# Wykorzystanie technologii semantycznych do modelowania wiedzy z zakresu cyberbezpieczeństwa

*Streszczenie*

Adiel Aviad

## 1. Uzasadnienie tematu badawczego

Wraz z coraz większą zależnością przedsiębiorstw od informatyki i technologii cyfrowych rośnie również ich ekspozycja na zagrożenia pochodzące z cyberprzestrzeni. Cała dziedzina cyberbezpieczeństwa bardzo mocno opiera się na wiedzy, którą nie tylko trudno pozyskać, ale również nią zarządzać. Wynika to z jej natury, sposobów tworzenia i wykorzystywania oraz samej struktury rynku cyberbezpieczeństwa. Dlatego też pożądane jest określenie sposobów usprawnienia zarządzania tym aspektem funkcjonowania przedsiębiorstw.

Jedną z kluczowych koncepcji w rozprawie są technologie semantyczne. Dostarczają one środki do kodowania semantyki danych niezależnie od ich zapisu syntaktycznego, co odróżnia je od tradycyjnych technologii informacyjnych, gdzie znaczenie musi być wstępnie zdefiniowane. Osiąga się to poprzez wprowadzenie warstwy abstrakcji nad istniejącymi technologiami informatycznymi, aby umożliwić łączenie danych, treści i procesów biznesowych. Kodowanie znaczenia opiera się na logice, co pozwala na sformalizowanie wiedzy w sposób zrozumiały dla maszyn. Z perspektywy użytkownika technologie semantyczne zapewniają lepiej dostosowany dostęp do zasobów wiedzy.

W niniejszej pracy przedstawiono podejście do wykorzystania technologii semantycznych w celu zarządzania wiedzą z dziedziny cyberbezpieczeństwa. Praca nie aspiruje do zarządzania bezpieczeństwem jako takim, ale ogranicza się do baz wiedzy, na których bezpieczeństwo bazuje. Celem pracy nie jest tworzenie nowej wiedzy

w dziedzinie cyberbezpieczeństwa, ale efektywniejsze wykorzystanie istniejących zasobów. Tym samym praca wnosi wkład do nauk o zarządzaniu poprzez zaproponowanie metod do podniesienia efektywności współdzielenia wiedzy oraz określenie konsekwencji dla zarządzania.

Na wiedzę o cyberbezpieczeństwie składa się z wiele różnego rodzaju bytów, m.in. zagrożenia, słabości, luki w zabezpieczeniach, ryzyka, produkty, technologie, praktyki, polityki, konfiguracje, środowiska organizacyjne itp. Sama wiedza z zakresu cyberbezpieczeństwa jest złożona i bardzo dynamiczna. Składa się na nią wiedza poszczególnych graczy rynkowych: producentów sprzętu (np. puntu dostępu, zapory ogniowe) i oprogramowania, w tym także produktów zabezpieczających, ekspertów ds. bezpieczeństwa, organów regulacyjnych i różnych agresorów - od samotnych hakerów przez zorganizowaną przestępczość do agencji wywiadowczych. Wiedza ta szybko ewoluuje, napędzana nowymi technologiami, odkrytymi problemami bezpieczeństwa, opracowanymi i przyjętymi środkami cyberbezpieczeństwa oraz zdobytymi nowymi danymi wywiadowczymi.

Obecnie kluczowa z punktu widzenia cyberbezpieczeństwa wiedza przechowywana jest w różnego rodzaju rozproszonych repozytoriach, najczęściej w postaci tabelarycznej, zwykle w relacyjnych bazach danych. Informacje o potencjalnie powiązanych ze sobą bytach często zbierane są niezależnie – przez różne organizacje i w ramach różnych inicjatyw. Taka reprezentacja nie sprzyja wykorzystywaniu wiedzy, gdyż problemem jest samo jej znalezienie, nie mówiąc o integracji i wnioskowaniu. Istotne jest zatem opracowanie modelu pozwalającego na połączenie różnych aspektów wiedzy z zakresu cyberbezpieczeństwa.

