



Widzisz więcej, reagujesz szybciej

Elastic Observability jako fundament
bezpieczeństwa operacyjnego banku



Co może pójść nie tak? Ogromne koszty każdej awarii...

\$65

millionów

Utrata przychodu

Social Media

£330

milionów

Całkowity koszt awarii
(wg niezależnego raportu)

Bank

>\$5M

Na godzinę

Średni koszt awarii

Financial Sector

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

Stan obecny: rozproszone narzędzia i silosy danych

Źródła danych

Core Banking

Systemy płatności

Infrastruktura IT

Kanały cyfrowe

Workstations

Narzędzia (bez integracji)

SIEM

Nagios/Zabbix

Syslog

APM Tool

Ticket System

Excel / e-mail

Efekt



Brak
widoczności



Wolna
reakcja



Silosy
wiedzy

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

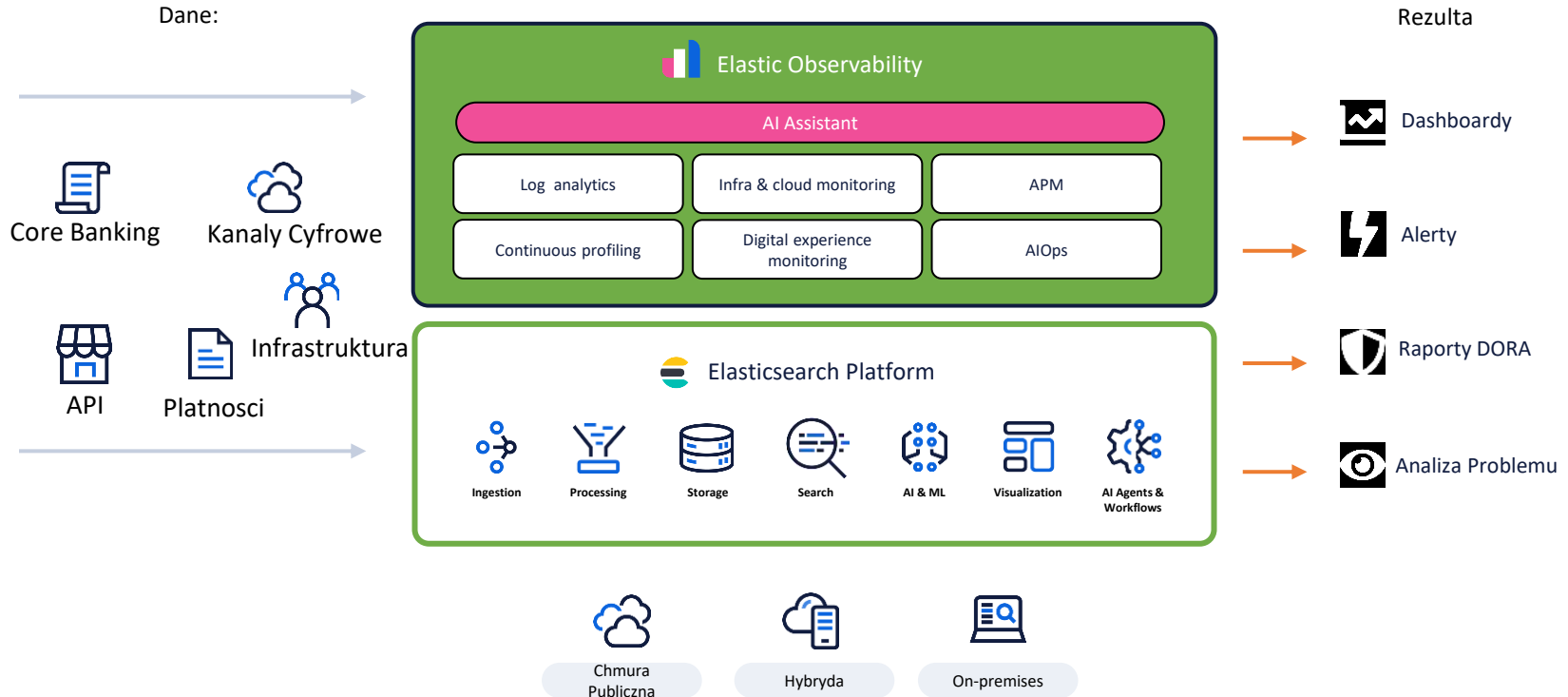
Jak system się zachowuje

Traces

Gdzie jest problem w RT

