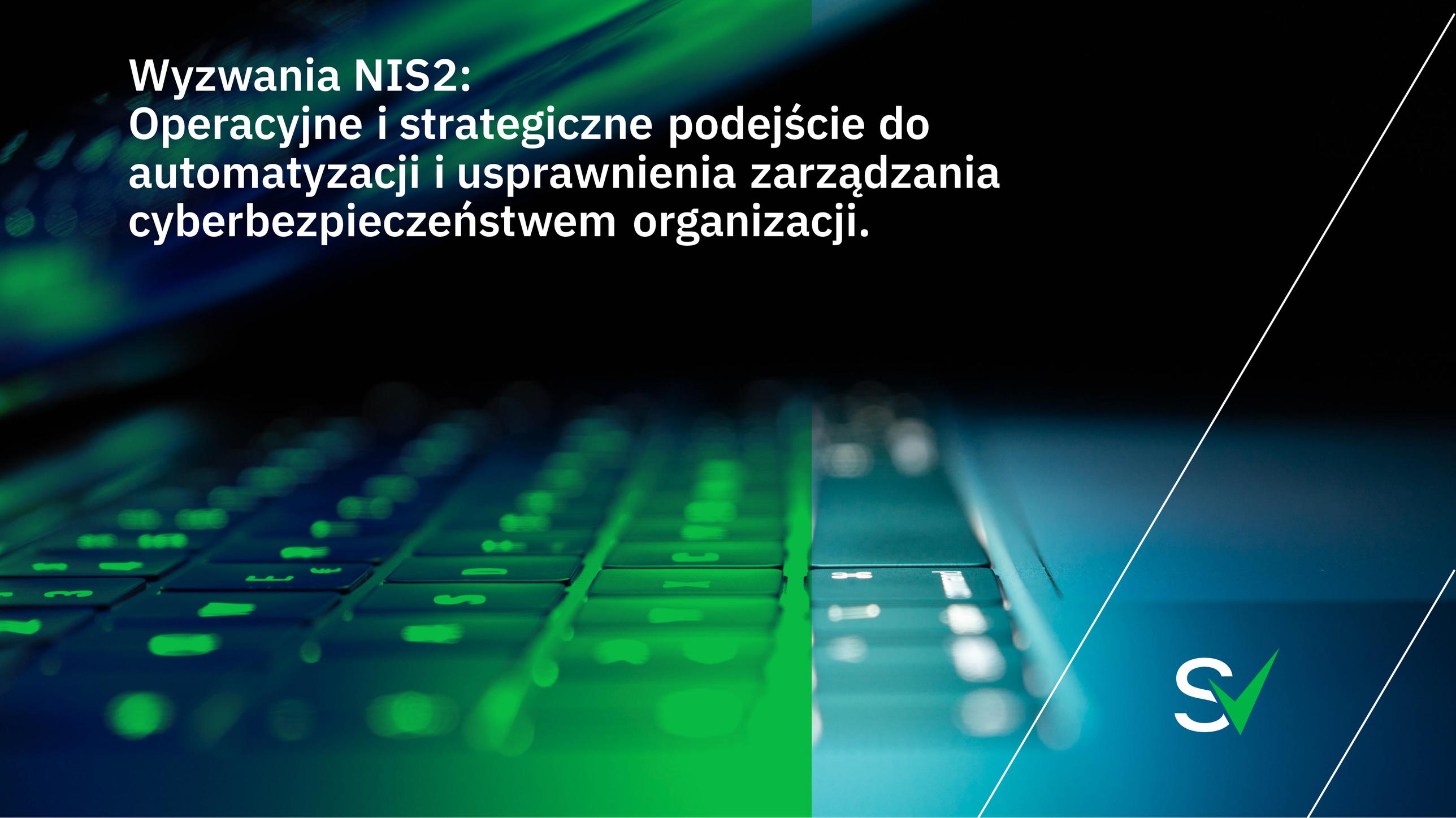
# Wyzwania NIS2:
# Operacyjne i strategiczne podejście do automatyzacji i usprawnienia zarządzania cyberbezpieczeństwem organizacji.



# NIS 2:
## Kluczowe informacje

Dyrektywa wchodzi w życie **17 października 2024 roku.**

Państwa UE dokonują transpozycji Dyrektywy.

01 **Wyeliminowanie rozbieżności** wdrażania przez państwa UE dyrektywy NIS (zakres, obowiązki podmiotów kluczowych, zgłaszanie incydentów, nadzór, egzekwowanie prawa)

02 **Rozszerzenie zakresu** na organizacje z sektorów, mających istotne znaczenie dla kluczowych rodzajów działalności społecznej i gospodarczej na rynku wewnętrznym (**określone w Załączniku I oraz II jako sektory kluczowe i ważne**), wprowadzenie kategorii **podmiotów kluczowych i ważnych** oraz **zasady wyraźnego progu wielkości** (organizacje średnie 50-249 pracowników i roczny obrót 10-50 mln EUR)

03 **Wzmocnienie wymogów** podejścia do **zarządzania ryzykiem**, zawierających minimalny wykaz podstawowych elementów bezpieczeństwa, które należy zastosować. Wprowadzenie bardziej precyzyjnych przepisów dotyczących procesu zgłaszania incydentów **(Artykuł 21 i 23**)

