Semantix

Elastic Essential I

Aula 1

Quem sou eu?

Eu sou Rodrigo Augusto Rebouças.

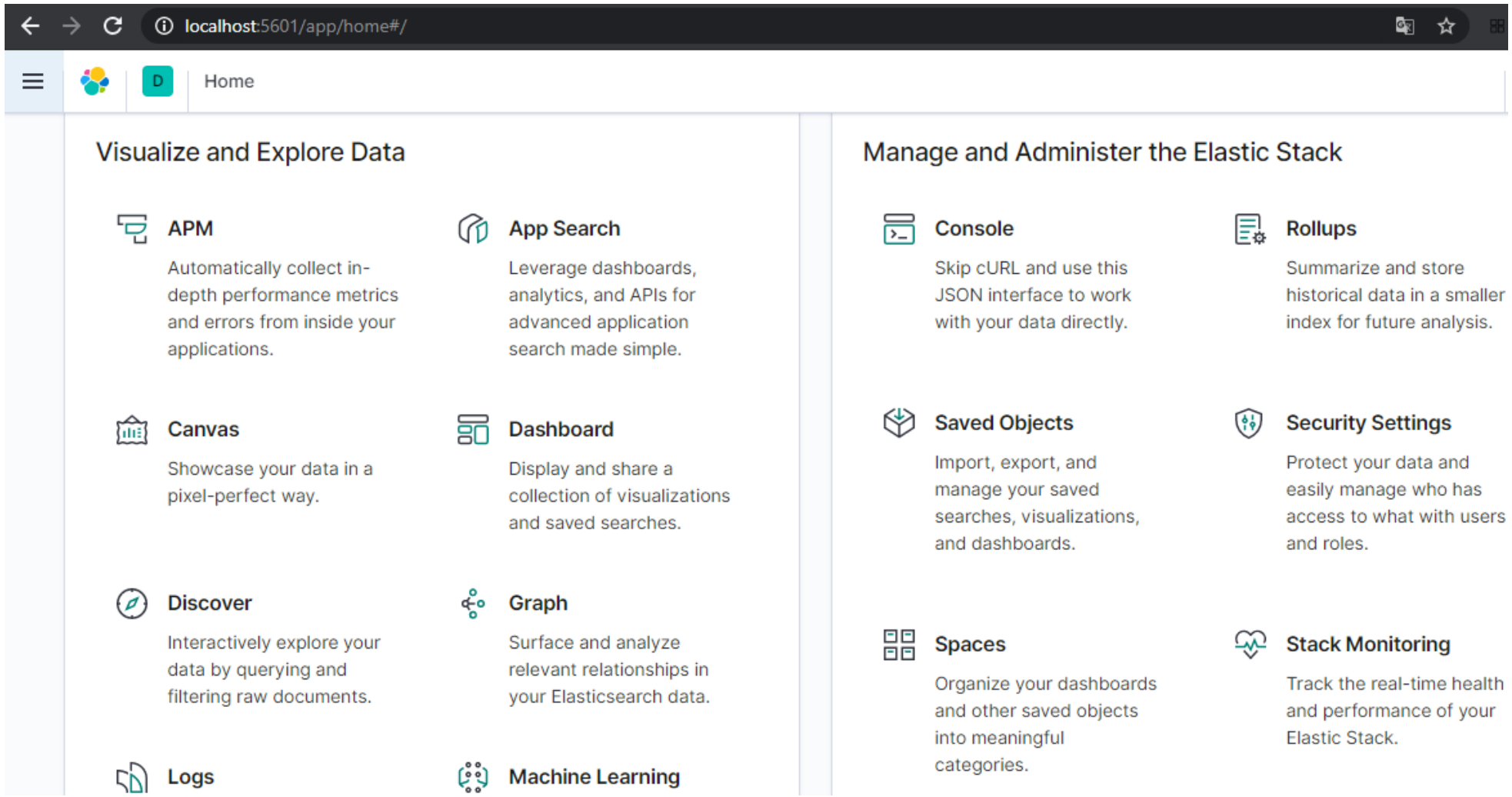
Engenheiro de dados da Semantix
Instrutor do Semantix Academy

