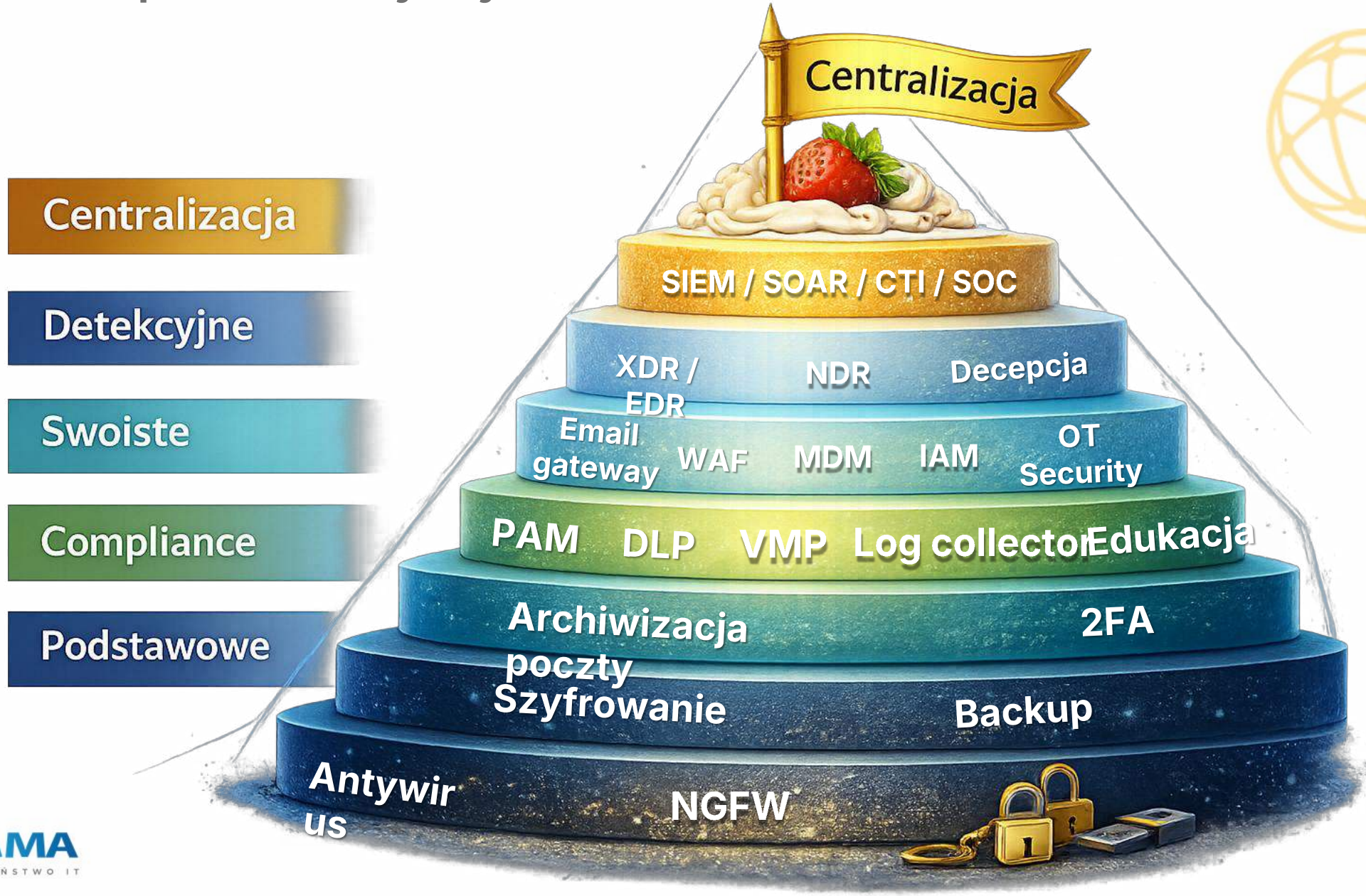
Synergia PAM i DLP, czyli jak projektując cyberbezpieczeństwo nie zapomnieć o najważniejszym czynniku

DAGMA

BEZPIECZEŃSTWO IT

Cyberbezpieczeństwo jest jak...



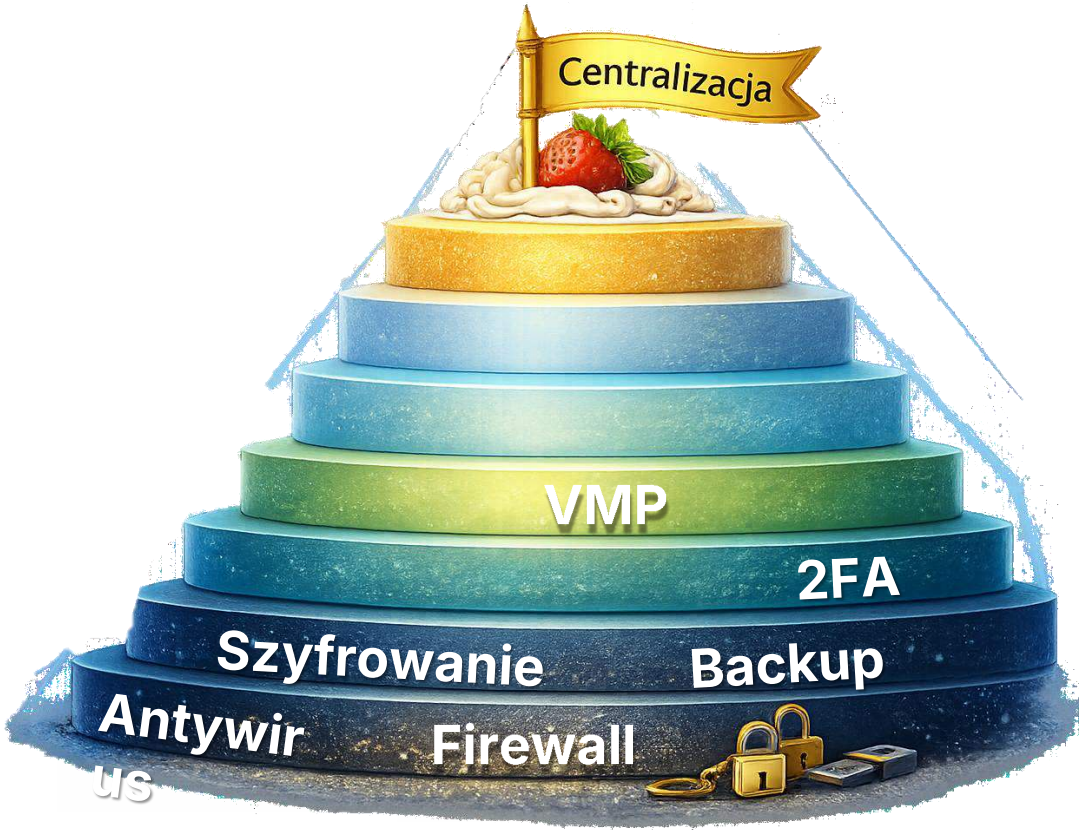
DAGMA
BEZPIECZEŃSTWO IT

Tymczasem cyberbezpieczeństwo historycznie...

DAGMA
BEZPIECZEŃSTWO IT

Tymczasem cyberbezpieczeństwo historycznie...

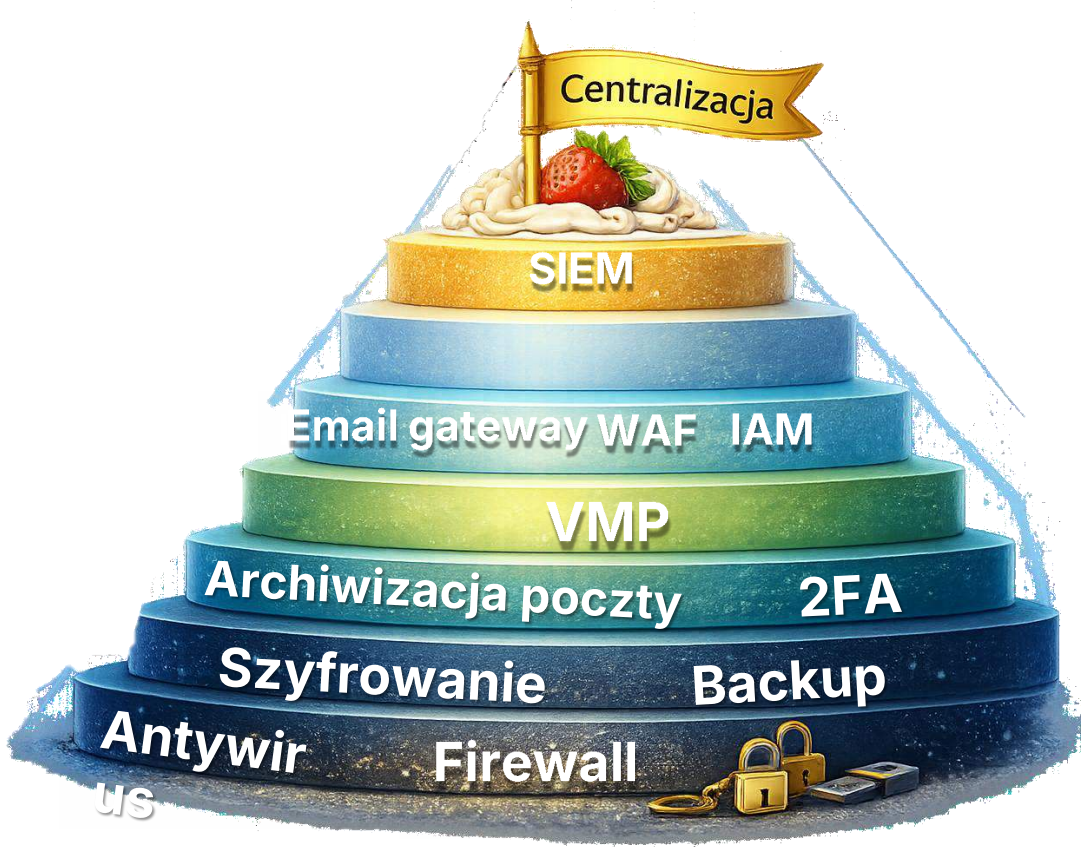
...1999



DAGMA
BEZPIECZEŃSTWO IT

Tymczasem cyberbezpieczeństwo historycznie...

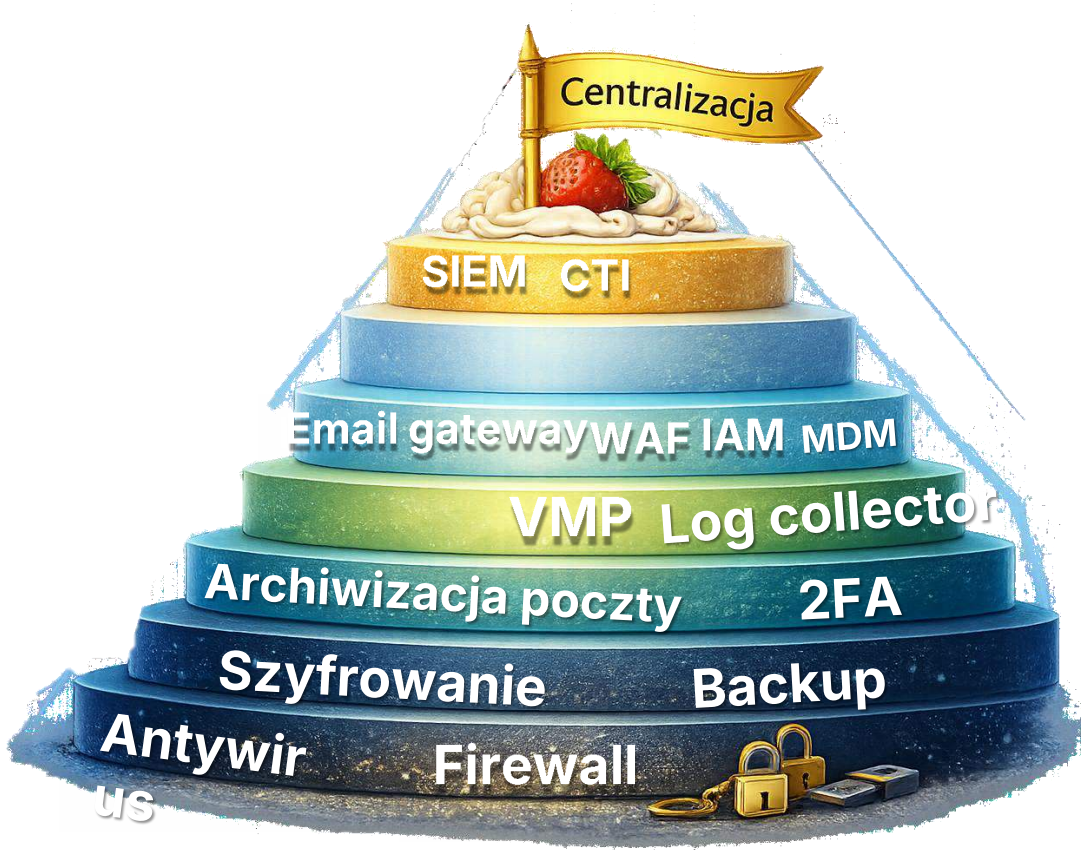
...2005



DAGMA
BEZPIECZEŃSTWO IT

Tymczasem cyberbezpieczeństwo historycznie...

