



Analiza i ocena efektywności narzędzi otwartoźródłowych w kontekście zapewnienia zgodności z wymaganiami regulacyjnymi UE

mgr inż. Krzysztof Pańtak

Promotor pracy dyplomowej: dr inż. Barbara Łukawska

Konsultant: dr inż. Arkadiusz Chrobot

Politechnika Świętokrzyska



Wzrost liczby podmiotów objętych ścisłymi obowiązkami cyberbezpieczeństwa w Polsce z **ok. 400 do około 38 000**. Wśród nich m.in. zakłady przetwórstwa spożywczego, hurtownie farmaceutyczne, firmy kurierskie, przedsiębiorstwa komunalne.



Rygorystyczne normy techniczne m.in. obsługa incydentów, ciągłość działania, higiena IT, polityki kontroli dostępu.



Wysokie koszty rozwiązań komercyjnych.



Wysokie kary: Do **10 mln EUR lub 2% globalnego obrotu** rocznego dla podmiotów kluczowych. Kary administracyjne w ustawie krajowej do **100 mln PLN**. Kary finansowe dla menedżerów do **300% miesięcznego wynagrodzenia** oraz tymczasowy zakaz pełnienia funkcji kierowniczych za rażące zaniedbania.

Narzędzia otwartoźródłowe jako kosztowo efektywna alternatywa.



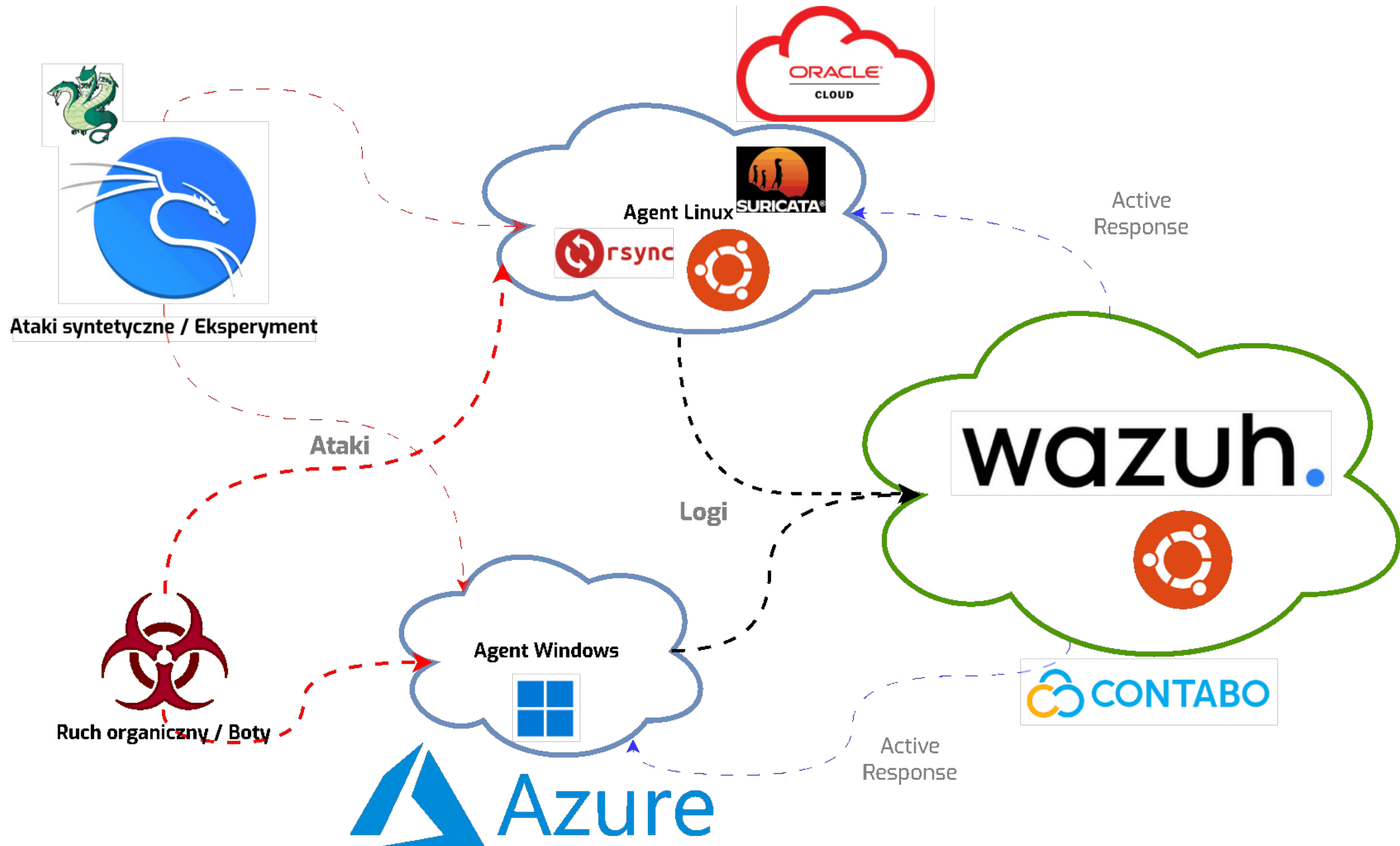
Promowanie standardów przez samą dyrektywę NIS2.