04 **Bardziej rygorystyczne środki nadzorcze** dla organów krajowych, większe możliwości w zakresie egzekwowania przepisów i harmonizacja systemów sankcji w państwach członkowskich (7-10 mln EUR/ 1,4%-2% obrotu)

05 **Skoordynowanie procesu ujawniania podatności** - unijna baza podatności publicznie znanych luk w produktach ICT i usługach ICT, obsługiwana przez ENISA

# Artykuł 3
## Podmioty ważne i kluczowe

### Załącznik I - Sektory kluczowe

1. Energetyka - energia elektryczna, system ciepłowniczy lub chłodniczy, ropa naftowa, gaz, wodór
2. Transport - transport lotniczy, transport kolejowy, transport wodny, transport drogowy
3. Bankowość
4. Infrastruktura rynków finansowych
5. Opieka zdrowotna
6. Woda pitna
7. Ścieki
8. Infrastruktura cyfrowa
9. Zarządzanie usługami ICT
10. Podmioty administracji publicznej
11. Przestrzeń kosmiczna

### Załącznik II - Sektory ważne

1. Usługi pocztowe i kurierskie
2. Gospodarowanie odpadami
3. Produkcja, wytwarzanie i dystrybucja chemikaliów
4. Produkcja, przetwarzanie i dystrybucja żywności
5. Produkcja:

- wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro,
- komputerów, wyrobów elektronicznych i optycznych,
- urządzeń elektrycznych,
- maszyn i urządzeń gdzie indziej niesklasyfikowana,
- pojazdów samochodowych, przyczep i naczep,
- pozostałego sprzętu transportowego

6. Dostawcy usług cyfrowych
7. Badania naukowe

# WYZWANIA W ZARZĄDZANIU CYBERBEZPIECZEŃSTWEM

Technologia

Ludzie

Pieniądze

# Artykuł 21
## Wymogi zarządzania ryzykiem

**Środki (...) bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy:**

a) politykę analizy ryzyka i bezpieczeństwa systemów informatycznych;
b) obsługę incydentu;
c) ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej, i zarządzanie kryzysowe;
d) bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami;
e) bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie;
f) polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;
g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa;
h) polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania;
i) bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami;
j) w stosownych przypadkach – stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.

# Artykuł 23
## Wykrywanie i zgłaszanie incydentów

**Incydent poważny:**

a) spowodował lub może spowodować **dotkliwe zakłócenia operacyjne usług lub straty finansowe** dla danego podmiotu;
b) **wpłynął** lub jest w stanie wpłynąć **na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe i niemajątkowe**.

**Zgłoszenia:**

a) bez zbędnej zwłoki, a w każdym razie w ciągu **24 godzin** od powzięcia wiedzy o poważnym incydencie – **wczesne ostrzeżenie**, w którym w stosownych przypadkach wskazuje się, czy poważny incydent został przypuszczalnie wywołany działaniem bezprawnym lub działaniem w złym zamiarze lub czy mógł wywrzeć wpływ transgraniczny;
b) bez zbędnej zwłoki, a w każdym razie w ciągu **72 godzin** od powzięcia wiedzy o poważnym incydencie – **zgłoszenie incydentu**, w stosownych przypadkach z aktualizacją informacji, o których mowa w lit. a), **i wskazaniem wstępnej oceny poważnego incydentu, w tym jego dotkliwości i skutków, a w stosownych przypadkach także wskaźników integralności systemu**;

**Sprawozdanie końcowe nie później niż miesiąc po zgłoszeniu incydentu:**

a) **szczegółowy opis incydentu, w tym jego dotkliwości i skutków;**
b) **rodzaj zagrożenia lub pierwotną przyczynę, która prawdopodobnie była źródłem incydentu;**
c) **zastosowane i wdrażane środki ograniczające ryzyko;**
d) w stosownych przypadkach transgraniczne skutki incydentu;

# Artykuł 12 i 21
## Obszar podatności

**Artykuł 12 - Skoordynowane ujawnianie podatności i europejska baza danych dotyczących podatności**

1. Każde państwo członkowskie wyznacza jeden spośród swoich CSIRT na koordynatora na potrzeby skoordynowanego ujawniania podatności.

(...)

c. negocjowanie harmonogramu **ujawniania oraz zarządzanie podatnościami**, których skutki mają wpływ na wiele podmiotów.

**Artykuł 21 - Środki zarządzania ryzykiem w cyberbezpieczeństwie**

(...)

2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy:

(...)

e. bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym **postępowanie w przypadku podatności i ich ujawnianie**;

# Artykuł 32 i 34
## Nadzór, egzekwowanie, kary...

**Artykuł 32, pkt 5 - Środki nadzoru i egzekwowania przepisów dla podmiotów kluczowych**

Jeżeli żądane działanie nie zostanie podjęte w wyznaczonym terminie, państwa członkowskie zapewniają, **by właściwe organy były uprawnione do**:

(...)
b) zwrócenia się do właściwych instytucji lub sądów, **zgodnie z prawem krajowym, o nałożenie tymczasowego zakazu pełnienia funkcji zarządczych w tym podmiocie kluczowym na osobę fizyczną wykonującą obowiązki zarządcze na poziomie dyrektora generalnego lub przedstawiciela prawnego w tym podmiocie.**