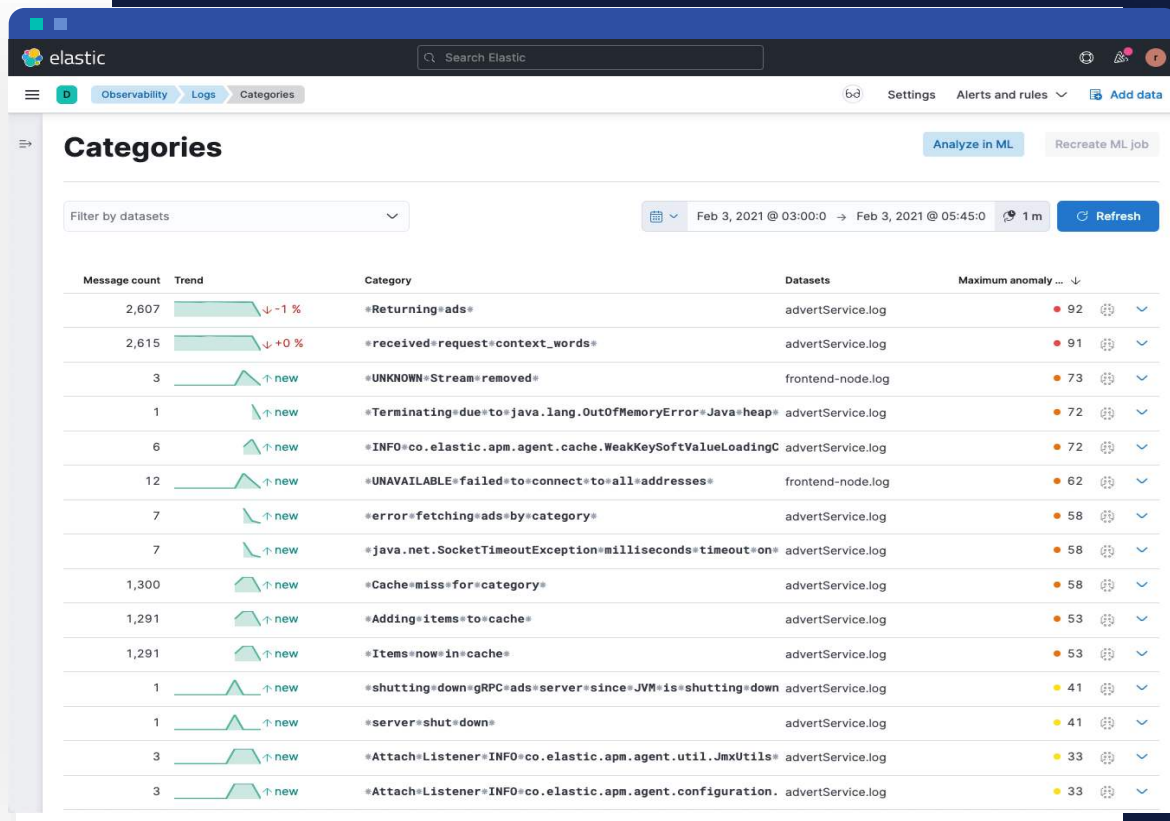
Elastic Observability

Ujednolicony pipeline danych



Log Analytics

- Centralne zarządzanie logami
- Korelacja zdarzeń i alertowanie

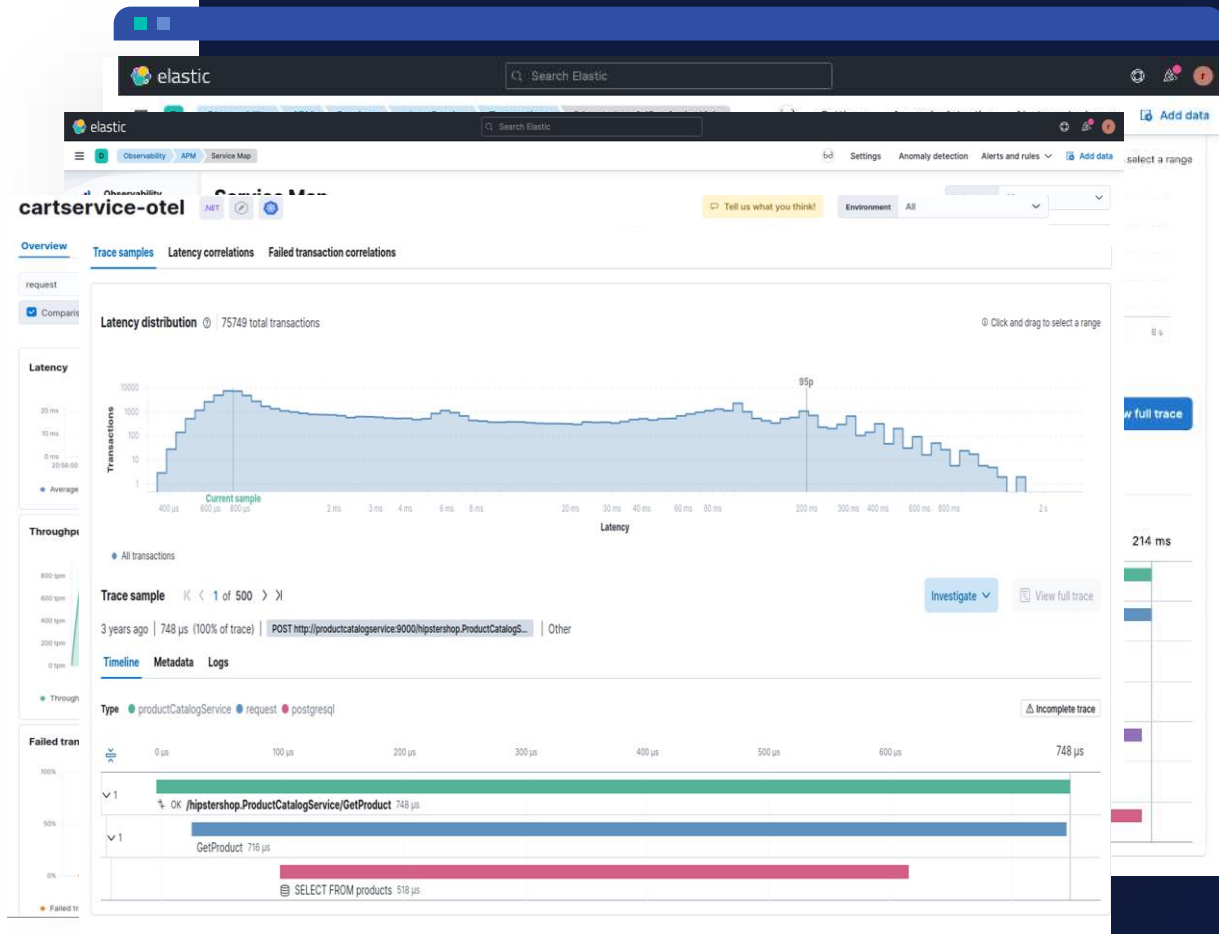


The screenshot shows the Elastic Observability interface for Log Analytics. The main view is titled "Categories" and displays a list of log categories with their message counts, trends, and anomaly scores. The interface includes a search bar, navigation tabs for "Observability", "Logs", and "Categories", and a "Refresh" button. The data is presented in a table with columns for Message count, Trend, Category, Datasets, and Maximum anomaly.

Message count	Trend	Category	Datasets	Maximum anomaly ... ↓
2,607	↓ -1 %	*Returning=ads*	advertService.log	92
2,615	↓ +0 %	*received=request=context_words*	advertService.log	91
3	↑ new	*UNKNOWN=Stream=removed*	frontend-node.log	73
1	↑ new	*Terminating=due=to=java.lang.OutOfMemoryError=Java=heap*	advertService.log	72
6	↑ new	*INFO=co.elastic.apm.agent.cache.WeakKeySoftValueLoadingC	advertService.log	72
12	↑ new	*UNAVAILABLE=failed=to=connect=to=all=addresses*	frontend-node.log	62
7	↑ new	*error=fetching=ads=by=category*	advertService.log	58
7	↑ new	*java.net.SocketTimeoutException=milliseconds=timeout=on*	advertService.log	58
1,300	↑ new	*Cache=miss=for=category*	advertService.log	58
1,291	↑ new	*Adding=items=to=cache*	advertService.log	53
1,291	↑ new	*Items=now=in=cache*	advertService.log	53
1	↑ new	*shutting=down=gRPC=ads=server=since=JVM=is=shutting=down	advertService.log	41
1	↑ new	*server=shut=down*	advertService.log	41
3	↑ new	*Attach=Listener=INFO=co.elastic.apm.agent.util.JmxUtils*	advertService.log	33
3	↑ new	*Attach=Listener=INFO=co.elastic.apm.agent.configuration.	advertService.log	33

