UpGreat
we know-how to do IT

LOG PLUS

A Teraz Polska!
LOG Plus – fundament zarządzania IT i bezpieczeństwa w jednej platformie

Konferencja 11 czerwca 2025

Prelegent

Dominika Maciaszek

IT Product Business Manager

Jestem specjalistą 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

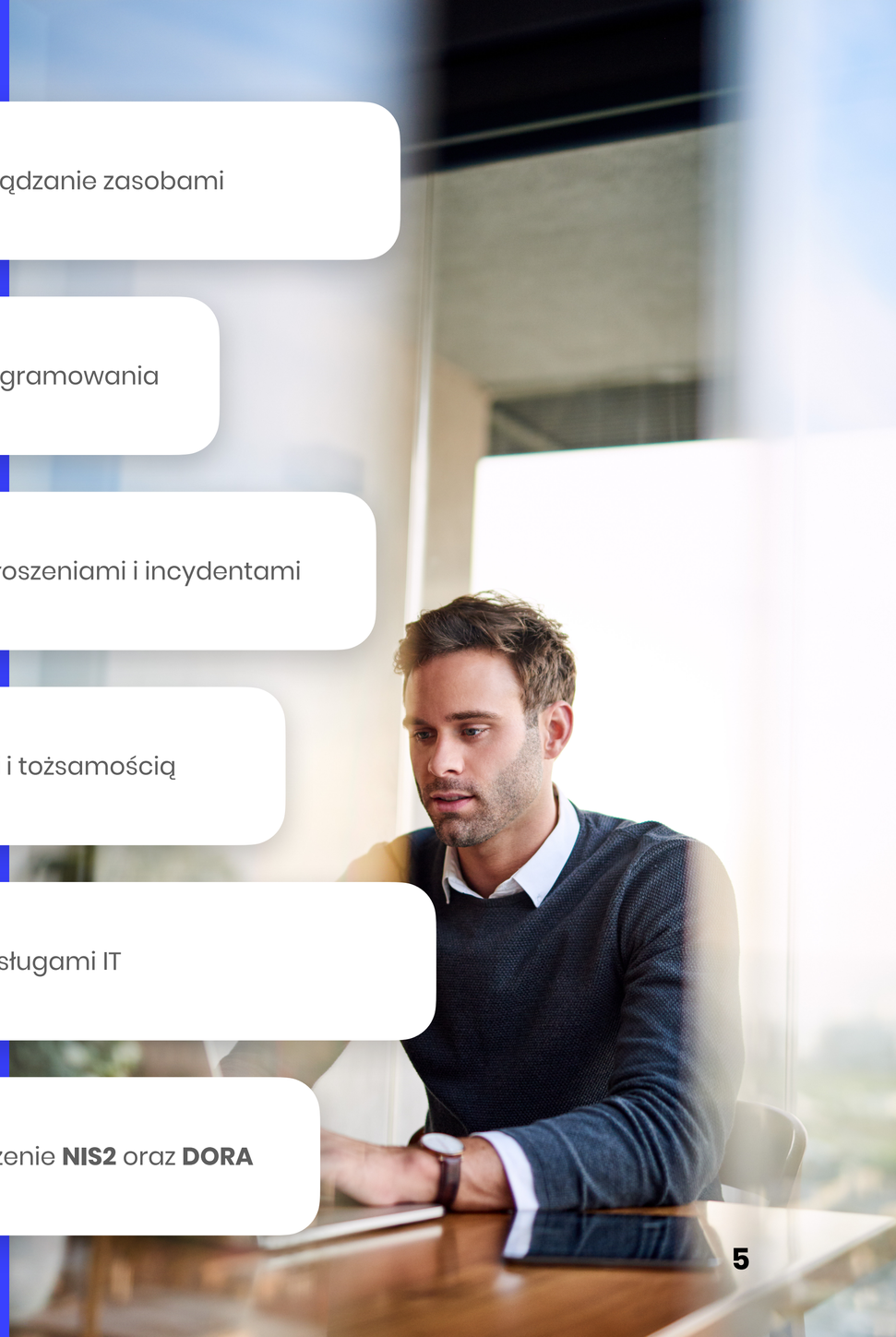
SAM - Zarządzanie licencjami oprogramowania

ITSM - Zarządzanie zgłoszeniami i incydentami

IDM - Zarządzanie dostępami i tożsamością

Zarządzanie usługami IT

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



LOG PLUS

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.

LOG PLUS

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

LOG PLUS

LOG PLUS

Fundament zarządzania IT i bezpieczeństwa w jednej platformie

LOG Plus

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.

