



A Teraz Polska!

**LOG Plus – fundament zarządzania IT i
bezpieczeństwa w jednej platformie**

Prelegent



 LOG PLUS

Dominika Maciaszek

IT Product Business Manager

Jestem specjalistką w zakresie wsparcia projektów informatycznych oraz rozwoju oprogramowania, z naciskiem na aspekty analityczne i biznesowe. Posiadam doświadczenie w realizacjach dla różnych branż, w tym w logistyki, ochrony zdrowia, oraz cyberbezpieczeństwie, co pozwala mi na wszechstronne podejście do realizowanych projektów i skuteczne łączenie potrzeb biznesowych z technologią.



O firmie

Dostarczamy rozwiązania do zarządzania infrastrukturą IT

Jesteśmy wiodącym na polskim rynku producentem oprogramowania, specjalizującym się w nowoczesnych rozwiązaniach, wspomagających zarządzanie zasobami informatycznymi (IT Asset Management), procesy biznesowe zgodnie ze standardami ITIL oraz bezpieczeństwo organizacji. Głównym celem producenta jest tworzenie inteligentnego systemu, nasyconego know-how, przy jednoczesnym zachowaniu intuicyjności i łatwości użycia dla jego odbiorców.

+20

lat działalności na
polskim rynku

+1000

zadowolonych klientów



Klienci

Wybrani klienci

Z oprogramowania LOG Plus korzystają firmy i organizacje z różnych sektorów. Są to zarówno korporacje, firmy z sektora MŚP oraz instytucje publiczne.

Czym jest oprogramowanie LOG Plus?

LOG Plus to kompletna platforma, wspierająca zespoły IT w najważniejszych obszarach.



ITAM – Zarządzanie zasobami



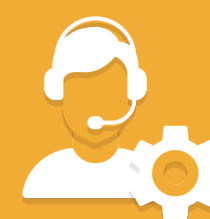
SAM – Zarządzanie licencjami oprogramowania



ITSM – Zarządzanie zgłoszeniami i incydentami



IDM – Zarządzanie dostępami i tożsamością



Zarządzanie usługami IT



Cyberbezpieczeństwo, Rozporządzenie **NIS2** oraz **DORA**

Najlepsze światowe praktyki

Jakie regulacje wspiera LOG Plus?

LOG Plus jest narzędziem stworzonym w oparciu o najlepsze światowe praktyki w zakresie zarządzania zasobami IT i nie tylko. Oprogramowanie jest zgodne z wytycznymi norm ISO/IEC 19770-1:2017, ISO 9001:2015, ISO/IEC 27001:2013 w tym także Rozporządzenia UE w zakresie ochrony danych osobowych oraz ITIL v4. Jako Środek Zarządzania Ryzykiem z obszaru bezpieczeństwa zasobów ludzkich, polityki kontroli dostępu i zarządzania zasobami **wspiera również dyrektywę NIS2 i rozporządzenie DORA.**





Bezpieczeństwo zaczyna się od świadomości co należy chronić

Nie da się skutecznie chronić czegoś, czego się nie zna. Bez znajomości własnych zasobów, danych i procesów – nawet najlepsze technologie zabezpieczające są jak zamki w drzwiach, których lokalizacji nie znamy.

Wyzwania Działów IT

✓ Rozproszenie zasobów

Zarządzanie coraz bardziej złożoną infrastrukturą hybrydową (chmura + lokalnie) i zapewnienie spójności między różnymi środowiskami.

✓ Brak narzędzi lub ich mnogość

Fragmentacja informacji, wiele źródeł lub – co gorsza – lokalne pliki Excel, każdy prowadzi swoje repozytorium wiedzy.

✓ Brak widoczności

Niedostateczna kontrola i trudności w uzyskaniu pełnej wiedzy o zasobach IT w organizacji uniemożliwia strategiczne podejmowanie decyzji, IT działa „na wyczucie”.

✓ Aktualność i bezpieczeństwo

Utrzymanie odpowiednich wersji wszystkich systemów, oprogramowania i urządzeń oraz zapewnienie ich bezpieczeństwa – jak zarządzać, kiedy nie wiadomo do końca czym?

✓ Ograniczone zasoby ludzkie

Jedna osoba musi pełnić wiele ról i nie zawsze posiada odpowiednie kompetencje, a wymagane od niej jest kompleksowe realizowanie zadań związanych z zarządzaniem IT.



Wymogi i regulacje

Na jakie regulacje i wymogi muszą dziś odpowiadać działy IT?

