

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



Cyberbezpieczeństwo jest jak...



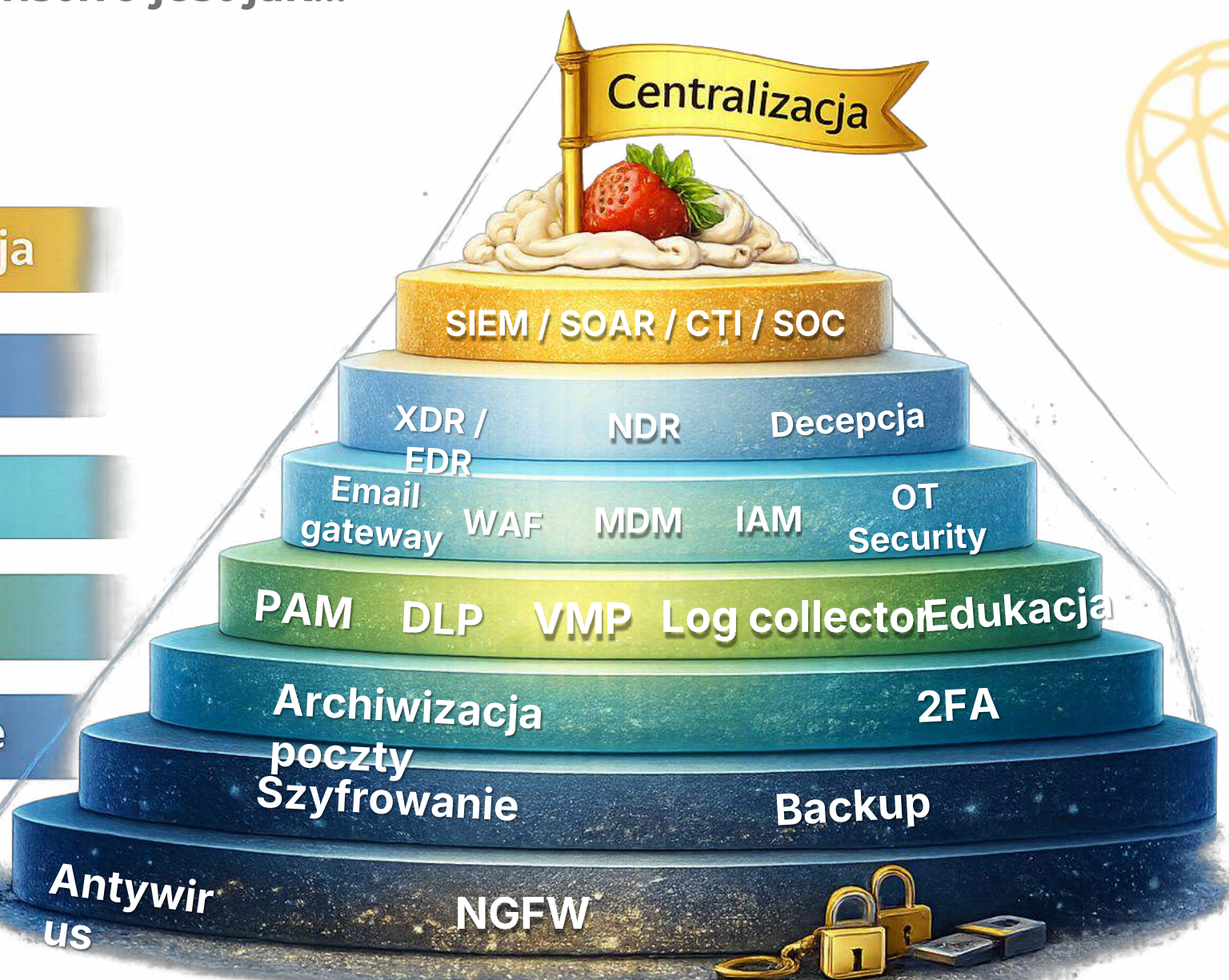
Centralizacja

Detekcyjne

Swoiste

Compliance

Podstawowe



Tymczasem cyberbezpieczeństwo historycznie...



NOD32, v.1.51
Some di
Version 1.50 a
NOD32.
COMPANY

NETAS
Secure Internet

wirt
P O

Rejestracja |
AIK

serwisy

S E R W I S
KAPITAŁOWY

F I R M Y

ENCYKLOPEDIA

WIADOMOŚCI

P O G O D A

B Ó L G Ł O W Y

D L A D Z I E C I

Polecamy

Quick links
Products
Services
Register your L
Partner area

Technology

Konferencja 3E
Ustrój emerytalny

Forum Wirtualnej
Polski

Księga Gości

Netscape

Glossary | Site map

ARCHIWUM

Archiwum

www.gazeta.pl

gazeta
WYBORCZA

ARCHIWUM PRENUMERATA OGŁOSZENIA

Dymisja Wąsacza

Premier żąda raportu o komputeryzacji ZUS. Po naszej publikacji prezes Janusz Wojciechowski przyznaje, że kontrola trwa za długo. Bierze winę na siebie i... zaprasza dziennikarzy na posiedzenie NIK

Prezes NIK Janusz Wojciechowski
Fot. Jacek Marczewski

Wczoraj wieczorem premier zwrócił się do marszałka Sejmu o "spowodowanie pilnego sporządzenia raportu w sprawie przebiegu komputeryzacji ZUS". Wyraził "zaniepokojenie faktem, że pomimo upływu roku od sporządzenia kontroli przez NIK, raport nie został przedstawiony. (...) nie pozostało to bez wpływu na funkcjonowanie ZUS i wywołało poważne konsekwencje dla budżetu państwa". | > |

Wtorek
BABICKI WOLNY, ALE NIE CAŁKIEM
Władze rosyjskie wypuściły dziś rano z aresztu korespondenta radia "Swoboda" Andrieja Babickiego. Wczoraj za jego uwolnieniem opowiedział się m.in. Władimir Putin. Babicki ma jednak nakaz pozostania w Moskwie.

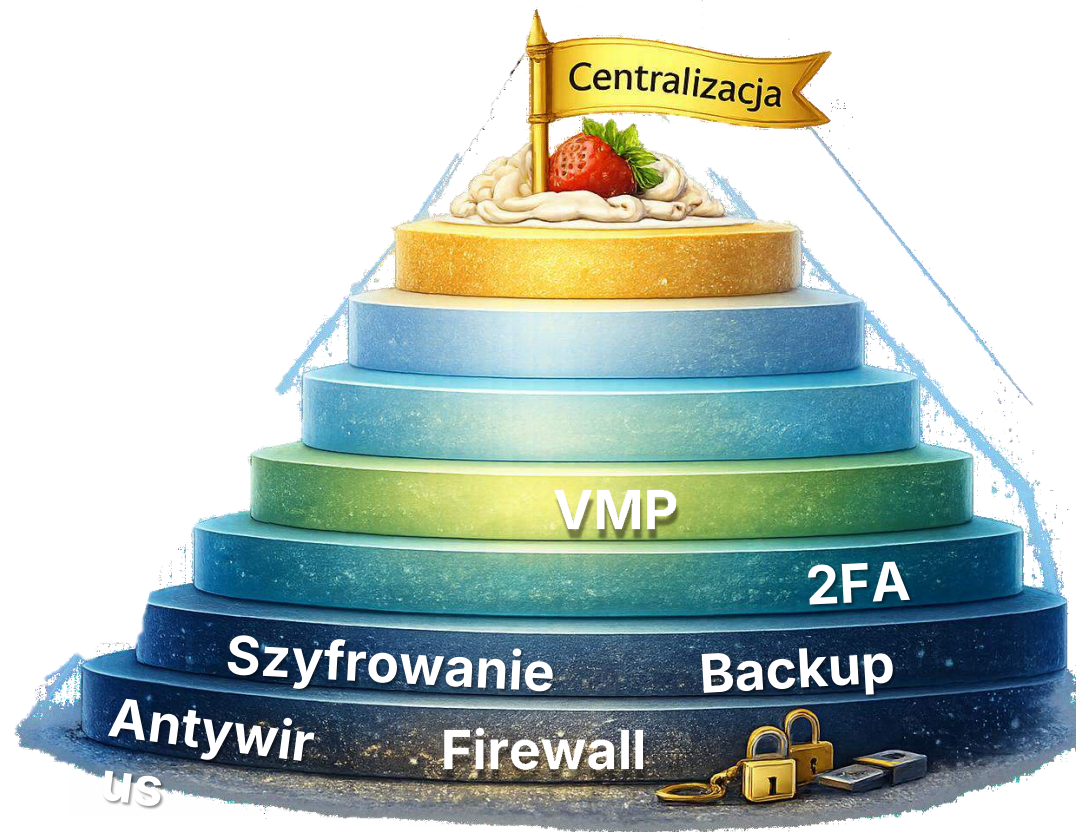
DYMISJA HAIDERA
Joerg Haider zrezygnował wczoraj niespodziewanie ze stanowiska przewodniczącego skrajnie prawicowej Partii Wolności. | > |

WERSJA WALENDZIAKA
Dębski zapowiadał "wietrzenie archiwów UKFiT i antykomunistyczne porządki". Nie

Trader.pl-duzo drobnych ogłoszen!