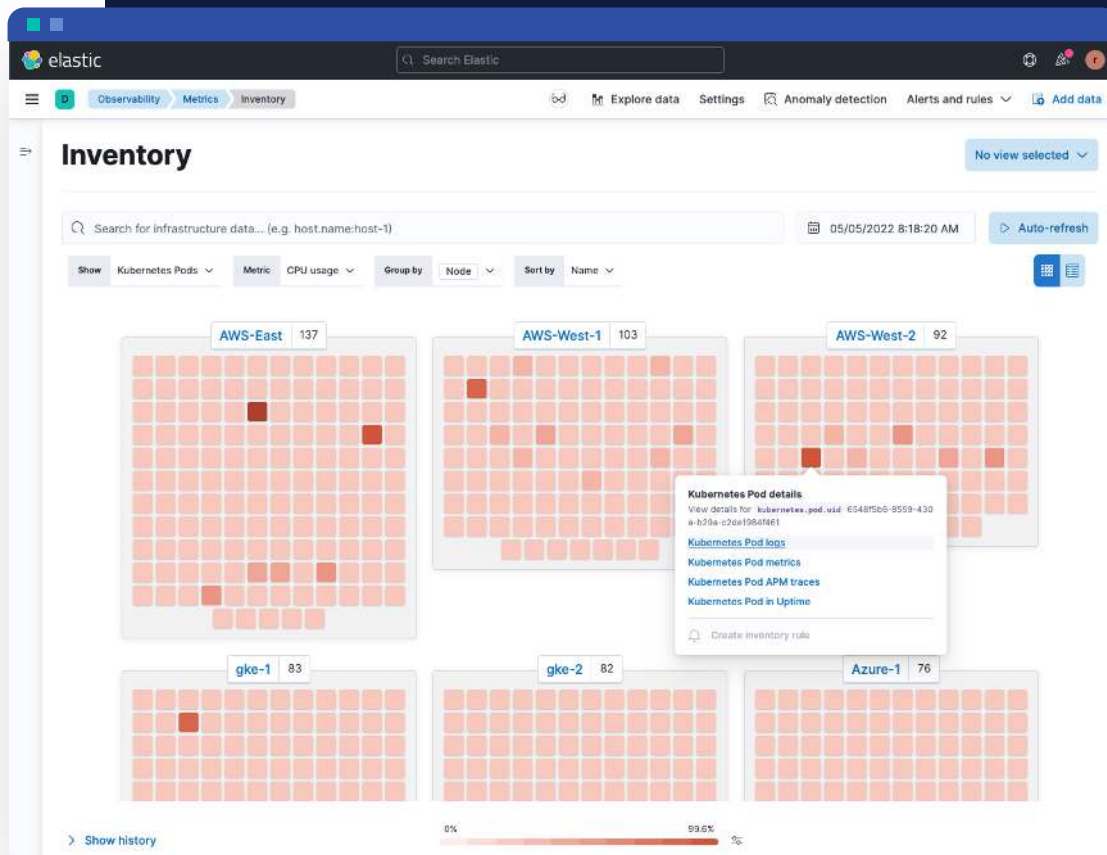
APM

- 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



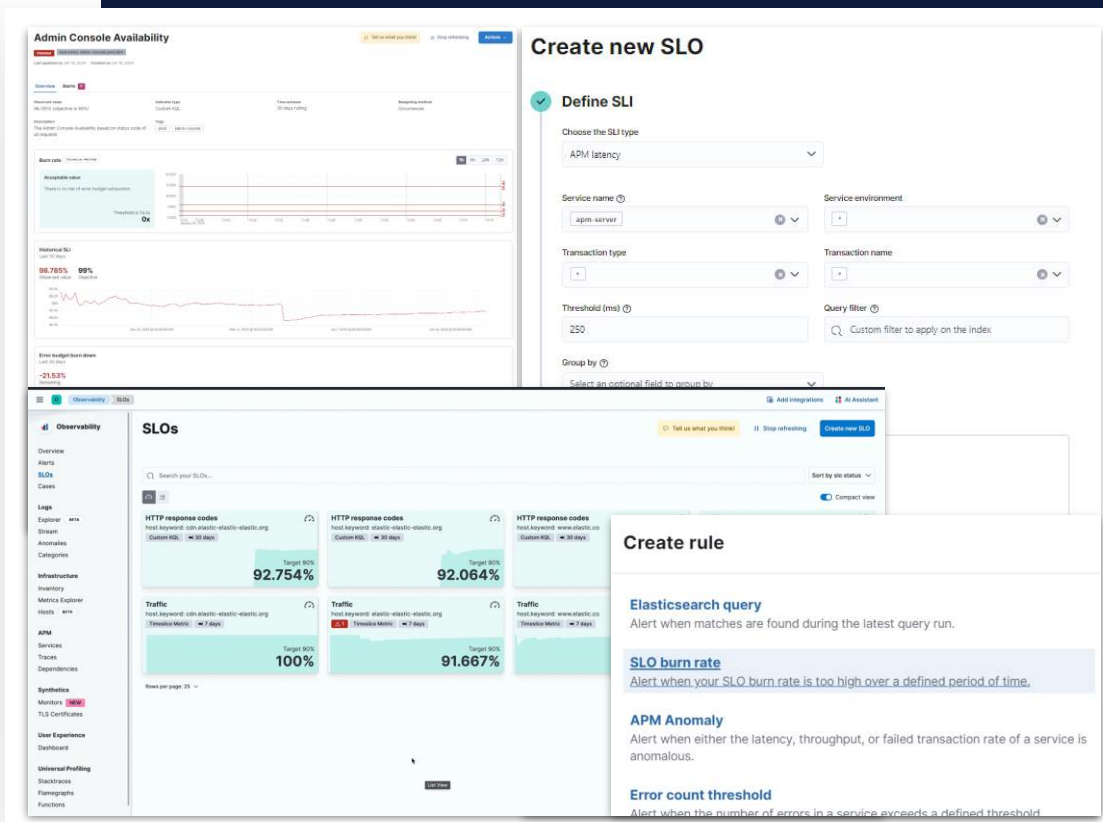
Infrastruktura

- 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



