PRZEGLĄD ROZWIĄZANIA

PLATFORMA MEDIGATE

Ochrona systemów cyberfizycznych w nowoczesnych sieciach medycznych

Wyzwania związane z cyberbezpieczeństwem w ochronie zdrowia

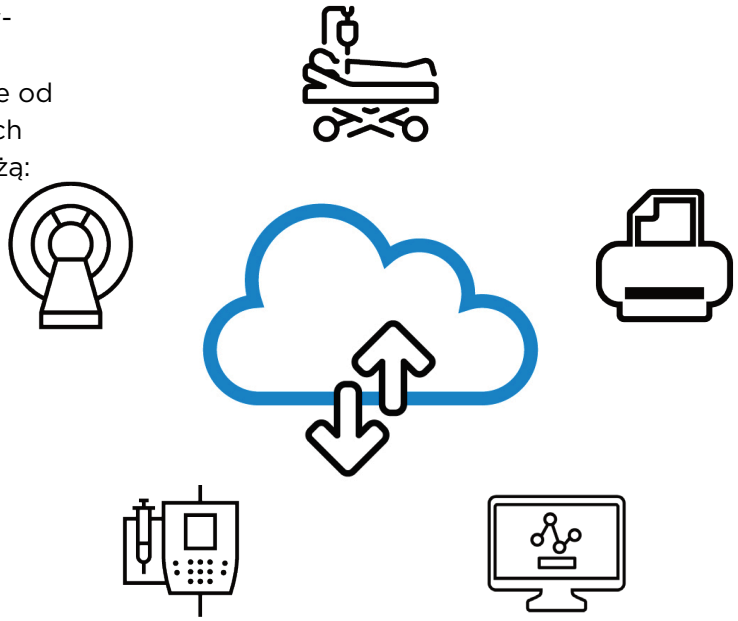
Nowoczesne sieci stosowane w ochronie zdrowia w olbrzymim stopniu zmieniły sposób, w jaki oferowana jest pomoc pacjentom. Infrastruktura systemów medycznych, personel i całe schematy pracy są ściśle zależne od szerokiego zakresu połączonych ze sobą urządzeń, które tworzą Rozszerzony Internet Rzeczy (ang. eXtended Internet of Things - XIoT). Ta rozległa cyberfizyczna sieć obejmuje niemal wszystko - od urządzeń medycznych, przez systemy zarządzania budynkiem (np. wentylacja, klimatyzacja i ogrzewanie), po sprzęt IoT taki jak drukarki sieciowe. Mimo ewidentnych zalet z punktu widzenia efektywności pracy, zacieśniająca się sieć połączeń tworzy nowe problemy związane z bezpieczeństwem i powierzchnie ataków, które mogą zagrozić funkcjonowaniu placówek, integralności danych, a nawet bezpieczeństwu pacjentów.

Medigate to czołowa na rynku platforma ochrony systemów cyberfizycznych stosowanych w ochronie zdrowia, pozwalająca placówkom bezpiecznie świadczyć nowoczesne usługi przy zapewnieniu pełnej efektywności. Medigate zapewnia cyberbezpieczeństwo wszystkich aspektów ochrony zdrowia - niezależnie od skali i stopnia dojrzałości środowiska. Do wybranych technologii stosowanych w ramach platformy należą:

- wykrywanie urządzeń,
- zarządzanie lukami i ryzykiem,
- ochrona sieci,
- wykrywanie zagrożeń,
- zarządzanie urządzeniami i cyklem życia,
- rozpoznanie operacyjne.