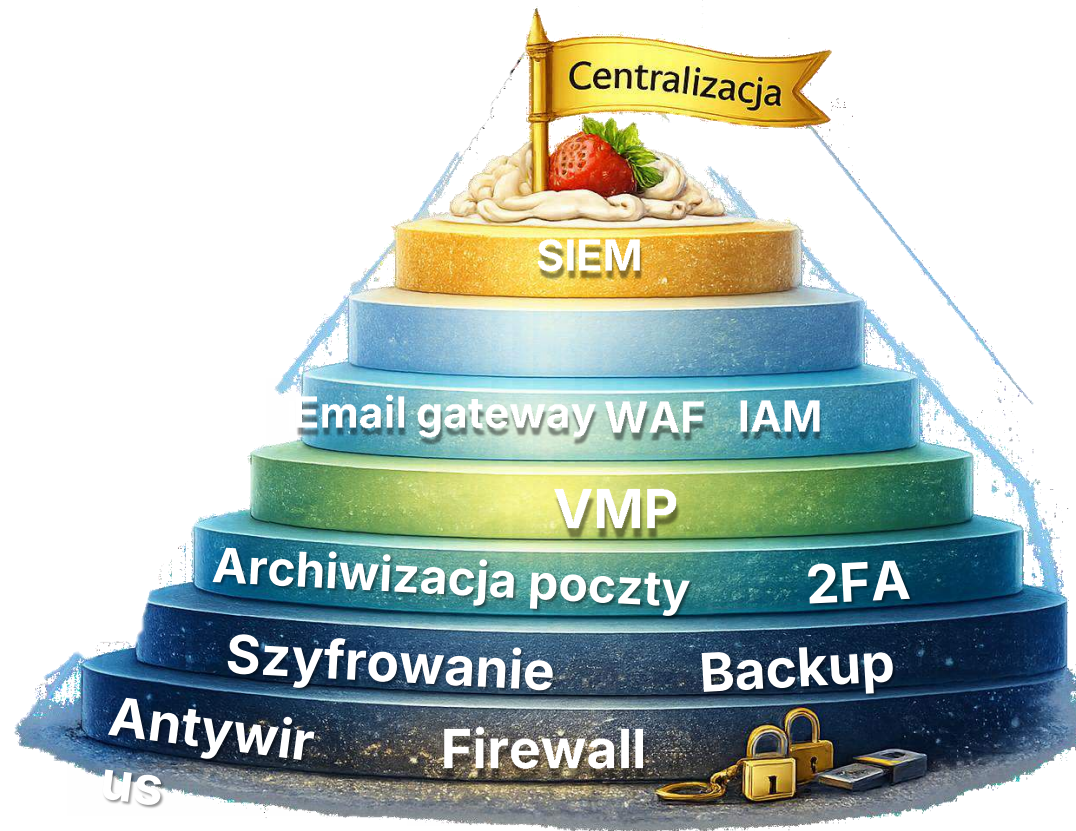
Tymczasem cyberbezpieczeństwo historycznie...

...1999



Tymczasem cyberbezpieczeństwo historycznie...

...2005



Tymczasem cyberbezpieczeństwo historycznie...

...2010



Tymczasem cyberbezpieczeństwo historycznie...

...DZIŚ



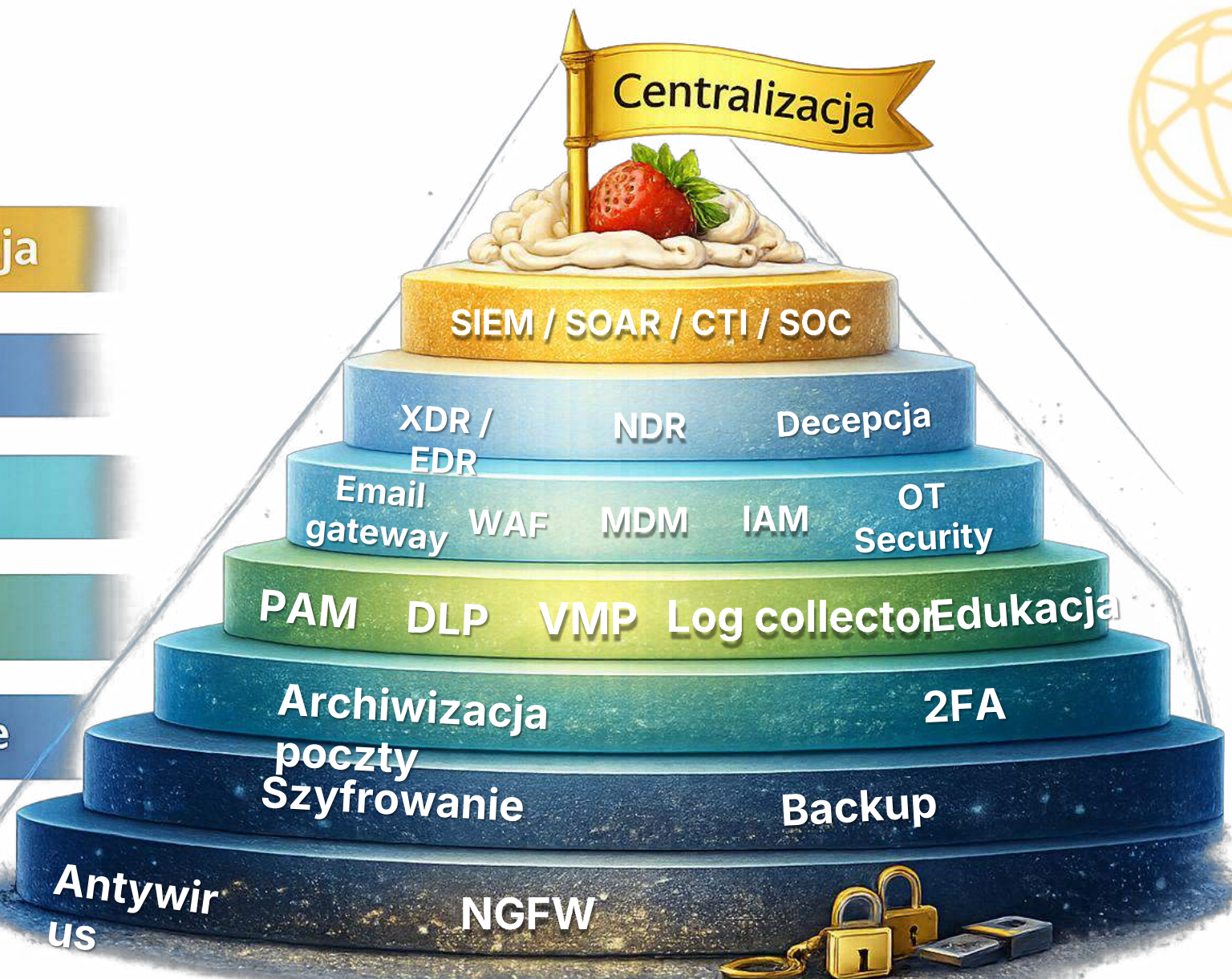
Centralizacja

Detekcyjne

Swoiste

Compliance

Podstawowe



Compliance !



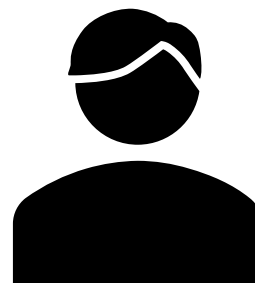
DLP - DATA LEAK
PREVENTION

safetica

PAM - PRIVILEGE ACCES
MANAGEMENT

 segura®

Compliance !



safetica

Zabezpieczenie danych
przed wyciekiem

 **segura**[®]

Zabezpieczenie
poświadczeń
administracyjnych



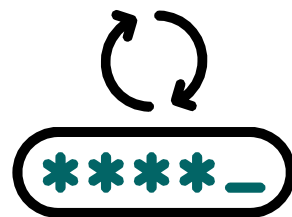


Rozwiązanie klasy PAM do zarządzania dostępami
uprzywilejowanymi

Co łączy każdy atak hackerski?



Co łączy (prawie) każdy atak hakerski?



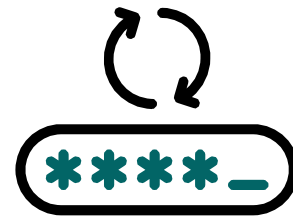
Poświadczenia administratora

=

RYZYO I PROBLEM

A co jeśli...

...administrator nie zna poświadczeń?



Poświadczenia administratora

=

RYZYO I PROBLEM

Dostęp bez hasła ?!

Rozwiązanie klasy PAM

Privilage

Access

Management



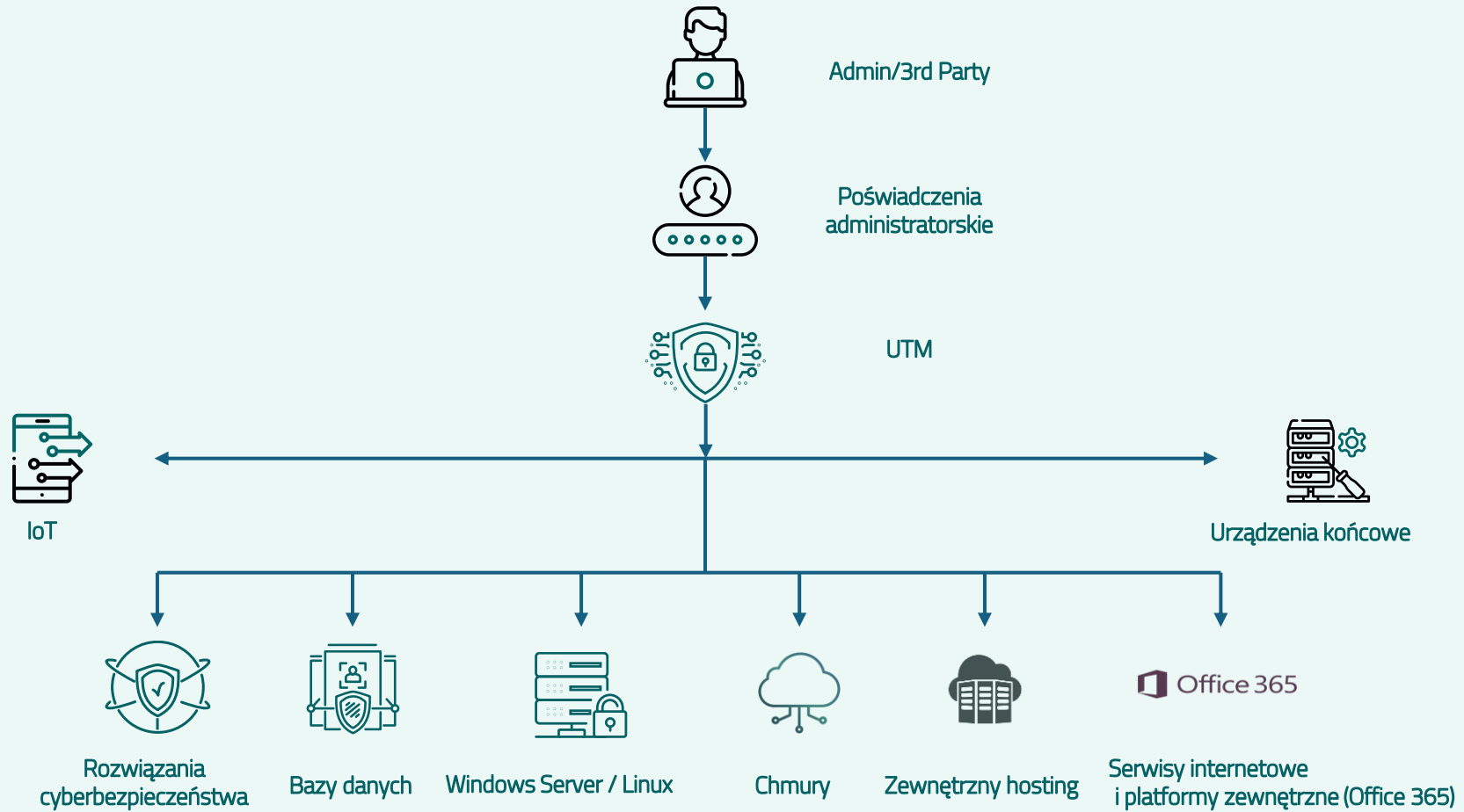
Na czym opierają się założenia PAM?