NIS2 DIRECTIVE

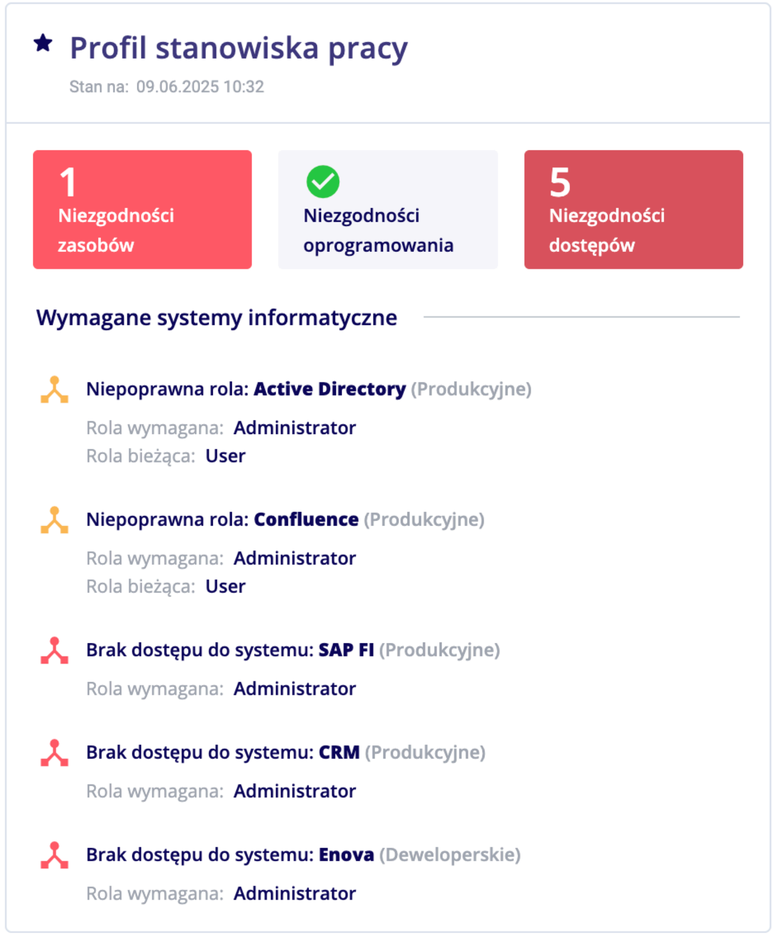
Należy sporządzić i prowadzić scentralizowany wykaz ewidencji aktywów oraz go aktualizować. (...) Ponadto, należy sporządzić procedurę zarządzania wszystkimi aktywami przypisanymi pracownikom lub osobom trzecim, a następnie zapewnić identyfikowalność tychże aktywów przez cały okres ich użytkowania.

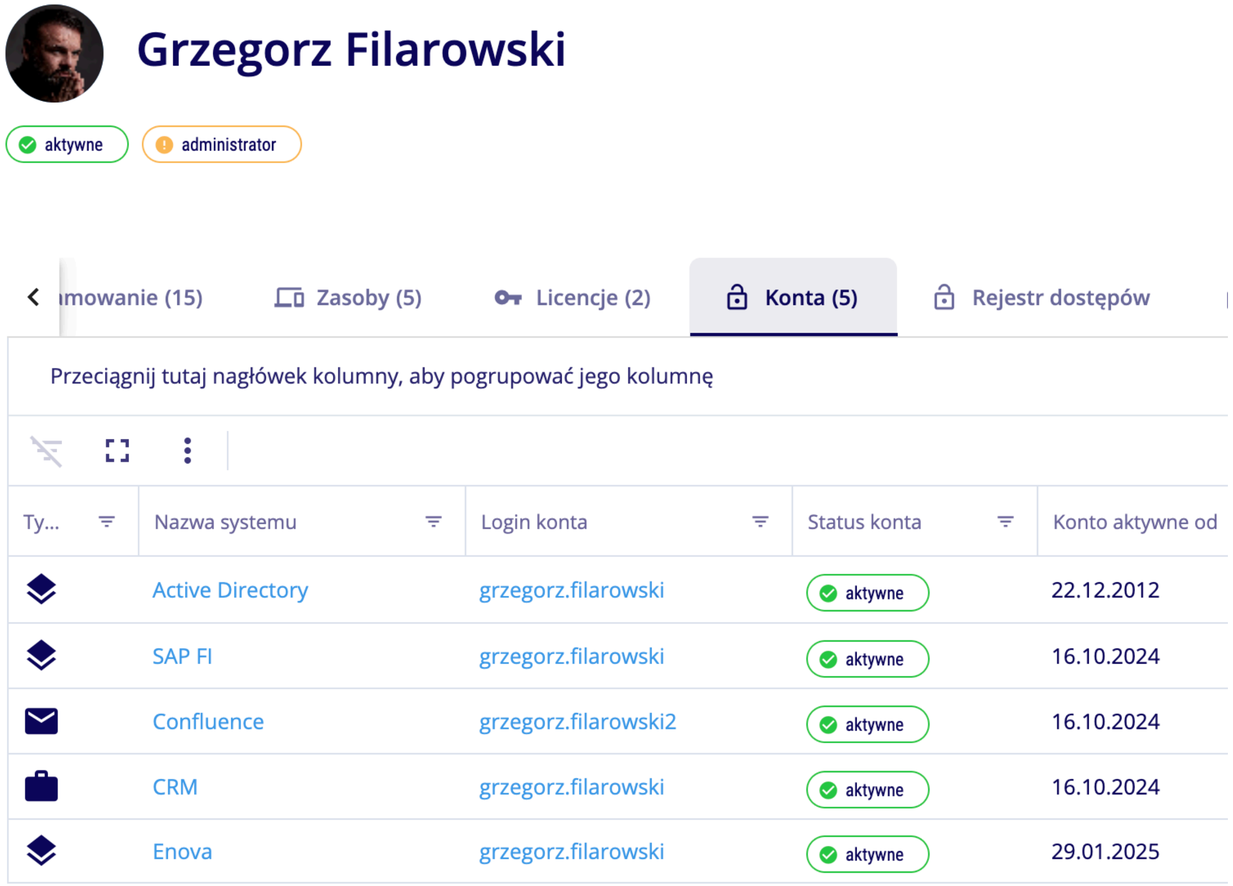
ISO

LOG PLUS

LOG Plus – Kontrola i nadzór nad dostępami

Zasada minimalnych uprawnień





LOG PLUS

LOG Plus – Kontrola i nadzór nad dostępami

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 dostępów do systemów informatycznych

    Nadanie dostępów do SI (akceptacja SBO w głównym procesie)

