

Trzy filary XDR

Czy Twoje bezpieczeństwo jest kompletne?

Mateusz Nowak, product manager

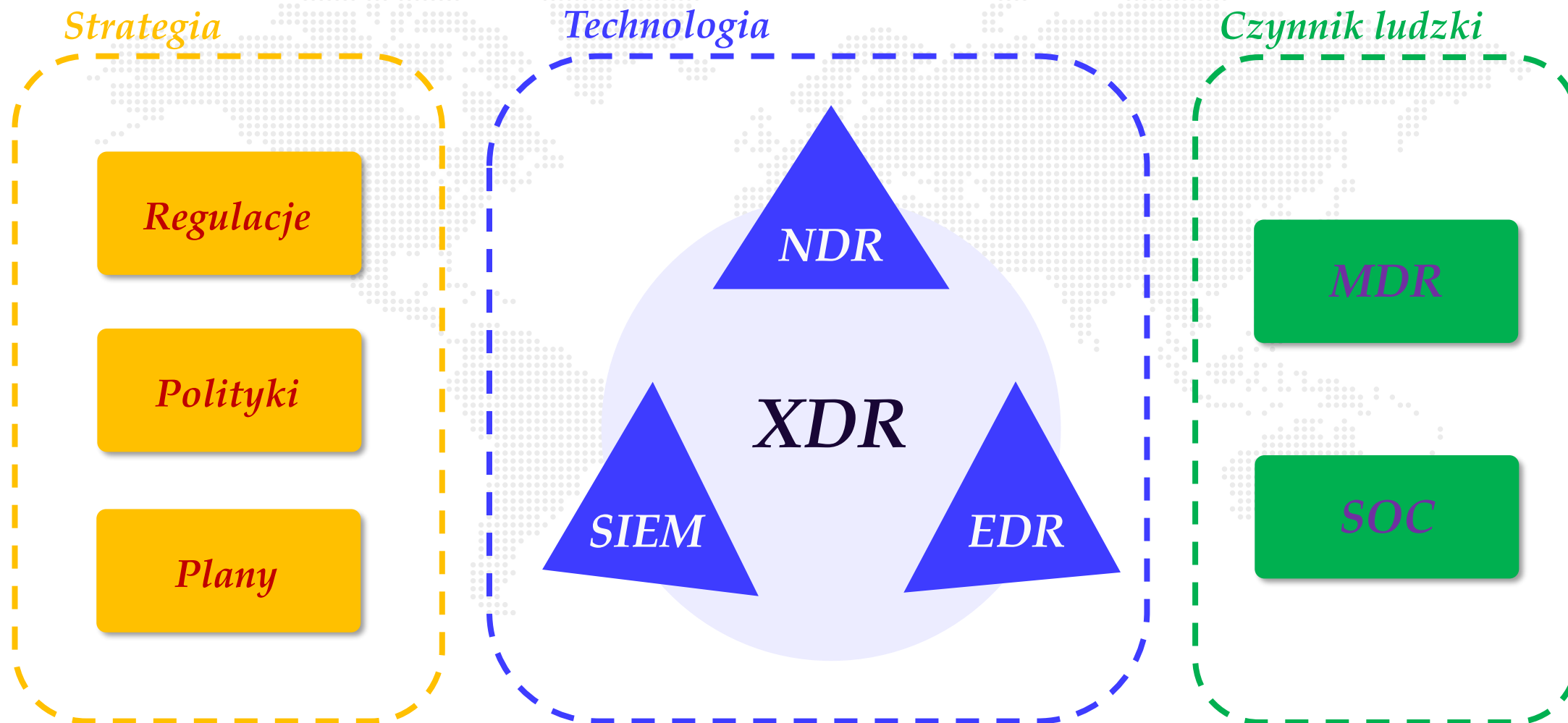
...DR

*...czyli
Detection and Response*

E(X)tendedDR

Rozwiązanie czy podejście?

XDR



XDR *Strategia*

Regulacje

- Regulacje europejskie, krajowe lub branżowe często są motywatorem do wprowadzania zmian
- Mogą też stanowić inspirację do tworzenia spójnej i kompletnej polityki bezpieczeństwa