Jedną z bardziej rozpowszechnionych inicjatyw jest opracowana przez NIST Information Technology Laboratory baza podatności na ataki (vulnerabilities) oraz powiązany z nią zbiór rekomendowanych konfiguracji sprzętu i oprogramowania. Inicjatywa SCAP – Security Content Automation Protocol (NIST, 2015) ma na celu standaryzację sposobów postępowania z lukami. Organizacje MITRE z kolei kategoryzuje wzorce ataków i pracuje nad standaryzacją informacji o zagrożeniach - inicjatywa STIX (MITER, 2015b) oraz inne, np. MAEC (MITER, 2015a). OWASP również pracuje nad zwiększenie bezpieczeństwa oprogramowania poprzez dzielenie się

wiedzą, a znany jest głównie z publikacji listy 10 największych w danym okresie zagrożeń (OWASP, 2015).

Motywacją do podjęcia prac nad niniejszą rozprawą była chęć integracji tych rozproszonych zasobów tak, aby zarówno poszczególne przedsiębiorstwa, jak i ich otoczenie rynkowe mogły odnieść korzyści ze zwiększenia poziomu cyberbezpieczeństwa. Wśród wielu rozpatrywanych podejść najbardziej obiecujące wydawało się wykorzystanie technologii semantycznych. Jest to podejście do reprezentacji wiedzy, które w celu zapewnienia jej jednoznacznej interpretacji wykorzystuje formalizm logiczny. Każdy opisywany byt, pojęcie, czy relacja ma swój globalnie unikatowy identyfikator. Zastosowanie formalizmy logicznego pozwala nie tylko na sprawdzenie wewnętrznej spójności wiedzy, ale również prowadzenie wnioskowania według określonych schematów. Ontologia, rozumiana jako formalna reprezentacja pojęć, właściwości i relacji między danymi, może być wykorzystywana do określania, z jakimi zagrożeniami spotykają się przedsiębiorstwa i jakie środki zaradcze mogą być brane pod uwagę. Semantyczne przetwarzanie może zapewnić elastyczność reprezentacji zarówno znanych już, jak i przyszłych zagrożeń, ataków, czy środków zaradczych.

## 2. Cele badawcze i teza

W celu zbadania możliwości wykorzystania technologii semantycznych do reprezentacji wiedzy o cyberbezpieczeństwie należy odnieść się do poszczególnych aspektów cyberbezpieczeństwa, istniejących (i przewidywanych do utworzenia) zasobów, oczekiwanych funkcjonalności i korzyści dla użytkowników oraz ogólnego wpływu na otoczenie przedsiębiorstw. Należy wziąć pod uwagę charakter tej wiedzy i przypadki jej użycia, a także wpływ na zachowanie różnych graczy, którzy ją tworzą i wykorzystują.

W tym celu sformułowane zostały następujące pytania badawcze:

**Q1: Jakie są aspekty wiedzy i zasoby, które należy modelować?**

W celu odpowiedzi na to pytanie badawcze opracowano metody i modele reprezentacji wiedzy z zakresu cyberbezpieczeństwa. Sama wiedza musi być jednoznacznie zapisana, a jej źródła muszą być zidentyfikowane.

**Q2: Jak reprezentować wiedzę o cyberbezpieczeństwie w sposób umożliwiający dodawanie nowych faktów w przyszłej?**

Istotną cechą wiedzy z zakresu bezpieczeństwa jest dynamika. Zagrożenia ciągle ewoluują, wraz ze zmieniającą się technologią oraz oprogramowaniem. Ważne jest elastyczne podejście do reprezentacji wiedzy, w szczególności łatwe dodawanie nowych faktów, a tym samym również łączenie różnych źródeł wiedzy. Proponowane podejście powinno zapewniać korzyści w porównaniu do istniejącej tabelarycznej reprezentacji wiedzy. Lepsza funkcjonalność powinna być osiągnięta dzięki dzieleniu się wiedzą oraz automatycznemu wnioskowaniu. Dla przedsiębiorstw istotna jest zdolność do reakcji na przyszłe scenariusze materializacji zagrożeń.