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.

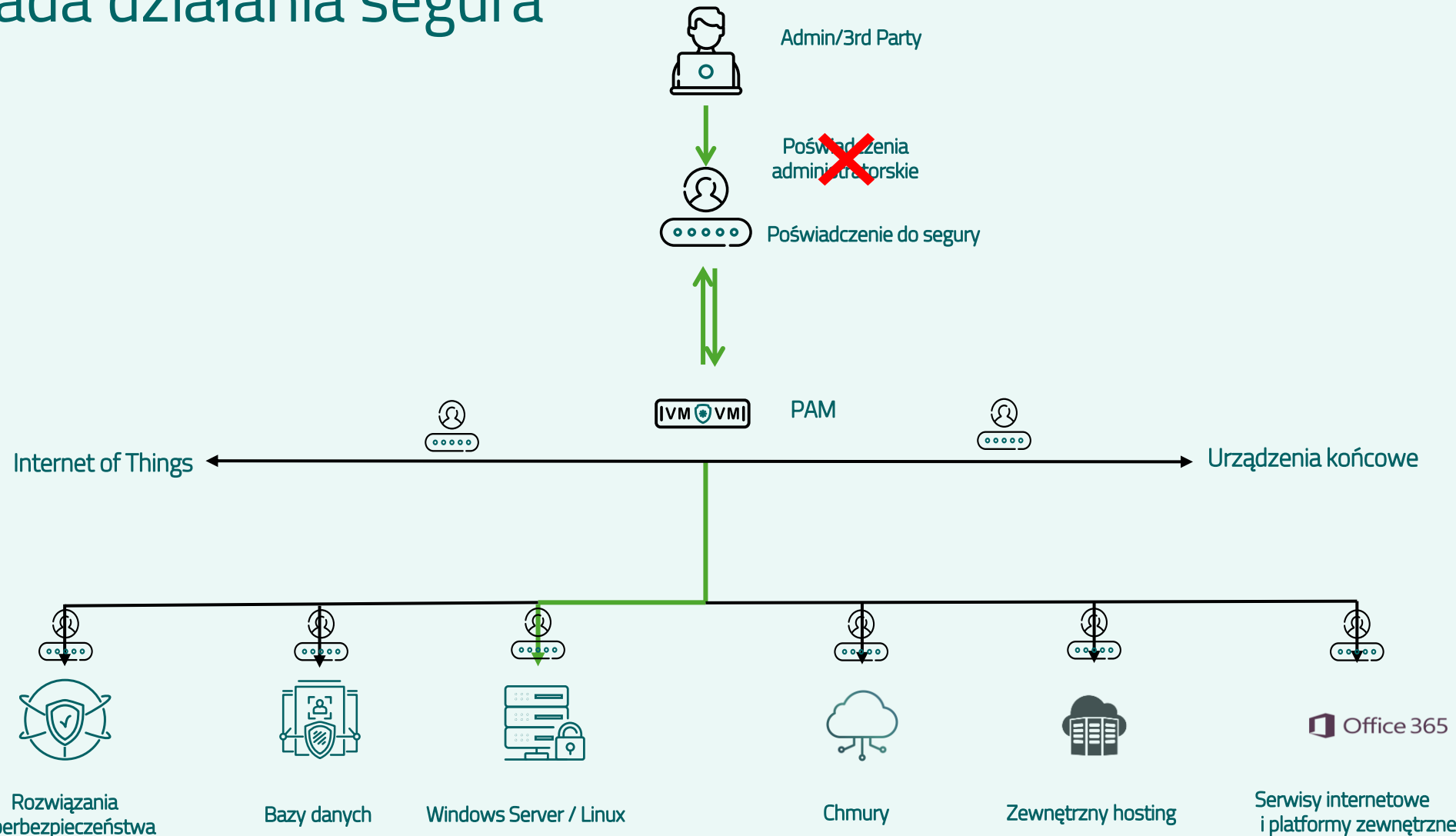
Zasada działania segura



Zasada działania segura



Zasada działania segura



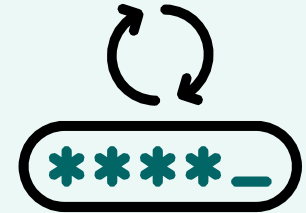
Co zyskujemy?



Mitygacja ryzyka pozyskania
poświadczeń administratorskich
podczas ataku



Mitygacja ryzyka
związanego z 3rd
party



Mitygacja ryzyka
„backdoor”

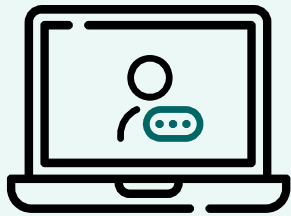


Zwiększenie zgodności z
compliance



Oszczędności i wygoda

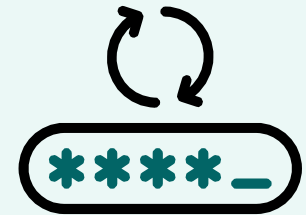
W jaki sposób?



Zarządzanie dostępem



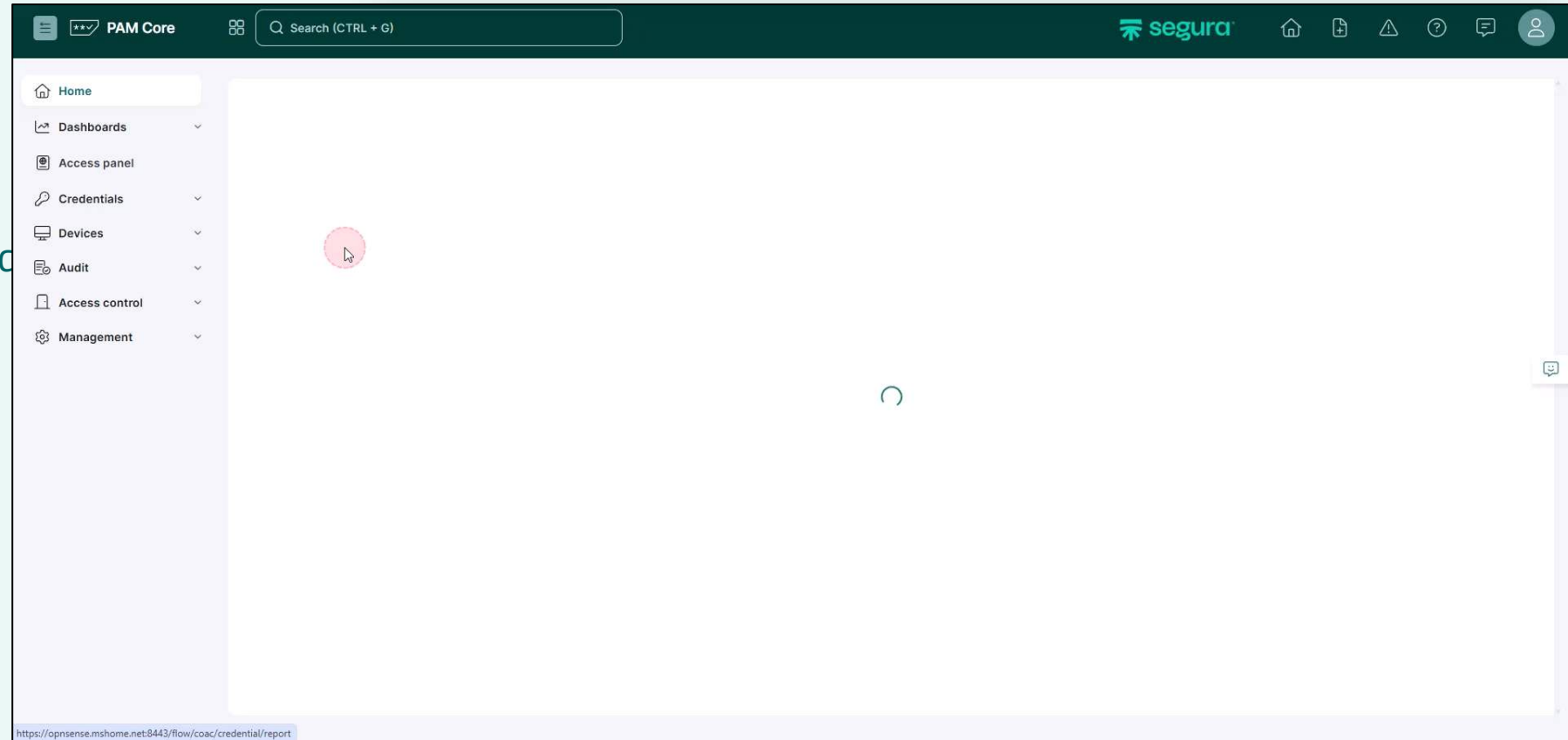
Zarządzanie sesją



Zarządzanie hasłami

Zarządzanie dostępem

- Zdefiniowanie zakresu
- Określenie kiedy może mieć dostęp
- Przypisywanie użytkowników do 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)

Command	Criticality	Type	Session type	Action during session	Occurrences	Score	Enabled
Session logs							
Search term: reboot <input type="button" value="Q Search"/>							
03/18/2025 10:06 AM	03/18/2025 10:07 AM	80	Łukasz Krysiak 192.168.200.201 ssh	10.0.30.100 administrator	03/18/2025 10:06:50		input
ps<BackSpace>asswd<Return>							
03/18/2025 10:06 AM	03/18/2025 10:07 AM	80	Łukasz Krysiak 192.168.200.201 ssh	10.0.30.100 administrator	03/18/2025 10:06:58		output
d							
=====							
Auditing command. Please wait...							
=====							
03/18/2025 10:06 AM	03/18/2025 10:07 AM	80	Łukasz Krysiak 192.168.200.201 ssh	10.0.30.100 administrator	03/18/2025 10:07:02		output
This command is blocked.							
administrator@10.0.30.100 /home/administrator\$							

Zarządzanie sesją (aktywne)

The screenshot displays the 'PAM Core' web interface for managing active sessions. The page title is 'Poświadczenia, urządzenia i informacja'. The main content area is titled 'Poświadczenia dostępu' and features a table of active sessions with various filters and a table of session details.

