

Nowoczesne podejście do cyberobrony - Obserwowalność i bezpieczeństwo jako jedna platforma

Powered by

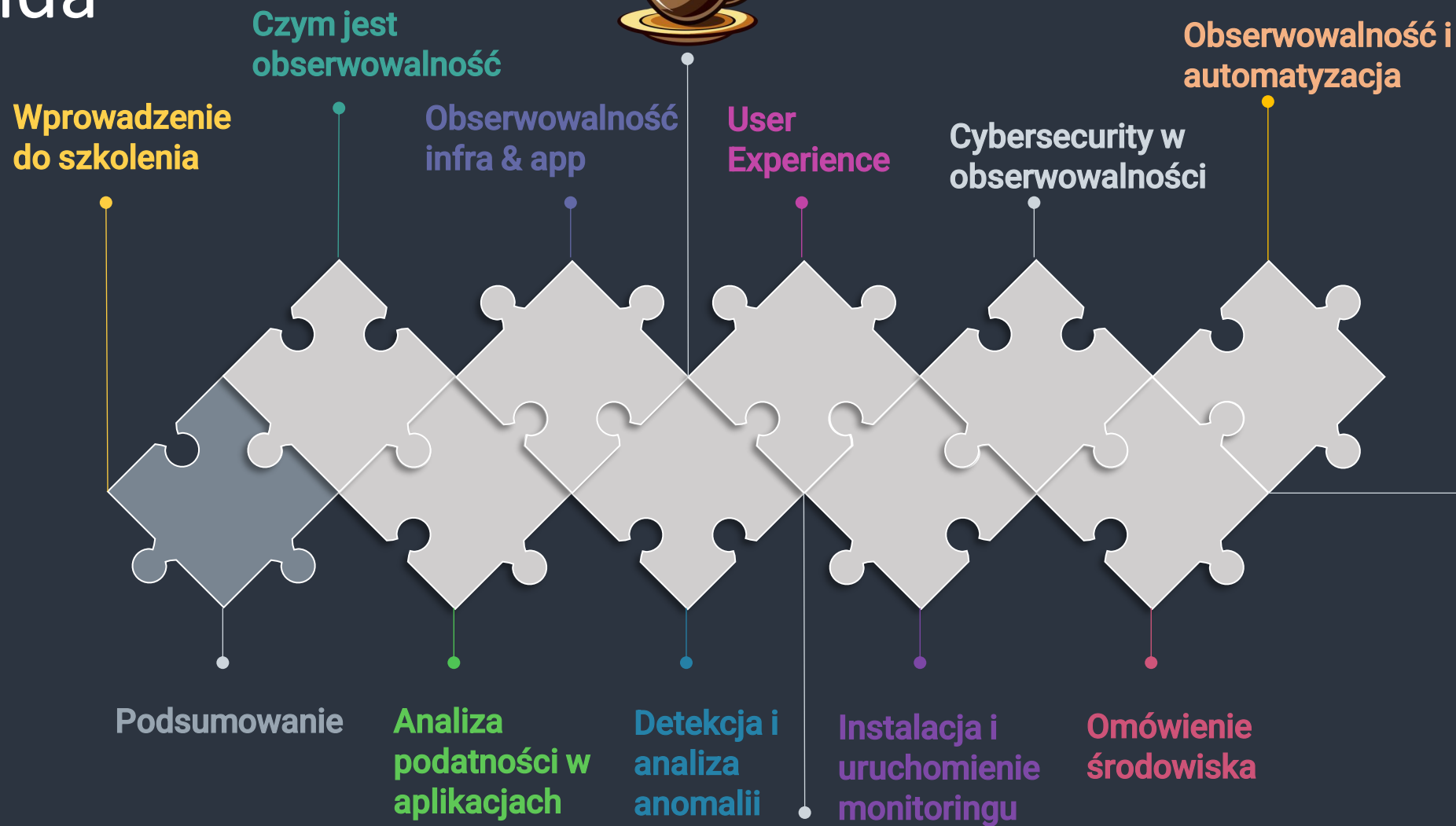
OMNILOGY

Dariusz Ziębicki
Tomasz Płoński



omnilogy

Agenda



Przedstawienie celu szkolenia



Krótkie omówienie poziomu wiedzy uczestników



Czym jest obserwowalność?

Obserwowalność czyli Observability pochodzi z teorii sterowania i inżynierii systemów. Oznacza zdolność do zrozumienia stanu wewnętrznego systemu na podstawie jego danych wyjściowych. W praktyce, szczególnie w informatyce i zarządzaniu systemami IT, odnosi się do możliwości monitorowania, analizowania i diagnozowania problemów w systemach, aplikacjach lub infrastrukturze.

o11y

Czym jest obserwowalność?

Obserwowalność != Monitoring 2.0

Monitoring bazuje na statycznym podejściu – przewidujemy, gdzie może nastąpić awaria i przygotowujemy się do tego konfigurując dashboardy i alarmy.

Obserwowalność bazuje na dynamicznej ocenie różnych sygnałów w celu określenia, jaki jest faktyczny stan system z możliwością wykrycia anomalii i dalszego wskazania źródła w szybkozmiennym środowisku.

o11y

Cele obserwowalności

Cele obserwowalności

1. Identyfikacja problemów i błędów

pomaga szybko wykrywać problemy w systemie (awarie, błędy czy spadki wydajności) – minimalizuje przestoje.

2. Szybkie rozwiązywanie incydentów

pomaga dogłębnie diagnozować źródła problemów i błędów oraz szybko je eliminować.

3. Zrozumienie zależności między komponentami

W złożonych systemach umożliwia identyfikację i analizę interakcji między różnymi usługami czy komponentami.

4. Monitorowanie wydajności

Śledzi kluczowe wskaźniki wydajności systemu (np. opóźnienia, przepustowość, wykorzystanie zasobów).

5. Przewidywanie potencjalnych problemów

Identyfikuje trendy prowadzące do przyszłych problemów, zmienia podejście z reaktywnego na proaktywne.

Źródła danych

Automatyzacja

Cele obserwowalności

Cele
obserwowalności

6. Zwiększenie dostępności systemu

Stale monitoruje i natychmiast reaguje na problemy - wspiera utrzymanie wysokiej dostępności usług.

Źródła danych

7. Zapewnienie lepszego doświadczenia użytkownika (UX)

Wykrywa i pomaga w rozwiązywaniu problemów z wydajnością i dostępnością - system a. działa, b. działa płynniej, co przekłada się na lepsze doświadczenia użytkowników końcowych.

Automatyzacja

8. Wsparcie w analizie wpływu zmian (rollback/rollforward)

Pokazuje wpływ wdrożonych zmian w kodzie lub konfiguracji na system, co jest kluczowe w procesie CI/CD.

9. Wykrywanie anomalii i zagrożeń bezpieczeństwa

Śledzenie nietypowych wzorców i zachowań umożliwia identyfikację potencjalnych zagrożeń oraz ochronę systemu przed atakami.

10. Optymalizacja kosztów przez monitorowanie użycia zasobów i funkcji biznesowych.

Źródła danych



Źródła danych

Metryki	Dane numeryczne opisujące system – czasy odpowiedzi, ilości req. http, % użycia CPU
Logi	Wpisy w plikach dzienników np. mikrouslug, access.log
Ślady	Przebiegi transakcji przez komponenty systemów
Zdarzenia	Informacje o tym, co wydarzyło się w systemie
Metadane	Dane opisujące obserwowane komponenty i inne dane
Sieć	Parametry jakościowe i logiczne wykorzystania sieci
Zachowanie	Sposoby integracji użytkowników lub systemów z aplikacjami
Kod	Widoczność wykonywanego kodu aplikacji na poziomie metod
Topologia	Zależności między komponentami na poziomie fizycznym i logicznym

Sposoby pozyskiwania danych

Agenci

Wyspecjalizowane komponenty integrujące się z monitorowanymi systemami i pozyskujący dane z wewnątrz aplikacji lub serwerów

OpenTelemetry

Otwarty standard, w którym programiści mogą wysyłać dane telemetryczne do systemów monitorujących

Exportery i integracje z API

Zdalne odpytywanie komponentów o dane telemetryczne

Log forwardery

Programy wysyłające pliki dzienników do systemów monitorujących

Wbudowane narzędzia chmurowe

Zwłaszcza w chmurze publicznej dedykowane usługi zbierające dane z chmury z możliwością ich udostępnienia

SNMP

Zbieranie danych przez protokół SNMP

Sesje użytkowników

Dane zbierane z końcówek użytkowników

Automatyzacja - obszary

Pozyskiwanie
danych

Wykrywanie
anomalii

Analiza źródła

Działania
naprawcze
sterowane
danymi

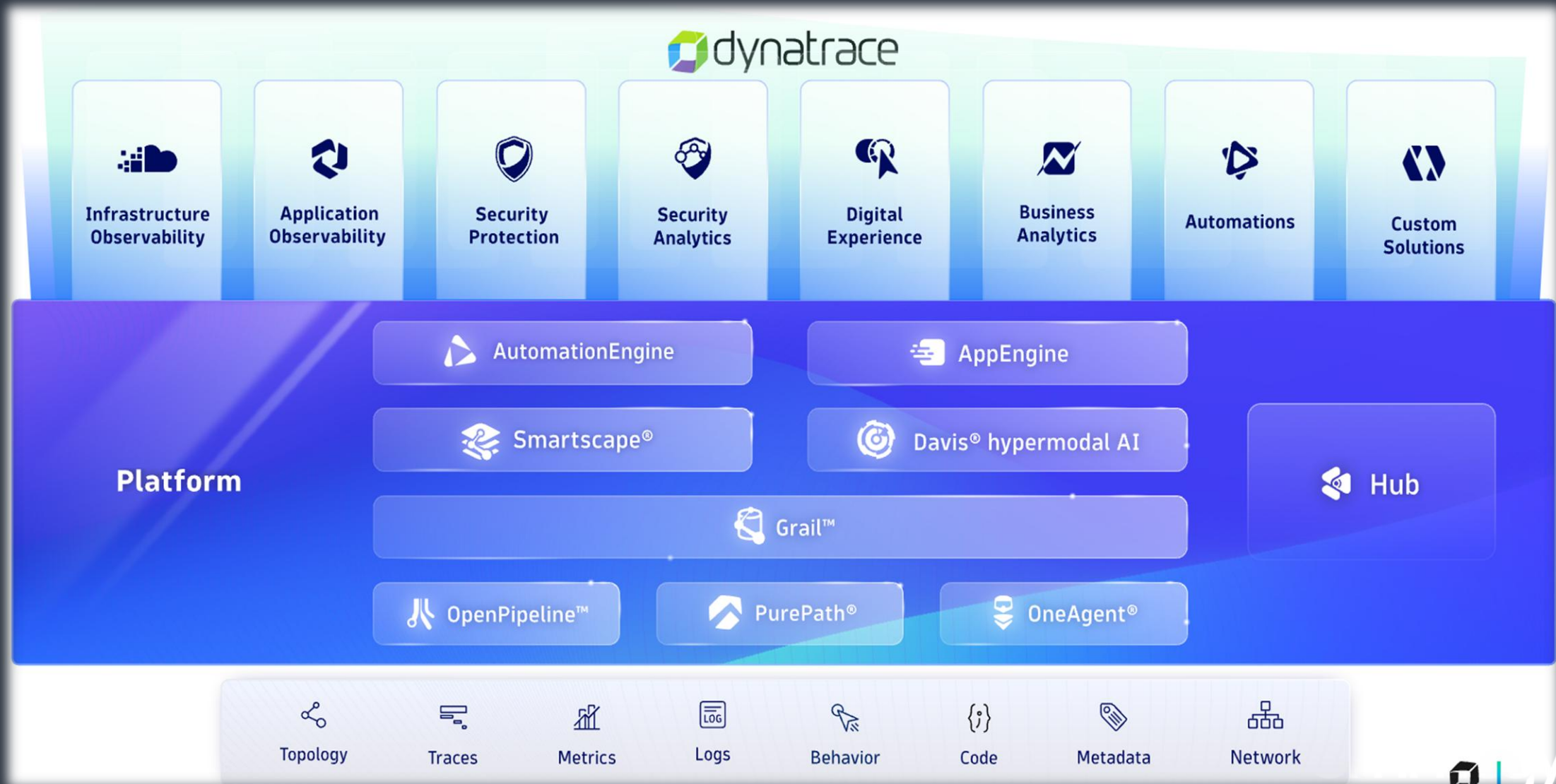
Czym jest
obserwowalność

Cele
obserwowalności

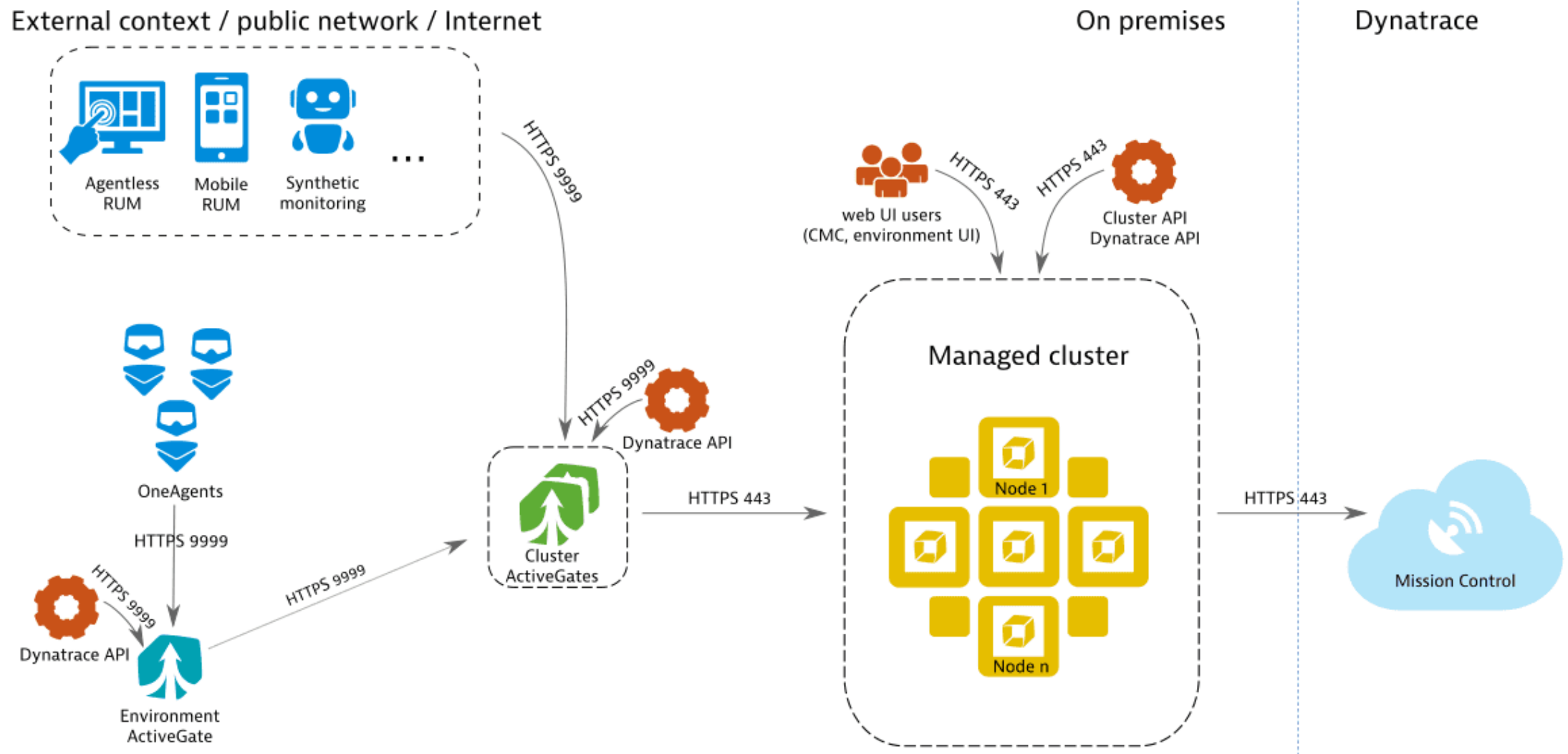
Źródła danych

Automatyzacja

Zautomatyzowana platforma Obserwowalności



Dynatrace Managed



Dostarczenie danych

OneAgent

Jest odpowiedzialny za zbieranie wszystkich sygnałów telemetrycznych w monitorowanym środowisku. Jeden OneAgent na host jest wymagany, aby zebrać wszystkie istotne dane monitorujące – nawet jeśli aplikacje są wdrożone w kontenerach Docker, architekturze mikrouslug w k8s lub infrastrukturze opartej na chmurze.



