Zero Trust jako odpowiedź na cyberprzestępczość

Jak chronić organizacje przed współczesnymi zagrożeniami?

Tomasz Janczewski

Akademia Marynarki Wojennej w Gdyni

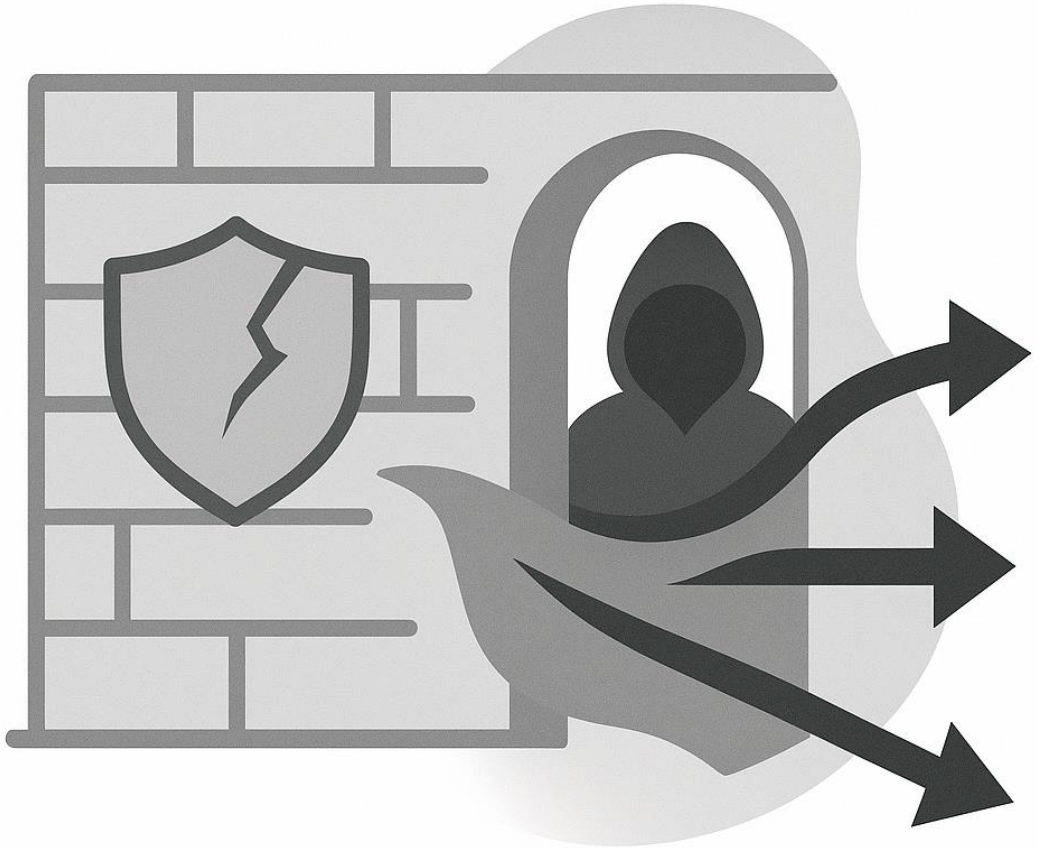
Gdynia 2025

Cel prezentacji

Zaprezentowanie praktycznego wdrożenia architektury Zero Trust jako skutecznej odpowiedzi na współczesne zagrożenia cyberprzestępczością, ze szczególnym uwzględnieniem automatyzacji, zastosowania narzędzi open source (EDR, SIEM, SOAR) oraz realnych wyzwań, przed którymi stoją zespoły bezpieczeństwa, analitycy SOC, informatycy śledczy i służby mundurowe.

Rosnące zagrożenia cyberprzestępczością

- Ransomware
- Phishing
- APT (Advanced Persistent Threats)
- Insider threats



Tradycyjny model bezpieczeństwa – dlaczego nie działa?

