kiedy został on rozpowszechniony.

Streszczenie

Streszczenie to miejsce, w którym umieszczamy nasze podsumowanie w formacie BLUF. BLUF, czyli najważniejsze informacje na początku (ang. *bottom line up front*), to amerykański termin wojskowy odnoszący się do podsumowania raportu, który przedstawia wszystkie ważne szczegóły na samym jego początku, aby zaoszczędzić czas czytelnika. Czytelnicy, którzy cierpią na chroniczny brak czasu, jak prezesi zarządu, docenią brak konieczności przekopywania się przez cały raport, aby dotrzeć do sedna sprawy.

Treść lub analiza

W sekcji tej znajduje się sedno pracy dochodzeniowej i w tym miejscu odpowiadamy na wszelkie wymagane pytania wywiadowcze zadane przez interesariusza. Sekcja analizy stanowi większość raportu i powinna być podzielona na akapity, które dostarczą czytelnikowi niezbędnych informacji do zrozumienia procesu i ustaleń dochodzenia. Upewnij się, że poświęciłeś czas na zdefiniowanie „i co z tego wynika" w raporcie, aby czytelnik zrozumiał jego znaczenie i kluczowe wnioski. Szczególnie ważne jest utrzymanie aktywnego i perswazyjnego tonu podczas opracowywania sekcji analizy, aby zainspirować czytelnika do podjęcia odpowiednich działań. Musisz również uważać, aby nie wypowiadać się w sposób autorytarny, ponieważ może to wiązać się z Twoją odpowiedzialnością cywilną. Na przykład nie powinieneś pisać, że nie jesteś *pewien*, że znalazłeś prawidłowy adres e-mail badanego podmiotu, ale że jest *wysoce prawdopodobne*, że ten e-mail można przypisać badanemu podmiotowi.

Podsumowanie

Ważne jest, aby na końcu raportu powtórzyć streszczenie dla czytelnika, a także skróconą wersję naszej analizy i ustaleń.

Zalecenia

Oprócz podsumowania musimy przedstawić czytelnikowi potencjalne środki zaradcze i/lub zalecane działania w oparciu o nasze ustalenia. Celem napisania raportu jest poinformowanie czytelnika o naszych ustaleniach, udzielenie odpowiedzi na wszelkie pytania i przedstawienie naszych profesjonalnych sugestii dotyczących dalszego postępowania.

Dodatek

Jeśli odwołujemy się do dużych obrazów, tabel lub szczegółów pomocniczych, należy je umieścić w załączniku i odpowiednio odwołać się do nich w raporcie.

PRZYKŁADOWA SPRAWA

Teraz gdy poznaliśmy umiejętności niezbędne do przeprowadzenia dochodzenia OSINT i kluczowe części raportu OSINT, użyjmy przykładowej sprawy, aby omówić, jak to wszystko połączyć.

Sprawa:
Nasz klient, „klient X", uważa, że jeden z jego pracowników ujawnia własność intelektualną w internecie, i chce, aby firma *Biuro detektywistyczne Jan Kowalski* przeprowadziła dochodzenie.

Wymagania:
Klient X chciałby uzyskać dowód kradzieży własności intelektualnej, aby wykorzystać go jako dowód sądowy w sprawie przeciwko pracownikowi, w tym poznać wszelkie szczegóły, które możemy znaleźć na temat tego, w jaki sposób pracownik mógł wykraść (eksfiltrować) dane. Dochodzenie potrwa tylko 30 dni, a następnie jednostronicowy raport zostanie przesłany do klienta X.