Dostarczenie
danych

Smartscape

Infrastruktura
onPrem

Infrastruktura
chmurowa

Kubernetes

Usługi

Analiza
problemów

Applications
2

Services
13

Processes
11

Hosts
1

Data centers
0

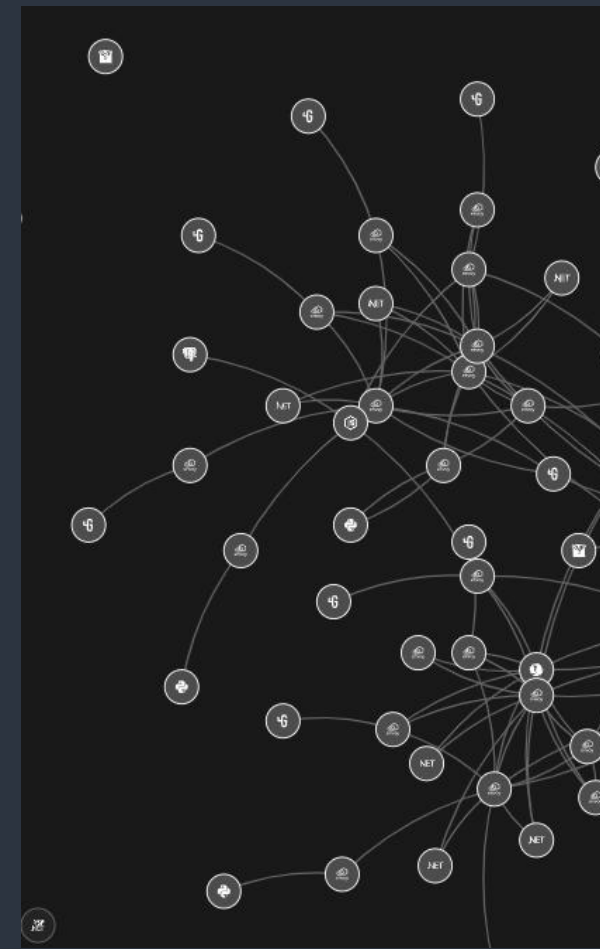
Smartscape

To technologia wizualizacji topologii środowiska w czasie rzeczywistym. Jest jedną z najpotężniejszych funkcji Dynatrace zasilającą silnik AI Davis wykrywający i analizujący anomalie.

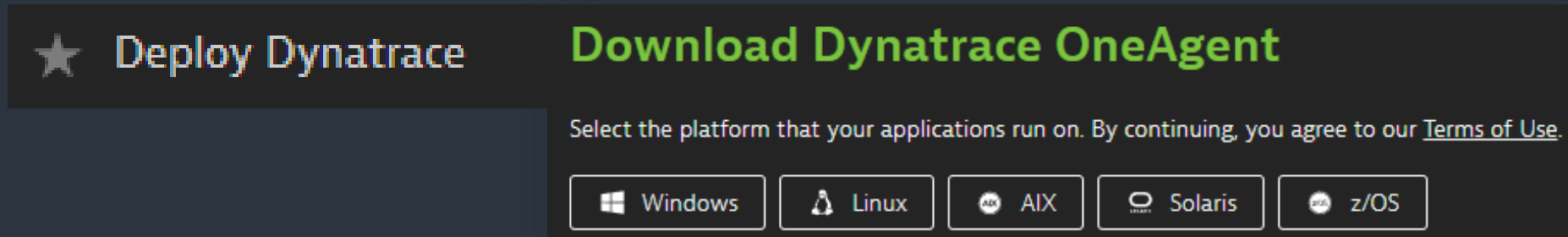
Automatyczne wykrywanie komponentów wykonywane jest na warstwach:

- Aplikacji
- Usług
- Procesów
- Hostów
- Centrum danych

Model buduje zależności pionowe oraz poziome, między komponentami tego samego typu.



Infrastruktura OnPrem

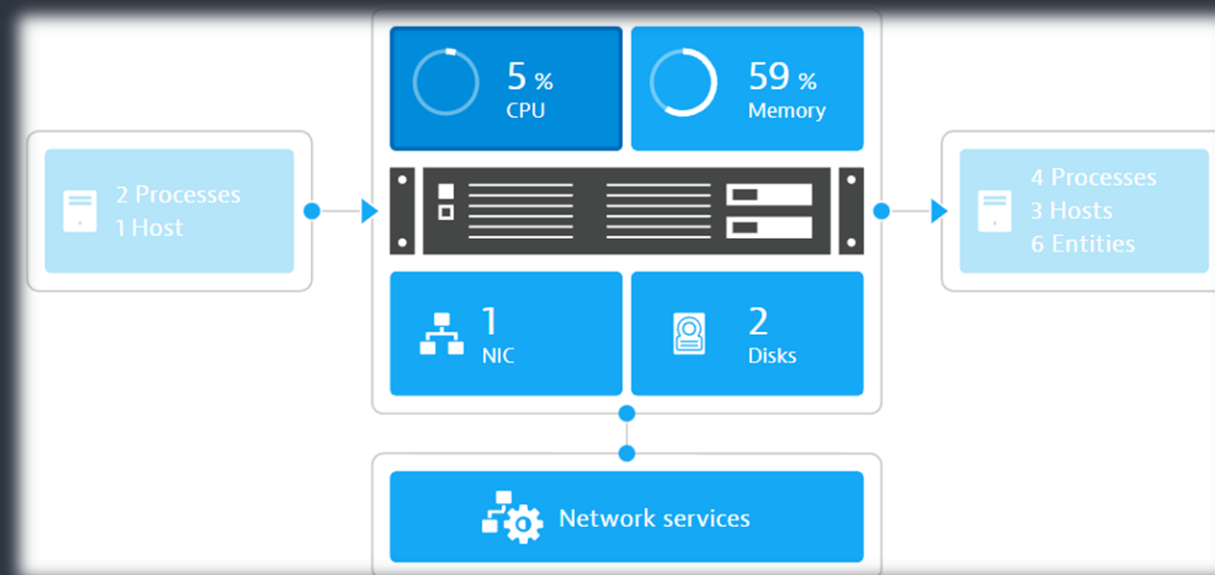


OneAgent instalowany jest na serwerach (wg OS).

Nie jest wymagana żadna konfiguracja.

Do osiągnięcia pełnej funkcjonalności wymagany jest restart procesów – wtedy następuje instrumentacja kodu aplikacji i włącza się głęboki monitoring

Infrastruktura OnPrem



Z perspektywy infrastrukturalnej zbierane są dane odnośnie całego serwera, działających na nim procesów, dysków, jakości sieci, komunikacji z innymi serwerami i procesami oraz logi.

Infrastruktura chmurowa

Dostarczenie
danych

Smartscape

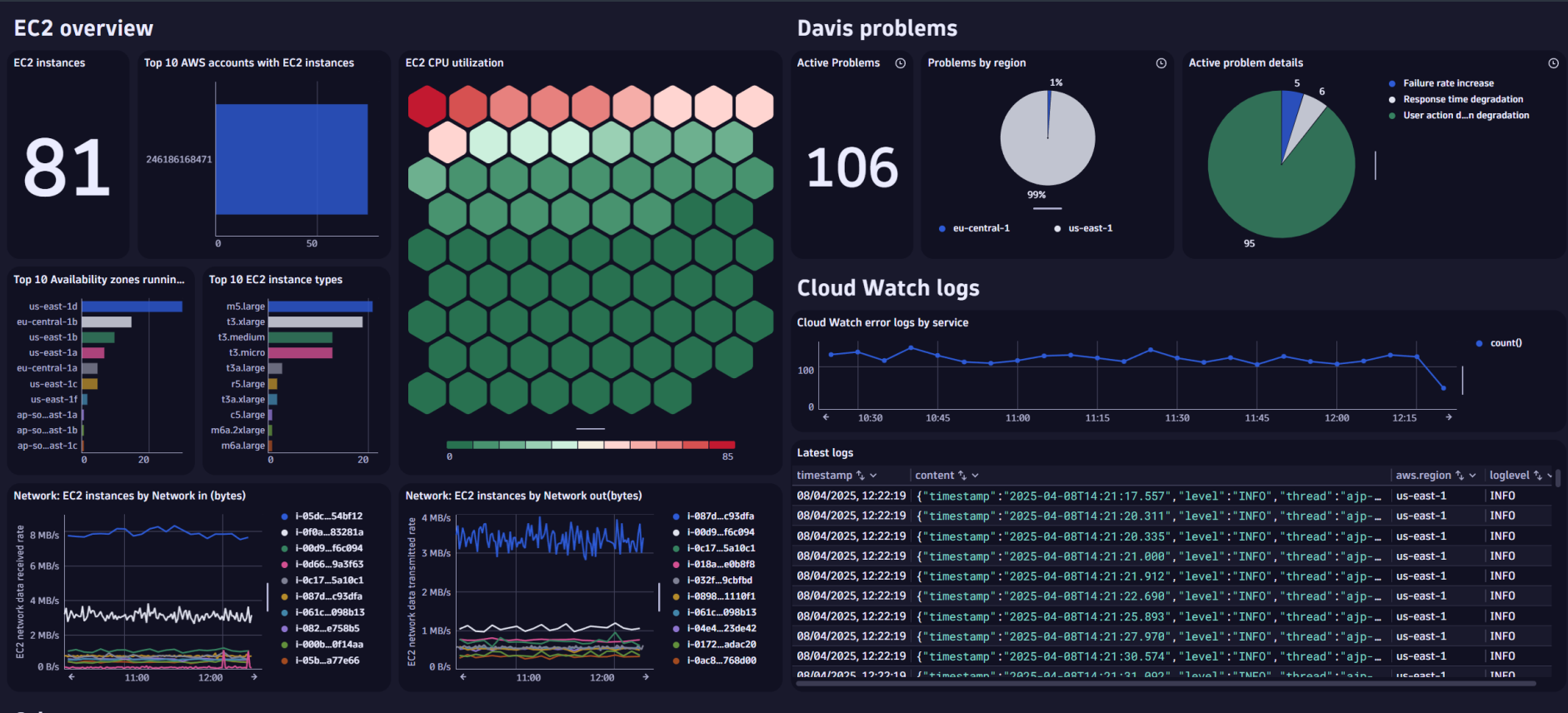
Infrastruktura
onPrem

Infrastruktura
chmurowa

Kubernetes

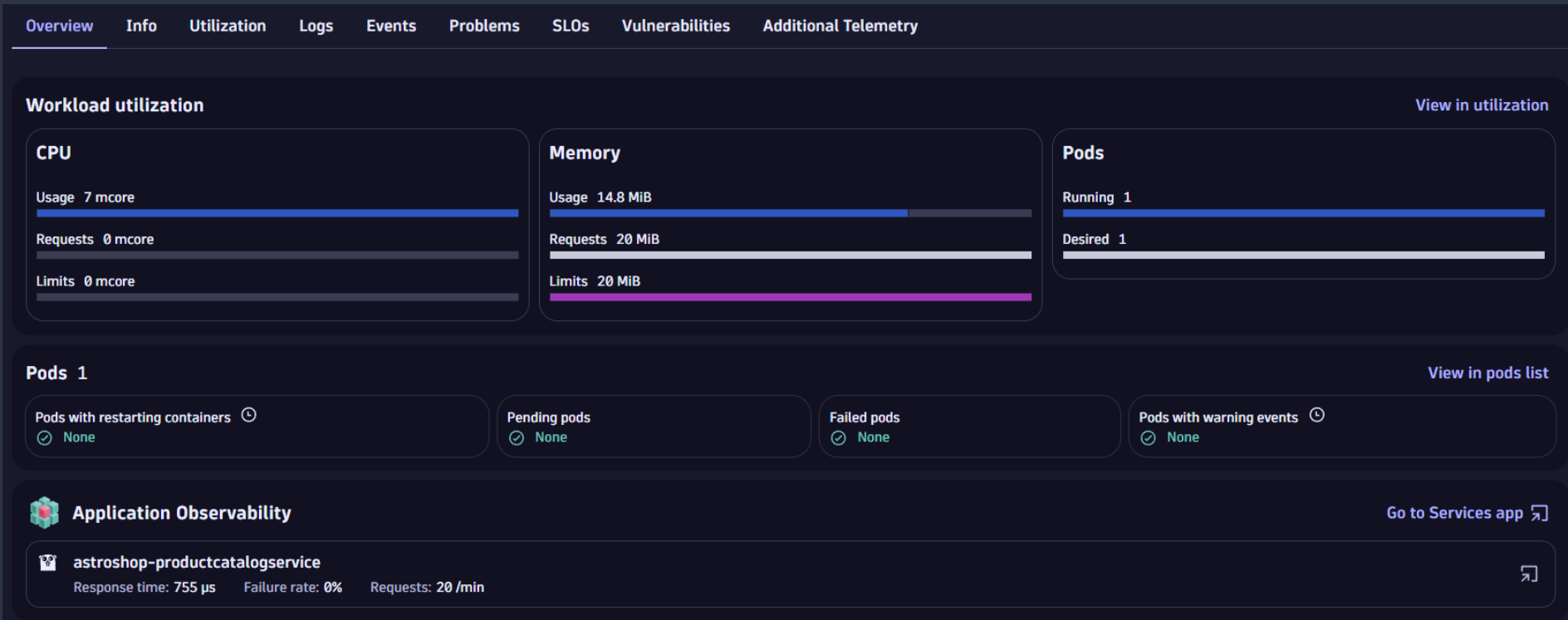
Usługi

Analiza
problemów



Chmura publiczna monitorowana jest poprzez integrację z natywnymi usługami zbierającymi dane telemetryczne (np. AWS Cloudwatch, Azure Monitor, GCP stackdriver) oraz za pomocą Oneagenta instalowanego na usługach

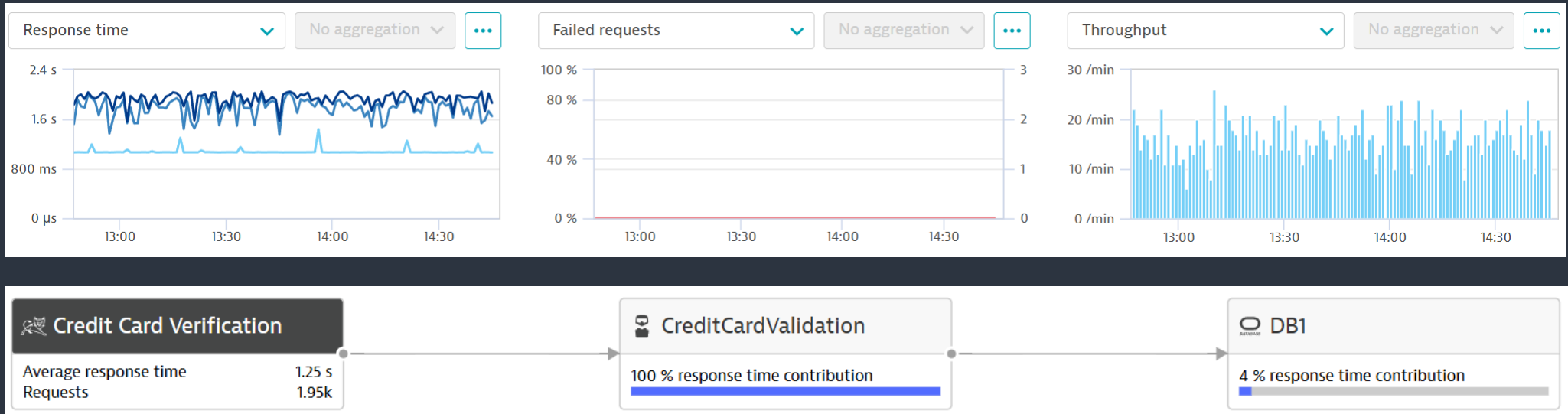
Kubernetes



Monitoring Kubernetes obejmuje warstwę fizyczną (worker nody) oraz logiczną – poziom klastra, namespace, workloads. Oprócz natywnych danych o działaniu samego Kubernetesa Dynatrace analizuje wydajność i dostępność działających na nim mikrouslug