Filters:

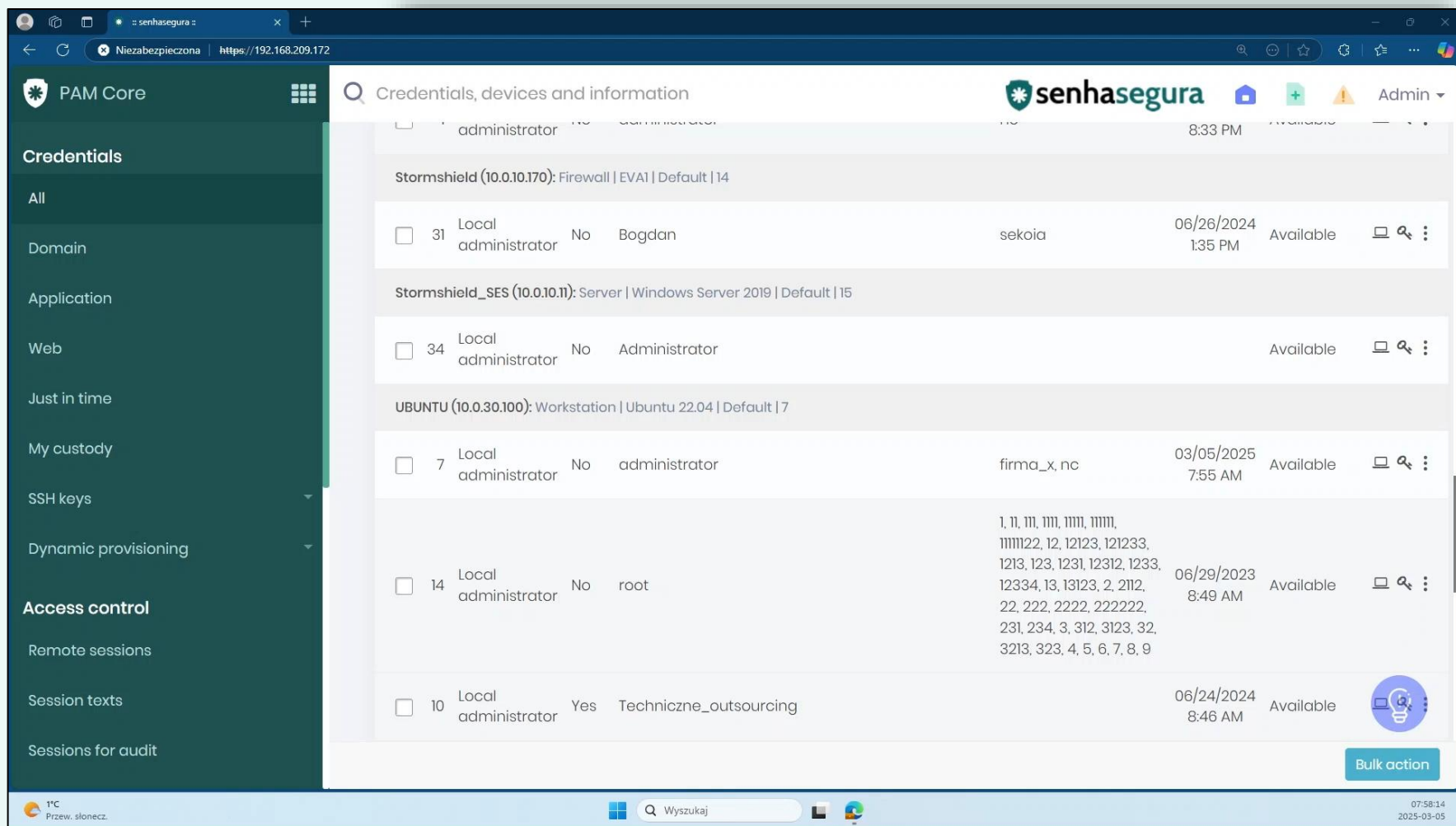
- Urządzenie: [Dropdown]
- Nazwa użytkownika: [Dropdown]
- Rodzaj poświadczenia: [Dropdown]
- Just in time (JIT): [Dropdown]
- Dodatkowe informacje: [Dropdown]
- Rodzaj urządzenia: [Dropdown]
- Produkt: [Dropdown]
- Producent: [Dropdown]
- Domena: [Dropdown]
- Iskaza: [Dropdown]
- Tyło połączenia: [Dropdown]
- Tagi poświadczeń: [Dropdown]
- Tagi urządzeń: [Dropdown]
- Identyfikator: [Text]
- Status: [Dropdown]
- Używaną od: [Text]
- Data do: [Text]
- Hasło wygenerowane: [Dropdown]
- Wyświetl: [Button]
- Wyczyść: [Button]

Table of Active Sessions:

ID	Rodzaj	Just in time (JIT)	Nazwa użytkownika	Dodatkowe informacje	Domena	Tagi	Ostatni podgląd hasła	Status sesji	Operacje
185.163.85.65 (185.163.85.65)	Web Application								
13	Local administrator	Nie	piotekm@diagma.pl					W toku	[Icons]
oaliefas.internat (10.0.10.10): Server Windows Server 2022 Default 3									
4	Local administrator	Nie	Administrator		oaliefas.internat	uprawnienia_admina	24.07.2024 15:05	Dostępna	[Icons]
10	Local User	Nie	piotekm@diagma.pl			administrator_sofet.co		W toku	[Icons]
LAP01 (0.0.10.10): Workstation Windows 10 Default 0									
6	Domain user	Nie	jankowalski		oaliefas.internat	administrator_sofet.co, uprawnienia_zywyke		Dostępna	[Icons]
LAP02 (0.0.10.12): Workstation Windows 10 Default 7									
7	Domain user	Nie	jankowalski		oaliefas.internat	uprawnienia_zywyke		Dostępna	[Icons]
LAP03 (0.0.10.13): Workstation Windows 10 Default 8									
8	Domain user	Nie	mianika@uper		oaliefas.internat	uprawnienia_zywyke		Dostępna	[Icons]
Router (10.0.10.1): Router OPNsense Default 10									
17	Local administrator	Nie	root		oaliefas.internat			Dostępna	[Icons]

Zarządzanie hasłami

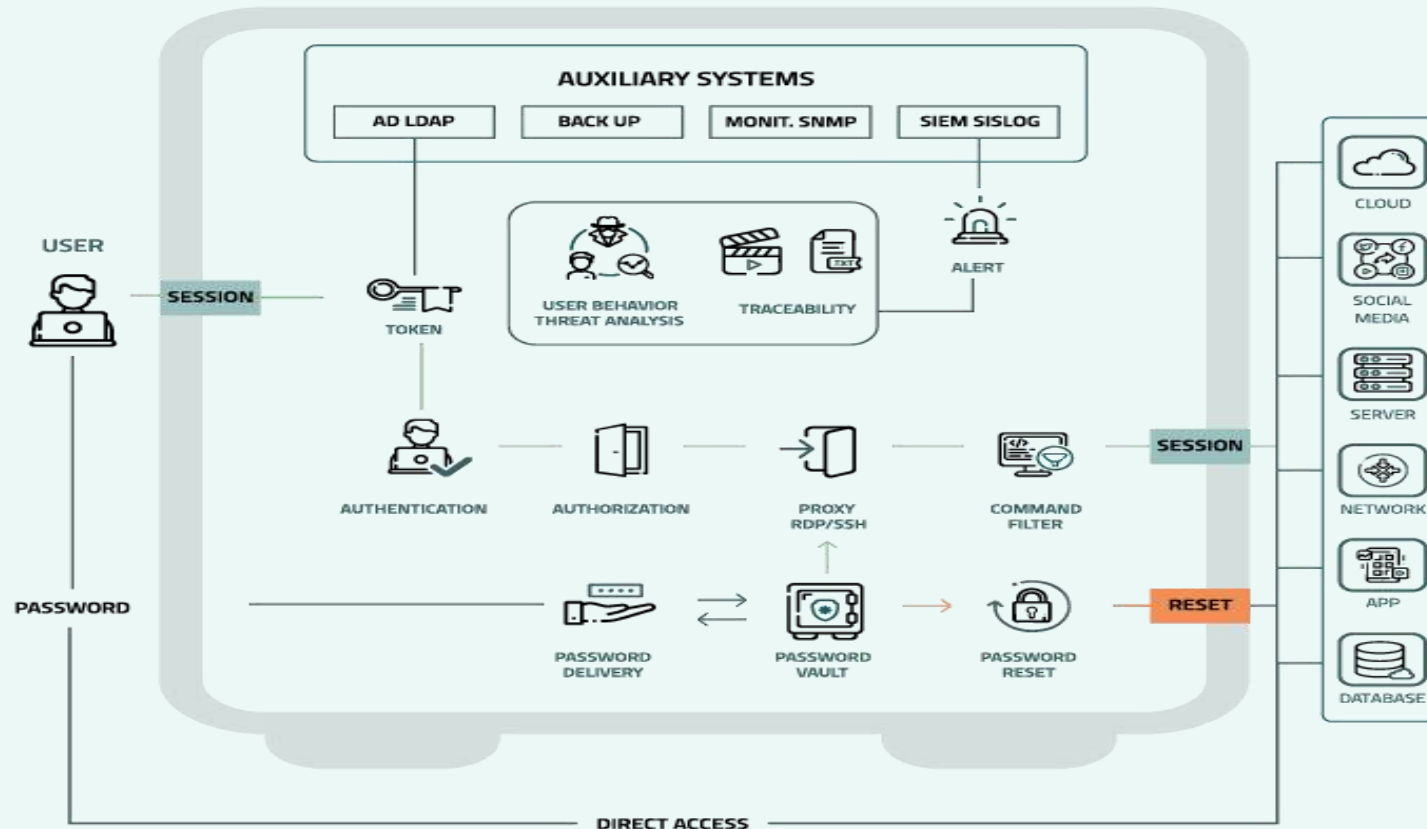
- Hasła paranoiczne
- Hasła rotujące
- Odpowiedzialność za hasła
- Obsługa kluczy SSH
- Obsługa 2FA
- Przechowywanie haseł w zaszyfrowanej architekturze



The screenshot displays the PAM Core web interface. The left sidebar shows navigation options: Credentials (All, Domain, Application, Web, Just in time, My custody, SSH keys, Dynamic provisioning), Access control (Remote sessions, Session texts, Sessions for audit), and a search bar. The main content area shows a list of credentials under the heading 'Credentials, devices and information'. The list includes entries for Stormshield (10.0.10.170), Stormshield_SES (10.0.10.11), and UBUNTU (10.0.30.100). Each entry shows details like ID, name, type, status, and last update. A 'Bulk action' button is visible at the bottom right.