Zalety platformy Medigate

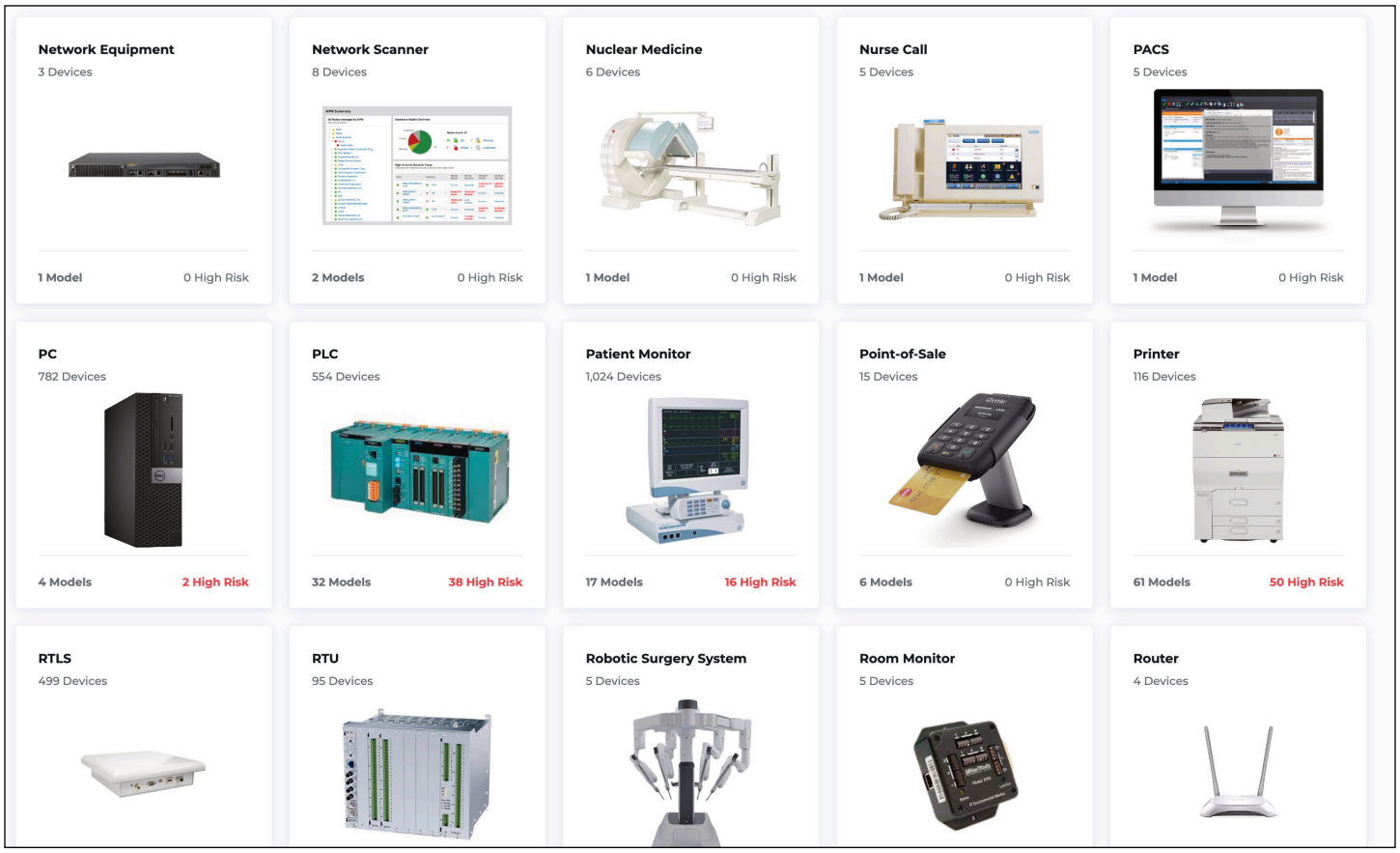
- Wdrożenie modułowej platformy zapewniającej cyberbezpieczeństwo ochrony zdrowia w modelu SaaS pozwala na zwiększenie jakości ochrony oraz odporności operacyjnej w ramach całej infrastruktury XIoT.
- Szczegółowe wykrywanie szerokiej gamy urządzeń przy użyciu różnych metod identyfikacji, pozwalających na dekodowanie unikatowych protokołów stosowanych w urządzeniach medycznych, zapewnia niezrównaną widoczność w sieci.
- Płynna integracja istniejących zasad bezpieczeństwa informacji oraz inżynierii klinicznej z rozległym ekosystemem technologii firmy Claroty.
- Zwiększenie wartości oraz zwrotu z inwestycji dzięki rozpoznaniu operacyjnemu oraz wglądowi w informacje o cyklu życia urządzeń, takie jak utylizacja sprzętu, śledzenie lokalizacji, inwentaryzacja i wiele więcej.