Zarządzanie SLO

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



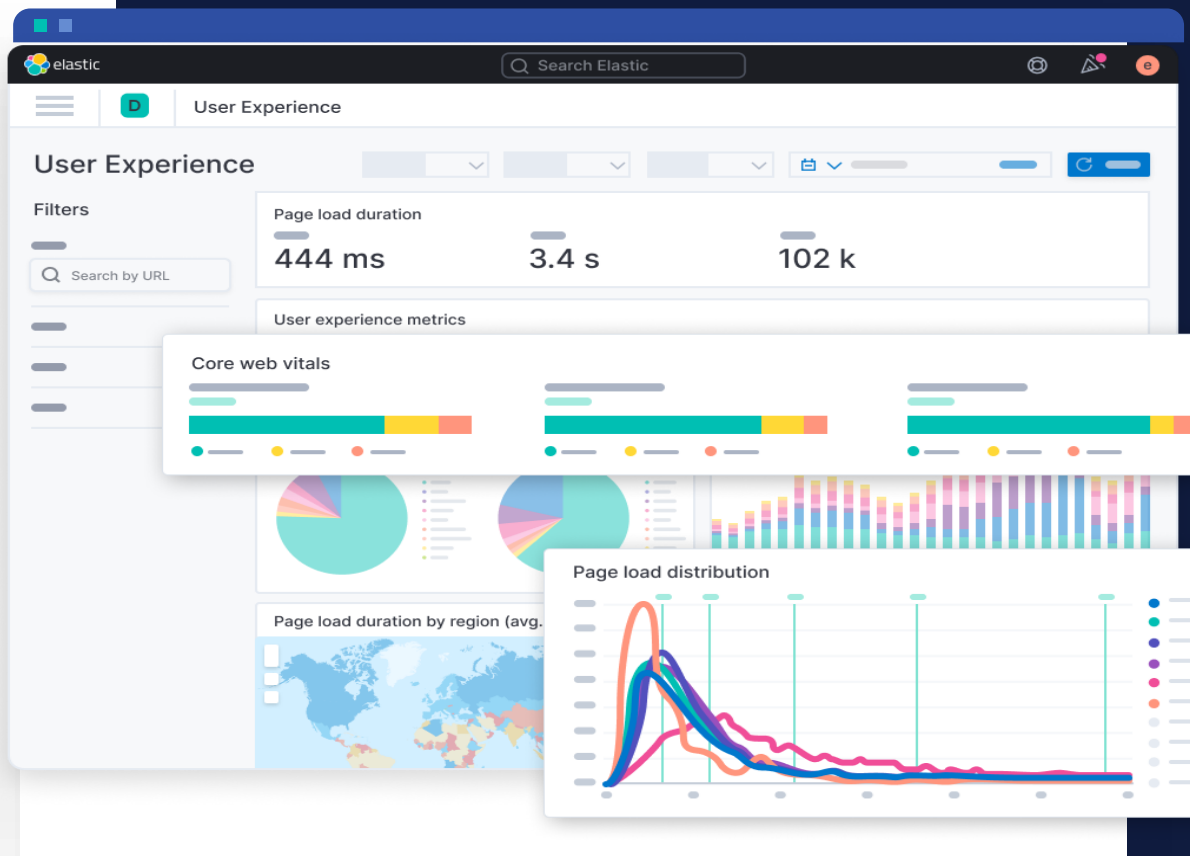
The screenshot displays the Elastic Observability SLO management interface, divided into three main sections:

- Admin Console Availability:** Shows a graph of availability over time with a target line and a current value of 99%. Below the graph, it indicates a budget burndown of -21.53%.
- Create new SLO:** A form for defining a new SLO. The "Define SLI" section is active, showing "APM latency" as the chosen SLI type. Other fields include "Service name" (apm-server), "Service environment", "Transaction type", "Transaction name", "Threshold (ms)" (250), and "Query filter" (Custom filter to apply on the index).
- SLOs Dashboard:** A grid of SLO widgets. The "SLOs" section is active, showing a search bar and a "Create new SLO" button. The dashboard displays several SLOs with their current values and target percentages:
 - HTTP response codes (host:keyword@elastic-elastic-elastic.org): 92.754% (Target 90%)
 - HTTP response codes (host:keyword@elastic-elastic-elastic.org): 92.064% (Target 90%)
 - Traffic (host:keyword@elastic-elastic-elastic.org): 100% (Target 90%)
 - Traffic (host:keyword@elastic-elastic-elastic.org): 91.667% (Target 90%)

On the right side, a "Create rule" section is visible, showing options for "Elasticsearch query", "SLO burn rate", "APM Anomaly", and "Error count threshold".

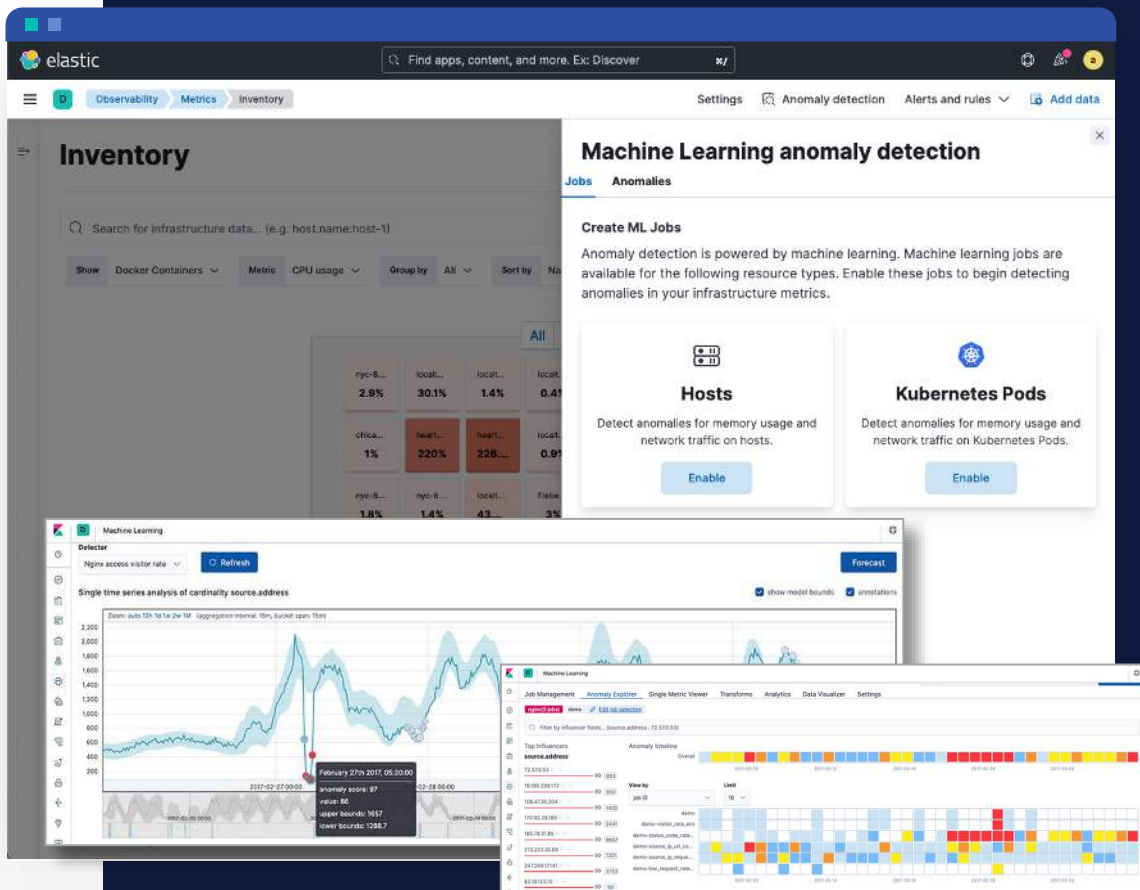
RUM & Syntetyczny Monitoring

- Rzeczywiste doświadczenie użytkownik
- Analiza wydajności według lokalizacji i urządzeń

