integrity partners

elastic

Widzisz więcej, reagujesz szybciej

Elastic Observability jako fundament bezpieczeństwa operacyjnego banku

Forum Bezpieczeństwa Banków | 6 maja 2026 | Warszawa

Co może pójść nie tak?
Ogromne koszty każdej awarii…

$65	£330	>$5M
millionów	milionów	Na godzinę
Utrata przychodu	Całkowity koszt awarii (wg niezależnego raportu)	Średni koszt awarii
Social Media	Bank	Financial Sector

https://itic-corp.com/category/itic-reports-surveys/ ; https://www.fca.org.uk/publication/final-notices/tsb-bank-plc-2022.pdf ;
https://www.forbes.com/sites/caileygleeson/2024/03/05/facebook-instagram-users-face-widespread-outage/

Skąd bierze się ślepota operacyjna?

Silosy danych

Logi w jednym systemie,
metryki w drugim,
alerty w trzecim

Brak korelacji

Bez kontekstu między
źródłami nie wiemy
co się naprawdę dzieje

Spóźniona reakcja

Brak kontekstu =
wolniejsza detekcja =
większe straty

W 80% przypadków poważnej awarii dało się jej uniknąć dzięki lepszemu zarządzaniu, procesom i konfiguracji

Źródło: Uptime Institute, Annual Outage Analysis 2024

Stan obecny: rozproszone narzędzia i silosy danych

Klasyczny monitoring vs Observability

Monitoring

Mówi: „Coś się stało”

- Reakcja na znane problemy
- Progi alertów (CPU > 90%), Alarm systemu bezpieczeństwa
- Dashboard per narzędzie
- Ręczna korelacja danych

Observability

Mówi: „Dlaczego i gdzie”

- Proaktywne wykrywanie anomalii
- Korelacja logs + metrics + traces
- Unified dashboard, jeden widok
- Nauczanie maszynowe do wykrywania faktycznych przyczyn awarii

