IT Solution FACTOR

IBM Gold Business Partner

SIEM w SOC, lub SOC ze SIEM

Dobre praktyki w wykorzystaniu systemów **SIEM/SOC** w organizacji nie tylko w czasie pandemii

Grzegorz Cebula - Presales & Implementation Director
Security & Business Continuity Unit, **IT Solution Factor**

IT Solution FACTOR

IBM Gold Business Partner

Warto wiedzieć- SIEM

IT Solution FACTOR

IBM Gold Business Partner

SIEM

Security Information and Event Management

Jedna konsola „Stanu bezpieczeństwa w sieci”

Monitorowanie i analiza wszystkich aktywności w organizacji
- Użytkownicy
- Administratorzy
- Maszyny
- Aplikacje

Sprawdzanie występowania znanych scenariuszy bezpieczeństwa i zgodności z polityką organizacji

Wykrywanie anomalii bez udziału operatora/administratora

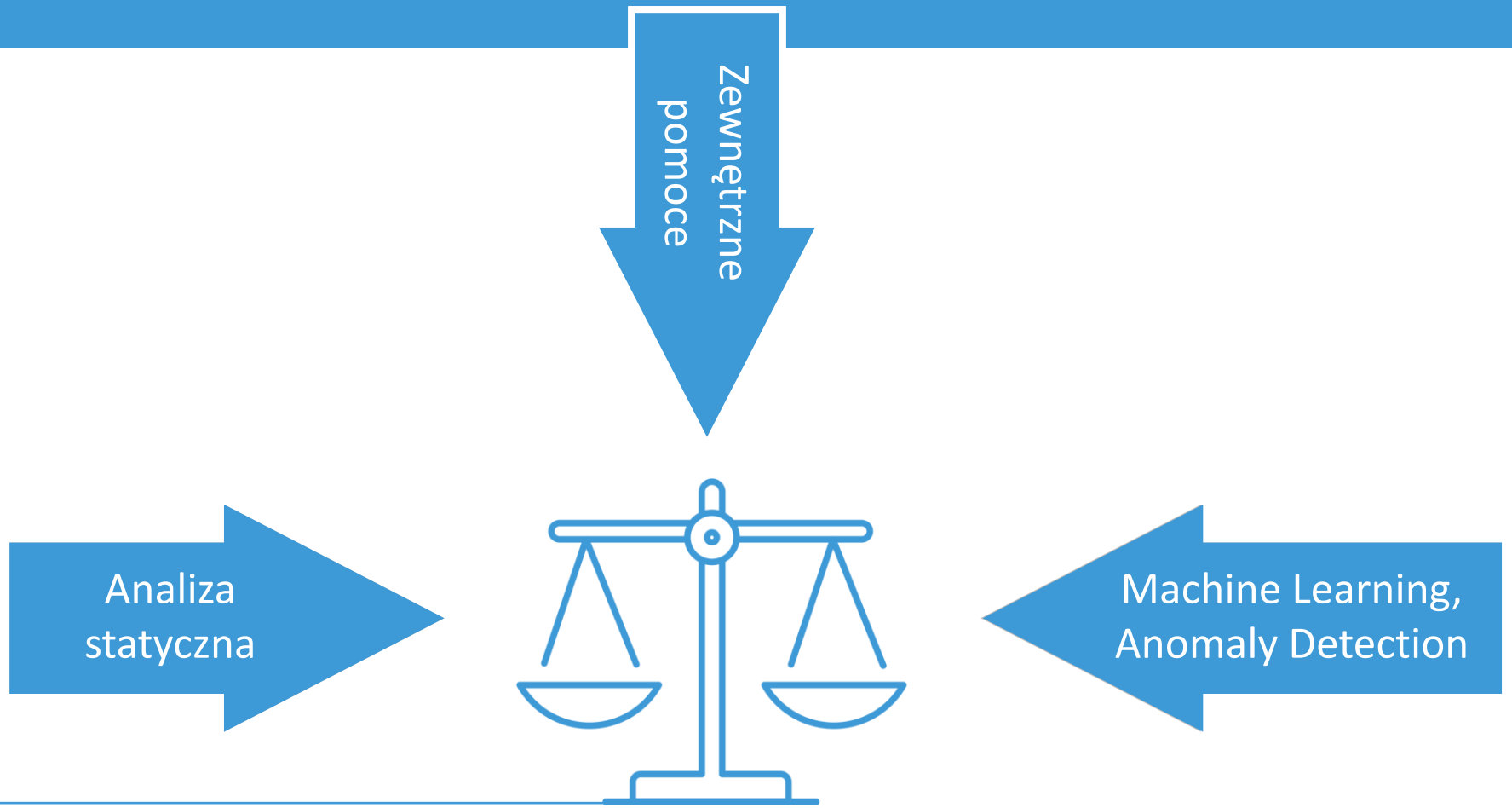
Historia do wglądu dla służb, analizy wstecznej

Zgodność z wymaganiami certyfikacji, akredytacji, branży, etc.