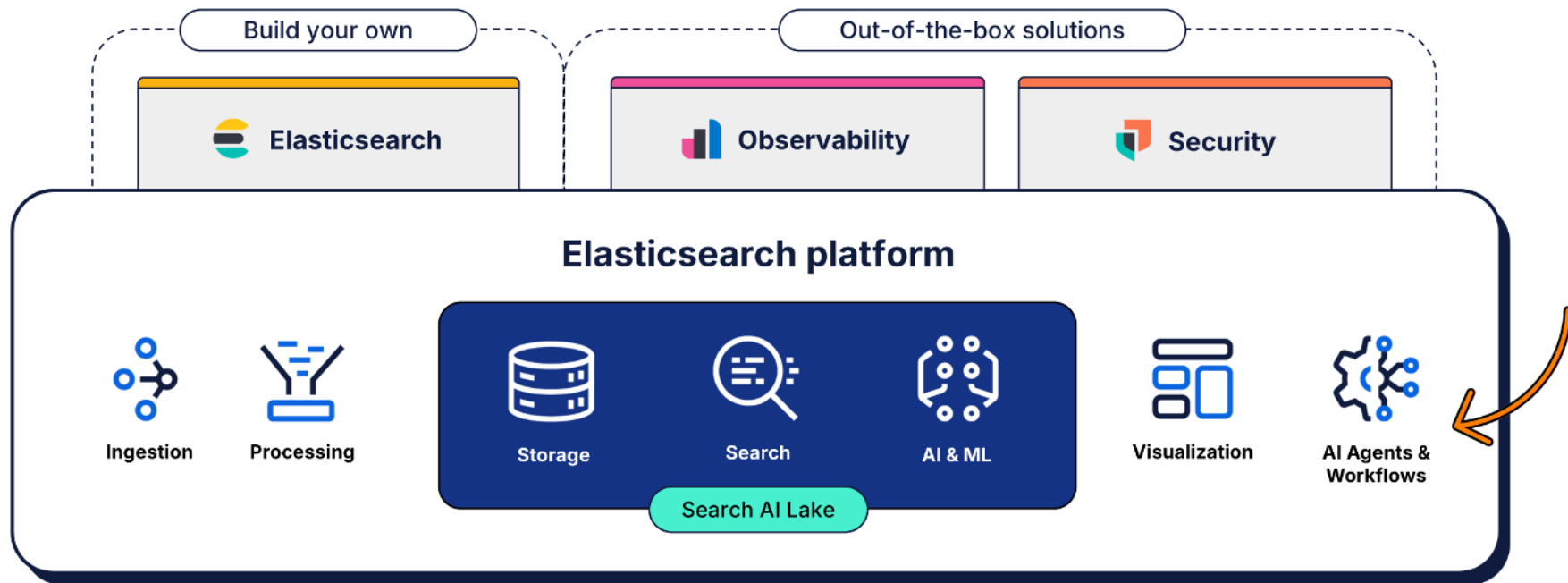


Jedna Platforma

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



Elastic Workflows: Data, Context, and **Action** Unified



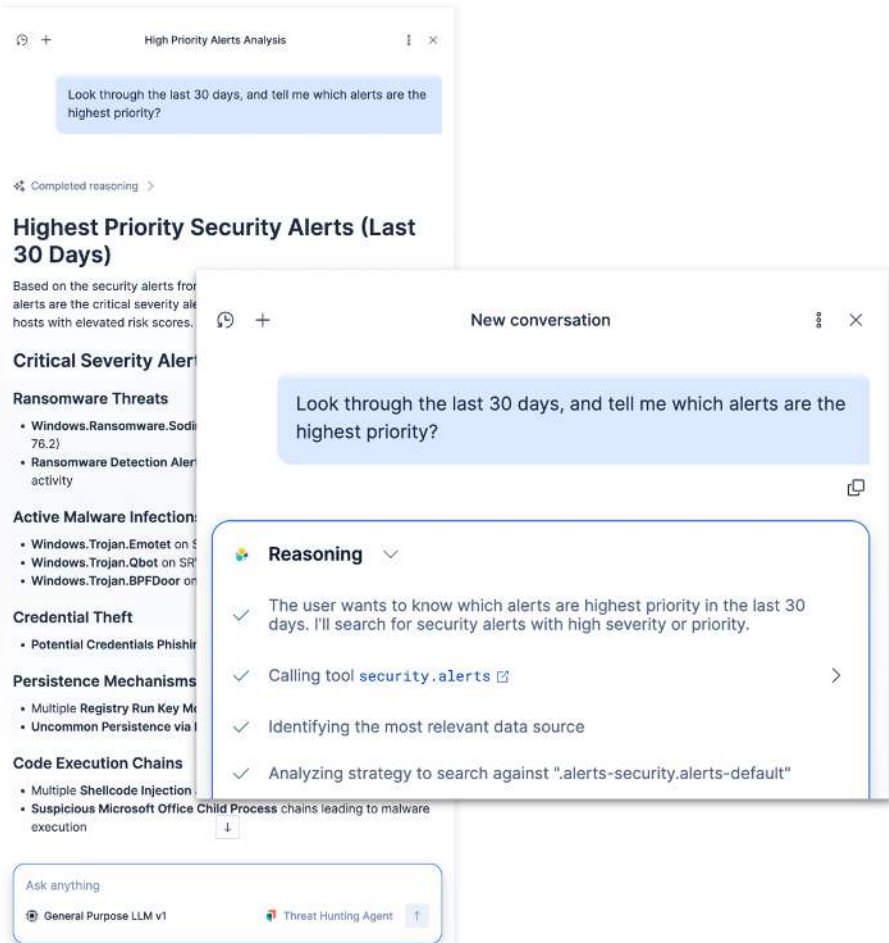
AI Assistant

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, ...

The screenshot displays the Elastic Observability 'Services' page. The interface includes a navigation menu on the left with options like Overview, Alerts, Cases, Logs, Stream, Anomalies, and Categories. The main content area shows a table of services with the following data:

Name	Environment	Latency	Throughput	Failed transaction rate
frontend-node	8 environments	2,979 ms	49.7 tpm	96%
productCatalogService	prod	9,546 ms	57.9 tpm	76%
opbeans-go	prod	6,533 ms	89.5 tpm	0%
filebeat-app	prod	4,889 ms	64.6 tpm	0%
metricbeat	8 environments	7,553 ms	54.8 tpm	0%
apm-server	testing	7,168 ms	97.8 tpm	0%
heartbeat	testing	3,828 ms	99.6 tpm	0%
opsbeans-python	prod	2,497 ms	79.4 tpm	0%



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.

The screenshot displays the Elastic Security interface. The top section shows a list of workflows, including 'National Parks Demo', 'Mark Alert as Closed', 'Add Alert Tag - TP', 'Send IP to VirusTotal', 'Send Hash to VirusTotal', 'Add Alert Tag - FP', 'Get Time', and 'Mark Alerts as Acknowledged'. Each workflow entry includes a status indicator (e.g., 'Last year', '3 minutes ago') and a toggle switch.

The bottom section shows the configuration for the 'Auto Triage AD' workflow. The configuration is as follows:

```
1 name: Auto Triage AD