Wykrywanie urządzeń

Efektywne cyberbezpieczeństwo zaczyna się od wiedzy na temat tego, co należy chronić. Dlatego podstawą solidnego zabezpieczenia ochrony zdrowia jest inwentaryzacja sprzętu. Platforma Medigate korzysta z obszernego zestawu protokołów XIoT, co pozwala na szczegółową, scentralizowaną identyfikację zasobów. Dzięki licznym i elastycznym metodom gromadzenia danych wraz z możliwością łączenia ich oraz wykorzystywania z uwzględnieniem unikatowych potrzeb danego środowiska, firma Claroty jest jedynym producentem, który może zagwarantować tak dogłębny poziom widoczności:

- **Monitoring pasywny:** ciągłe badanie ruchu sieciowego celem identyfikacji urządzeń i profili komunikacyjnych.
- **Ekosystem integracji:** płynna integracja z popularnymi systemami CMMS i narzędziami do zarządzania urządzeniami pozwala na dodatkowe wzbogacenie profili zasobów.

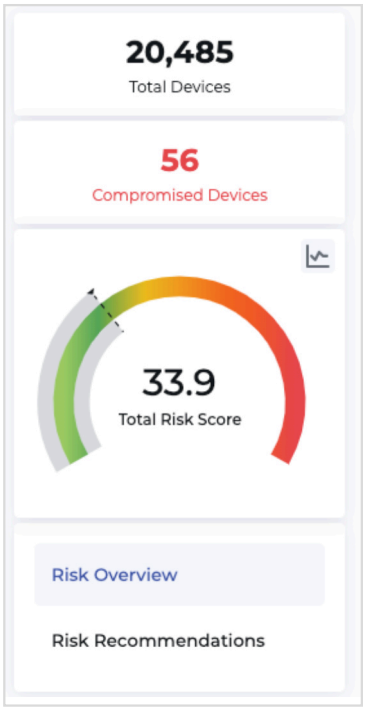


Przegląd urządzeń w platformie Medigate

Zarządzanie lukami i ryzykiem

Ze względu na naturę jednostek ochrony zdrowia, bezpieczne skanowanie w poszukiwaniu luk oraz ich usuwanie bez negatywnego wpływu na komfort personelu i pacjentów może być sporym wyzwaniem. Platforma Medigate upraszcza zarządzanie lukami i ryzykiem poprzez korelowanie zasobów z różnymi źródłami informacji o podatnościach, generowanie oceny ryzyka oraz automatyczne priorytetyzowanie zaleceń usuwania problemów w oparciu o ich potencjalny wpływ na funkcjonowanie placówki oraz bezpieczeństwo pacjentów.