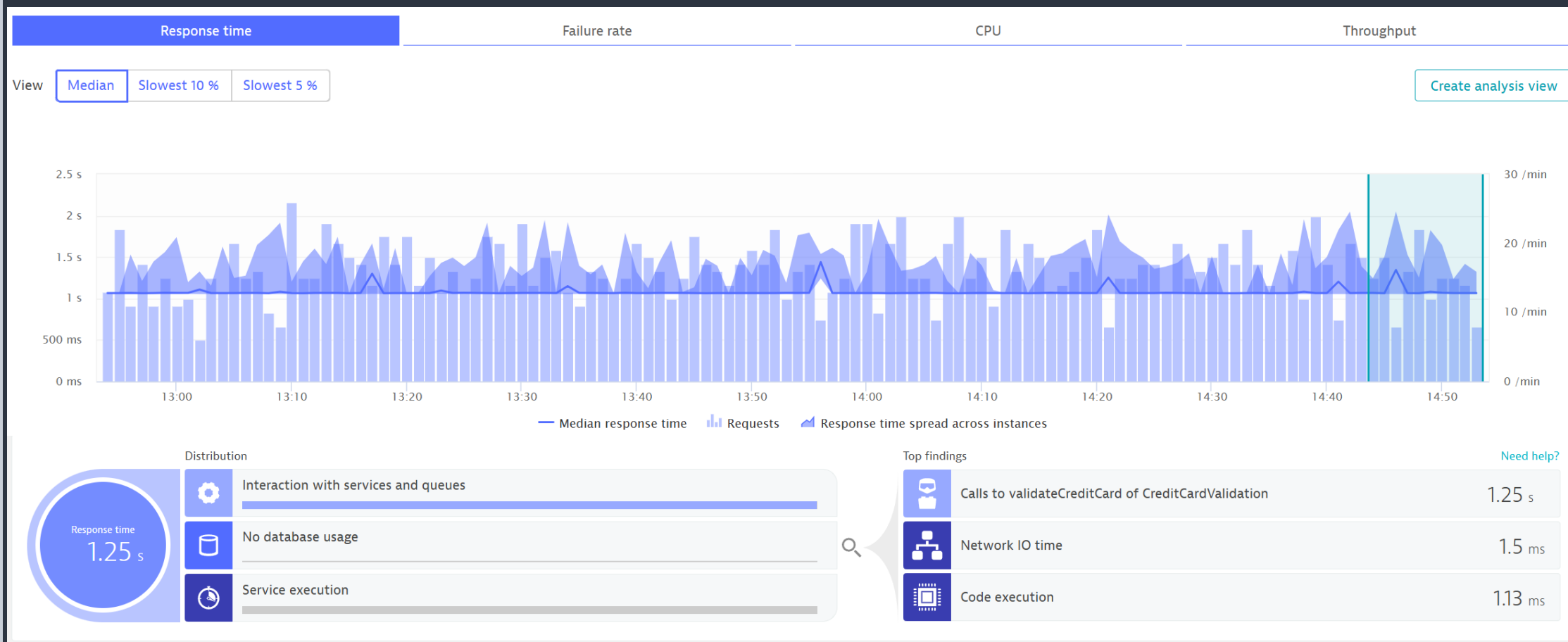
Usługi

- Dostarczenie danych
- Smartscape
- Infrastruktura onPrem
- Infrastruktura chmurowa
- Kubernetes
- Usługi
- Analiza problemów



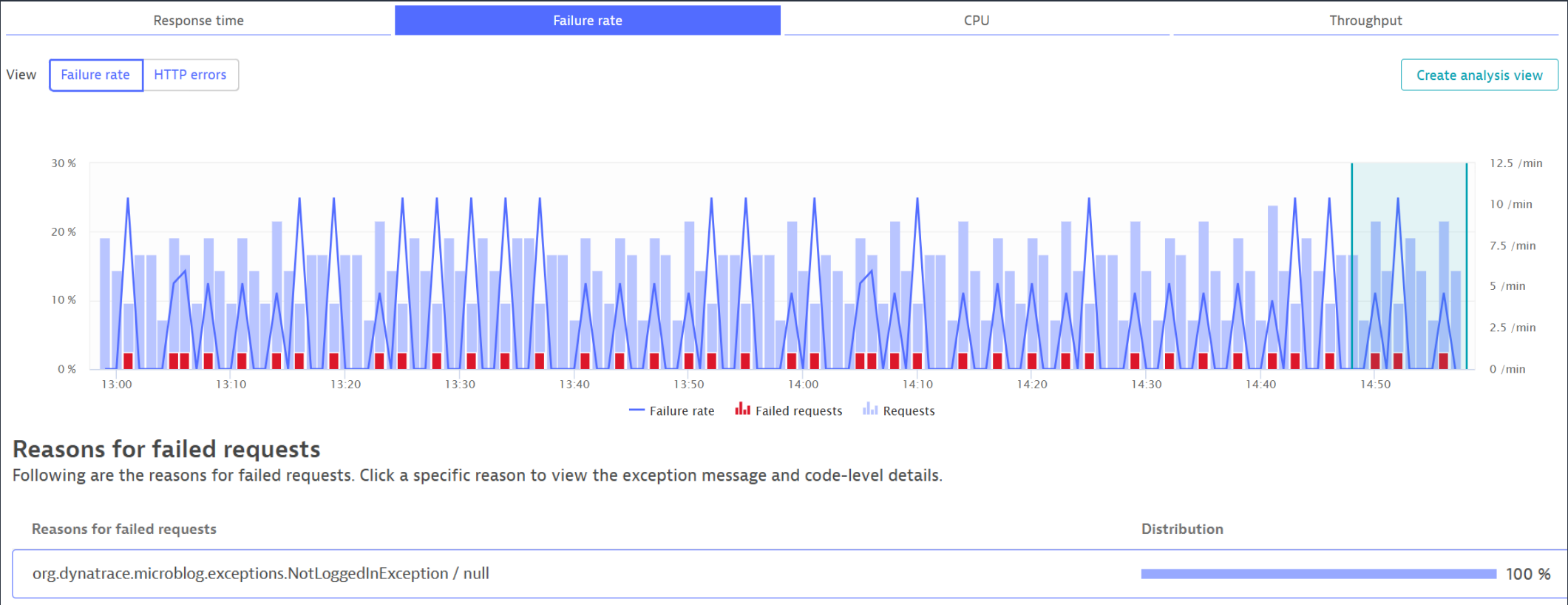
Usługi reprezentują wykonywalną część aplikacji, która przyjmuje żądanie, przetwarza je np. wywołując kolejne usługi i zwraca wynik. Dynatrace automatycznie analizuje każde wywołanie usługi na poziomie kodu wykonawczego wykrywając wąskie gardła.

Usługi – czasy odpowiedzi



Analiza czasów odpowiedzi usługi bazuje na percentylach (50,90).
Automatycznie wykonywana jest weryfikacja, czy czasy wynikają z
własnego kodu usługi, wolnej bazy danych lub innej usługi

Usługi - błędy



Wykrywając błędy w działaniu usługi Dynatrace automatycznie analizuje kod wywołań w celu wskazania źródła błędu.

Davis – hipermodal AI

Dostarczenie
danych

Smartscape

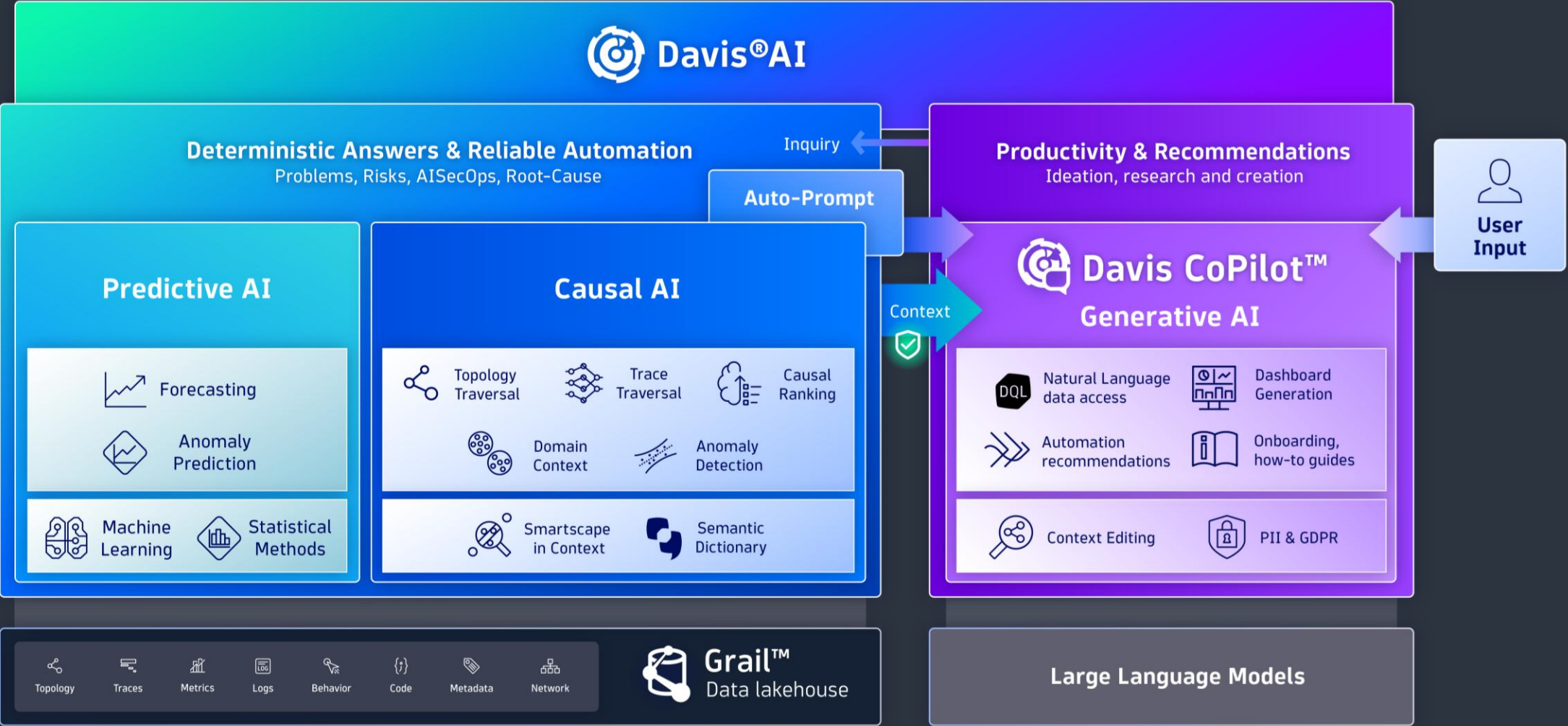
Infrastruktura
onPrem

Infrastruktura
chmurowa

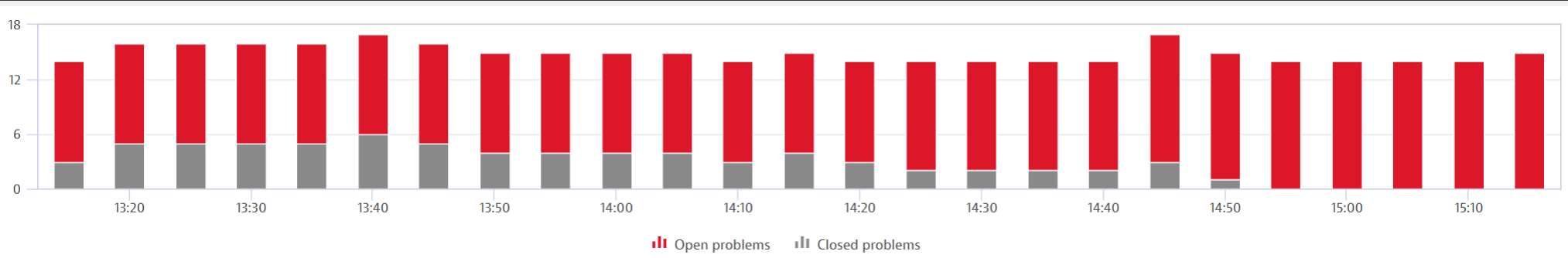
Kubernetes

Usługi


Analiza
problemów





Problem




Problem to anomalia wykryta na co najmniej jednym komponencie – przekroczenie przynajmniej jednego progu alertowego. Jeden problem agreguje anomalie wykryte na wielu komponentach, jeżeli z modelu Smartcape wynika, że są one ze sobą powiązane. Eliminuje zjawisko “alarm storming”.

 **www.easytravel.com: User action duration degradation**
➤ Problem P-25041626 detected at 07:58 - 08:19 (was open for 20 minutes).

 Affected applications
1

 Affected services
6

 Affected infrastructure
2

Dostarczenie
danych

Smartscape

Infrastruktura
onPrem

Infrastruktura
chmurowa

Kubernetes

Usługi

Analiza
problemów

Severity

- ☐ Monitoring unavailable
- ☐ Availability
- ☐ Error
- ☐ Slowdown
- ☐ Resource
- ☐ Custom

Problem

Problemy mogą dotyczyć niedostępności, zwiększonego poziomu błędów, wzrostów czasów odpowiedzi, nadmiernej użycia lub błędów po stronie infrastruktury lub dowolnie zdefiniowanego alarmu na bazie każdej metryki, jaka jest w systemie.

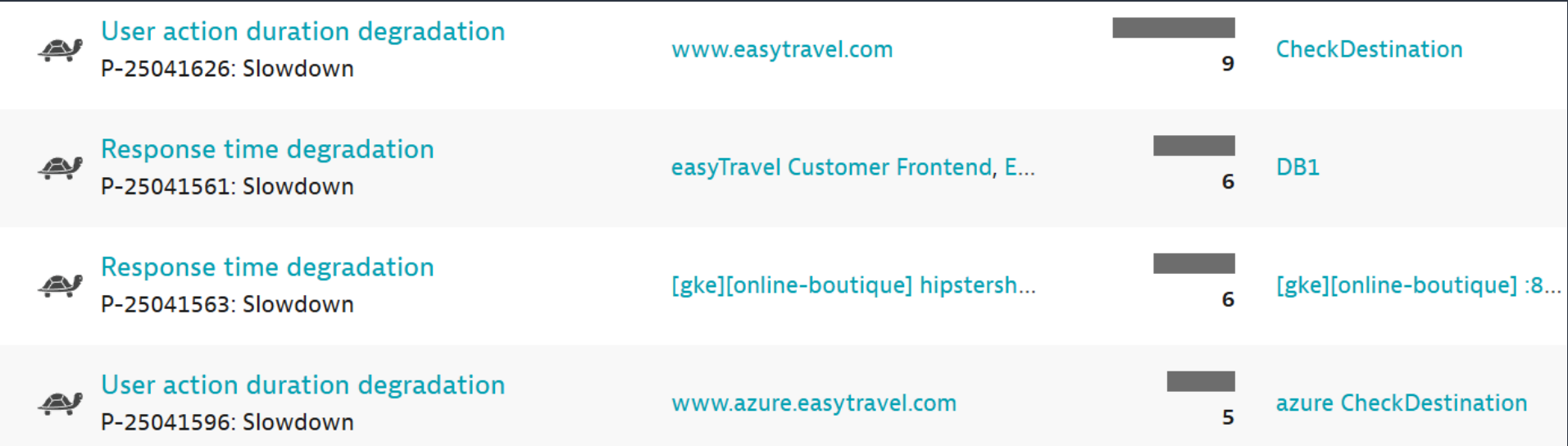
Standardowo problem na warstwie aplikacji/usługi bazują na automatycznie, dynamicznie budowanych progach, dla infrastruktury na predefiniowanych wartościach.

W przypadku jednoczesnego wystąpienia wielu różnych grup anomalii agregowane one są w jeden problem i pozycjonowane wg Severity.

Analiza problemów wydajnościowych

Problemy wydajnościowe związane są przekroczeniem oczekiwanych czasów odpowiedzi. Oznaczane są jako:

- User action duration degradation – gdy problem jest widoczny dla użytkownika końcowego,
- Response time degradation – gdy jest widoczny tylko na poziomie usług



Analiza problemów wydajnościowych

Po wykryciu problem prezentowany jest największy wpływ wystąpienia anomalii oraz przyczyna:

Dostarczenie
danych

Smartscape

Infrastruktura
onPrem

Infrastruktura
chmurowa


Kubernetes

Usługi

Analiza
problemów

2 impacted applications

35.4+ User actions per minute impacted

 **www.angular.easytravel.com**
Web application


User action duration degradation

The current response time (~1.81 s) exceeds the auto-detected baseline (612.5 ms) by 195.35 %. Incident occurred with user action /easytravel/rest/journeys/?match.

Affected user actions	User action	
10.8 /min	/easytravel/rest/journeys/?match	
Browser	Geolocation	OS
All	All	All


Root cause

Based on our dependency analysis all incidents have the same root cause

 **DB1**
Database

Custom deployment event


Deployment change

 **4 Service response time degradation events**
The current response time (~250.19 ms) exceeds the auto-detected baseline (~20.29 ms) by 1132.79 %. Service DB1 has a slowd...