Trzy filary Observability

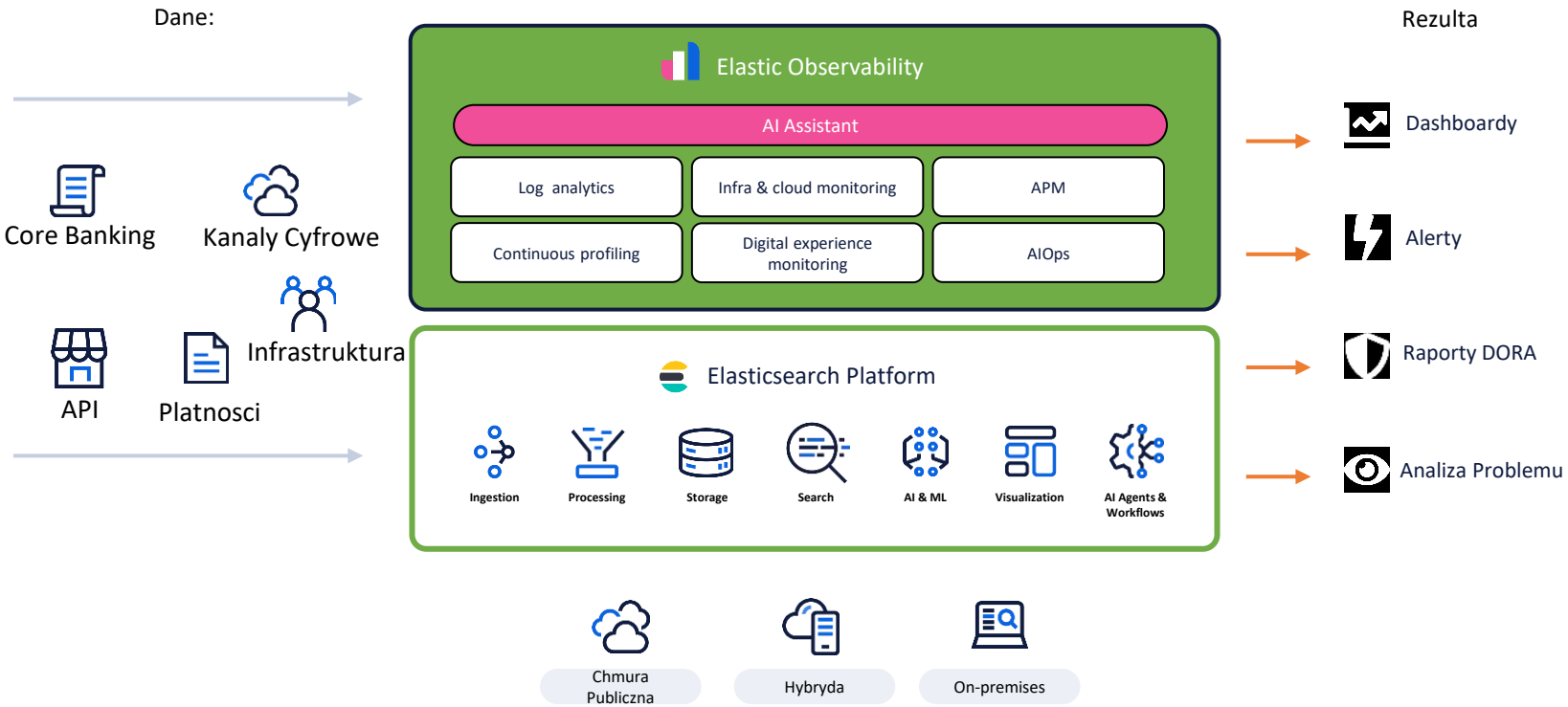
Logi
Co się wydarzyło

Metryki
Jak system się zachowuje

Traces
Gdzie jest problem w RT

Źródło: Gartner „Innovation Insight for Observability” 2024

Elastic Observability
Ujednolicony pipeline danych



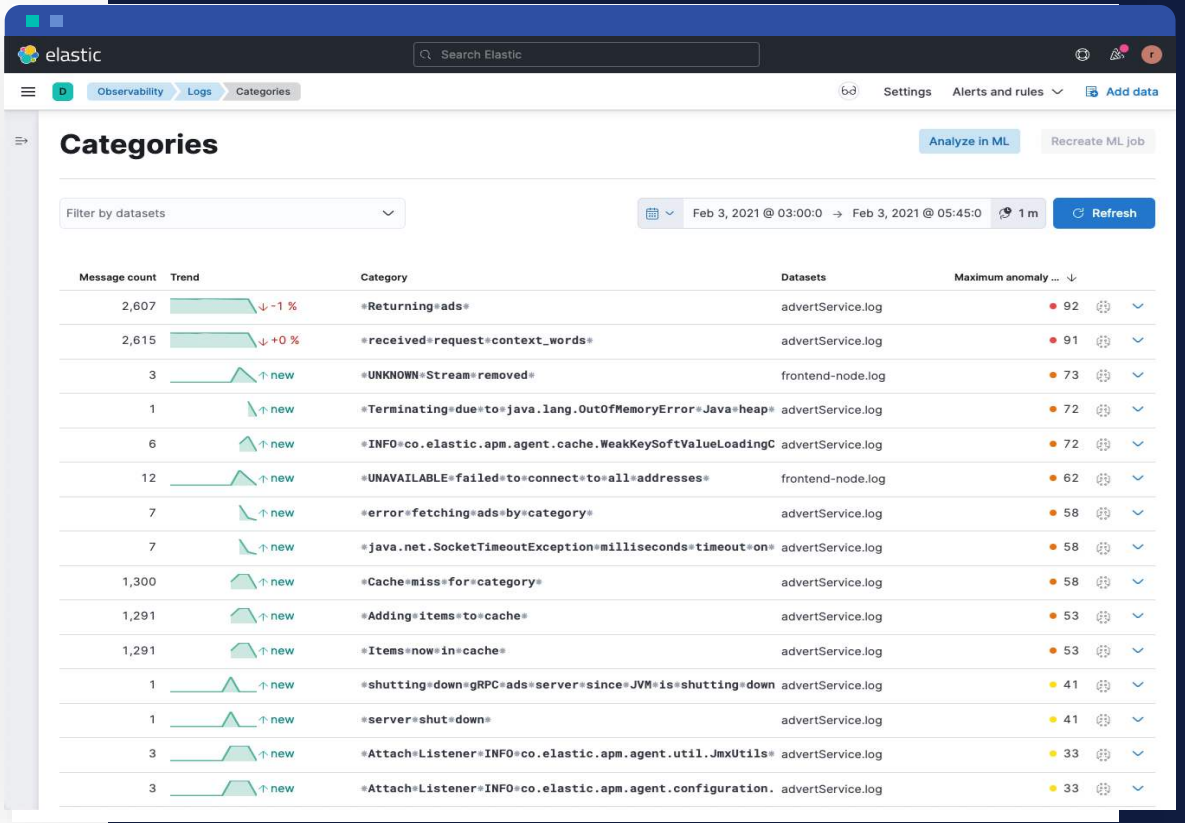
1: Elastic Survey
2: Forrester TEI

elastic

Elastic Observability

Log Analytics

