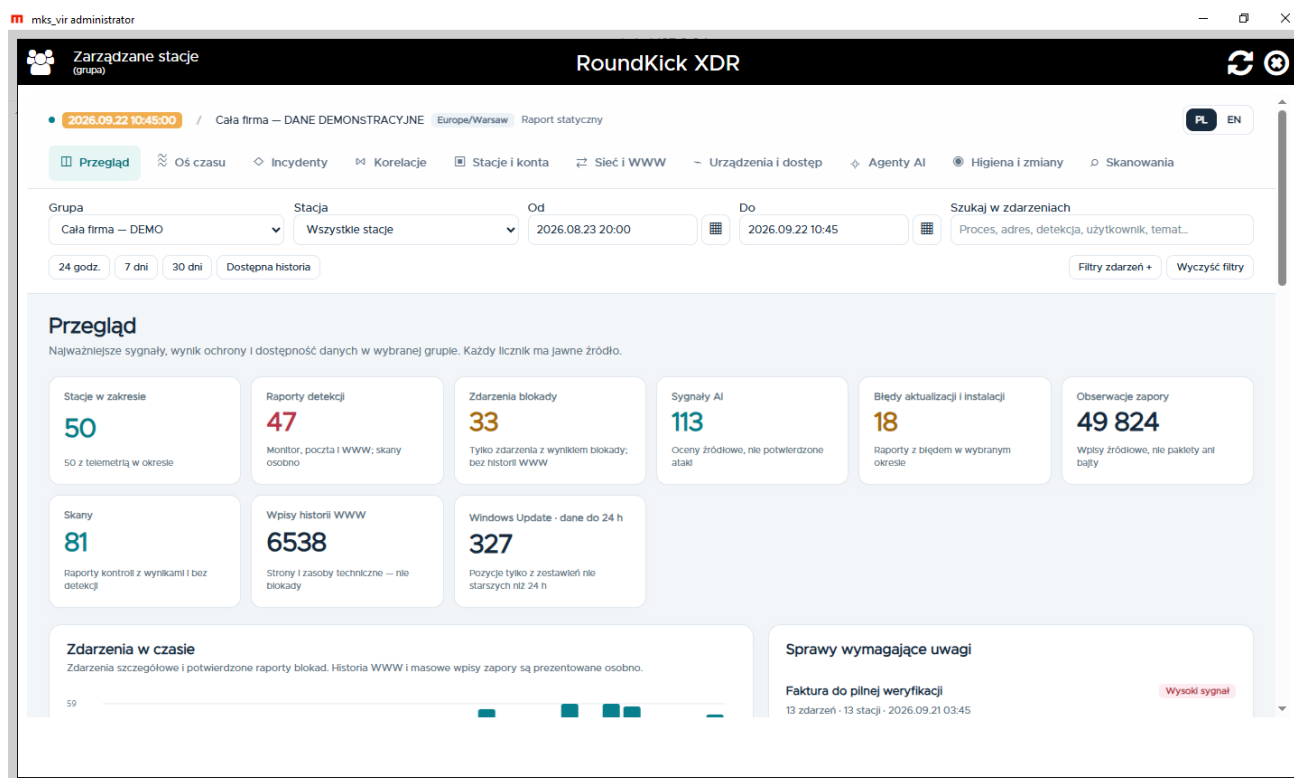


mks_vir administrator – instrukcja „RoundKick XDR”

Wprowadzenie

RoundKick XDR jest raportem analitycznym łączącym w jednym miejscu informacje z ochrony antywirusowej, skanów, zapory, WWW, urządzeń, sesji użytkowników, agentów AI, wydajności systemów oraz danych o aktualizacjach. Raport służy do szybkiego znalezienia zdarzeń wymagających uwagi i przejścia od podsumowania do dowodów źródłowych.

Raport statyczny – widok przedstawia stan danych z chwili wygenerowania raportu; nie jest konsolą czasu rzeczywistego; data i godzina w lewym górnym rogu określają moment wygenerowania



Nawigacja i filtry

Górny pasek jest wspólny dla wszystkich zakładek. Pozwala wybrać grupę, stację, zakres czasu oraz wyszukiwać tekstowo. Przyciski „24 godz.”, „7 dni”, „30 dni” i „Dostępna historia” szybko ustawiają zakres analizy:

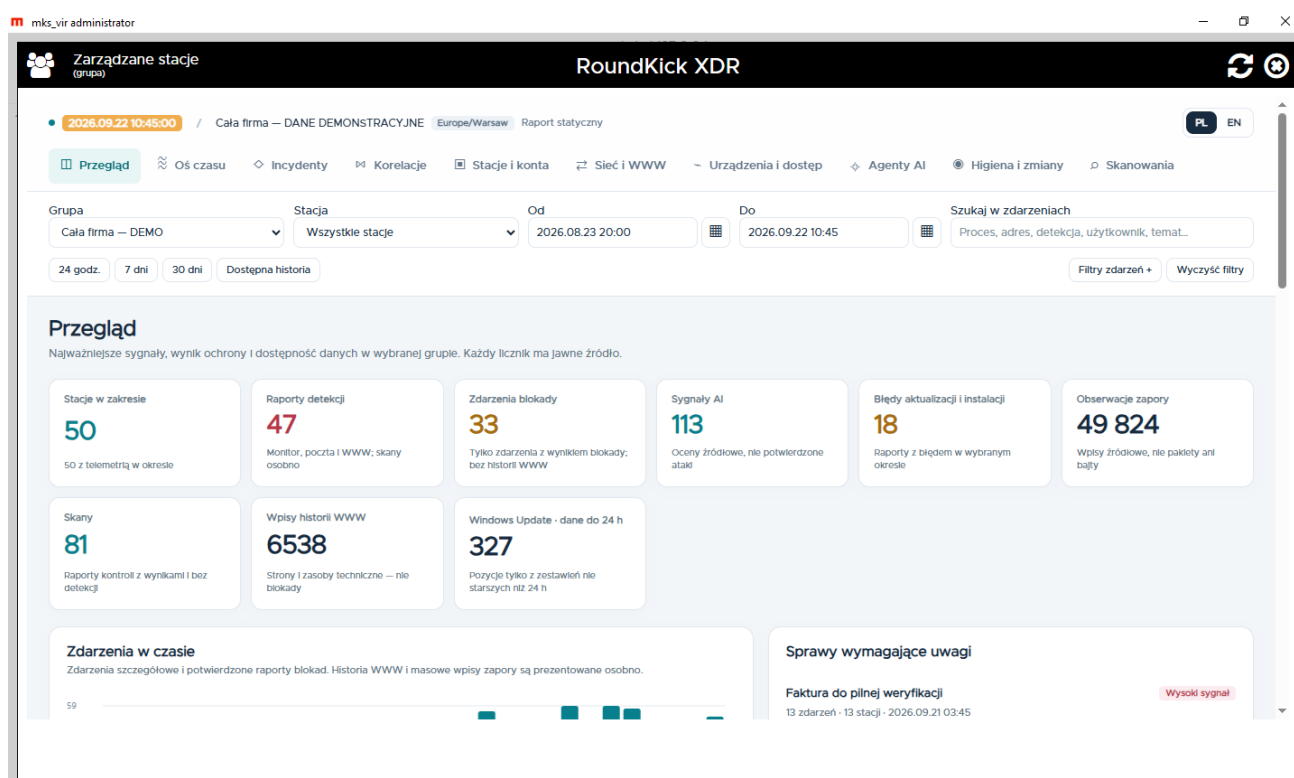
- **Grupa** – ogranicza raport do wybranej jednostki organizacyjnej i jej stacji
- **Stacja** – pozwala analizować pojedynczy komputer
- **Od / Do** – definiuje analizowany przedział czasu
- **Szukaj w zdarzeniach** – przeszukuje m.in. procesy, adresy, detekcje, użytkowników i tematy

- **Filtry zdarzeń** – umożliwiają zawężanie według kategorii, priorytetu, wyniku ochrony, użytkownika, źródła, kodu raportu i statusu
- **Wyczyść filtry** – przywraca neutralny stan filtrów zdarzeń

Wiek raportu – jeżeli raport ma więcej niż 1 godzinę, data wygenerowania jest oznaczana pomarańczowym tłem; po przekroczeniu 24 godzin tło staje się czerwone; to sygnał aktualności raportu, nie alarm bezpieczeństwa

Przegląd

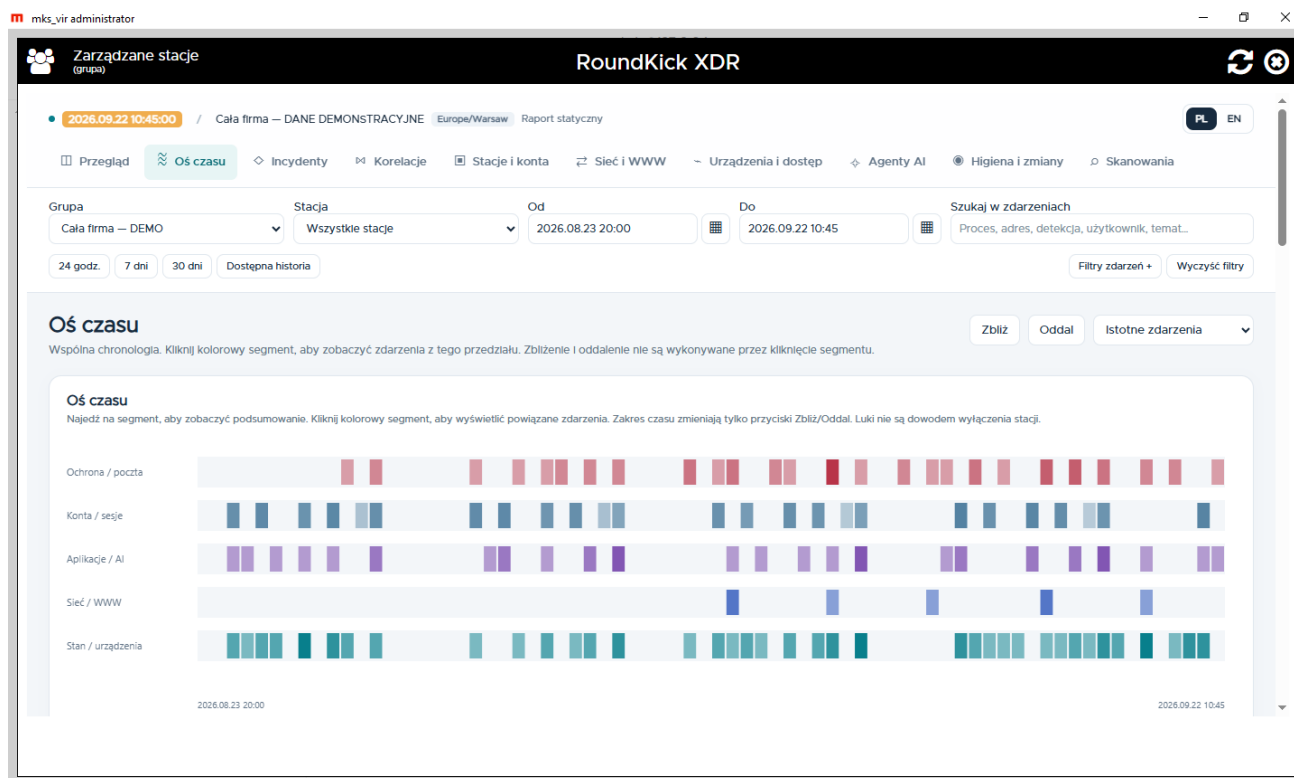
Przegląd jest stroną startową. Pokazuje najważniejsze liczniki oraz skróty do danych wymagających dalszej analizy. Kliknięcie kafelka może otworzyć właściwy widok szczegółowy; po powrocie do Przeglądu automatyczny filtr drill-down jest usuwany, a ręcznie ustawione filtry użytkownika pozostają.