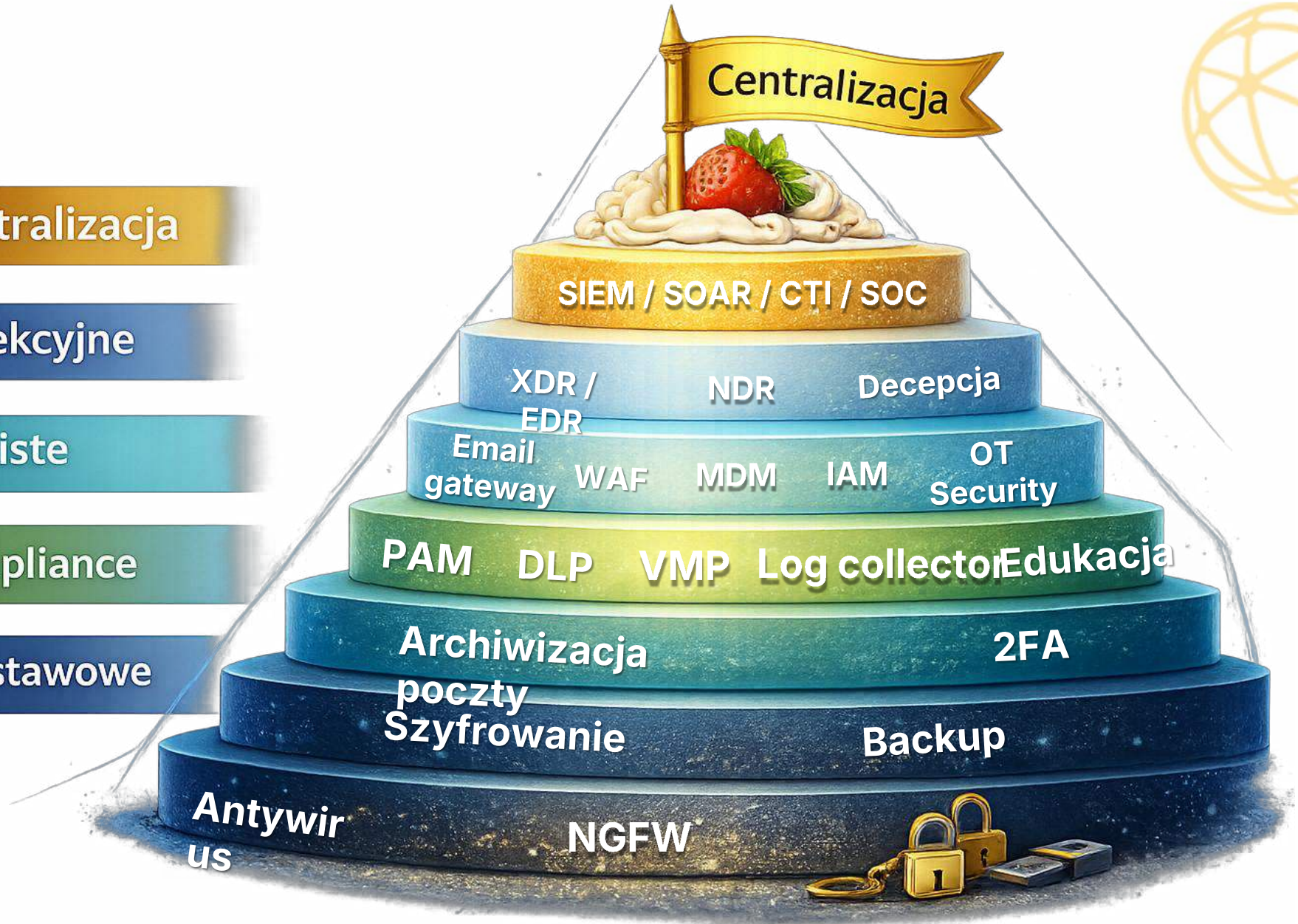
...2010



DAGMA
BEZPIECZEŃSTWO IT

Tymczasem cyberbezpieczeństwo historycznie...

...DZIŚ



DAGMA
BEZPIECZEŃSTWO IT

Compliance !

DLP - DATA LEAK PREVENTION

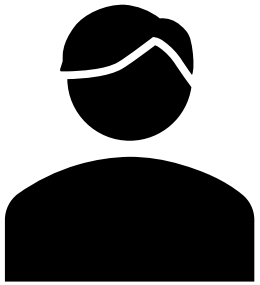
safetica

PAM - PRIVILAGE ACCES MANAGEMENT

segura®

DAGMA
BEZPIECZEŃSTWO IT

Compliance !



safetica

Zabezpieczenie danych przed wyciekiem

segura®

Zabezpieczenie poświadczeń administracyjnych

DAGMA
BEZPIECZEŃSTWO IT

segura®

Rozwiązanie klasy PAM do zarządzania dostępami uprzywilejowanymi

DAGMA
BEZPIECZEŃSTWO IT

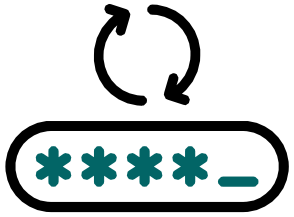
segura®

Co łączy każdy atak hakerski?

DAGMA
BEZPIECZEŃSTWO IT

segura

Co łączy (prawie) każdy atak hakerski?



Poświadczenia administratora

=

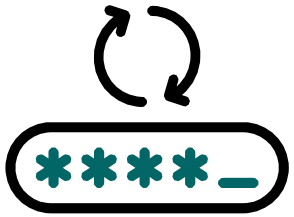
RYZYKO I PROBLEM

DAGMA
BEZPIECZEŃSTWO IT

segura

A co jeśli...

...administrator nie zna poświadczeń?



Poświadczenia administratora

=

RYZYKO I PROBLEM

DAGMA
BEZPIECZEŃSTWO IT

segura

Dostęp bez hasła ?!

Rozwiązanie klasy PAM

Privilage

Access

Management

DAGMA
BEZPIECZEŃSTWO IT

segura®

segura®

Na czym opierają się założenia PAM?

Na czym opierają się założenia PAM?

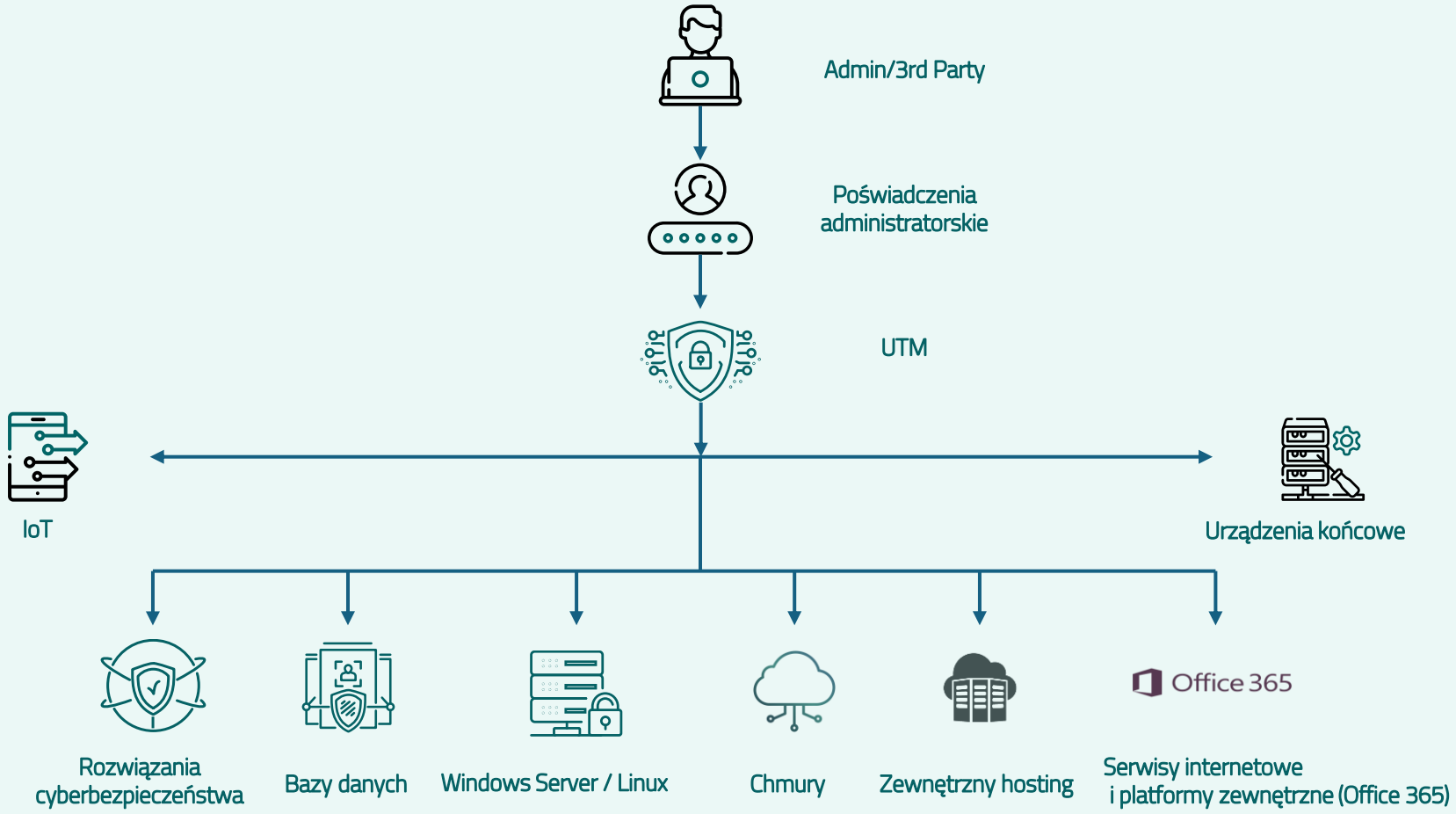
Zasada najmniejszych przywilejów

Zasada zakładająca, że dany użytkownik, **program czy proces** powinien mieć **minimalną ilość uprawnień** aby zapewnić mu możliwość wykonywania zadania na czas.

DAGMA
BEZPIECZEŃSTWO IT

segura

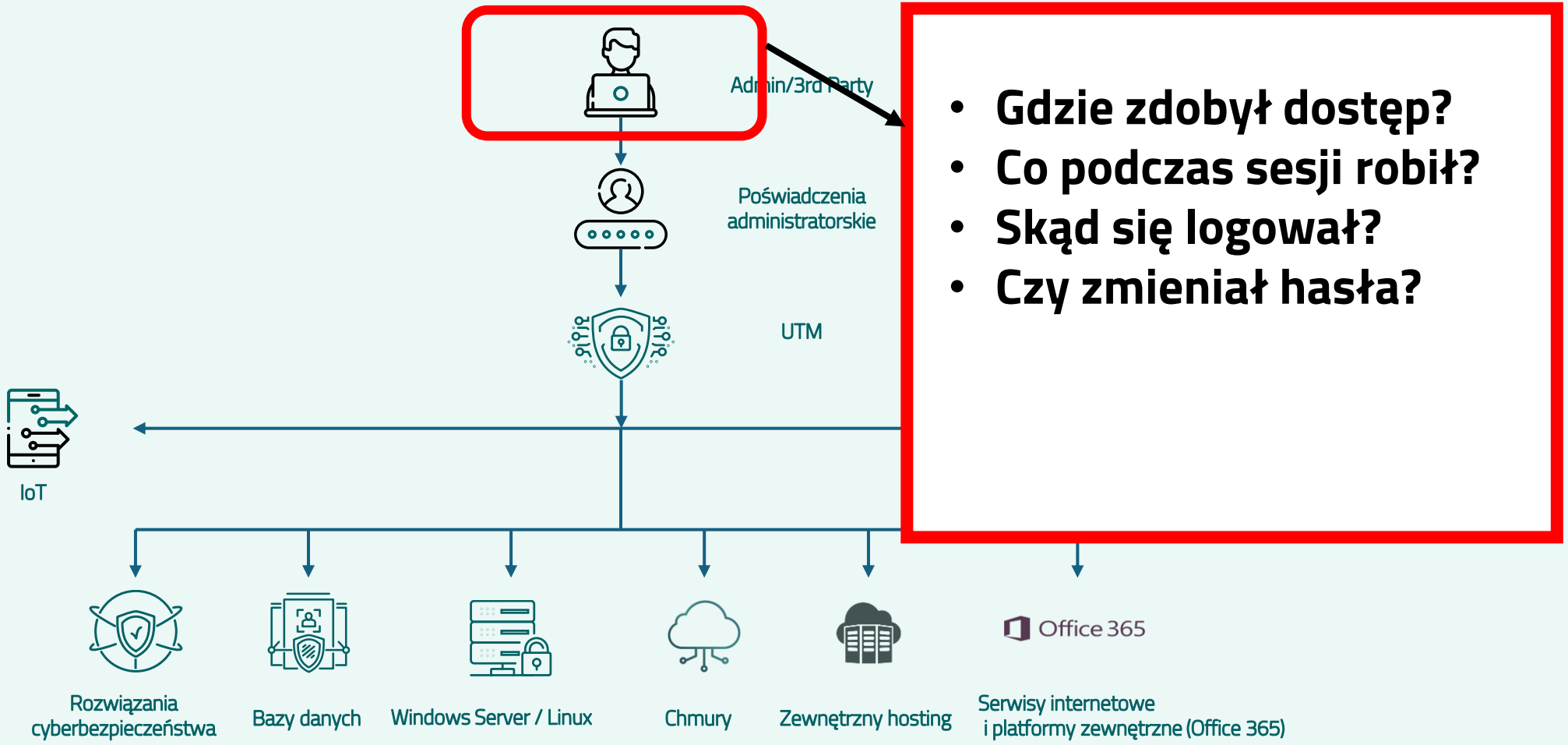
Zasada działania segura



DAGMA
BEZPIECZEŃSTWO IT

segura

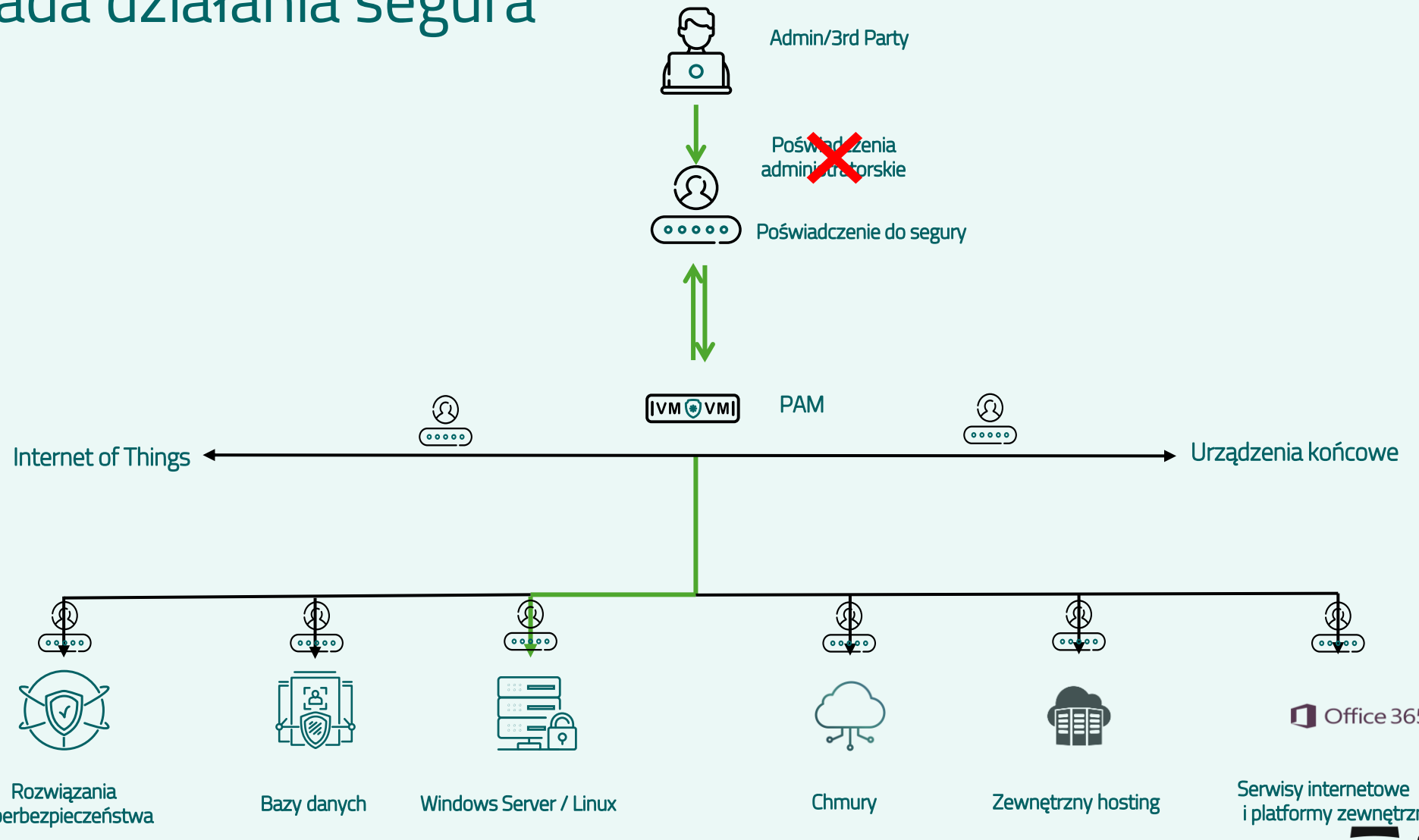
Zasada działania segura



DAGMA
BEZPIECZEŃSTWO IT

segura

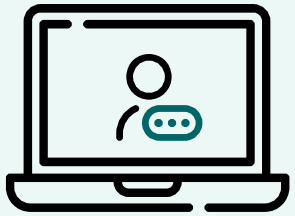
Zasada działania segura



DAGMA
BEZPIECZEŃSTWO IT

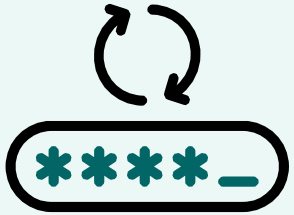
segura

Co zyskujemy?