Você pode me encontrar em:
rodrigo.augusto@semantix.com.br

Kibana

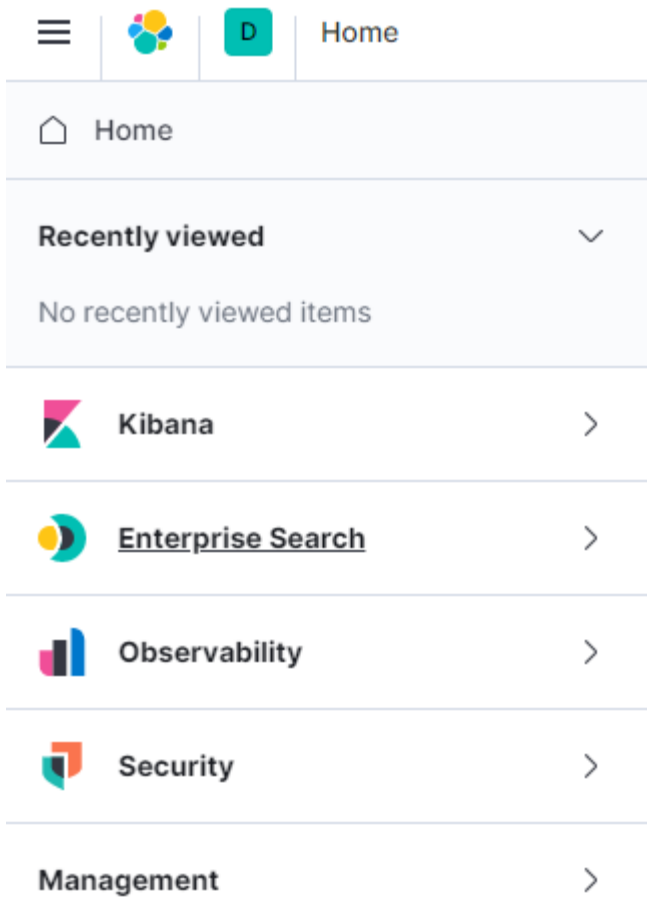
Semantix

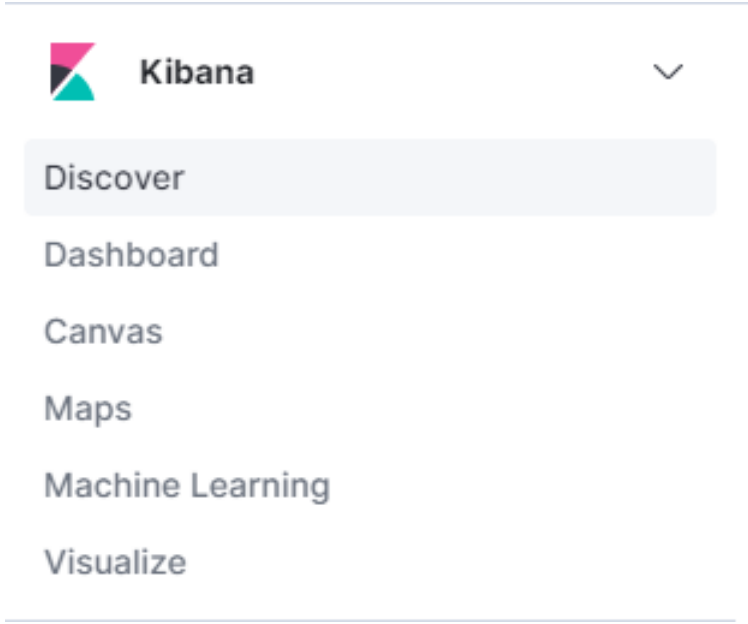
Interface Kibana



Semantix

Menu Kibana

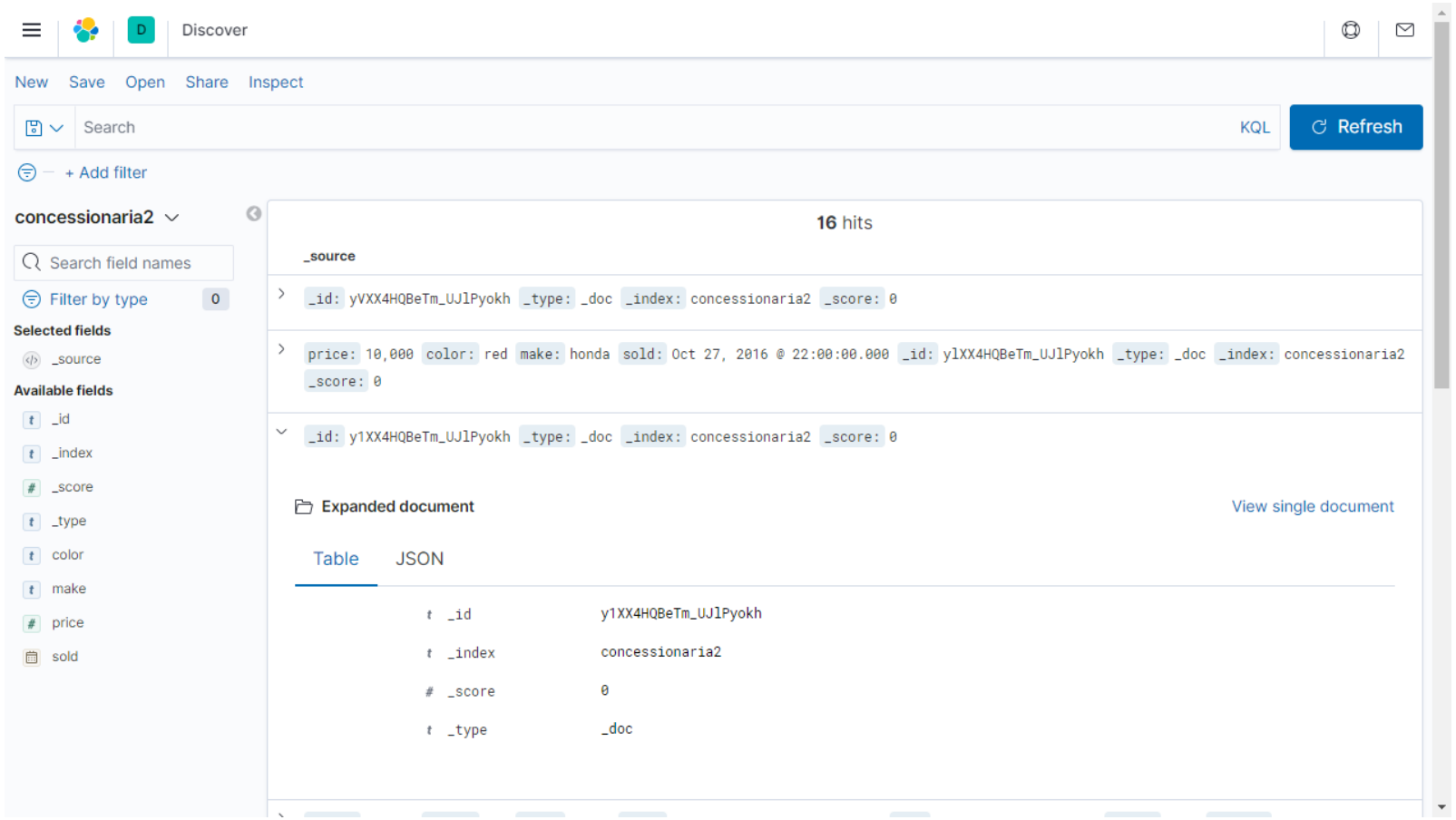




Semantix

Guia Discover

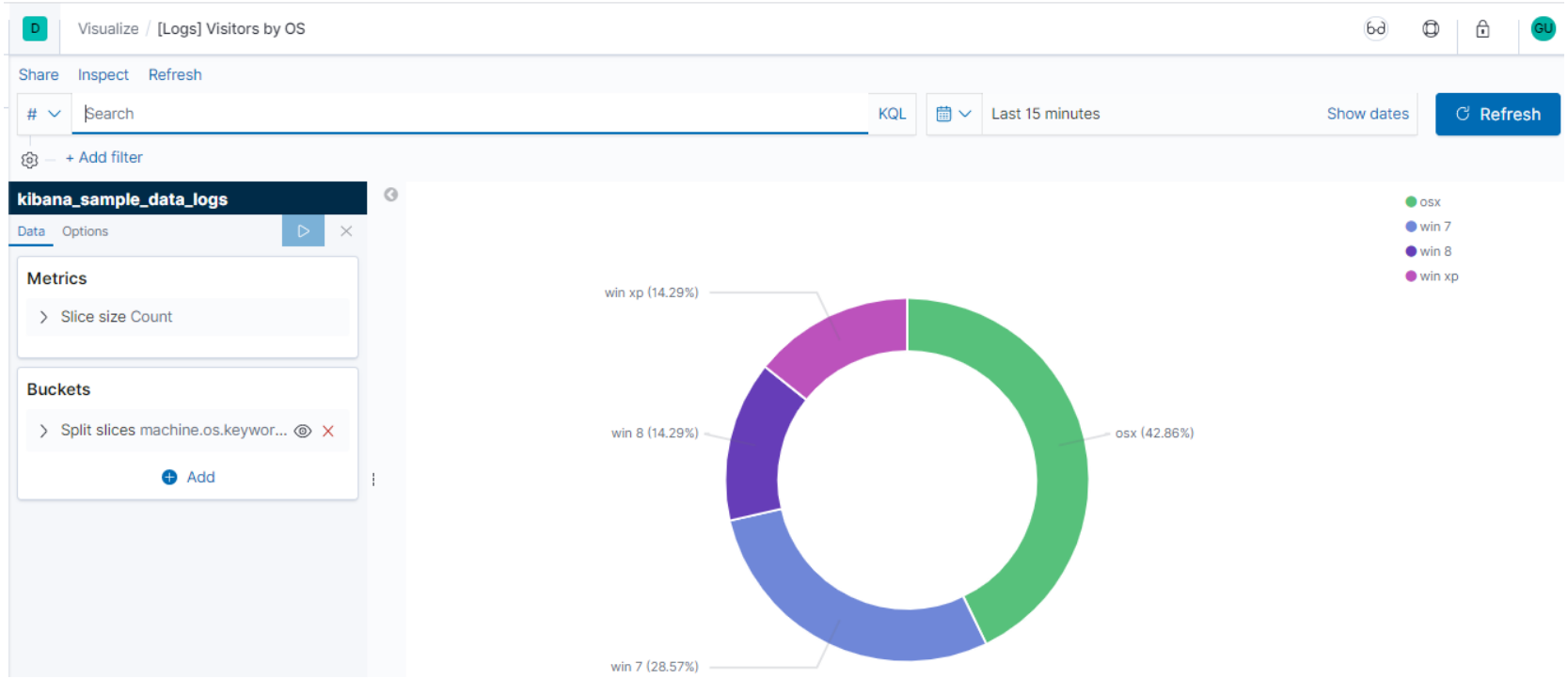
- Acessar, pesquisar e filtrar dados do índice selecionado
- Detalhes de campos da pesquisa
- Salvar pesquisas para usar no discover, visualizações e dashboards



Semantix

Guia Visualize

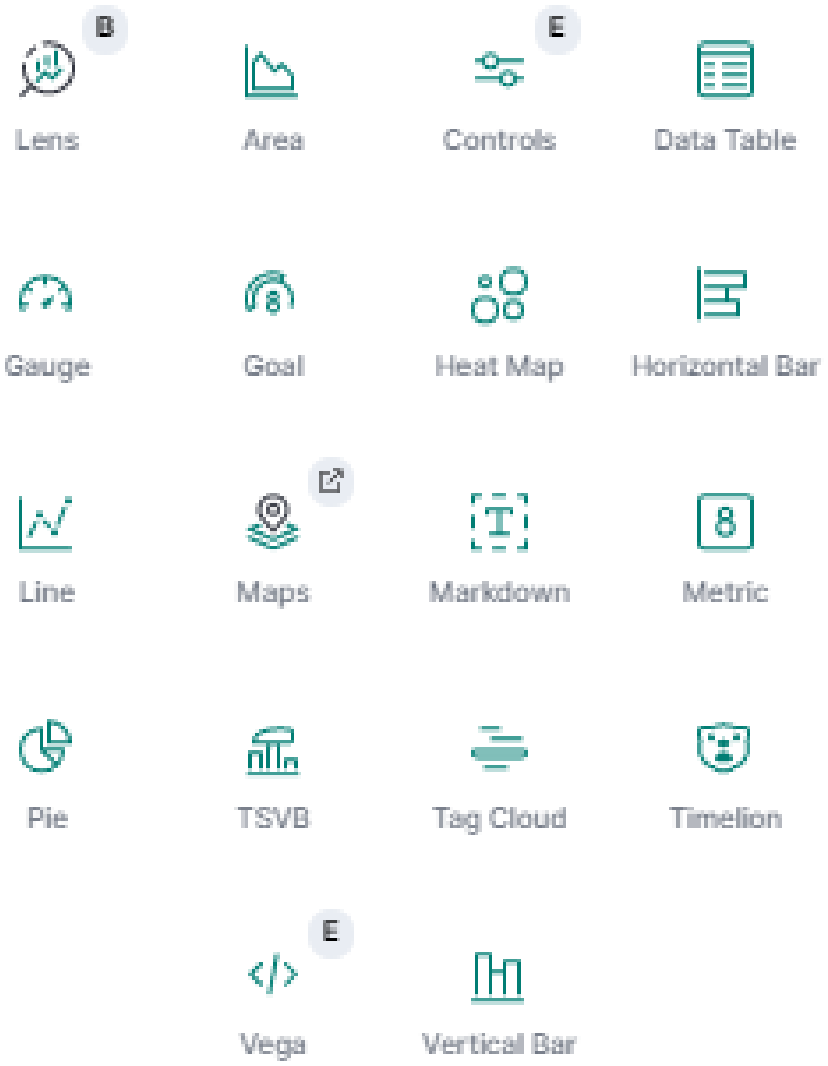
- Criar, editar e salvar visualizações dos dados
  - Consultas
  - Filtros
  - Agregações