**Q3: W jaki sposób można łączyć różne rozproszone zasoby?**

Sposób modelowania wiedzy o cyberbezpieczeństwie powinien odnosić się do możliwości integracji zasobów z różnych źródeł w sposób nie ograniczający funkcjonalności z racji różnego pochodzenia poszczególnych części wiedzy.

**Q4: W jaki sposób można przenieść istniejącą wiedzę do reprezentacji semantycznej?**

Model reprezentacji wiedzy stanowi zaledwie pewne ramy. Istotne jest wskazanie, w jaki sposób istniejące zasoby wiedzy z zakresu cyberbezpieczeństwa mogą zostać przetłumaczone na pojęcia z proponowanego modelu. Powinny zostać opracowane metody wskazujące ścieżki migracji zasobów tabelarycznych do postaci semantycznej.

**Q5: Jakie są czynniki organizacyjne motywujące do ponownego wykorzystanie wiedzy z zakresu cyberbezpieczeństwa?**

Oprócz poprawnego odniesienia się do aspektów technicznych należy na problem ponownego wykorzystania wiedzy spojrzeć również z punktu widzenia biznesowego. Ułatwienia w zakresie technologii zwiększają skłonność firm do korzystania z określonych rozwiązań. Zabezpieczenia mogłyby być wprowadzane szybciej i niższym kosztem. Następujące cele wspierające powinny zostać uwzględnione: zwiększenie wykorzystania i kompletności wiedzy, zmniejszenie wpływu efektów zewnętrznych oraz umożliwienie korzystania z ekonomii skali. W ten sposób firmy

miałyby większą motywację do przekazywania wiedzy i korzystania ze wspólnej wiedzy, która byłaby bardziej kompletna, bardziej użyteczna i o wyższej wartości. Korzyści odnoszą więc nie tylko bezpośredni użytkownicy wiedzy, ale także pośrednio poprawiają „bezpieczeństwo środowiskowe". Organizacje w łatwiejszy sposób podnosząc swój poziom bezpieczeństwa wpływałyby na wyższy poziom bezpieczeństwa całego otoczenia rynkowego.

W rozprawie zamieszczono następującą tezę:

**Wykorzystanie technologii semantycznych do modelowania wiedzy o cyberbezpieczeństwie poprawia ogólny poziom bezpieczeństwa organizacji poprzez umożliwienie współdzielenia wiedzy, wnioskowania nowych faktów oraz świadome zarządzanie ryzykiem.**

Proces badawczy prowadzony był zgodnie z metodologią *design science* opracowaną przez Hevnera (AR Hevner & Chatterjee, 2010). Zgodnie z podejściem projektowym w nauce problemy badawcze rozwiązuje się projektując nowe artefakty. Poniżej znajduje się lista artefaktów, które określają również wkład pracy doktorskiej do nauki:

**A1. Model zagrożeń związanych z Internetem oparty na zasobach cyberbezpieczeństwa i określonych aspektach wiedzy.**

Artefakt ten obejmuje identyfikację zasobów wiedzy o cyberbezpieczeństwie, a także głównych jej aspektów. Badając określone zasoby i aspekty opracowujemy propozycję podejścia semantycznego opartą na całości wiedzy o cyberbezpieczeństwie, zamiast rozważać ją w konkretnych przypadkach.

**A2. Metoda semantycznej reprezentacji wiedzy o cyberbezpieczeństwie.**

Jest to rdzeń semantycznego podejścia do zarządzania wiedzą z zakresu cyberbezpieczeństwa. Zaproponowano reprezentację semantyczną, zapewniającą uniwersalność i uwzględniającą różne aspekty wiedzy. Poniższe artefakty uszczegóławiają poszczególne aspekty wiedzy.