- **Stacje w zakresie** – liczba stacji objętych bieżącym filtrem
- **Raporty detekcji** – raporty ochrony monitor/poczta/WWW; wyniki skanów są liczone osobno
- **Zdarzenia blokady** – tylko zdarzenia, dla których źródło zgłasza wynik blokady; nie obejmuje historii WWW
- **Sygnały AI** – sygnały źródłowe do analizy, nie automatycznie potwierdzone ataki
- **Obserwacje zapory** – liczba wpisów źródłowych; nie pakietów ani bajtów
- **Windows Update** – licznik wykorzystuje wyłącznie odpowiednio świeże zestawienia stacji i zachowuje datę danych

Oś czasu

Oś czasu grupuje zdarzenia w pasach tematycznych: ochrona/pocztą, konta/sesje, aplikacje/AI, sieć/WWW oraz stan/urządzenia. Intensywność koloru odzwierciedla liczbę zdarzeń w danym przedziale.



- Najechnanie na segment wyświetla tooltip z kategorią, zakresem czasu i podsumowaniem zawartości
- Kliknięcie segmentu nie zmienia zakresu Od-Do. Zaznacza przedział i pokazuje listę zdarzeń poniżej
- Animowane trójkąty pod zaznaczonym segmentem kierują uwagę do panelu „Zdarzenia w zaznaczonym segmencie”
- ESC lub „Wyczyść zaznaczenie” usuwa lokalne zaznaczenie segmentu
- „Zbliź” i „Oddal” są jedynymi operacjami zmieniającymi skalę czasu

Agregacja – segment osi czasu może reprezentować wiele zdarzeń; w przypadku zapory interfejs rozróżnia agregaty od liczby obserwacji źródłowych

Incydenty

Zakładka **Incydenty** prezentuje sprawy utworzone przez reguły analityczne na podstawie zdarzeń i wspólnych cech. Są to pozycje do weryfikacji, a nie automatyczna lista potwierdzonych ataków.

mks_vir administrator

Zarządzane stacje (grupa) RoundKick XDR

2026.09.22 10:45:00 / Cała firma — DANE DEMONSTRACYJNE Europe/Warsaw Raport statyczny

Przegląd Oś czasu Incydenty Korelacje Stacje i konta Sieć i WWW Urządzenia i dostęp Agenty AI Higiena i zmiany Skanowania

Grupa: Cała firma — DEMO Stacja: Wszystkie stacje Od: 2026.08.23 20:00 Do: 2026.09.22 10:45 Szukaj w zdarzeniach: Proces, adres, detekcja, użytkownik, temat...

24 godz. 7 dni 30 dni Dostępna historia Filtry zdarzeń Wyczyść filtry

Incydenty

Automatycznie powiązane zdarzenia do analizy — nie lista potwierdzonych ataków. Każda sprawa podaje podstawę połączenia.

Sprawa analityczna

SPRAWA ANALITYCZNA	PRIORYTET	ZDARZENIA SZCZEGÓŁOWE	STACJE W SPRAWIE	OSTATNIA OBSERWACJA
Faktura do pilnej weryfikacji	Wysoki sygnał	13	13	2026.09.21 03:45:00
HEUR.Backdoor.Script	Wysoki sygnał	7	7	2026.09.20 06:45:55
JS.Downloader.A	Wysoki sygnał	5	4	2026.09.20 02:47:20
Trojan.GenericKD.74210911	Wysoki sygnał	4	4	2026.09.19 03:45:25
Win32.Agent.CX	Wysoki sygnał	7	5	2026.09.19 02:46:21
Wynik skanowania - PRAKTYKANT-12 · C:\Users\praktikant3\Downloads	Do sprawdzenia	1	1	2026.09.22 01:45:00
Wynik skanowania - BIURO-01 · C:\Users\ksiegowosc\Downloads	Do sprawdzenia	1	1	2026.09.18 02:45:00
...	...	1	1	2026.09.17 22:45:00

- Priorytet pomaga ustalić kolejność analizy, ale nie zastępuje oceny administratora
- Kliknięcie sprawy otwiera oś czasu zdarzeń, podstawę powiązania i dowody źródłowe
- Ten sam fakt może wystąpić także w **Korelacjach** lub innych zakładkach – nie oznacza to dodatkowej infekcji

Interpretacja – w szczegółach zawsze sprawdź „Podstawę powiązania”; zgodność pól lub bliskość czasu może uzasadniać wspólną analizę, ale nie zawsze dowodzi związku przyczynowego

Korelacje

Korelacje pokazują związki między różnymi mechanizmami i źródłami danych. Ich celem jest uwidocznienie sekwencji, które w osobnych tabelach byłyby trudne do zauważenia.