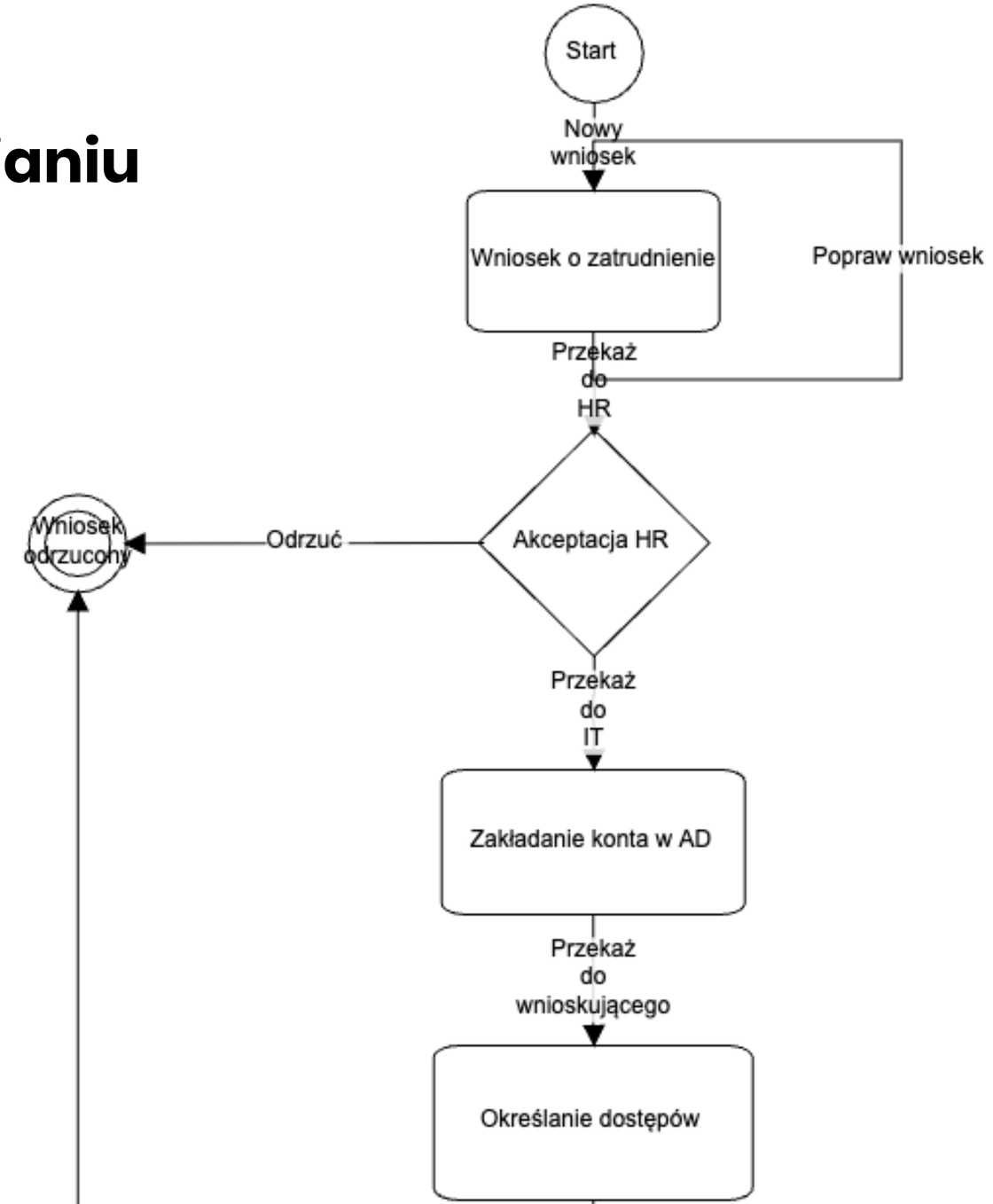
    Proces nadawania dostępów, w którym akceptacja przełożonego oraz Właściciela Systemu (SBO) odbywa się w głównym procesie. Realizacja nadawania dostępów przez zespół ASI przebiega w ramach podprocesów.

    Nadanie dostępów do SI (akceptacja SBO w podprocesie)