**A3: Metoda semantycznej reprezentacji języka STIX na potrzeby analityki cyberzagrożeń.**

Ten artefakt demonstruje semantyczną reprezentację aspektu analityki cyberzagrożeń (cyber threat intelligence) poprzez zapewnienie reprezentacji semantycznej dla STIX (Structured Threat Information Expression), który jest językiem opisującym informacje wywiadowcze o zagrożeniach cybernetycznych.

**A4: Metoda semantycznej reprezentacji frameworka CVSS dla oceny podatności na zagrożenia.**

Ten artefakt demonstruje semantyczną reprezentację aspektu oceny podatności na zagrożenia (vulnerability scoring) poprzez zapewnienie reprezentacji semantycznej dla CVSS (Common Vulnerability Scoring System).

**A5: Metoda semantycznej reprezentacji metody CORAS do oceny ryzyka.**

Ten artefakt demonstruje semantyczną reprezentację aspektu oceny ryzyka (risk assessment) poprzez dostarczenie reprezentacji semantycznej dla CORAS, która jest metodą oceny cyberzagrożeń.

Wszystkie reprezentacje są ze sobą powiązane, tworząc zintegrowany model składający się z kilku aspektów wiedzy. Uwzględniona jest też możliwość rozszerzenia modelu o kolejne aspekty (np. schematy ataków).

**A6: Metoda konwersji danych tabelarycznych na postać semantyczną w celu umożliwienia wielokrotnego wykorzystania istniejących zasobów.**

Metoda ta umożliwia wykorzystanie danych istniejących już w zasobach wiedzy, wskazanych w części nieoryginalnej pracy. Zasoby takie mogą mieć postać relacyjnej bazy danych lub być dostępne w prostej postaci tabelarycznej. Aby możliwe było włączenie ich do zasobów semantycznych (w tym tzw. powiązanych danych otwartych – linked open data), konieczne jest przetłumaczenie ich do postaci RDF (Resource Description Framework), zgodnie z zaproponowanym w rozprawie modelem.

**A7: Metoda wnioskowania nowej wiedzy w obszarze zarządzania ryzykiem.**

Ten artefakt demonstruje implementację wnioskowania semantycznego, które umożliwia wyciąganie konkluzji na podstawie istniejącej wiedzy. W zaprezentowanym w rozprawie przykładzie na podstawie ogólnej wiedzy z zakresy cyberbezpieczeństwa

oraz informacji o posiadanym przez przedsiębiorstwo oprogramowaniu wyciągane są wnioski o związanych z nim zagrożeniach, co stanowi wejście do zarządzania ryzykiem.

## 3. Struktura rozprawy

Rozprawa składa się z 6 rozdziałów zgrupowanych w dwie części. Pierwsza część - nieoryginalna – stanowi wprowadzenie do dwóch istotnych z punktu widzenia problematyki rozprawy obszarów: cyberbezpieczeństwo oraz technologie semantyczne. Przeprowadzona została analiza literatury oraz dokonano przeglądu istniejących źródeł danych będących przedmiotem zainteresowania przedsiębiorstw w zakresie bezpieczeństwa. W drugiej części – oryginalnej – przedstawiono zaproponowane w rozprawie rozwiązanie problemu badawczego. Zaprezentowane zostały modele oraz metody stanowiące wkład rozprawy do nauki, określane zbiorczo jako artefakty. Dokonano ewaluacji metody oraz przedyskutowano wpływ na przedsiębiorstwa i ogólne otoczenie rynkowe z punktu widzenia technicznego oraz zarządczego.