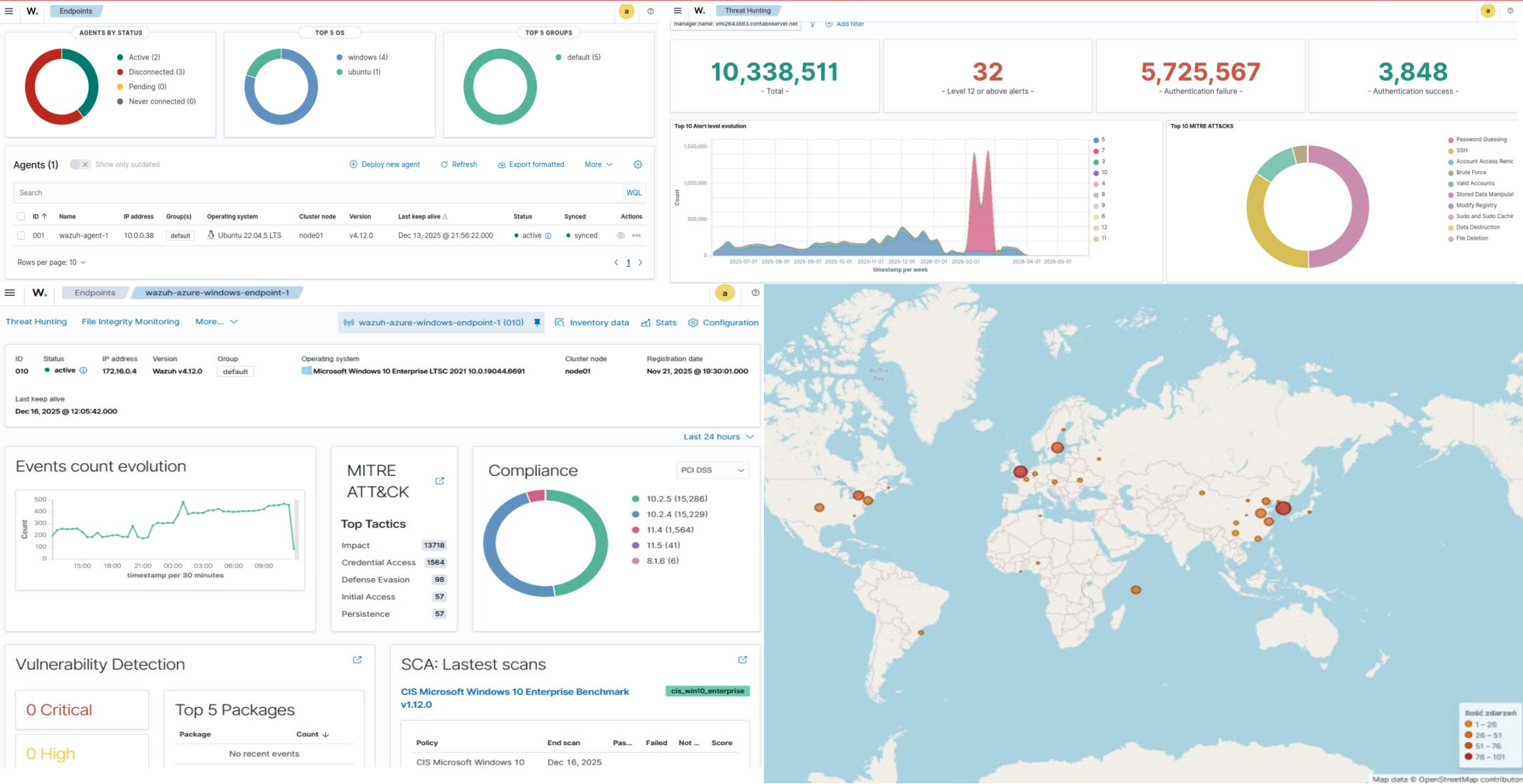


Główny cel pracy:

Empiryczna weryfikacja technicznej zgodności narzędzi Open Source z wymogami UE.









