THE NEW ERA OF EXPOSURE MANAGEMENT

Odkryj i zabezpiecz całą powierzchnię ataku

– w tym nieznane i niezarządzane zasoby

runZero · Kappa Data Polska

IT · OT · IoT
jeden inwentarz

0 agentów
bez poświadczeń

NIS2 / KSC2
zarządzanie aktywami

Kappa Data
THE ART OF
IT INFRASTRUCTURE, SECURITY AND IOT DISTRIBUTION

AGENDA – 30 MINUT

Od problemu do konsoli – i do tego, co z tego wynika dla NIS2 / KSC2.

1	**Czego nie widać w sieci**	dlaczego atakowane są drukarki, kamery i PLC	5 min
2	**Dlaczego skaner i EDR nie wystarczą**	martwe punkty klasycznego podejścia	5 min
3	**Jak działa runZero**	bez agentów, bez poświadczeń – architektura	5 min
4	**Konsola krok po kroku**	instalacja, inwentarz, topologia, ryzyka	10 min
5	**NIS2 / KSC2 i następny krok**	co runZero realnie pokrywa · trial · Q&A	5 min

RUNZERO – O FIRMIE

Firma założona w 2018 r. przez HD Moore'a – twórcę Metasploita.

2018

założenie firmy przez HD Moore'a, twórcę Metasploita

500+

klientów z sektora komercyjnego i publicznego

18K+

użytkowników bezpłatnej edycji Community

Dla admina: narzędzie pisane przez ludzi od ofensywnego bezpieczeństwa – patrzy na sieć tak, jak atakujący.

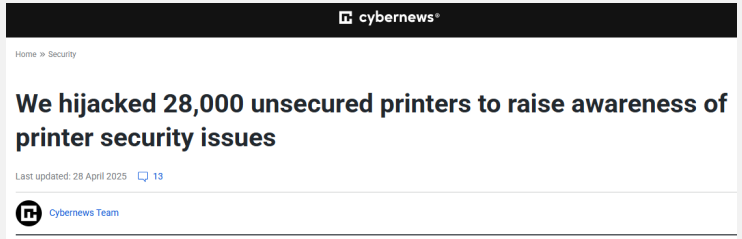
Dane wg runZero (2025).

NIE TYLKO ZASOBY KRYTYCZNE SĄ ATAKOWANE

Kamery, drukarki, sterowniki PLC, urządzenia „smart” – to dziś realne wejście do sieci.











Raport pełnomocnika rządu ds. cyberbezpieczeństwa

Z opublikowanego w kwietniu br. **raportu pełnomocnika rządu ds.** cyberbezpieczeństwa wynika, że w **2023 r.** odnotowano ponad **80 tys. incydentów cyberbezpieczeństwa** co stanowi **100-procentowy** wzrost cyberataków w **porównaniu do 2022 r.**

Wniosek: atakujący nie wybiera najlepiej chronionego serwera – wybiera urządzenie, o którym zapomnieliście.

DZISIEJSZA POWIERZCHNIA ATAKU

Złożona, dynamiczna i stale rosnąca – a spis zasobow starzeje się w dniu zapisu.

NIS2 art. 21 · lit. i

CO JEST PODATNE NA ATAK

- **Wewnętrzne · zewnętrzne**
- **IT · OT · IoT**
- **Mobilne · chmurowe**
- **Zarządzane · niezarządzane**

ROSNĄCA ZŁOŻONOŚĆ

- Łączenie i przenikanie OT / IT
- IoT wszędzie
- Migracje do chmury, BYOD, wirtualizacja

PRZYKŁADOWE ZASOBY W JEDNEJ ORGANIZACJI

Strona WWW	VPN	Domeny	Serwery w Internecie
Firewall	Bramy Zero Trust	Data center	Chmura
Kontenery	Repozytorium kodu	Środowisko dev	Usługi zewnętrzne
Przejęta firma	Serwery	Laptop + hotspot	Smartfon
Drukarka	Kamera IP	Urządzenie IoT	Termostat
Terminal POS			

KLASYCZNE PODEJŚCIE = MARTWE PUNKTY

Priorytetem jest zwykle lista CVE – a większość realnego ryzyka leży gdzie indziej.

NIS2 art. 21 · lit. e

11%

– tylko tyle krytycznych zagrożeń to znane podatności (CVE)

Dane wg runZero.

CO TRAKTUJEMY PRIORYTETOWO

- CVE z wysokim score
- KEV – podatności aktywnie wykorzystywane
- tylko część powierzchni, widoczna i monitorowana

CO NALEŻY TRAKTOWAĆ PRIORYTETOWO

- **! Zero-day**
- **! Błędne konfiguracje**
- **! Sprzęt end-of-life**
- **! Domyślne hasła**
- **! Zasoby wewnętrzne wystawione na zewnątrz**
- **! Otwarty dostęp do baz danych**
- **! Problemy z segmentacją**
- **! Usługi publicznie wystawione**
- **! Wygasłe certyfikaty**
- **! Współdzielone klucze**
- **! Porzucone podsieci**

TRADYCYJNE SKANERY NIE NADĄŻAJĄ

Zagrożenia się zmieniły, atakujący są szybsi – a większość urządzeń nie ma agenta.

60%
urządzeń pozostaje w dużej mierze niewidocznych

43%
urządzeń w firmie działa bez agentów

70%
incydentów ma źródło w zasobach bez agenta

72%
atakujących znajduje słaby punkt w < 5 h

51%
sieci OT połączonych z IT

74%
urządzeń OT ma krytyczne podatności

33%
urządzeń IoT ma krytyczne podatności

11%
krytycznych ryzyk to znane CVE

DLACZEGO STARE SKANERY ZOSTAŁY W TYLE

Ograniczona widoczność OT, IoT i zasobów nieznanych

Zbyt wolne i skomplikowane

Skupienie wyłącznie na CVE

Dużo fałszywych alarmów

Dane wg runZero – źródła badań w materiałach producenta.