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

    Odebranie dostępów do SI

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



LOG PLUS

LOG Plus – Kontrola i nadzór nad dostępami

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

Szukaj

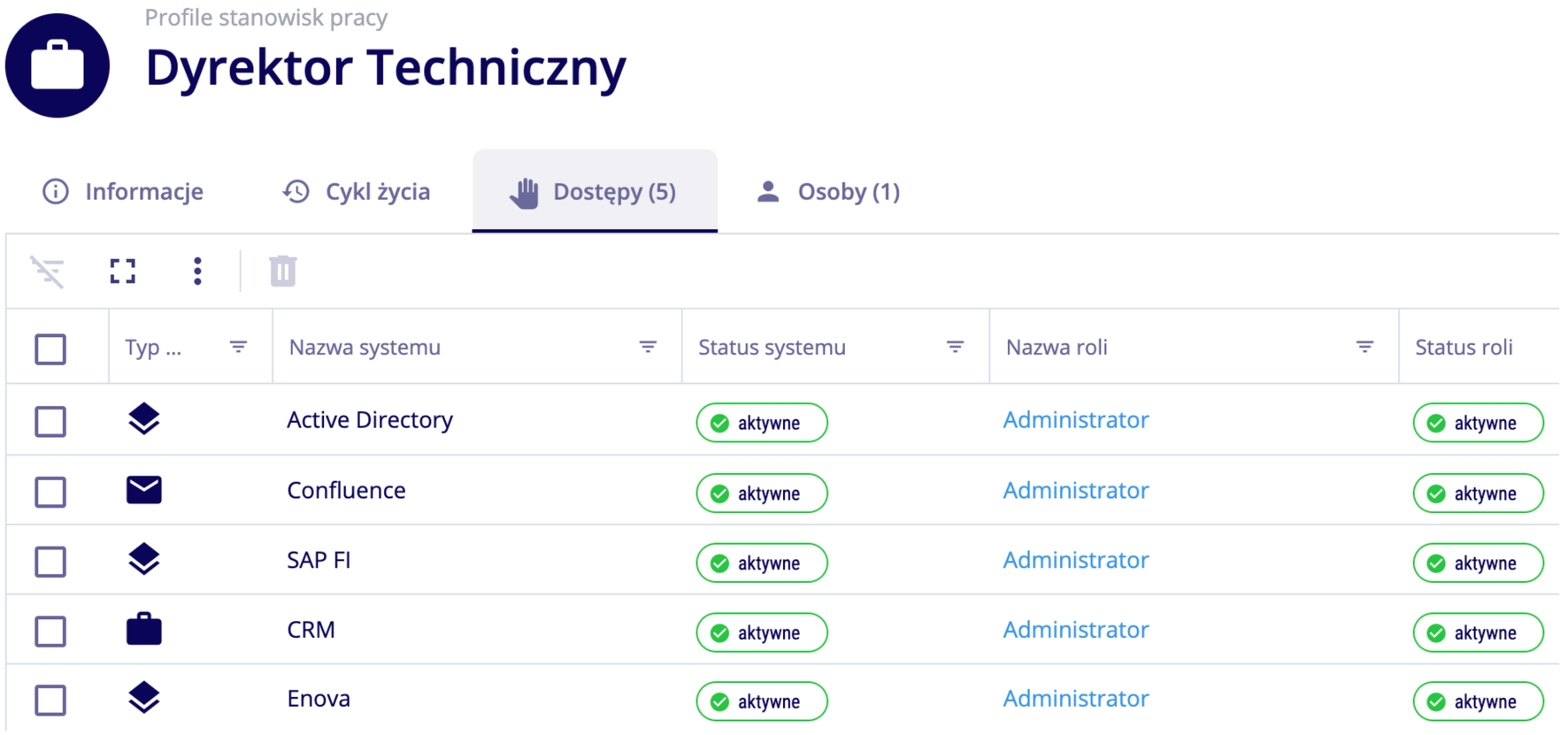
Kolumny

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

LOG PLUS

LOG Plus – Kontrola i nadzór nad dostępami

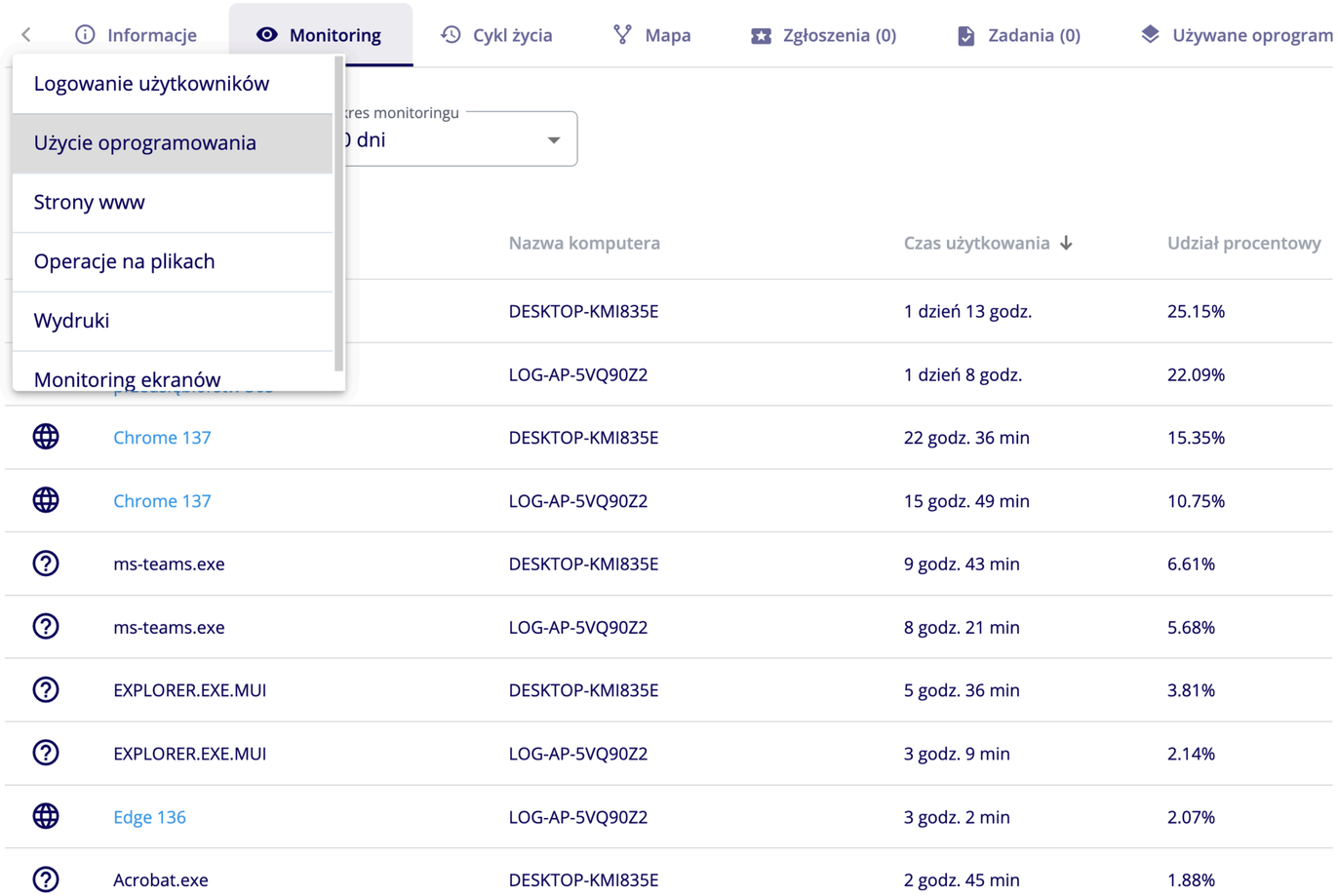
Automatyczne przypisywanie i odbieranie uprawnień, zakładanie kont Active Directory