Podane przez klienta selektory początkowe:
Adres e-mail: *pracownik02@firma-klienta-x.com*
Imię i nazwisko: Pracownik Zostanie_wyrzucony_z_pracy

Zbieranie danych i piwotowanie:
W tym projekcie możemy skupić się głównie na naszym podmiocie i na tym, z kim wchodzi w interakcje online, aby określić jego możliwości i motywy działania. Punkty zwrotne (ang. *pivot points*) mogą obejmować następujące elementy:

- Konta w mediach społecznościowych
- Nazwy użytkowników
- Przyjaciele
- Rodzina
- Adresy e-mail
- Obecność online
- Obecność w ciemnej sieci

Wzbogacanie danych:
Niektóre przykłady wzbogacania danych w tym scenariuszu obejmują następujące elementy:

- Płatne narzędzia do sprawdzania przeszłości
- Dochodzeniowe bazy danych
- Dane tablicy rejestracyjnej
- Pobrane bazy danych (dane pochodzące z naruszeń)

Analiza:
Analiza jest przeprowadzana przy użyciu danych ogólnodostępnych wzbogaconych o informacje z płatnej bazy danych. Wszystkie zebrane informacje i procesy są dokumentowane w dokumencie oprogramowania One Note hostowanym w sieci firmy *Biuro detektywistyczne Jan Kowalski*.

Wizualizacja:
Selektory są przechwytywane w tabeli programu One Note z wyszczególnieniem, gdzie każdy z nich został znaleziony, wraz z podaniem adekwatności przypadku. Proces zbierania jest dokumentowany za pomocą mapy myśli wyłącznie do użytku wewnętrznego analityka.

Raportowanie:
Po 30 dniach opracowywany jest jednostronicowy raport oparty na wymaganiach interesariuszy i rozpowszechniany zgodnie z ich żądaniem.

Przykładowy raport

Biuro detektywistyczne Jan Kowalski

Raport OSINT dla Klienta X

Nazwa projektu: Klient X, Kradzież własności intelektualnej 004
Data: 16 maja 2022 r.
Godzina: 11:00 EST
Śledczy: Jan Kowalski

Streszczenie:
Analitycy z Biura detektywistycznego Jan Kowalski (BdJK) zaobserwowali poprzez analizę typu OSINT sprzedaż własności intelektualnej klienta X przez użytkownika „Ipthief" na forum internetowym „Money4IP", zlokalizowanym w tzw. „ciemnej sieci" (Dark Web), za 74 800 dolarów. Konto Paypal wzmiankowane w poście było powiązane z adresem e-mail „employee02@clientxcompany.com", który został dostarczony do biura BdJK jako początkowy selektor. Opierając się na powiązaniu tematu z dostarczoną wiadomością e-mail, jest wysoce prawdopodobne, że pracownik ukradł własność intelektualną klientowi X, zapisując stosowne pliki na zewnętrzną pamięć USB (pendrive) w celu sprzedaży w ciemnej sieci z zyskiem.

Analiza:
Obserwacja nr 1: Adres e-mail „employee02@clientxcompany.com" został zaobserwowany w danych, których bezpieczeństwo zostało naruszone, powiązanych z hasłem „ipthief".

Obserwacja nr 2: W swoim poście na forum „Money4IP" zlokalizowanym w Ciemnej sieci użytkownik „Ipthief" wspomina, że pracuje dla klienta X i że dokonał eksfiltracji danych za pomocą pendrive'a.

Rysunek 1. Zrzut ekranu postu użytkownika ipthief na forum Money4IP w „ciemnej sieci"

Obserwacja nr 3: W tym samym poście zamieszczonym na forum internetowym „Money4IP" w Ciemnej sieci, użytkownik „Ipthief" prosi o zapłatę 74 800 dolarów za pośrednictwem serwisu PayPal na adres „employee02@clientxcompany.com".

Podsumowanie:
Na podstawie obserwacji poczynionych przez BdJK jest wysoce prawdopodobne, że pracownik Zostaniewyrzuconyzpracy świadomie dokonał eksfiltracji własności intelektualnej klienta X na pendrive w celu sprzedaży tych informacji na forum „Money4IP" znalezionym w ciemnej sieci.