The screenshot shows the 'Korelacje' (Correlations) section of the RoundKick XDR interface. The top navigation bar includes 'Zarządzane stacje (grupa)' and 'RoundKick XDR'. Below the navigation bar, there are filters for 'Grupa' (Cala firma — DEMO), 'Stacja' (Wszystkie stacje), 'Od' (2026.08.23 20:00), and 'Do' (2026.09.22 10:45). The 'Korelacje' section displays a summary of correlations with four metrics: 'Powiązane epizody' (27), 'Stacje z powiązaniami' (18), 'Unikalne zdarzenia źródłowe' (54), and 'Epizody ze zmianą zapory' (3). A section titled 'Znalezione powiązania' (Found correlations) is also visible at the bottom.

Przykładowe typy korelacji:

- niebezpieczna poczta → późniejsze wykrycie monitora na tej samej stacji
- zdarzenie WWW → wykrycie monitora
- monitor ↔ komunikacja programu obserwowana przez zaporę
- wykrycie monitora → zmiana aktywności zapory
- USB → późniejsze zdarzenie monitora
- AI → monitor przy zgodności obiektu lub ścieżki

Szczegóły korelacji

Po otwarciu korelacji raport przedstawia jej elementy w kolejności czasu, różnice czasowe między etapami oraz informację „*Dlaczego powiązano*”. Każde połączenie może mieć inną podstawę: zgodne pola, wspólny kontekst albo tylko zbieżność czasową.

Zarządzane stacje (grupa) RoundKick XDR

2026.09.22 10:45:00 / Cała firma — DANE DEMONSTRACYJNE Europe/Warsaw Raport statyczny

Przegląd Oś czasu Incydenty **Korelacje** Stacje i konta Sieć i WWW Urządzenia i dostęp Agenty AI Higiena i zmiany Skanowania

Poczta -> Wykrycie monitora -> Sieć i WWW
PRAKTYKANT-01 - 2026.09.21 03:45:00 - 2026.09.21 03:50:59

Epizod 9 Wróć do listy - ESC

Elementy są uporządkowane według pierwszej obserwacji. Strzałki oznaczają kolejność, nie przyczynę. Przy jednakowych czasach kolejność jest nierozstrzygnięta. Zdarzenia w serii mogą się przeplatać; dokładne pary i pełna lista są poniżej.

Time	Event	Count	Link
2026.09.21 03:45:00	Niebezpieczna poczta	1 zdarzeń	Wspólny kontekst / Pokaż zdarzenia
2026.09.21 03:45:37	Wykrycie monitora	1 zdarzeń	Pokaż zdarzenia
2026.09.21 03:46:00	Monitor -> Komunikacja programu	25 agregatów	Zgodne pola / Pokaż komunikację
2026.09.21 03:46:00	Monitor -> Zmiana aktywności zapory	25 agregatów	Zbieżność czasowa / Pokaż komunikację

Wynik działania monitora
Usunięto: 1
1: wykrycia z odpowiadającymi wpisami kwarantanny (nie dodatkowe infekcje)

Dlaczego powiązano

Poczta -> Monitor
Ta sama stacja, raport poczty poprzedza wykrycie monitora o nie więcej niż 5 minut. Zgodna nazwa detekcji może wzmacniać kontekst, ale nie jest wymagana. Brak identyfikatora wiadomości i załącznika: nie potwierdzamy, że wykryty plik pochodzi z tego maila.
Odstęp: 37 s - 37 s - 1 par źródłowych

Wspólny kontekst

- Linia czasowa pokazuje kolejność obserwacji, a nie automatycznie przyczynę
- Jeżeli dostępne są zgodne pola obiektu lub programu, interfejs wskazuje je jako silniejsze uzasadnienie
- Zdarzenia źródłowe pozostają dostępne do otwarcia – korelacja nie zastępuje dowodów
- Filtry **Korelacji** pozwalają ograniczać listę według typu i podstawy powiązania

Stacje i konta

Zakładka prezentuje bieżący inwentarz stacji w zakresie raportu oraz obserwowane konta i sesje. Karta stacji łączy informacje o systemie, telemetrii, skanach i stanie aktualizacji.

The screenshot shows the RoundKick XDR web interface. The top navigation bar includes 'Zarządzane stacje (grupa)' and 'RoundKick XDR'. The main content area is titled 'Stacje i konta' and displays a list of stations. The 'Inwentarz' tab is selected, showing a table of station data.

Grupa	Stacja	Od	Do	Szukaj w zdarzeniach
Cala firma — DEMO	Wszystkie stacje	2026.08.23 20:00	2026.09.22 10:45	Proces, adres, detekcja, użytkownik, temat...

24 godz. 7 dni 30 dni Dostępna historia Filtry zdarzeń Wyczyść filtry

Stacje i konta

Bieżący inwentarz stacji oraz konta i sesje obserwowane w dostępnej telemetrii.

Inwentarz Konta Przedziały sesji Aplikacje

Bieżący inwentarz. Filtry czasu i zdarzeń nie odtwarzają wcześniejszych wersji tej konfiguracji. Zakres grupy i stacji pozostaje aktywny.