Events on:
Service **DB1**

6 impacted services

933+ Requests per minute impacted

 **[gke][online-boutique] hipstershop.CurrencyService (grpc://hipstershop.CurrencyService)**
External rpc service

Kubernetes cluster

Kubernetes namespace

Kubernetes service


Kubernetes workload

Response time degradation

The current response time (~591.72 ms) exceeds the auto-detected baseline (~99.99 ms) by 491.75 %. Service [gke][online-boutique] hipstershop.CurrencyService (grpc://hipstershop.CurrencyService) has a slowd...

Root cause

Based on our dependency analysis all incidents have the same root cause


 **[gke][online-boutique] :8080**
Web request service

Kubernetes cluster

Kubernetes namespace

Kubernetes service

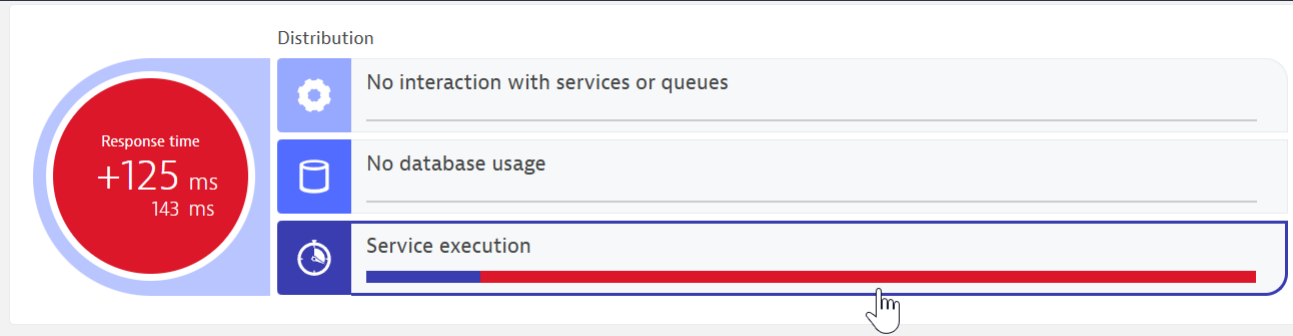
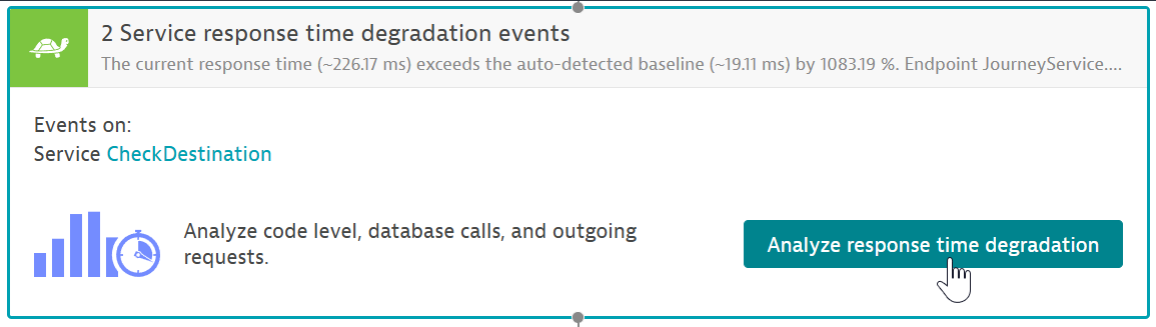
Kubernetes workload

 **4 Service response time degradation events**
The current response time (~2.89 s) exceeds the auto-detected baseline (~582.84 ms) by 396.48 %. Endpoint /cart/checkout h...

Events on:

Analiza problemów wydajnościowych

Najprościej podążać za podpowiedziami i udostępnianymi funkcjami analitycznymi:

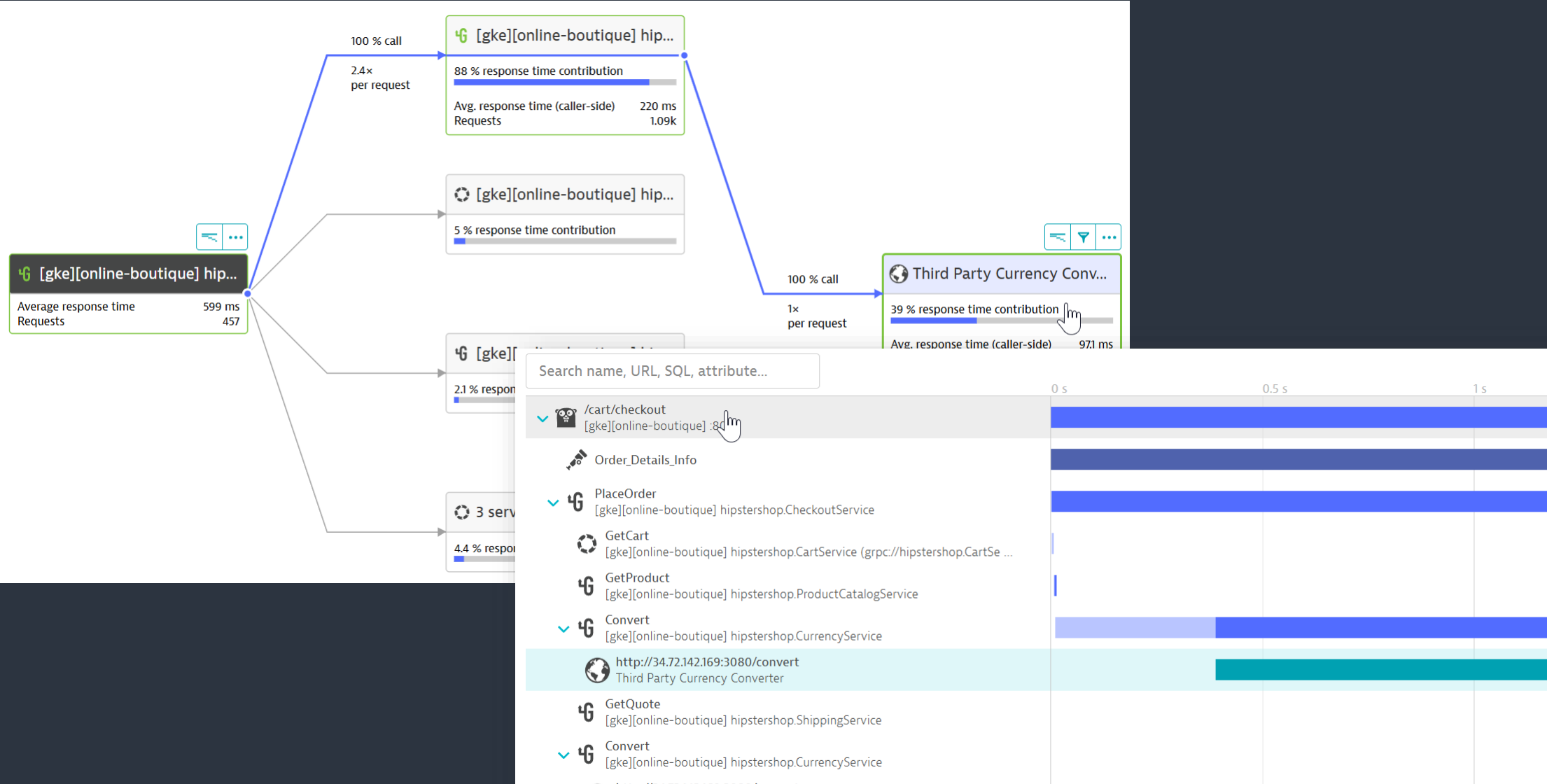


Top hotspots

Method	Contribution breakdown	Overall contribution
LocationParser.calculateSectionIndex EasyTravel Util com.dynatrace.easytravel.util	<div></div>	96.1 %

Analiza problemów wydajnościowych

Lub wybrać analizę ręczną opartą o Service flow i distributed traces:



Dostarczenie
danych

Smartscape

Infrastruktura
onPrem

Infrastruktura
chmurowa

Kubernetes






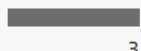


Usługi

Analiza
problemów

Analiza błędów

Problemy typu Error związane są z zarejestrowaniem zwiększonej liczby błędów. Oznaczone są jako:

- Failure rate increase – gdy problem dotyczy zwiększonej liczby błędów na usłudze,
- Javascript error rate increase – agent w przeglądarce rejestruje zwiększoną liczbę błędów javascript
- Request error rate increase – agent w przeglądarce rejestruje zwiększoną liczbę błędów http
- Request error rate increase – agent w przeglądarce rejestruje zwiększoną liczbę błędów biznesowych, wyzwalanych przez kod aplikacji.


 Failure rate increase P-25041578: Error	azure AuthenticationService		1	azure AuthenticationService...
 Custom error rate increase P-25041577: Error	www.angular.easytravel.com		1	EasytravelService
 Failure rate increase P-25041569: Error	azure EasytravelService, azure B...		3	azure JourneyService
 JavaScript error rate increase P-25041562: Error	www.angular.easytravel.com		1	

Analiza błędów

Po wykryciu problem prezentowany jest największy wpływ wystąpienia anomalii oraz przyczyna:

1 impacted service

16.2+ Requests per minute impacted



azure AuthenticationService

Web service

Failure rate increase

The error rate increased to 23.64 %.

Service azure AuthenticationService has a failure rate increase.

Affected requests:


16.2 /min

Endpoint

All methods affected


Root cause

Based on our dependency analysis all incidents have the same root cause



azure AuthenticationService

Web service




Service failure rate increase event

The error rate increased to 23.64 %. Service azure AuthenticationService has a failure rate increase.

Events on:

Service [azure AuthenticationService](#)




Understand which requests fail and the underlying root causes and errors.

Analyze failure rate degradation

Analiza błędów

Najprościej podążać za podpowiedziami i udostępnianymi funkcjami analitycznymi:




2 Service failure rate increase events

Your custom threshold of 25 % was exceeded to 100 %. Endpoint getLatestStatus has...

Events on:

Service [\[eks\]\[easytrade-live-debugger\] OrderController](#)





Understand which requests fail and the underlying root causes and errors.


Analyze failure rate degradation

Reasons for failed requests

Following are the reasons for failed requests. Click a specific reason to view the exception message and code-level details.

Reasons for failed requests	Distribution	Failed requests
<div> jakarta.servlet.ServletException</div>	<div><div></div>100 %</div>	3.12k (+2.9k)
Request processing failed: java.lang.ArithmeticException: / by zero	<div><div></div>69 % (-31.4 %)</div>	2.14k (+1.92k)
Request processing failed: java.lang.ArithmeticException	<div><div></div>31 % (+31 %)</div>	979 (+979)

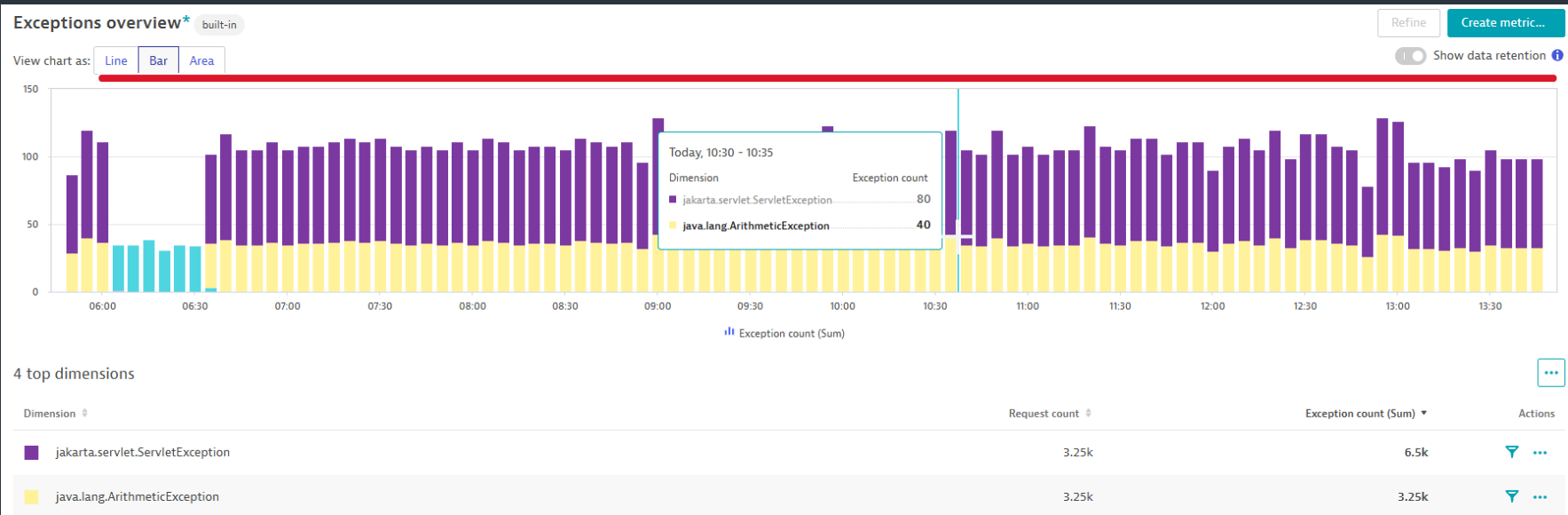
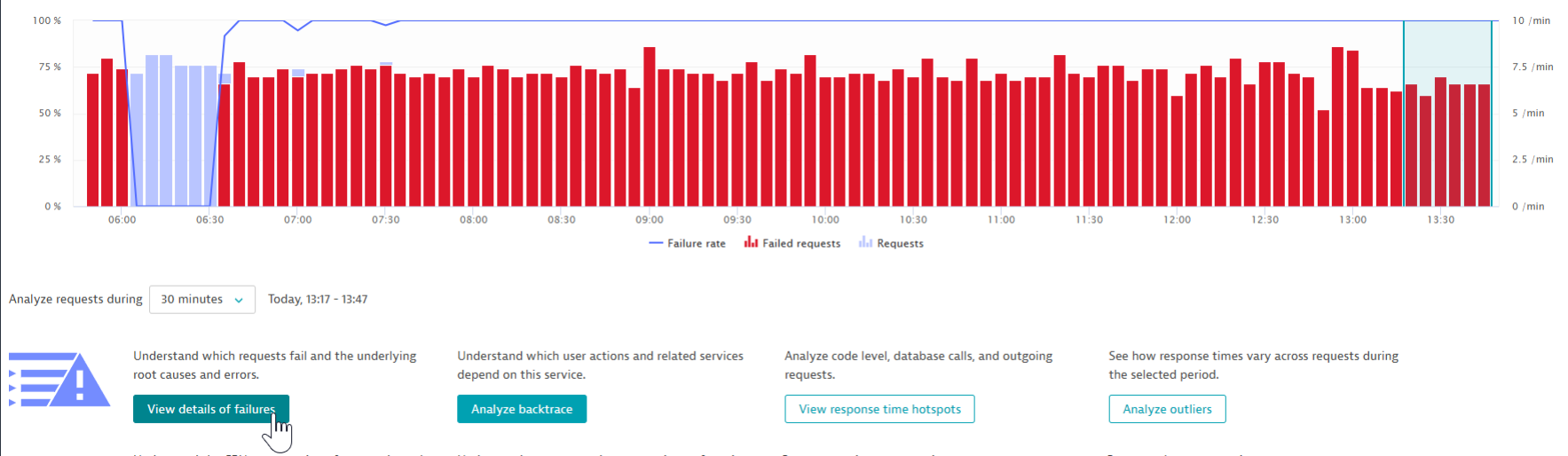
Related error logs 

 Filter log by content or status

Timestamp	Status	Content	Details
2025-04-09T11:43:20.719Z	ERROR	1 --- [nio-8080-exec-2] o.a.c.c.C.[.[./].[dispatcherServlet] : Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: java.lang.ArithmeticException: / by zero] with root cause java.lang.ArithmeticException: / by zero at com.dynatrace.easytrade.creditcardorderservice.OrderController.CountArythmeticSequenceTotal(OrderController.java:307) ~ [!/:1.1.93] at com.dynatrace.easytrade.creditcardorderservice.OrderController.CountSequenceTotal(OrderController.java:297) ~	

Analiza problemów wydajnościowych

Lub wybrać analizę ręczną opartą o Details of failures lub Exception analysis:



Dostarczenie
danych

Smartscape

Infrastruktura
onPrem

Infrastruktura
chmurowa

Kubernetes

Usługi

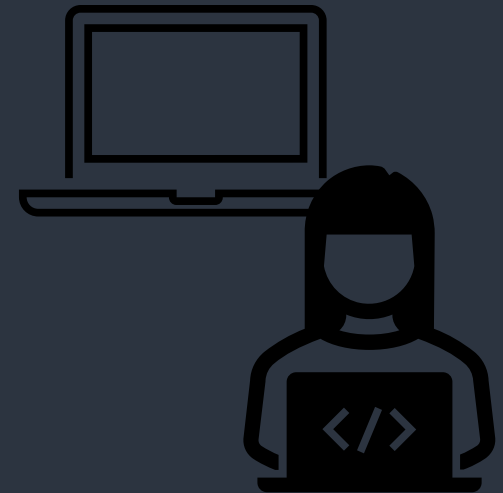
Analiza
problemów



10 minut

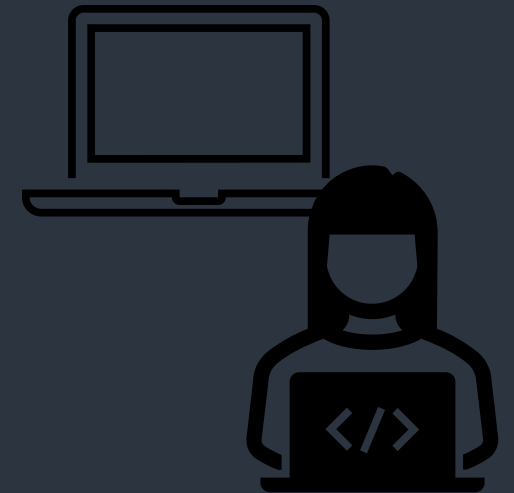
RUM - Real User Monitoring

Dynatrace RUM daje możliwość lepszego poznania użytkowników dzięki analizie wydajności w czasie rzeczywistym. Obejmuje to wszystkie działania użytkowników oraz ich wpływ na wydajność. Identyfikowane są problemy lub błędy, które się pojawiły, a także oceny doświadczeń użytkowników, podziały geolokacyjne i wiele więcej. Można również uzyskać wgląd w zachowanie użytkowników, na przykład dowiedzieć się, ilu klientów powraca na stronę.