**Artykuł 34 – Ogólne warunki nakładania administracyjnych kar pieniężnych na podmioty kluczowe i ważne**

(...)
4. Państwa członkowskie zapewniają, **by podmioty kluczowe dokonujące naruszeń art. 21 lub 23** podlegały zgodnie z ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w maksymalnej wysokości **co najmniej 10 000 000 EUR lub co najmniej 2 % łącznego rocznego światowego obrotu** w poprzednim roku obrotowym przedsiębiorstwa, do którego należy podmiot kluczowy, przy czym zastosowanie ma kwota wyższa.
5. Państwa członkowskie zapewniają, **by podmioty ważne dokonujące naruszeń** art. 21 lub 23 podlegały zgodnie z ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w maksymalnej wysokości **co najmniej 7 000 000 EUR lub 1,4 % łącznego rocznego światowego obrotu** w poprzednim roku obrotowym przedsiębiorstwa, do którego należy podmiot ważny, przy czym zastosowanie ma kwota wyższa.

# Artykuł 33
## Środki nadzoru – podmioty ważne

**Punkt 1:**

W przypadku otrzymania dowodu […], że podmiot ważny […] nie stosuje się do niniejszej dyrektywy, w szczególności jej w art. 21 i 23, państwa członkowskie zapewniają, by […] właściwe organy podjęły działania w postaci środków nadzoru […].

**Punkt 2 – zakres nadzoru:**

a) **kontrole na miejscu** i nadzór zdalny ex post prowadzonymi przez przeszkolonych specjalistów;
b) **ukierunkowany audyt bezpieczeństwa** prowadzonymi przez niezależną instytucję lub właściwy organ;
c) **skany bezpieczeństwa** na podstawie obiektywnych, niedyskryminacyjnych, sprawiedliwych i przejrzystych kryteriów szacowania ryzyka,
d) **wnioski o udzielenie informacji** niezbędnych do oceny środków zarządzania ryzykiem w cyberbezpieczeństwie, w **tym polityki cyberbezpieczeństwa**,
e) **wnioski o udzielenie dostępu do danych, dokumentów i informacji** koniecznych do wykonywania ich zadań nadzorczych;
f) **wnioski o przedstawienie dowodów realizacji polityki cyberbezpieczeństwa**, takich jak wyniki audytu bezpieczeństwa

**Punkt 4 – uprawnienia państw członkowskich – m.in.:**

d) nakazanie danym podmiotom, by […] zapewniły zgodność swoich środków zarządzania ryzykiem w cyberbezpieczeństwie z art. 21 lub wypełniły obowiązki zgłaszania incydentów określone w art. 23;
f) nakazania danym podmiotom, by […] wdrożyły zalecenia wydane w wyniku audytu bezpieczeństwa;
g) nakazania danym podmiotom, by w określony sposób podały do wiadomości publicznej informacje o naruszeniach przez nie niniejszej dyrektywy;
h) zastosowania lub zwrócenia się o zastosowanie przez właściwe organy lub sądy, zgodnie z prawem krajowym, administracyjnej kary pieniężnej na podstawie art. 34 oprócz środków, o których mowa w lit. a)–g) niniejszego ustępu

# Jak automatyzować i usprawniać?

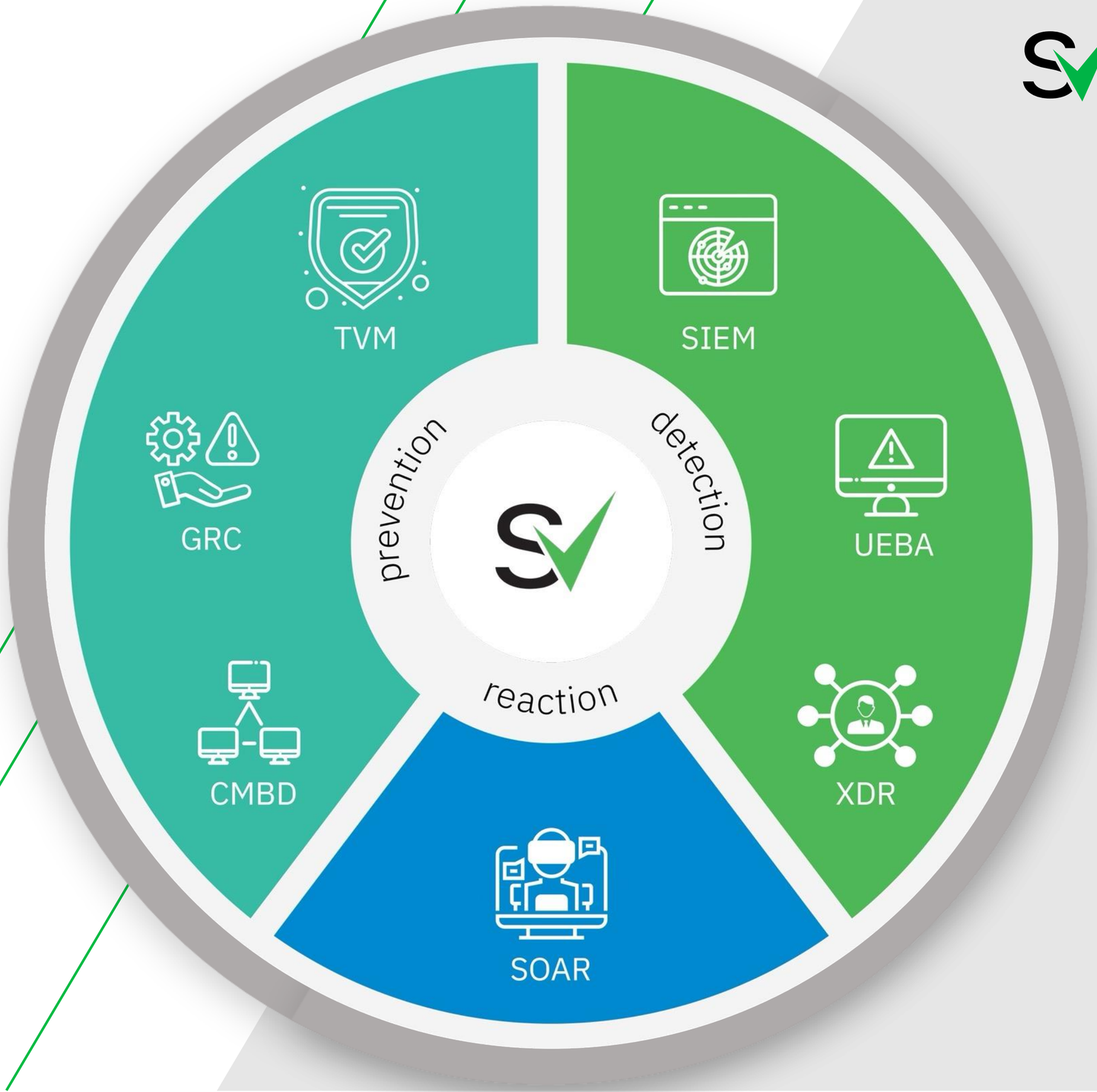
Konsolidacja kluczowych narzędzi IT SEC w ramach jednej platformy technologicznej.