- ✓ NIS2 (dyrektywa UE) – nowe obowiązki w zakresie cyberbezpieczeństwa dla podmiotów kluczowych i ważnych
- ✓ DORA (Digital Operational Resilience Act) – wymogi dla sektora finansowego dotyczące odporności cyfrowej
- ✓ RODO / GDPR – ochrona danych osobowych, ciągłość zgodności
- ✓ Lokalne ustawy i regulacje branżowe – np. KNF, UODO, KSC



NIS2



**Fundament zarządzania IT i
bezpieczeństwa w jednej platformie**

Bezpieczeństwo danych, kontrola dostępu i zarządzanie aktywami

(...) W związku z tym w ramach swoich środków zarządzania ryzykiem w cyberbezpieczeństwie podmioty kluczowe i ważne powinny zająć się również bezpieczeństwem zasobów ludzkich i prowadzić odpowiednią politykę kontroli dostępu.



Należy sporządzić i prowadzić scentralizowany wykaz ewidencji aktywów oraz go aktualizować. (...) Ponadto, należy sporządzić procedurę zarządzania wszystkimi aktywami przypisanymi pracownikom lub osobom trzecim, a następnie zapewnić identyfikowalność tychże aktywów przez cały okres ich użytkowania.



Zasada minimalnych uprawnień

★ Profil stanowiska pracy

Stan na: 09.06.2025 10:32

1
Niezgodności zasobów

✓
Niezgodności oprogramowania

5
Niezgodności dostępów

Wymagane systemy informatyczne

👤

Niepoprawna rola: **Active Directory** (Produkcyjne)

Rola wymagana: Administrator

Rola bieżąca: User

👤

Niepoprawna rola: **Confluence** (Produkcyjne)

Rola wymagana: Administrator

Rola bieżąca: User

🚫

Brak dostępu do systemu: **SAP FI** (Produkcyjne)

Rola wymagana: Administrator

🚫

Brak dostępu do systemu: **CRM** (Produkcyjne)

Rola wymagana: Administrator

🚫

Brak dostępu do systemu: **Enova** (Deweloperskie)

Rola wymagana: Administrator



Grzegorz Filarowski

✓ aktywne

! administrator

<

Planowanie (15)

Zasoby (5)

Licencje (2)

Konta (5)

Rejestr dostępów

Przeciągnij tutaj nagłówek kolumny, aby pogrupować jego kolumnę

Ty...		Nazwa systemu		Login konta		Status konta		Konto aktywne od
		Active Directory		grzegorz.filarowski		aktywne		22.12.2012
		SAP FI		grzegorz.filarowski		aktywne		16.10.2024
		Confluence		grzegorz.filarowski2		aktywne		16.10.2024
		CRM		grzegorz.filarowski		aktywne		16.10.2024
		Enova		grzegorz.filarowski		aktywne		29.01.2025

Bezpieczeństwo przy zatrudnianiu i zwalnianiu pracowników

▼ **Wnioski (13)**

Tutaj zgłosisz wnioski w ramach usług świadczonych przez IT

> **IT (10)**

Zgłoszenia dotyczące wniosków IT

▼ **SI (3)**

Wnioski w zakresie dostępu do systemów informatycznych

Nadanie dostępu do SI (akceptacja SBO w głównym procesie)

