

SOLID CYBER

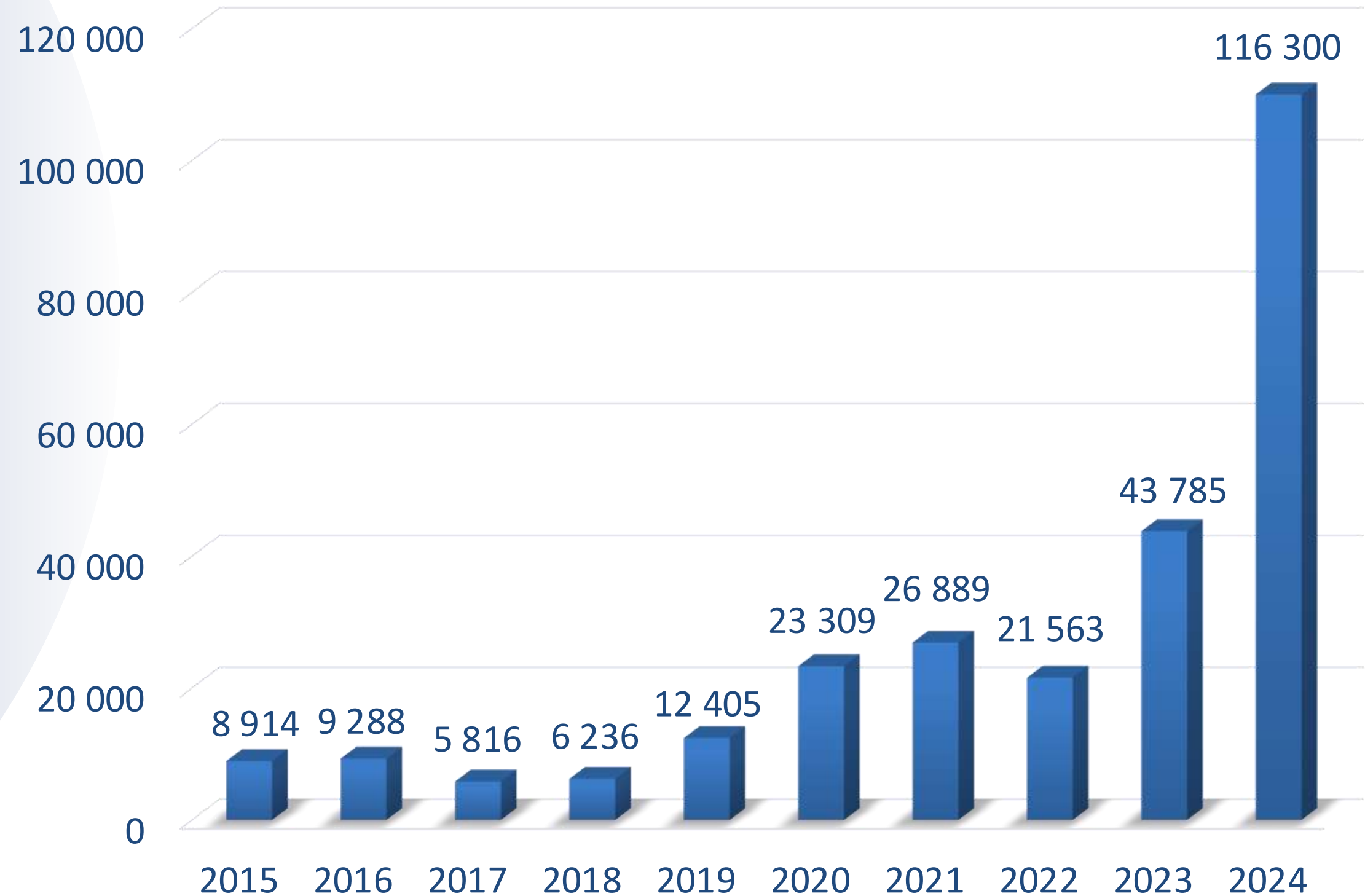
NIS2: kara dla zarządu, konsekwencje dla
biznesu – jak zabezpieczyć się już dziś?

www.solidcyber.pl



CYBERBEZPIECZEŃSTWO W LICZBACH

DANE CSIRT





~~Czy firma padnie ofiarą ataku?~~

->

Kiedy firma padnie ofiarą ataku?