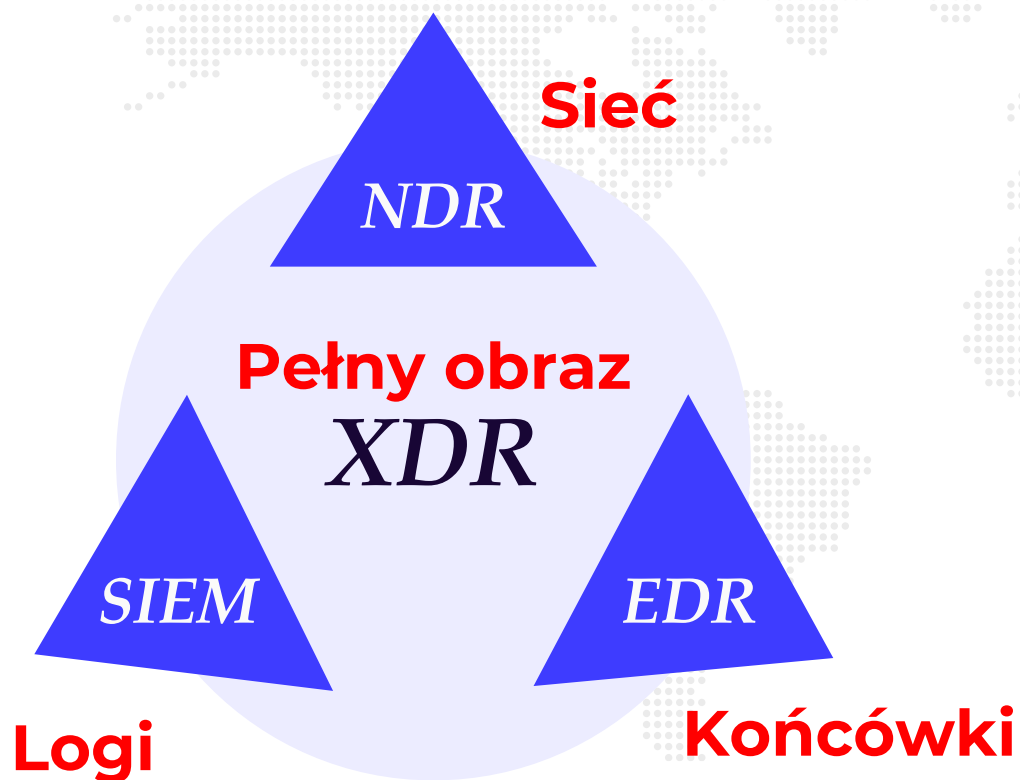
Polityki

- Organizacyjny zbiór deklaracji, procedur i wymogów
- Ich rolą jest ukształtowanie standardów systemów bezpieczeństwa, zachowań pracowników, schematów postępowania w sytuacjach awaryjnych i walidacji poprawności wdrożenia, adaptacji oraz działania

Plany

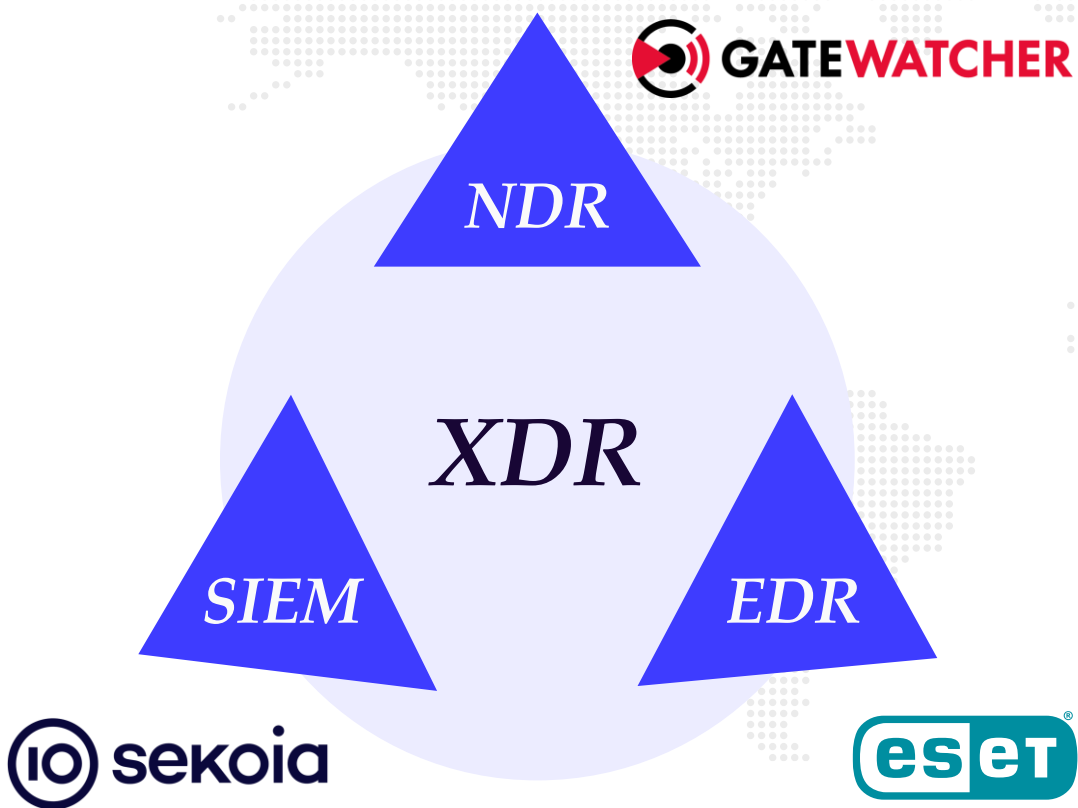
- Każda strategia powinna zawierać w sobie plany rozwoju i ewolucji, w celu dostosowania się do bieżących i przyszłych zmian otoczenia
- Dzisiejsze ograniczenia (np. związane z zatrudnieniem, kompetencjami czy budżetem) powinny być zaadresowane w planach