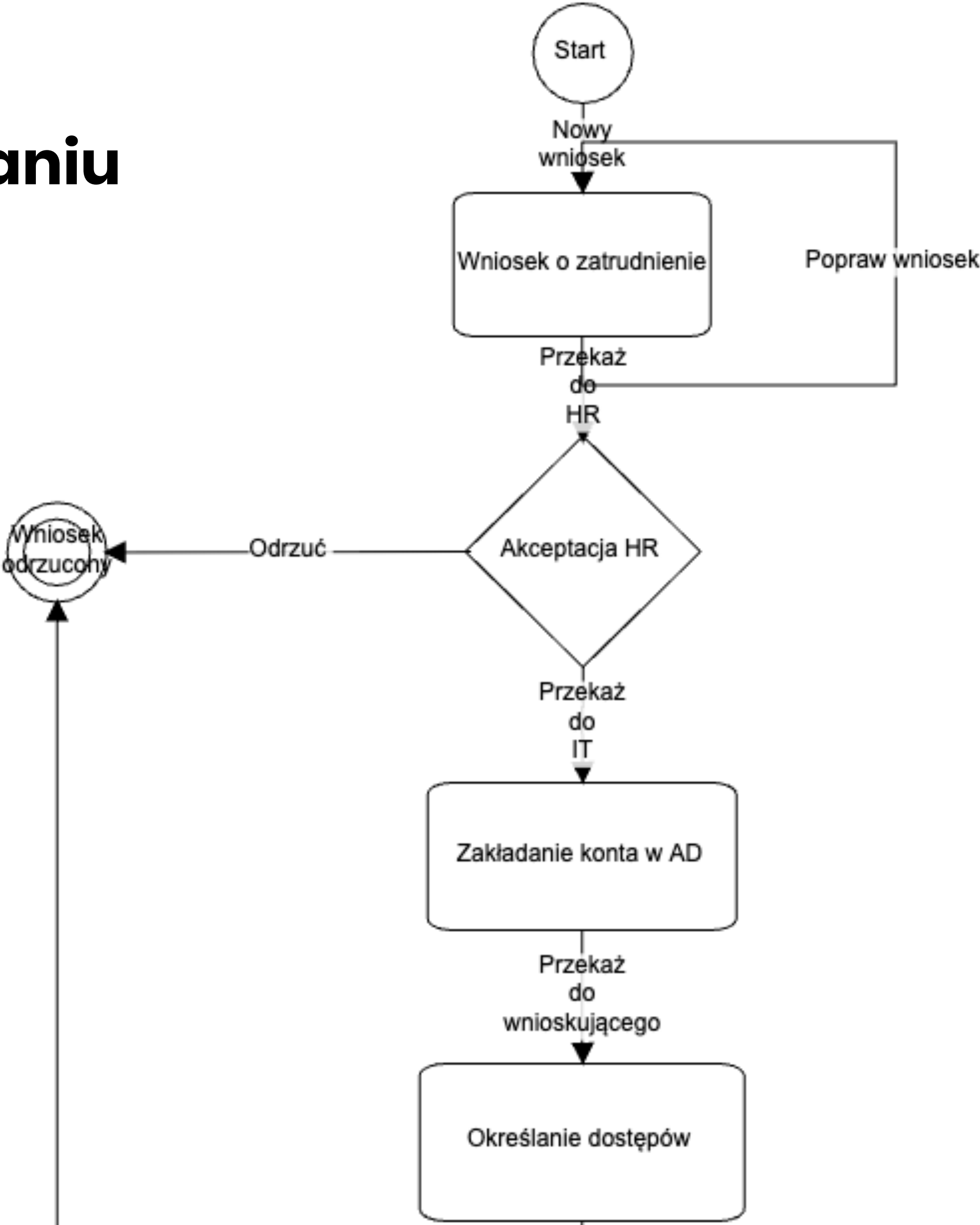
Proces nadawania dostępu, w którym akceptacja przełożonego oraz Właściciela Systemu (SBO) odbywa się w głównym procesie. Realizacja nadawania dostępu przez zespół ASI przebiega w ramach podprocesów.

Nadanie dostępu do SI (akceptacja SBO w podprocesie)

Proces nadawania dostępu, w którym akceptacja przełożonego odbywa się w głównym procesie. Akceptacja Właściciela Systemu (SBO) oraz dalsza realizacja przez zespół ASI mają miejsce w podprocesach.

Odebranie dostępu do SI

Proces odbierania dostępu, w którym wstępna weryfikacja odbywa się w głównym procesie. Realizacja zadania przez zespół ASI przebiega w ramach podprocesów.



Monitorowanie i kontrola dostępów

Realizacja wstrzymana lub zablokowana

DM #388 Wniosek o nadanie dostępu do systemu informatycznego

Zgłaszający: Dominika Maciaszek, Utworzono: 04.06.2025, Ostatnia modyfikacja: 04.06.2025 14:24, Priorytet: Normalny

Nadawanie dostępów



Czat

Informacje

Załączniki (0)

Dostępy (6)

Zadania (9)

Relacje (6)

Zgłoszenia (2)

Ewaluacja

Decyzja	Powią...	Osoba	System informatyczny	Rola	Login	Profil stanowiska pracy
	Nadanie do...	Ada Mazurek	Active Directory	Administrator	AdaMazur	Dyrektor Techniczny
	Nadanie do...	Ada Mazurek	Confluence	Administrator	AdaMazur	Dyrektor Techniczny
		Ada Mazurek	SAP FI	Administrator	AdaMazur	Dyrektor Techniczny
		Ada Mazurek	CRM	Administrator	AdaMazur	Dyrektor Techniczny
		Ada Mazurek	P1	User	AdaMazur	
		Ada Mazurek	Enova	Administrator	AdaMazur	Dyrektor Techniczny