Semantix

Guia Visualize

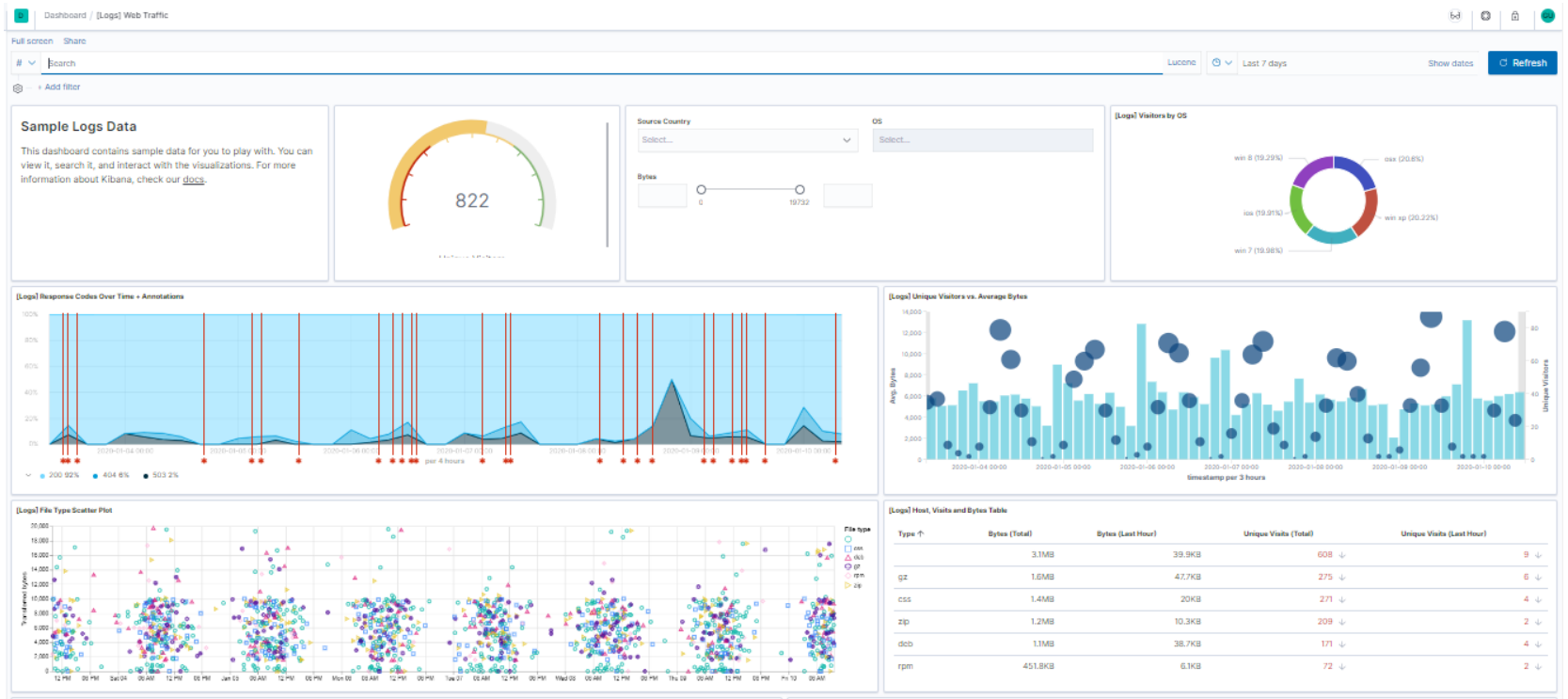
- Tipos de Visualizações



Semantix

Guia Dashboard

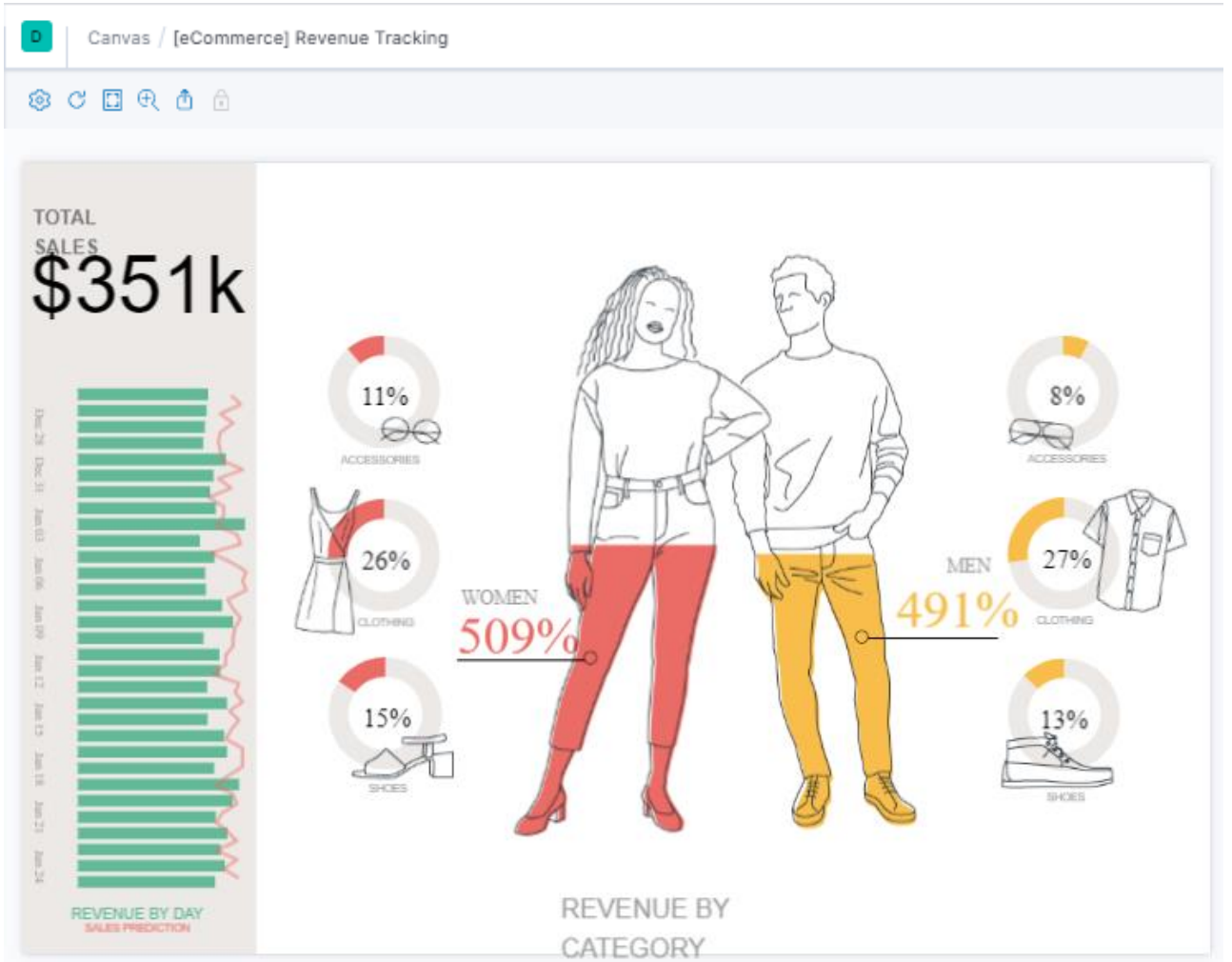
- Combinar várias visualizações de dados em um único lugar



Semantix

Guia Canvas

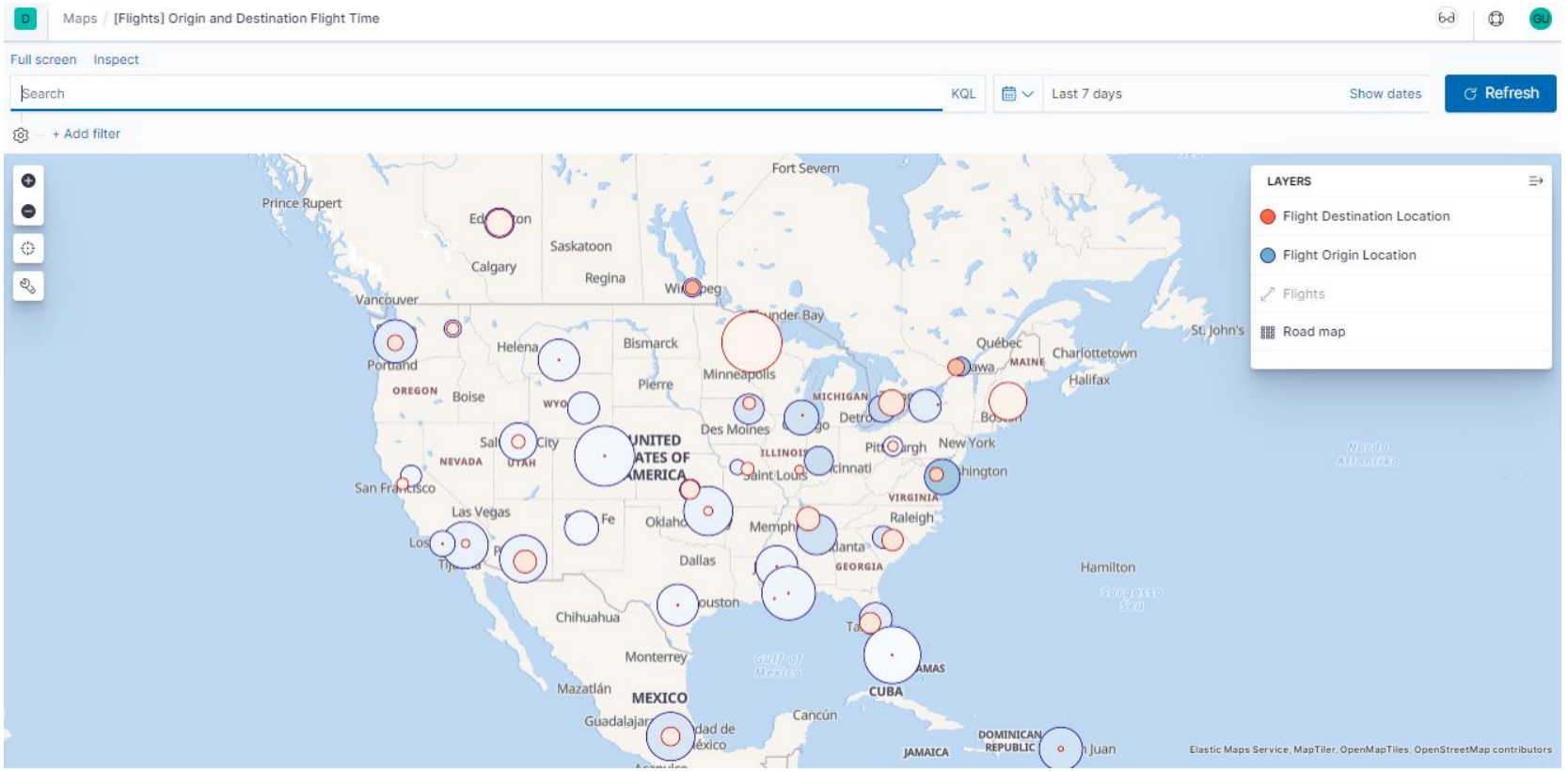
- Visualização e apresentação de dados
  - Páginas
  - Combinação
    - Cores
    - Imagens
    - Texto