KLUCZOWE REGULACJE PRAWNE

- DYREKTYWA **NIS2**
- USTAWA O KRAJOWYM SYSTEMIE
CYBERBEZPIECZEŃSTWA (**KSC**)



Których sektorów dotyczy NIS2

Dyrektywa NIS2 dotyczy firm, które działają w **sektorach o wysokim stopniu krytyczności**. Są to:

- energia
- energia elektryczna, w tym systemy produkcji, dystrybucji i przesyłu oraz punkty ładowania
- ciepłownictwo i chłodnictwo
- ropa naftowa, w tym rurociągi produkcyjne, magazynowe i przesyłowe
- gaz, w tym systemy dostaw, dystrybucji i przesyłu oraz magazynowanie
- wodór
- transport lotniczy, kolejowy, wodny i drogowy
- infrastruktura bankowa i rynku finansowego, jak instytucje kredytowe, operatorzy systemów obrotu i partnerzy centralni
- zdrowie, w tym podmioty świadczące opiekę zdrowotną, producenci podstawowych produktów farmaceutycznych i wyrobów medycznych o krytycznym znaczeniu oraz laboratoria referencyjne UE
- woda pitna
- ścieki
- infrastruktura cyfrowa, w tym dostawcy usług centrów danych, usług przetwarzania w chmurze, publicznych sieci łączności elektronicznej i publicznie dostępnych usług łączności elektronicznej
- usługi zarządzane przez TIK (między przedsiębiorstwami)
- przestrzeń.

NIS2 dotyczy również innych sektorów krytycznych, takich jak:

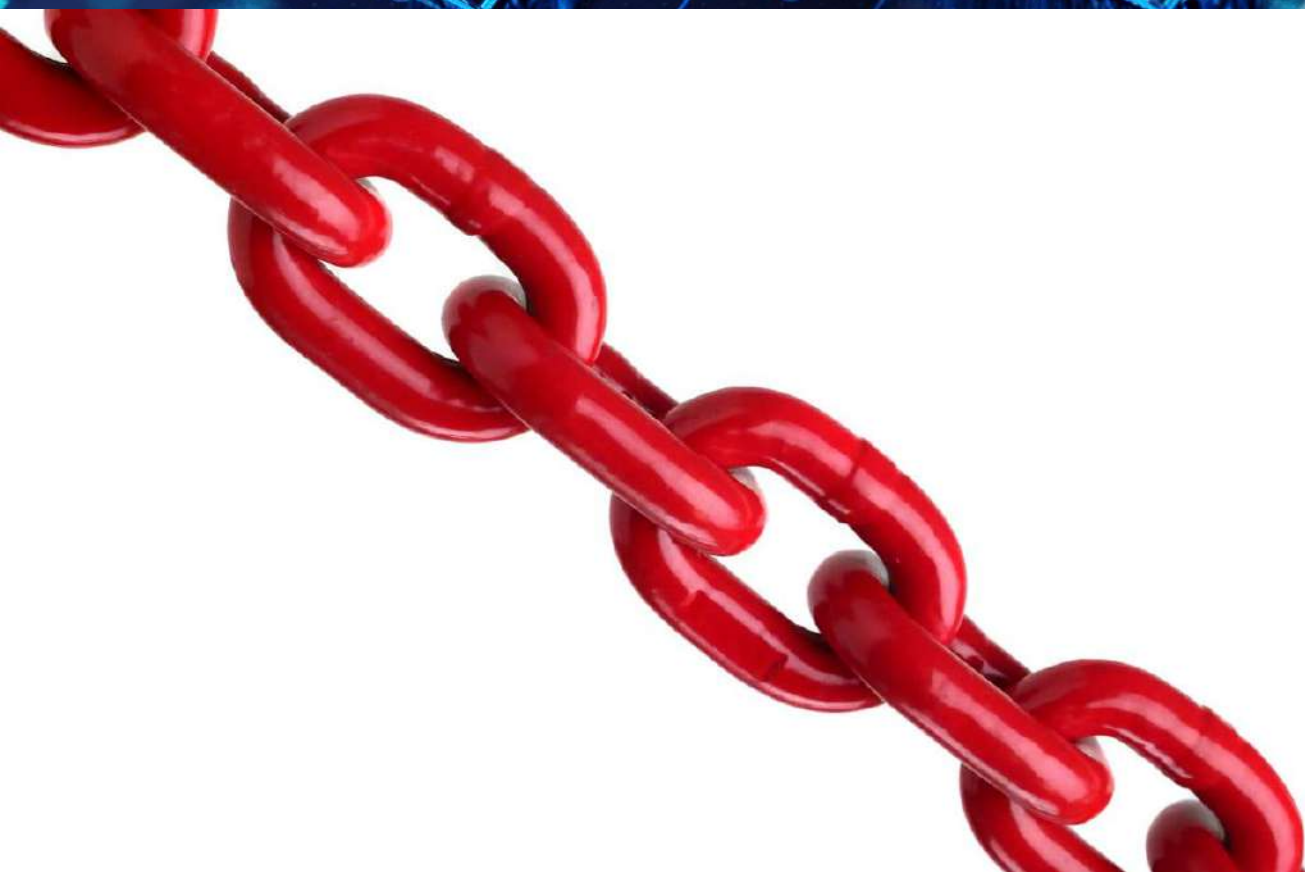
- usługi pocztowe i kurierskie
- **gospodarka odpadami**
- produkcja, wytwarzanie i dystrybucja chemikaliów
- produkcja, przetwarzanie i dystrybucja żywności
- produkcja, w szczególności wyrobów medycznych, komputerowych, elektronicznych i optycznych, niektórych rodzajów sprzętu elektrycznego i maszyn, pojazdów silnikowych i innego sprzętu transportowego
- dostawcy usług cyfrowych w zakresie internetowych platform handlowych, wyszukiwarek i sieci społecznościowych.