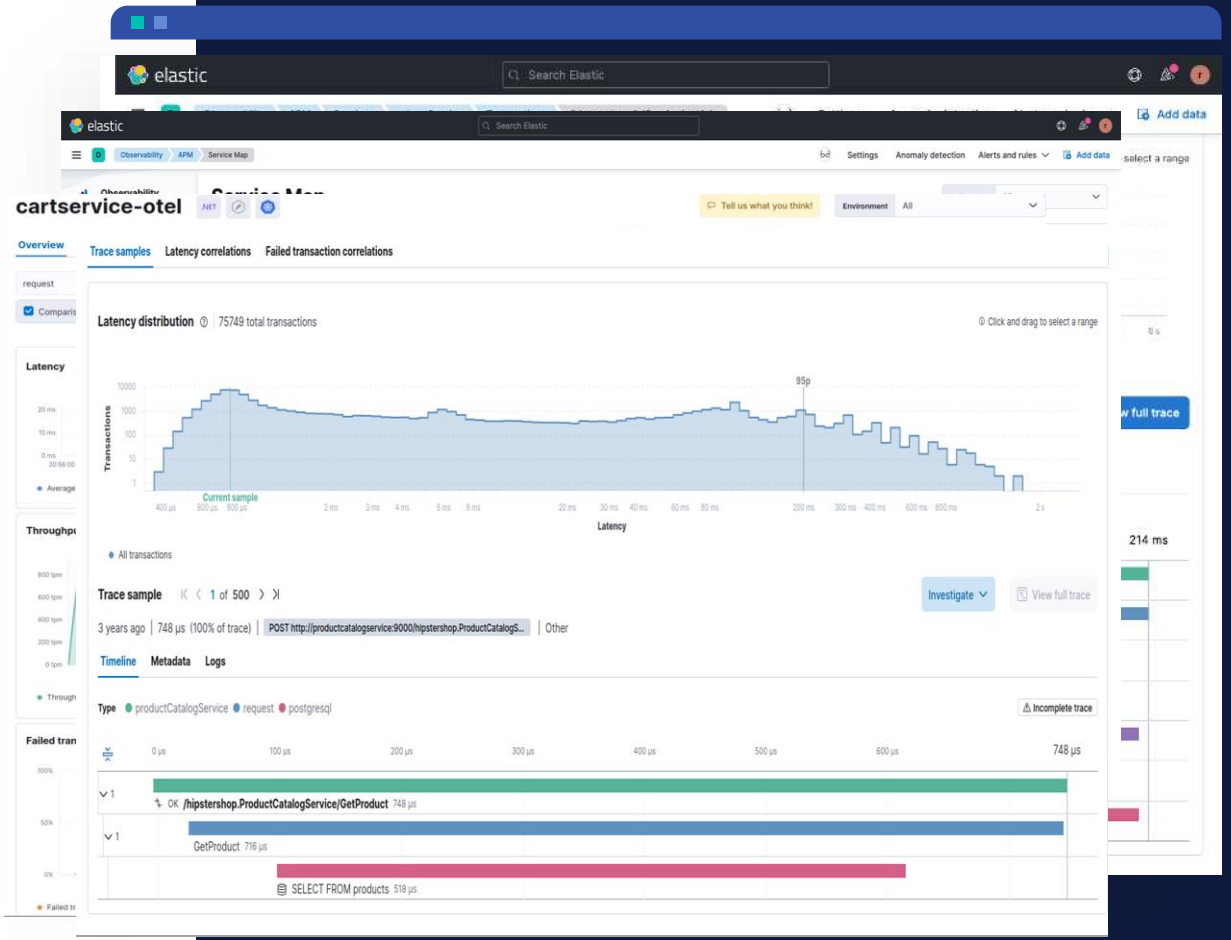
- Centralne zarządzanie logami
- Korelacja zdarzeń i alertowanie



Elastic Observability

APM

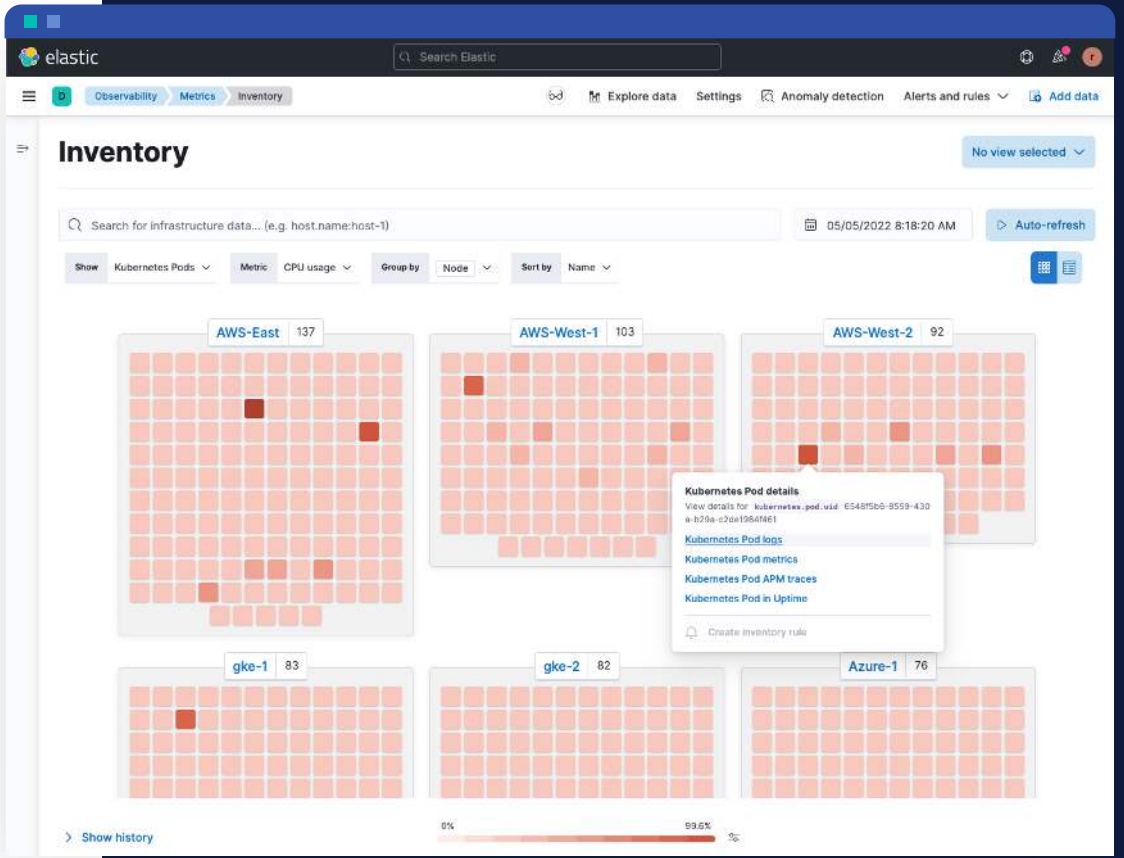
- Popraw jakość kodu dzięki "end-to-end distributed tracing"
- Szybkie rozwiązywanie problemy dzięki wskaźnikom kondycji opartym na ML
- Identyfikuj przyczyny spowolnień i błędów
- Gotowe wsparcie dla OpenTelemetry i natywnych agentów