Semantix

Guia Maps

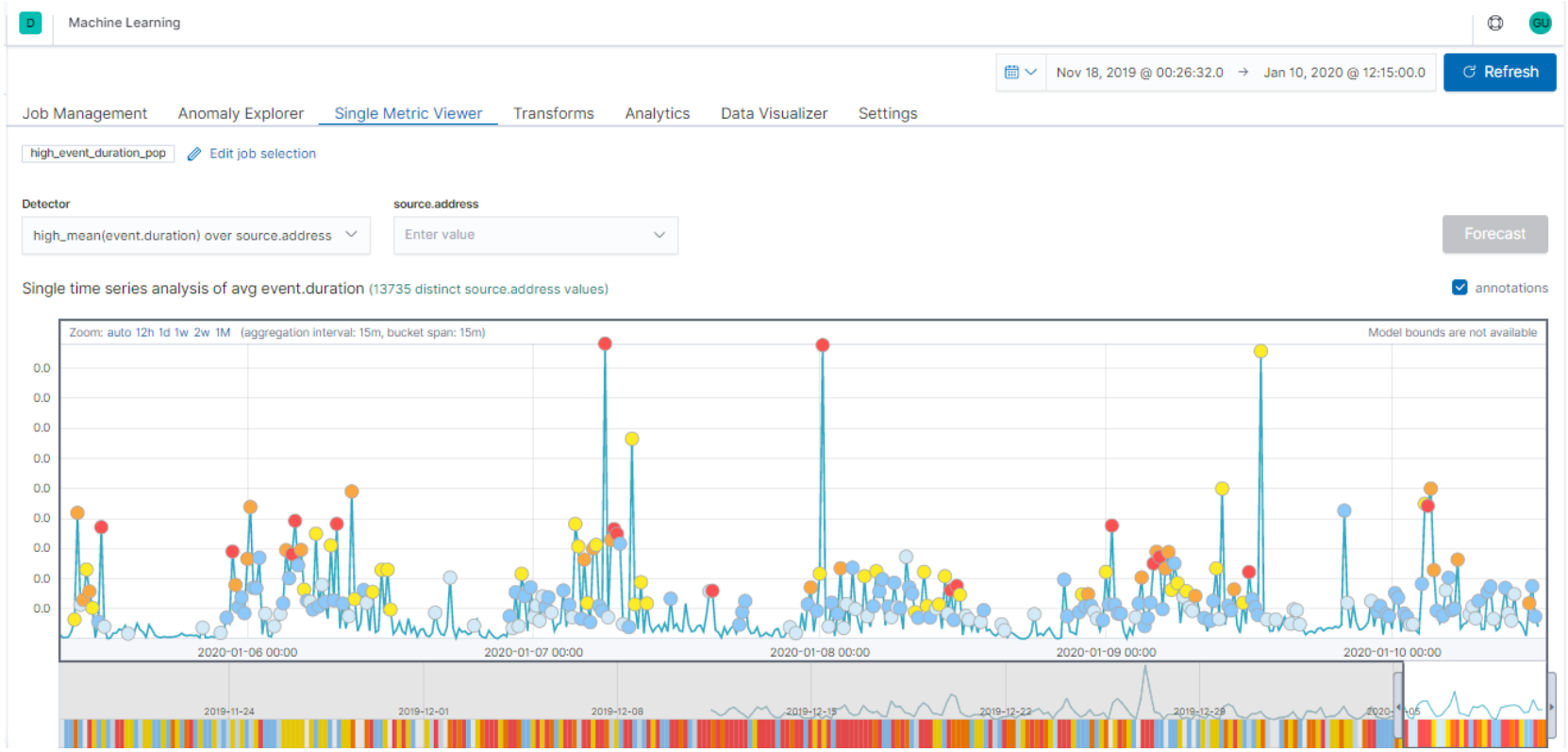
- Analisar dados geográfico em tempo real
  - Mapas com várias camadas e índices
  - Carregar arquivos GeoJSON



Semantix

Guia Machine Learning

- Gerenciamento de Jobs
  - Detector de anomalias
- Carregamento de dados

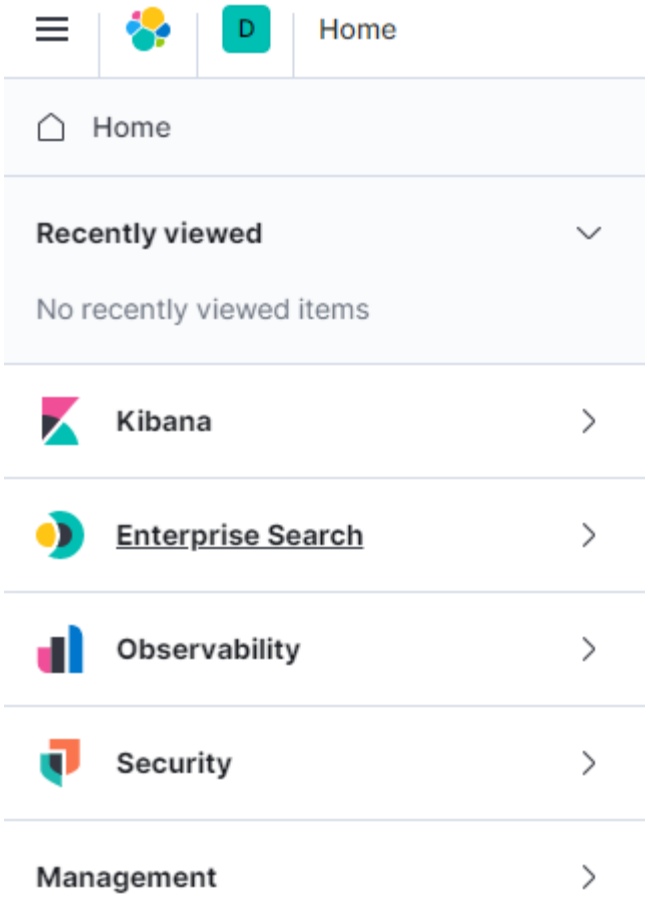


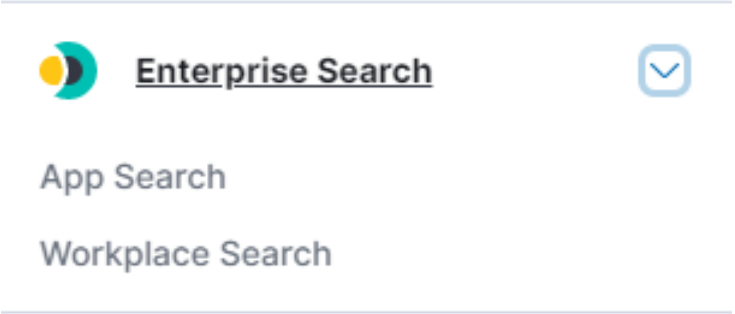
Semantix

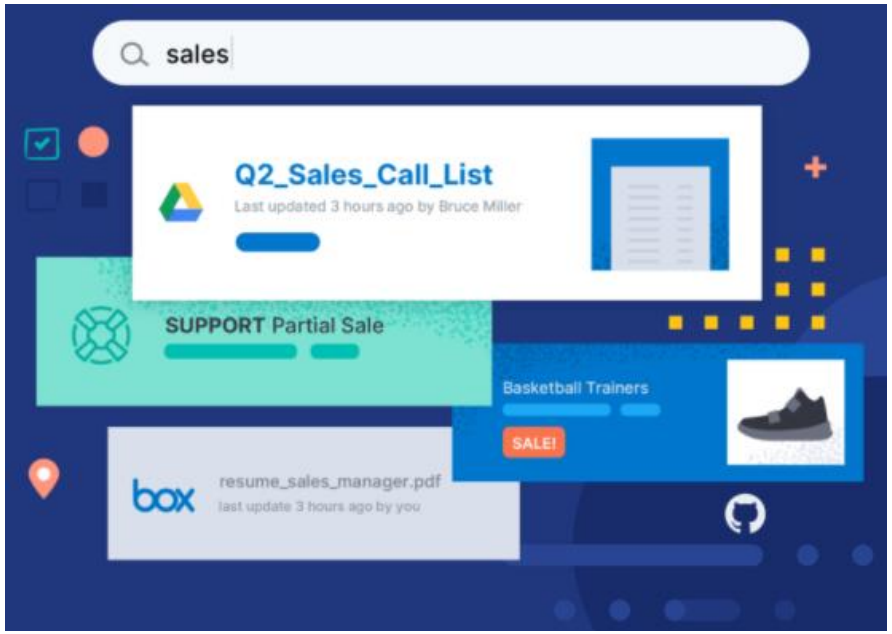
Enterprise Search

Semantix

Menu Enterprise Search







Semantix

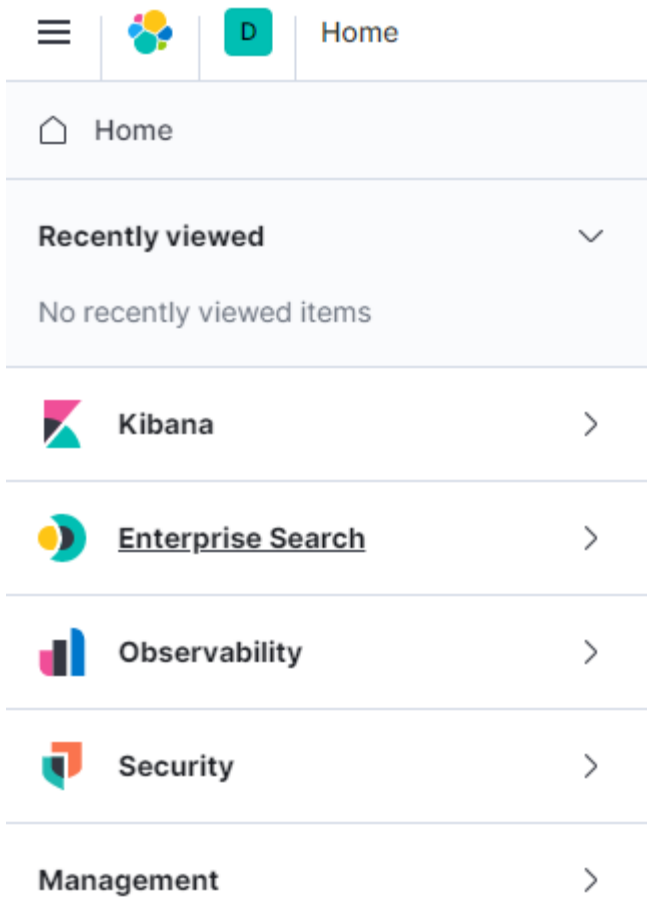
Guias App Search

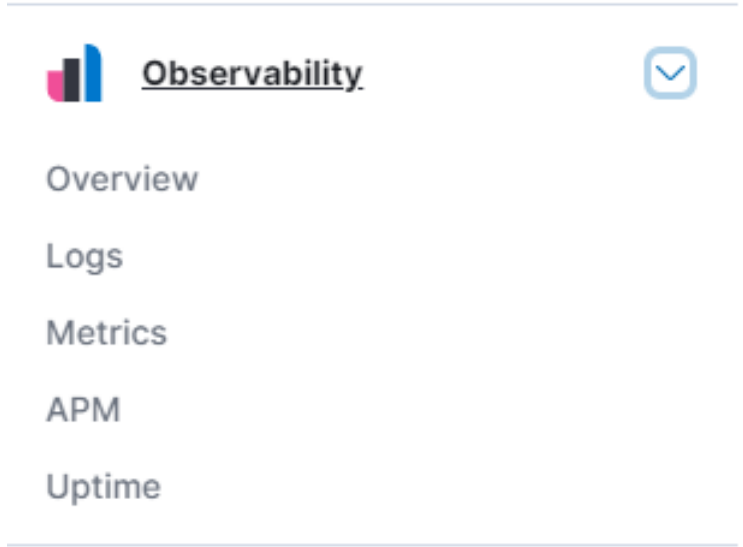
- Enterprise Search
  - https://www.elastic.co/guide/en/enterprise-search/7.9/index.html
- Pacotes
  - App Search
    - Fornecer ferramentas para projetar e implantar uma pesquisa poderosa em seus sites e aplicativos móveis
    - https://www.elastic.co/guide/en/app-search/current/index.html
  - Workplace Search
    - Unificar suas plataformas de conteúdo (Google Drive, Salesforce) em uma experiência de pesquisa personalizada
    - https://www.elastic.co/guide/en/workplace-search/current/index.html