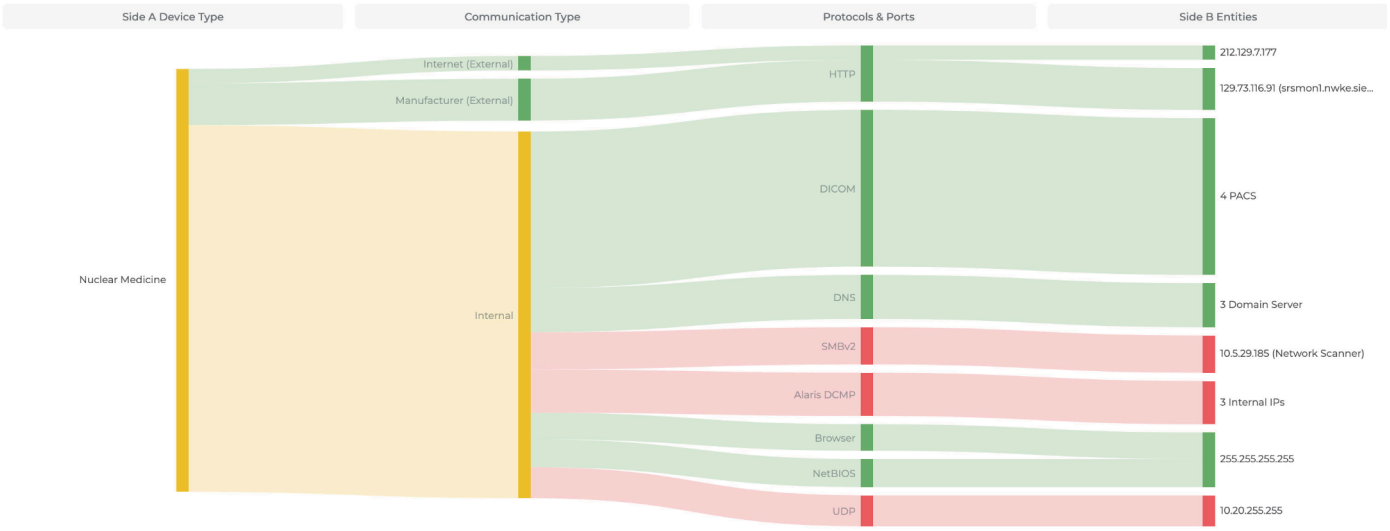
- **Identyfikacja ryzyka:** korzystaj z różnych źródeł wiedzy cyberwywiadowczej, takich jak bazy podatności czy formularze MDS2, oraz z łat oferowanych przez producentów sprzętu i oprogramowania, by z łatwością wykrywać problemy z bezpieczeństwem w swoim środowisku.
- **Kolejność usuwania problemów:** identyfikuj najpoważniejsze zagrożenia, by w pierwszej kolejności efektywnie usuwać najbardziej krytyczne podatności.
- **Mierzenie postępów w rozwoju bezpieczeństwa:** elastyczne raportowanie pozwala lepiej zrozumieć obecną postawę cyberbezpieczeństwa i obserwować postępy we wdrażaniu ochrony.



Wskaźnik ryzyka w platformie Medigate

Ze względu na wyspecjalizowaną naturę komunikacji między urządzeniami stosowanymi w ochronie zdrowia oraz konieczność nieograniczonego przemieszczania się w ramach organizacji, wdrożenie ochrony sieci poprzez kontrolę zasad może być kosztowne i trudne. Efektywna strategia ochrony sieci wymaga pełnego wglądu w komunikację urządzeń celem dokonania prawidłowej segmentacji urządzeń i wymuszania polityk bezpieczeństwa.

- **Mapowanie komunikacji sieciowej:** platforma Medigate profiluje całą komunikację między urządzeniami w sieci, co pozwala lepiej zrozumieć, w jaki sposób i co dokładnie przesyła oraz odbiera każdy sprzęt.
- **Segmentacja sieci:** platforma automatycznie tworzy i umożliwia testowanie zalecanych zasad komunikacji z uwzględnieniem wymogów określonej sieci oraz najlepszych rynkowych praktyk.
- **Wymuszanie stosowania zasad:** bezpieczna komunikacja jest możliwa dzięki dostosowywaniu zalecanych zasad sieciowych oraz płynnej integracji z istniejącymi zasobami, takimi jak mechanizmy NAC czy zapory sieciowe.