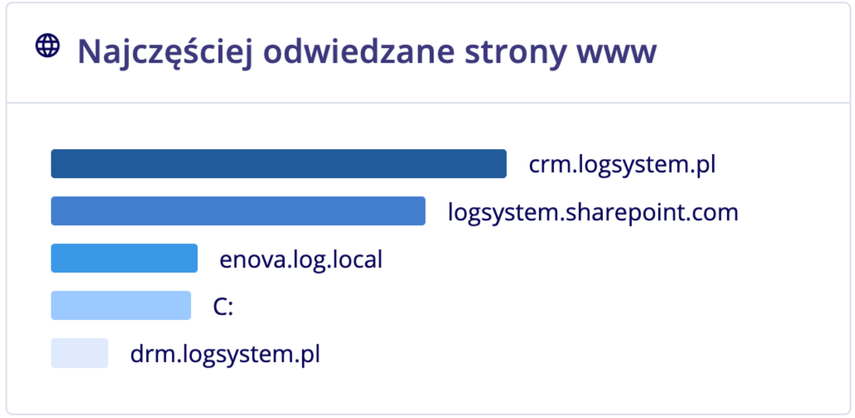


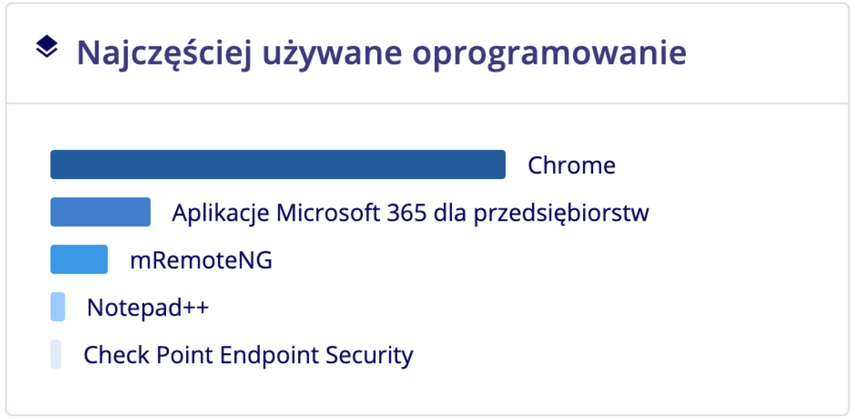
LOG PLUS

LOG Plus - bezpieczeństwo

Monitorowanie działań użytkowników



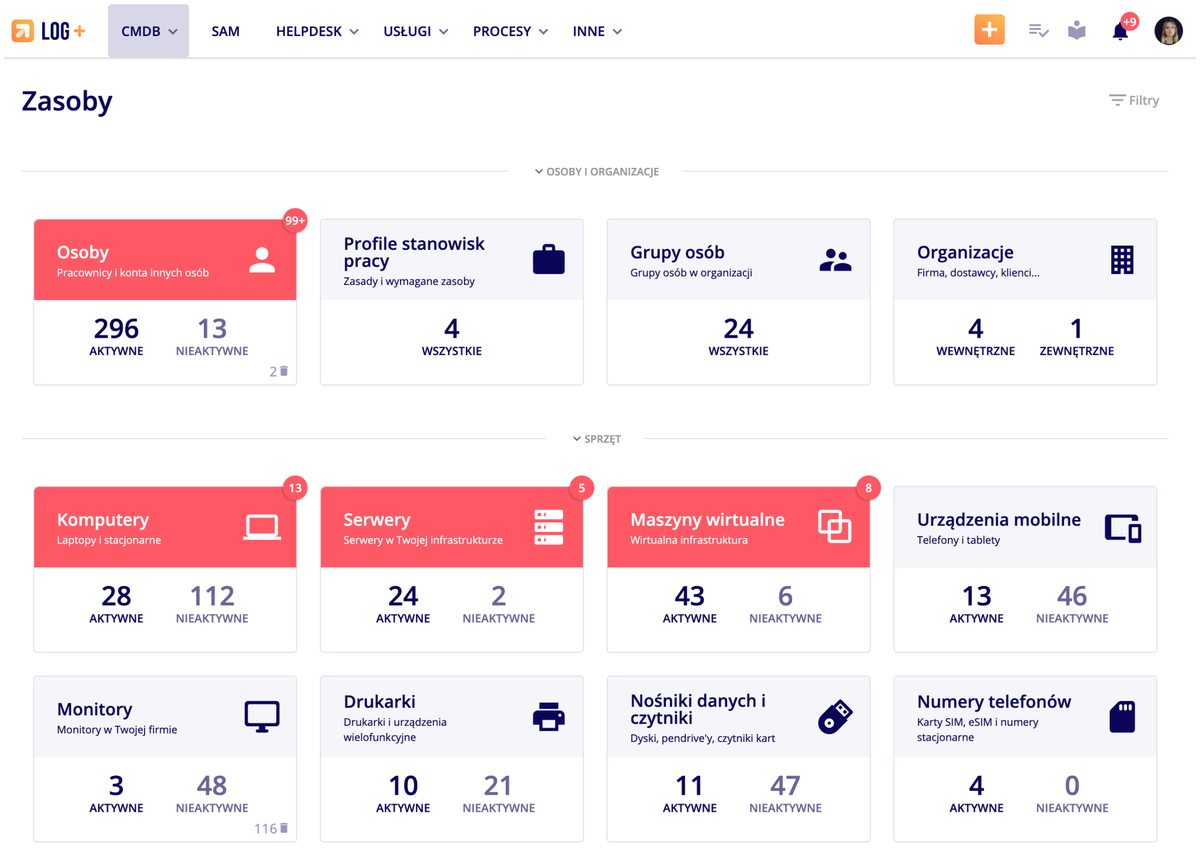




LOG PLUS

LOG Plus – Zarządzanie aktywami

Identyfikacja i kategoryzacja wszystkich aktywów



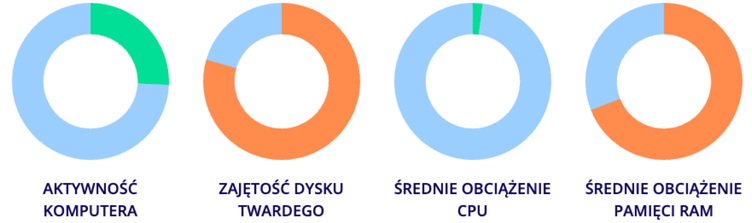
LOG PLUS

Aktywność w ostatnich

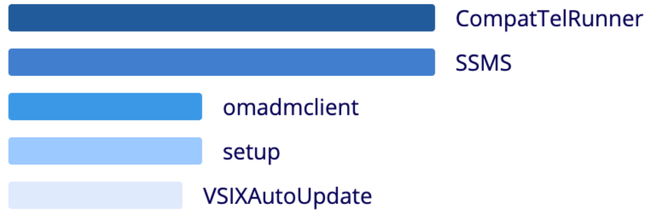
30 dniach

Stan na: 09.06.2025 11:15

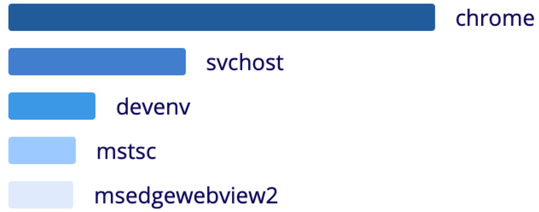
Statystyki komputera