Observability

Semantix

Menu Observability

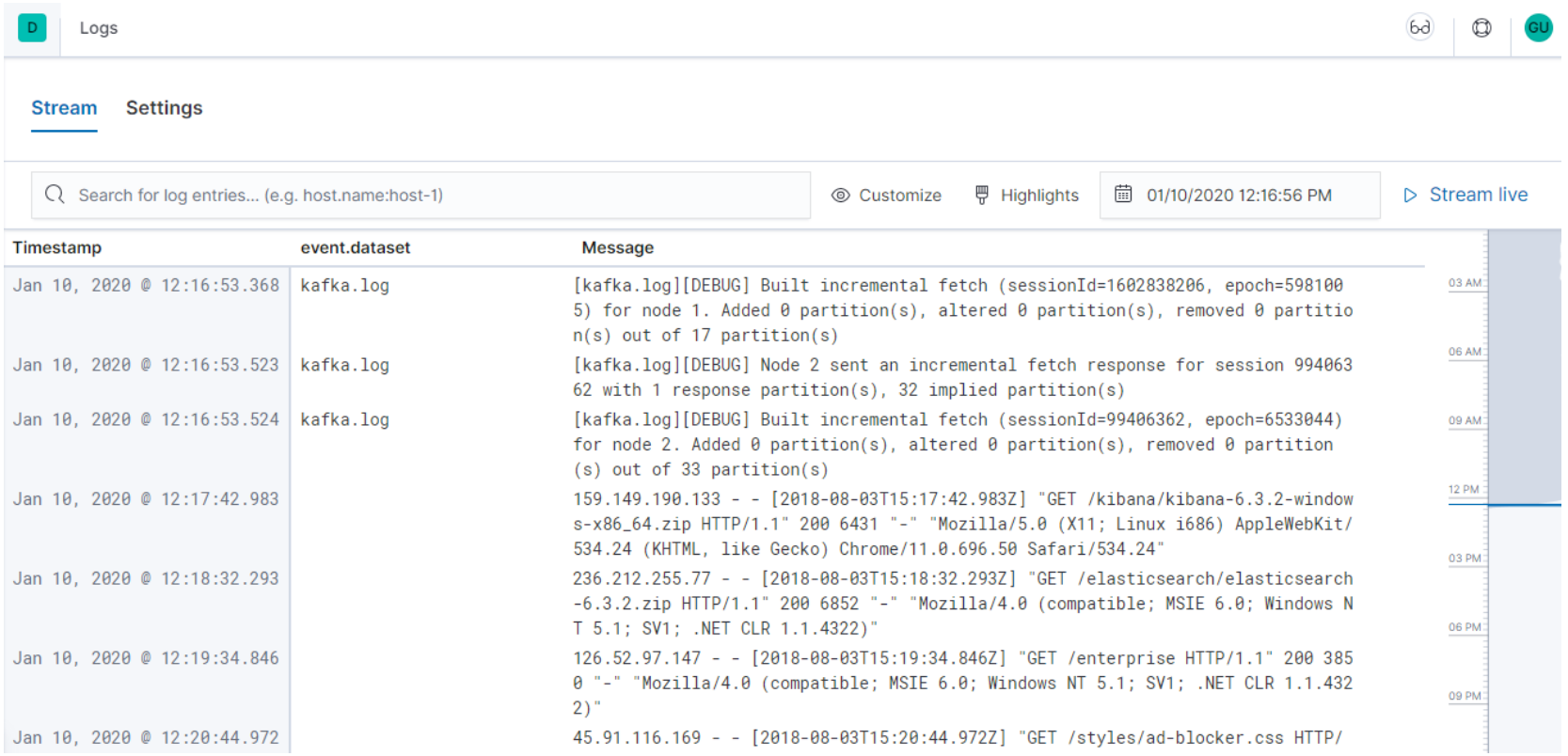




Semantix

Guia Logs

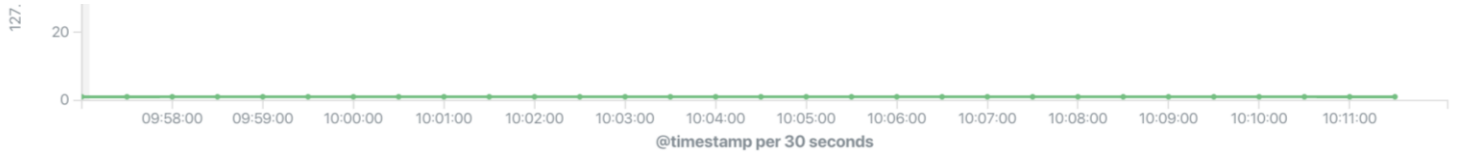
- Logs em tempo real
  - Filebeat
  - Visualizar campos dos logs
  - Visualizar no Uptime



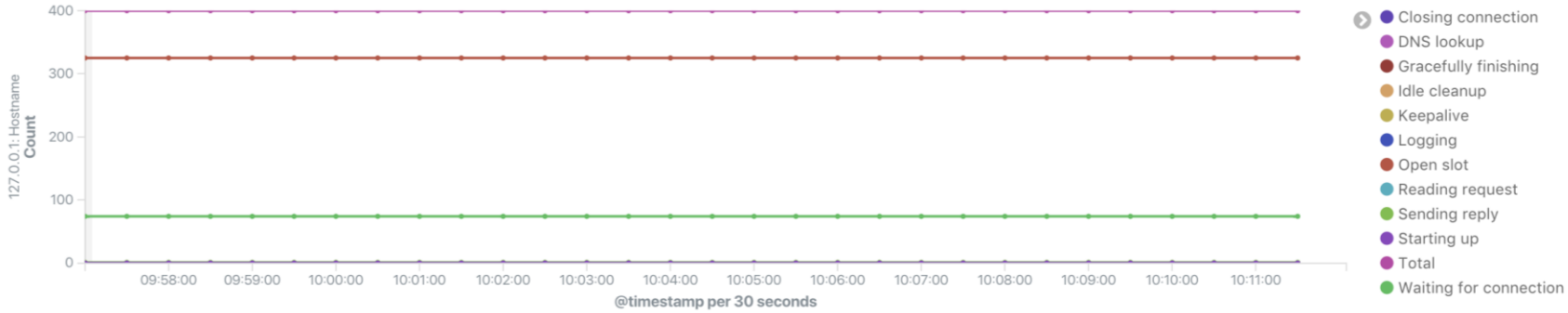
Semantix

Guia Metrics

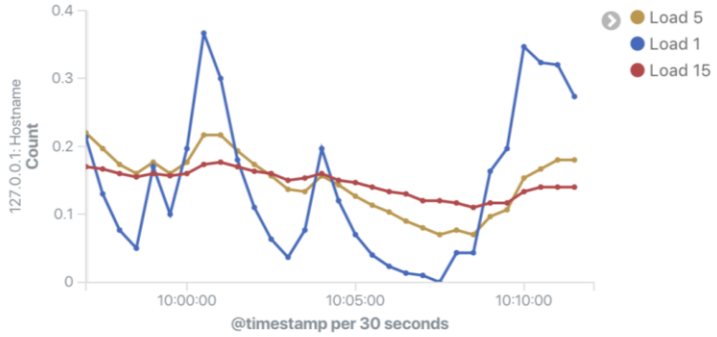
- Metricas em tempo real
  - Metricbeat



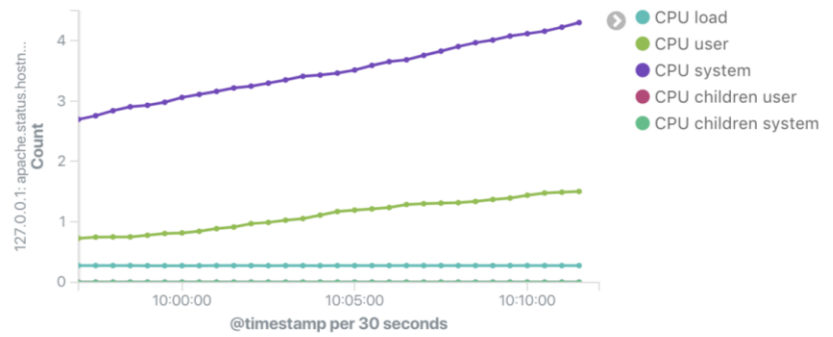
Scoreboard [Metricbeat Apache]



Load1/5/15 [Metricbeat Apache]