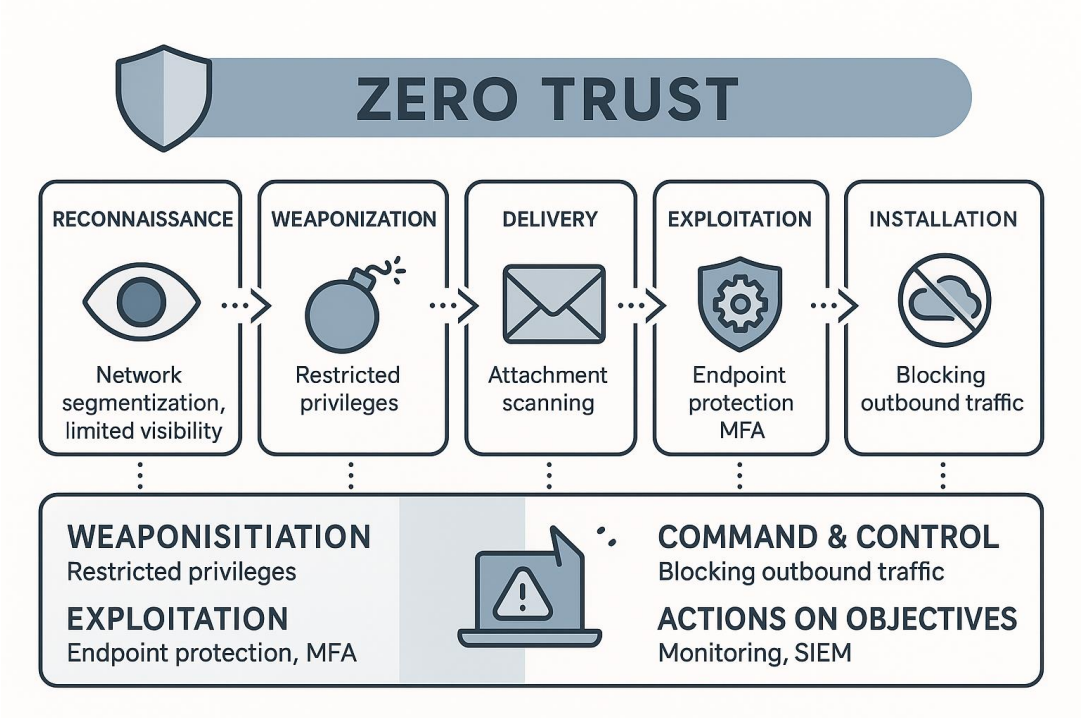
Model „zaufania perymetrycznego” – nieadekwatny wobec dzisiejszych zagrożeń.

Założenia architektury Zero Trust

- Nigdy nie ufaj, zawsze weryfikuj
- Weryfikacja tożsamości i kontekstu
- Dostęp minimalny (least privilege)

Zero Trust a cyberprzestępczość – połączenie

Zero Trust minimalizuje skutki działań cyberprzestępców, nawet jeśli pokonają perymetr.