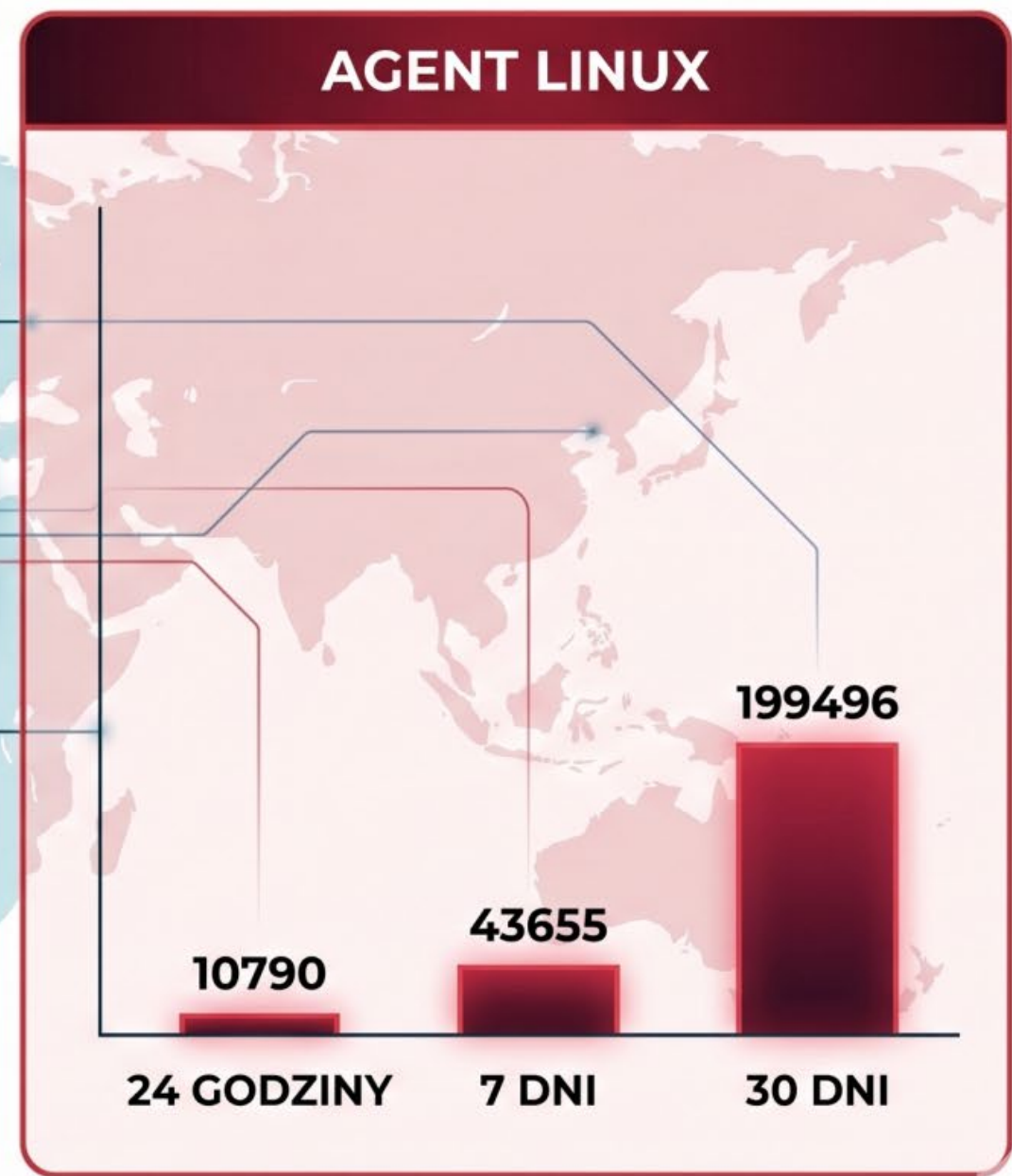
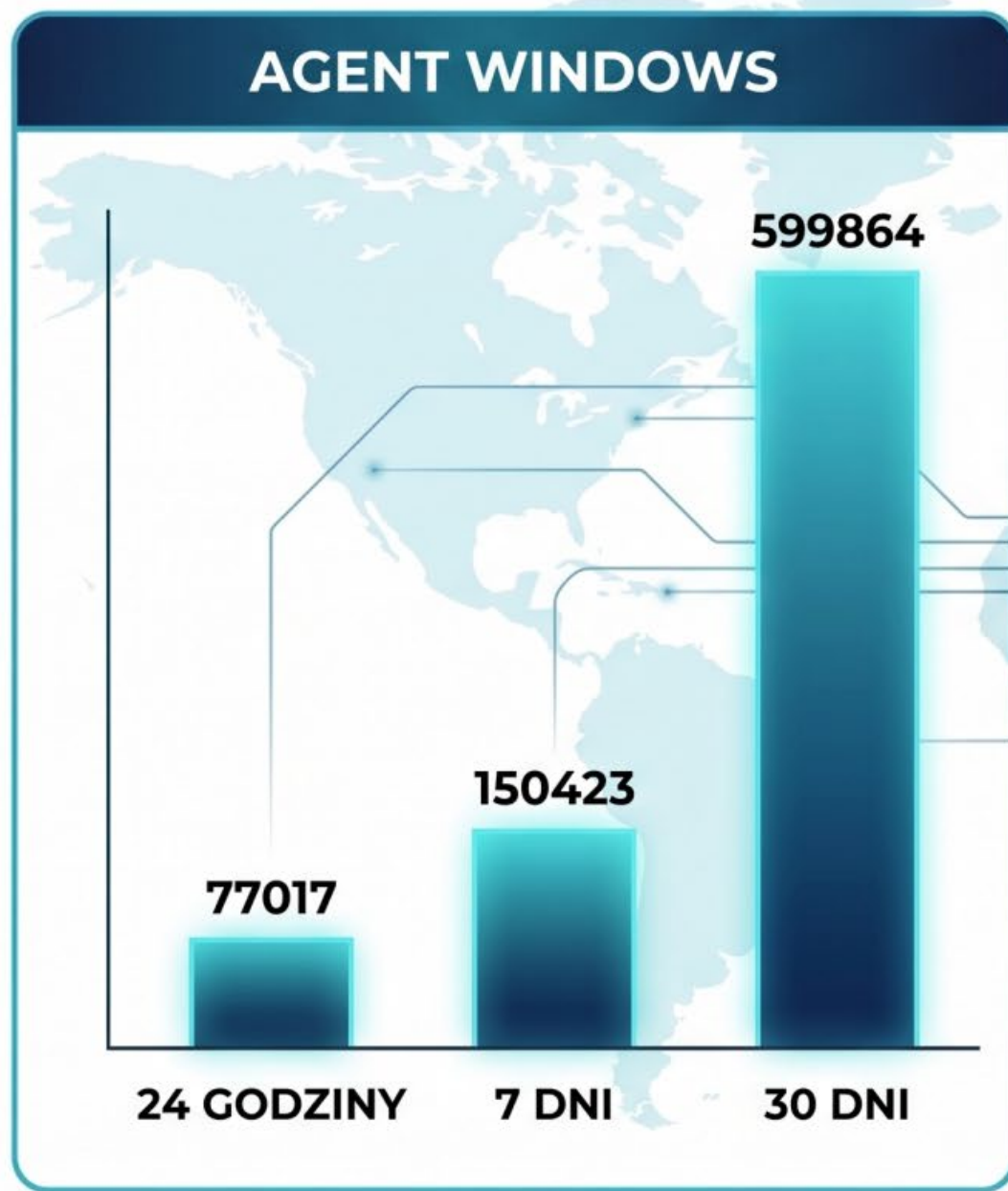
Faza 1 - Obserwacja pasywna