Zalecenia:
BdJK zaleca zainstalowanie blokady interfejsów USB lub zainstalowanie oprogramowania blokującego na wszystkich systemach firmy, a także aktywne monitorowanie forów internetowych w Ciemnej sieci pod kątem postów dotyczących klienta X.

Dodatek:
Dodatkowe obserwowane selektory:

Adres e-mail	Willbfired@email123.com
Nazwa użytkownika	Ipthief2

2.8. Fazy rozpowszechniania i konsumpcji

Lowenthal uważa, że fazy rozpowszechniania i konsumpcji nie powinny być traktowane w normalnym pięcioetapowym procesie oddzielnie, ale powinny być połączone w jedną fazę[40]. Kiedy raport jest rozpowszechniany wśród interesariuszy, to nawet jeśli materiał jest przekonujący, niekoniecznie motywuje ich do działania. Dodanie konsumpcji jako osobnego kroku w oficjalnym procesie ma większe szanse na wywołanie dyskusji i reakcji. Ponadto kluczowy jest sposób, w jaki interesariusz konsumuje dane wywiadowcze i rozumie swoje obowiązki jako interesariusza w danym dochodzeniu, a my możemy mu w tym pomóc poprzez sformalizowane raportowanie i podpowiedzi (ang. *tippers*).

Podpowiedzi

Czasami konieczne może być natychmiastowe zgłoszenie krytycznych informacji interesariuszowi w celu podjęcia przez niego natychmiastowych działań. W poprzednim przykładzie raportu widzimy coś, co wydaje się być sprzedażą własności intelektualnej na rynku Dark Web. Jest to dobry przykład scenariusza, w którym interesariusz nie będzie chciał czekać na sfinalizowany raport, ale raczej otrzyma alert wywiadowczy lub podpowiedź zawierającą szybkie streszczenie w formacie BLUF zawierające ustalenia i możliwe do zastosowania środki zaradcze.

Faza informacji zwrotnej

Od samego początku faza planowania i wymagań musi ustanowić aktywną komunikację między interesariuszami a analitykami. Istotne jest, aby komunikacja była utrzymywana przez cały proces, a nawet poza fazą rozpowszechniania. Ta ciągła komunikacja pozwoli analitykom ocenić, jak dobrze odpowiedziano na początkowe pytania dotyczące wymagań i umożliwi odpowiednie dostosowanie analizy. Podobnie, spójne informacje zwrotne pomogą określić, czy należy odpowiedzieć na więcej pytań i czy wymagane jest dalsze gromadzenie danych.

Wyzwania w cyklu wywiadowczym

Cykl wywiadowczy ma na celu informowanie i kierowanie procedurami w całej społeczności wywiadowczej i poza nią, ale z pewnością nie jest pozbawiony wyzwań. W wywiadzie i bezpieczeństwie narodowym Arthur Hulnick przedstawia kilka wyzwań, które widzi w cyklu wywiadowczym w jego obecnym formacie. Sugeruje, że jako analitycy nie powinniśmy oczekiwać ani polegać na interesariuszach, którzy zapewnią odpowiednie wytyczne w fazie planowania cyklu.[41] Ten fałszywy pomysł, że system wywiadowczy automatycznie powiadomi interesariuszy o problemach, tworzy sytuację reaktywną, a nie proaktywną. Ostatecznie ten brak proaktywności utrudnia

[40] Mark M. Lowenthal, *Intelligence: from secrets to policy*.

[41] Arthur S. Hulnick, *What's wrong with the Intelligence Cycle*, „Intelligence and National Security", 21, 6, 2006, s. 959 – 979, *doi: 10.1080/02684520601046291*.

rozpoczęcie fazy zbierania danych, ponieważ analitycy oczekują na wskazówki. Lepszym podejściem według Hulnicka jest postrzeganie procesów planowania i gromadzenia jako równorzędnych i działających równolegle, a nie sekwencyjnie.