PROD-01	PROD-02	PROD-03	PROD-04
demo-prod-01	demo-prod-02	demo-prod-03	demo-prod-04
Grupa	Grupa	Grupa	Grupa
Produkcja	Produkcja	Produkcja	Produkcja
PROD-01	PROD-02	PROD-03	PROD-04
Nazwa systemowa	Nazwa systemowa	Nazwa systemowa	Nazwa systemowa
System	System	System	System
Windows 11 Pro	Windows 11 Pro	Windows 11 Pro	Windows 11 Pro
IP	IP	IP	IP
10.20.1.21	10.20.1.22	10.20.1.23	10.20.1.24
Baza ochrony	Baza ochrony	Baza ochrony	Baza ochrony
2026.09.19	2026.09.21	2026.09.18	2026.09.20
Ostatnie dane	Ostatnie dane	Ostatnie dane	Ostatnie dane
2026.09.22 04:41:00	2026.09.22 04:03:00	2026.09.22 04:20:00	2026.09.22 04:27:00
Raporty ochrony Zapora Sesje użytkowników	Raporty ochrony Zapora Sesje użytkowników	Raporty ochrony Zapora Sesje użytkowników	Raporty ochrony Zapora Sesje użytkowników
Wydajność Agenty AI	Wydajność Agenty AI	Wydajność Agenty AI	Wydajność Agenty AI

- Kliknięcie stacji otwiera jej szczegóły i ostatnie istotne zdarzenia
- Dane inwentarzowe są migawką stanu – nie należy traktować ich jako pełnej historii zmian
- Sesje użytkowników służą jako kontekst; nie każdy zapis logowania oznacza aktywną pracę osoby

Sieć i WWW

Zakładka rozdziela komunikację aplikacji, historię WWW, blokady WWW, detekcje WWW oraz pocztę. To rozróżnienie jest istotne przy interpretacji aktywności użytkownika i ochrony.

Najaktywniejsze procesy

Proces	Liczba wpisów
C:\Windows\System32\svchost.exe	12 236
C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE	12 228
C:\Program Files\Microsoft OneDrive\OneDrive.exe	12 040
C:\Program Files\Microsoft\Edge\Application\msedge.exe	11 893
C:\Users\praktykant1\Downloads\Invoice_661.exe	185
C:\Users\praktykant2\Downloads\Invoice_725.exe	185
C:\Users\praktykant3\Downloads\Invoice_437.exe	185

Cele komunikacji

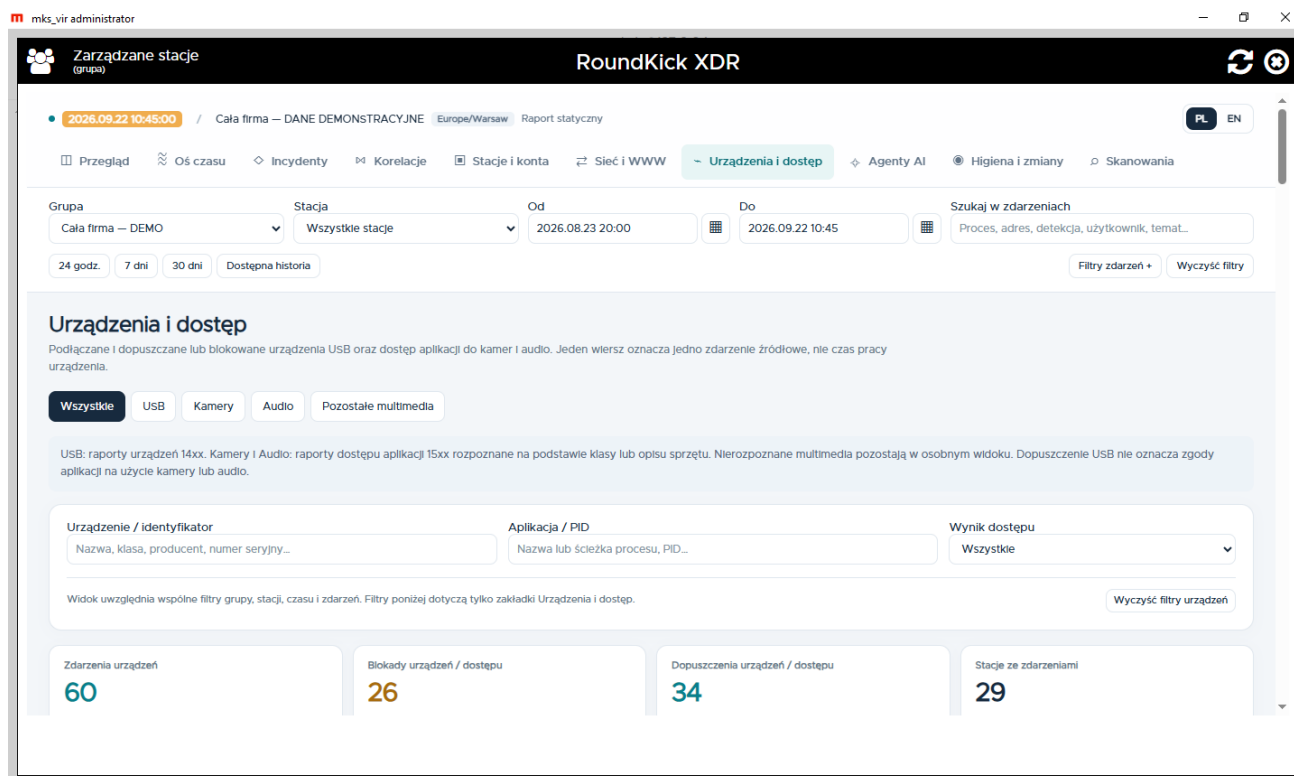
Adres	Liczba wpisów
portal.arcabit.pl	5521
www.linkedin.com	5494
stackoverflow.com	5470
outlook.office.com	5459
www.google.com	5442
www.microsoft.com	5374
www.microsoft.com	5374