- 30-dniowy ciągły monitoring organicznych cyberataków z Internetu na publiczne interfejsy (SSH/RDP). Ocena skali realnego zagrożenia.



Faza 2 - Eksperyment

- Obsługa incydentów
- Ciągłość działania
- Higiena IT (Podatności)
- Kontrola dostępu



AGENT WINDOWS

1.  Rosja
15022 zdarzenia
2.  Niemcy
8978 zdarzenia
3.  Belgia
5470 zdarzenia
4.  Francja
4022 zdarzenia
5.  Nigeria
3511 zdarzenia

AGENT LINUX

1. Chiny 
170 zdarzeń
2. USA 
137 zdarzeń
3. Korea Południowa 
101 zdarzeń
4. Wielka Brytania 
82 zdarzeń
5. Szwecja 
71 zdarzeń



Krytyczne alerty dla nmap i Hydra.

Moduł Active Response wymagał ręcznego naprawienia parserów JSON



Własne dekodery XML dla logów kopii zapasowych. Poprawne wykrycie awarii.

Mechanizm File Integrity Monitoring zarejestrował próbę sabotażu i edycji kodu skryptów.



Prawidłowa identyfikacja starych bibliotek na systemie Windows.

Problem False Positives.



Trudność implementacji natywnego Geo-Fencingu. Konieczność skorzystania z polityki białych list.

Poprawne alerty krytyczne przy właściwym haśle podanym z nieznanego IP.

Wysoka zgodność techniczna z NIS2



Brak „bezpieczeństwa przez ukrycie”



Efektywna, ale nie „darmowa” alternatywa



Konieczność optymalizacji reguł i ryzyko „zmęczenia alertami”



Fałszywe alarmy



Wsparcie społeczności Open Source





Dziękuję za uwagę

mgr inż. Krzysztof Pańtak

krzysztofpantak@gmail.com

Politechnika Świętokrzyska