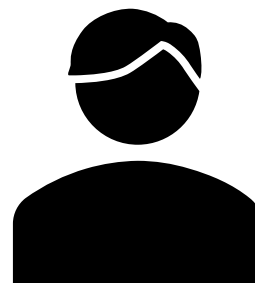
ID	Name	Type	Status	Last Update	Availability
31	Local administrator	No	Bogdan	06/26/2024 1:35 PM	Available
34	Local administrator	No	Administrator		Available
7	Local administrator	No	administrator	03/05/2025 7:55 AM	Available
14	Local administrator	No	root	06/29/2023 8:49 AM	Available
10	Local administrator	Yes	Techniczne_outsourcing	06/24/2024 8:46 AM	Available

Jaki efekt otrzymamy?





Compliance !



safetica

Zabezpieczenie danych
przed wyciekiem

 **segura**[®]

Zabezpieczenie
poświadczeń
administracyjnych



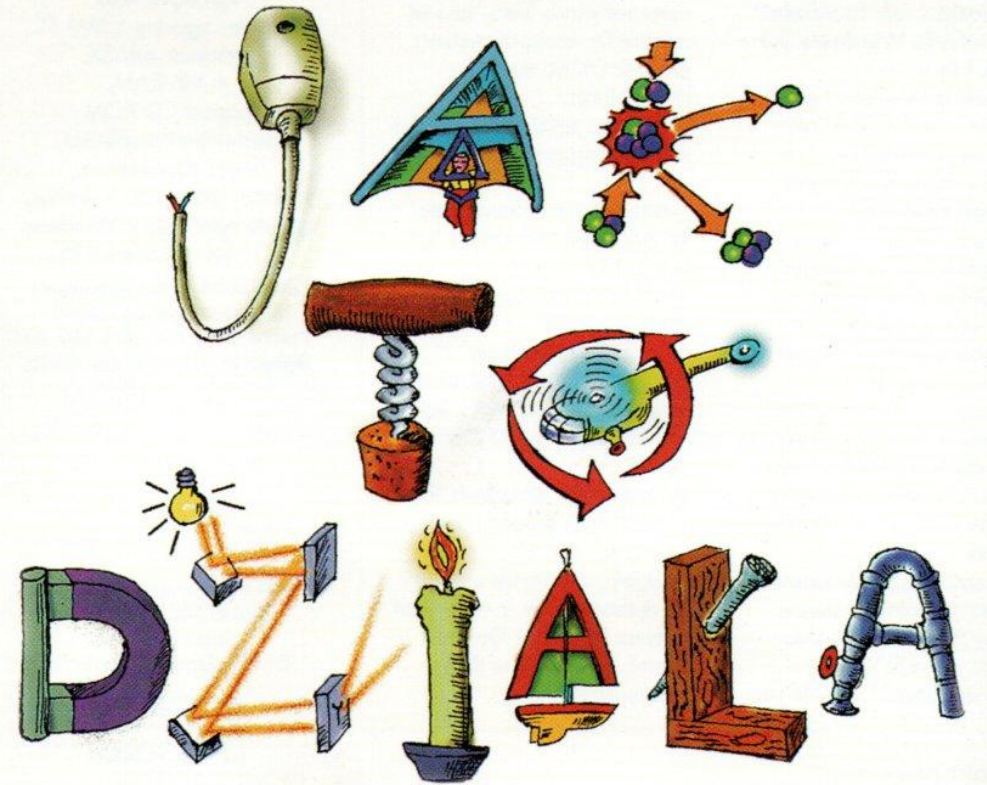
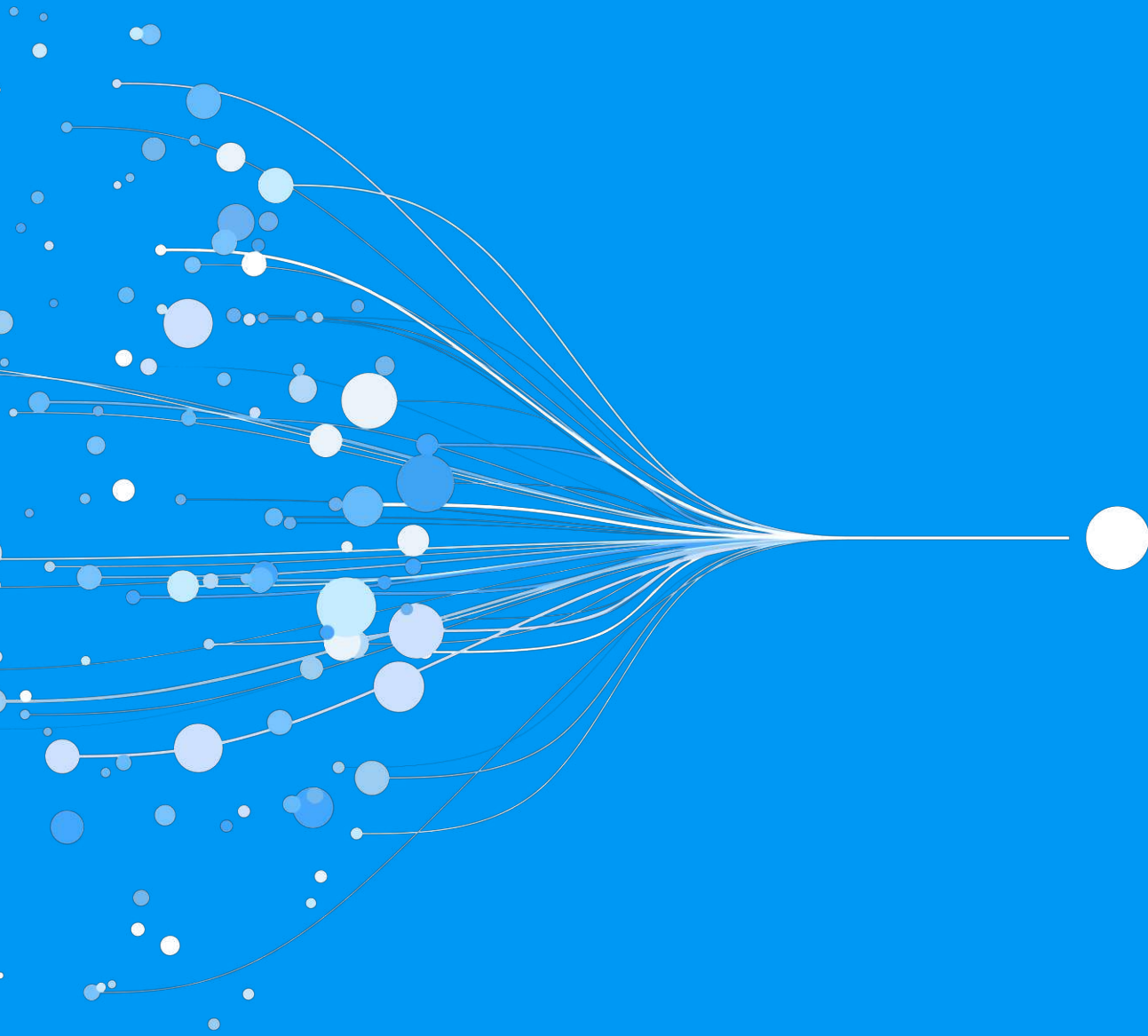
A world map composed of a grid of small dots in light gray. Overlaid on the map are several small icons: a yellow circle with a crosshair in the North Atlantic, a blue 'S' in the North Pacific, and a green star in the South Atlantic.

safetica

Rozwiązanie klasy DLP do zabezpieczania danych

Rozwiązanie klasy DLP do zabezpieczania danych

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



FASCYNUJĄCY PRZEWODNIK po magicznym świecie DLP

MULTIMEDIA

Jak działa Safetica?

Ochrona danych
z Safetica

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

KONFIGURUJ

ANALIZUJ

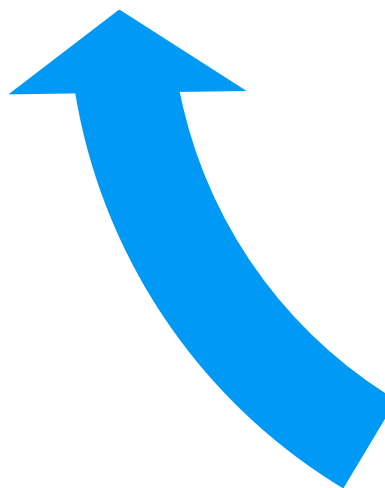
OPTYMALIZUJ

Dodatkowe
integracje

Klasyfikacja
danych

S

Określenie
poziomu
uprawnień



Klasyfikacja danych

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Dane osobowe

Dane z CRM

Know-How

Informacje z serwera plików

Dane już sklasyfikowane

Dane z systemu kadrowo-płacowego

Dane pochodzące z aplikacji

KONFIGURUJ

Zawartość

**Klasyfikacja
danych**

Pliki zaszyfrowane

**Źródło
pochodzenia**

PESEL

ANALIZUJ

**Ręczna
klasyfikacja**

Numer karty kredytowej

**Zewnętrzne
klasyfikatory**

Numer dowodu osobistego

Słowa kluczowe

OPTYMALIZUJ

Typ pliku

Regex

**Automatyczna
klasyfikacja (AI)***

...itd.