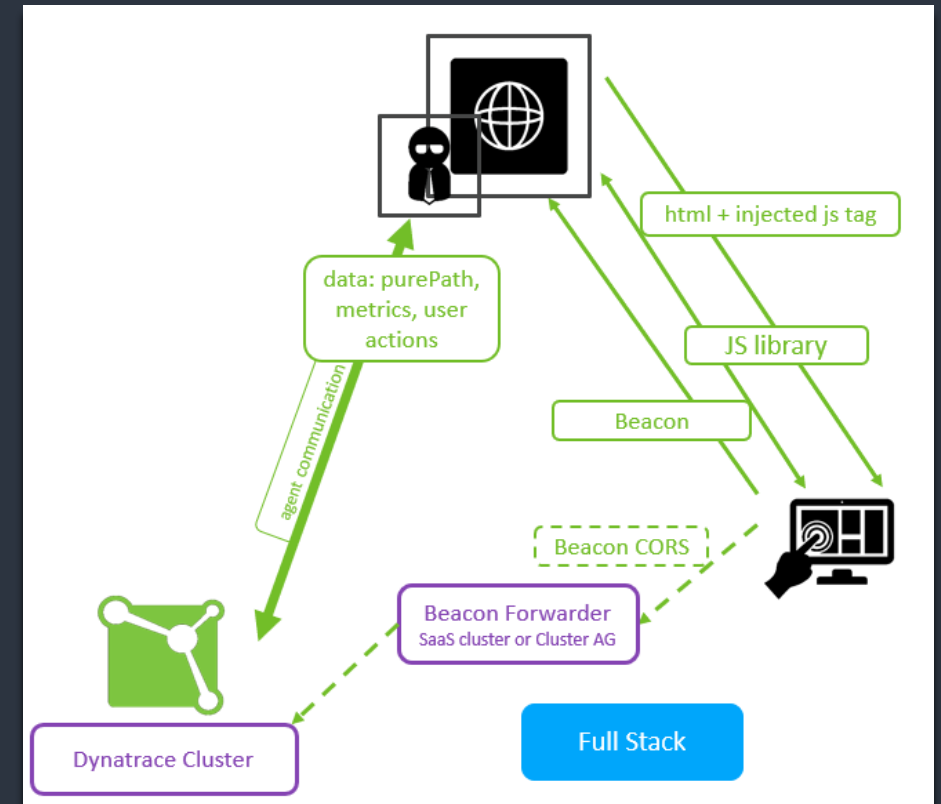
RUM - Real User Monitoring

- Dynatrace Real User Monitoring (RUM) zbiera metryki z przeglądarek internetowych klientów i koreluje dane z przeglądarki z informacjami po stronie serwera uzyskanymi z Dynatrace OneAgent.
- Dane przeglądarki internetowej są zbierane za pomocą agenta JavaScript, który jest umieszczany wewnątrz kodu HTML stron internetowych Twojej aplikacji. Istnieją dwa sposoby wstrzyknięcia znacznika JavaScript: automatyczny, czyli „Full Stack”, oraz manualny, czyli „Agentless”.



RUM – Automatyczne wstrzykiwanie agenta

- Opcja automatyczna jest rekomendowana
- Wstrzykiwanie OneAgent JavaScript taga jest automatyczne dla:
 - Java
 - Apache HTTP Server
 - IIS
 - NGINX
 - Node.js
- RUM JavaScript agent wysyła zwrótnie dane do monitorowanego serwera

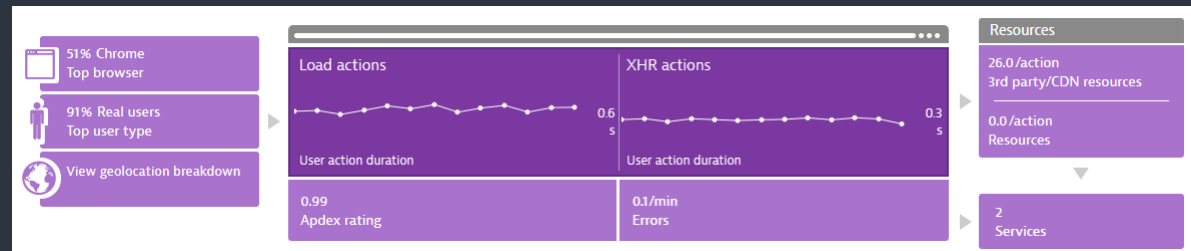


Aplikacje

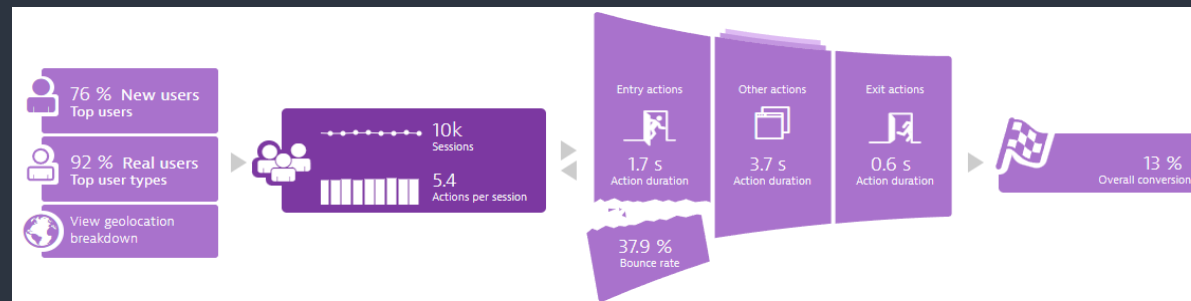
Aplikacja grupuje doświadczenia użytkownika z interakcji z systemem z poziomu:

- Przeglądarki – Aplikacja web. Oznaczenie aplikacji wg domeny lub url
- Urządzenia mobilnego – aplikacja natywna mobilna. Oznaczenie aplikacji w kodzie aplikacji.

Pozwala na analizę z perspektywy wydajności (czasy odpowiedzi, błędy, APDEX, dostępność)



Lub perspektywy biznesowej (liczba sesji, konwersja, porzucenia, nowi/powracający użytkownicy)

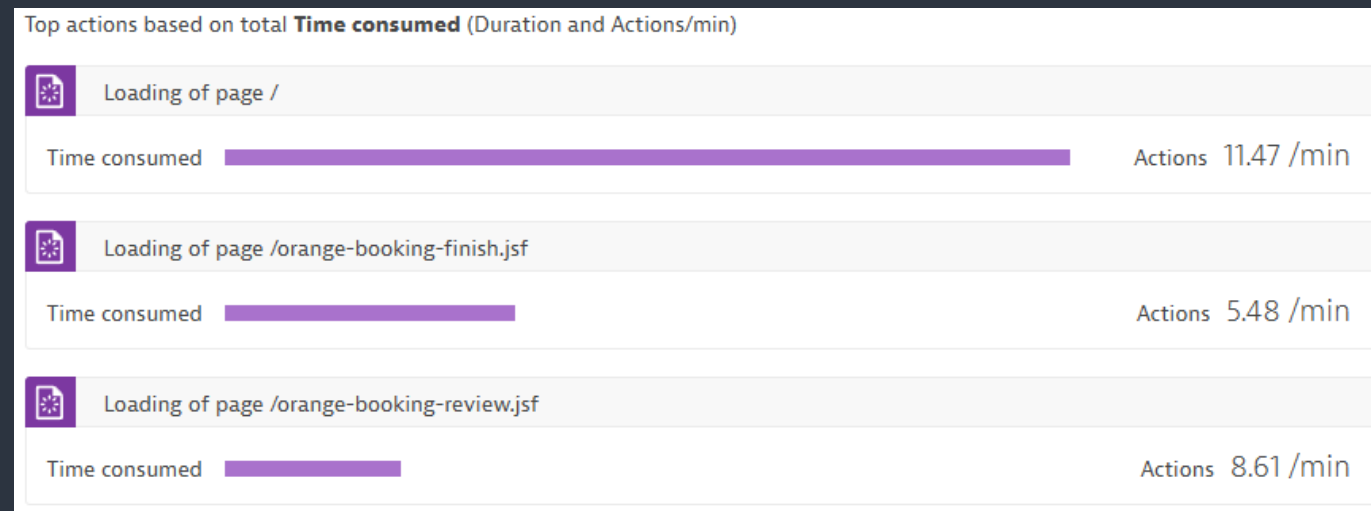


Akcje użytkowników

Akcja użytkownika to interakcja z przeglądarką internetową, która wiąże się z wywołaniem serwera www/aplikacyjnego, co potencjalnie może obejmować wiele zagnieżdżonych wywołań.

Typy akcji użytkownika:

- Akcja ładowania (Load action)
- Akcja XHR (XHR action)
- Akcja niestandardowa (Custom action)



Akcje użytkowników

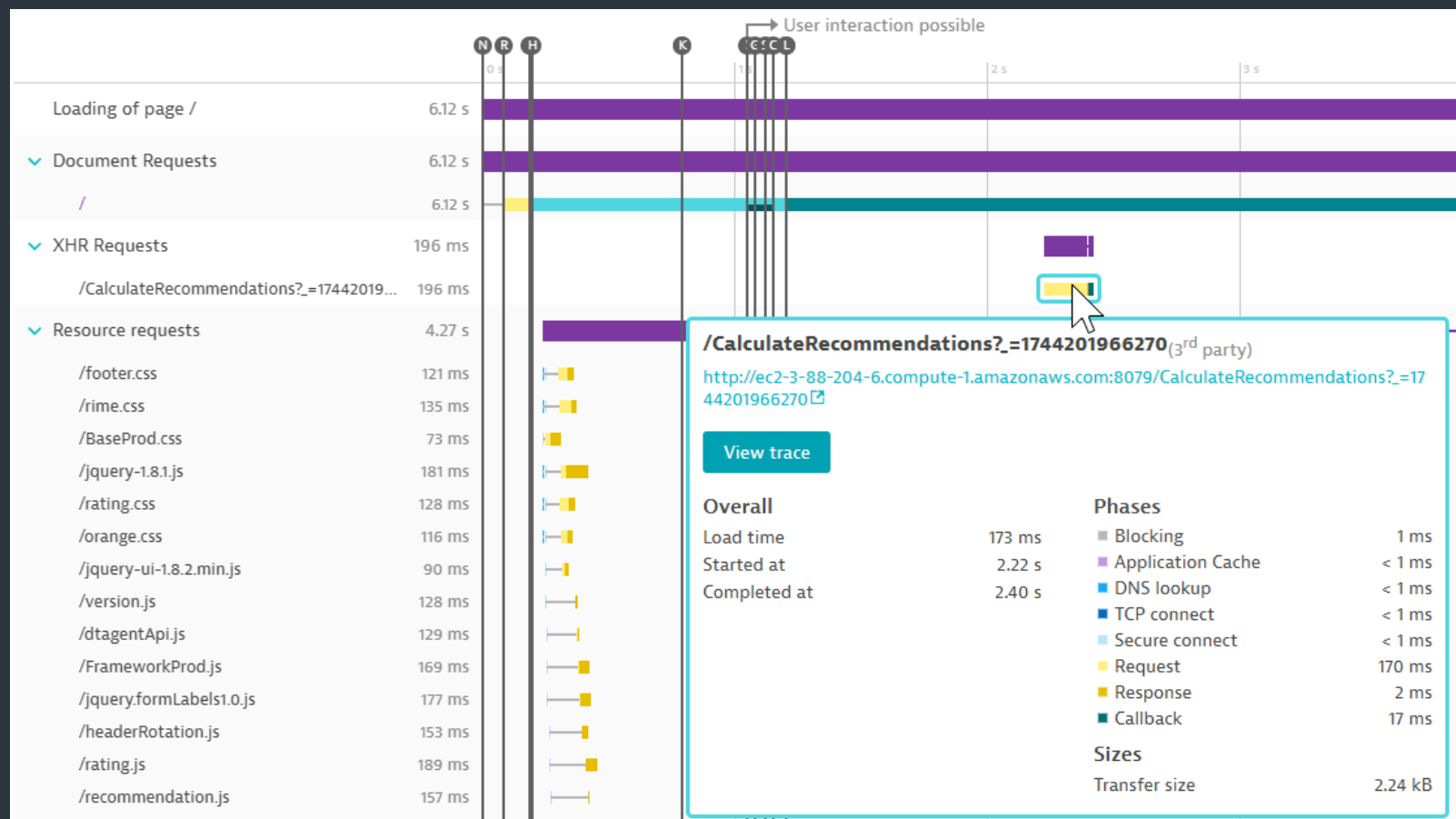
Akcja ładowania (Load action) - faktyczne ładowanie strony w przeglądarce. Jeśli wpiszesz adres URL w przeglądarce i naciśniesz Enter, wystąpi akcja ładowania. Podczas akcji ładowania ładowanych jest wiele zasobów, takich jak obrazy, HTML i CSS. Nazwy akcji ładowania opierają się na nazwie strony HTML (np. „ładowanie strony index.html”).

Akcja XHR (XHR action) - Większość nowoczesnych aplikacji, w tym aplikacje jednostronicowe (single page applications), zmienia strony za pomocą JavaScript, a cała komunikacja z serwerem internetowym odbywa się za pomocą wywołań API. Nazwy opierają się na adresie URL XHR (np. „http://easytravel/api/login”).

Niestandardowe akcje użytkownika (Custom user actions) - Użytkownik może je zdefiniować za pomocą JavaScript API dla RUM.