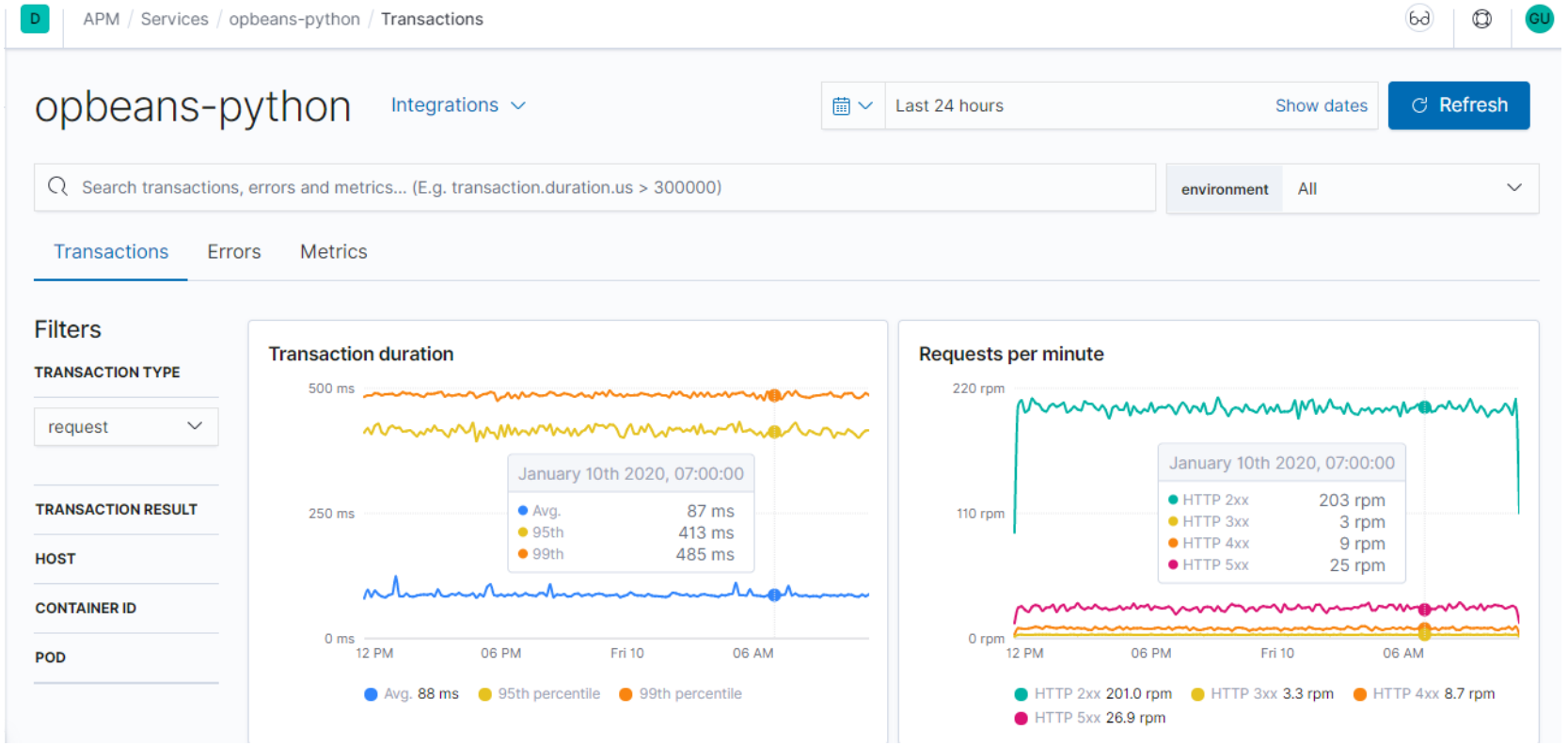
CPU usage [Metricbeat Apache]



Semantix

Guia APM

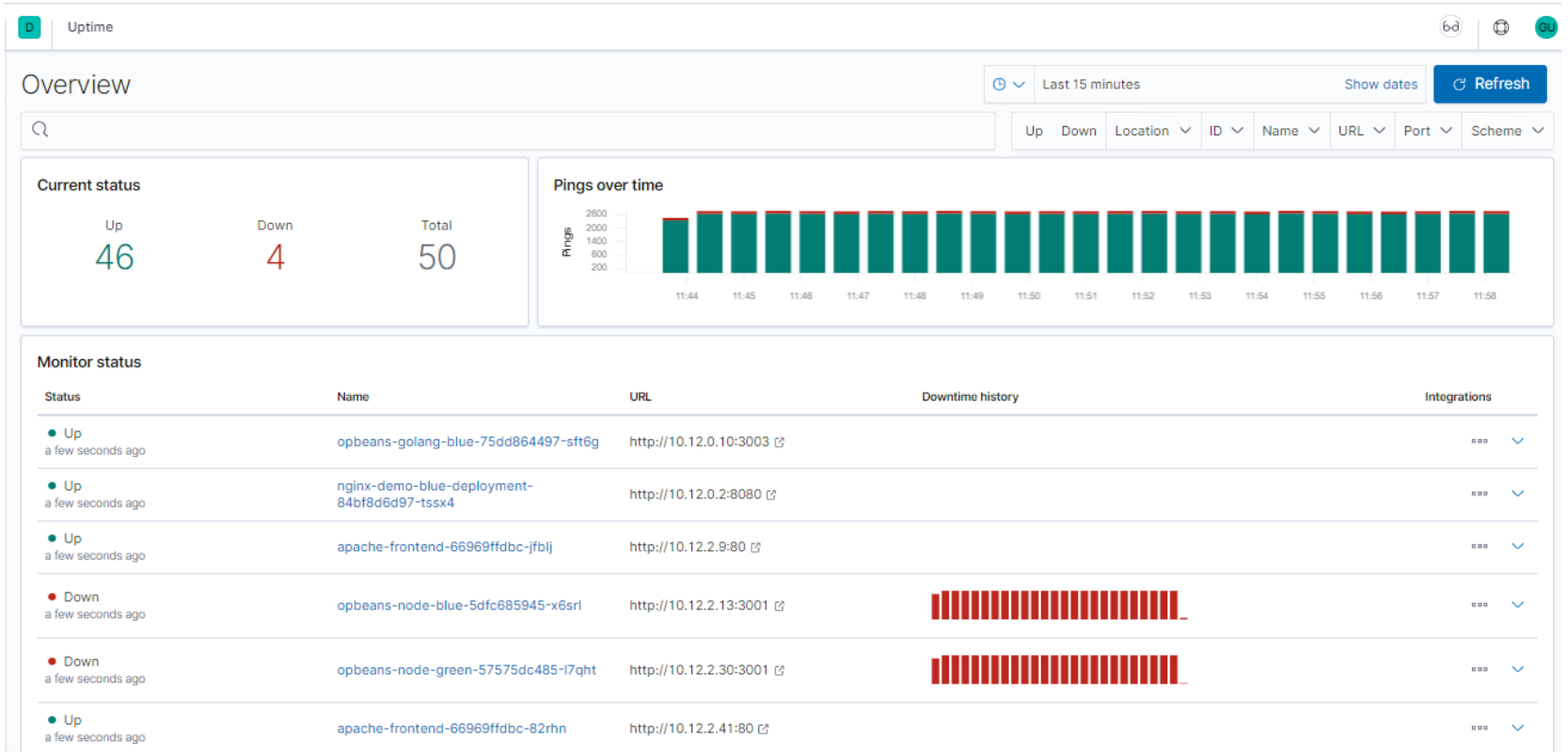
- Application Performance Monitoring
- Permite monitorar o desempenho de milhares de aplicativos em tempo real