Procesy najbardziej obciążające CPU



Procesy najbardziej obciążające RAM



LOG Plus – Zarządzanie aktywami

Monitorowanie cyklu życia aktywów

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

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

Wykrycie oprogramowania: LOG Plus Agent 4.3

29.05.2025 11:28

Odinstalowanie oprogramowania: Firefox 138

29.05.2025 10:32

LOG PLUS

LOG Plus ITSM

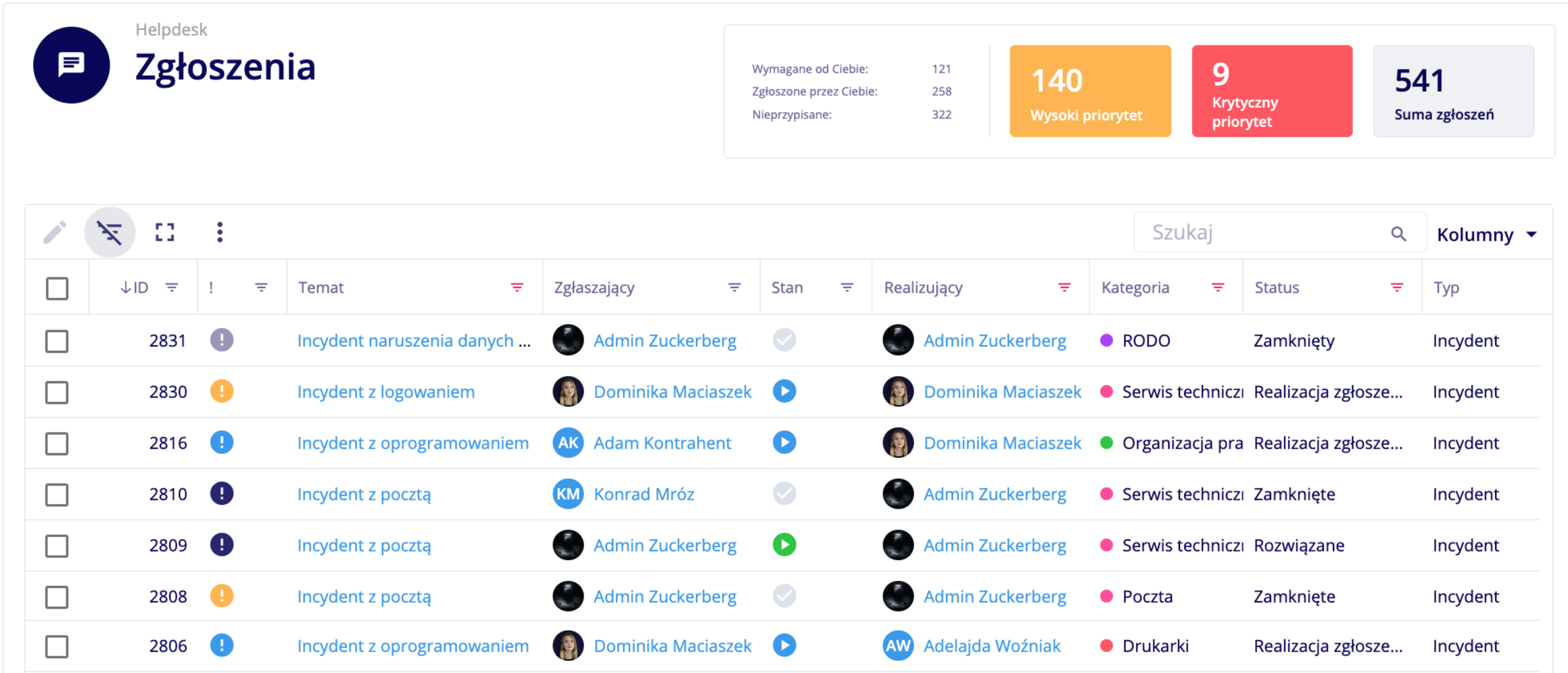
Obsługa incydentu

„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.