Klasyfikacja danych

KONFIGURUJ

Zawartość

Źródło pochodzenia

ANALIZUJ

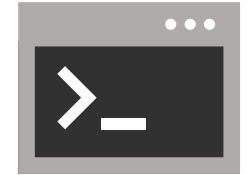
Ręczna klasyfikacja

Zewnętrzne klasyfikatory

OPTYMALIZUJ

Typ pliku

Automatyczna klasyfikacja (AI)*



Aplikacje
(po kategoriach)



Foldery
(Sieciowe lub lokalne)



Strony www
(Po domenach lub URL)

* Tylko w wersji

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Zawartość

Źródło
pochodzenia

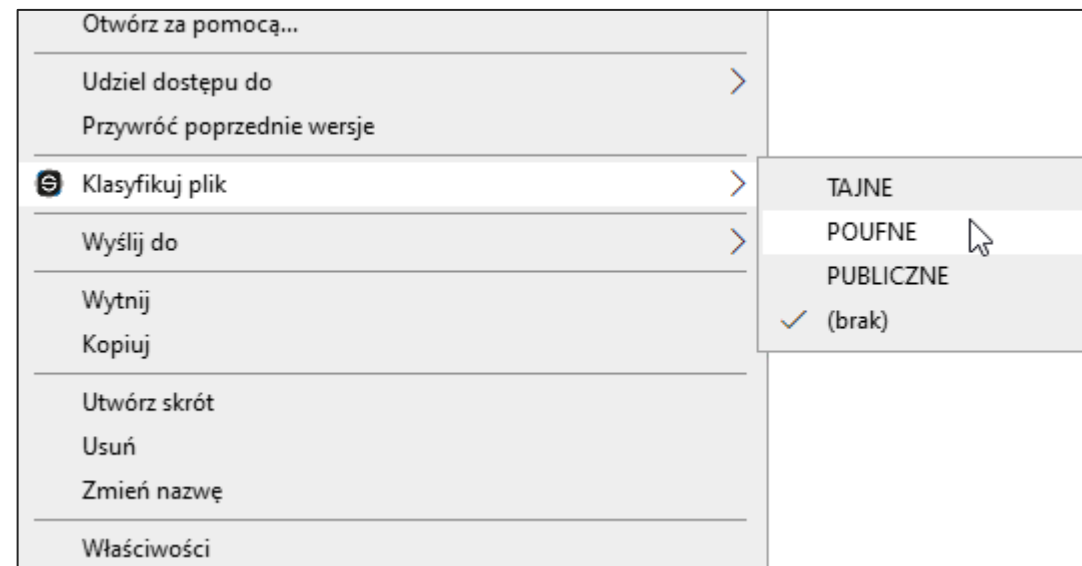
Ręczna
klasyfikacja

Zewnętrzne
klasyfikatory

Typ pliku

Automatyczna
klasyfikacja (AI)*

Klasyfikacja danych



KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Zawartość

Źródło
pochodzenia

Ręczna
klasyfikacja

Zewnętrzne
klasyfikatory

Typ pliku

Automatyczna
klasyfikacja (AI)*

Klasyfikacja danych

SECLORE

netwrix

TITUS

 **GREENmod**
SYSTEM DO KLASYFIKACJI PLIKÓW I POCZTY ELEKTRONICZNEJ



* Tylko w wersji

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Zawartość

Źródło
pochodzenia

Ręczna
klasyfikacja

Zewnętrzne
klasyfikatory

Typ pliku

Automatyczna
klasyfikacja (AI)*

Klasyfikacja
danych

.pdf

.xlsx

.dng

.txt

.dwg

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Zawartość

Źródło
pochodzenia

Ręczna
klasyfikacja

Zewnętrzne
klasyfikatory

Typ pliku

Automatyczna
klasyfikacja (AI)*

Klasyfikacja danych

Plik	Klasyfikacja danych	Urządzenie
Pracownicy.txt	Wykrywanie wstępne +2	S11CLOUD
Kolo ratunkowe na wypowiedzeniu.txt	Osobowe DDZ Wy +3	DESKTOP-JS6T005
Test Risk Management.txt	Wykrywanie wstępne Wykryto reguły klasyfikacji: • Wykrywanie peseli i DO (31x)	DESKTOP-K2ADG5N
Test RM2.txt		DESKTOP-K2ADG5N
gay-precision.txt	Wykrywanie wstępne +2	W10P-2
gay-fixed.txt	Wykrywanie wstępne Dane wrażliwe Dane wrażliwe PL	
Zrzut ekranu 2025-06-13 141147.png	Wykrywanie wstępne +2	S11CLOUD
Lista klientów.txt	Dyski Chmurowe +3	S11CLOUD
Lista klientów (1).txt	Dyski Chmurowe +3	S11CLOUD

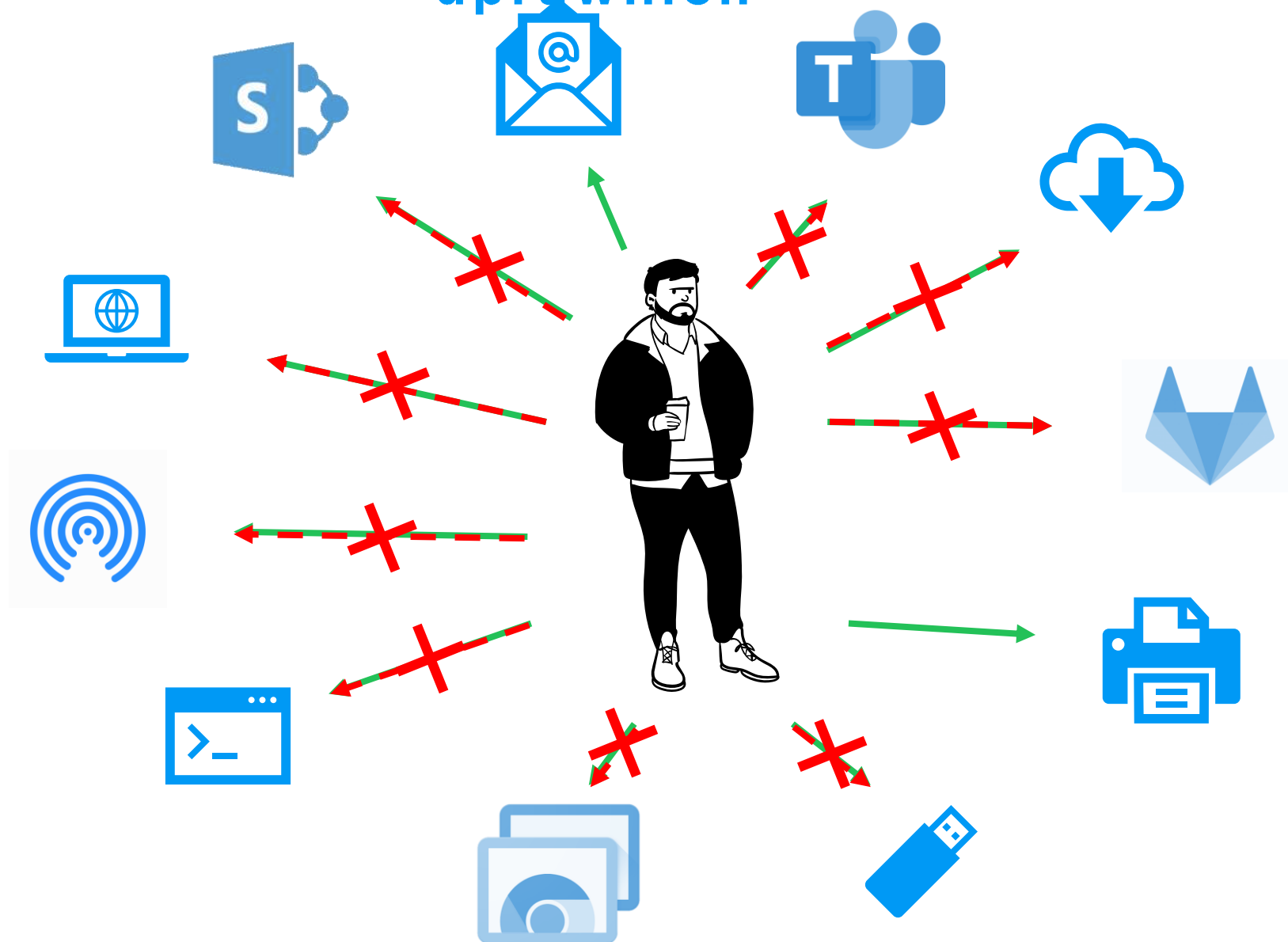
* Tylko w wersji

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

Określenie poziomu uprawnień



Dodatkowe integracje

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ



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

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

Wysłanie CV do Grażynki z działu HR

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

Wysłanie kartoteki pacjenta na prywatny mail

4h Program CRM

3h Facebook.com

program kadrowo-płacowy

Pobranie .exe z torrenty.org

Kopiowanie pliku z folderu „wrażliwe dane”

Przesłanie pliku na firmową stronę

Edycja pliku .docx

Wejście na stronę Salesforce.com

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

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

Przesłanie pliku na firmową stronę

Kopiowanie pliku z folderu „wrażliwe dane”