Pierwszy rozdział jest wprowadzeniem do rozprawy i opisuje w szczególności zakres, motywację oraz metodologię. W rozdziale 2. opisana została dziedzina cyberbezpieczeństwa, ze szczególnym naciskiem na zasoby wiedzy o zagrożeniach, lukach bezpieczeństwa oraz sposobach zapobiegania im. Dokonano przeglądu inicjatyw zmierzających do powiązania tych zasobów wiedzy. Uwzględniono również aspekty zarządcze związane z wiedzą o cyberbezpieczeństwie – tutaj odniesiono się do zarządzania ryzykiem. Rozdział 3. prezentuje technologie semantyczne jako podejście do reprezentacji wiedzy, pozwalające w szczególności na łatwe współdzielenie wiedzy oraz wnioskowanie o nowych faktach na podstawie ogólnych reguł. W rozdziale 4. omówione zostały wyzwania związane z dostępem do wiedzy z obszaru cyberbezpieczeństwa. Zaproponowano, w jaki sposób mogłyby one został zaadresowane przez technologie semantyczne. Wprowadzony został model ontologii dla poszczególnych subdomen cyberbezpieczeństwa, omówionych w rozdziale 2. Wyjaśniono, w jaki sposób można lepiej zarządzać dostępną wiedzą przy użyciu podejścia semantycznego. W rozdziale tym opracowane zostały artefakty od A1 do

A6. Następnie w rozdziale 5. przedstawiono implementację zaproponowanego modelu wraz z ewaluacją i weryfikacją podejścia. Przedstawiono na konkretnym przykładzie sposób konwersji rozproszonych zasobów w formie tabel do reprezentacji semantycznej, pozwalającej na przeprowadzenie wnioskowania. Stanowi to uzupełnienie artefaktu A6 oraz stanowi opracowanie artefaktu A7. Na podstawie weryfikacji pytań kompetencyjnych uzasadniono poprawność podejścia. Wreszcie w rozdziale 6. przeprowadzono dyskusję nad osiągniętymi rezultatami oraz ich konsekwencjami, szczególnie w obszarze minimalizacji ryzyka związanego z zagrożeniami płynącymi z cyberprzestrzeni oraz podnoszenia ogólnego poziomu bezpieczeństwa przedsiębiorstw. Wiedza reprezentowana zgodnie z zaproponowanym w rozprawie modelem przy pomocy technologii semantycznych jest bardziej dostępna i bardziej kompletna, możliwe jest jej automatyczne przetwarzanie oraz wnioskowanie o nowych faktach na podstawie reguł. Takie podejście oznacza efektywniejsze zarządzanie wiedzą, co prowadzi do przewidywanego większego bezpieczeństwa w organizacjach. Na końcu zarysowano również przyszłe kierunki badań.

## 4. Źródła danych i metody badawcze

Podczas przygotowywania rozprawy wykorzystano dwa główne źródła: literaturę oraz otwarte bazy wiedzy (dane). Literatura dotycząca wiedzy z zakresu cyberbezpieczeństwa przedstawiona została w rozdziale 2. Literatura dotycząca technologii semantycznych jest z kolei przedmiotem rozdziału 3., gdzie opisane zostały standardy, technologie i narzędzia. Rozważania literaturowe z zakresu cyberbezpieczeństwa, zgodnie z metodyką systematycznego przeglądu literatury, prowadzone były w kilku aspektach:

a. Czy jest to szczegółowy wkład do listy pojęć z rozważanego obszaru wiedzy, np. zagrożenie, podatność, luka bezpieczeństwa, program wykorzystujący lukę (tzw. exploit), dowód ataku, środek zapobiegawczy itp.

b. Czy jest to ogólny wkład w zakresie cyberbezpieczeństwa, dostarczający informacji o poszczególnych bytach?

c. Czy jest to zasób danych (np. strona internetowa), który udostępnia użyteczny zbiór faktów o poszczególnych bytach w postaci pozwalającej na zasilenie proponowanego modelu cyberzagrożeń?

d. Czy jest to praca poruszająca zagadnienie radzenia sobie z dostępną wiedzą dotyczącą cyberbezpieczeństwa?

Ostatni rodzaj prac może dotyczyć również systemów analityki cyberzagrożeń (cyber threat intelligence) lub świadomości sytuacyjnej (situational awareness). Prace dotyczące metod, takich jak zarządzania ryzykiem, rozpatrywane są głównie w aspekcie wiedzy, którą dostarczają lub wykorzystują. Prace dotyczące rynku wiedzy o cyberbezpieczeństwie są rozpatrywane oddzielnie, jako perspektywa (np. zarządzanie), aby określić możliwy wpływ i wartość przedstawianych koncepcji.