Semantix

Guia Uptime

- Monitoramento em tempo real
  - Heartbeat

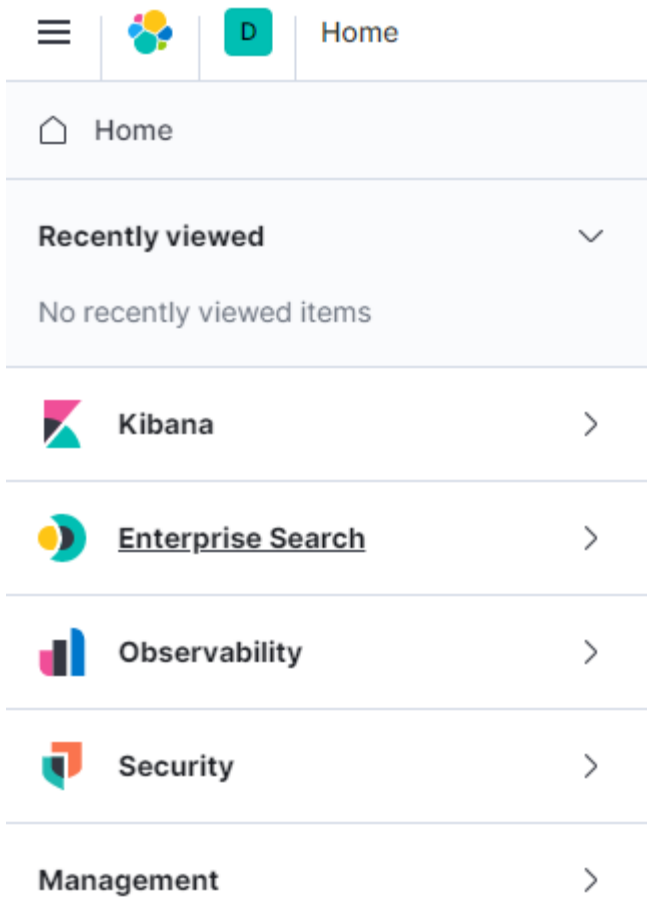


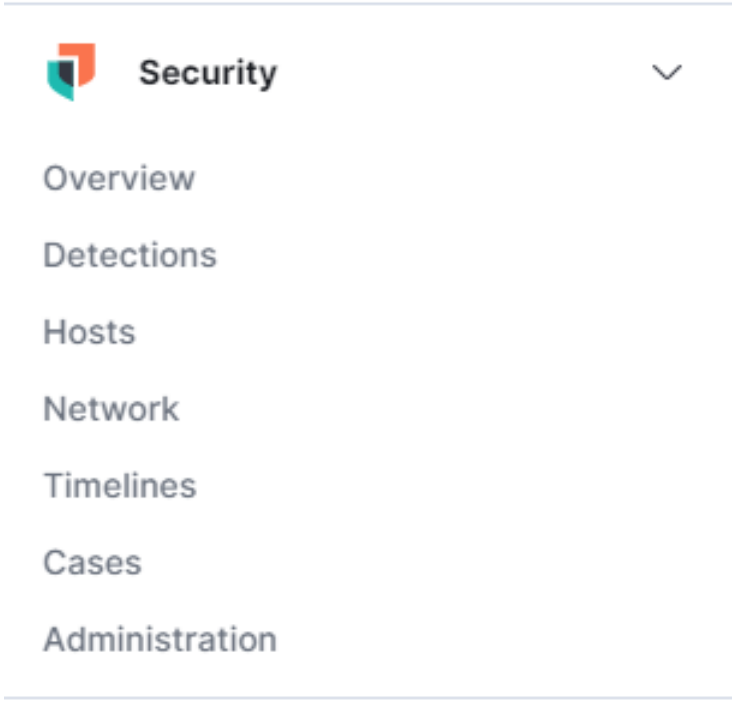
Semantix

Security

Semantix

Menu Security

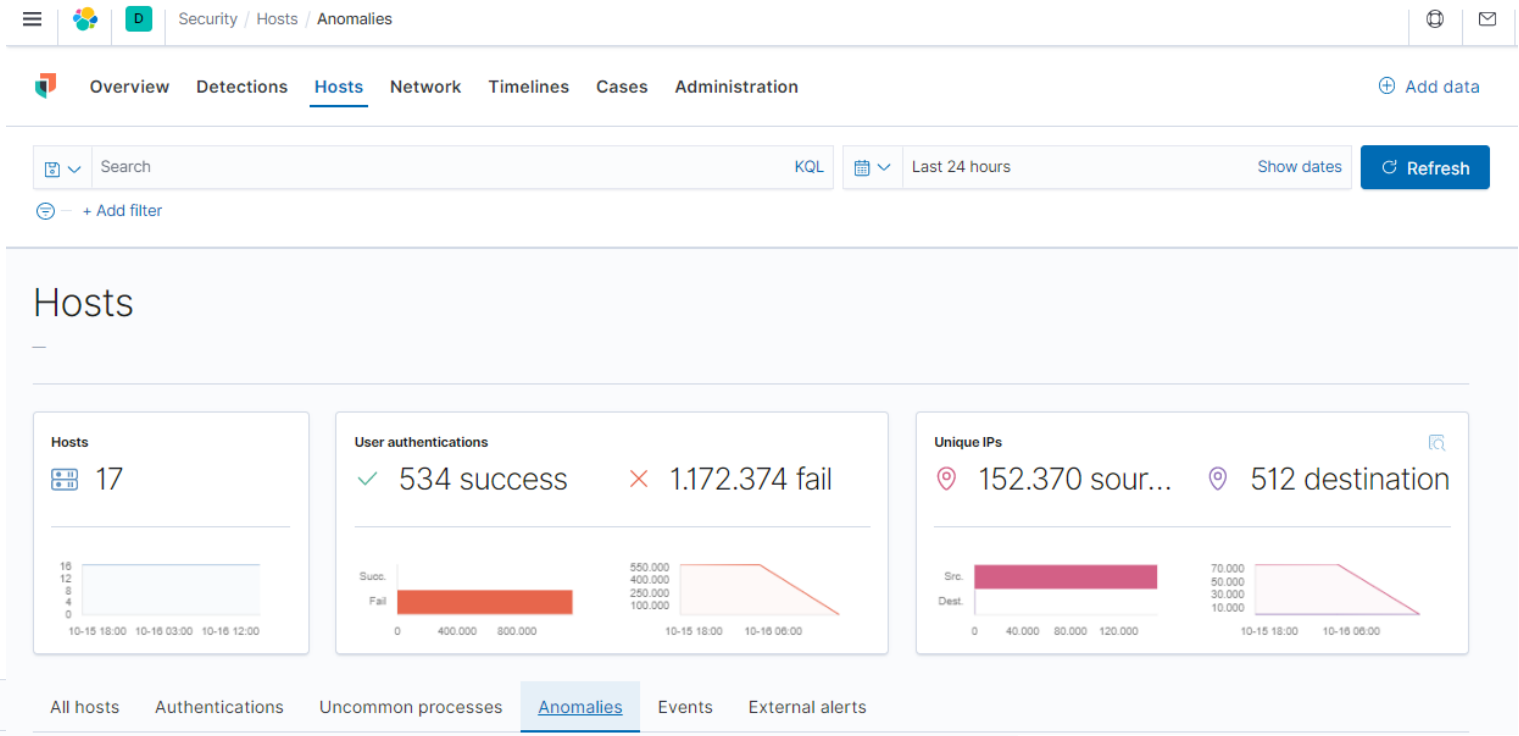


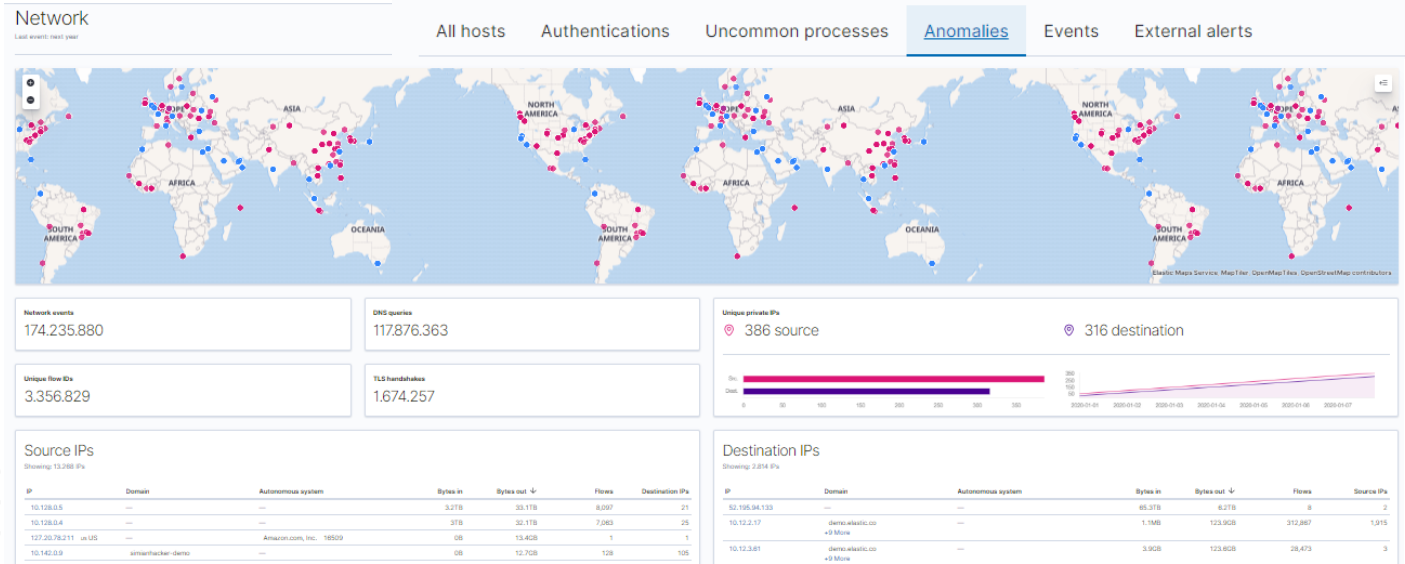


Semantix

Guia Overview - Security

- SIEM
  - Security Information & Event Management
- Análise de eventos de segurança relacionados ao host e a rede
  - Investigações de alertas
  - Procura de ameaças