Elastic Observability

Infrastruktura

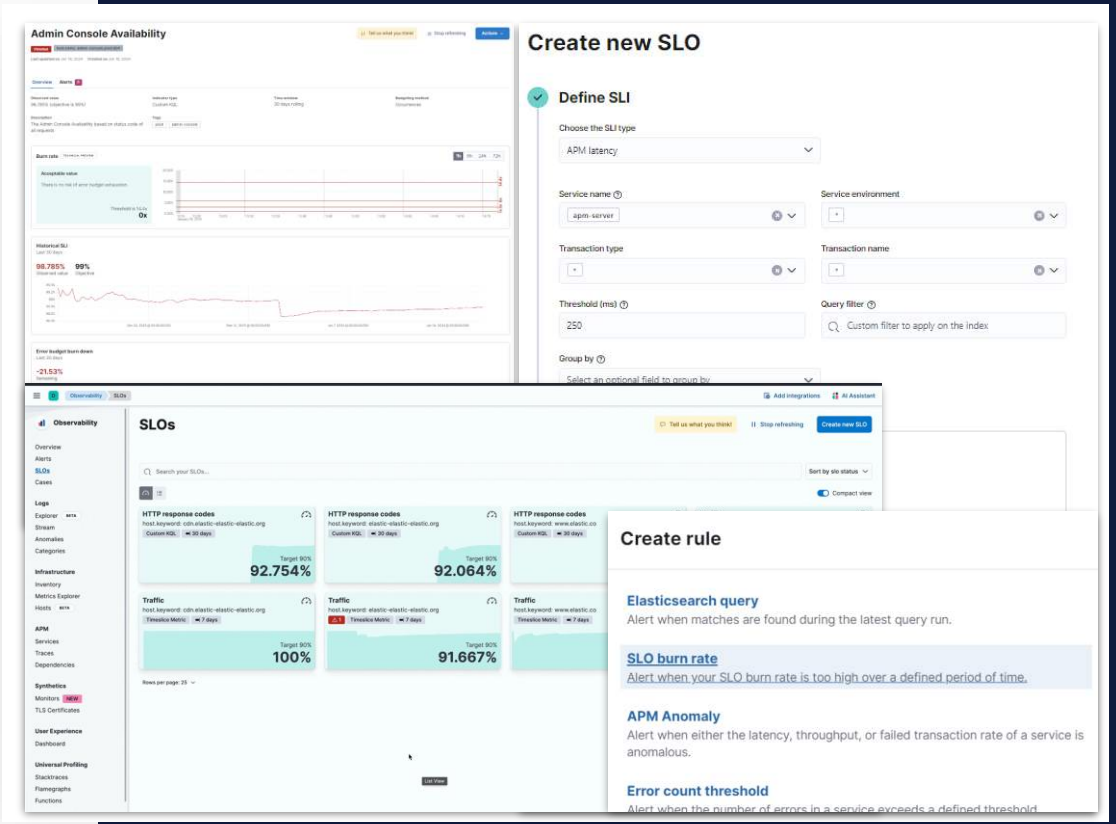
- Monitoring metryk architektury (cloud-native i 3-tier)
- 500+ integracji: AWS, Azure, i Google Cloud
- Kubernetes (on-prem lub w chmurze)
- Szybka izolacja problemów w złożonych architekturach