EDR, SKANER PODATNOŚCI CZY RUNZERO?

Nie „zamiast”, tylko „razem”: EDR robi wykrywanie z uwierzytelnieniem, runZero – całą resztę.

	Skaner podatności	EDR (endpoint)	runZero
Metoda	uwierzytelniona / aktywna (ograniczona bez poświadczeń)	uwierzytelniona (agent)	**bez uwierzytelnienia**
Agenci i poświadczenia	zalecane – bez nich wyniki słabe	wykorzystuje istniejących agentów	**bez agentów**
Zasięg	endpointy + urządzenia sieciowe	endpointy on-prem, chmura, efemeryczne	**IT, OT, IoT, niezarządzane i nieznane**
Typ zagrożeń	CVE	CVE	**także ryzyka spoza CVE**
Wpływ na sieć	wysoki	minimalny	**niski**

Efekt: EDR zostaje tam, gdzie jest agent – runZero dokłada to, czego agent nigdy nie zobaczy. Klienci znajdują średnio 25% więcej zasobów (wg runZero).

RUNZERO – PEŁNA WIDOCZNOŚĆ POWIERZCHNI ATAKU

Bez agentów · bez poświadczeń · bez dodatkowego sprzętu – SaaS, on-prem lub air-gapped.

NIS2 art. 21 · lit. i, e, f

25%

więcej zasobów niż tradycyjne narzędzia (wg runZero) – często te najbardziej podatne

JAK ZBIERA DANE

Aktywne skanowanie | **Pasywne wykrywanie** | **Integracje API**

Brakujące 25% to zwykle: zasoby bez podstawowych zabezpieczeń, niezarządzane lub źle skonfigurowane, przypadkiem wystawione do Internetu, przestarzałe (EoL).

1 Pełna widoczność

- Wszystkie zasoby IT, OT i IoT – także nieznane
- Jeden widok – wewnątrz i z zewnątrz
- Dokładny fingerprint każdego zasobu

2 Wykrywanie ekspozycji

- Podatności, które inne narzędzia pomijają
- Reakcja na zero-day bez ponownego skanu
- Ryzyka OT, IoT i zasobów niezarządzanych

3 Priorytetyzacja ryzyka

- Krytyczne podatności wg analizy ryzyka
- Kontekst i atrybuty zasobu
- Wskazówki naprawcze

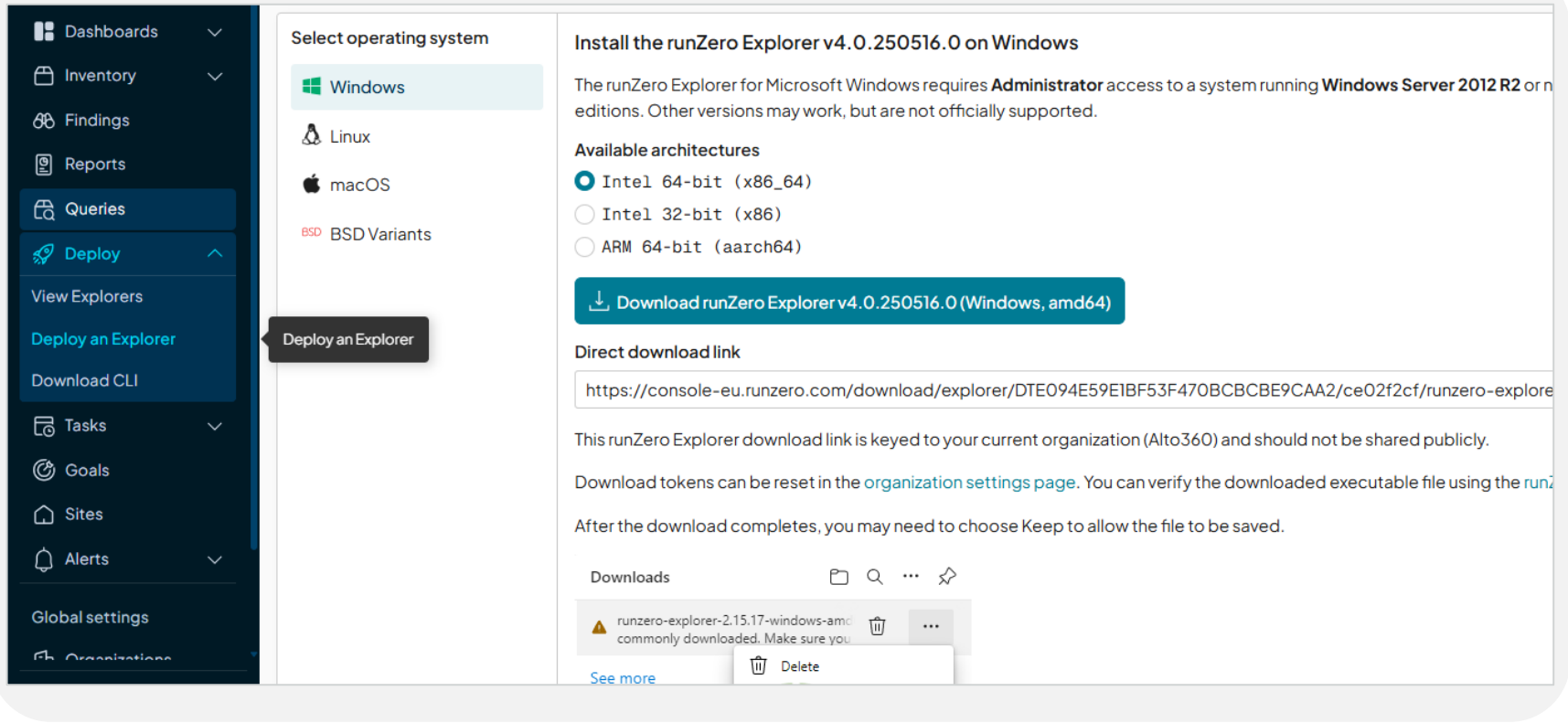
4 Zgodność i raportowanie

- Wykrywanie i monitorowanie zasobów
- Prostsze raporty zgodności
- Cele i wskaźniki (KPI) poprawy

Fingerprint bez hasła: system, producent, model, rola urządzenia – rozpoznane z samego ruchu sieciowego.