Akcje użytkowników

Dla każdej, pojedynczej akcji albo dla grupy takich samych akcji, można wygenerować tzw. Waterfall - prezentujący szczegóły analogiczne jak na zakładce Sieć w narzędziach programistycznych przeglądarki:

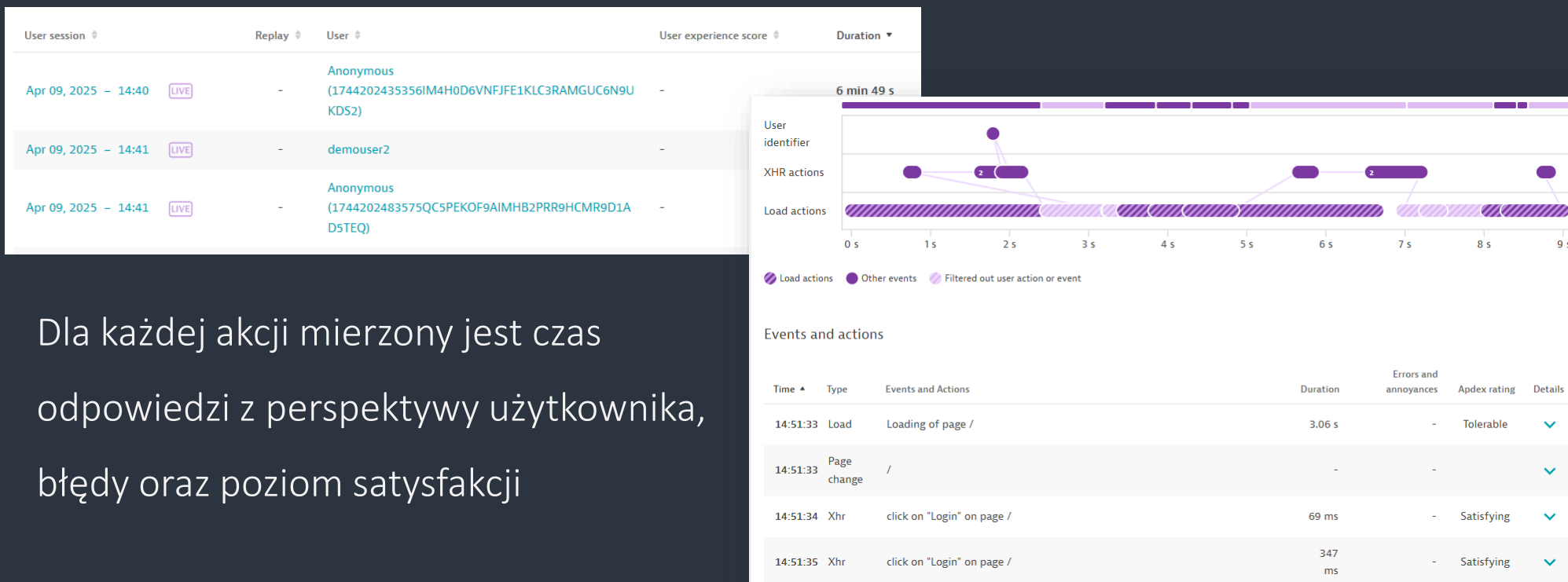


Sesja

Sesja użytkownika, czasami nazywana „wizytą”, to grupa akcji użytkownika wykonanych w aplikacji web/mobilnej w ograniczonym przedziale czasu.

W interfejsie użytkownika aktywne sesje (live) użytkowników są odróżniane od zakończonych.

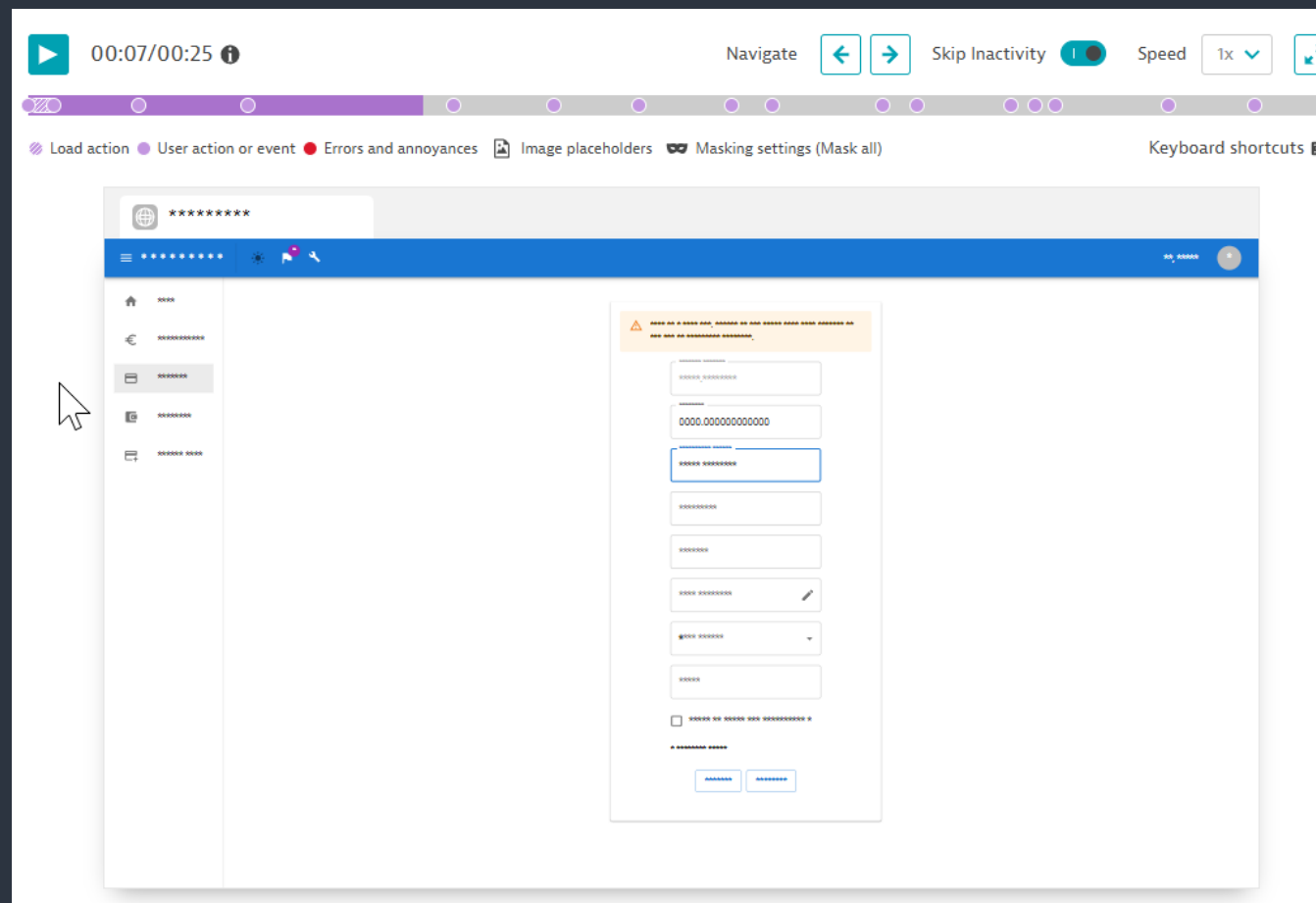
Dynatrace pozwala monitorować sesje użytkowników anonimowo, lub identyfikując nazwę użytkownika:



Dla każdej akcji mierzony jest czas odpowiedzi z perspektywy użytkownika, błędy oraz poziom satysfakcji

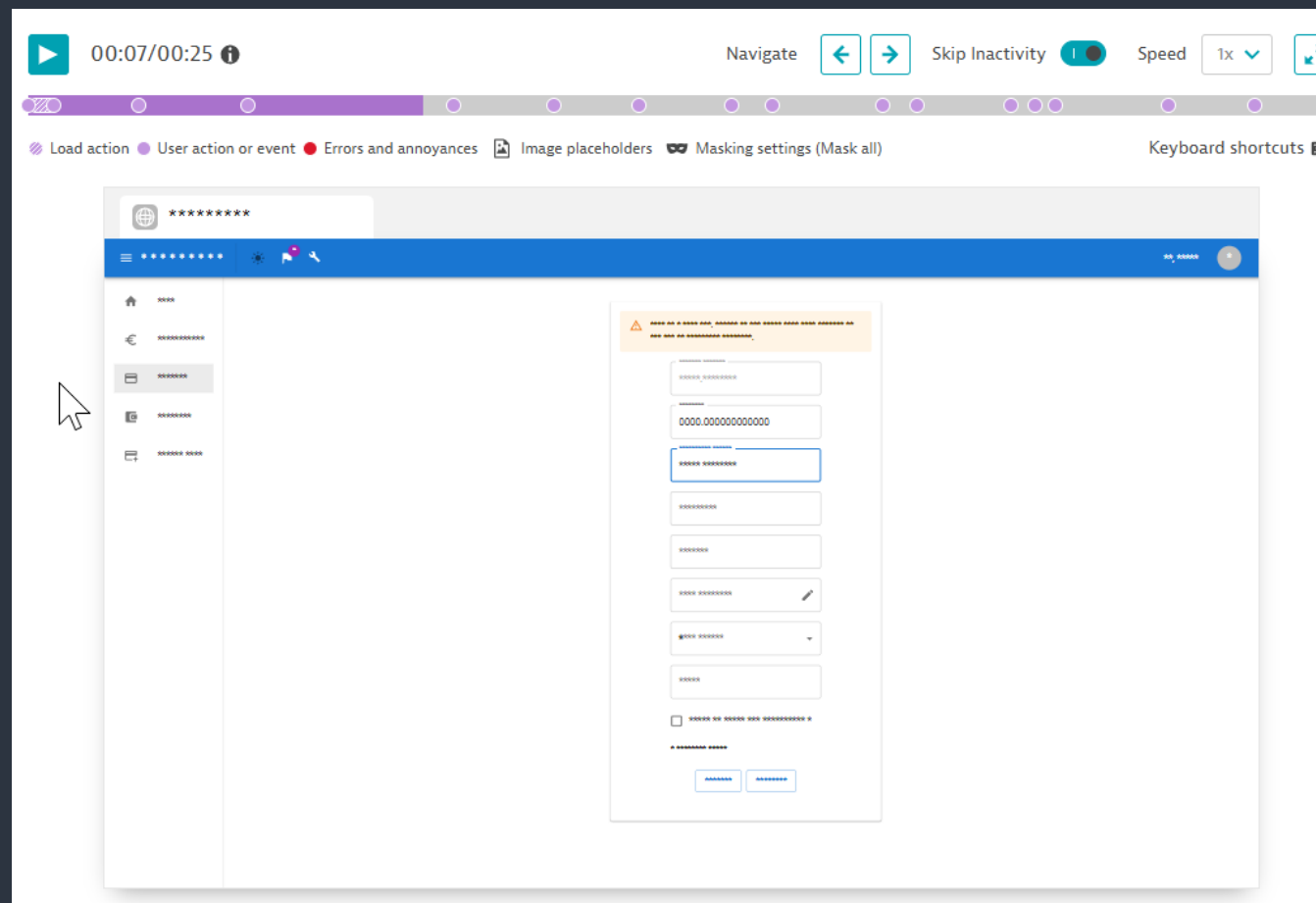
Session Replay

Sesja oprócz sekwencji akcji mogą odtwarzać w postaci filmu dokładnie co użytkownik robił oraz co widział. Operator może odtworzyć taką sesję w playerze. Dane wyświetlane mogą podlegać anonimizacji:



Session Replay

Sesja oprócz sekwencji akcji mogą odtwarzać w postaci filmu dokładnie co użytkownik robił oraz co widział. Operator może odtworzyć taką sesję w playerze. Dane wyświetlane mogą podlegać anonimizacji:



Zalety monitorowania syntetycznego

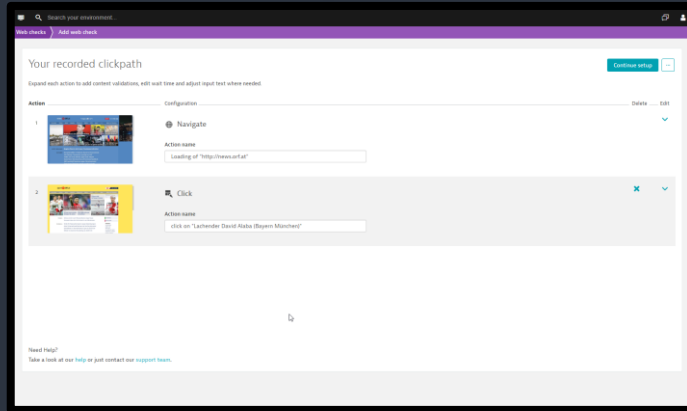
Monitorowanie syntetyczne (Synthetic Monitoring) zapewnia całodobową globalną widoczność aplikacji.

- Symuluje kluczowe dla biznesu ścieżki klientów.
- Monitorowanie SLA — obserwuj swoją aplikację przez całą dobę, 7 dni w tygodniu.
- Zarządzanie wydajnością CDN i usługami zewnętrznymi.
- Proaktywna analiza problemów.



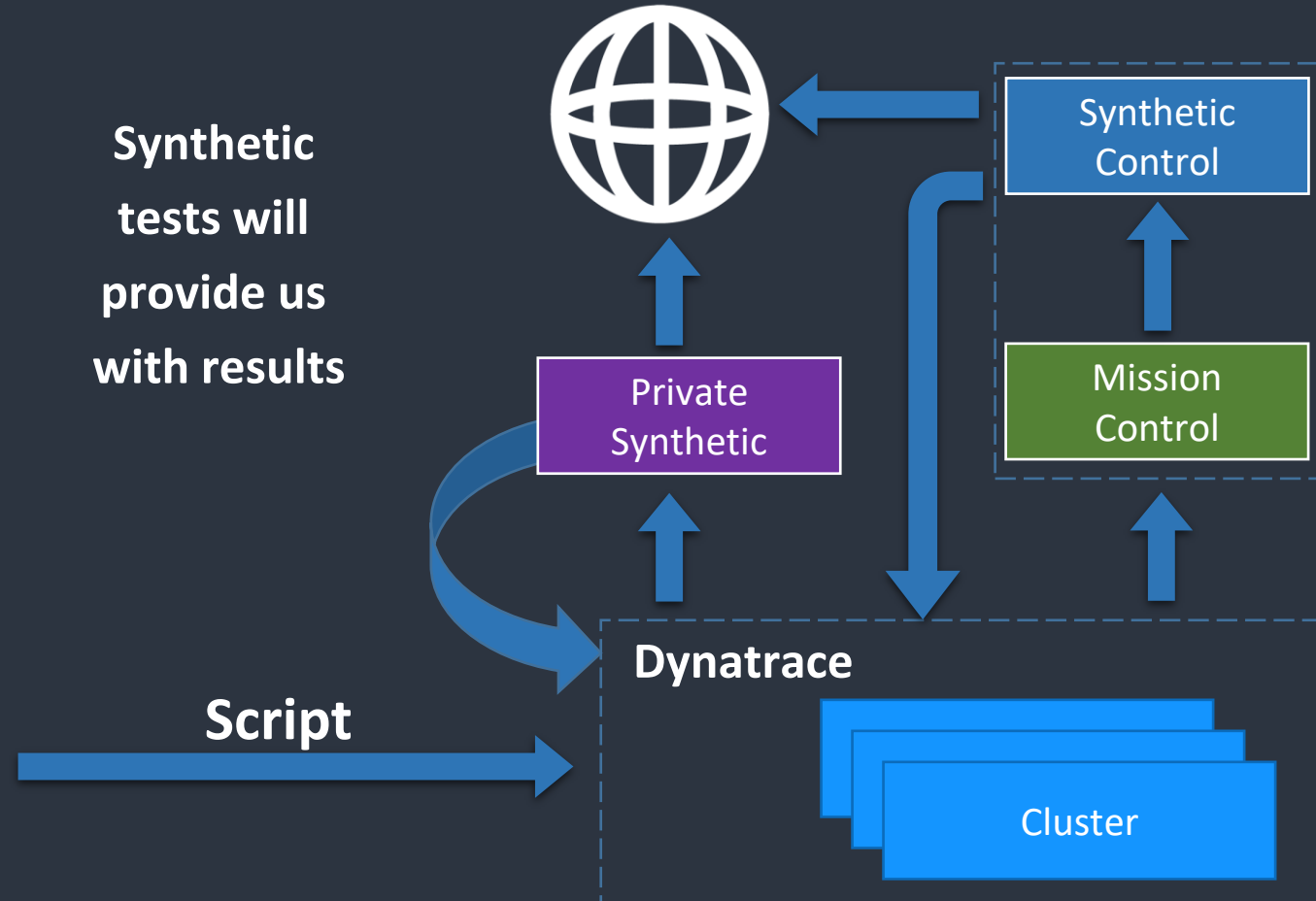
Synthetic monitoring – Jak działa?

Record clickpath



Update clickpath locally
verify by playback

Synthetic
tests will
provide us
with results



Typy monitorów syntetycznych

Monitory przeglądarkowe dla pojedynczego URL (Single-URL browser monitors)

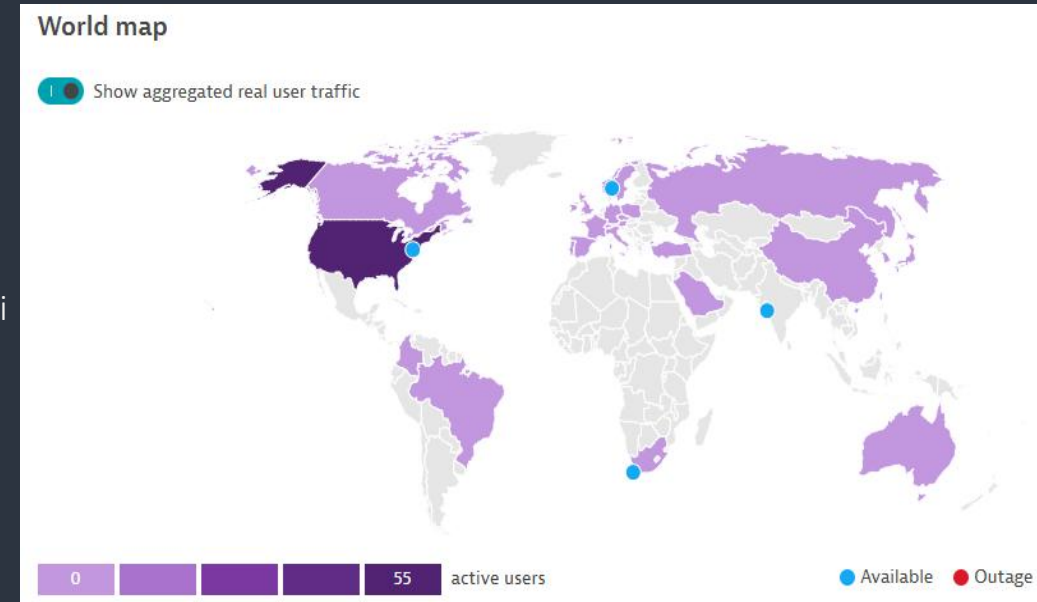
- Są odpowiednikiem symulowanego użytkownika odwiedzającego aplikację internetową.