Strategiczna perspektywa:

- ✅ Inwentaryzacja kluczowych zasobów IT i procesów
- ✅ Ciągła i dynamiczna analiza ryzyka cyberzagrożeń

Aspekt operacyjny:

- ✅ Wykrywanie i reakcja na incydenty poważne
- ✅ Obsługa krytycznych podatności



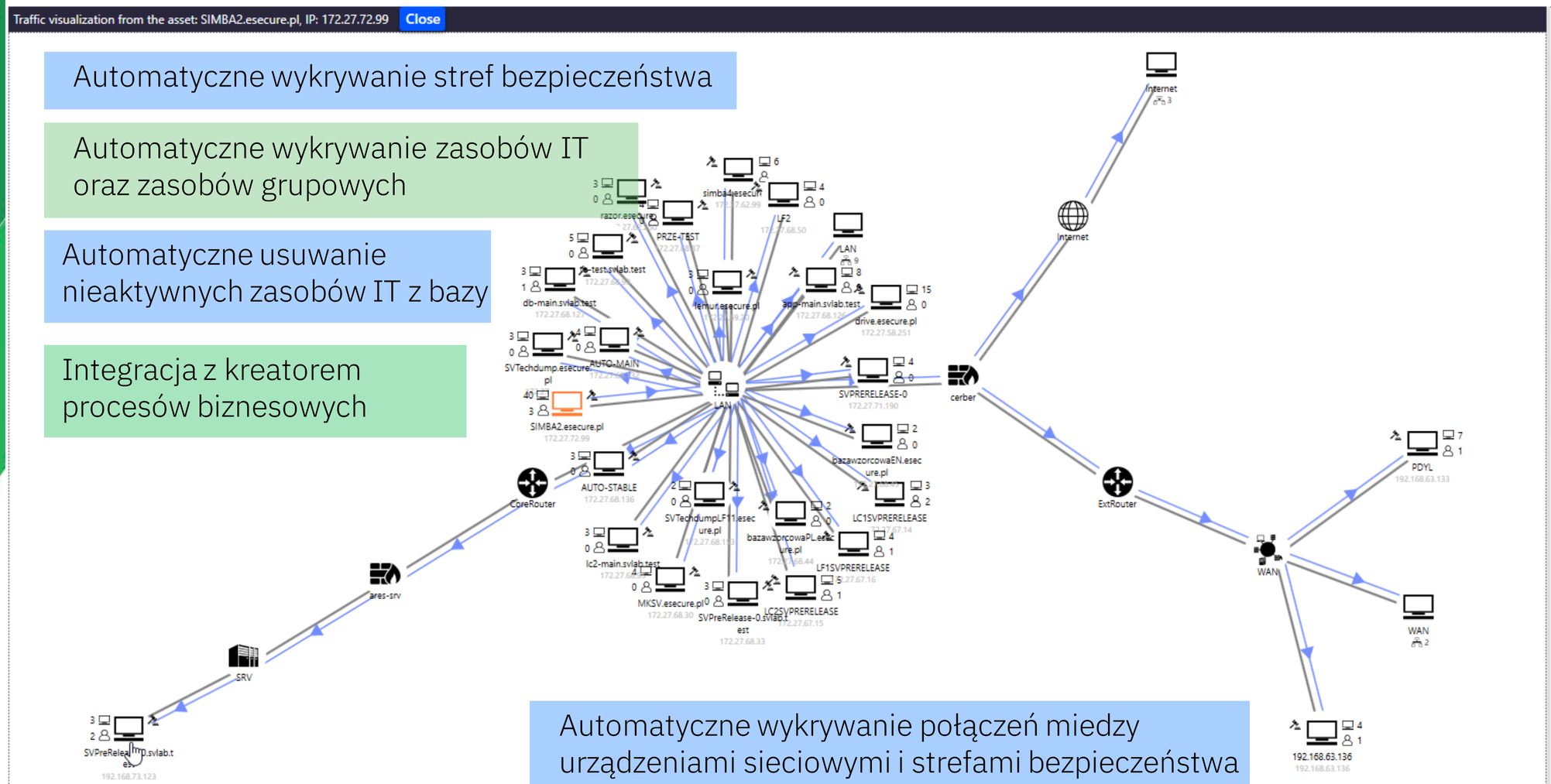
# Automatyczna inwentaryzacja - CMDB

Automatyczne wykrywanie stref bezpieczeństwa

Automatyczne wykrywanie zasobów IT oraz zasobów grupowych

Automatyczne usuwanie nieaktywnych zasobów IT z bazy

Integracja z kreatorem procesów biznesowych

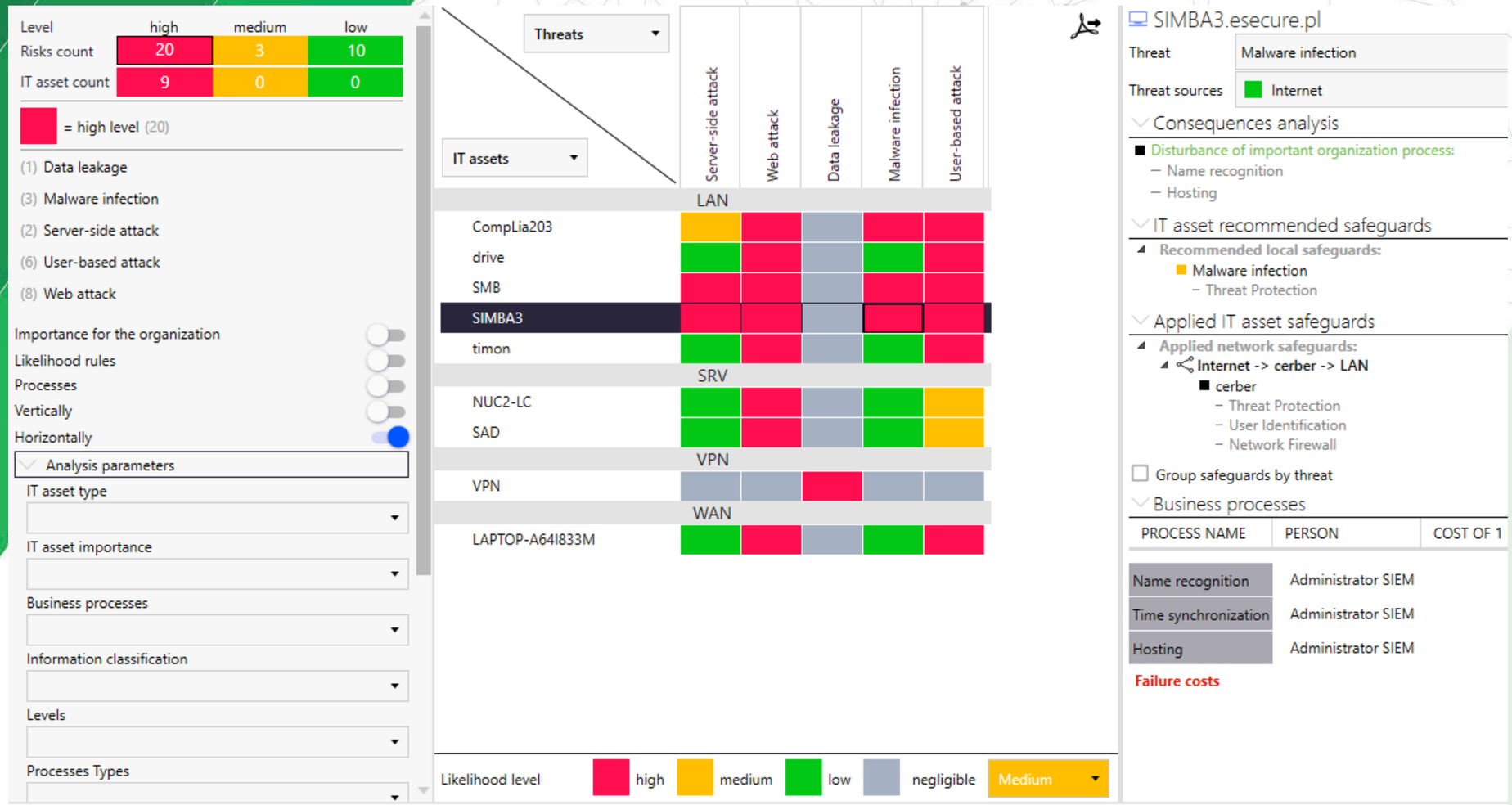


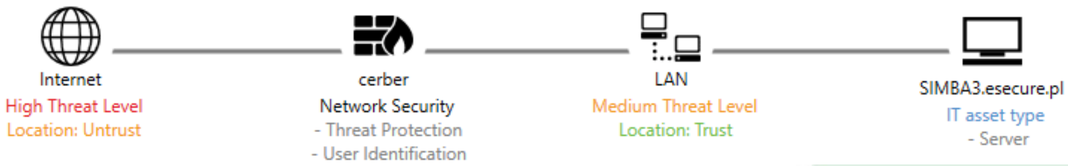

| RULE | SEVERITY | EVENTS |