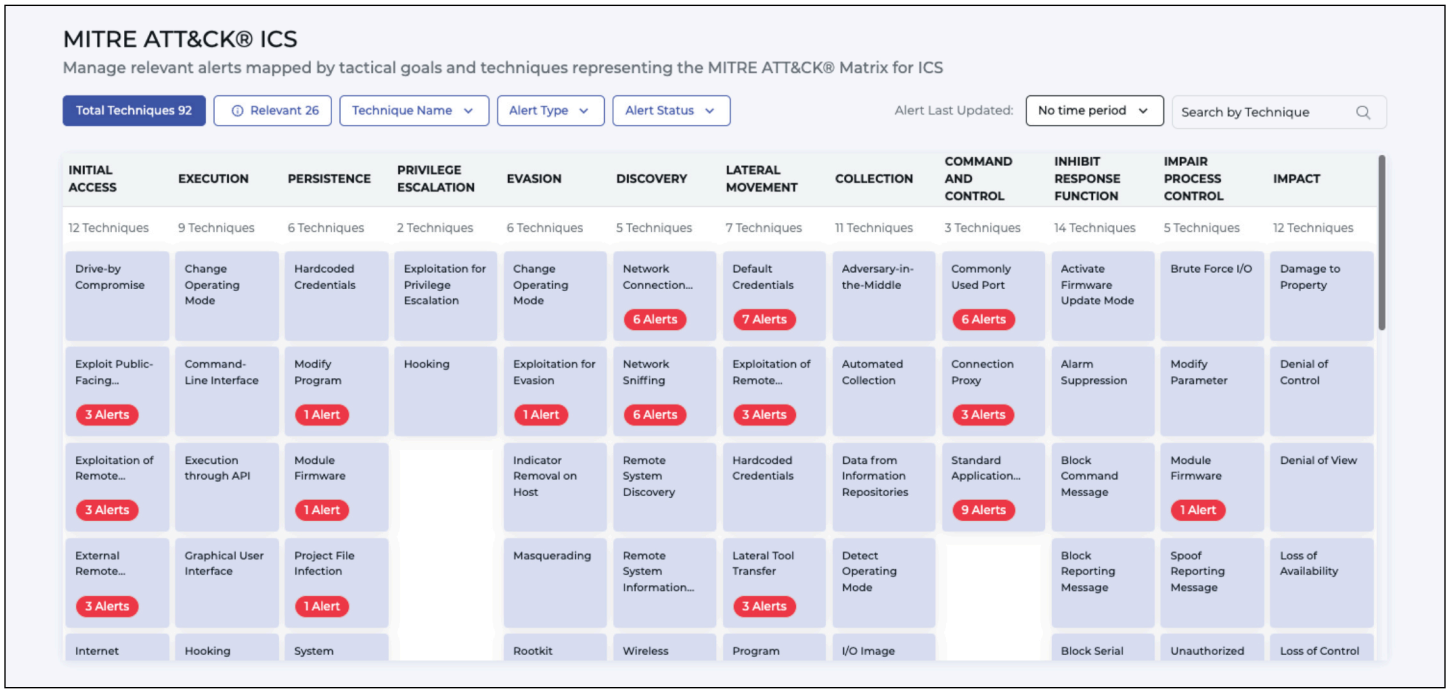


Mapa zasad komunikacji między urządzeniami

Wykrywanie zagrożeń

Żadna organizacja ochrony zdrowia nie jest odporna na zagrożenia, dlatego zagwarantowanie sprawnego wykrywania i reagowania jest kluczowe. Platforma Medigate została wyposażona w zunifikowany panel z informacjami i alertami oferujący zautomatyzowane metody monitorowania, nadawania priorytetów oraz reagowania na zagrożenia pojawiające się na urządzeniach.

- **Wykrywanie znanych zagrożeń:** rozwiązanie błyskawicznie identyfikuje znane zagrożenia, takie jak ransomware, szkodliwe oprogramowanie i inne zdarzenia rozpoznawane na bazie sygnatur.
- **Wykrywanie nieznanych zagrożeń:** alerty dotyczące zagrożeń, zgodności oraz funkcjonowania placówki pozwalają szybko wykrywać nieznane zagrożenia, takie jak nietypowe zachowanie i ruch sieciowy, ataki dnia zerowego czy istotne zmiany stanu urządzeń.
- **Własne komunikaty z ostrzeżeniami:** Medigate pozwala na tworzenie własnych alertów uwzględniających poszczególne metody komunikacji, takie jak kategoria urządzenia czy protokół. Pozwala to na zwiększenie widoczności i wdrażanie skuteczniejszej strategii ochrony.
- **Szerokie możliwości integracji:** platforma może być płynnie integrowana z istniejącymi rozwiązaniami SIEM oraz EDR, by rozszerzyć możliwości działu SOC.