Mitygacja ryzyka pozyskania poświadczeń administratorskich podczas ataku

Mitygacja ryzyka związanego z 3rd party



Mitygacja ryzyka „backdoor”

§

Zwiększenie zgodności z compliance

$

Oszczędności i wygoda

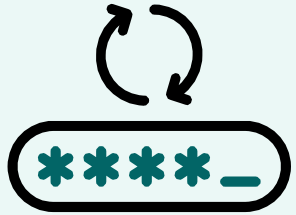
DAGMA
BEZPIECZEŃSTWO IT

segura

W jaki sposób?

Zarządzanie dostępem

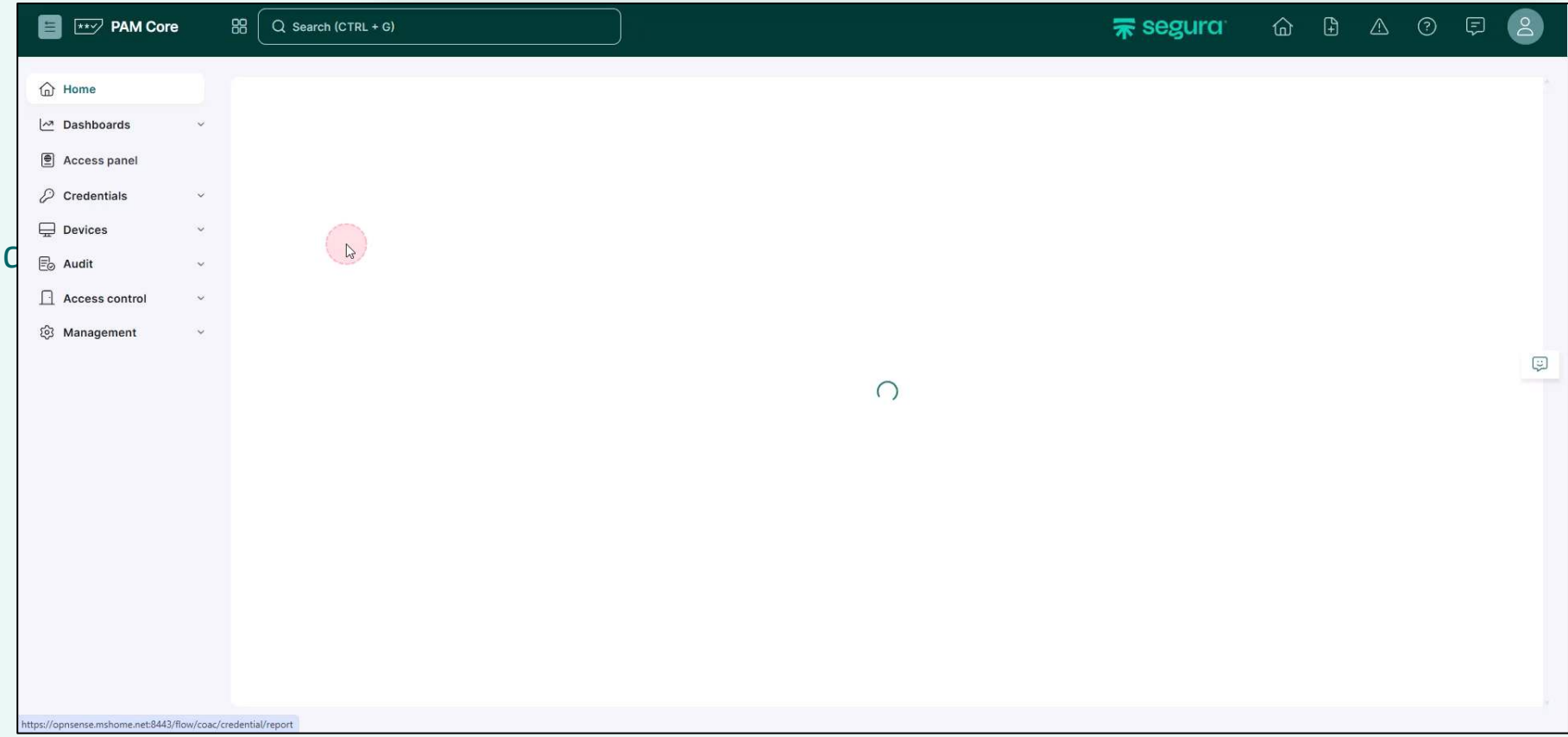
Zarządzanie sesją



Zarządzanie hasłami

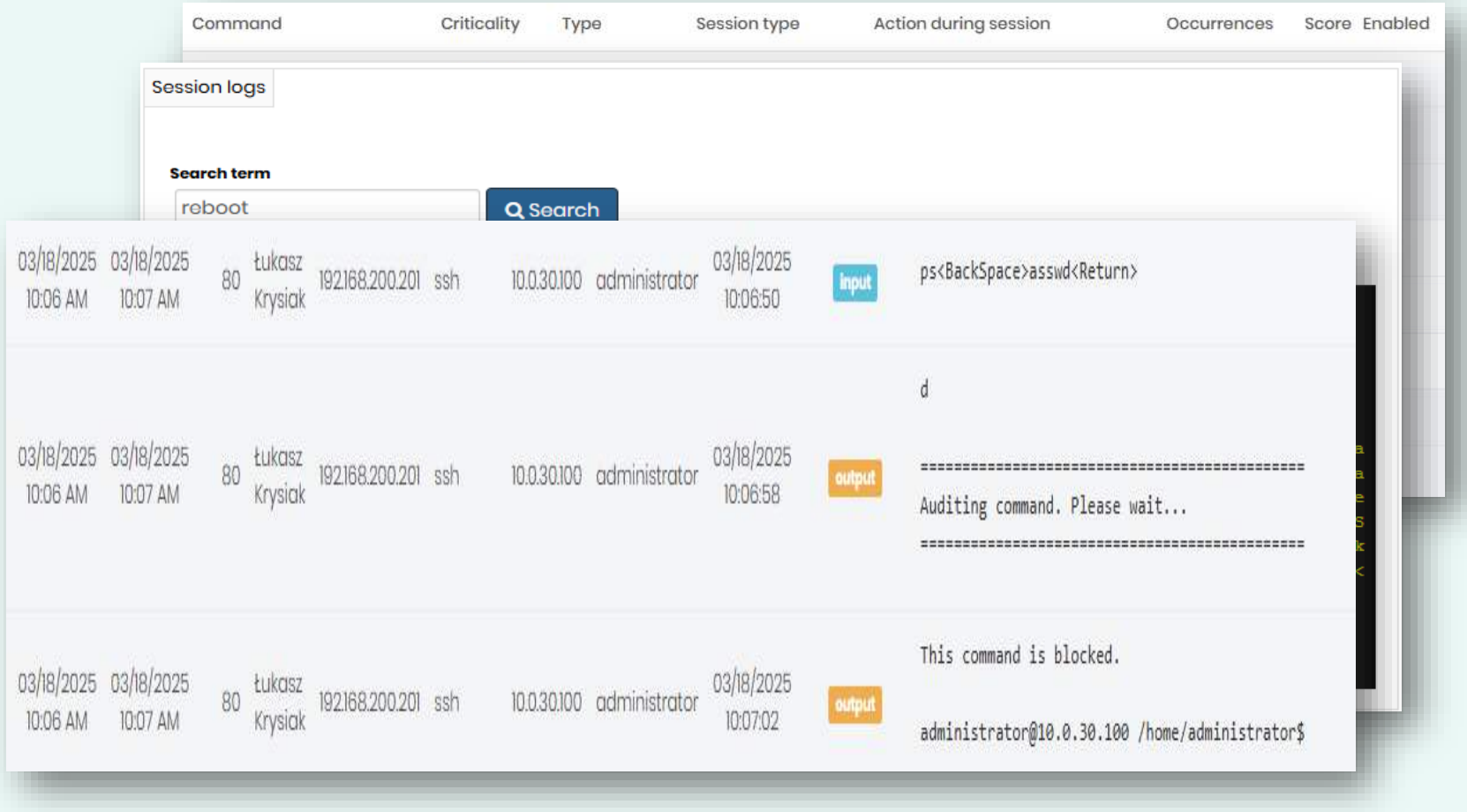
Zarządzanie dostępem

- Zdefiniowanie zakresu
- Określenie kiedy może mieć dostęp
- Przypisywanie użytkowników d grup
- Dodatkowa autoryzacja przy próbie dostępu
- Poświadczenia JiT
- Dostęp nadzwyczajny
- Analiza behawioralna

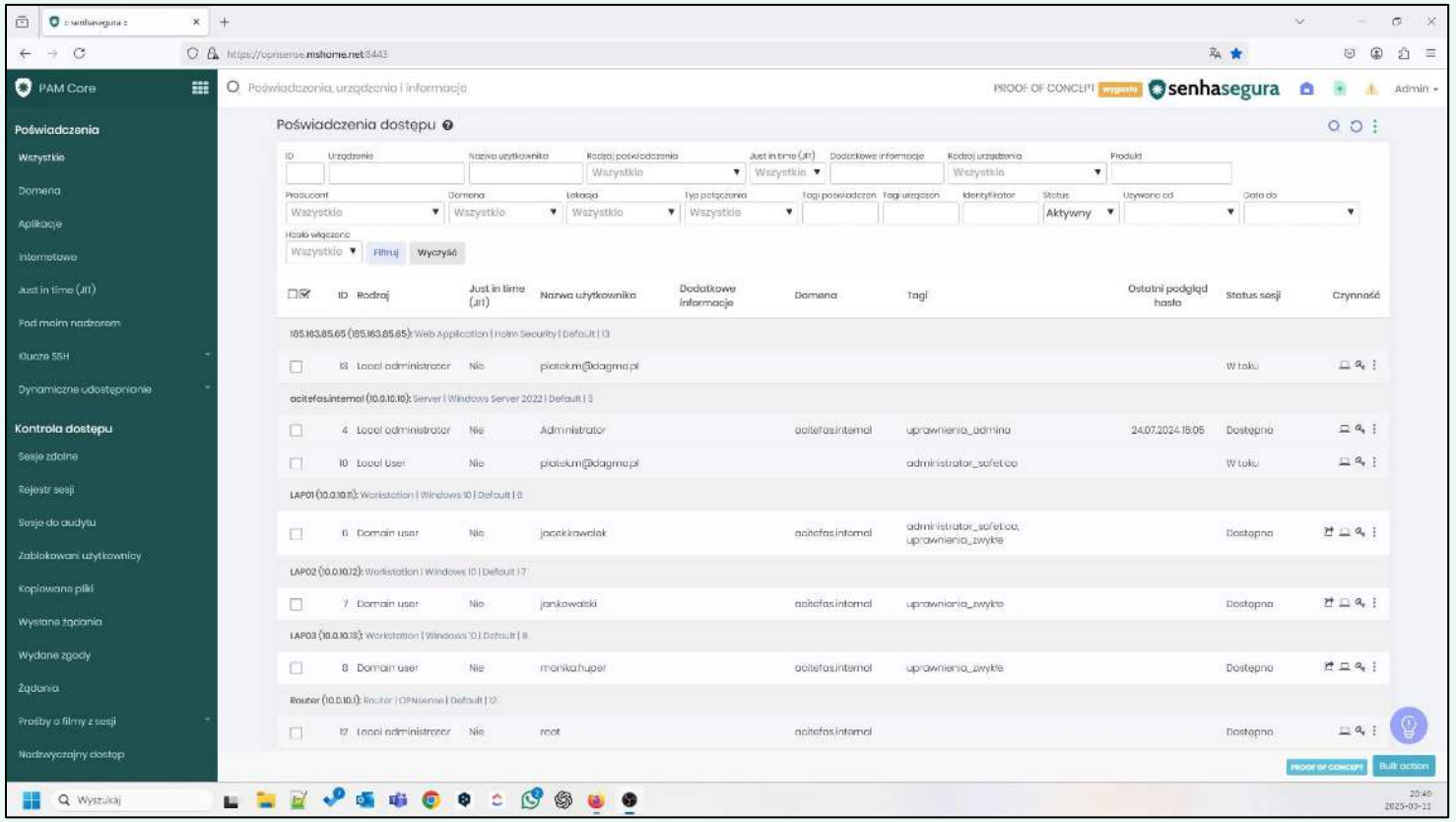


Zarządzanie sesją (pasywne)

- Audyt komend („komendy zakazane”
- OCR
- Analiza przyciśnięć klawiatury
- Raporty z sesji
- Logi z sesji (integracja z SIEM)