KROK 1 – INSTALACJA EXPLORERA

Windows, Linux, macOS lub BSD – pobierasz instalator prosto z konsoli.



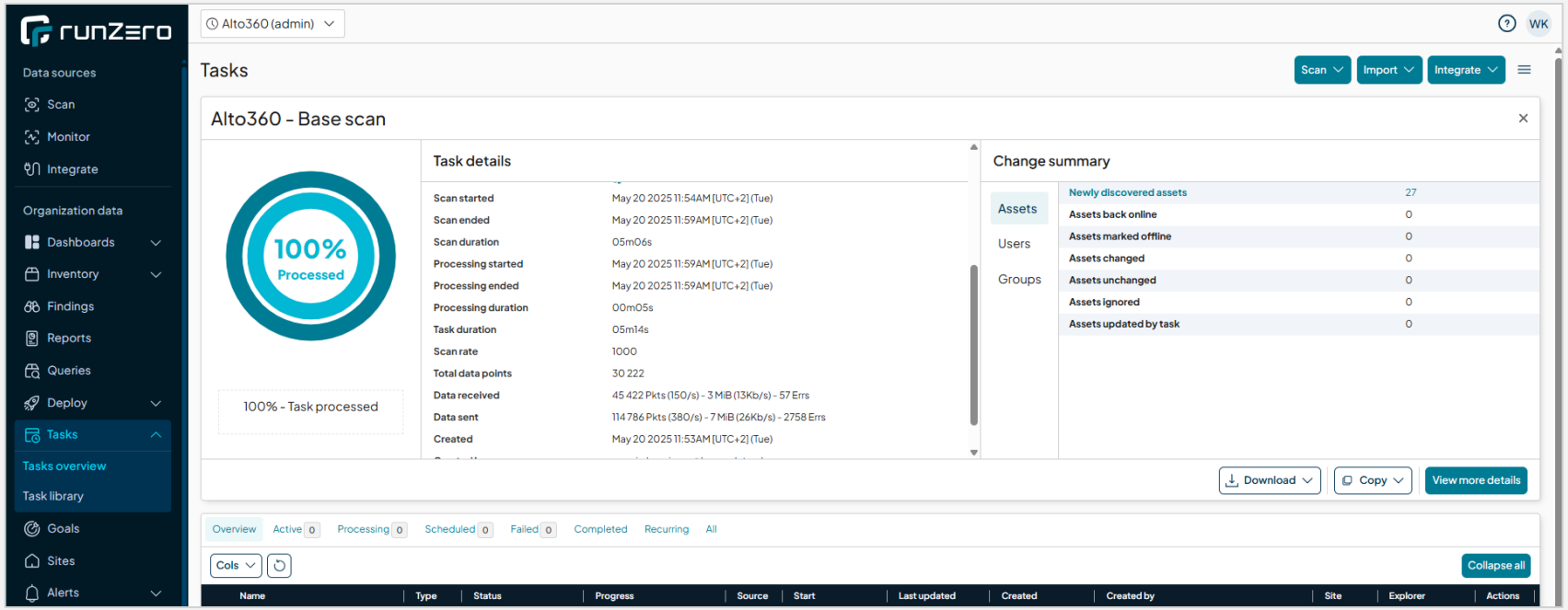
NA CO PATRZEĆ

- Wybór systemu i architektury
- Link przypisany do Twojej organizacji – nie udostępniaj go
- Wymagane uprawnienia administratora

KROK 2 – PIERWSZY SKAN

Zadanie skanowania: postęp, czas trwania i podsumowanie zmian.