Art. 8. Obowiązek wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej.

e) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem **monitorowania w trybie ciągłym**.



KONSEKWENCJE NIEPRZESTRZEGANIA REGULACJI



- **Wysokie kary finansowe** – kary mogą sięgać nawet kilkudziesięciu mln zł.
- **Utrata licencji** – poważne naruszenia mogą skutkować cofnięciem zezwoleń na działalność.
- **Odpowiedzialność prawna** – w przypadku naruszenia przepisów zarząd może ponosić osobistą odpowiedzialność.
- **Utrata reputacji** – incydenty cybernetyczne mogą prowadzić do spadku zaufania klientów.



KONSEKWENCJE NIEPRZESTRZEGANIA PRZEPISÓW

Firma	Kwota	Rok
Poczta Polska	27 124 000	2022
McDonald's	16 932 657	2025
Fortum Marketing and Sales Polska	4 911 732	2022
Morele	3 800 000	2022
Facebook	4 500 000	2021
Telekomunikacja Polska	3 000 000	2019
Klinika ginekologiczna	1 500 000	2022
Cyfrowy Polsat	1 136 975	2021
Res-Gastro	238 345	2023

NA JAKIE ATAKI TRZEBA BYĆ PRZYGOTOWANYM?

- **Phishing i Social Engineering**
- **Ransomware i Wymuszenia**
- **Ataki na infrastrukturę**
- **Ataki na łańcuch dostaw**
- **Ataki na przestarzałe systemy**