Ścieżki kliknięć w przeglądarce (Browser clickpaths)

- To symulowane wizyty użytkownika monitorujące kluczowe dla biznesu przepływy pracy aplikacji. Pozwalają na rejestrowanie dokładnej sekwencji kliknięć użytkownika.

Monitory HTTP (HTTP monitors)

- Wykorzystują proste żądania HTTP.
- Minimalny interwał wynosi 1 minutę.
- Mogą być używane do sprawdzania witryny internetowej lub punktu końcowego API.



Security Overview

Dynatrace poprzez funkcjonalność agenta wykrywa podatności w bibliotekach oraz kodzie aplikacji. Dla problemów związanych z bezpieczeństwem jest dedykowany kanał powiadomień

Security
overview

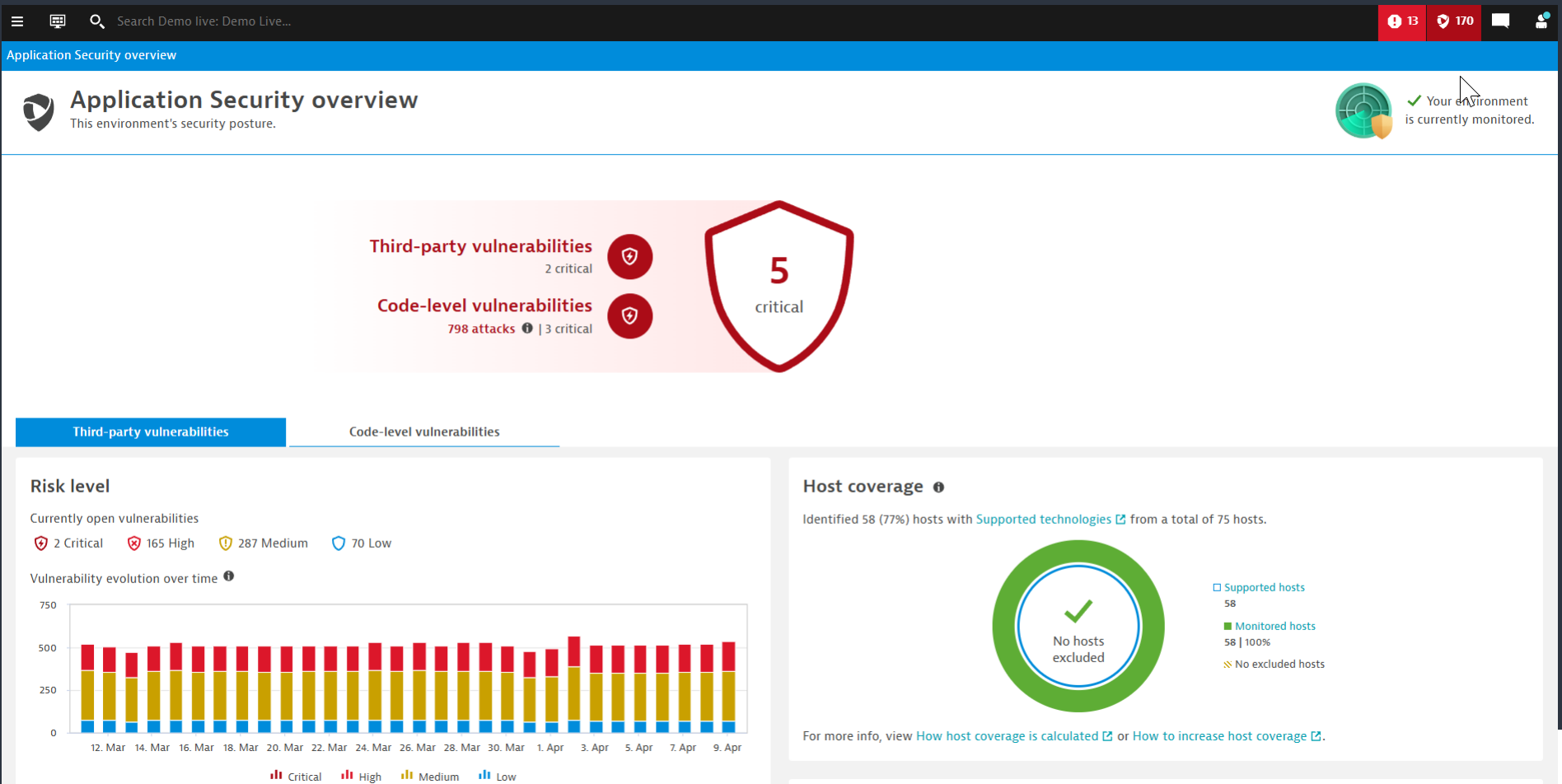
Konfiguracja

3rd party

Code-level

Compliance

Analiza logów



Konfiguracja

Brak

Sprowadza się wyłącznie do włączenia, wskazania (opcjonalnie) gdzie ma działać i na jakich technologiach.

Vulnerability Analytics: General settings

Automated [Runtime Vulnerability Analytics](#) helps you quickly and completely understand each detected vulnerability in your environment and how to remediate it, allowing you to prioritize which vulnerabilities to fix first. Note: Enabling Third-party or Code-level Vulnerability Analytics consumes Application Security units. For details, see the [Application Security Monitoring documentation](#).

Third-party Vulnerability Analytics

Code-level Vulnerability Analytics

☒ Enable Third-party Vulnerability Analytics

Global third-party vulnerability detection control

Monitor

Global third-party vulnerability detection control defines the default for all processes.

Technologies

Vulnerability Analytics can be enabled/disabled per supported technology.

☒

 .NET

☒

 .NET runtimes

☒

 Go

☒

 Java

☒

 Java runtimes

☒

 Kubernetes

Vulnerability Analytics: General settings

Automated [Runtime Vulnerability Analytics](#) helps you quickly and completely understand each detected vulnerability in your environment and how to remediate it, allowing you to prioritize which vulnerabilities to fix first. Note: Enabling Third-party or Code-level Vulnerability Analytics consumes Application Security units. For details, see the [Application Security Monitoring documentation](#).

Third-party Vulnerability Analytics

Code-level Vulnerability Analytics

☒ Enable Code-level Vulnerability Analytics

Global Java code-level vulnerability detection control ⓘ

Monitor

Global Java code-level vulnerability detection control defines the default for all process groups. You can use monitoring rules to override the default for certain processes.

Global .NET code-level vulnerability detection control ⓘ Early adopter

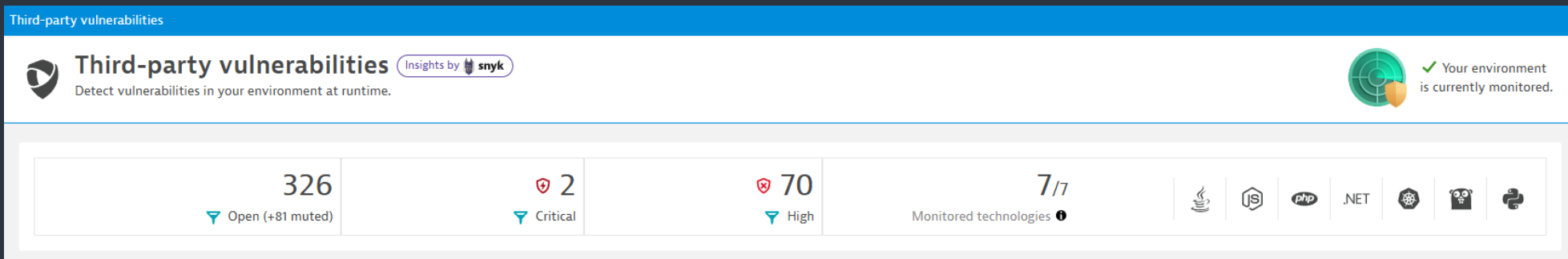
Do not monitor

Global .NET code-level vulnerability detection control defines the default for all process groups. You can use monitoring rules to override the default for certain processes.

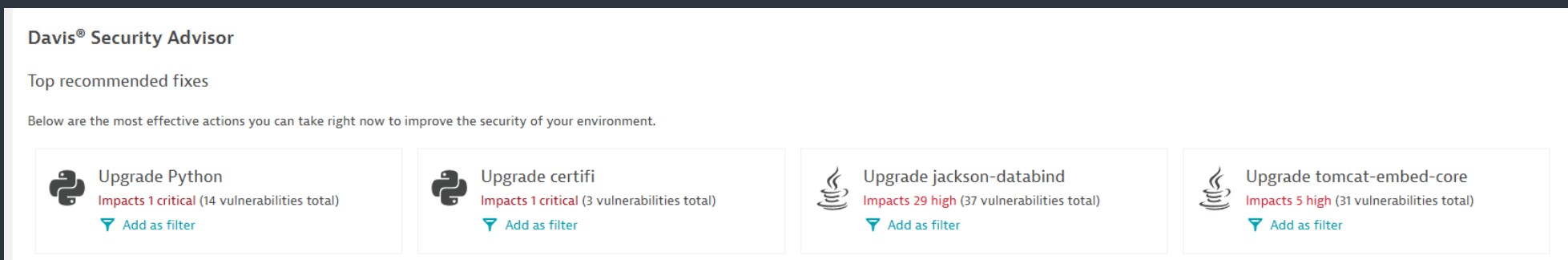
Podatności w bibliotekach

Agent inwentaryzuje biblioteki, które są używane przez procesy aplikacyjne.

Inwentaryzacja jest trzymana na serwerze – tam odbywa się analiza podatności na podstawie wpisów w SNYK I NVD.



Podatności są grupowane wg krytyczności. Dodatkowo Davis Security Advisor podpowiada co poprawić, aby mieć największy uzysk.



DSS vs CVSS

Security overview

Konfiguracja

3rd party

Code-level

Application
Protection

Compliance

Analiza logów

Dynatrace do priorytetyzacji podatności wykorzystuje własny score:

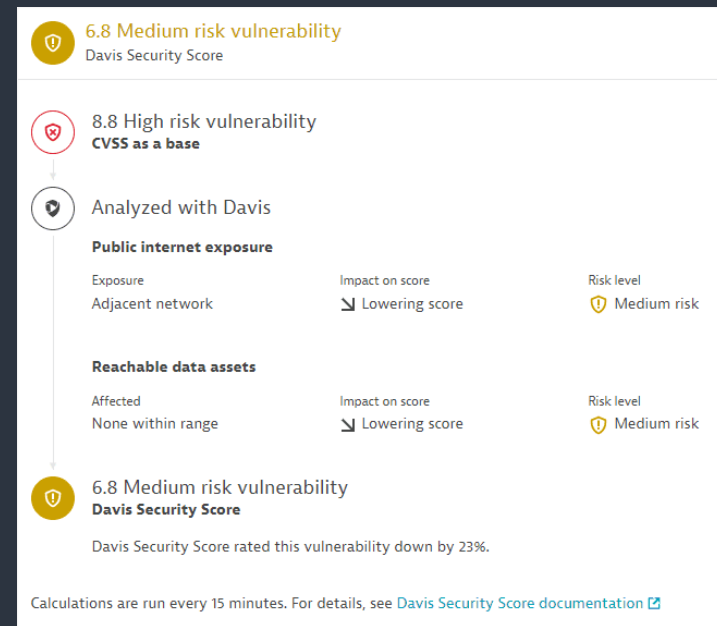
Davis Security Score. DSS jako wartość bazową bierze wartość CVSS – score nie może być wyższy niż CVSS.

Davis może obniżyć score na bazie analizy modelu Smartscape oraz transakcji przechodzących przez aplikację:

- Poprzez kontekst ekspozycji do publicznego internetu.

Wykorzystywana jest metryka Modified Attack Vector (MAV) – jeżeli Dynatrace stwierdzi, że komponent nie jest dostępny z internetu oryginalny AV jest obniżany.

- Poprzez kontekst dostępu do danych. Wykorzystywane są metryki Modified Confidentiality (MC) and Modified Integrity (MI). Jeżeli Dynatrace oceni, że nie ma dostępu do danych oryginalne wartości C oraz I są obniżane.



Risk assessment

Security overview

Konfiguracja

3rd party

Code-level

Application
Protection

Compliance

Analiza logów

Risk assessments pozwala filtrować wykryte podatności wg:

- Dostępności komponentu z internetu,
- Dostępności publicznych exploitów,
- Dostępu komponentu do baz danych,
- Wykorzystania przez aplikację funkcji, która zawiera podatność.

Filtered by: Risk assessment: Public internet exposure X Risk assessment: Public exploit published X Risk assessment: Reachable data assets X Risk assessment: Vulnerable functions in use X

2 vulnerabilities detected

Powered by Davis Security Score

Public internet exposure Reachable data assets Vulnerable functions Public exploit

<input type="checkbox"/> Vulnerability	Davis Security Score	Status	Affected entities	First detected	Details
<input type="checkbox"/> S-1328: Arbitrary File Upload org.apache.tomcat:tomcat-coyote	High 8.3	Open	Process groups: 19	721 d 3 h ago	✓
<input type="checkbox"/> S-1592: Stack-based Buffer Overflow org.yaml:snakeyaml	Medium 4.3	Open	Process groups: 6	763 d 4 h ago	✓

Public internet exposure

Public network

**Reachable data assets**

Within range

**Vulnerable functions**

In use

**8.3**High
risk**Public exploit**

Public exploit published

**Process groups**

19 affected

**Vulnerable component**

tomcat-coyote


Code-level












Dynatrace zaczyna sprawdzać biblioteki i kod własny, aby wykrywać podatności na poziomie kodu. Podatność na poziomie kodu to problem bezpieczeństwa wynikający z błędu w kodzie aplikacji.