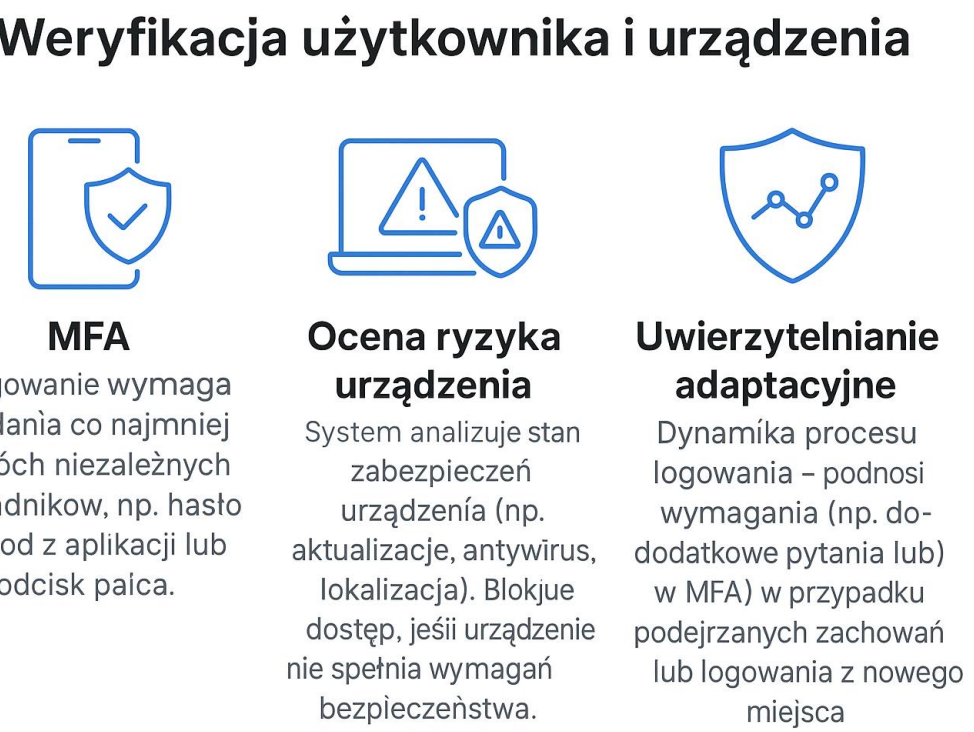


Kluczowe komponenty Zero Trust

- Identyfikacja i uwierzytelnianie
- Kontrola dostępu
- Mikrosegmentacja
- Monitorowanie i analiza