|---|---|---|
| Spoofing process | 10 | 15 |
| Trusted Developer Utilities Proxy... | 5 | 12 |
| Triggered Execution of cmd | 5 | 12 |
| Triggered Execution of PowerShell | 5 | 12 |
| Accessibility Features | 5 | 1 |
| Searching for credentials in files | 5 | 24 |
| Batch login to Windows host | 5 | 1 |
| Same user account activity on diff... | 0 | 12 |
| Same user account activity on diff... | 0 | 12 |
| Privileged user logged in through... | 0 | 8 |
| A Kerberos service ticket accepted | 0 | 3 |
| Threat alert when browsing the In... | 0 | 2 |
| Remote login to Windows host | 0 | 1 |
| Windows computer unlocked | 0 | 4 |
| Privileged user authentication | 0 | 6 |
| Account enumeration reconnaissa... | 0 | 1 |
| Process hash detected as a stand... | 0 | 1 |

Automatyczne wykrywanie połączeń miedzy urządzeniami sieciowymi i strefami bezpieczeństwa

Integracja z narzędziami detekcji incydentów i podatności

# Analiza ryzyka cyberzagrożeń – GRC




Silnik GRC oparty o reguły prawdopodobieństwa (priorytetyzacja), słowniki i wyniki z CMDB

Automatyczna wizualizacja potencjalnych wektorów ataków

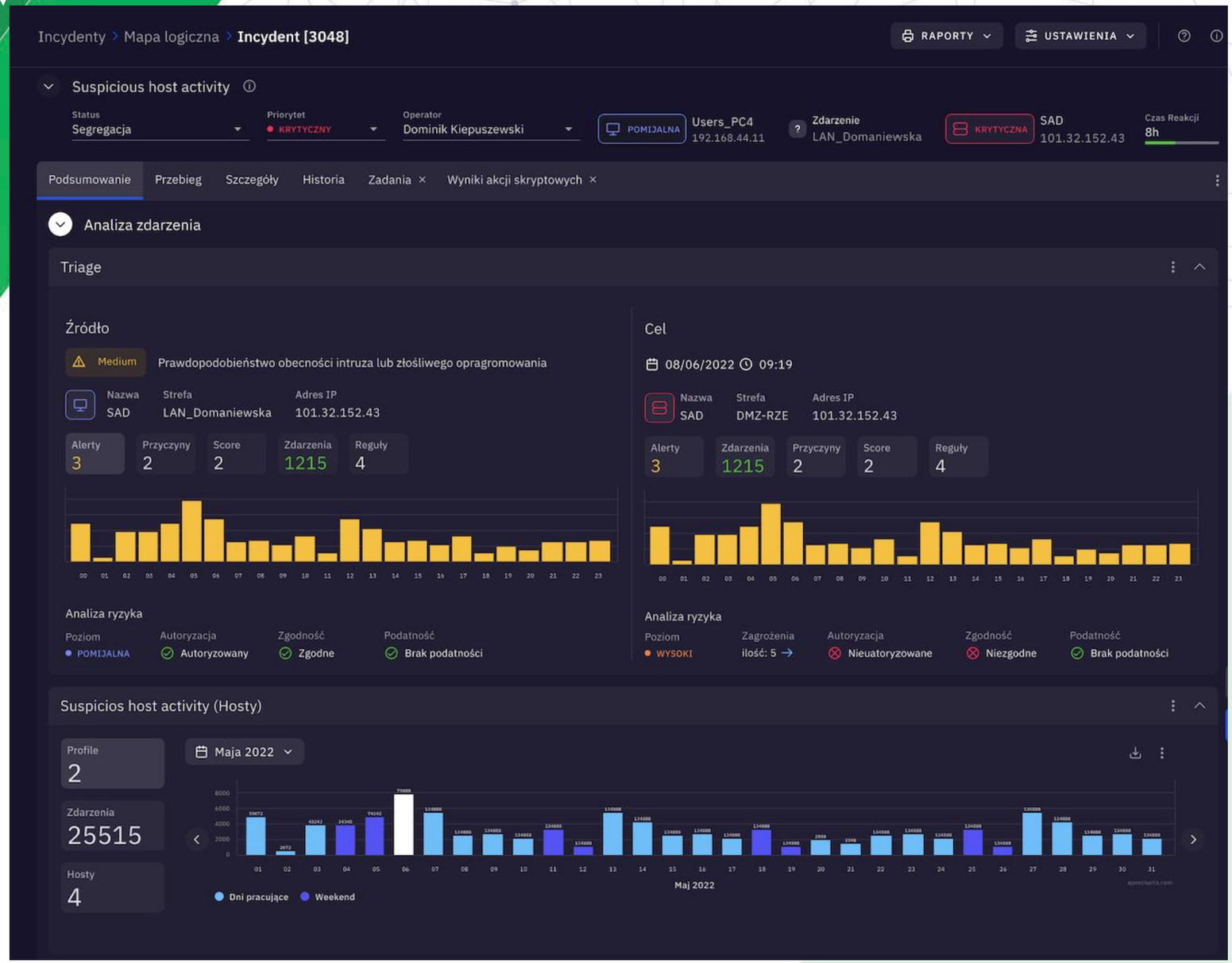
Automatyczna informacja o konsekwencjach zmaterializowania się zagrożenia