- **Komunikacja** – agregaty wpisów zapory według stacji, programu, hosta, portu, kierunku i wyniku
- **Historia WWW** – odwiedzane lub żądane hosty, także zasoby techniczne i działające w tle
- **Blokady WWW** – osobne raporty polityki/blokad. Historia WWW nie jest listą blokad
- **Detekcje WWW** – wykrycia treści lub obiektów WWW raportowane przez ochronę
- **Pocztą** – raporty dotyczące wiadomości i wykryć w poczcie

Historia WWW – klasyfikacja „użytkowa / techniczna / niejednoznaczna” jest heurystyczna; źródło nie zawiera procesu, referera ani informacji, czy użytkownik świadomie otworzył dany host

Urządzenia i dostęp

Widok łączy decyzje dotyczące USB oraz dostępu aplikacji do kamer, audio i pozostałych urządzeń multimedialnych.



mks_vir administrator

Zarządzane stacje (grupa) RoundKick XDR

2026.09.22 10:45:00 / Cala firma — DANE DEMONSTRACYJNE Europe/Warsaw Report statyczny

Przegląd Oś czasu Incydenty Korelacje Stacje i konta Sieć i WWW **Urządzenia i dostęp** Agenty AI Higiena i zmiany Skanowania

Grupa: Cala firma — DEMO Stacja: Wszystkie stacje Od: 2026.08.23 20:00 Do: 2026.09.22 10:45 Szukaj w zdarzeniach: Proces, adres, detekcja, użytkownik, temat...

24 godz. 7 dni 30 dni Dostępna historia Filtry zdarzeń Wyczyść filtry

Urządzenia i dostęp

Podłączane i dopuszczane lub blokowane urządzenia USB oraz dostęp aplikacji do kamer i audio. Jeden wiersz oznacza jedno zdarzenie źródłowe, nie czas pracy urządzenia.

Wszystkie USB Kamery Audio Pozostałe multimedia

USB: raporty urządzeń 14xx. Kamery i Audio: raporty dostępu aplikacji 15xx rozpoznane na podstawie klasy lub opisu sprzętu. Nierozpoznane multimedia pozostają w osobnym widoku. Dopuszczenie USB nie oznacza zgody aplikacji na użycie kamery lub audio.

Urządzenie / identyfikator: Nazwa, klasa, producent, numer seryjny... Aplikacja / PID: Nazwa lub ścieżka procesu, PID... Wynik dostępu: Wszystkie

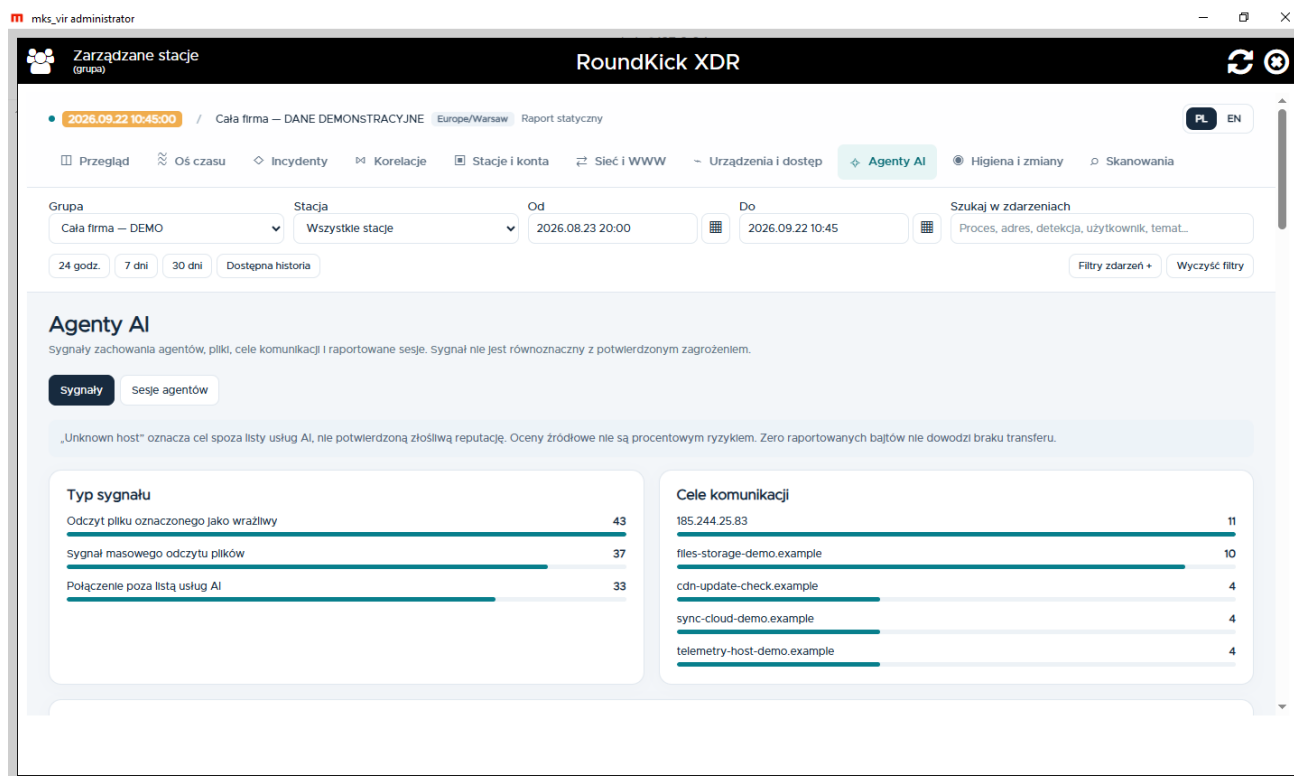
Widok uwzględnia wspólne filtry grupy, stacji, czasu i zdarzeń. Filtry poniżej dotyczą tylko zakładki Urządzenia i dostęp. Wyczyść filtry urządzeń