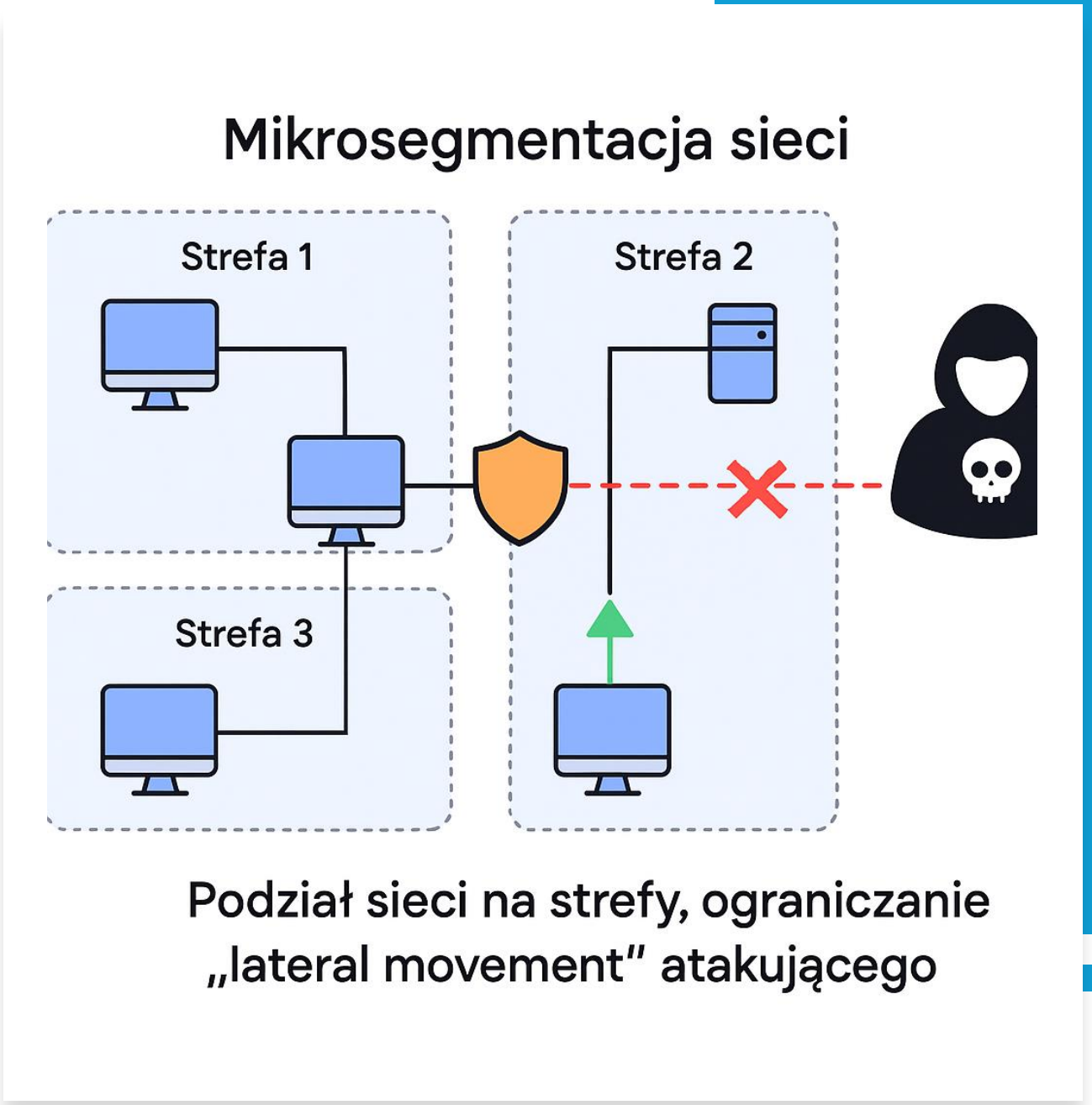
Weryfikacja użytkownika i urządzenia

- MFA
- Ocena ryzyka urządzenia
- Uwierzytelnianie adaptacyjne



Mikrosegmentacja sieci

Podział sieci na strefy, ograniczanie „lateral movement” atakującego.



Least Privilege Access

Każdy ma dostęp tylko do niezbędnych zasobów.

Monitorowanie i analiza (SOC)

- Ciągła obserwacja
- Wykrywanie nietypowych zachowań
- Automatyczne reakcje

Automatyzacja w Zero Trust

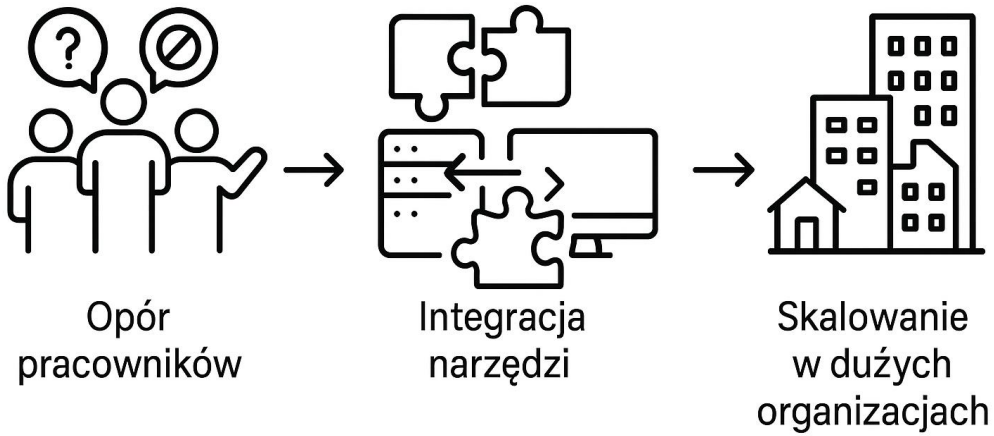
- SOAR
- Playbooki
- Szybka reakcja na incydenty

Wdrożenie Zero Trust – krok po kroku

1. Audyt i klasyfikacja zasobów
2. Wprowadzenie MFA
3. Mikrosegmentacja
4. Monitoring
5. Automatyzacja reakcji

Najczęstsze wyzwania przy wdrożeniu

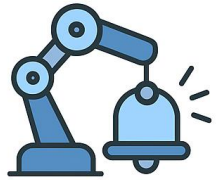
- Opór pracowników
- Integracja narzędzi
- Skalowanie w dużych organizacjach