Elastic Observability

Zarzadzanie SLO

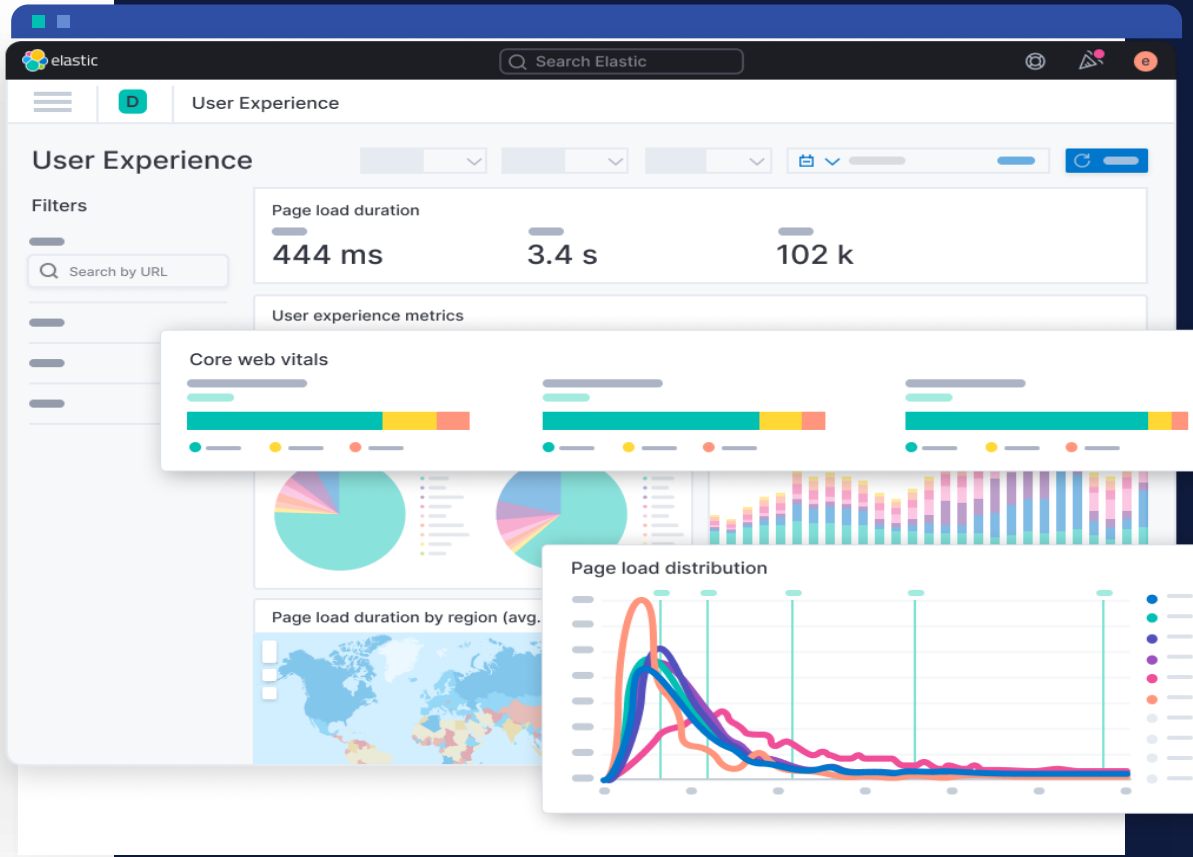
- Zapewnij niezawodność usług dzięki zarządzaniu SLO
- Definiuj i monitoruj biznesowe oraz operacyjne SLO/SLI
- Integrate SLOs and alerts widgets into dashboards to visualize alongside other KPIs



Elastic Observability

RUM & Syntetyczny Monitoring

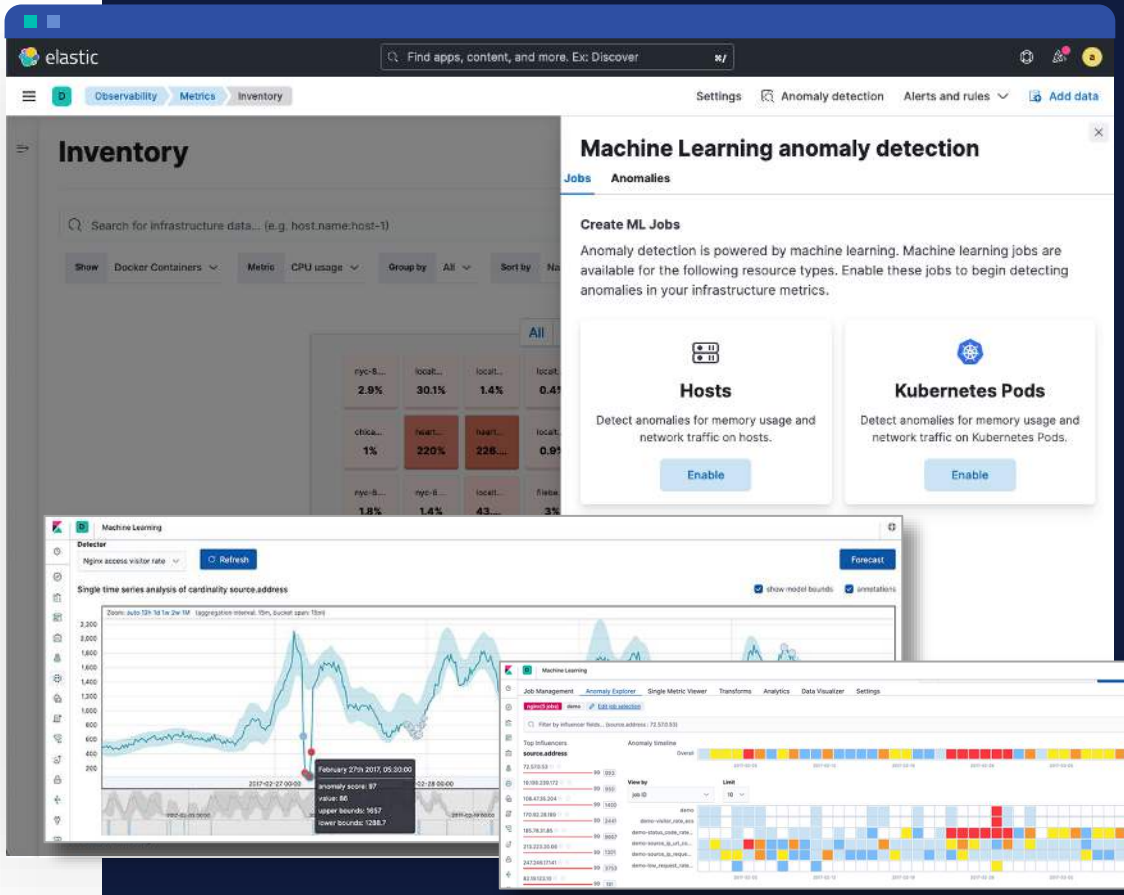
- Rzeczywiste doświadczenie użytkownik
- Analiza wydajności według lokalizacji i urządzeń