Automatyczne przypisywanie i odbieranie uprawnień, zakładanie kont Active Directory



Profile stanowisk pracy

Dyrektor Techniczny

 Informacje

 Cykl życia

 Dostępy (5)

 Osoby (1)



☐	Typ ...	Nazwa systemu	Status systemu	Nazwa roli	Status roli
☐		Active Directory	 aktywne	Administrator	 aktywne
☐		Confluence	 aktywne	Administrator	 aktywne
☐		SAP FI	 aktywne	Administrator	 aktywne
☐		CRM	 aktywne	Administrator	 aktywne
☐		Enova	 aktywne	Administrator	 aktywne

Monitorowanie działań użytkowników

Informacje

Monitoring

Cykl życia

Mapa

Zgłoszenia (0)

Zadania (0)

Używane oprogram

Logowanie użytkowników

Użycie oprogramowania

Strony www

Operacje na plikach

Wydruki

Monitoring ekranów

adres monitoringu

0 dni

	Nazwa komputera	Czas użytkowania ↓	Udział procentowy
	DESKTOP-KMI835E	1 dzień 13 godz.	25.15%
	LOG-AP-5VQ90Z2	1 dzień 8 godz.	22.09%
 Chrome 137	DESKTOP-KMI835E	22 godz. 36 min	15.35%
 Chrome 137	LOG-AP-5VQ90Z2	15 godz. 49 min	10.75%
 ms-teams.exe	DESKTOP-KMI835E	9 godz. 43 min	6.61%
 ms-teams.exe	LOG-AP-5VQ90Z2	8 godz. 21 min	5.68%
 EXPLORER.EXE.MUI	DESKTOP-KMI835E	5 godz. 36 min	3.81%
 EXPLORER.EXE.MUI	LOG-AP-5VQ90Z2	3 godz. 9 min	2.14%
 Edge 136	LOG-AP-5VQ90Z2	3 godz. 2 min	2.07%
 Acrobat.exe	DESKTOP-KMI835E	2 godz. 45 min	1.88%

 Najczęściej odwiedzane strony www

crm.logsystem.pl

logsystem.sharepoint.com

enova.log.local

C:

drm.logsystem.pl

 Najczęściej używane oprogramowanie

Chrome

Aplikacje Microsoft 365 dla przedsiębiorstw

mRemoteNG

Notepad++

Check Point Endpoint Security

Identyfikacja i kategoryzacja wszystkich aktywów

Zasoby

Filtry

OSOBY I ORGANIZACJE

Osoby

Pracownicy i konta innych osób

296 AKTYWNE13 NIEAKTYWNE

99+

2 🗑️

Profile stanowisk pracy

Zasady i wymagane zasoby

4 WSZYSTKIE

Grupy osób

Grupy osób w organizacji

24 WSZYSTKIE

Organizacje

Firma, dostawcy, klienci...