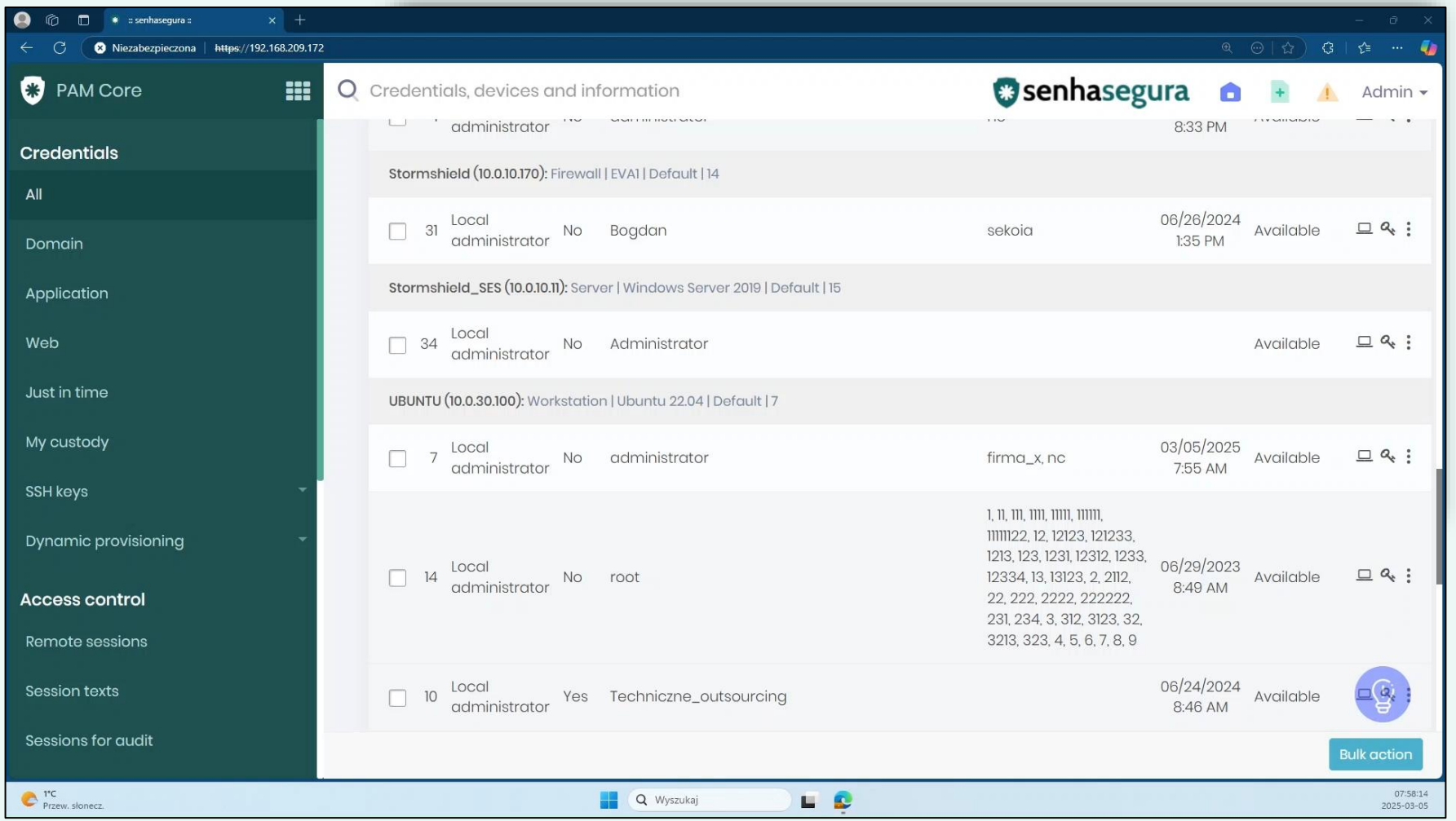


Zarządzanie sesją (aktywne)

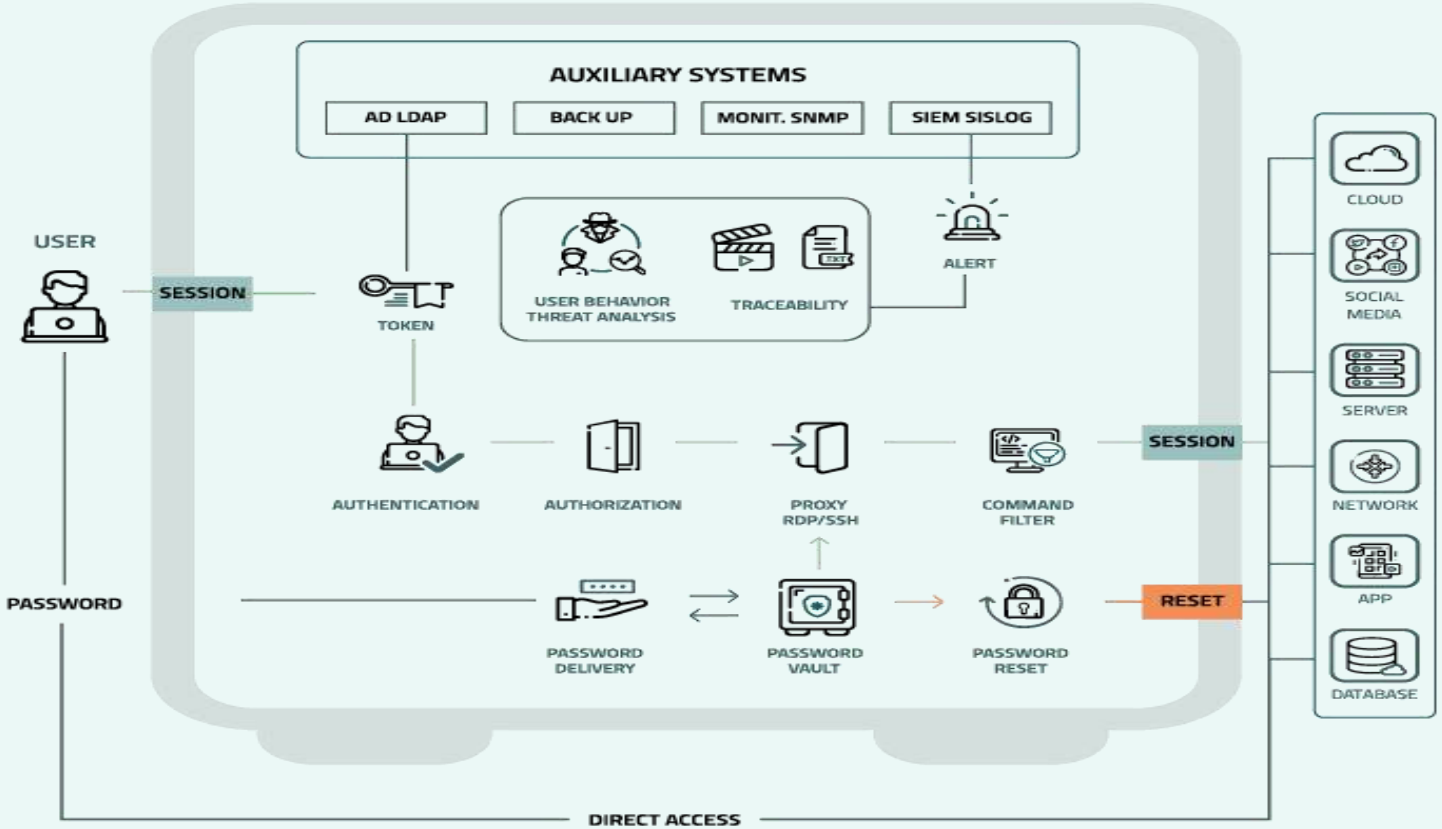


Zarządzanie hasłami

- Hasła paranoiczne
- Hasła rotujące
- Odpowiedzialność za hasła
- Obsługa kluczy SSH
- Obsługa 2FA
- Przechowywanie haseł w zaszyfrowanej architekturze



Jaki efekt otrzymamy?



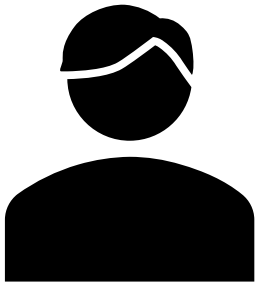
DAGMA
BEZPIECZEŃSTWO IT

segura

DAGMA
BEZPIECZEŃSTWO IT

segura®

Compliance !



safetica

Zabezpieczenie danych przed wyciekiem

segura®

Zabezpieczenie poświadczeń administracyjnych

DAGMA
BEZPIECZEŃSTWO IT

safetica

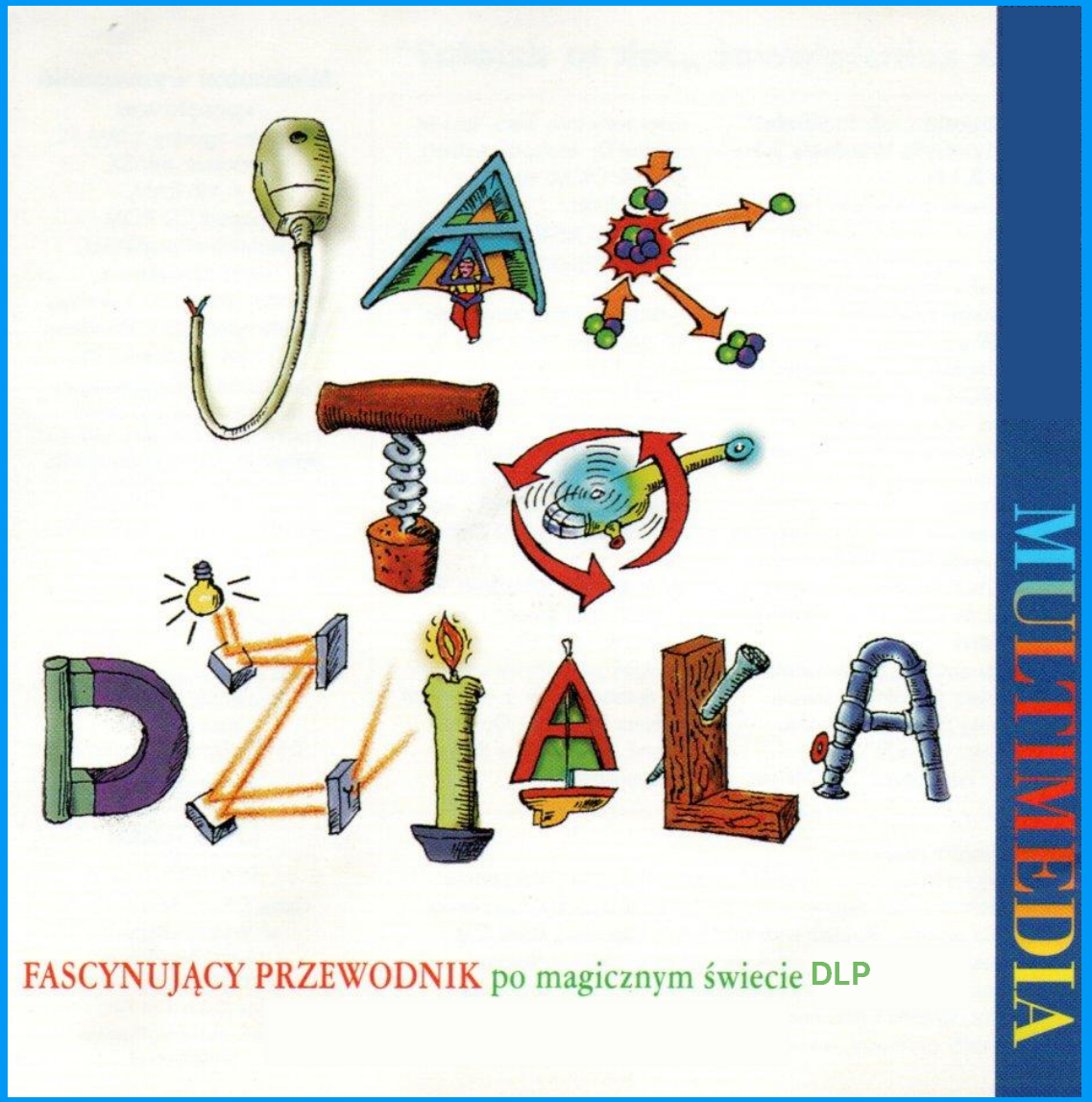
Rozwiązanie klasy DLP do zabezpieczania danych

DAGMA
BEZPIECZEŃSTWO IT

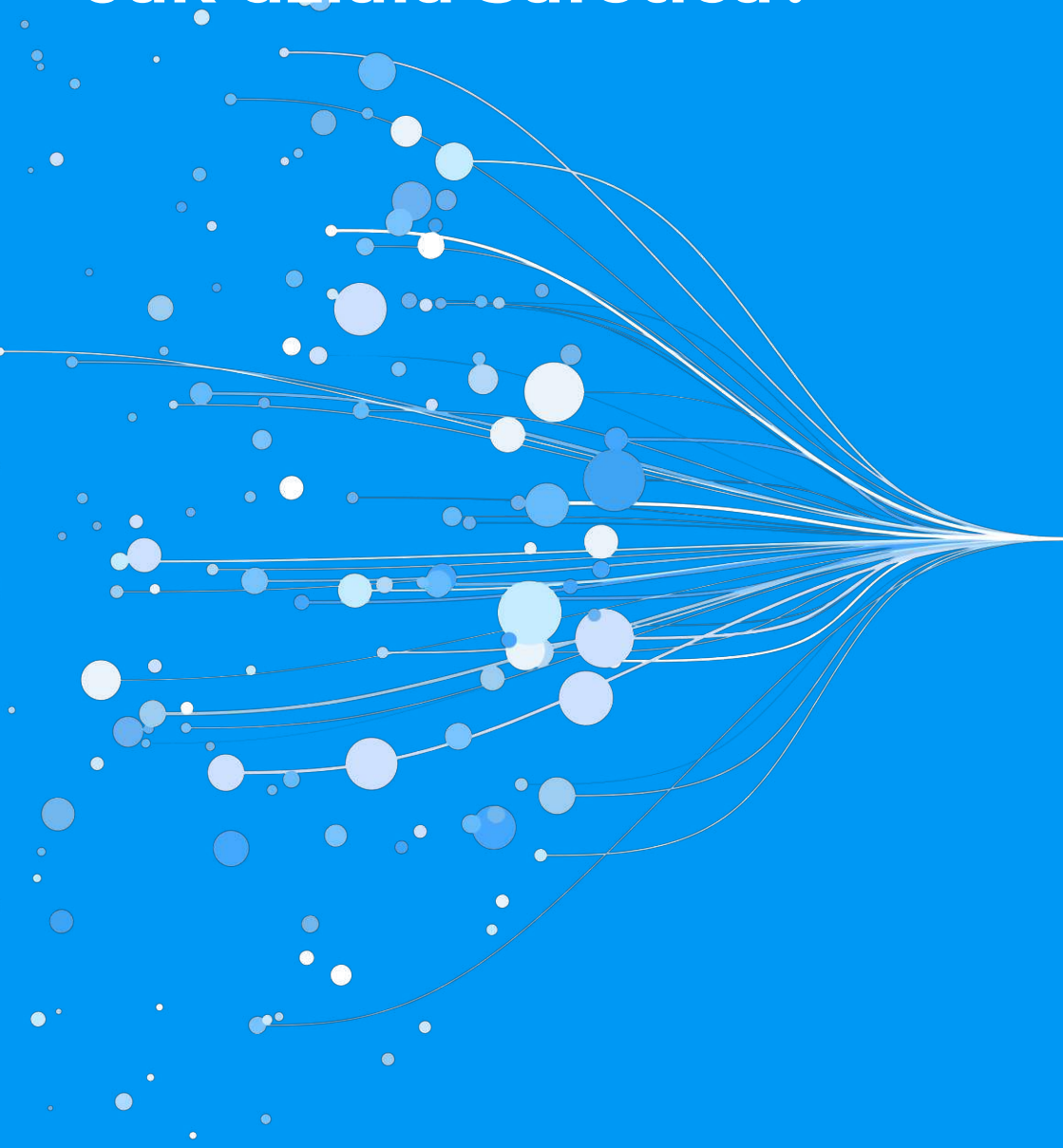
Rozwiązanie klasy DLP do zabezpieczania danych

- Zarządzanie ryzykiem
- Zabezpieczenie know-how
- Minimalizacja incydentu bezpieczeństwa

DAGMA
BEZPIECZEŃSTWO IT


JAK
DZIAŁA
FASCYNUJĄCY PRZEWODNIK po magicznym świecie DLP
MULTIMEDIA

Jak działa Safetica?