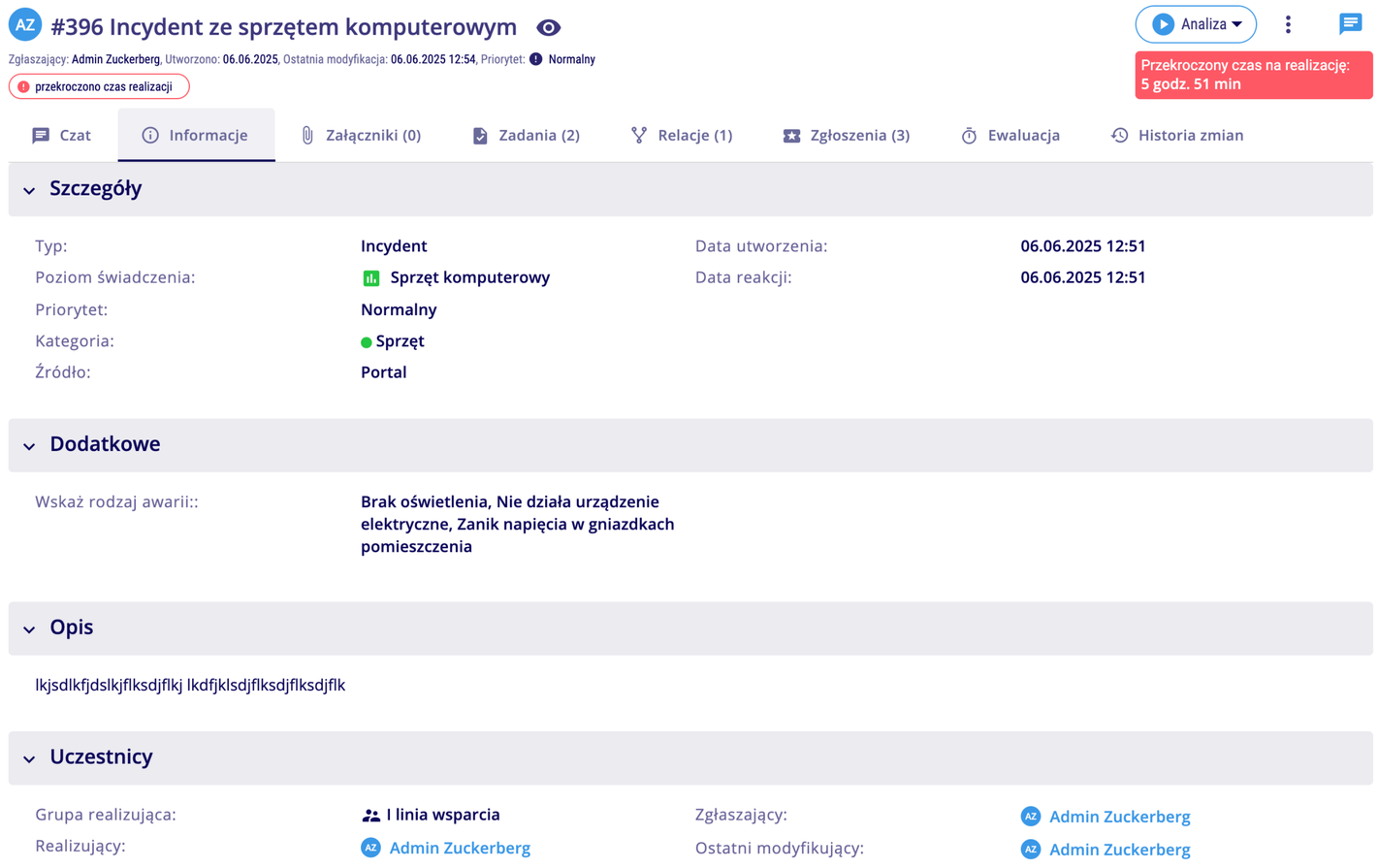
LOG Plus – zarządzanie incydentami i zgłoszeniami

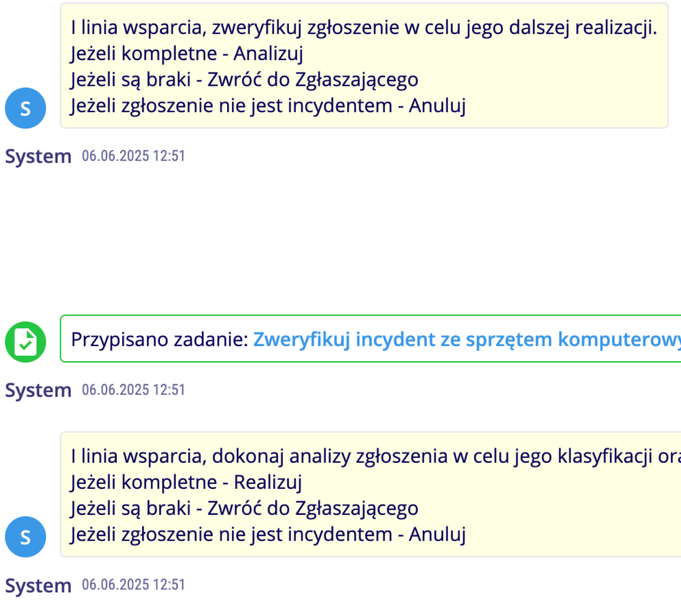
Rejestrowanie i monitorowanie incydentów