IT Solution FACTOR

IBM Gold Business Partner

SIEM – Top 3



IT Solution FACTOR

IBM Gold Business Partner

Nasz wiodący partner SIEM

IBM Gold Business Partner TM

- **Qradar** dla wszystkich i wszędzie – security intelligence
- **Wszystkie** opcje instalacji
- Bogata, gotowa **funkcjonalność** (źródła, reguły, aplikacje)
- Pierwsze efekty w **godzinach** od wdrożenia
- Modularny **kombajn** od podstawy do pełnego narzędzia śledczego
- Ciekawe licencjonowanie
- Przyjazny **interfejs**
- Bogata oferta integracji + **API**

IT Solution FACTOR

IBM Gold Business Partner

Warto wiedzieć- SOC

IT Solution FACTOR

IBM Gold Business Partner

SOC

- Security Operation Center
- Zorganizowana centralna jednostka zarządzania bezpieczeństwem organizacji
- Wykorzystuje posiadane już narzędzia, w tym SIEM, do monitorowania i reagowania
- Reagowanie na zdarzenia oraz ograniczanie ryzyka
- Wyróżniki:
  - Wiedza
  - Zorganizowanie
  - Plany awaryjne i rozwoju
  - Reagowanie na otoczenie (np. C19)
  - Wszystkie aspekty bezpieczeństwa w zarządzaniu

IT Solution FACTOR

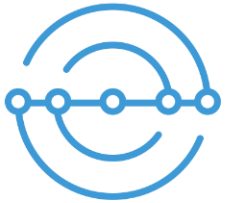
IBM Gold Business Partner

Nasz wiodący partner SOC

IBM Gold Business Partner ™

Oprogramowanie wspierające działanie SOC – Platforma Resilient

- Gotowa integracja z wiodącymi SIEM
- Automatyzacje
- Dynamiczne play-book’i
- Instalacje lokalne i chmurowe, wersja SaaS



Systemy bezpieczeństwa

- IPS
- skanery aplikacji, kodu, sieciowe
- ochrona stacji i telefonów
- automatyczne patchowanie

IT Solution FACTOR

IBM Gold Business Partner

Nasz wiodący partner SOC

IBM Gold Business Partner ™

Usługi IBM w zakresie bezpieczeństwa - Managed Security Services

- SOC dzierżawiony
- Obsługa trudnych incydentów

Subskrypcje bezpieczeństwa

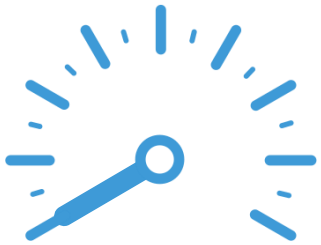
- X-force
- Watson for security
- Machine Learning

IT Solution FACTOR

IBM Gold Business Partner

To wszystko po to by...

... Zmniejszyć / Skrócić / Ograniczyć *



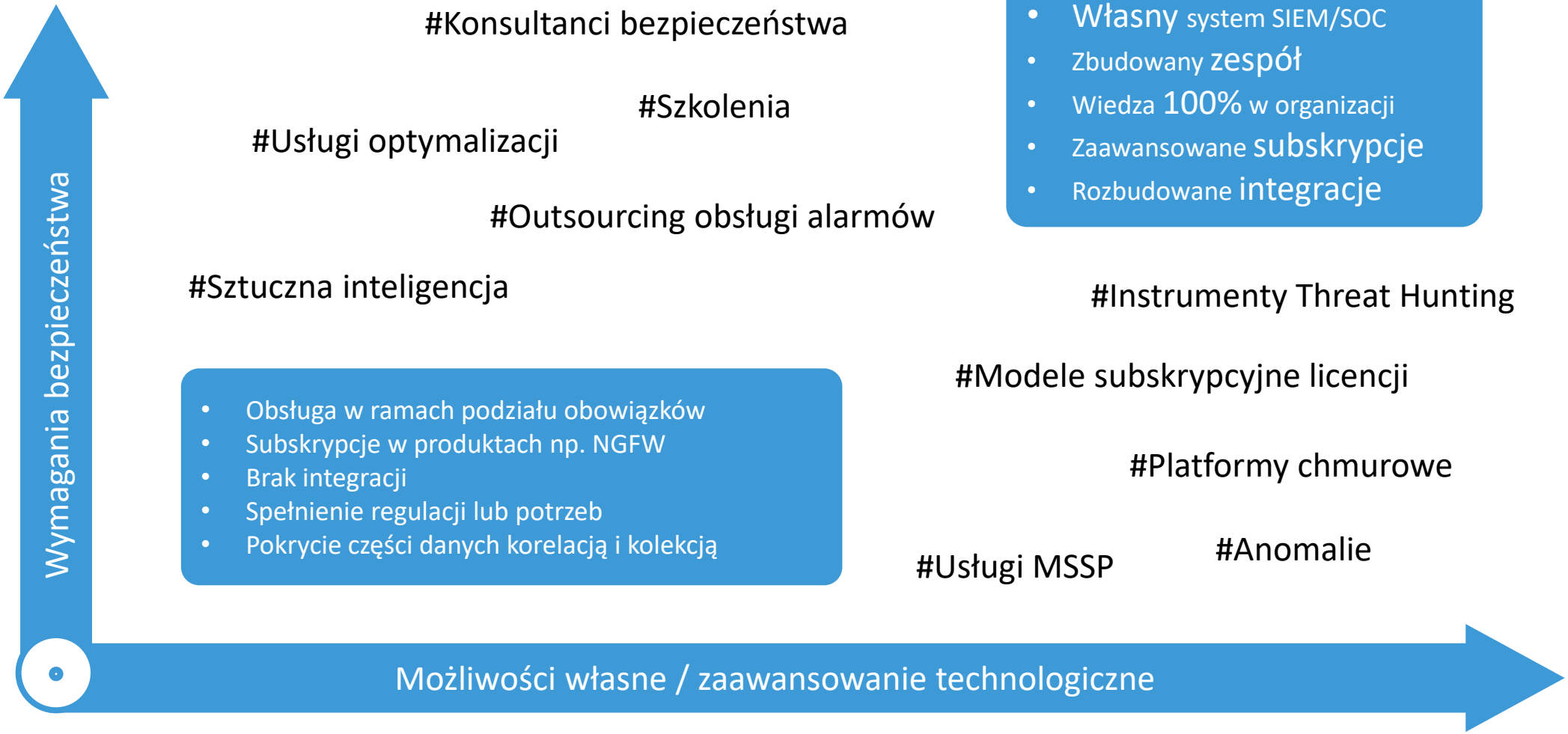
- **Mean Time to Detect (MTTD):** średni czas jaki zajmuje wykrycie incydentu bezpieczeństwa
- **Mean Time to Respond/Remediate (MTTR):** średni czas reakcji na wykryte zagrożenie