Automatyczna sugestie obniżenia poziomu ryzyka cyber dla zasobu IT lub procesu

Możliwość opracowania strategii i planów postepowania z ryzykiem

Integracja z narzędziami detekcji incydentów i podatności

# Wykrywanie i obsługa incydentów – SIEM/UEBA




Usprawnienie w zakresie dostarczenia informacji kontekstowych o zasobach IT i użytkownikach

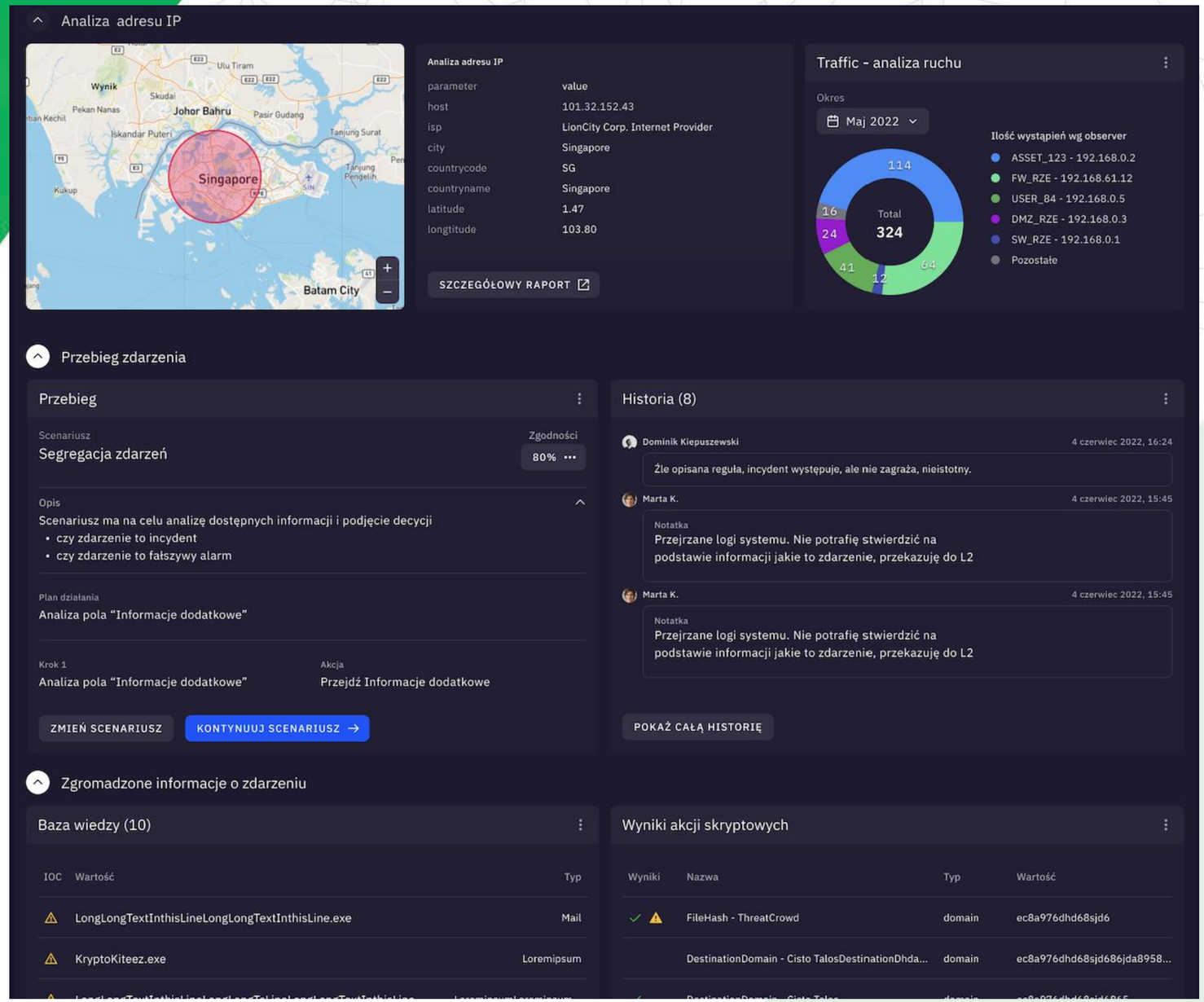
Jeden panel podsumowania zawierający natychmiastowy wgląd w logi bezpieczeństwa

Uzupełniające informacje z silnika UEBA – analiza AI pod kątem anomalii w zachowaniu systemów i użytkowników

Dwukierunkowa integracja z narzędziami typu Vulnerability Management

Zdefiniowany mechanizm czasów SLA i jasna ścieżka eskalacji

# Wykrywanie i obsługa incydentów – SIEM/SOAR




Automatyczna reakcja na zdarzenie i incydent bezpieczeństwa – gotowe scenariusze reakcji