Zdarzenia urządzeń: 60 Blokady urządzeń / dostępu: 26 Dopuszczenia urządzeń / dostępu: 34 Stacje ze zdarzeniami: 29

- USB i dostęp aplikacji do multimediów są odrębnymi rodzajami zdarzeń
- Dopuszczenie urządzenia USB nie oznacza automatycznie zezwolenia aplikacji na korzystanie z kamery lub mikrofonu
- Raport pokazuje wyniki dopuszczenia/blokady zgodnie ze źródłem i umożliwia filtrowanie po typie urządzenia

Agenty AI

Zakładka **Agenty AI** prezentuje sygnały zgłaszane przez moduły analityczne: operacje na plikach, masowe odczyty, komunikację sieciową i inne zachowania. Sygnał AI jest materiałem do analizy, a nie automatycznie potwierdzonym atakiem.



- Kliknięcie sygnału pokazuje dane źródłowe, sesję AI i dostępny kontekst procesu/obiektu
- Wartość „UnknownHost” nie oznacza automatycznie, że host jest szkodliwy
- Jeżeli źródło wskazuje *blocked=false*, oznacza to brak zgłoszonej blokady przez ten mechanizm
- Powiązania z zaporą lub monitorem mogą być widoczne także w zakładce **Korelacje**

Higiena i zmiany

Zakładka obejmuje wydajność, aktualizacje i instalacje, Windows Update oraz jakość i dostępność telemetry. Jej celem jest pokazanie stanu środowiska, który może mieć znaczenie podczas analizy bezpieczeństwa.

2026.09.22 10:45:00 / Cala firma — DANE DEMONSTRACYJNE Europe/Warsaw Raport statyczny

Przełącznik: 2026.08.23 20:00 2026.09.22 10:45

Grupa: Cala firma — DEMO Stacja: Wszystkie stacje

Wydajność, aktualizacje, konfiguracja i jakość danych. USB, kamery i audio są w zakładce Urządzenia i dostęp. Inwentarz nie jest historią zmian.

Wydajność Aktualizacje i instalacje **Windows Update** Stan i aktualizacje Uprawnienia i polityki Jakość danych

Oczekujące aktualizacje według ostatniego dostępnego pliku wuc.txt każdej stacji. Data pochodzi z nagłówka pliku, nie z czasu jego modyfikacji ani daty wydania aktualizacji. To zestawienie stanu, nie historia instalacji. Filtry grupy, stacji i wyszukiwania działają; zakres czasu osi oraz filtry zdarzeń nie zmieniają tych zestawień. Do zawężenia użyj Wiek danych.

ZAKRES URZĄDZEŃ: Windows i stacje z plikiem WUC WYNIK ZESTAWIENIA: Wszystkie WIEK DANYCH: Wszystkie SZUKAJ AKTUALIZACJI / KB: Nazwa aktualizacji, KB, stacja...

Wyczyść filtry Windows Update

ZAKRES URZĄDZEŃ	WYNIK ZESTAWIENIA	WIEK DANYCH	SZUKAJ AKTUALIZACJI / KB
Zestawienia z poprawną datą	50	Pozycje aktualizacji w zestawieniach	327
Stacje z pozycjami oczekującymi	45	Stacje z pustą listą	5
Brak / niepełne dane	0		

- **Windows Update** korzysta z pliku stacji zawierającego listę aktualizacji oczekujących na instalację oraz datę zestawienia
- Pusta, prawidłowo datowana lista oznacza „*brak pozycji w zestawieniu*”. Brak pliku lub błędna data nie są interpretowane jako zero aktualizacji
- Wiek danych jest jawnie pokazywany. Stare zestawienie pozostaje dostępne, ale jego aktualność należy uwzględnić w ocenie
- Wydajność pokazuje CPU i RAM całego systemu. Nie pozwala przypisać obciążenia konkretnemu procesowi bez dodatkowych danych

Skanowania

Skanowania mają osobną zakładkę, dzięki czemu wyniki kontroli plików nie są mieszane z raportami monitora, poczty i WWW.

Zarządzane stacje (grupa) RoundKick XDR

2026.09.22 10:45:00 / Cala firma — DANE DEMONSTRACYJNE Europe/Warsaw Raport statyczny

Przegląd Oś czasu Incydenty Korelacje Stacje i konta Sieć i WWW Urządzenia i dostęp Agenty AI Higiena i zmiany Skanowania

Grupa: Cala firma — DEMO Stacja: Wszystkie stacje Od: 2026.08.23 20:00 Do: 2026.09.22 10:45 Szukaj w zdarzeniach: Proces, adres, detekcja, użytkownik, temat...

24 godz. 7 dni 30 dni Dostępna historia Filtry zdarzeń Wyczyść filtry

Skanowania

Historia wykonanych kontroli, pełne wyniki i powiązane dowody. Skany bez detekcji pozostają częścią historii.