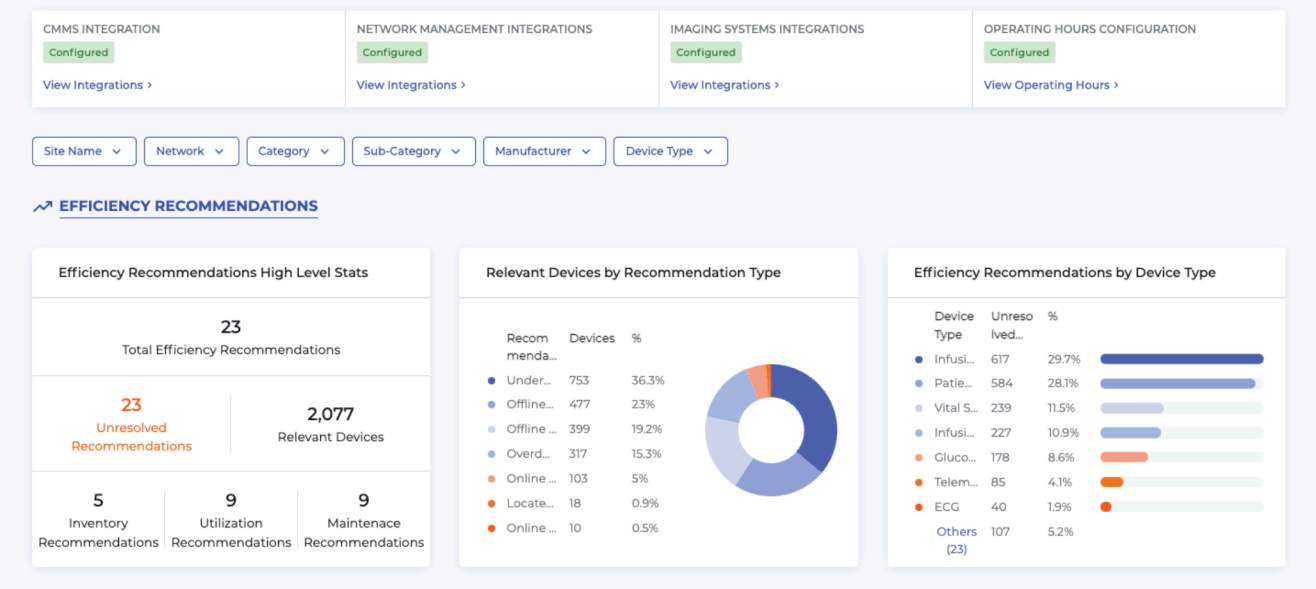


Mapowanie alertów generowanych przez platformę Medigate zgodnie ze standardem MITRE ATT&CK

Zarządzanie urządzeniami i cyklem życia

Dostęp do pełnego i zgodnego ze stanem faktycznym inwentarza przy jednoczesnym ciągłym monitorowaniu pełnego cyklu życia każdego urządzenia może być sporym wyzwaniem. Medigate eliminuje niezgodności i konieczność ręcznego śledzenia atrybutów urządzeń poprzez automatyzację procesu wykrywania oraz monitorowania. Dzięki temu możliwe jest pełne zrozumienie stanu i sposobu wykorzystania urządzeń, a także zachodzących zmian, co pozwala na efektywne zarządzanie całym sprzętem funkcjonującym w ramach placówki ochrony zdrowia.

- **Metryki wykorzystania urządzenia:** pełny wgląd w urządzenia XIoT i sposób ich wykorzystania, lokalizację, a nawet efektywność pracy.
- **Kompletny inwentarz i zarządzanie sprzętem:** identyfikacja, śledzenie i automatyczne przypisywanie zadań zarządzania zmianami (MoC) do określonych członków zespołu w oparciu o grupy lub przynależność sprzętu.
- **Monitorowanie i zarządzanie cyklem życia urządzeń:** usprawnioną komunikację w ramach platformy Medigate zapewniają funkcje tworzenia zaawansowanych raportów, planowania oraz automatycznego uruchamiania i wysyłania.