Analiza wykrywa podatności typu:

- SQL injection
- command injection
- JNDI injection
- SSRF

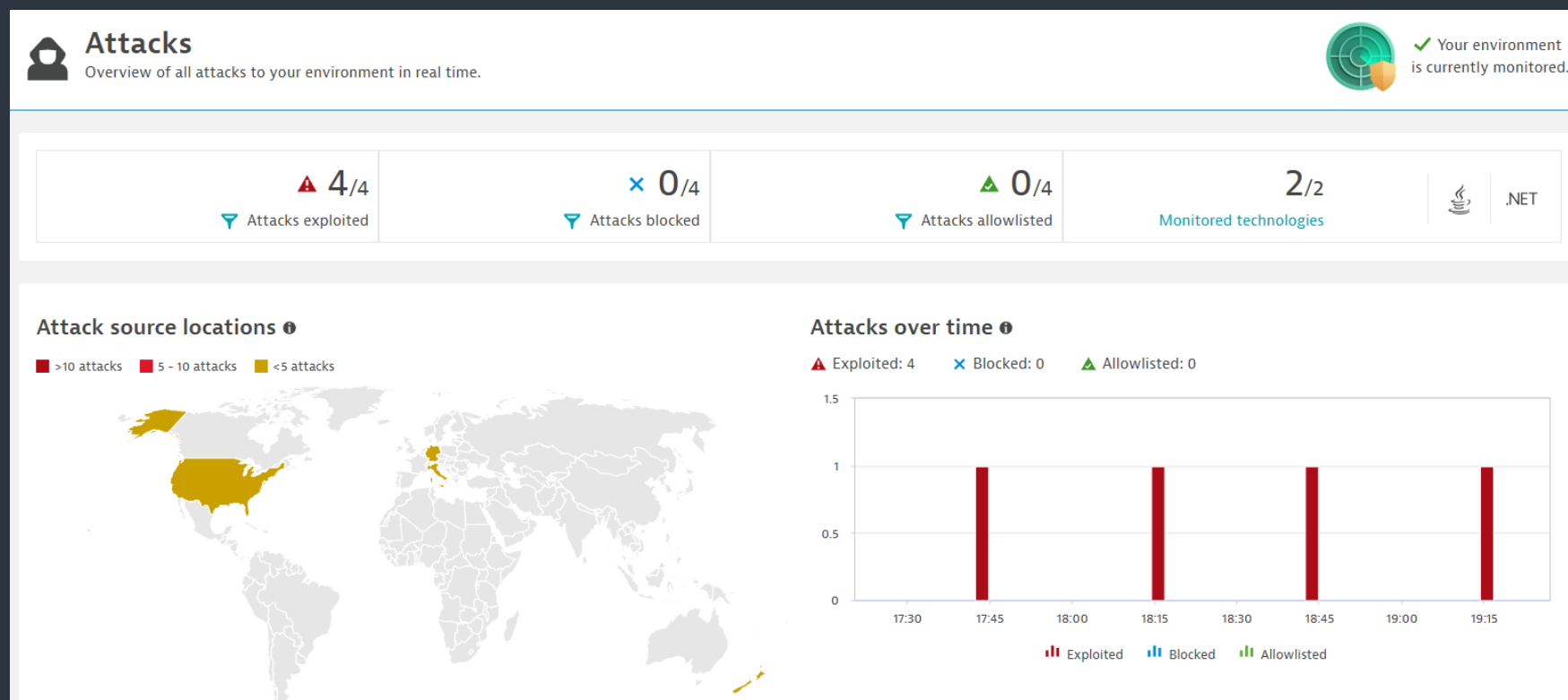
3 vulnerabilities detected

 Public internet exposure  Reachable data assets

<input type="checkbox"/> Vulnerability 	Risk level 
<input type="checkbox"/> S-2004: SQL injection at MembershipController+<GetMembershipStatus>d_3.Move... MembershipService.dll unguard-membership-service-*	 Critical  
<input type="checkbox"/> S-2005: SQL injection at MembershipController+<GetMembershipStatus>d_3.Move... MembershipService.dll unguard-membership-service-*	 Critical  
<input type="checkbox"/> S-2011: Improper input validation at JndiManager.lookup():128 SpringBoot org.dynatrace.ssrfservice.Application unguard-proxy-service-*	 Critical  

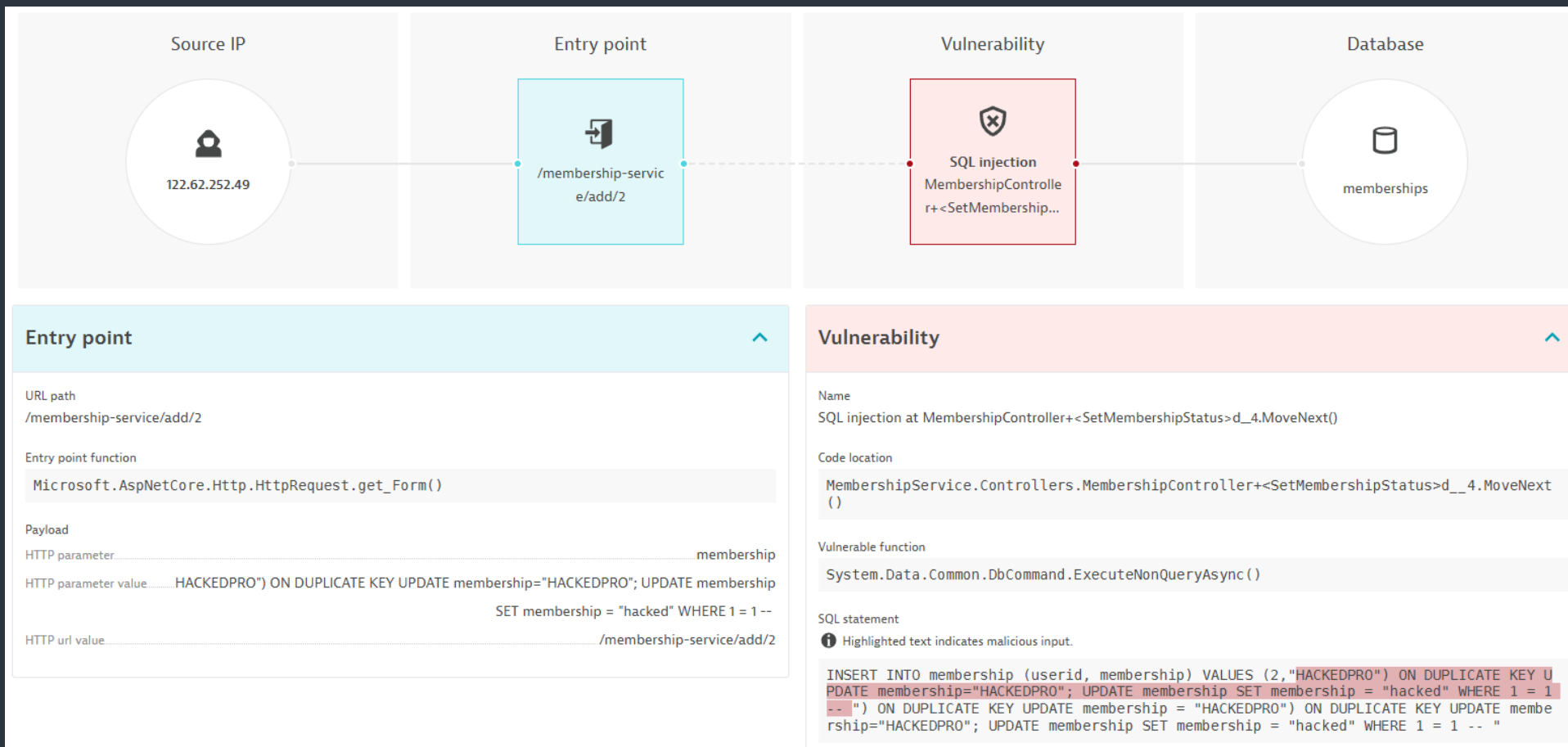
Application protection

Wykrywając podatność w kodzie, Dynatrace może analizować wykonywane transakcje w kierunku wykorzystania podatności




Application protection

Dla każdego ataku prezentowane są jego szczegóły – między innymi typ, zaatakowany process, entry point, IP atakującego. Wyświetlany jest wektor ataku oraz parametry



Application protection

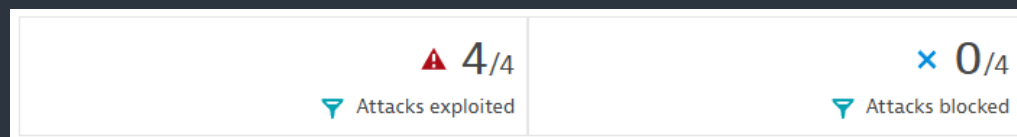
Automatycznie prezentowane są logi aplikacyjne z czasu ataku:

Process-related logs around attack timestamp			
Timestamp	State	Content	
Apr 09 19:16	Info	info: MembershipService.Controllers.MembershipController[0] GET requested => userid: 5184	
Apr 09 19:16	Info	info: MembershipService.Controllers.MembershipController[0] Executing query: SELECT membership FROM membership WHERE userid = 5184	
Apr 09 19:16	Info	info: MembershipService.Controllers.MembershipController[0] Membership status of userid 5184: FREE	
Apr 09 19:16	Info	info: MembershipService.Controllers.MembershipController[0] INSERT requested => userid: 2, membership: HACKEDPRO") ON DUPLICATE KEY UPDATE membership="HACKEDPRO"; UPDATE membership SET membership = "hacked" WHERE 1 = 1 --	
Apr 09 19:16	Info	info: MembershipService.Controllers.MembershipController[0] Executing query: INSERT INTO membership (userid, membership) VALUES (2,"HACKEDPRO") ON DUPLICATE KEY UPDATE membership="HACKEDPRO"; UPDATE membership SET membership = "hacked" WHERE 1 = 1 -- ") ON DUPLICATE KEY UPDATE membership = "HACKEDPRO") ON DUPLICATE KEY UPDATE membership="HACKEDPRO"; UPDATE membership SET membership = "hacked" WHERE 1 = 1 -- "	
View all process-related logs			

Application protection

Dynatrace może pracować w trybie wykrycia ataku ale również blokowania – w zależności od konfiguracji.

Blokada ataku następuje na poziomie pojedynczej transakcji – pozostałe, prawidłowe transakcje nie są zatrzymywane.



Application Protection: General settings

[Runtime Application Protection](#) allows you to control how Dynatrace handles incoming attacks to your applications on a global scale. To set up specific rules or exceptions, go to the [Monitoring rules](#) settings page.

☒ Enable Runtime Application Protection

Note: This functionality consumes Application Security units. For details, see the [Application Security Monitoring documentation](#).

Define global incoming attack control

Attack control Java

Block; incoming attacks detected and blocked.

Attack control .NET Early adopter

Monitor; incoming attacks detected only.

Security Posture Management

Security overview

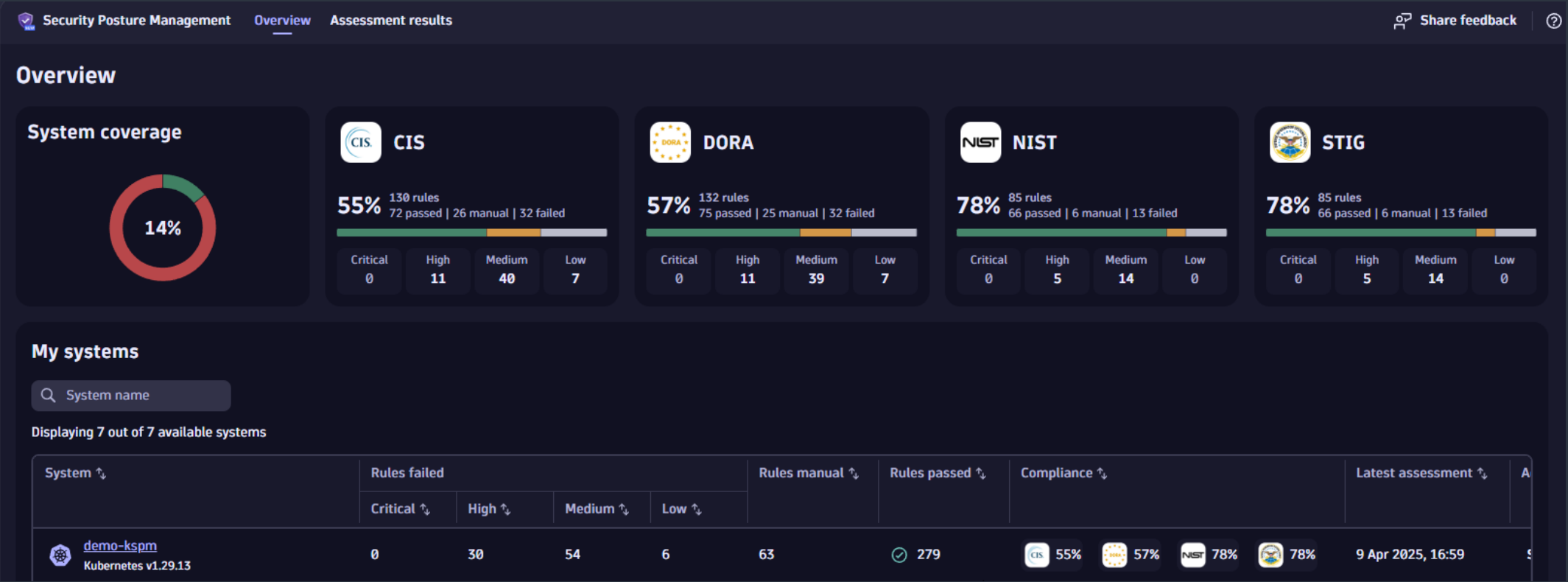
Konfiguracja

3rd party

Code-level &
Application
Protection

Compliance

Analiza logów



Security Investigator

Security overview

Konfiguracja

3rd party

Code-level &
Application
Protection

Compliance

Analiza logów

Security Investigator

+ Case

Upload

Threat hunting

Share

2024-03-06 21:00 to 2024-03-06 23:50

Rerun

```
1 fetch logs
2 | filter k8s.container.name == "coredns"
3 | parse content, "[' LD:severity ']"
4 IPADDR:source_ip ':'
5 INT:source_port '-'
6 INT:id
7 ' ' (LD:type LD:class LD:name LD:proto LONG:size LD:do LONG:bufsize)(fs=" ") ' '
8 LD:rcode ' '
9 LD:flags ' '
```


1,000 records

Executed at: 3/7/2024, 10:45:36, Timeframe: 3/6/2024, 21:00:00 - 23:50:00, Scanned bytes: 120 MB

Find keywords

timestamp (timestamp)	content (string)	severity...	source_ip (ip_addres...	source_port (long)	id (lon...	ty
2024-03-06T23:25:21.575+01...	[INFO] 172.31.29.138:35790 - 44809 "A IN 1b0a0f.2f736269...	INFO	172.31.29.138	35790	44809	A
2024-03-06T23:25:21.604+01...	[INFO] 172.31.29.138:39403 - 5208 "A IN 1b0c0f.6f67696e0...	INFO	172.31.29.138	39403	5208	A
2024-03-06T23:25:21.621+01...	[INFO] 172.31.29.138:40203 - 21239 "A IN 1b0d0f.313a476e...	INFO	172.31.29.138	40203	21239	A
2024-03-06T23:25:22.682+01...	[INFO] 172.31.29.138:54665 - 39367 "A IN 090107.65776f67...	INFO	172.31.29.138	54665	39367	A
2024-03-06T23:25:22.691+01...	[INFO] 172.31.29.138:47884 - 58825 "A IN 090207.4a745a5...	INFO	172.31.29.138	47884	58825	A
2024-03-06T23:25:22.710+01...	[INFO] 172.31.29.138:51825 - 19627 "A IN 090407.466a593...	INFO	172.31.29.138	51825	19627	A
2024-03-06T23:25:22.719+01...	[INFO] 172.31.29.138:36161 - 21206 "A IN 090507.58434a7...	INFO	172.31.29.138	36161	21206	A
2024-03-06T23:25:22.736+01...	[INFO] 172.31.29.138:50176 - 59040 "A IN 090707.496a6f67...	INFO	172.31.29.138	50176	59040	A
2024-03-06T23:25:23.784+01...	[INFO] 172.31.29.138:35343 - 55098 "A IN 6d0207.4a745a5...	INFO	172.31.29.138	35343	55098	A
2024-03-06T23:25:23.794+01...	[INFO] 172.31.29.138:56457 - 51656 "A IN 6d0307.5a32556...	INFO	172.31.29.138	56457	51656	A
2024-03-06T23:25:23.802+01...	[INFO] 172.31.29.138:41911 - 7980 "A IN 6d0407.466a5932...	INFO	172.31.29.138	41911	7980	A
2024-03-06T23:25:23.811+01...	[INFO] 172.31.29.138:57537 - 49168 "A IN 6d0507.58434a7...	INFO	172.31.29.138	57537	49168	A
2024-03-06T23:25:23.819+01...	[INFO] 172.31.29.138:58939 - 46972 "A IN 6d0607.56755a3...	INFO	172.31.29.138	58939	46972	A
2024-03-06T23:25:24.815+01...	[INFO] 172.31.29.138:37761 - 21911 "A IN 4e0103.4c696e7...	INFO	172.31.29.138	37761	21911	A
2024-03-06T23:25:24.825+01...	[INFO] 172.31.29.138:42893 - 64006 "A IN 4e0203.342e616...	INFO	172.31.29.138	42893	64006	A
2024-03-06T23:25:24.837+01...	[INFO] 172.31.29.138:49712 - 40008 "A IN 4e0303.696e757...	INFO	172.31.29.138	49712	40008	A
2024-03-06T23:25:25.870+01...	[INFO] 172.31.29.138:44570 - 13838 "A IN 720107.65776f67...	INFO	172.31.29.138	44570	13838	A
2024-03-06T23:25:25.882+01...	[INFO] 172.31.29.138:32842 - 15748 "A IN 720207.4a745a5...	INFO	172.31.29.138	32842	15748	A
2024-03-06T23:25:25.902+01...	[INFO] 172.31.29.138:44820 - 43322 "A IN 720407.466a593...	INFO	172.31.29.138	44820	43322	A

Query tree



Legend

- #1 Analyze Kubernetes audit logs
- #2 Investigate potential target
- #4 Find out how the commands were sent to the pod
- #3 Identify what data the pod sent out

Evidence lists

IoC

String

0

Attacker d...

String

tiitha-maliciousd...

Suspicious

IP

198.51.100.2

Safe

IP

0

Suspicious pod

IP

172.31.29.138

Notes

Security overview

Konfiguracja

3rd party

Code-level &
Application
Protection

Compliance

Analiza logów