Metodologia wykorzystana w rozprawie ma na celu wsparcie głównego argumentu: reprezentacja wiedzy o cyberbezpieczeństwie z wykorzystaniem technologii semantycznych przynosi przedsiębiorstwo określone korzyści w zakresie współdzielenia tej wiedzy oraz wykorzystania jej do wnioskowania. Tak postawiony cel oznacza, że adekwatną metodologią do rozwiązania związane z nim problemu badawczego jest *design science*. Zgodnie z ramami i wytycznymi zaproponowanymi w (Hevner, March, Park i Ram, 2004) dla design science w systemach informacyjnych, będących częścią systemów zarządczych, skupiono się na przypadku wiedzy o cyberbezpieczeństwie oraz wskazano jego istotność i znaczenie poprzez wskazanie na implikacje.

Zgodnie z listą artefaktów przedstawionych we wstępie do pracy opracowany został model zagrożeń związanych z Internetem oparty na zasobach cyberbezpieczeństwa i określonych aspektach wiedzy. Jego powstanie było poprzedzone analizą trudności w zarządzaniu wiedzą, trudności w dzieleniu się i wykorzystywaniu wiedzy, braku zachęt do wielokrotnego wykorzystania wiedzy oraz kosztami związanymi z lukami w wiedzy. Odnosząc się do wiedzy o cyberbezpieczeństwie, która ze względu na swój rozmiar i dynamikę jest trudna do opanowania, w rozprawie odniesiono się do kilku jej kluczowych aspektów, istotnych z punktu widzenia potencjalnych konsumentów wiedzy. Poszczególne aspekty rozpatrywane są pod kątem korzyści, jakie można

uzyskać dzięki technologii semantycznej w zakresie cyberbezpieczeństwa i oceny ryzyka.

Ocena projektu w ramach *design science* jest osiągana poprzez analityczne badanie zdolności do lepszego wykorzystania wiedzy oraz możliwości ekspansji modelu w celu uwzględnienia nowej wiedzy w tej dynamicznej dziedzinie. W rozprawie wykazano elastyczność w zakresie nowych danych i nowych przypadków użycia, automatyzacji wnioskowania, współdzielenia wiedzy i uzgadniania nowych faktów, np. potencjalnych punktów ataku. Wkład obejmuje identyfikację znaczących zasobów wiedzy o cyberbezpieczeństwie, identyfikację aspektów, semantyczną reprezentację tych aspektów. Rygor naukowy, jeden z filarów design science, jest zapewniony poprzez stosowanie ugruntowanych w dziedzinie modelowania semantycznego standardów oraz technologii, formalizację podejścia w postaci logicznej oraz przykładowe implementacje opracowane w celu weryfikacji podejścia. Stosowane są rozwiązania zgodne ze stanem wiedzy w dziedzinie (ontologie, model danych RDF, edytor semantyczny FluentEditor, język zapytań SPARQL).

## 5. Rezultaty

Zgodnie z pierwotną koncepcją internetu semantycznego (semantic web) przedstawioną w (Berners-Lee, Hendler i Lassila, 2001) dane umieszczone w internecie miały mieć nadane znaczenie poprzez odwołanie do wspólnie i jednoznacznie zdefiniowanych pojęć, tzw. ontologii. Tak jak tradycyjny internet łączy dokumenty, tak internet semantyczny pozwala na dalszą strukturyzację dokumentów i wiązanie ze sobą danych. Technologie semantyczne zapewniają środki nie tylko do reprezentacji wiedzy, ale również do zdobywania nowej wiedzy poprzez wnioskowanie – wyciąganie nowych faktów na podstawie określonych przesłanek. W związku z tym słabości, zagrożenia, czy środki zaradcze mogą być definiowane bezpośrednio, ale najciekawsze są automatyczne wnioskowania, które stają się możliwe dzięki formalnej reprezentacji wiedzy.