Ochrona danych
z Safetica

KONFIGURUJ

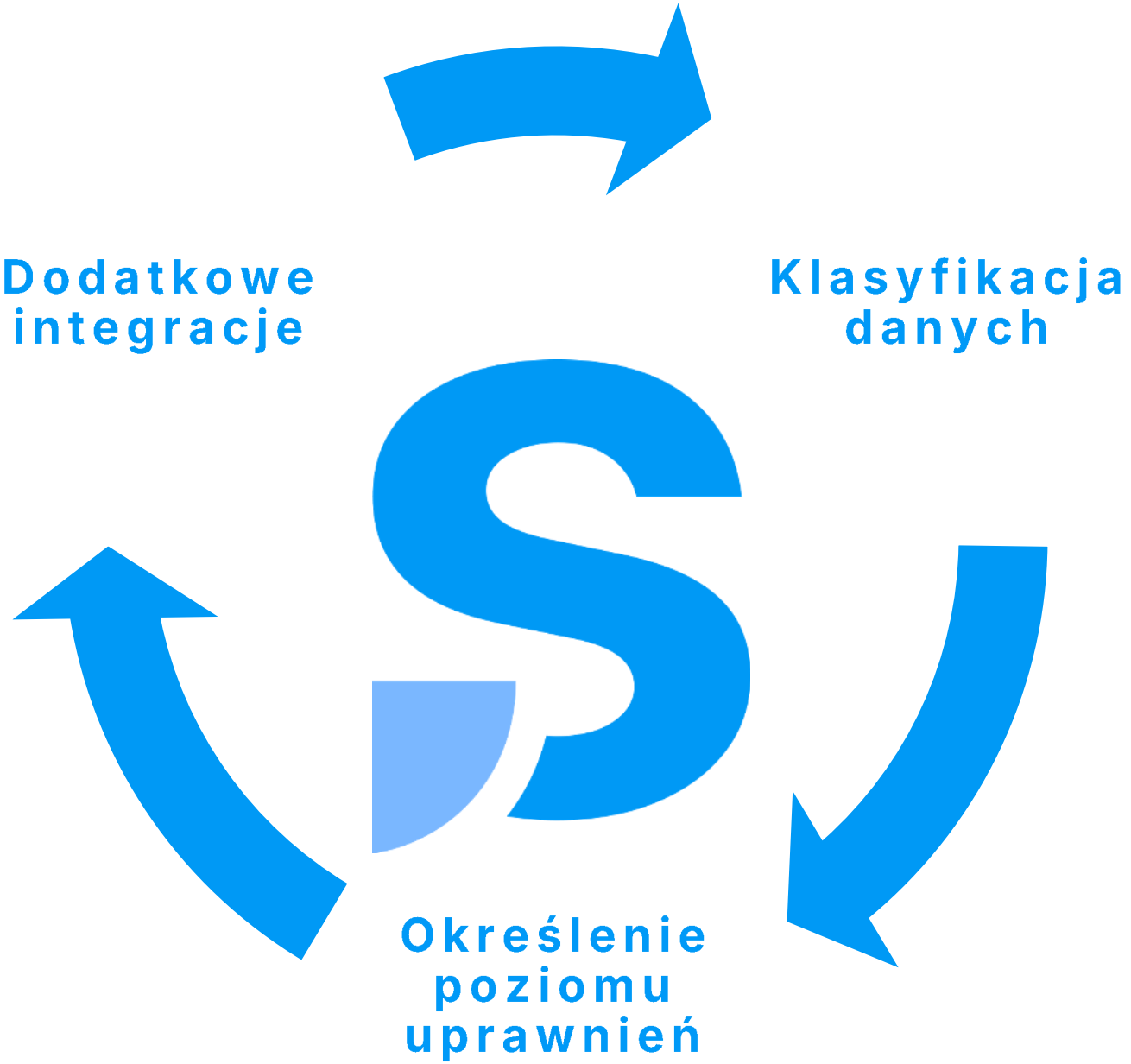
ANALIZUJ

OPTYMALIZUJ

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ



KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Klasyfikacja danych

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Klasyfikacja danych

- Zawartość
- Źródło pochodzenia
- Ręczna klasyfikacja
- Zewnętrzne klasyfikatory
- Typ pliku
- Automatyczna klasyfikacja (AI)*

Pliki zaszyfrowane

PESEL

Numer karty kredytowej

Numer dowodu osobistego

Słowa kluczowe

Regex

...itd.

* Tylko w wersji

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Klasyfikacja danych

- Zawartość
- Źródło pochodzenia
- Ręczna klasyfikacja
- Zewnętrzne klasyfikatory
- Typ pliku
- Automatyczna klasyfikacja (AI)*

Aplikacje
(po kategoriach)

Foldery
(Sieciowe lub lokalne)

Strony www
(Po domenach lub URL)

* Tylko w wersji

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Klasyfikacja danych

- Zawartość
- Źródło pochodzenia
- Ręczna klasyfikacja
- Zewnętrzne klasyfikatory
- Typ pliku
- Automatyczna klasyfikacja (AI)*

* Tylko w wersji

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Klasyfikacja danych

- Zawartość
- Źródło pochodzenia
- Ręczna klasyfikacja
- Zewnętrzne klasyfikatory
- Typ pliku
- Automatyczna klasyfikacja (AI)*

SECLORE

netwrix

TITUS

GREENmod
SYSTEM DO KLASYFIKACJI PLIKÓW I POCZTY ELEKTRONICZNEJ

* Tylko w wersji

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Klasyfikacja danych

- Zawartość
- Źródło pochodzenia
- Ręczna klasyfikacja
- Zewnętrzne klasyfikatory
- Typ pliku
- Automatyczna klasyfikacja (AI)*

.pdf

.xlsx

.dng

.txt

.dwg

* Tylko w wersji

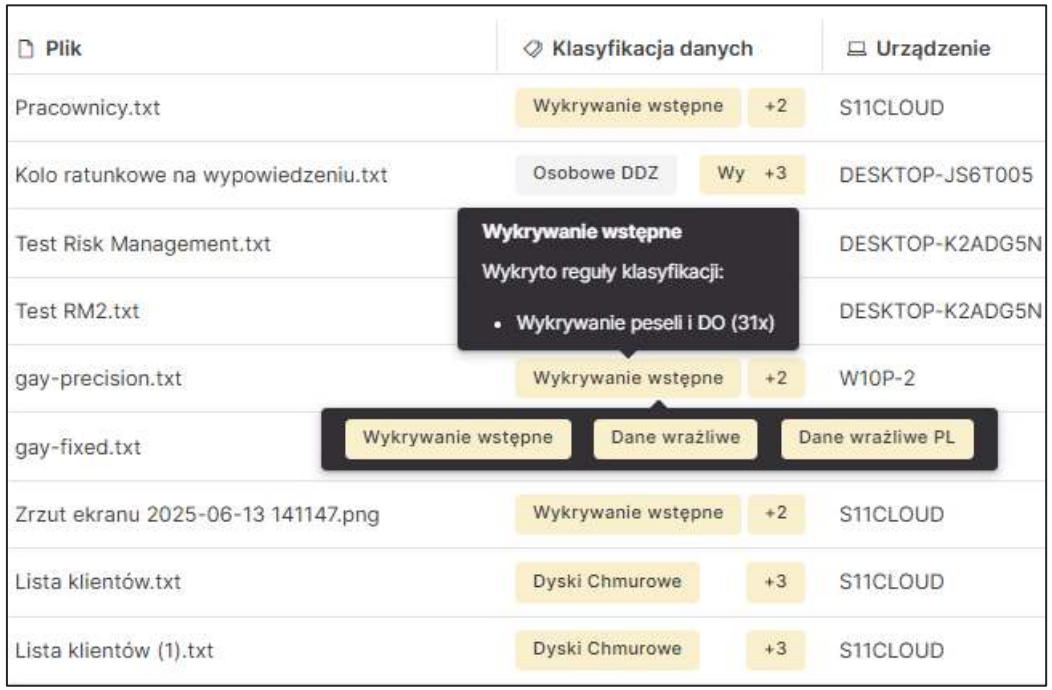
Klasyfikacja danych

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

- Zawartość
- Źródło pochodzenia
- Ręczna klasyfikacja
- Zewnętrzne klasyfikatory
- Typ pliku
- Automatyczna klasyfikacja (AI)*



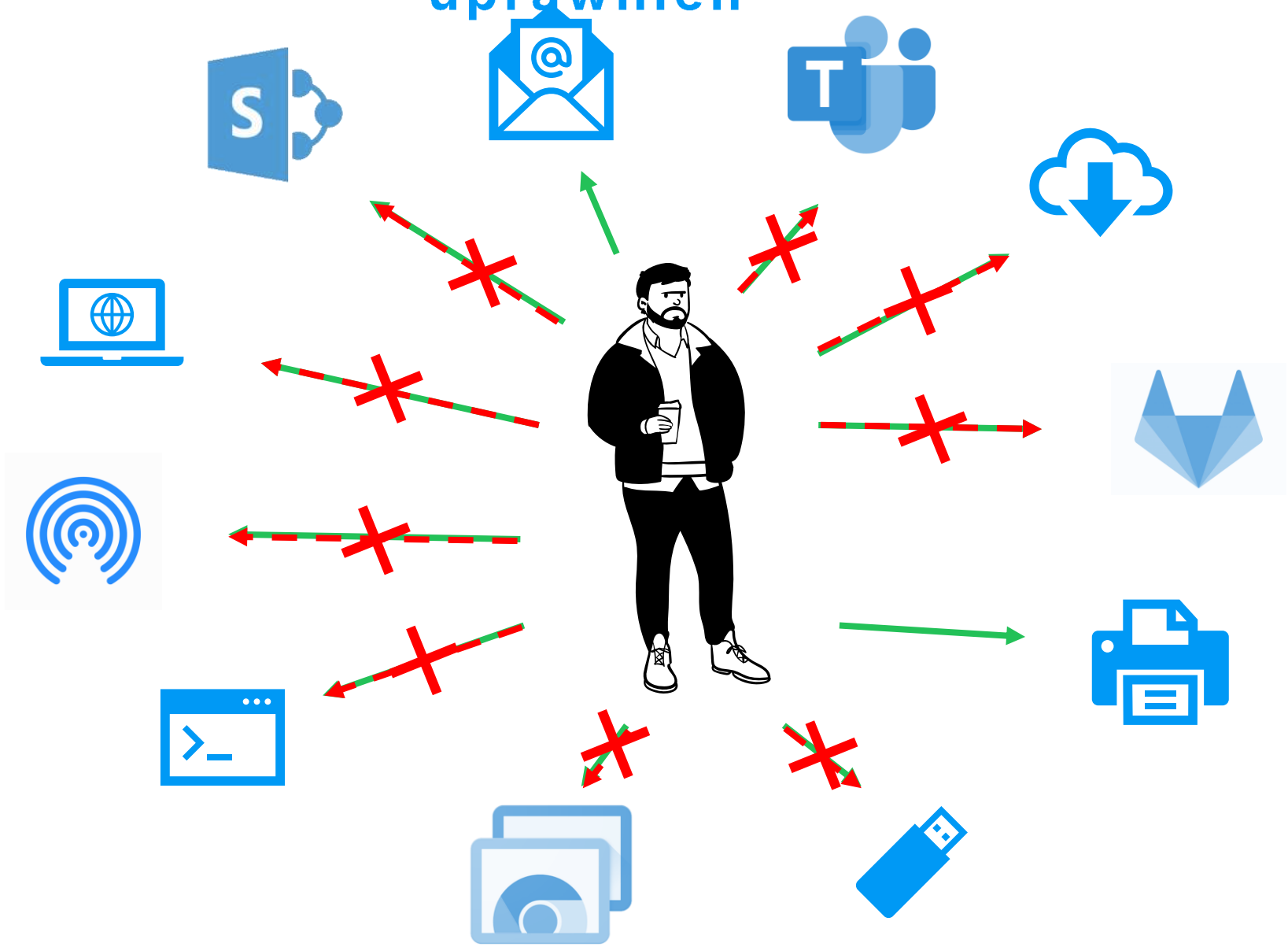
* Tylko w wersji

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Określenie poziomu uprawnień