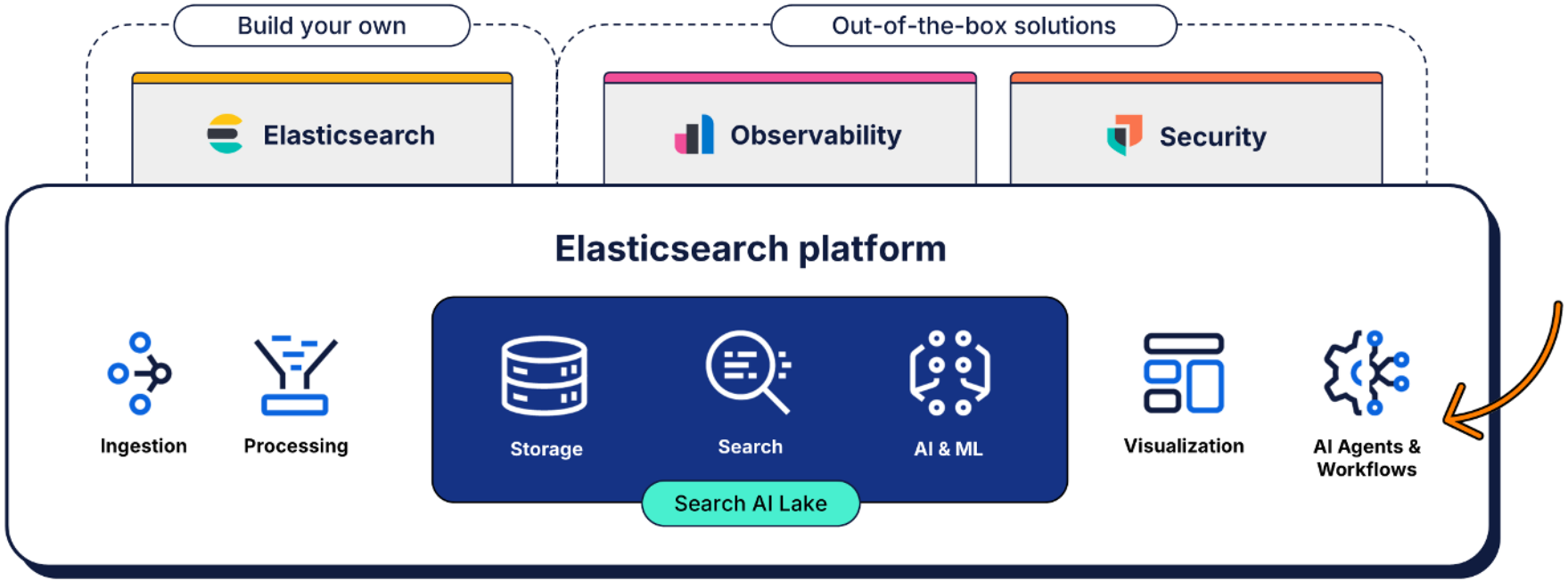
Elastic Observability

Jedna Platforma

- "Out-of-the-box" machine learning
- Wykrywanie anomalii i analiza przyczyn problemow oparta na AI dla wszystkich danych
- Automatyczne korelacje APM do znajdowania przyczyn awarii
- Skraca MTTD i MTTR