NIS2 art. 21 · lit. i



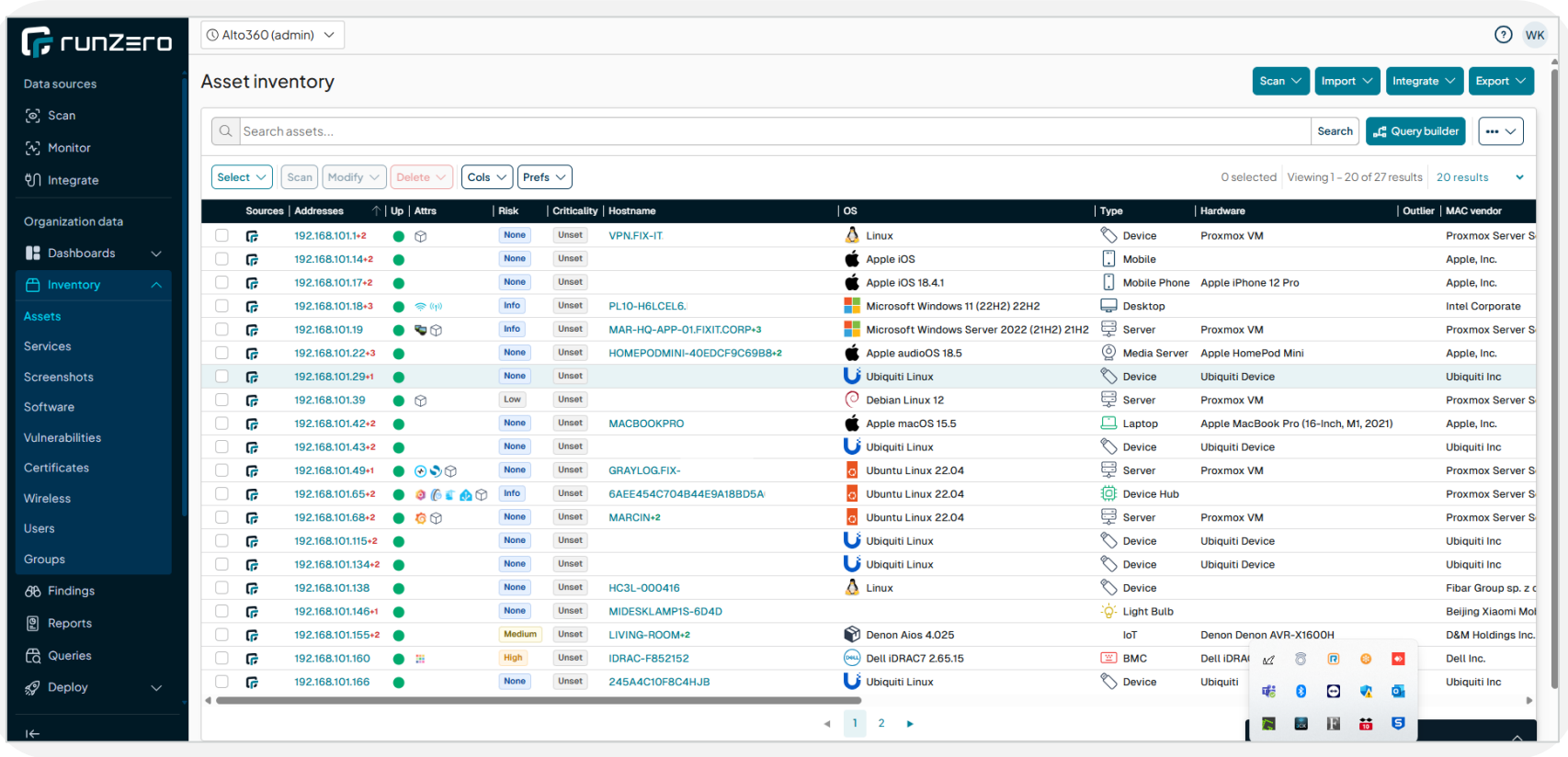
NA CO PATRZEĆ

- Nowe, zmienione i offline zasoby po każdym skanie
- Statystyki: liczba hostów, pakietów, czas
- Skany cykliczne – inwentarz zawsze aktualny

KROK 3 – INWENTARZ ZASOBÓW

Jedna lista: adresy, system, typ, producent, ryzyko, krytyczność.

NIS2 art. 21 · lit. i



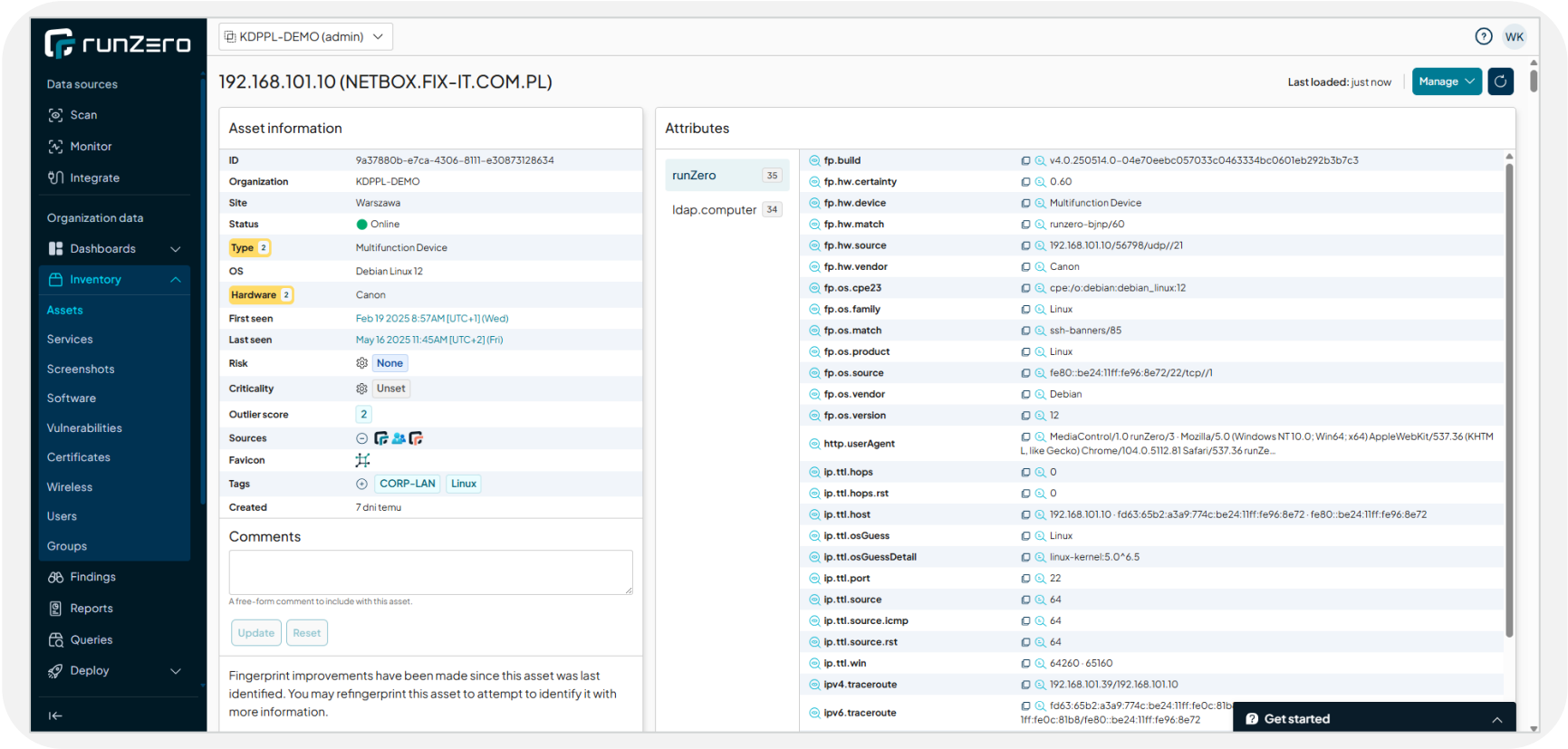
NA CO PATRZEĆ

- IT, OT, IoT, mobile – w jednej tabeli
- Filtry i zapytania, eksport do CSV / API
- Kolumny ryzyka i krytyczności

KROK 4 – SZCZEGÓŁY ZASOBU

Fingerprint urządzenia bez logowania: system, sprzęt, usługi, historia.