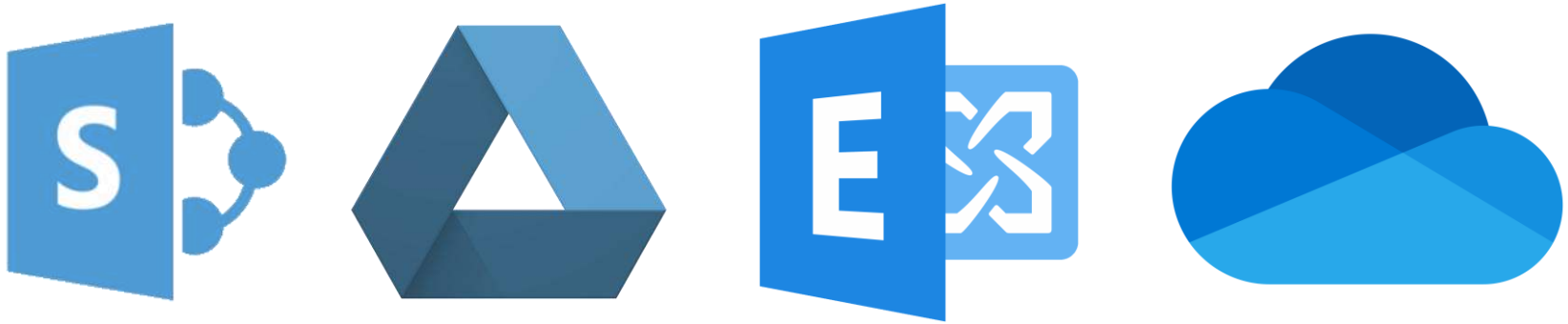


KONFIGURUJ

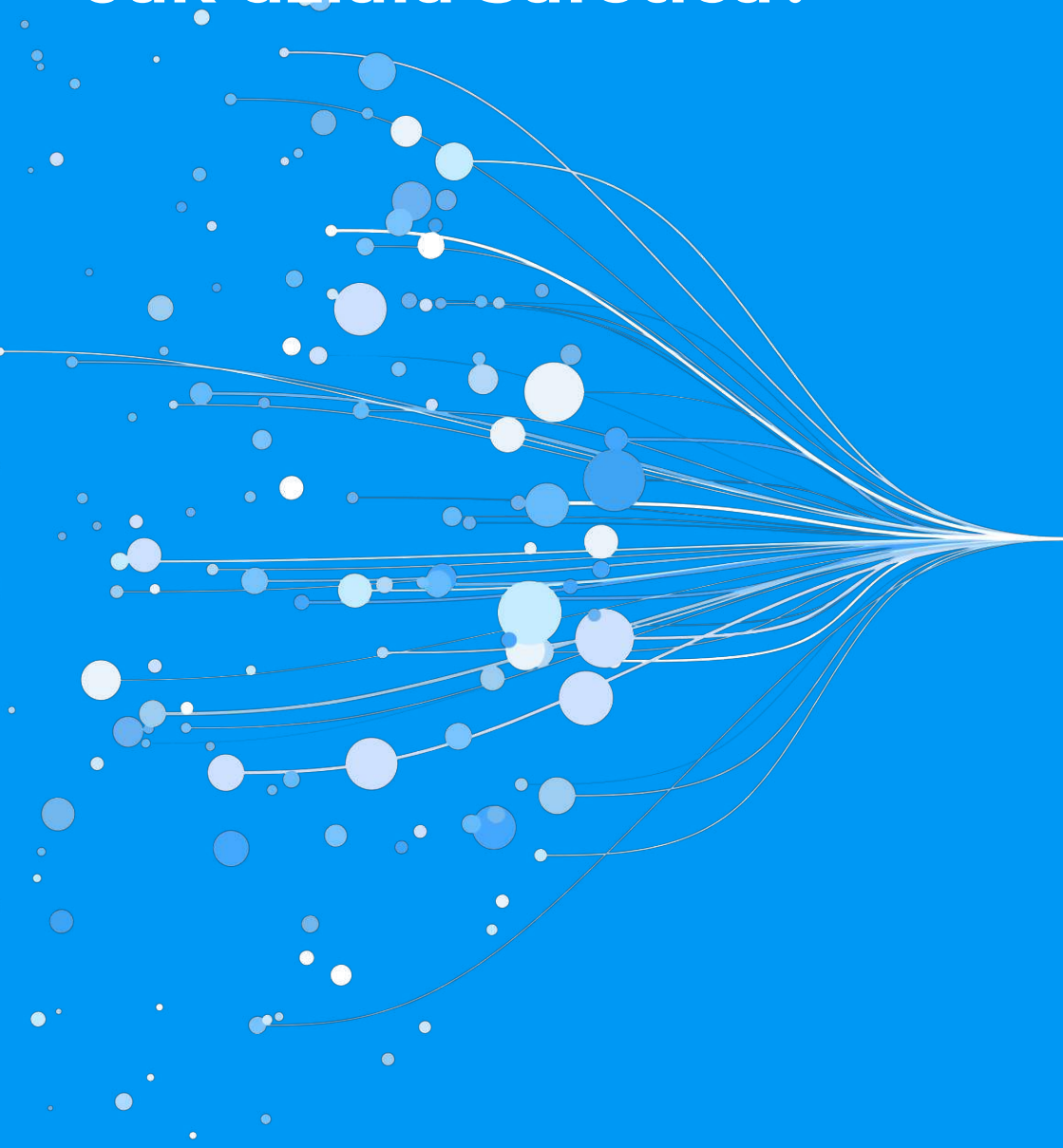
ANALIZUJ

OPTYMALIZUJ

Dodatkowe integracje



Jak działa Safetica?



Ochrona danych
z Safetica

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Monitorowanie aktywności

+

Raportowanie

KONFIGURUJ

ANALIZUJ

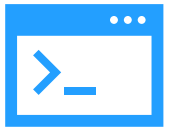
OPTYMALIZUJ

Monitorowanie aktywności
+
Raportowanie

Strony WWW

E-mail

Chmura

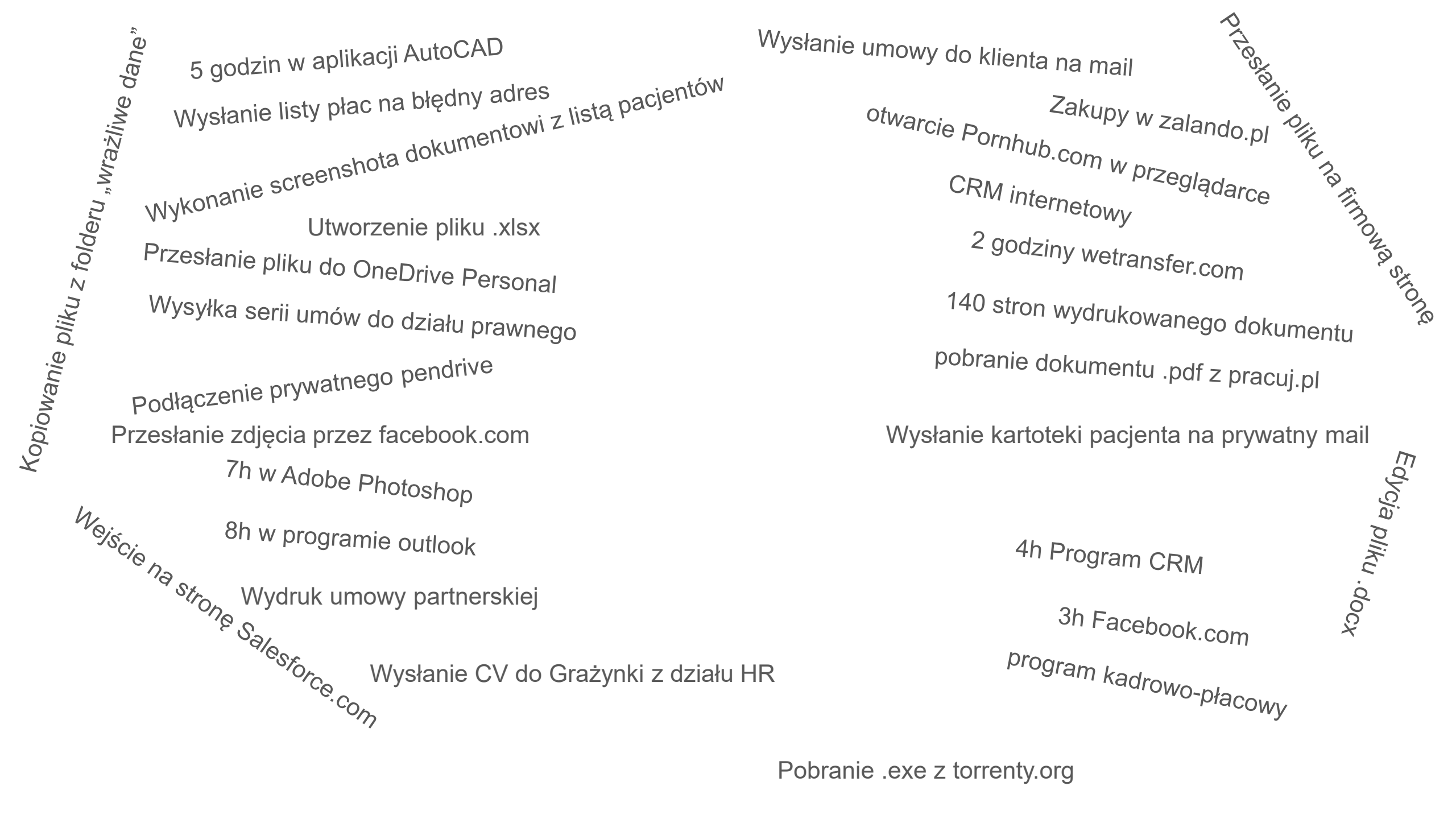


Aplikacje

Urządzenia

Drukowanie

Operacje na plikach


Kopiowanie pliku z folderu „wrażliwe dane”
5 godzin w aplikacji AutoCAD
Wysłanie listy płac na błędny adres
Wykonanie screenshota dokumentowi z listą pacjentów
Utworzenie pliku .xlsx
Przesłanie pliku do OneDrive Personal
Wysyłka serii umów do działu prawnego
Podłączenie prywatnego pendrive
Przesłanie zdjęcia przez facebook.com
7h w Adobe Photoshop
8h w programie outlook
Wydruk umowy partnerskiej
Wejście na stronę Salesforce.com
Wysłanie CV do Grażynki z działu HR
Pobranie .exe z torrenty.org
Wysłanie umowy do klienta na mail
Przesłanie pliku na firmową stronę
Zakupy w zalando.pl
otwarcie Pornhub.com w przeglądarce
CRM internetowy
2 godziny wetransfer.com
140 stron wydrukowanego dokumentu
pobranie dokumentu .pdf z pracuj.pl
Wysłanie kartoteki pacjenta na prywatny mail
Edycja pliku .docx
4h Program CRM
3h Facebook.com
program kadrowo-płacowy

Audyt Bezpieczeństwa

5 godzin w aplikacji AutoCAD

Wysłanie listy płac na błędny adres

Wykonanie screenshota dokumentowi z listą pacjentów

Utworzenie pliku .xlsx

Przesłanie pliku do OneDrive Personal

Wysyłka serii umów do działu prawnego

Wysłanie umowy do klienta na mail

Zakupy w zalando.pl

otwarcie Pornhub.com w przeglądarce

CRM internetowy

2 godziny wetransfer.com

140 stron wydrukowanego dokumentu

pobranie dokumentu .pdf z pracuj.pl

Kopiowanie pliku z folderu „wrażliwe dane”

Przesłanie pliku na firmową stronę

Podłączenie prywatnego pendrive

Przesłanie zdjęcia przez facebook.com

7h w Adobe Photoshop

8h w programie outlook

Wydruk umowy partnerskiej

Wejście na stronę Salesforce.com

Wysłanie kartoteki pacjenta na prywatny mail

Podłączenie Pendrive służbowego

4h Program CRM

3h Facebook.com

program kadrowo-płacowy

Edycja pliku .docx

Wysłanie CV do Grażynki z działu HR

Pobranie .exe z torrenty.org

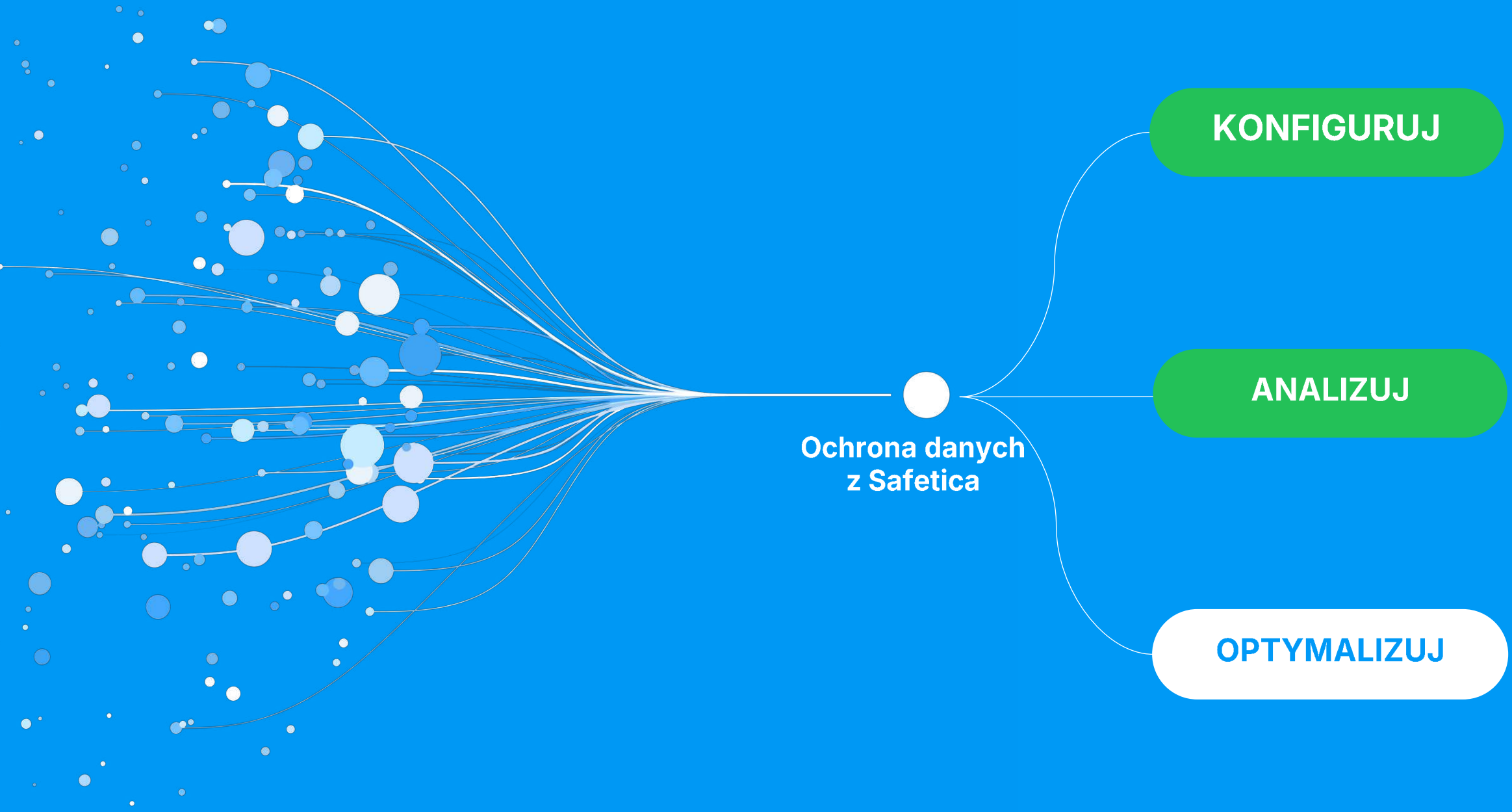

Audyt Bezpieczeństwa
Kopiowanie pliku z folderu „wrażliwe dane”
5 godzin w aplikacji AutoCAD
Wysłanie listy płac na błędny adres
Wykonanie screenshota dokumentowi z listą pacjentów
Utworzenie pliku .xlsx
Przesłanie pliku do OneDrive Personal
Wysyłka serii umów do działu prawnego
Wysłanie umowy do klienta na mail
Zakupy w zalando.pl
otwarcie Pornhub.com w przeglądarce
CRM internetowy
2 godziny wetransfer.com
140 stron wydrukowanego dokumentu
pobranie dokumentu .pdf z pracuj.pl
Przesłanie pliku na firmową stronę
Podłączenie prywatnego pendrive
Przesłanie zdjęcia przez facebook.com
7h w Adobe Photoshop
8h w programie outlook
Wydruk umowy partnerskiej
Wejście na stronę Salesforce.com
Wysłanie CV do Grażynki z działu HR
Pobranie .exe z torrenty.org
Wysłanie kartoteki pacjenta na prywatny mail
Podłączenie Pendrive służbowego
4h Program CRM
3h Facebook.com
program kadrowo-płacowy
Edycja pliku .docx

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Monitorowanie aktywności
+
Raportowanie