Innym poważnym wyzwaniem, jakie dostrzega Hulnick, jest to, że ze względu na obawy społeczności wywiadowczej, obawy związane z bezpieczeństwem i osobiste bariery psychologiczne, procesy analityczne i gromadzenia danych często działają oddzielnie od siebie. Ten brak zaangażowania w proces może prowadzić interesariuszy do konstruowania wymagań mających na celu wyłącznie potwierdzenie ich poglądów, zamiast pozostawania otwartym na wyniki. Gdy wyniki są korzystne dla interesariusza, może on postrzegać analizę jako potwierdzenie własnej opinii, a zatem bezużyteczną, ponieważ była to wiedza wywiadowcza, którą już posiadał. W przypadku konfliktu z opinią interesariusza, może on również lekceważyć analizę i postrzegać ją jako potencjalną próbę ingerencji.

Cykl wywiadowczy nie jest oczywiście doskonały, a ponieważ OSINT rozciąga się na tak wiele różnych dziedzin, wszyscy wykonujemy naszą analizę w sposób unikalny, z różnymi priorytetami lub misjami. Dlatego powinniśmy konsekwentnie ponownie oceniać cykl wywiadowczy i stosować go zgodnie z naszym konkretnym sektorem OSINT. Realistycznie rzecz biorąc, cykl wywiadowczy powinien pozostać płynny, a każdy zespół analityków musiałby rozważyć przeszkody zarówno na szerszym poziomie, jak i na poziomie specyficznym dla ich roli.[42]

[42] *https://www.asisonline.org/globalassets/security-management/current-issues/2018/01/white-paper_intelligence-cycle_11-29-17.pdf.*

DOSTRZEGAJ TO, CO POZOSTAJE NIEWIDOCZNE DLA INNYCH!

OSINT (ang. open source intelligence) polega na pozyskiwaniu danych wywiadowczych z ogólnodostępnych źródeł. Jest to zestaw praktycznych umiejętności, które przydadzą się nie tylko analitykom — metody białego wywiadu okazują się pomocne na wielu ścieżkach kariery, a także w życiu codziennym. Łatwo się przekonasz, że OSINT pozwala uzyskać niezwykle cenne informacje, a przy tym jest satysfakcjonującym i ciekawym zajęciem!

Dzięki tej książce nauczysz się gromadzić publicznie dostępne informacje, korzystać z wiedzy o cyklu życia wrażliwych danych i przekształcać je w informacje wywiadowcze przydatne dla zespołów zajmujących się bezpieczeństwem. Opanujesz proces gromadzenia i analizy danych, poznasz również strategie, które należy wdrożyć podczas poszukiwania informacji z publicznie dostępnych źródeł. Ugruntujesz wiedzę na temat bezpieczeństwa operacyjnego i uświadomisz sobie, w jaki sposób niektórzy używają publicznie dostępnych danych do nielegalnych celów. Książkę tę szczególnie docenią inżynierowie społeczni i specjaliści do spraw bezpieczeństwa, a także kadra kierownicza.

Najciekawsze zagadnienia:

- strategie stosowania urządzeń IoT do gromadzenia danych wywiadowczych
- pozyskiwanie danych przy użyciu publicznie dostępnych informacji transportowych
- techniki poprawy bezpieczeństwa operacyjnego
- zagrożenia związane z ogólnodostępnymi danymi
- metody gromadzenia danych wywiadowczych stosowane przez najlepsze zespoły do spraw bezpieczeństwa

RAE BAKER jest starszym analitykiem OSINT w Deloitte. Specjalizuje się w wywiadzie morskim, rozpoznaniu osobowym i rozpoznaniu środowisk korporacyjnych. Zdobyła kilka znaczących certyfikatów branżowych, takich jak SANS GOSI, Associate of ISC2 (CISSP), AWS Solutions Architect, a także tytuł Most Valuable OSINT.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-289-0590-0
9 788328 905900
Cena: 99,00 zł
WILEY