XDR Technologia



- Rolą technologii jest zapewnienie:
 - widoczności
 - detekcji
 - optymalizacji pracy analityka
- Polityka organizacji powinna zakładać jakie środki techniczne są właściwe i adekwatne dla jej kontekstu

XDR Technologia



- Rolą technologii jest zapewnienie:
 - widoczności
 - detekcji
 - optymalizacji pracy analityka
- Polityka organizacji powinna zakładać jakie środki techniczne są właściwe i adekwatne dla jej kontekstu

XDR Czynniki ludzkie

- Skuteczne egzekwowanie polityk i wykorzystanie technologii wymaga czasu oraz kompetencji specjalistów
- Zadaniami zespołów odpowiedzialnych za bezpieczeństwo jest: wykrywanie, analiza i reakcja
- Brak adekwatnych zasobów wewnętrznych można kompensować outsourcingiem

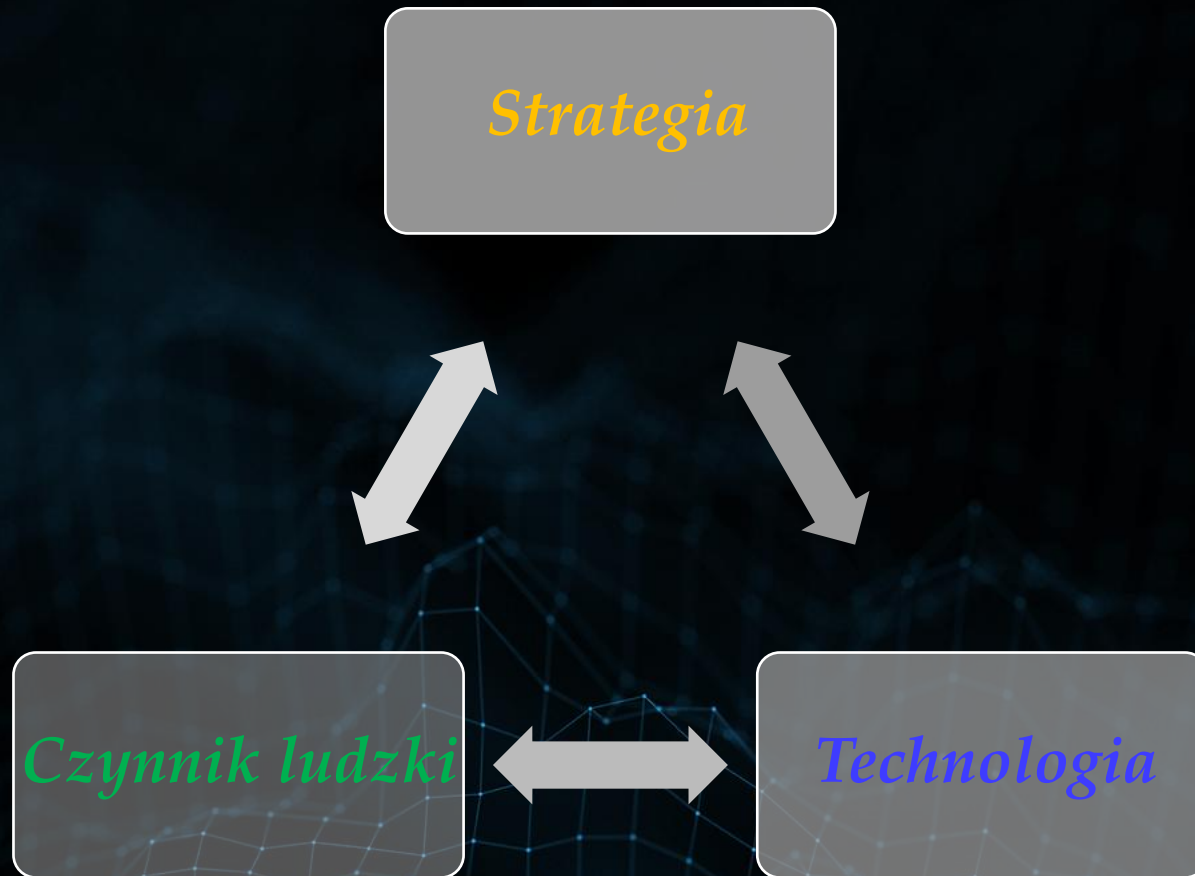
MDR

Manage Service

SOC

Security operations center

Czy bezpieczeństwo jest kompletne?



- Czy nasza polityka spełnia wszystkie wymagania formalne?
- Czy nasza polityka jest zakomunikowana i realizowana przez wszystkich pracowników?
- Czy modyfikujemy politykę wraz ze zmieniającym się otoczeniem?
- Czy weryfikujemy zgodności formalne i techniczne?
- Czy wykorzystywane rozwiązania są adekwatne do zagrożeń?
- Czy systemy detekcyjne dają nam możliwość wykrycia i remediacji zagrożeń na wczesnym etapie?
- Czy personel odpowiedzialny za bezpieczeństwo ma stosowne kompetencje i czas na realizację swoich zadań?

Itd. ...

Kontakt:



Mateusz Nowak
Product Manager

nowak.m@dagma.pl
795 518 758