Audyt Bezpieczeństwa

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

Wysłanie kartoteki pacjenta na prywatny mail

Podłączenie Pendrive służbowego

4h Program CRM

3h Facebook.com

program kadrowo-płacowy

Edycja pliku .docx

Pobranie .exe z torrenty.org

Monitorowanie aktywności + Raportowanie

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

safetica

AUDYT BEZPIECZEŃSTWA



Ochrona danych
z Safetica

KONFIGURUJ

ANALIZUJ

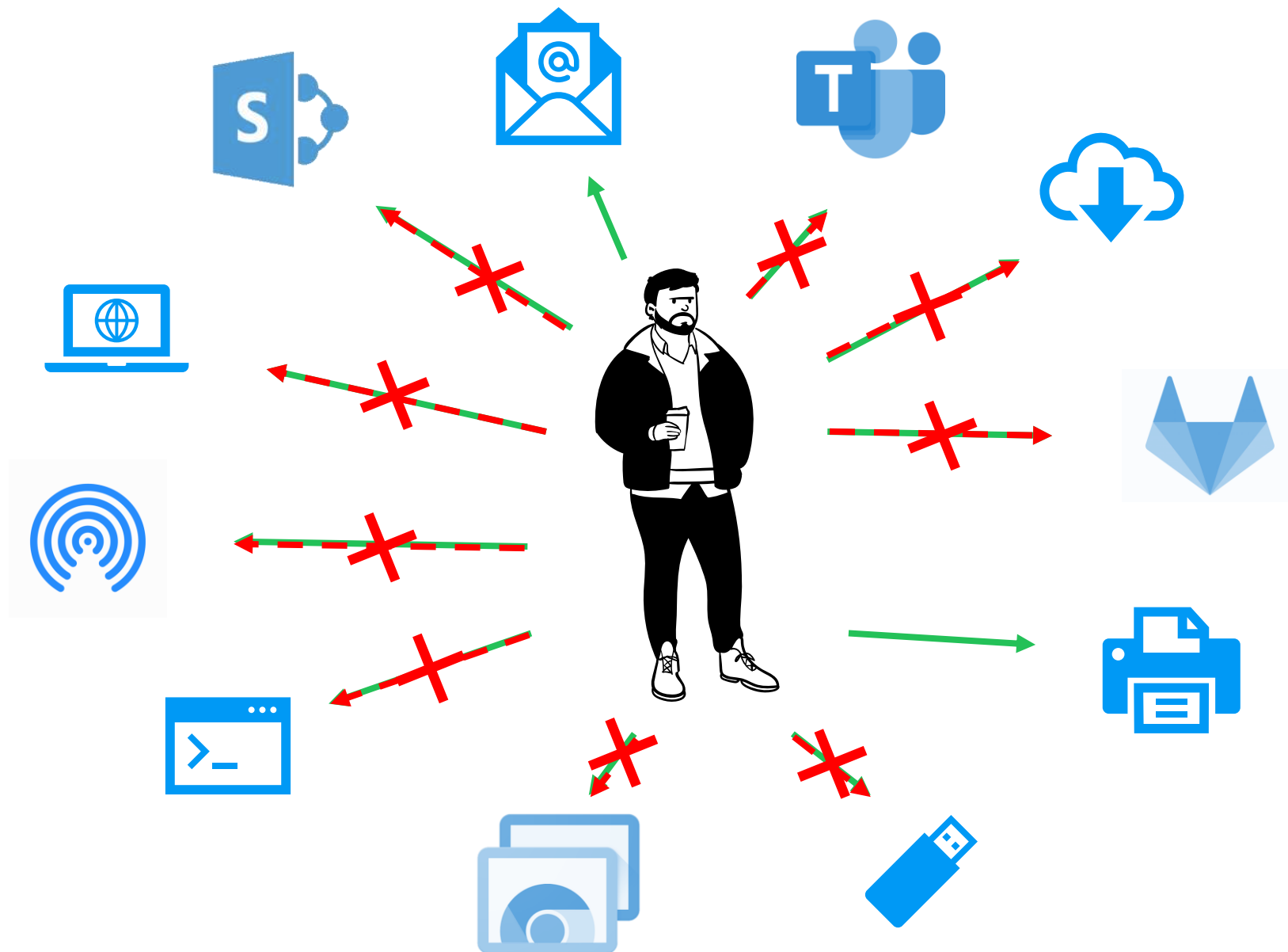
OPTYMALIZUJ

Skalowanie systemu

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ

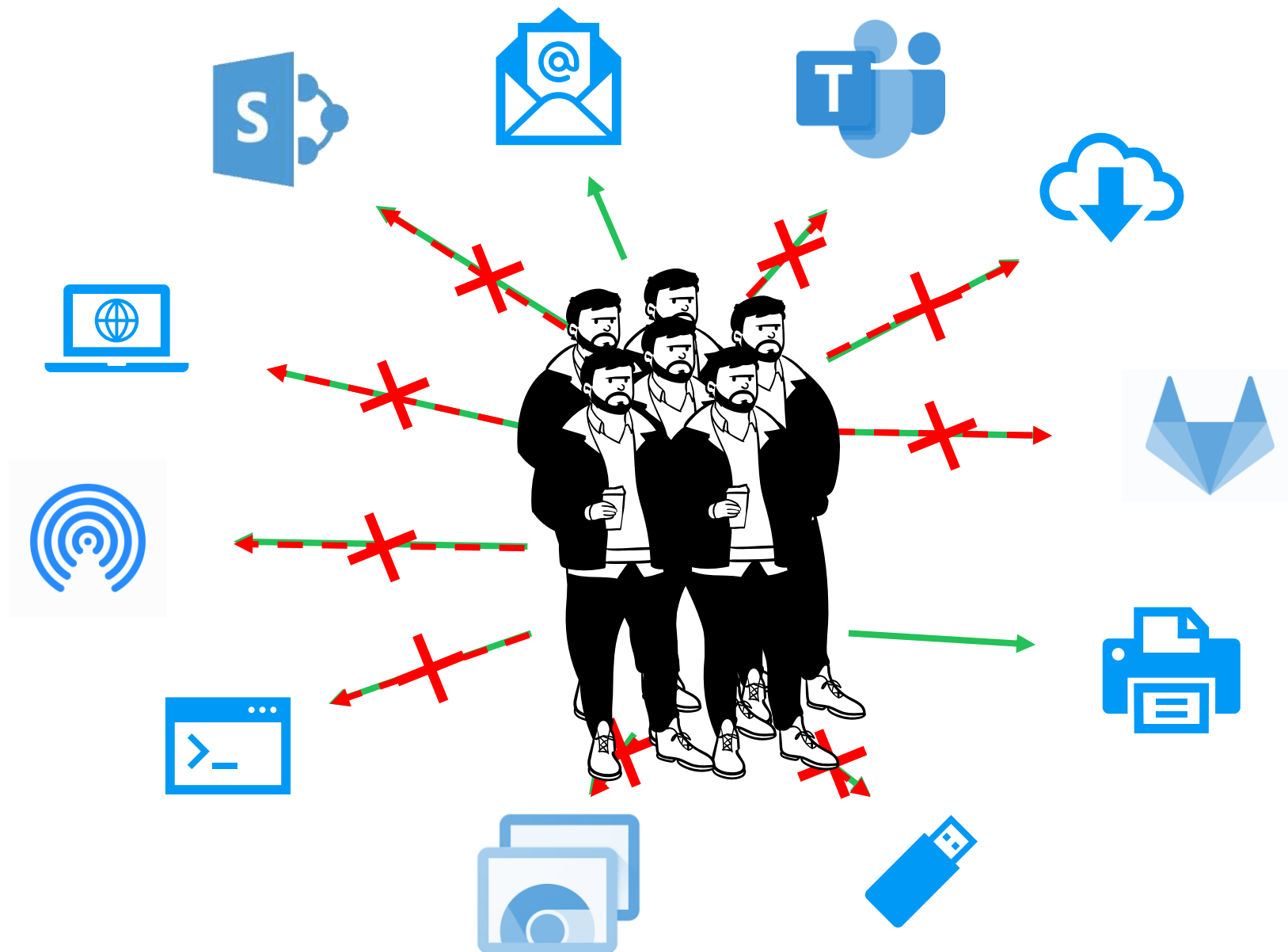


Skalowanie systemu

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ



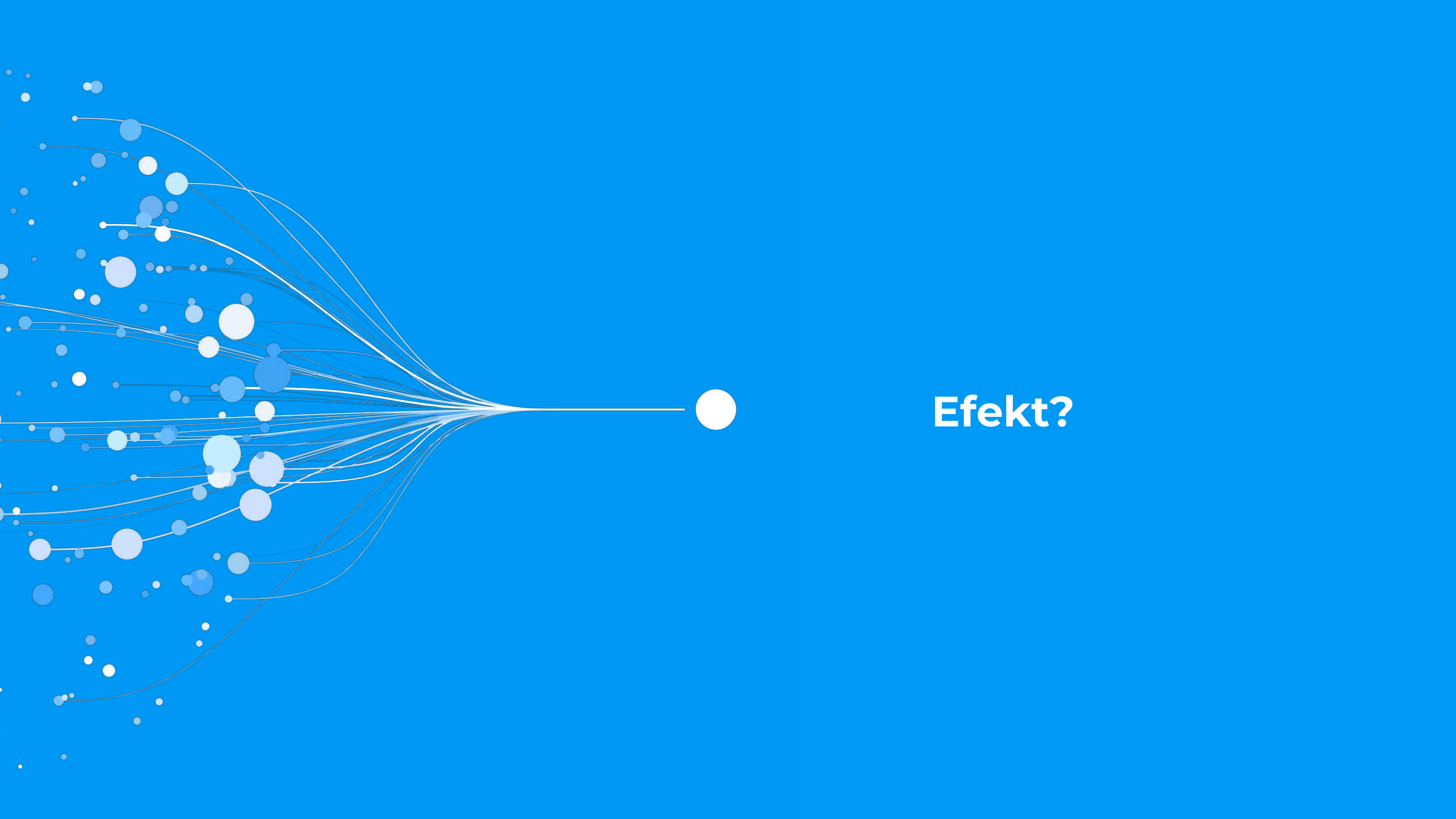


Ochrona danych
z Safetica

KONFIGURUJ

ANALIZUJ

OPTYMALIZUJ



Efekt?