NIS2 art. 21 · lit. i



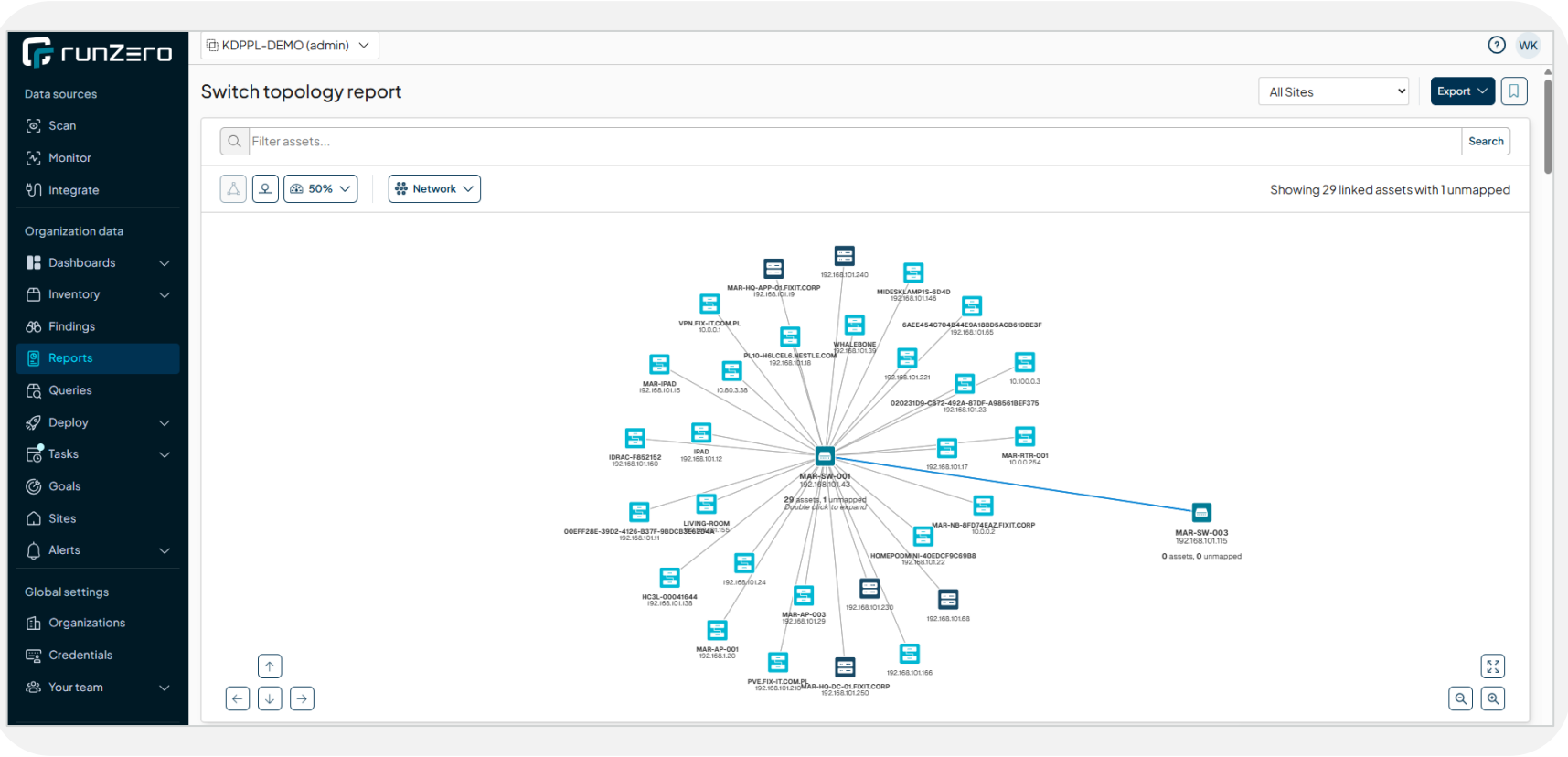
NA CO PATRZEĆ

- Setki atrybutów z każdego źródła danych
- Pierwsze i ostatnie wykrycie zasobu
- Tagi, właściciel, krytyczność, komentarze

KROK 5 – TOPOLOGIA PRZEŁĄCZNIKÓW

Mapa połączeń: który zasób wisi na którym porcie przełącznika.