Podejście semantyczne ogólnie, a technologia semantyczna w szczególności najlepiej pasuje do dziedzin, gdzie mamy do czynienia z rozproszonym tworzeniem wiedzy.

W niniejszej rozprawie zidentyfikowaliśmy takie dopasowanie technologii semantycznej z dziedziną wiedzy o cyberbezpieczeństwie. Podejście semantyczne może mieć zastosowanie tam, gdzie istnieje konieczność centralizacji artefaktów, ciągłe uzupełnianie wiedzy, potrzeba dzielenia się wiedzą, dobrze określone implikacje lub relacje, potrzeba automatycznego rozumowania na poziomie „znaczenia", potrzeba integracji zasobów danych i wyników pracy różnych społeczności. Ta technologia i jej cechy nadają się łatwo do reprezentowania cyberzagrożeń, ryzyka i wiedzy z nimi związanej. Dzielenie się wiedzą może można również poprawić za pomocą technologii semantycznej. Wiedza z zakresu cyberbezpieczeństwa może być współdzielona między ekspertami ds. bezpieczeństwa, producentami i organami regulacyjnymi. Ponadto można budować wspólne rozumienie pojęć, co nie zostało jeszcze osiągane przez społeczności zajmujące się cyberbezpieczeństwem. Zarządzanie artefaktami poprzez abstrakcję umożliwia wykorzystanie wiedzy o innych artefaktach do obsługi nowych artefaktów za pomocą klasyfikacji. Złożone rozumowanie wykorzystuje inne relacje, które łączą różne koncepcje, np. zagrożenie i atak.

Integracja wiedzy w tak kompleksowej formie może być interesująca zarówno dla osób odpowiedzialnych za cyberbezpieczeństwo w organizacjach, jak i dla potencjalnych agresorów. Niemniej jednak jest bardziej prawdopodobne, że taka wiedza pomoże bardziej tym pierwszym. Wynika to z faktu, że obrońcy potrzebują szerokiej wiedzy, podczas gdy atakujący zazwyczaj koncentrują się na konkretnej podatności lub kilku wektorach ataku. Ponadto napastnicy chcieliby mieć więcej wiedzy na temat architektury organizacji i jej ochrony, a nie wiedzy o bezpieczeństwie ogólnego przeznaczenia. Tymczasem dostęp do informacji o firmie mają tylko osoby odpowiedzialne za bezpieczeństwo – nie jest to wiedza powszechnie współdzielona. Ponadto ocena „dobrego" lub „złego" jest często subiektywna (jak w przypadku etycznych hakerów obsługujących organy ścigania).

Potencjalni odbiorcy pracy to osoby zainteresowane wiedzą o cyberbezpieczeństwie z punktu widzenia obrony. Obejmuje to zarówno tych, którzy zajmują się rzeczywistą obroną w organizacjach, jak i tych, którzy zajmują się zabezpieczaniem produktów i technologii.

Przeprowadzone badania potwierdziły tezę, że technologie semantyczne umożliwiają poprawę ogólnego poziomu bezpieczeństwa organizacji poprzez umożliwienie współdzielenia wiedzy, wnioskowanie nowych faktów oraz świadome zarządzanie ryzykiem.

## 6. Literatura


Berners-Lee, T., Hendler, J., & Lassila, O. (2001). The Semantic Web. *Scientific American*, *284*(5), 34–43. https://doi.org/10.1038/scientificamerican0501-34

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design Science Research in Information Systems. *MIS Quarterly*, *28*(1), 75–105.

Hevner, A. R., & Chatterjee, S. (2010). *Design Research in Information Systems. Theory and Practice*. Springer US. https://doi.org/10.1007/978-1-4419-5653-8

MITRE. (2015a). Malware Attribute Enumeration and Characterization.

MITRE. (2015b). Structured Threat Information eXpression (STIX).

NIST. (2015). Security Content Automation Protocol (SCAP).

OWASP. (2015). The Open Web Application Security Project (OWASP).