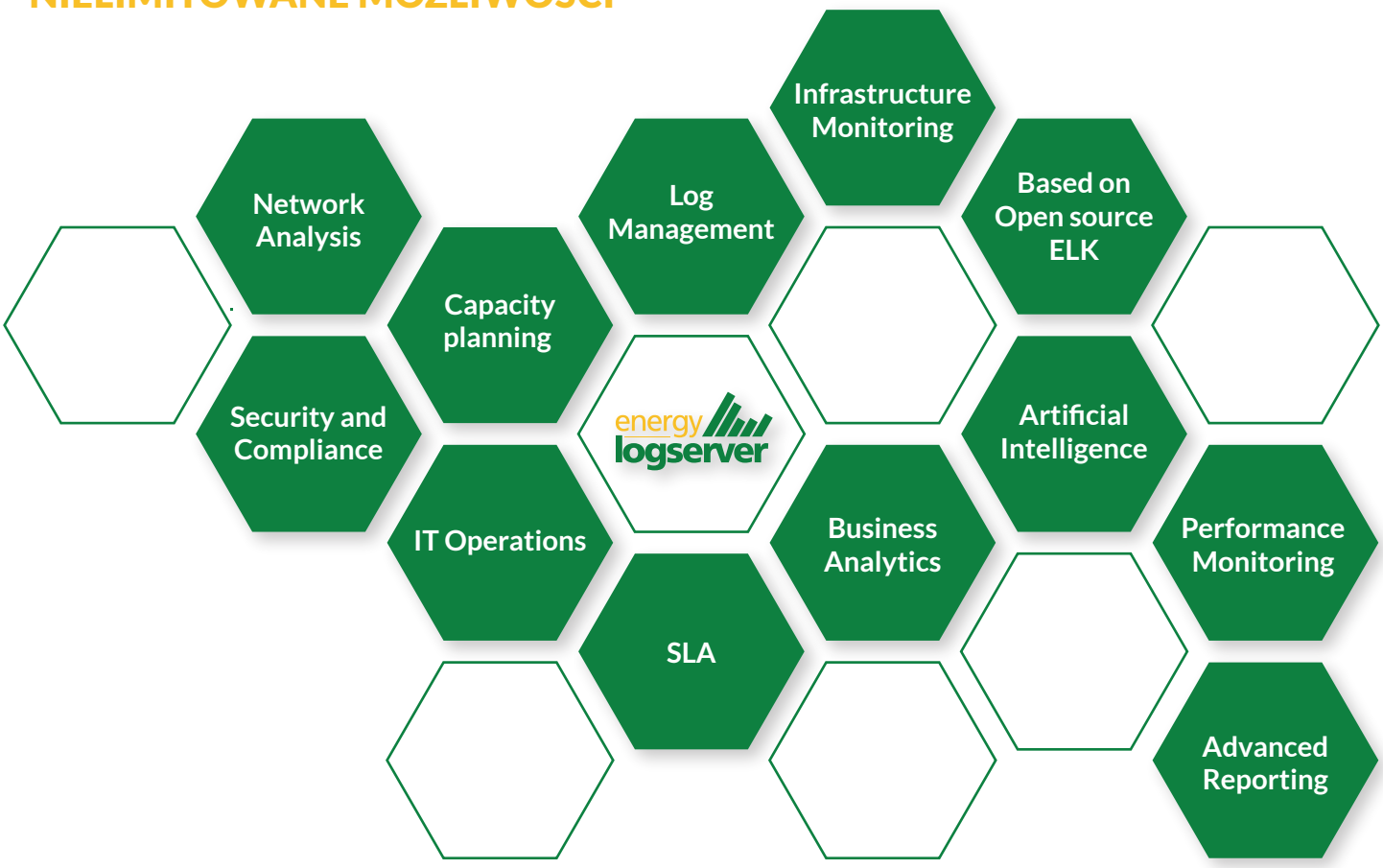
energy logserver

Innowacyjne, polskie rozwiązanie pozwalające na centralizację zdarzeń systemów IT.

Projekt Energy Logserver został stworzony z myślą objęcia centralizacją zdarzeń wszystkich obszarów IT w organizacji. System pozwala na natychmiastowy przegląd logów, ich wielowymiarową analizę i raportowanie – skala nie ma znaczenia.

JEDNA PLATFORMA, NIELIMITOWANE MOŻLIWOŚCI



- BAZUJE NA ELASTICSEARCH
- AGREGACJA I KORELACJA LOGÓW
- WIZUALIZACJA DANYCH
- RAPORTOWANIE
- ALARMOWANIE
- WYDAJNOŚĆ I SLA

LOG MANAGEMENT & SIEM & NETWORK ANALYSIS PLAN

Energy Logserver to nie tylko wysokowydajna platforma do zarządzania logami bezpieczeństwa.
Dodatkowo oferuje m.in. alertowanie oraz korelację zdarzeń z bazą gotowych reguł korelacyjnych. W toku rozwoju rozwiązania stworzony został również bogaty pakiet funkcjonalności, które czynią z niej niezwykle efektywny system klasy SIEM (Security Information & Event Management). SIEM Plan pozwala na jeszcze skuteczniejszą i precyzyjniejszą pracę nad wykrywaniem i zarządzaniem incydentami bezpieczeństwa.

Funkcjonalności	Log Management Plan	SIEM Plan	Network Analysis Plan
Integracja z Active directory, Radius, SSO	+	+	+
Alertowanie i raportowanie	+	+	+
Analiza protokołów Netflow	+	+	+
Uczenie maszynowe i sztuczna inteligencja	+	+	+
Monitorowanie infrastruktury IT	+	+	+
Monitorowanie wydajności aplikacji	+	+	+
Predefiniowane parsery dla różnych źródeł	Ponad 100 źródeł	+	+
Reguły korelacyjne	+	Ponad 700	+
Zarządzanie incydentami i ryzykiem	+	+	+
Playbook	+	+	+
Integracje z MISP IoC, MITRE ATT&CK, CIS	-	+	-
Normy zgodności GDPR, PCI DSS, NIST 800-53, HIPAA	-	+	-
Endpoint Detection and Response (EDR)	-	+	-
Monitorowanie integralności plików	-	+	-
Wykrywanie podatności	-	+	-
Network IDS	-	-	+
Analiza ruchu sieciowego	-	-	+

Skontaktuj się z nami:

logserver@bakotech.pl

+48 12 376 95 08

Ul. Drukarska 18/5,
30-348 Kraków

bako tech®