** W granicznych przypadkach nawet uzyskać policzalne wartości*

IT Solution FACTOR

IBM Gold Business Partner

Zarządzanie bezpieczeństwem - po polsku



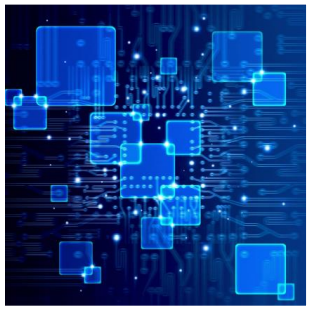
IT Solution FACTOR

IBM Gold Business Partner

Przyszłość bezpieczeństwa z SIEM w SOC

IT Solution FACTOR

IBM Gold Business Partner



Przyszłość bezpieczeństwa z SIEM w SOC

Koordynacja branżowa i technologiczna

- Interfejsy i języki

Wsparcie zewnętrznych dostawców „on-line”

- Dobre praktyki
- Nowe możliwości

Więcej chmury

- Narzędzia analityczne
- Pojemności „na żądanie”

Operatorzy, producenci SIEM przygotowują ofertę dla firm

IT Solution FACTOR

IBM Gold Business Partner

Przyszłość bezpieczeństwa z SIEM w SOC

Więcej autokonfiguracji i automatyzacji

- Źródła logów
- Które logi potrzebne?
- Jakie dane mają sens

Wzbogacanie danych

- Co powinno być dodane do logów i dlaczego

Reguły

- Które mają sens dla zestawu danych?
- Automatyczne dodawanie

Baza wiedzy

- Co robić z wynikami?

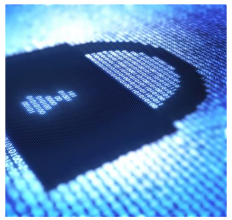
IT Solution FACTOR

IBM Gold Business Partner

Jak to w praktyce bywa … - **SIEM/SOC**

IT Solution FACTOR

IBM Gold Business Partner



Jak to w praktyce bywa …- SIEM/SOC

- Security Information – TAK! ale Event Management – NIE!
- Kto to będzie obsługiwał?
- Kto to będzie konfigurował?
- Problemy kadrowe – baza wiedzy, uniwersalizm, uproszczenia
- Integracje – skomplikowane
- Oczekiwania rezultatów w biznesie
- Utrzymanie aktualności konfiguracji
- Rozwój źródeł danych
- Odpowiednie miejsce zespołu w strukturach
  - brak komunikacji
  - niewystarczające uprawnienia

IT Solution FACTOR

IBM Gold Business Partner

ITSF + IBM = komplementarność w projektach bezpieczeństwa

Usługi ITSF dla oferty IBM

- Doradztwo i dobór rozwiązań
- Wykonywanie projektów przedwrożeniowych
- Realizacja wdrożeń i integracji
- Pomoc w utrzymaniu systemów bezpieczeństwa, administracja
- Konsultacje
- Przeglądy i audyty instalacji
- Usługi wsparcia 24/7

Idealne **połączenie** dla sektora finansowego

IT Solution FACTOR

IBM Gold Business Partner™

wiedza i najwyższe kompetencje
w integracji infrastruktury
i oprogramowania

sprawdzona
i godna zaufania
technologia