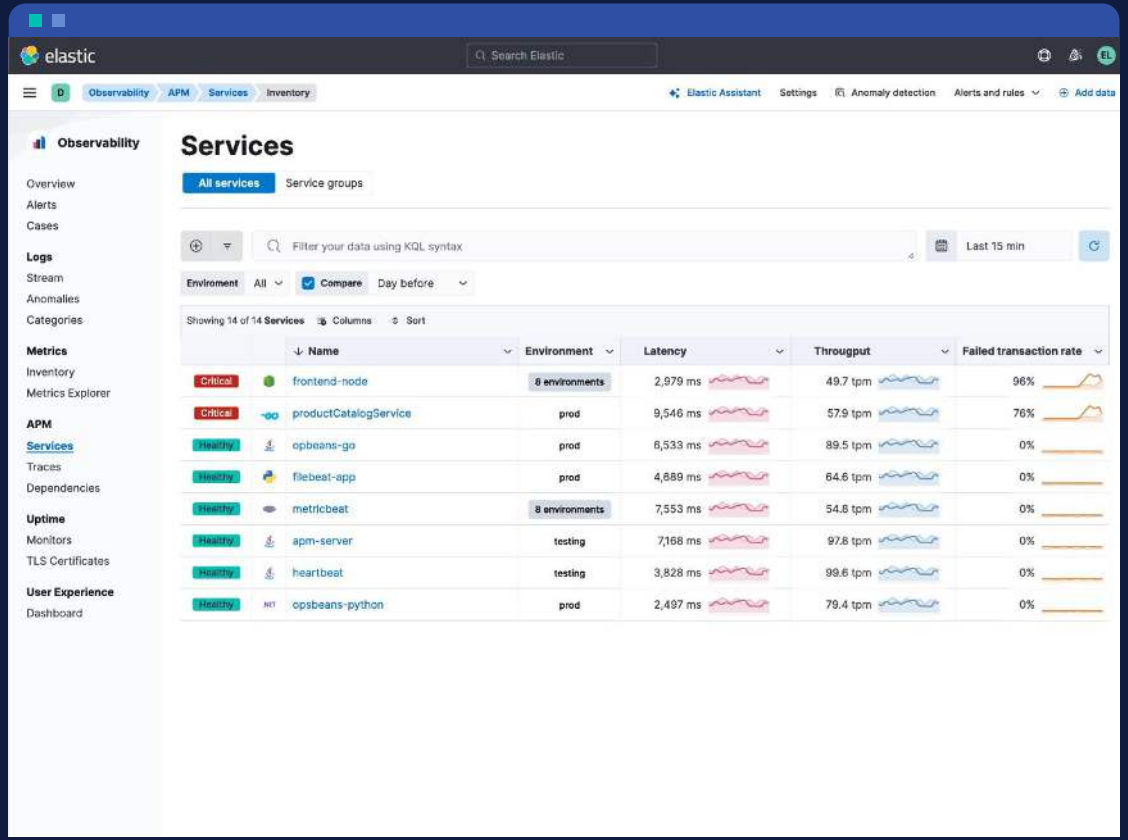
Elastic Workflows: Data, Context, and Action Unified