4 WEWNĘTRZNE1 ZEWNĘTRZNE

SPRZĘT

Komputery

Laptopy i stacjonarne

28 AKTYWNE112 NIEAKTYWNE

13

Serwery

Serwery w Twojej infrastrukturze

24 AKTYWNE2 NIEAKTYWNE

5

Maszyny wirtualne

Wirtualna infrastruktura

43 AKTYWNE6 NIEAKTYWNE

8

Urządzenia mobilne

Telefony i tablety

13 AKTYWNE46 NIEAKTYWNE

Monitory

Monitory w Twojej firmie

3 AKTYWNE48 NIEAKTYWNE

116 🗑️

Drukarki

Drukarki i urządzenia wielofunkcyjne

10 AKTYWNE21 NIEAKTYWNE

Nośniki danych i czytniki

Dyski, pendrive'y, czytniki kart

11 AKTYWNE47 NIEAKTYWNE

Numery telefonów

Karty SIM, eSIM i numery stacjonarne

4 AKTYWNE0 NIEAKTYWNE

Aktywność w ostatnich

30 dniach

Stan na: 09.06.2025 11:15

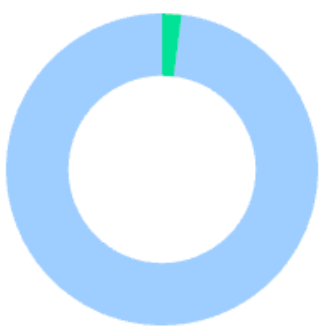
Statystyki komputera



AKTYWNOŚĆ KOMPUTERA



ZAJĘTOŚĆ DYSKU TWARDEGO

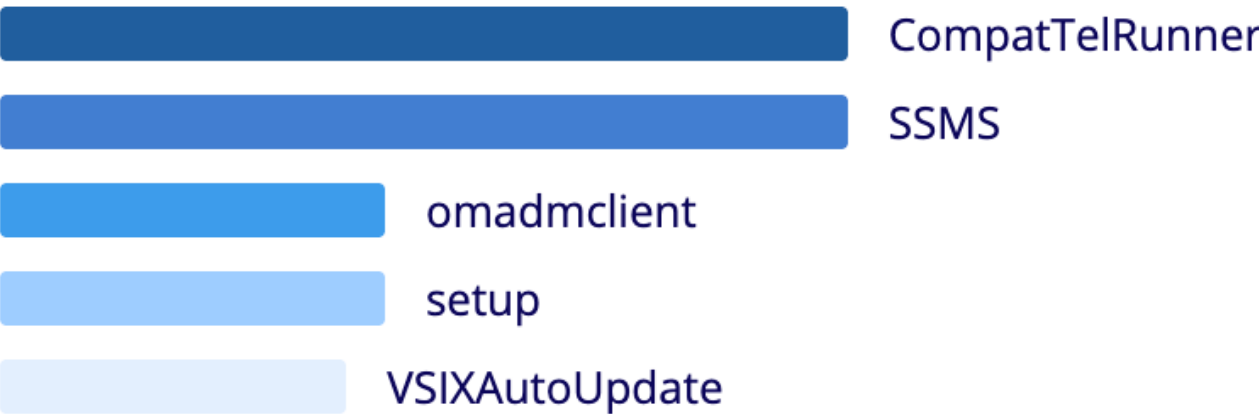


ŚREDNIE OBCIĄŻENIE CPU

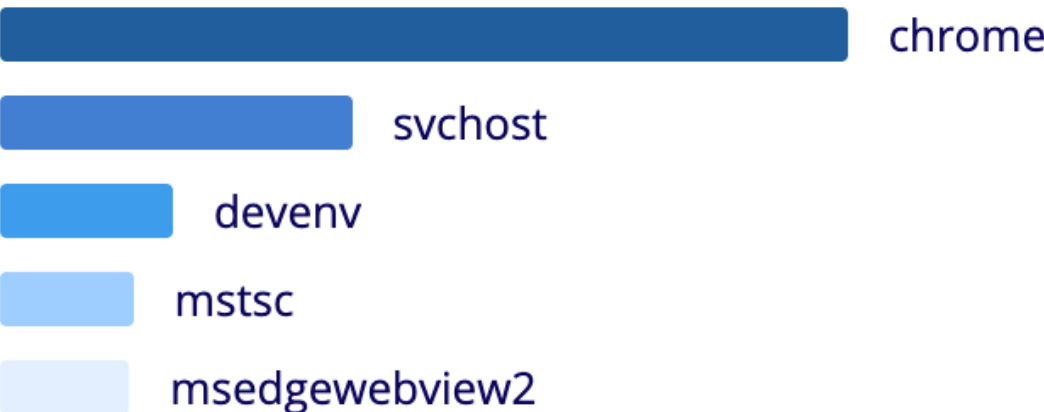


ŚREDNIE OBCIĄŻENIE PAMIĘCI RAM

Procesy najbardziej obciążające CPU



Procesy najbardziej obciążające RAM



Monitorowanie cyklu życia aktywów

Zmiana profilu agenta z Komputery basic na
Komputery LOG-WRO-RD-D

29.05.2025 15:40

Odinstalowanie oprogramowania: LOG Plus
Agent 4.2

29.05.2025 11:28

Odinstalowanie oprogramowania: Firefox 138

29.05.2025 10:32

Wykrycie oprogramowania: Edge 137

30.05.2025 10:32

Zmiana wartości opis: wcześniej: Brak teraz:
Zmiana opisu

29.05.2025 15:40 przez Admin Zuckerberg

Wykrycie oprogramowania: LOG Plus Agent
4.3

29.05.2025 11:28

Obsługa incydentu

„**Obsługa incydentu**” oznacza działania i procedury mające na celu zapobieżenie incydentowi, wykrywanie i analizowanie go, ograniczanie jego zasięgu lub reagowanie na niego i przywrócenie normalnego działania.



Polityka zarządzania incydentami. Incydenty związane z bezpieczeństwem informacji należy kontrolować, rejestrować i przetwarzać oraz reagować na nie zgodnie z konkretnymi odpowiedzialnościami wprowadzonymi i zatwierdzonymi przez kierownictwo. Należy również wprowadzić odpowiednie procedury komunikacji i eskalacji.