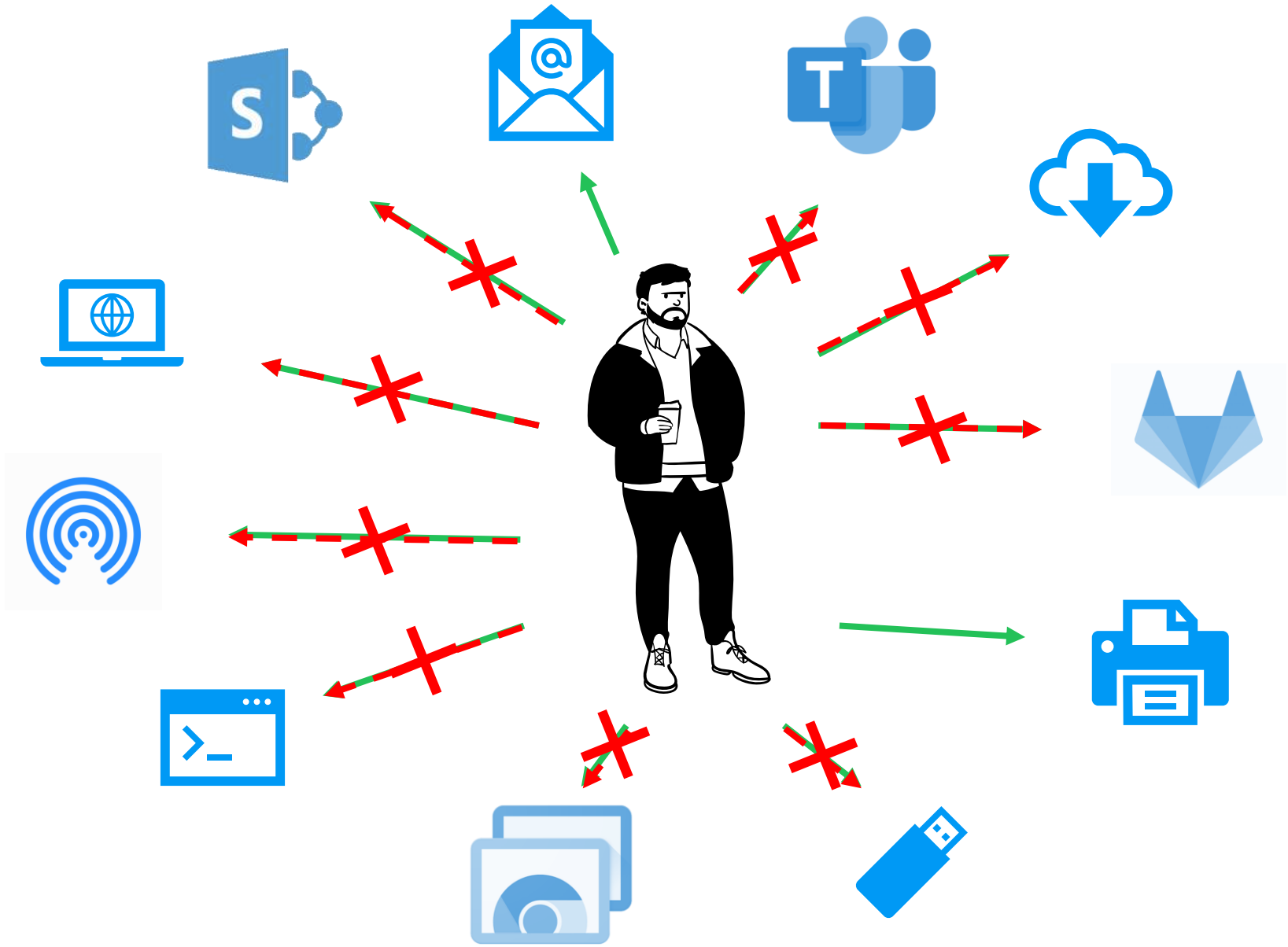

Ochrona danych
z Safetica
KONFIGURUJ
ANALIZUJ
OPTYMALIZUJ

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Skalowanie systemu

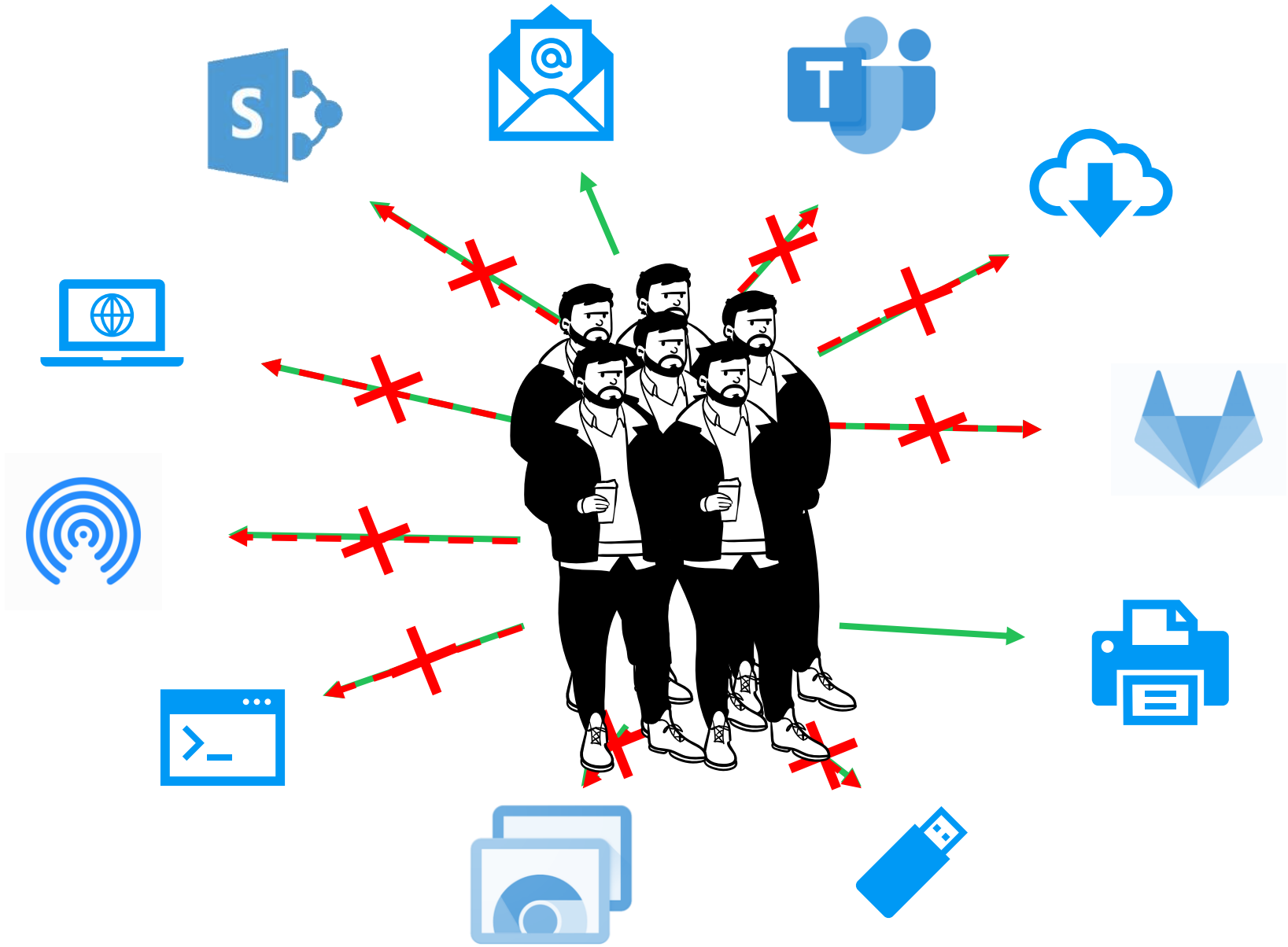


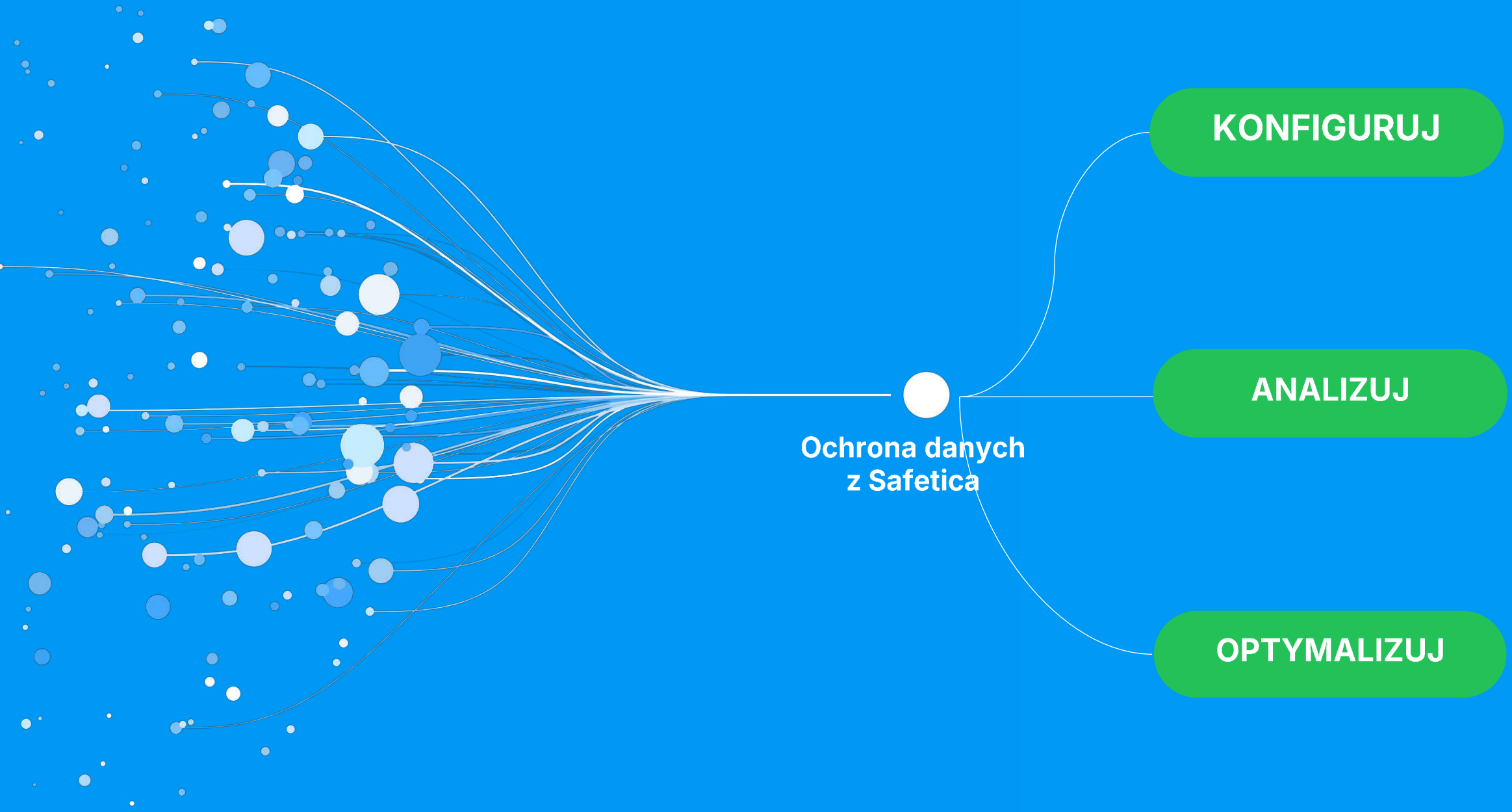
KONFIGURUJ

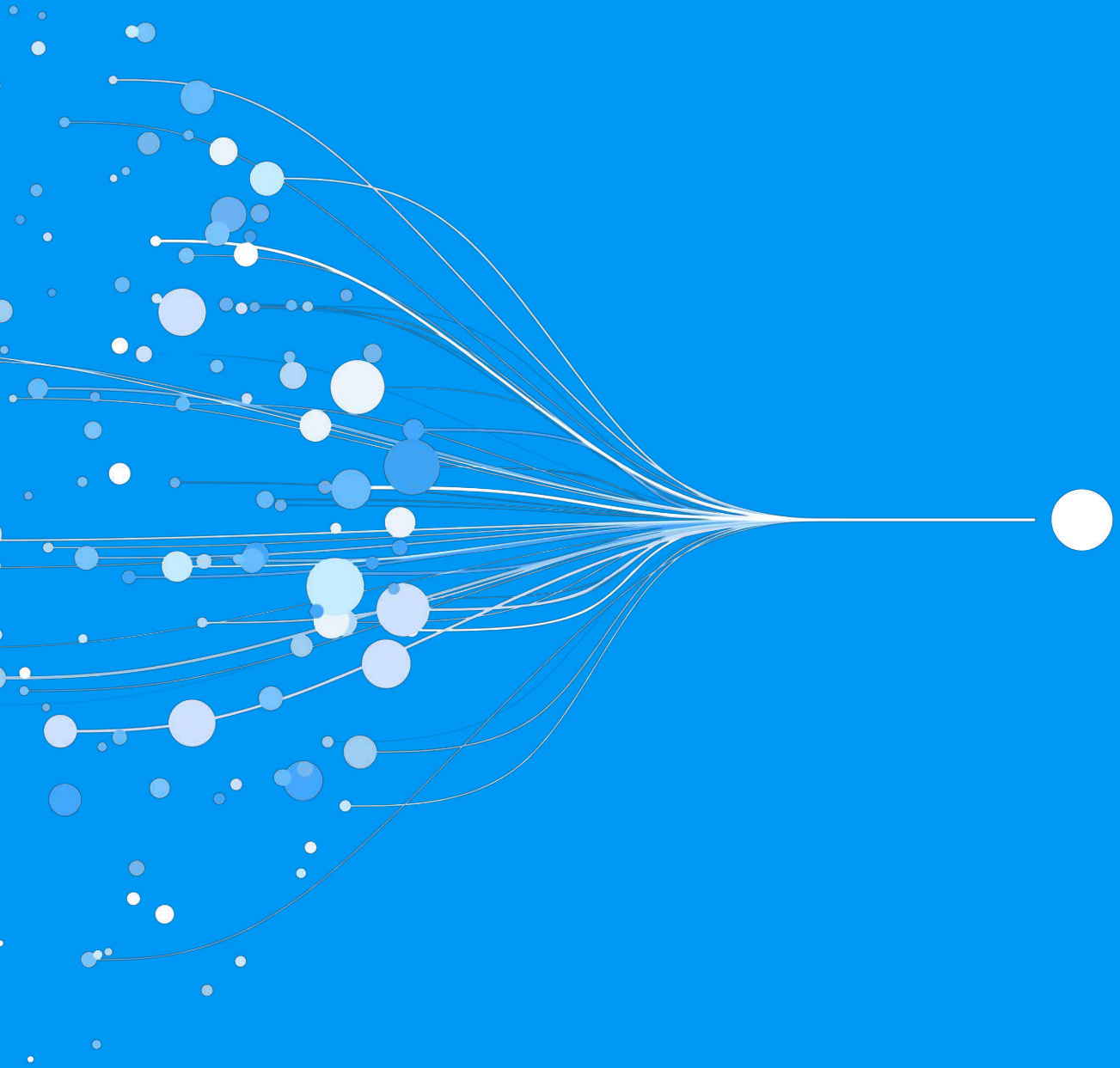
ANALIZUJ

OPTYMALIZUJ

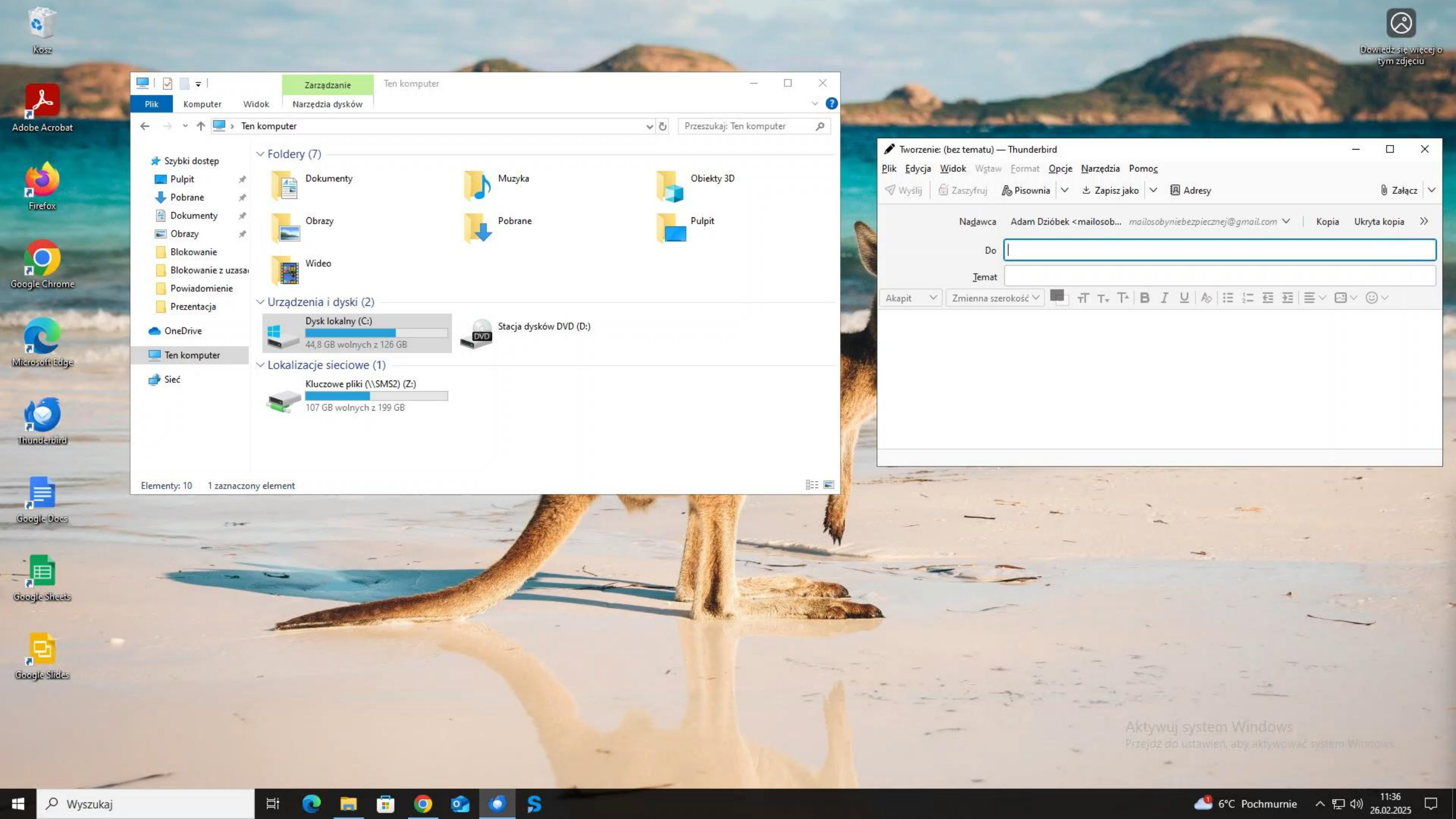
Skalowanie systemu

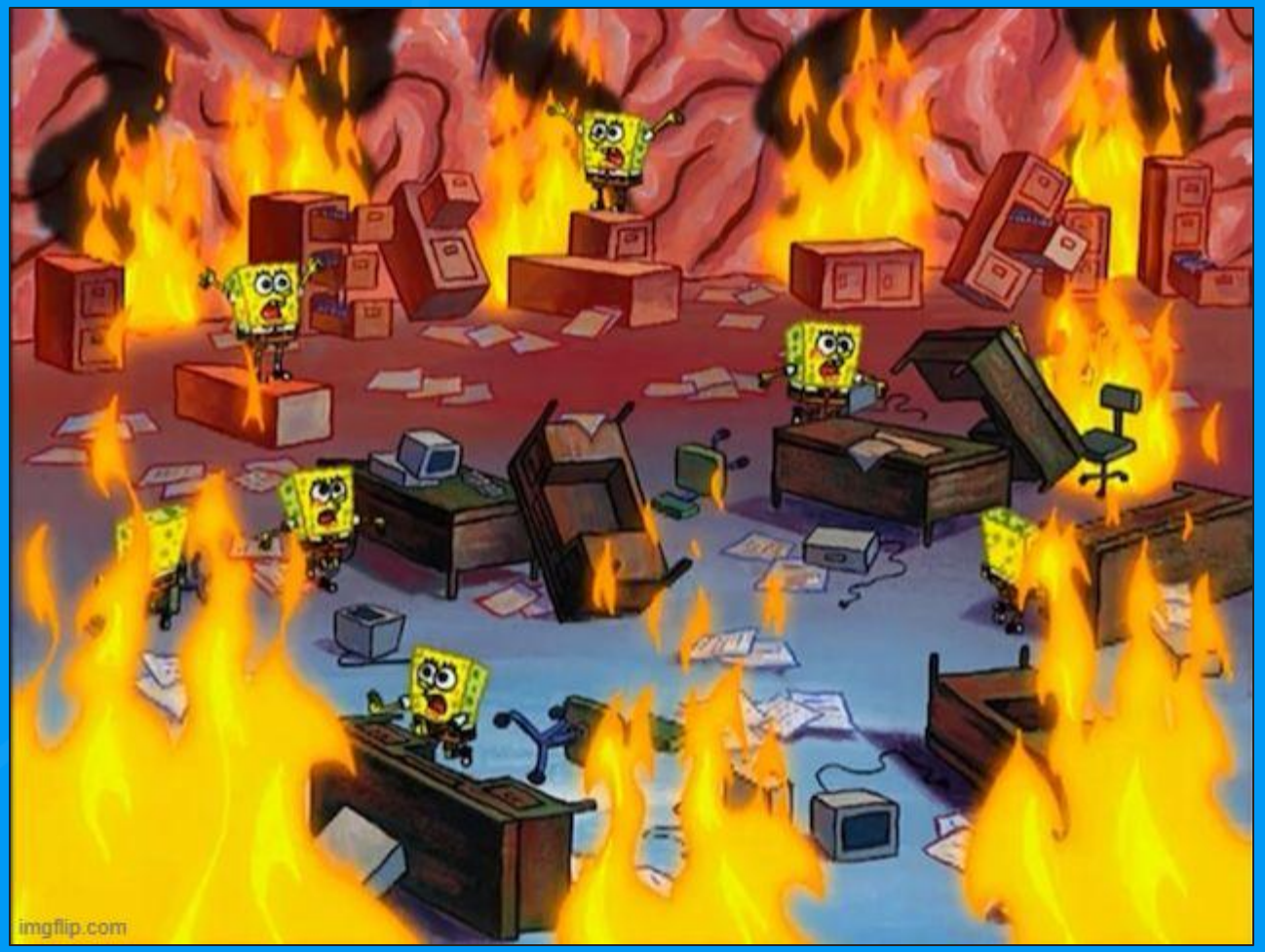


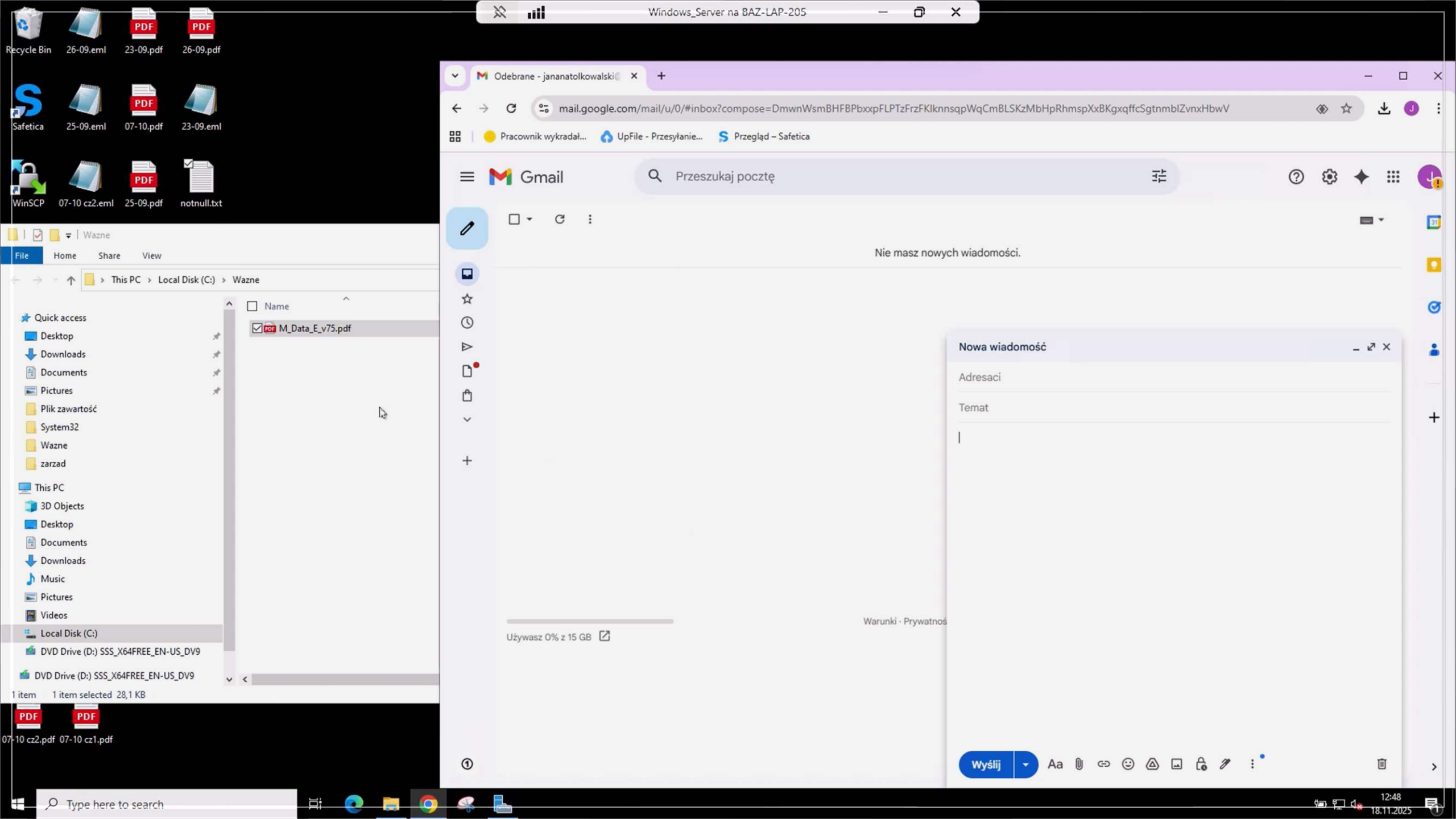

Ochrona danych
z Safetica
KONFIGURUJ
ANALIZUJ
OPTYMALIZUJ



Efekt?

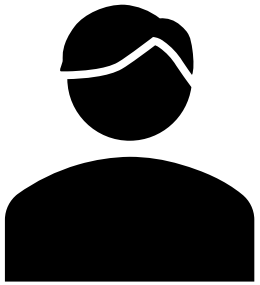

Kosz
Dowiedz się więcej o tym zdjęciu
Adobe Acrobat
Firefox
Google Chrome
Microsoft Edge
Thunderbird
Google Docs
Google Sheets
Google Slides
Zarządzanie
Ten komputer
Plik
Komputer
Widok
Narzędzia dysków
Ten komputer
Przeszukaj: Ten komputer
Szybki dostęp
Pulpit
Pobrane
Dokumenty
Obrazy
Blokowanie
Blokowanie z uzasa
Powiadomienie
Prezentacja
OneDrive
Ten komputer
Sieć
Foldery (7)
Dokumenty
Muzyka
Obiekty 3D
Obrazy
Pobrane
Pulpit
Wideo
Urządzenia i dyski (2)
Dysk lokalny (C:)
44,8 GB wolnych z 126 GB
Stacja dysków DVD (D:)
Lokalizacje sieciowe (1)
Kluczowe pliki (\\SMS2) (Z:)
107 GB wolnych z 199 GB
Elementy: 10
1 zaznaczony element
Tworzenie: (bez tematu) — Thunderbird
Plik
Edycja
Widok
Wstaw
Format
Opcje
Narzędzia
Pomoc
Wyślij
Zaszyfruj
Pisownia
Zapisz jako
Adresy
Załącz
Nadawca
Adam Dzióbek <mailosob...
mailosobyniebezpiecznej@gmail.com
Kopia
Ukryta kopia
Do
Temat
Akapit
Zmienna szerokość
Aktywuj system Windows
Przejdź do ustawień, aby aktywować system Windows.
Wyszukaj
6°C Pochmurnie
11:36
26.02.2025


imgflip.com


Windows_Server na BAZ-LAP-205
Recycle Bin
26-09.eml
23-09.pdf
26-09.pdf
Safetica
25-09.eml
07-10.pdf
23-09.eml
WinSCP
07-10 cz2.eml