NIS2 art. 21 · lit. a, e



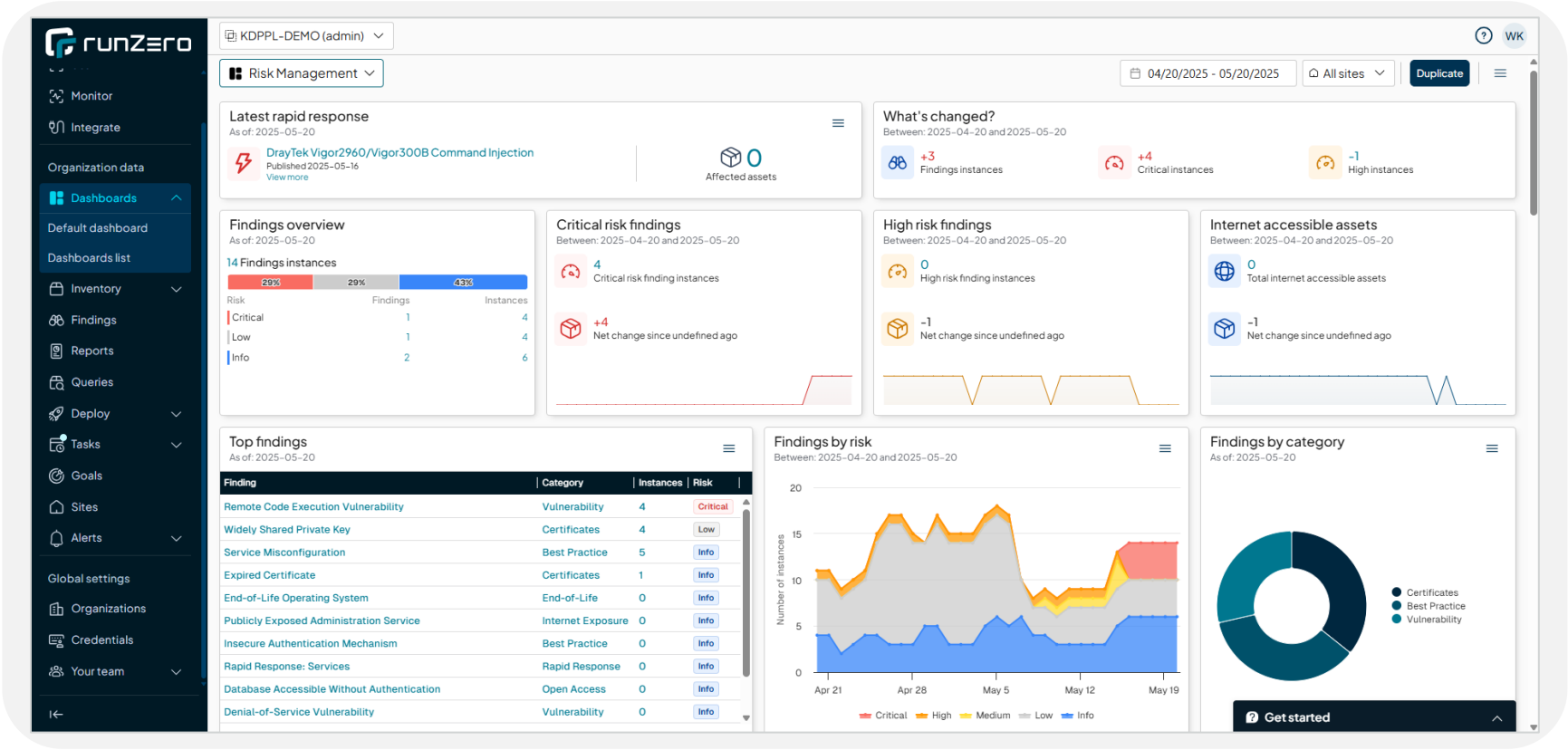
NA CO PATRZEĆ

- Szybkie lokalizowanie nieznanych urządzeń
- Weryfikacja segmentacji w praktyce
- Zasoby niepowiązane – do wyjaśnienia

KROK 6 – ZARZĄDZANIE RYZYKIEM

Co się zmieniło, krytyczne ryzyka i zasoby dostępne z Internetu.

NIS2 art. 21 · lit. a, e



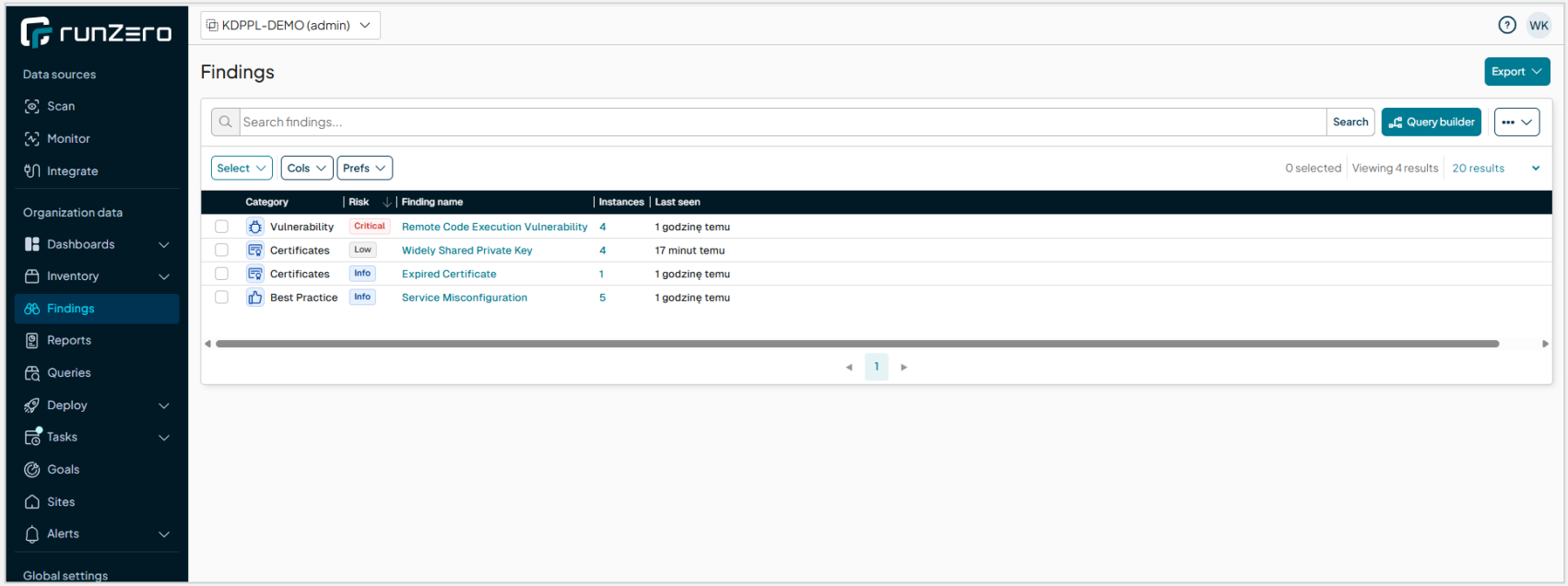
NA CO PATRZEĆ

- Szybka reakcja na nowe zagrożenia (Rapid Response)
- Ryzyka krytyczne i wysokie w czasie
- Zasoby dostępne z Internetu