Rejestrowanie i monitorowanie incydentów



Helpdesk

Zgłoszenia

Wymagane od Ciebie: 121

Zgłoszone przez Ciebie: 258

Nieprzypisane: 322

140

Wysoki priorytet

9

Krytyczny priorytet

541

Suma zgłoszeń



Szukaj

Kolumny

☐	↓ ID	!	Temat	Zgłaszający	Stan	Realizujący	Kategoria	Status	Typ
☐	2831	!	Incydent naruszenia danych ...	 Admin Zuckerberg	✓	 Admin Zuckerberg	RODO	Zamknięty	Incydent
☐	2830	!	Incydent z logowaniem	 Dominika Maciaszek	▶	 Dominika Maciaszek	Serwis techniczny	Realizacja zgłosze...	Incydent
☐	2816	!	Incydent z oprogramowaniem	 Adam Kontrahent	▶	 Dominika Maciaszek	Organizacja pra	Realizacja zgłosze...	Incydent
☐	2810	!	Incydent z pocztą	 Konrad Mróz	✓	 Admin Zuckerberg	Serwis techniczny	Zamknięte	Incydent
☐	2809	!	Incydent z pocztą	 Admin Zuckerberg	▶	 Admin Zuckerberg	Serwis techniczny	Rozwiązane	Incydent
☐	2808	!	Incydent z pocztą	 Admin Zuckerberg	✓	 Admin Zuckerberg	Poczta	Zamknięte	Incydent
☐	2806	!	Incydent z oprogramowaniem	 Dominika Maciaszek	▶	 Adelajda Woźniak	Drukarki	Realizacja zgłosze...	Incydent

Obsługa incydentów

AZ

#396 Incydent ze sprzętem komputerowym

Zgłaszający: Admin Zuckerberg, Utworzono: 06.06.2025, Ostatnia modyfikacja: 06.06.2025 12:54, Priorytet: Normalny

przekroczono czas realizacji

Przekroczony czas na realizację: 5 godz. 51 min

Czat

Informacje

Załączniki (0)

Zadania (2)

Relacje (1)

Zgłoszenia (3)

Ewaluacja

Historia zmian

Szczegóły

Typ:

Incydent

Data utworzenia:

06.06.2025 12:51

Poziom świadczenia:

Sprzęt komputerowy

Data reakcji:

06.06.2025 12:51

Priorytet:

Normalny

Kategoria:

Sprzęt

Źródło:

Portal

Dodatkowe

Wskaż rodzaj awarii::

Brak oświetlenia, Nie działa urządzenie elektryczne, Zanik napięcia w gniazdkach pomieszczenia

Opis

lkjsdlkfjdslkjflksdjflkj lkdfjklsdjflksdjflksdjflk

Uczestnicy

Grupa realizująca:

I linia wsparcia

Zgłaszający:

AZ

 Admin Zuckerberg

Realizujący:

AZ

 Admin Zuckerberg

Ostatni modyfikujący:

AZ

 Admin Zuckerberg

S

I linia wsparcia, zweryfikuj zgłoszenie w celu jego dalszej realizacji.

Jeżeli kompletne - Analizuj

Jeżeli są braki - Zwróć do Zgłaszającego

Jeżeli zgłoszenie nie jest incydemtem - Anuluj

System 06.06.2025 12:51

Przypisano zadanie: Zweryfikuj incydent ze sprzętem komputerowym

System 06.06.2025 12:51

S

I linia wsparcia, dokonaj analizy zgłoszenia w celu jego klasyfikacji oraz dalszej realizacji.

Jeżeli kompletne - Realizuj

Jeżeli są braki - Zwróć do Zgłaszającego

Jeżeli zgłoszenie nie jest incydemtem - Anuluj

System 06.06.2025 12:51

LOG PLUS

Przewidywanie ryzyk i reagowanie na przerwy w dostępności

Profil usługi w grupie: Usługi IT

Dostęp do poczty email

w eksploatacji

przerwa w dostępności

Informacje

SLA (1)

Nieaktywne usługi (1)

Aktywne usługi (1)

Zakończone usługi (0)

Informacje podstawowe

Grupa usług:

Usługi IT

Typ usługi:

Biznesowa

Ważność:

Ważna

Wersja:

Rodzaj dostawcy:

Wewnętrzny

Rodzaj klienta:

Wewnętrzny

Właściciel biznesowy:

Wymagane zasoby i usługi

1 x Serwer i VM:

1 x Licencja:

1 x Urządzenie sieciowe:

Opcjonalne zasoby i usługi

Brak

Informacje finansowe

Wynik finansowy do końca roku:

- 3 643.25 PLN

Nakład inwestycyjny (CAPEX):

8 000.00 PLN

Roczny nakład operacyjny (OPEX):

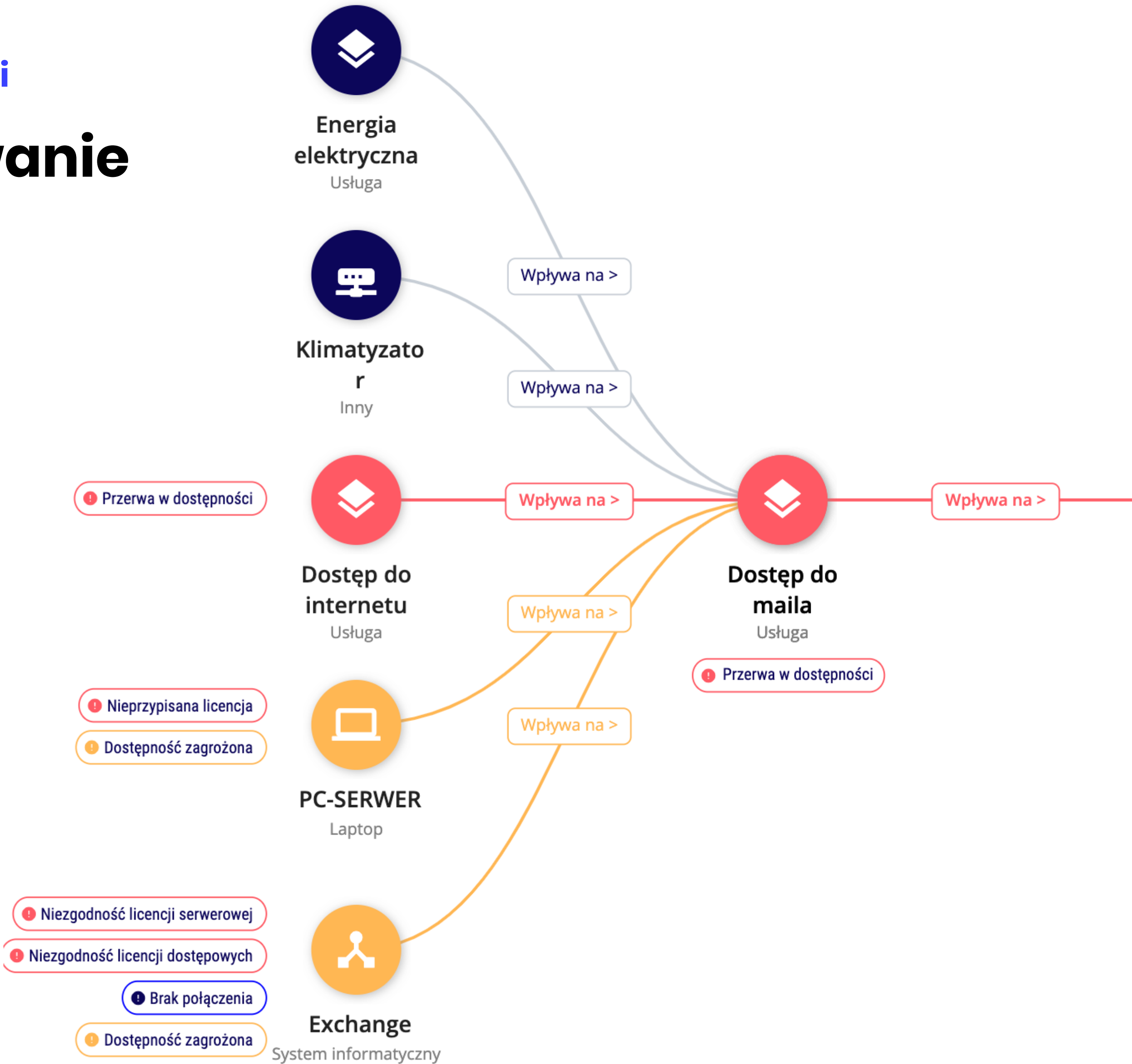
12 000.00 PLN

Sugerowana cena dla klienta:

150.00 PLN / płatność miesięczna

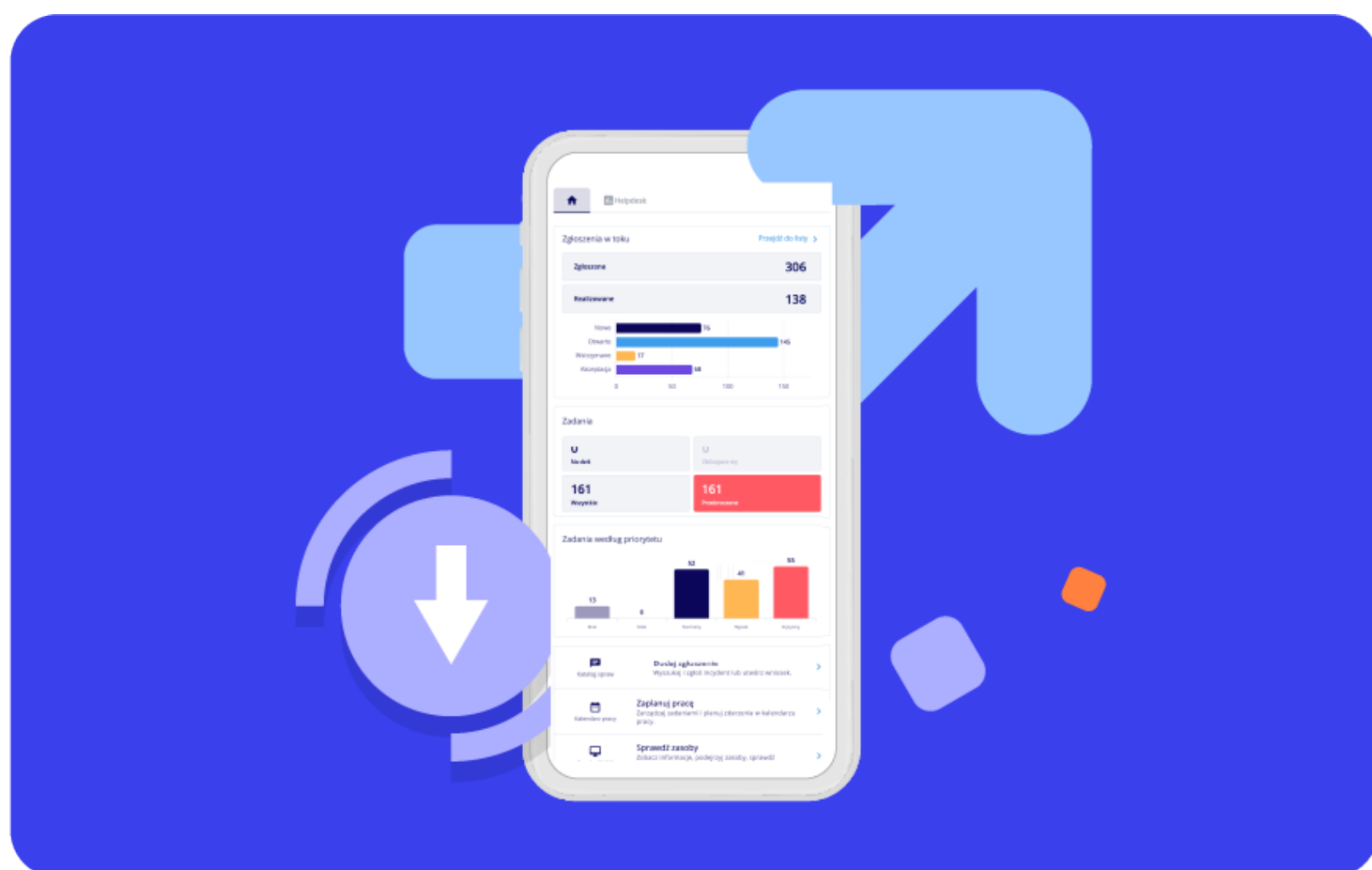
Maksymalna liczba klientów:

20





**Jak to wygląda w praktyce –
LOG Plus DEMO**



logplus.io

Wypróbuj w pełni funkcjonalną wersję demonstracyjną, zawierającą wszystkie rozwiązania LOG Plus!

DEMO LOG Plus

- ✓ 14 dni okresu testowego
- ✓ Dostępna pełna funkcjonalność systemu
- ✓ Możliwość testowania z poziomu przeglądarki bez instalacji
- ✓ Możliwość testowania na własnym środowisku
- ✓ Dostęp do szczegółowej dokumentacji oprogramowania
- ✓ Możliwość indywidualnych konsultacji
- ✓ Możliwość zadawania pytań



**Dziękuję za uwagę
i zapraszam do dyskusji!**



logplus.io