25-09.pdf
notnull.txt
Wazne
File
Home
Share
View
This PC
Local Disk (C:)
Wazne
Quick access
Desktop
Downloads
Documents
Pictures
Plik zawartość
System32
Wazne
zarzad
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_X64FREE_EN-US_DV9
Name
M_Data_E_v75.pdf
1 item
1 item selected 28,1 KB
07-10 cz2.pdf
07-10 cz1.pdf
Odebrane - jananatolkowalski
mail.google.com/mail/u/0/#inbox?compose=DmwnWsmBHFBPbxxpFLPTzFrzFKIknnsqpWqCmBLSKzMbHpRhmspXxBKgxqffcSgtnmbIZvnxHbwV
Pracownik wykradał...
UpFile - Przesyłanie...
Przegląd – Safetica
Gmail
Przeszukaj pocztę
Nie masz nowych wiadomości.
Nowa wiadomość
Adresaci
Temat
Wyślij
Używasz 0% z 15 GB
Warunki · Prywatność
Type here to search
12:48
18.11.2025

DAGMA
BEZPIECZEŃSTWO IT

Compliance !



safetica

Zabezpieczenie danych przed wyciekiem

segura®

Zabezpieczenie poświadczeń administracyjnych

DAGMA
BEZPIECZEŃSTWO IT

„...Zyskaliśmy:
•Pełen wgląd w to, co dzieje się z firmowymi danymi
•Inteligentne blokady
•Raporty, które w końcu da się czytać
•Bezpieczeństwo, które się opłaca - lepiej zapobiegać, niż później się tłumaczyć...”

Maciej Lendzioszek
Specjalista ds. IT
BS w Czyżewie

„Jako informatyk, najbardziej w systemie SEGURA cenię to, że raz na zawsze rozwiązuje problem „kto ma dostęp do czego”.

Dwa punkty, które dla mnie wygrywają:

- **Pełna kontrola nad połączeniami**: Dokładnie widzę, co robią firmy zewnętrzne na naszych serwerach.
- **Koniec z rozdawaniem haseł**: I to jest hit. Ludzie z zewnątrz łączą się z naszymi systemami, ale w ogóle nie znają do nich haseł.

Krótko mówiąc: SEGURA to mniej stresu dla mnie i wyższy poziom bezpieczeństwa dla Banku.”

Michał Wierzbicki
Informatyk
BS Siedlce

Mateusz Piątek
Safetica I Holm Security I Segura
piatek.m@dagma.pl
+48 532 570 255