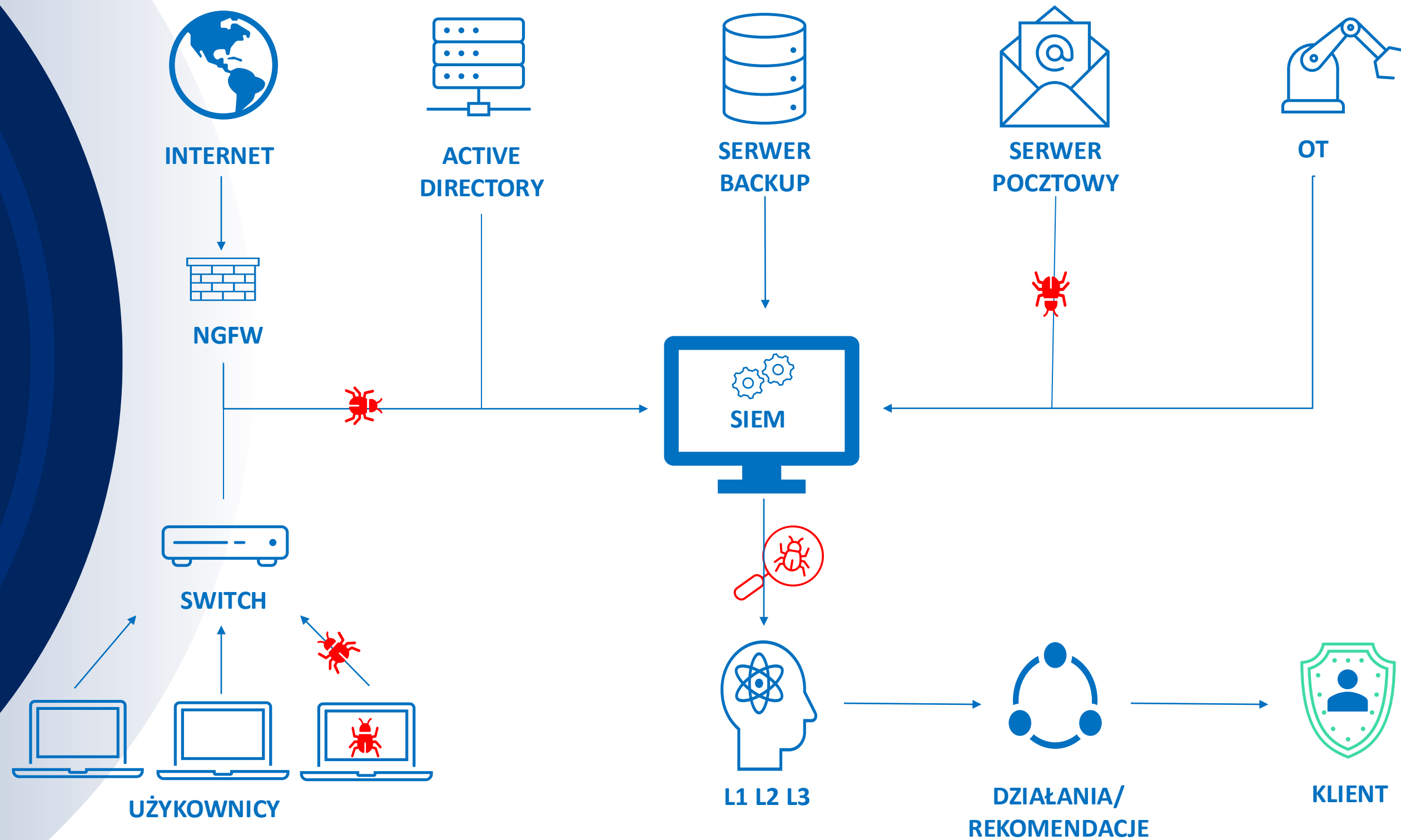


JAK SIĘ SKUTECZNIE BRONIĆ PRZED ATAKAMI?

- Szkolenia i edukacja pracowników
- Silna polityka dostępu i zarządzanie tożsamością
- Zaawansowane zabezpieczenia systemów IT
- Regularne testy penetracyjne i audyty bezpieczeństwa
- Segmentacja sieci i Zero Trust Security
- Zarządzanie dostępami
- Monitoring i analiza zagrożeń w czasie rzeczywistym
- Plan reagowania na incydenty



USŁUGA SOC (art. 8. NIS2)





CELE SOC'a

1 Wykrywanie Anomalii

2 Prewencja

3 Reakcja na incydenty

4 Poprawa zabezpieczeń

= Spokojny sen



KORZYŚCI Z WDROŻENIA SOCa

- Ciągłe monitorowanie i wykrywanie zagrożeń
- Szybka reakcja na incydenty
- Zgodność regulacyjna
- Dostęp do specjalistów
- Poprawa ciągłości biznesowej
- Zwiększenie zaufania klientów
- Dostęp do zaawansowanych technologii

Dzięki usłudze SOC, firmy mogą nie tylko **chronić** swoje **systemy** przed cyberatakami, ale także budować odporność operacyjną, która jest kluczowa w dynamicznym środowisku cyfrowym i zapewnić **zgodność** z dyrektywą **NIS2**

SOLID
SECURITY

SOLID CYBER

ZAUFALI NAM

TUZ
UBEZPIECZENIA


eurofinance
ubezpieczenia


wygodne płatności

 **Partner**
TOWARZYSTWO UBEZPIECZEŃ I REASEKURACJI S.A.

DATAWAY
We support DATA world

 **GRUPA
BIUROLAND**

ITH

SOLID
MCG



Maciej Cieśła

Prezes zarządu SOLID CYBER



mciesla@solidsecurity.pl

+48 785 560 672

Edward Bergtold

Dyrektor Sprzedaży



ebergtold@solidsecurity.pl

+48 453 696 393