Narzędzia wspierające Zero Trust

SIEM

np. Splunk, QRadar



SOAR

Cortex XSOAR

EDR/XDR

np. CrowdStrike, SentinelOne

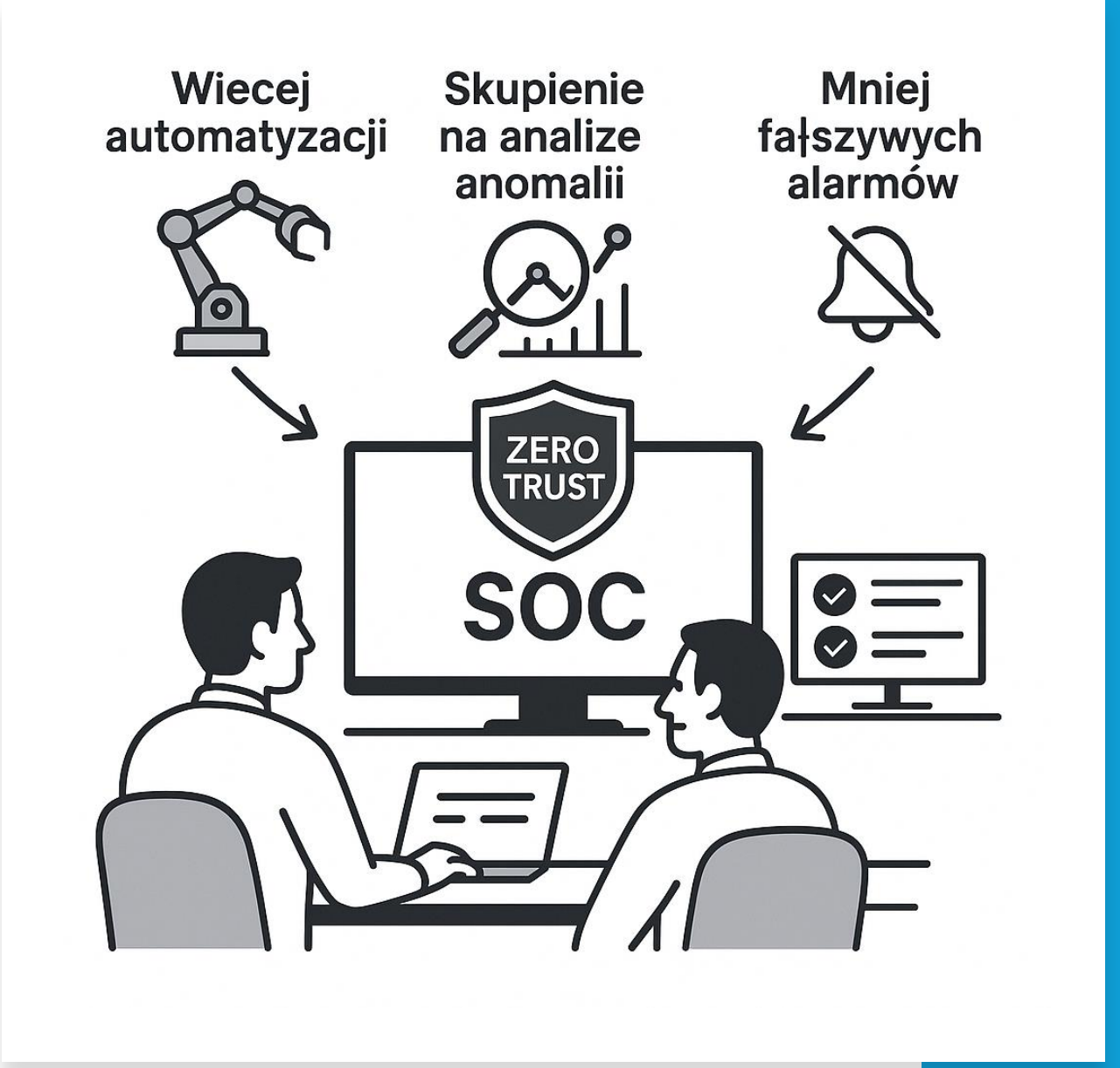
Identity Management

np. Okta, Azure AD

- SIEM (np. Splunk, QRadar)
- SOAR (np. Cortex XSOAR)
- EDR/XDR
- Identity Management

Jak Zero Trust zmienia rolę SOC?

- Więcej automatyzacji
- Skupienie na analizie anomalii
- Mniej fałszywych alarmów



Wsparcie dla informatyki śledczej

- Lepsza widoczność ruchu
- Dokładne logi
- Szybsze ustalanie wektora ataku

Zero Trust a reakcja na incydenty

- Szybsza izolacja
- **Ograniczanie szkód**
- Lepsze narzędzia analityczne.

Współpraca z policją i służbami

- Szybsze przekazywanie informacji
- **Standaryzacja logów**
- Łatwiejsza współpraca poprzez automatyzację
- Wcześniejsze wychwytywanie problematycznych przypadków

Przyszłość Zero Trust

- AI w Zero Trust
- Automatyczne uczenie polityk bezpieczeństwa
- Nowe wyzwania (IoT, OT)

Najważniejsze wnioski

- Zero Trust nie jest produktem, to proces
- Automatyzacja i monitoring to fundamenty
- Każda organizacja może być celem

Kontakt i materiały dodatkowe

Prelegent: Tomasz Janczewski

E-mail: tomasz@janczewski.it

Materiały:

https://github.com/tjancz/zero-trust-cybercrime-xxi

Dziękuję