Historia skanów Wykryte obiekty Stacje i skanowanie Porównanie skanów

Wynik skanu: Wszystkie Rodzaj zakresu: Wszystkie Akcja pozycji: Wszystkie Powiązanie z kwarantanną: Wszystkie

Zakres zawiera: Detekcja zawiera: Ścieżka obiektu zawiera: Baza użyta do skanu: Wszystkie

Wyczyść filtry skanowania

Skanów
81
Liczby dotyczą raportów i pozycji kolejnych skanów — nie unikalnych plików, infekcji ani ataków.

Z detekcjami
13
Skanów

Bez detekcji
68
Bez detekcji w skanowanym zakresie. Nie jest to potwierdzenie bezpieczeństwa całej stacji.

- **Historia** – lista raportów skanowania wraz z zakresem, liczbą przeskanowanych obiektów i wynikiem
- **Wyniki / trafienia** – szczegółowe pozycje wykryte podczas skanów
- **Stacje** – podsumowanie aktywności skanowania na poszczególnych komputerach
- **Porównanie** – porównanie dwóch raportów w celu zobaczenia zmian wyników i zakresu

UWAGA! Raport skanu bez detekcji nie dowodzi, że cały komputer jest wolny od zagrożeń; znaczenie wyniku zależy od zakresu skanowania i dostępności telemetrii

Szczegóły zdarzeń i dowody

Wiersze tabel i sprawy analityczne są interaktywne. Po kliknięciu raport otwiera panel szczegółów z czasem, stacją, użytkownikiem, procesem, obiektem/celami, wynikiem ochrony oraz odwołaniami do źródeł.

Zarządzane stacje (grupa)

RoundKick XDR

2026.09.22 10:45:00 / Cała firma — DANE DEMONSTRACYJNE Europe/Warsaw Raport stacji

Przegląd Oś czasu Incydenty Korelacje Stacje i konta

Grupa: Cała firma — DEMO Stacja: Wszystkie stacje Od: 2026.09.22

24 godz. 7 dni 30 dni Dostępna historia

Incydenty
Automatycznie powiązane zdarzenia do analizy — nie lista potwierdzonych ataków. Każda sprawa posiada historię.

Sprawa analityczna

SPRAWA ANALITYCZNA

Faktura do pilnej weryfikacji

HEUR.Backdoor.Script

JS.Downloader.A

Trojan.GenericKD.74210911

Win32.Agent.CX

Wynik skanowania - PRAKTYKANT-12 · C:\Users\praktykant3\Downloads

Wynik skanowania - BIURO-01 · C:\Users\Ksiegowosc\Downloads

Podstawa powiązania

Zgodnie pola nadawcy, odbiorcy, tematu i detekcji. Brak Message-ID — nie utożsamiamy tych raportów z jedną wiadomością.

13 Zdarzenia szczegółowe 13 Stacje w sprawie 13 Dowodów

Oś czasu

CZAS	STACJA	KATEGORIA	ZDARZENIE	OBIEKT / CEL	KONTO	WYNIK OCHRONY
2026.09.21 03:45:00	PRAKTYKANT-01	Poczta	Niebezpieczna zawartość pocztą - RiskySite.02	Faktura do pilnej weryfikacji	praktykant 1	Brak informacji
2026.09.19 03:45:00	PRAKTYKANT-02	Poczta	Niebezpieczna zawartość pocztą - Trojan.GenericKD.74210911	Faktura do pilnej weryfikacji	praktykant 2	Brak informacji
2026.09.18 06:45:00	BIURO-01	Poczta	Niebezpieczna zawartość pocztą - JS.Downloader.A	Faktura do pilnej weryfikacji	piotr.m	Brak informacji
2026.09.17 06:45:00	PRAKTYKANT-03	Poczta	Niebezpieczna zawartość pocztą - JS.Downloader.A	Faktura do pilnej weryfikacji	praktykant 4	Brak informacji

- „Dowody źródłowe” wskazują konkretny plik i pozycję danych, z których powstała obserwacja
- „Najbliższe zdarzenia” służą jako kontekst czasowy i nie są automatycznie przyczyną analizowanego zdarzenia
- W przypadku skanów, kwarantanny i aktualizacji raport zachowuje pełne szczegóły źródłowe, jeśli są dostępne

Eksport, język i zalecany sposób pracy

Eksport danych

Widoki tabelaryczne umożliwiają eksport do pliku z rozszerzeniem **.csv**. Pola są rozdzielane tabulatorem, dzięki czemu dane można wygodnie otworzyć w arkuszu kalkulacyjnym. Eksport zachowuje zabezpieczenie przed interpretacją danych jako formuł arkusza.

Język

Przełącznik PL / EN w prawym górnym rogu zmienia język interfejsu raportu. Dane źródłowe i nazwy plików nie są tłumaczone.

Zalecany sposób analizy

1. **Przegląd** – sprawdź liczniki i „Sprawy wymagające uwagi”
2. **Incydenty / Korelacje** – zobacz, czy kilka źródeł opisuje wspólną sytuację

3. **Oś czasu** – ustal kolejność zdarzeń i wybierz interesujący segment
4. **Stacja / czas** – zawęż filtry do jednej stacji i krótszego przedziału
5. **Szczegóły** – otwórz zdarzenia i sprawdź dowody źródłowe
6. **Eksport** – jeżeli potrzebujesz dalszej analizy, wyeksportuj bieżący widok

Zasada interpretacji – **RoundKick XDR** łączy i porządkuje dane, ale nie zastępuje oceny administratora; szczególnie korelacja czasowa, sąsiedztwo zdarzeń lub wspólny host nie powinny być traktowane jako automatyczny dowód związku przyczynowego