KROK 7 – USTALENIA (FINDINGS)

Lista ryzyk także spoza CVE: certyfikaty, błędne konfiguracje, dobre praktyki.

NIS2 art. 21 · lit. e, h



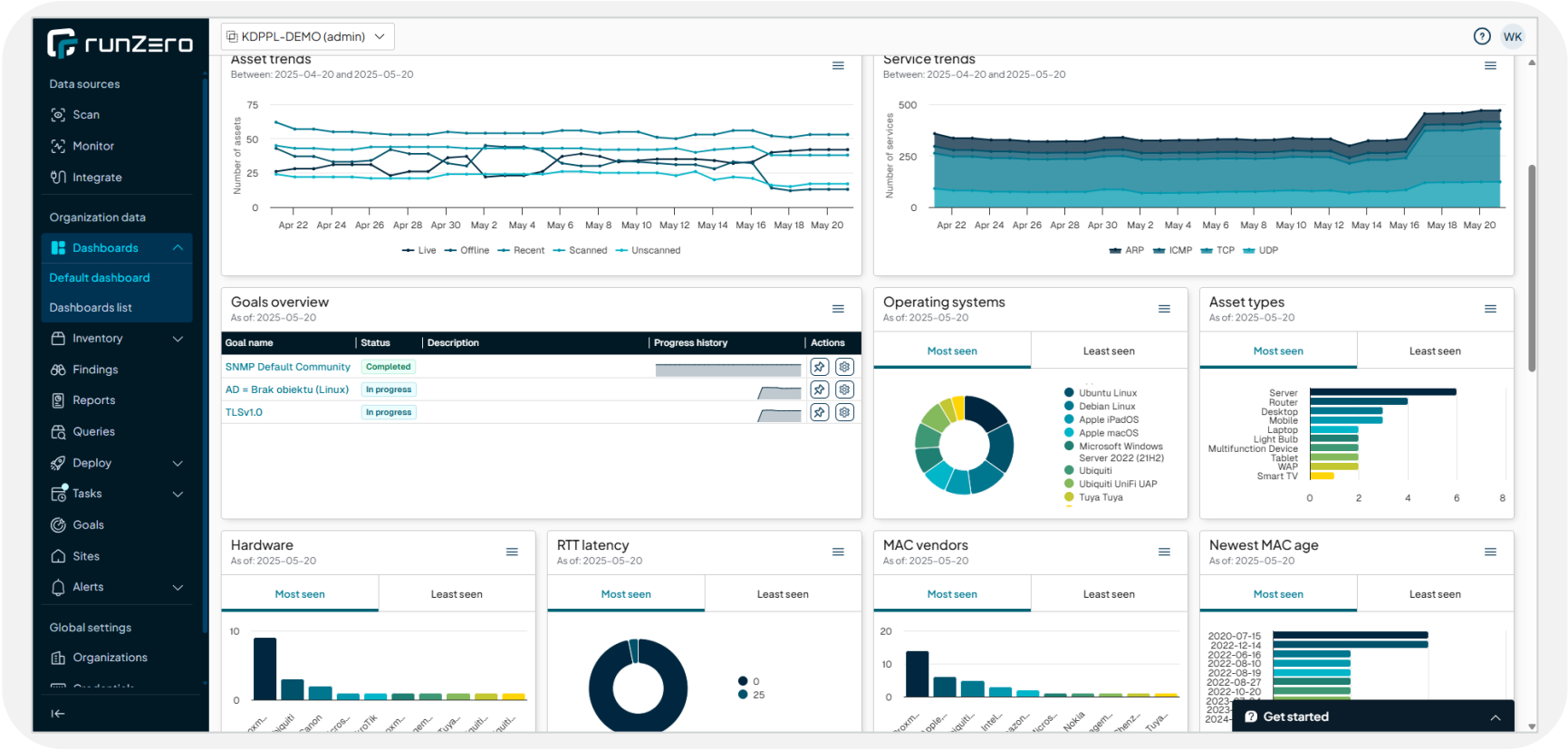
NA CO PATRZEĆ

- Kategorie: podatności, certyfikaty, best practice
- Liczba instancji i ostatnie wykrycie
- Eksport do zgłoszeń / ITSM

KROK 8 – DASHBOARD I CELE

Trendy zasobów i usług, systemy, typy urządzeń, cele poprawy.