LOG Plus - zarządzanie incydentami i zgłoszeniami

Obsługa incydentów





LOG PLUS

LOG Plus – zarządzanie incydentami i zgłoszeniami

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:	

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**

Wymagane zasoby i usługi

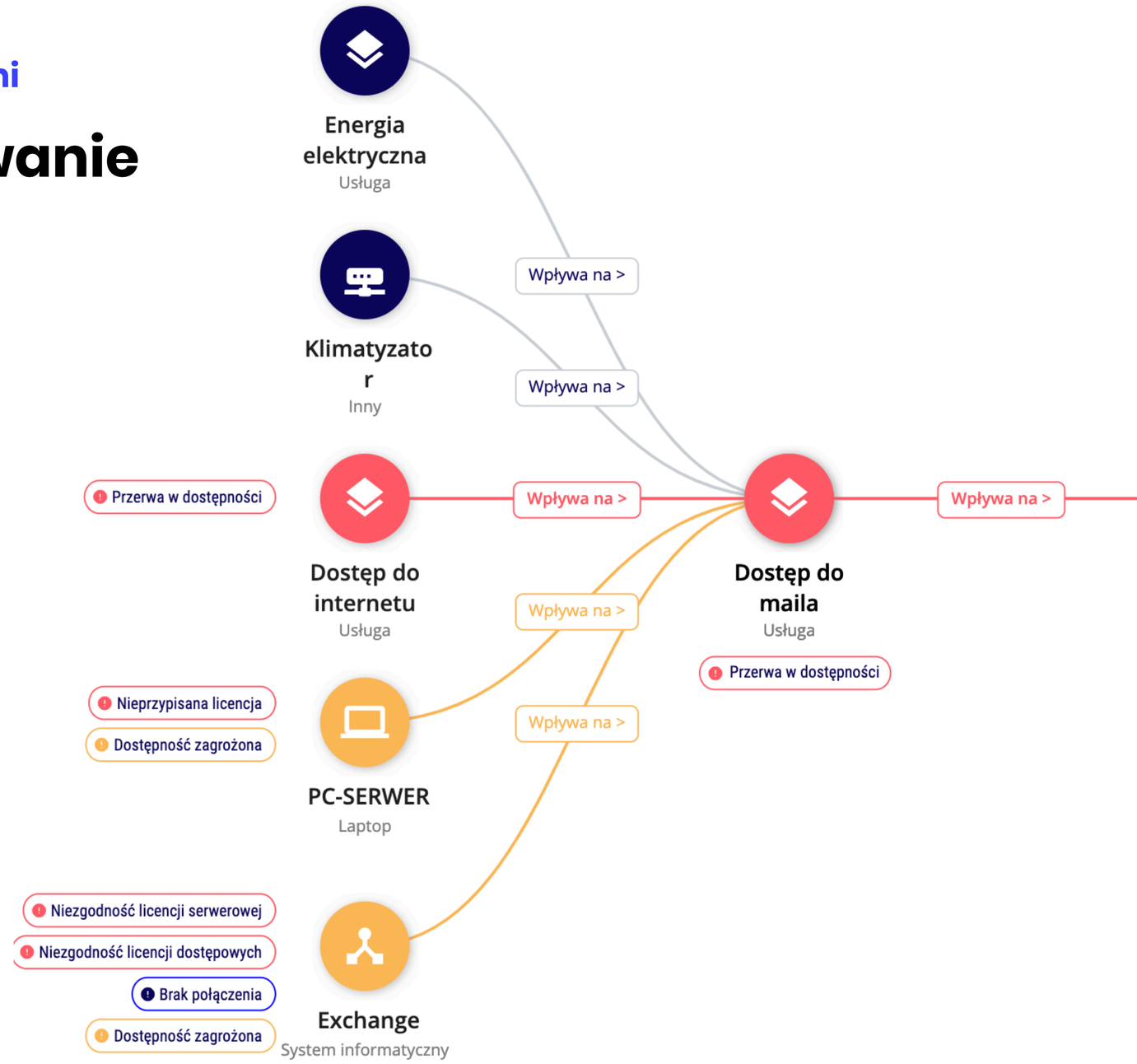
1 x Serwer i VM:

1 x Licencja:

1 x Urządzenie sieciowe:

Opcjonalne zasoby i usługi

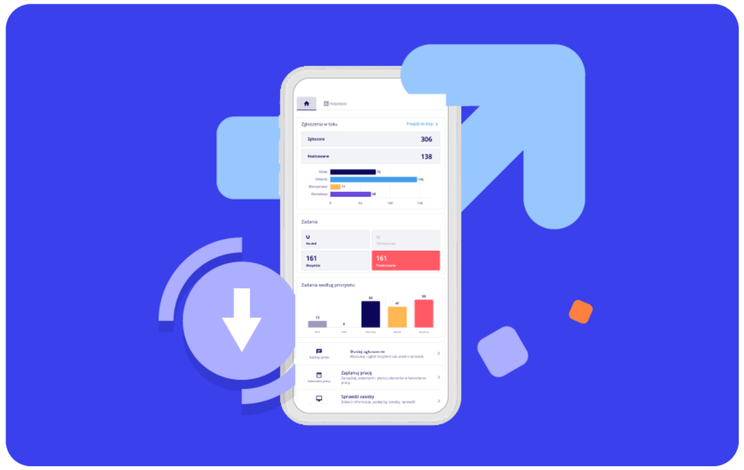
Brak



LOG PLUS

LOG PLUS

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

LOG PLUS

Dziękuję za uwagę
i zapraszam do dyskusji!

logplus.io