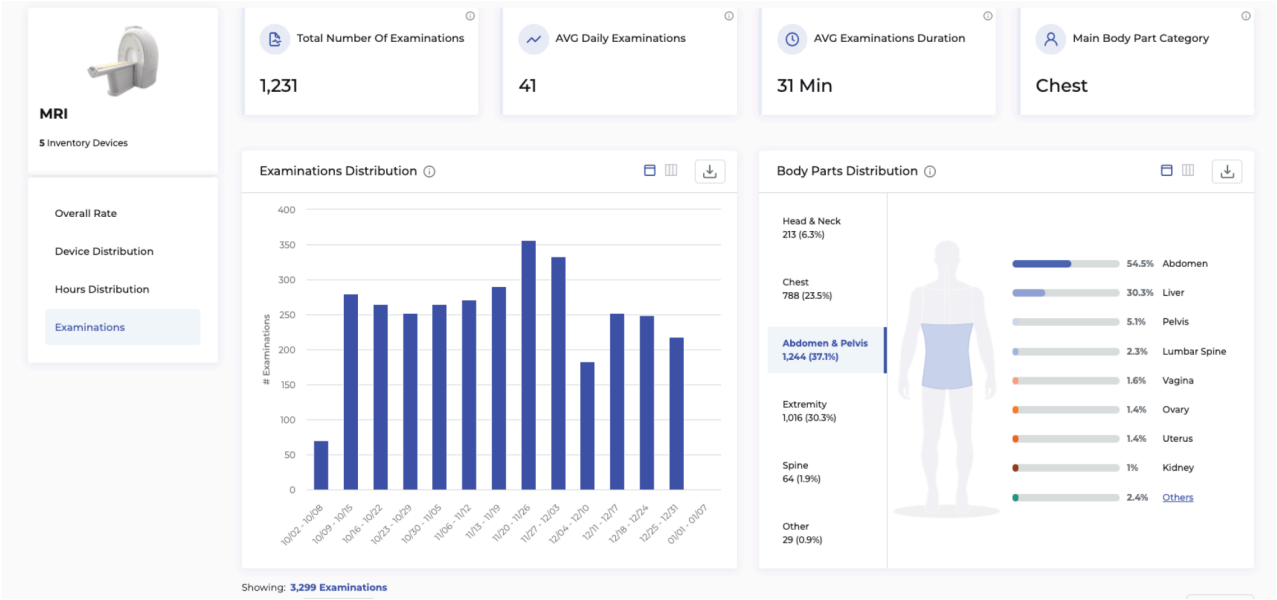


Panel prezentujący przegląd wydajności operacyjnej w platformie Medigate

Rozpoznanie operacyjne

Środowiska placówek ochrony zdrowia stanowią skomplikowaną sieć urządzeń, metod pracy i personelu. Wszystko musi płynnie współdziałać, by możliwe było zapewnienie pacjentom odpowiedniego poziomu opieki oraz bezpieczeństwa. Platforma Medigate powstała z myślą o optymalizacji pracy takich jednostek oraz o zapewnieniu maksymalnego wykorzystania wszystkich urządzeń, by optymalizować koszty, zwiększać zyski i miminalizować ryzyko. Dzięki dostępowi do informacji o liczbie, stopniu wykorzystania i przepustowości urządzeń w Twoim środowisku, Medigate pozwala na:

- **zwiększenie wydajności:** automatyzacja czasochłonnych zadań, takich jak audyt CMMS, oraz przywracanie sprawności urządzeń,
- **optymalizację potrzeb zakupowych:** wykorzystanie rynkowych standardów inwentaryzacji i utylizacji sprzętu pozwala odpowiednio dostosować liczebność urządzeń, równoważyć obciążenie w poszczególnych placówkach oraz renegocjować umowy najmu czy konserwacji,
- **rozszerzenie stopnia wykorzystania urządzeń:** identyfikacja, szacowanie i działania kompensujące w okresie końca życia urządzeń, by możliwe było ich maksymalne wykorzystanie.



Panel prezentujący przegląd wykorzystania urządzenia do rezonansu magnetycznego w różnych placówkach

Modułowa platforma zapewniająca cyberbezpieczeństwo jednostek ochrony zdrowia

Platforma Medigate to modułowe rozwiązanie przeznaczone dla wszystkich placówek ochrony zdrowia - niezależnie od stopnia dojrzałości funkcjonujących w nich systemów cyberbezpieczeństwa. Medigate obejmuje **pakiet technologii podstawowych**, zapewniających opisane wcześniej funkcje, a także **moduły zaawansowane**, oferujące bardziej rozbudowane możliwości.