NIS2 art. 21 · lit. f



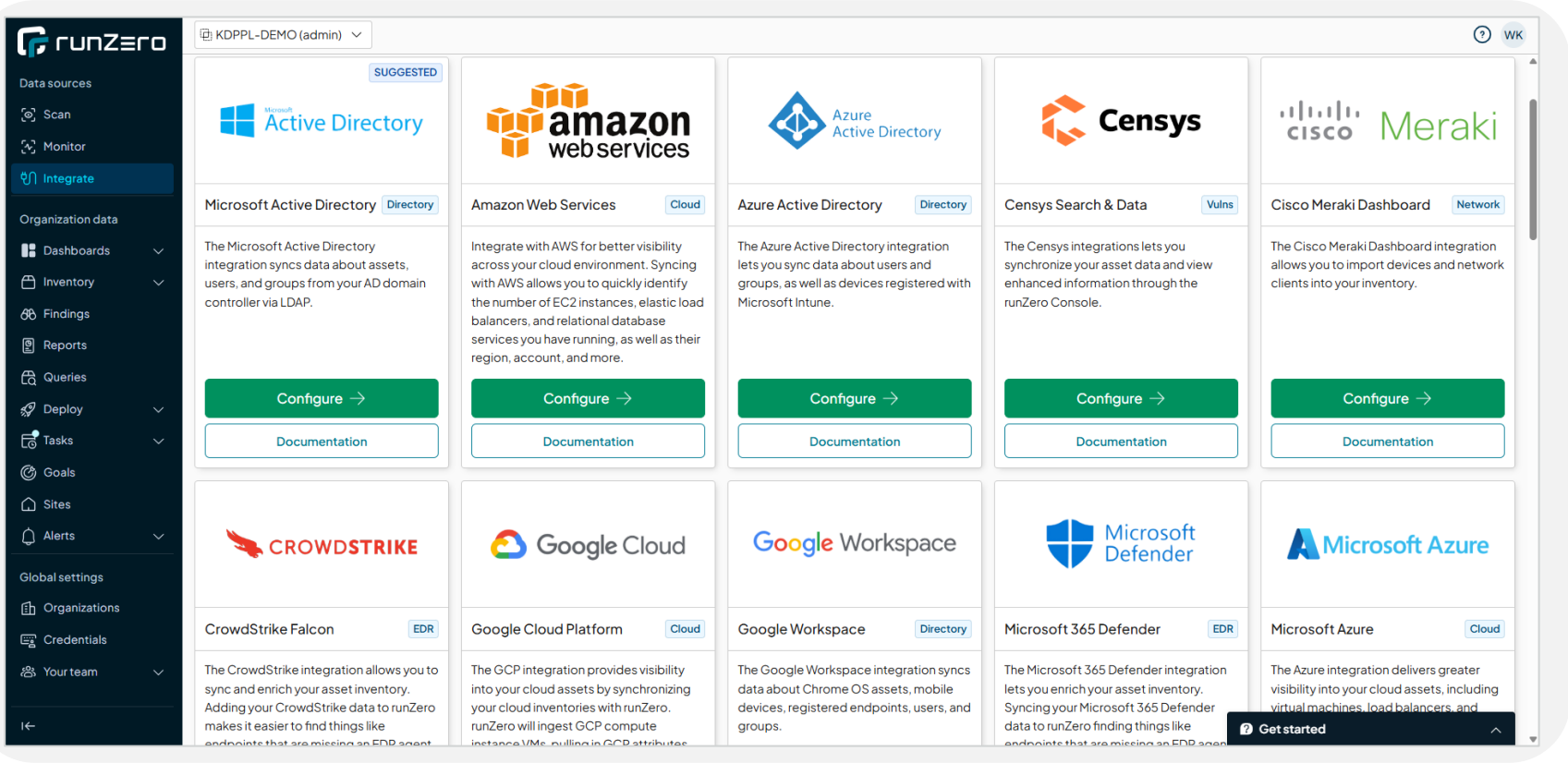
NA CO PATRZEĆ

- Trend zasobów: nowe, offline, przeskanowane
- Systemy operacyjne i producenci (MAC)
- Cele (Goals) – np. zero domyslnych hasel SNMP

KROK 9 – INTEGRACJE

Połącz dane z narzędziami, które już masz.

NIS2 art. 21 · lit. b, i



NA CO PATRZEĆ

- AD, Entra / Azure, Google Workspace
- AWS, Azure, Google Cloud, Meraki
- CrowdStrike, Microsoft Defender, Censys

GDZIE RUNZERO ODPOWIADA NA NIS2 / KSC2

Art. 21 NIS2 (w KSC2: art. 8) – uczciwie: gdzie runZero realizuje wymóg, a gdzie tylko go wspiera.

Wymóg (NIS2 art. 21 ust. 2)	Co daje runZero	Poziom
i) zarządzanie aktywami	aktualny inwentarz IT / OT / IoT, właściciele, krytyczność	**realizuje**
a) analiza ryzyka	kontekst zasobów i ekspozycji, zasoby dostępne z Internetu	**realizuje**
e) podatności i utrzymanie	ryzyka CVE i spoza CVE, EoL, Rapid Response dla zero-day	**realizuje**
f) ocena skuteczności	cele (Goals), trendy, raporty – dowody dla audytora	**realizuje**
d) łańcuch dostaw	widoczność urządzeń zarządzanych przez dostawców	**wspiera**
g) cyberhigiena	wykrywa przestarzałe systemy i brak zabezpieczeń	**wspiera**
h) kryptografia · j) MFA	wykrywa certyfikaty, stare protokoły, brak MFA – nie wdraża ich	**wspiera**
b) obsługa incydentu (24 / 72 h)	bieżący obraz zasobów i ich ekspozycji w trakcie incydentu	**wspiera**

runZero wspiera środki techniczne – nie „daje zgodności”. Zgodność to proces SZBI + dowody jego działania.

NASTĘPNY KROK

Sprawdźcie na własnej sieci, co jeszcze się w niej kryje.

1

Bezpłatny trial

21 dni pełnej wersji runZero – na własnej sieci

2

PoC z Kappa Data

instalacja Explorera i pierwszy skan z naszym inżynierem

Kontakt: Kappa Data Polska

info@kappadata.pl · +48 22 104 40 40 · www.kappadata.pl

Dziękuję – pytania?

runZero · Kappa Data Polska

info@kappadata.pl · +48 22 104 40 40

Kappa Data
THE ART OF
IT INFRASTRUCTURE, SECURITY AND IOT DISTRIBUTION