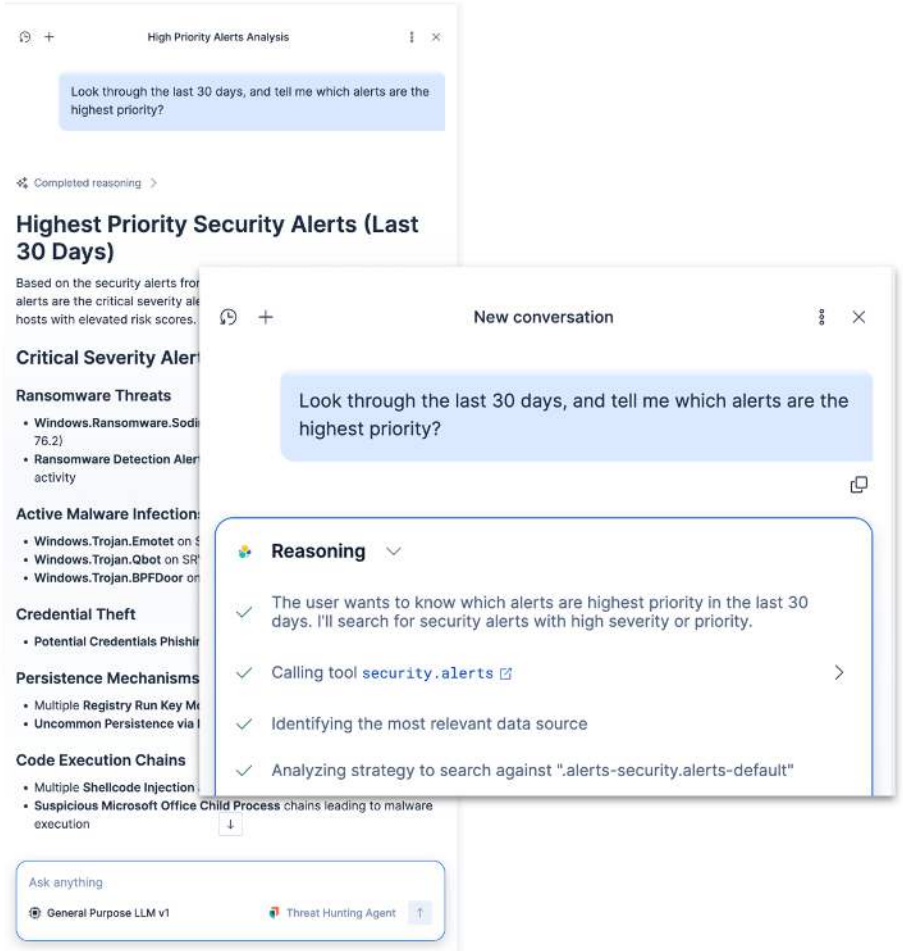


AI Assistant

Powered by ESRE Elasticsearch Relevance Engine™

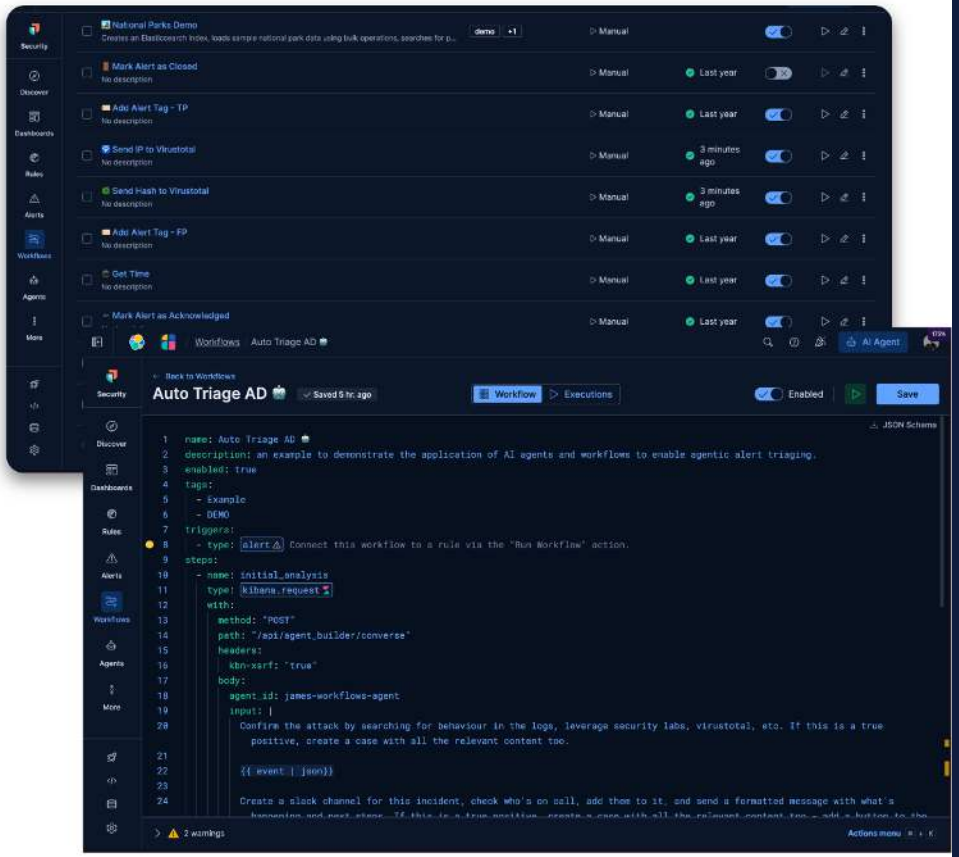
- Przyspiesz zarządzanie incydentami i analizę przyczyn źródłowych
- Interaktywnie eksploruj problemy i wdrażaj rozwiązania z wykorzystaniem generatywnej AI
- Wyniki dostosowane do kontekstu i specyfiki Twojego biznesu, którym możesz zaufać
- Oparte na Twoich własnych danych, dokumentach wewnętrznych, runbookach, raportach incydentów, …





Agent Builder (Threat Hunting Agent)

- **Przyspiesz Threat Hunting dzięki kolejnemu przełomowi w konwersacyjnej AI.**
- Wstępnie załadowany z narzędziami specyficznymi dla bezpieczeństwa, umożliwiającymi szybkie dochodzenia.
- Łatwo rozszerzalny poprzez dodawanie własnych narzędzi.
- Użytkownicy mogą definiować i wykorzystywać narzędzia, w tym:
  - **Zapytania ES|QL:** Definiuj i uruchamiaj ustrukturyzowane, zaawansowane wyszukiwania.
  - **Wyszukiwanie indeksów (Baza wiedzy):** Uzyskaj dostęp do kluczowej wiedzy i kontekstu bezpieczeństwa.
  - **Przepływy pracy:** Natychmiast uruchamiaj zautomatyzowane działania naprawcze.



Workflows

Dane, Kontekst i Działanie
Elastic Workflows Automation wbudowany w platformę Elasticsearch.

- Definiuj automatyzację reagującą na zdarzenia (takie jak alerty),
- Łącz automatyzację opartą na regułach z agentami AI, aby automatyzować zarówno rutynowe, jak i złożone zadania .
- Żadnych zewnętrznych narzędzi. Żadnych dodatkowych kosztów integracji.

Typowa ścieżka adaptacji klienta

elastic

Wyniki i mierzalny wpływ

70%

Redukcja czasu na monitoring i rozwiązywanie incydentów
(z dni do minut)

Ok 60%

mniej false positives

(dzięki korelacji ML)

5x

szybsza Root Cause Analysis

(jeden interfejs, pełny kontekst)

ROI dla zarządu

Koszt 1 incydentu

4,88 mln $ — średni globalny koszt naruszenia danych
6,08 mln $ — sektor finansowy
+ koszty reputacyjne, kary regulatora (GDPR/DORA)

vs.

Koszt Observability platformy

Ułamek kosztu jednego incydentu
+ wartość operacyjna i regulacyjna

Źródło: Elastic Customer Success Stories; Forrester TEI Study of Elastic Observability 2023, Ponemon Cost of a Data Breach 2024

Widzisz więcej, reagujesz szybciej.

Kluczowe wnioski

- Silosy danych
- Observability ≠ monitoring
- Szybka reakcja wymaga pełnej obserwowalności

Jeśli masz pytania – skontakuj się z prowadzącymi

Łukasz Grudzień
Security Management Team Leader
Integrity Partners
Tel: +48 664 126 755
lukasz.grudzien@integritypartners.pl

Michał Stasiak
Senior Solution Architect
Elastic
Tel:+48 534090481
michal.stasiak@elastic.co