	Medigate - technologie podstawowe	Medigate - moduły zaawansowane
Widoczność i wgląd w zasoby	Fundament platformy Medigate, zapewniający kompletny wgląd w inwentarz urządzeń, wraz z wieloma wyspecjalizowanymi metodami wykrywania, obejmującymi najszerszy w branży wachlarz protokołów stosowanych w sprzęcie medycznym oraz IoT. W rezultacie otrzymujesz niezrównaną szczegółowość profili urządzeń, łącznie z takimi informacjami jak numer seryjny, wersja oprogramowania układowego, system operacyjny i wiele więcej.	
Wykrywanie anomalii i zagrożeń	Skuteczny i łatwy w dostosowywaniu silnik wykrywania zagrożeń bazujący na identyfikacji behawioralnej oraz reagowaniu na anomalie, wraz z mapowaniem zidentyfikowanych niebezpieczeństw zgodnie ze standardem MITRE ATT&CK.	Rozszerzone możliwości wykrywania, wraz z sygnaturami znanych zagrożeń, a także własnymi alertami pozwalającymi na bardziej szczegółowe monitorowanie i ostrzeganie o unikatowych zachowaniach urządzeń.
Zarządzanie lukami i ryzykiem	Precyzyjne identyfikowanie luk i zagrożeń oraz ocena możliwości reagowania w oparciu o różne źródła danych cyberwywiadowczych, autorskie modelowanie ryzyka oraz integrację z istniejącymi rozwiązaniami zarządzania punktami końcowymi.	Kompletne zarządzanie lukami i ryzykiem, łącznie z funkcjami generowania zaleceń dotyczących całej sieci i nadawania im priorytetów, symulowaniem ryzyka oraz rozbudowanymi możliwościami w zakresie integracji celem identyfikowania podatności.
Zarządzanie ochroną sieci	Mapowanie i wizualizacja komunikacji między urządzeniami, łącznie z mapą świata przedstawiającą połączenia zewnętrzne, ustanowienie podstaw segmentacji sieci oraz integracja z istniejącą infrastrukturą sieciową.	Zestaw zalecanych zasad komunikacji z możliwością dostosowywania, monitorowania, optymalizowania i wymuszania poprzez integrację z zaporami oraz mechanizmami NAC. Moduł jest niezbędny w środowiskach poszukujących pragmatycznego podejścia do bezpieczeństwa sieci i chcących wdrażać metody zerowego zaufania.
Wydajność urządzeń medycznych	Rozpoznanie operacyjne realizowane na urządzeniach, łącznie z ich aktywnością, lokalizacją oraz mapowaniem poprzez integracje, a także informacje o końcu życia sprzętu.	Moduł oferujący użytkownikom możliwość monitorowania, badania wydajności i optymalizowania wykorzystania urządzeń w obrębie sieci w celu maksymalizacji wartości operacyjnej i zwiększenia współczynnika zwrotu z inwestycji (ROI).

Informacje o Claroty

Claroty zapewnia bezpieczeństwo systemów cyberfizycznych w branży przemysłowej, ochrony zdrowia oraz w środowiskach komercyjnych. Zunifikowana platforma firmy integruje się z istniejącą infrastrukturą klientów, by zapewniać kompletną kontrolę, widoczność, zarządzanie lukami i ryzykiem, wykrywanie zagrożeń, a także bezpieczny zdalny dostęp. Dzięki wsparciu czołowych firm inwestycyjnych oraz producentów z branży przemysłowej, rozwiązania Claroty funkcjonują w tysiącach organizacji na całym świecie. Siedziba firmy znajduje się w Nowym Jorku, a lokalne przedstawicielstwa funkcjonują w Europie, regionie Azji i Pacyfiku oraz w Ameryce Łacińskiej.

Więcej informacji znajduje się na stronie claroty.com.