Pełen wgląd w workflow incydentu z możliwością analizy historii przebiegu

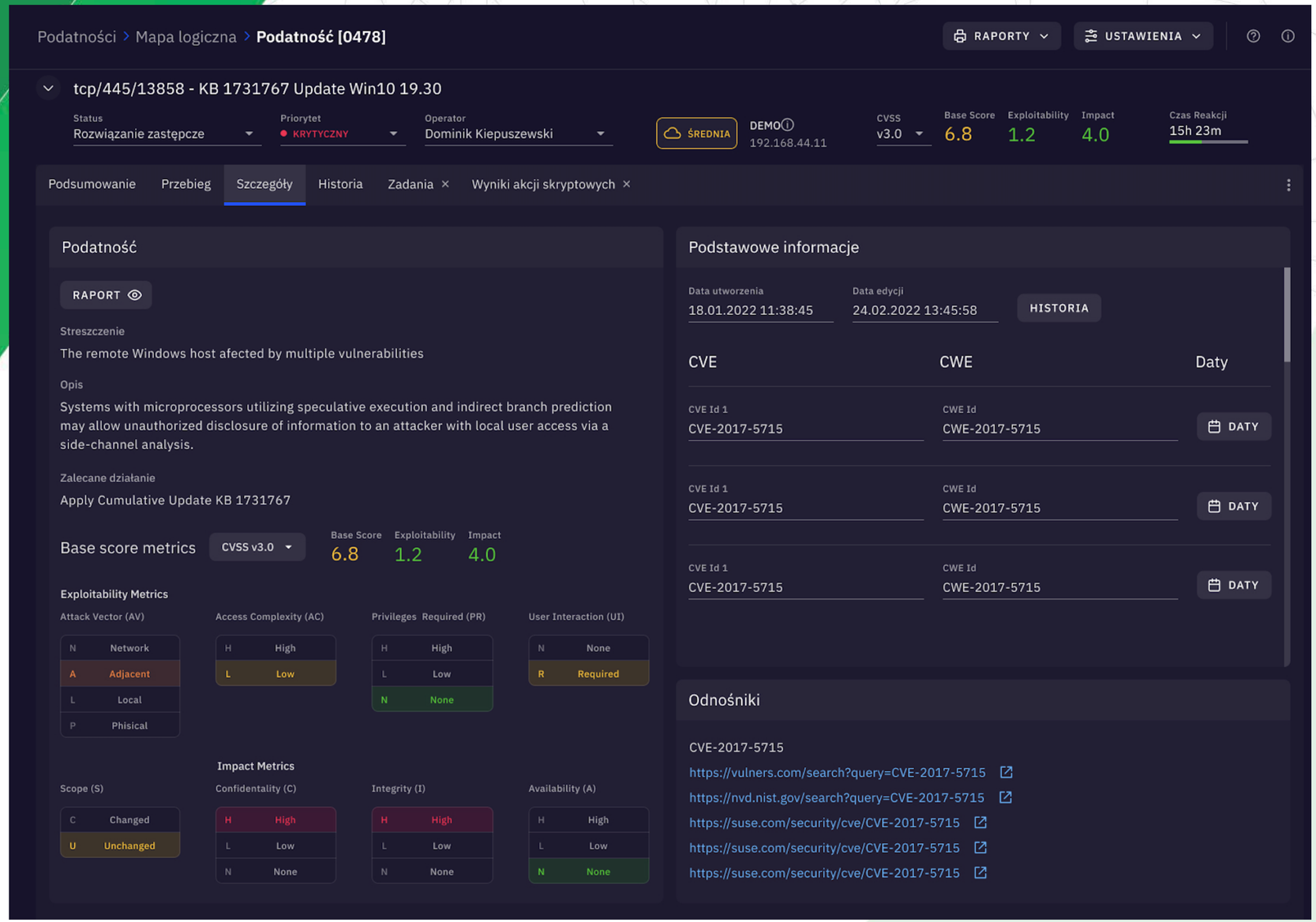
Integracja z narzędziami CTI i wewnętrzną bazą wiedzy w celu automatycznej weryfikacji wykrytego zagrożenia

Automatyczny wgląd w wyniki akcji skryptowych

Gotowe formularze zgłoszeniowe do CSIRT

Natychmiastowe informacje o wektorze ataku

# Wykrywanie i obsługa podatności – TVM




Automatyczna reakcja na krytyczną podatność - scenariusze reakcji (manualne i automatyczne)

Dwukierunkowa integracja z wieloma silnikami skanującymi dla ułatwienia procesu VM

Integracja z narzędzia CMDB i GRC celem priorytetyzacji biznesowej podatności oraz natychmiastowego wglądu w jej kontekst organizacyjny

Wzbogacenie narzędzi wykrywania incydentów o możliwe informacje dotyczące wykorzystania danej podatności

# Podsumowanie

secureVISIO

01 NIS 2 wprowadza **większy zakres podmiotów objętych prawnym obowiązkiem utrzymania cyberbezpieczeństwa** (podmioty kluczowe i ważne) oraz **bardziej rygorystyczne mechanizmy raportowania incydentów i konsekwencje zaniedbania cyberbezpieczeństwa**

02 **Automatyzacja i usprawnienie** w określonych obszarach NIS 2 można osiągnąć z wykorzystaniem zintegrowanych platform zarządzania bezpieczeństwem jak **SecureVisio**

03 Proces wyboru platformy musi uwzględniać **poziom integracji w jej ramach kilku narzędzi z obszaru strategicznego jak i operacyjnego bezpieczeństwa IT – CMDB, GRC, SIEM, UEBA, SOAR, TVM, XDR**

04 Platforma cyber jako centralny punkt dowodzenia musi uwzględniać możliwość integracji ze **źródłami CTI** oraz być wyposażona w **automatyczne mechanizmy reakcji**.

secureVISIO

# Dziękuję za uwagę

www.securevisio.com