2 description: an example to demonstrate the application of AI agents and workflows to enable agentic alert triaging.
3 enabled: true
4 tags:
5   - example
6   - DEMO
7 triggers:
8   - type: alert
9 steps:
10  - name: initial_analysis
11    type: kibana_request
12    with:
13      method: "POST"
14      path: "/api/agent_builder/converse"
15      headers:
16        | kbn-xsrf: "true"
17      body:
18        | agent_id: james-workflows-agent
19        | input: |
20          | Confirms the attack by searching for behaviour in the logs, leverage security labs, virustotal, etc. If this is a true
21          | positive, create a case with all the relevant content too.
22          |
23          | {{ event | toJson }}
24
25 Create a slack channel for this incident, check who's on call, add them to it, and send a formatted message with what's
26 happened, and mock some... If this is a true positive, create a case with all the relevant content too, add a button to the
```

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.

Zacznij z:
Log analytics

1

2

Rozwijaj o:
+ APM
+ Infrastructure
+ Digital experience
(RUM + Synthetics)

3

Rozwijaj o:
Observability for Customer
Experiences

2

1

Zacznij z:
Search apps

Rozwijaj o:
DevSecOps

3

2

Rozwijaj o:
+ Endpoint
+ Cloud
+ XDR

1

Zacznij z:
SIEM

3

Rozwijaj o:
Trusted Customer
Experiences

Typowa ścieżka adaptacji klienta

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



Widzisz więcej, reagujesz szybciej.

Kluczowe wnioski

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



Jeśli masz pytania – skontaktuj 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