Dowiedz się więcej o tym zdjęciu

Ten komputer

Przeszukaj: Ten komputer

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

Do:

Temat:

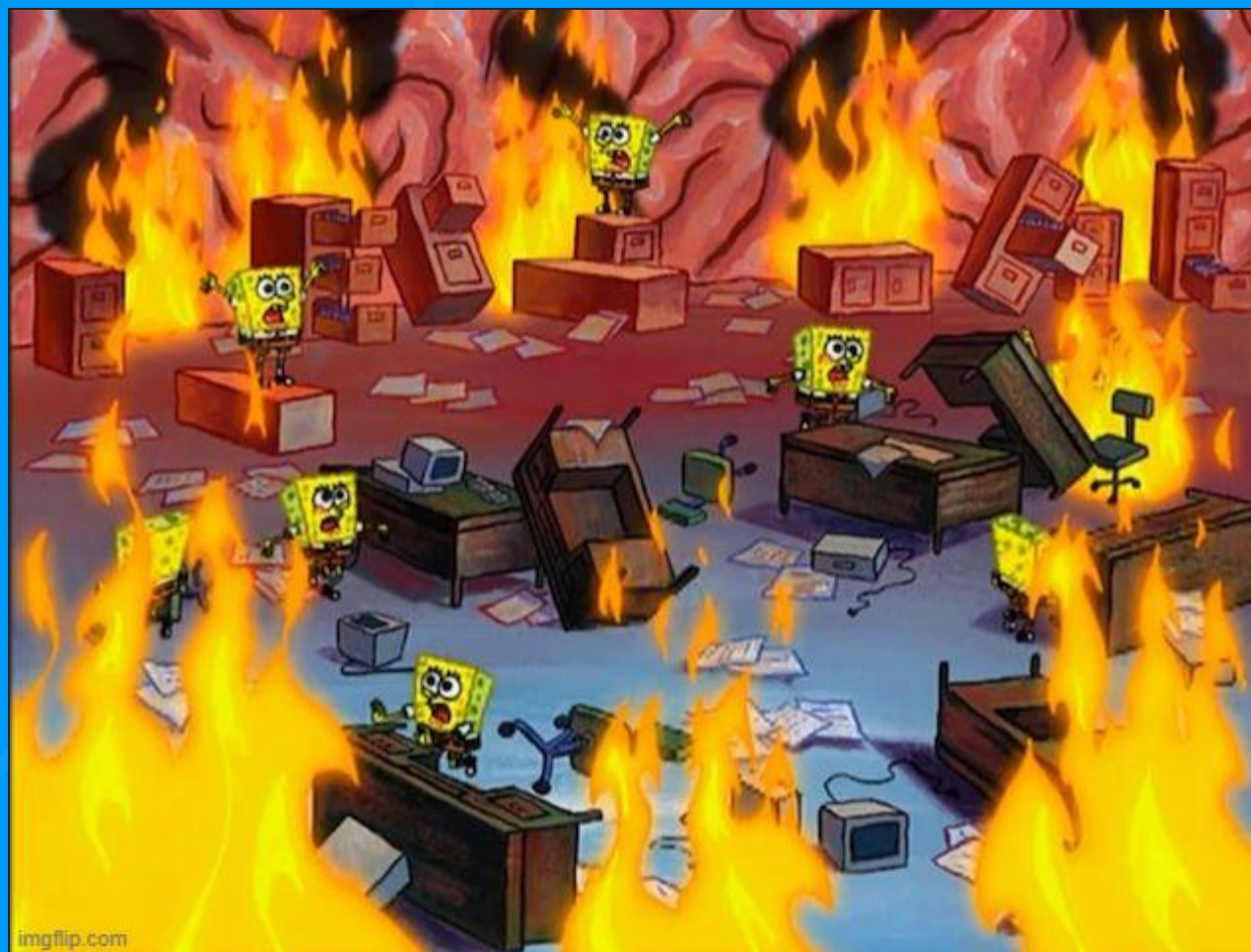
Wyślij Zszyfruj Pisownia Zapisz jako Adresy Załącz

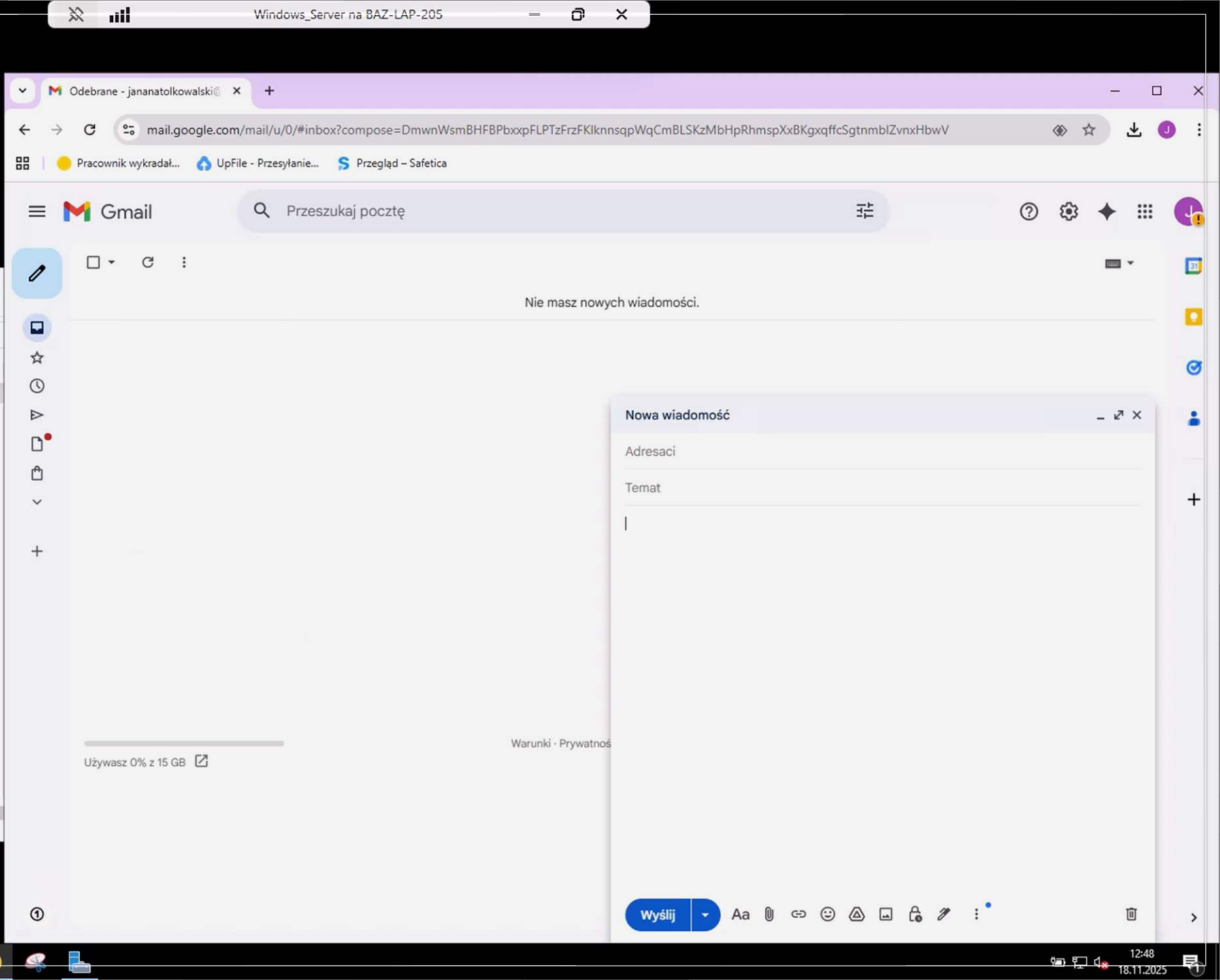
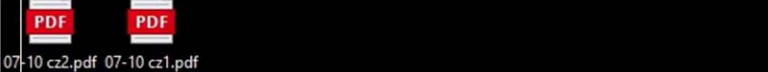
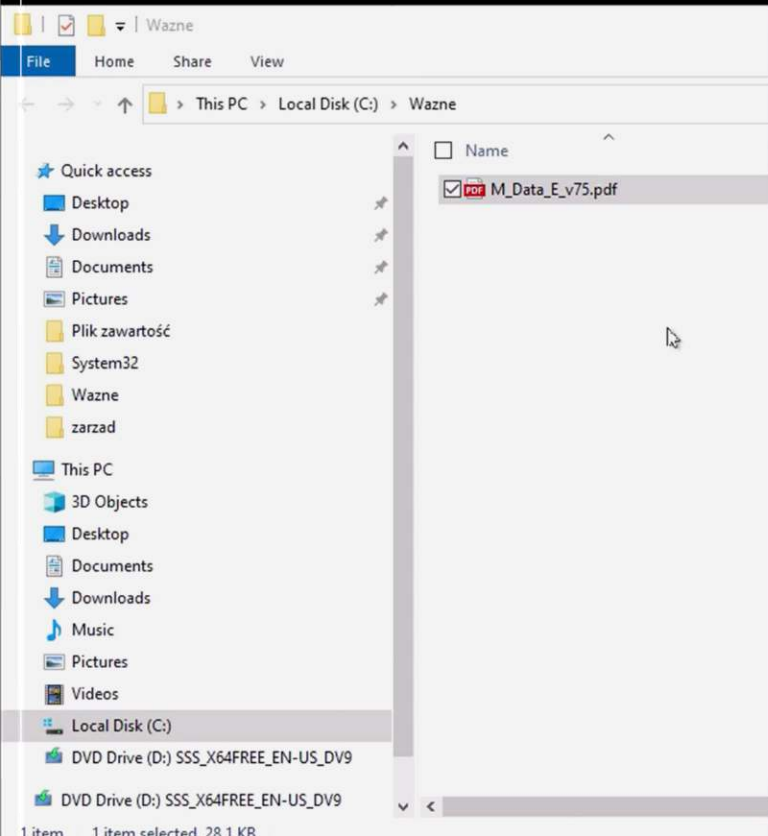
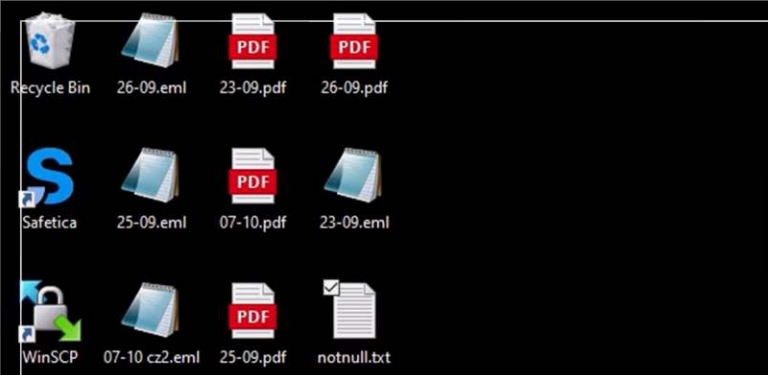
Nagawka Adam Dzióbek <mailosob... mailosoby niebezpiecznej@gmail.com> | Kopia Ukryta kopia

Akapit Zmienna szerokość

B I U

Aktywuj system Windows
Przejdź do ustawień, aby aktywować system Windows.

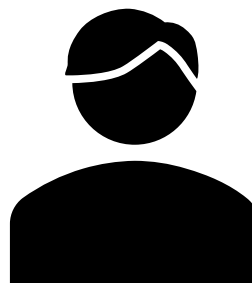






safetica

Compliance !



safetica

Zabezpieczenie danych
przed wyciekiem

 **segura**[®]

Zabezpieczenie
poświadczeń
administracyjnych



„...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



Mateusz Piątek

Safetica | Holm Security | Segura

piatek.m@dagma.pl

+48 532 570 255

„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