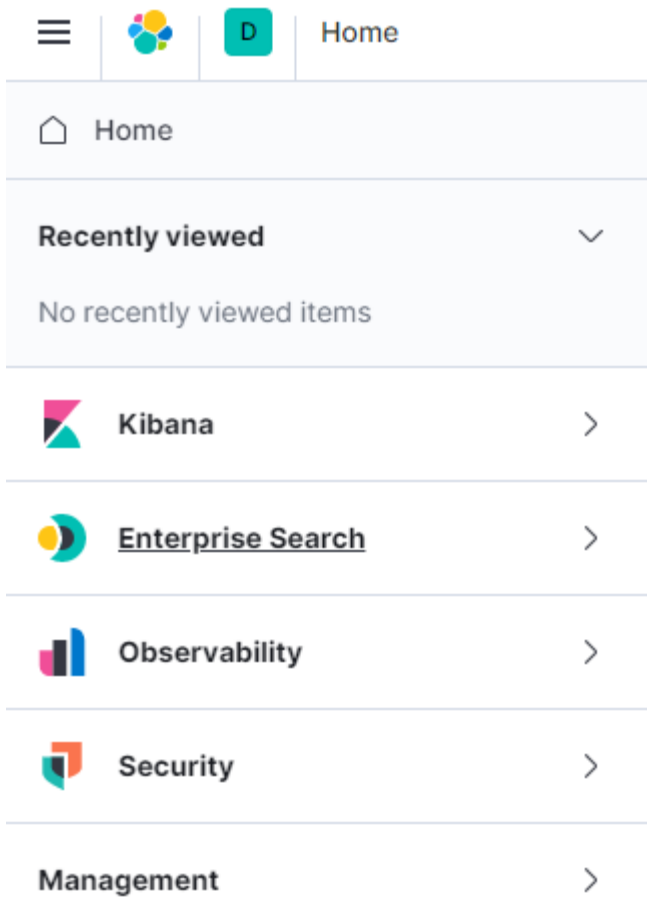


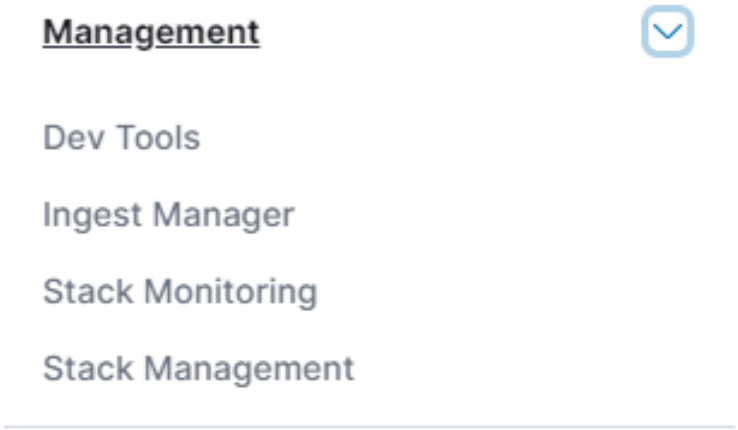
Semantix

Management

Semantix

Menu Management

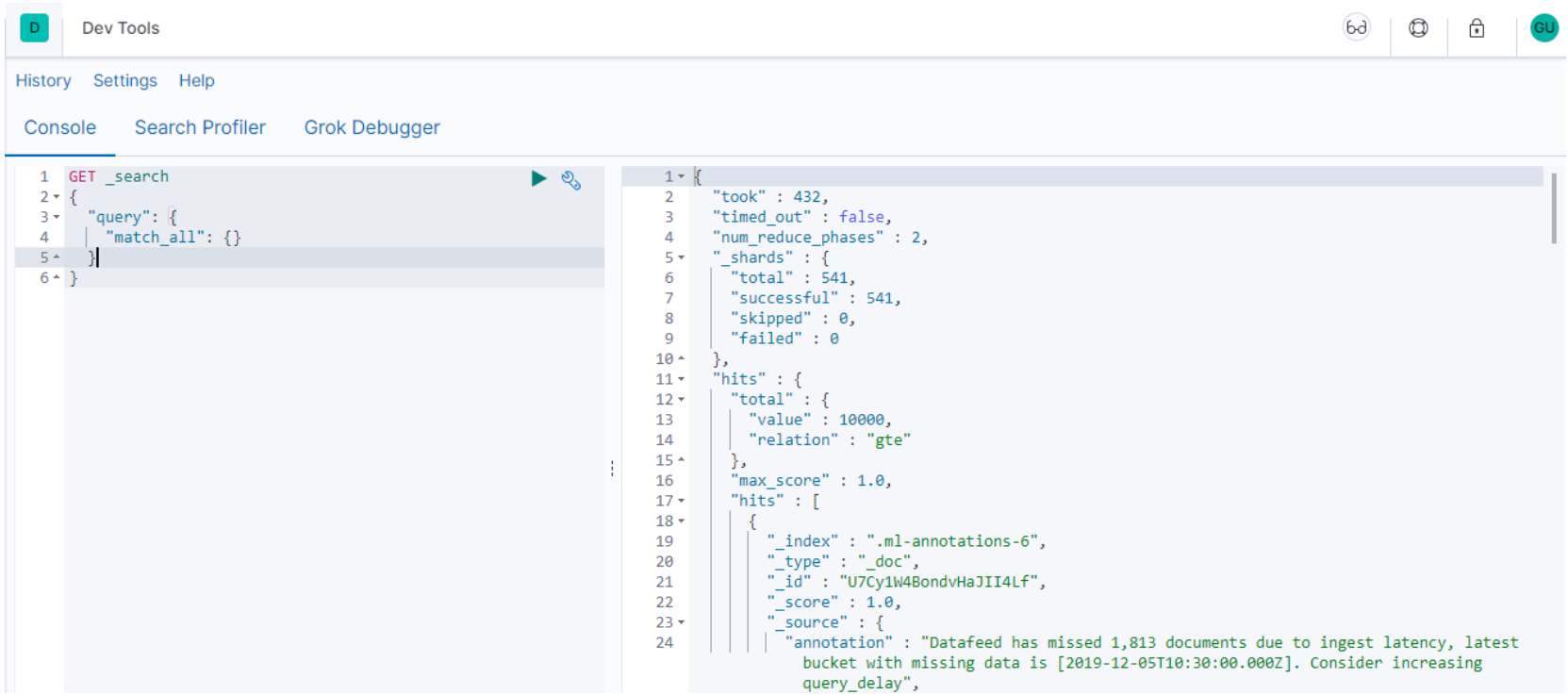




Semantix

Guia Dev Tools

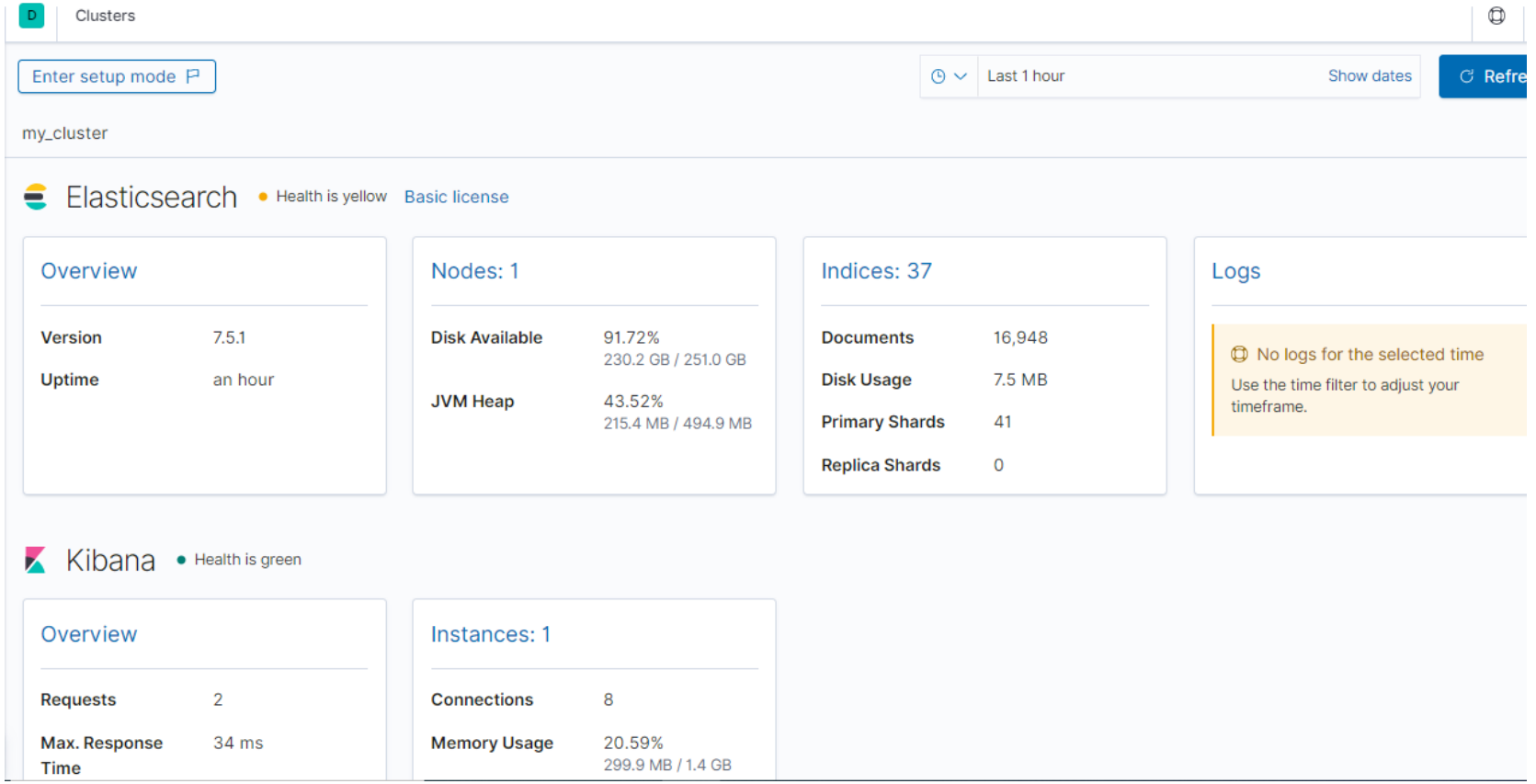
- Digitar request e enviá-las ao Elasticsearch



Semantix

Guia Stack Monitoring

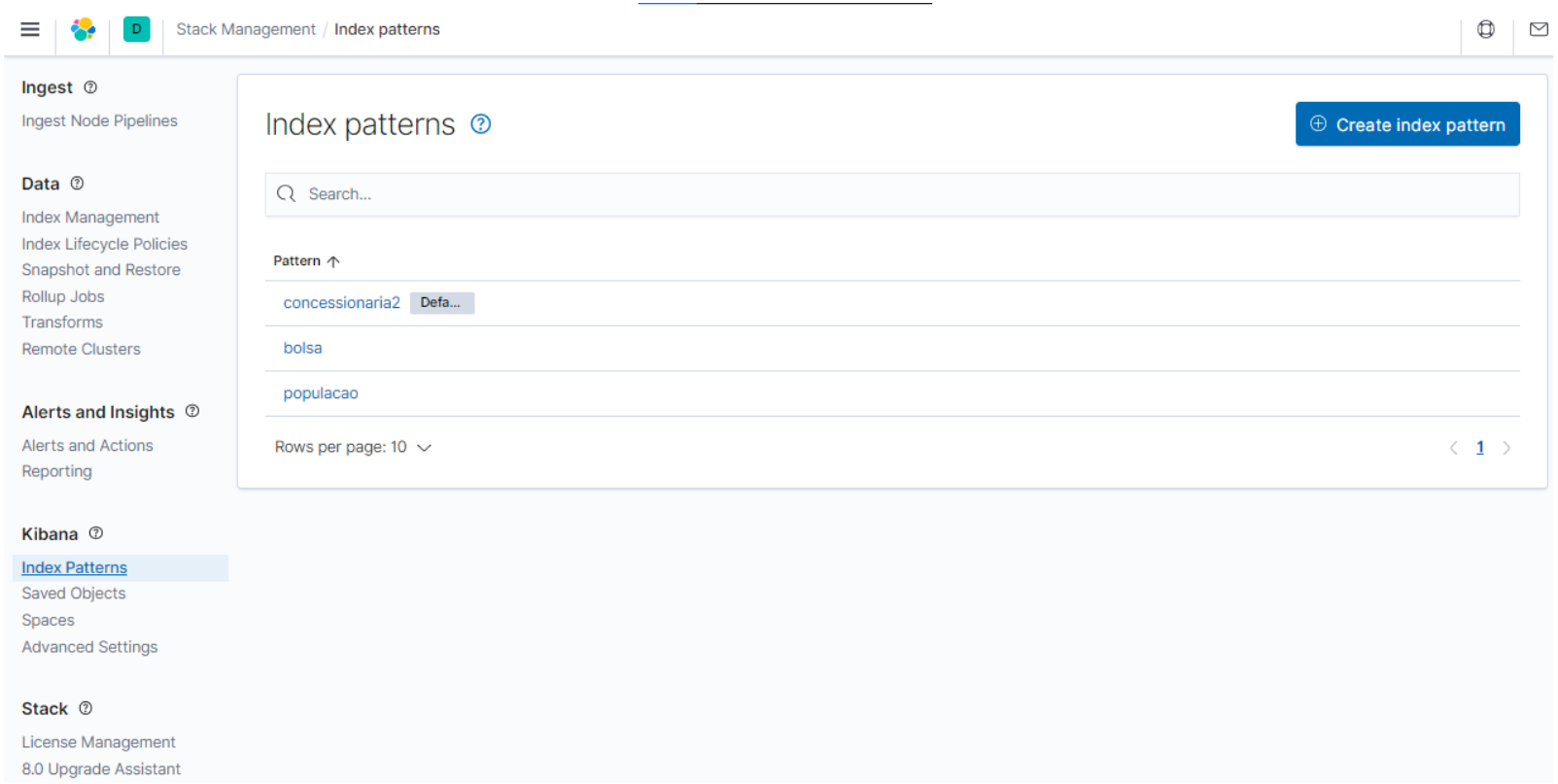
- Monitorar
  - Armazenamento
    - Disco
    - Memória
    - Heap
  - Saúde
    - Shards Primários
    - Shards Réplicas



Semantix

Guia Management

- Gestão dos índices
  - Saúde
  - Configurações
  - Ciclo de vida
  - Backup
- Index para Visualizações
  - Index pattern
- Configurações do kibana
- Segurança e regras de usuário



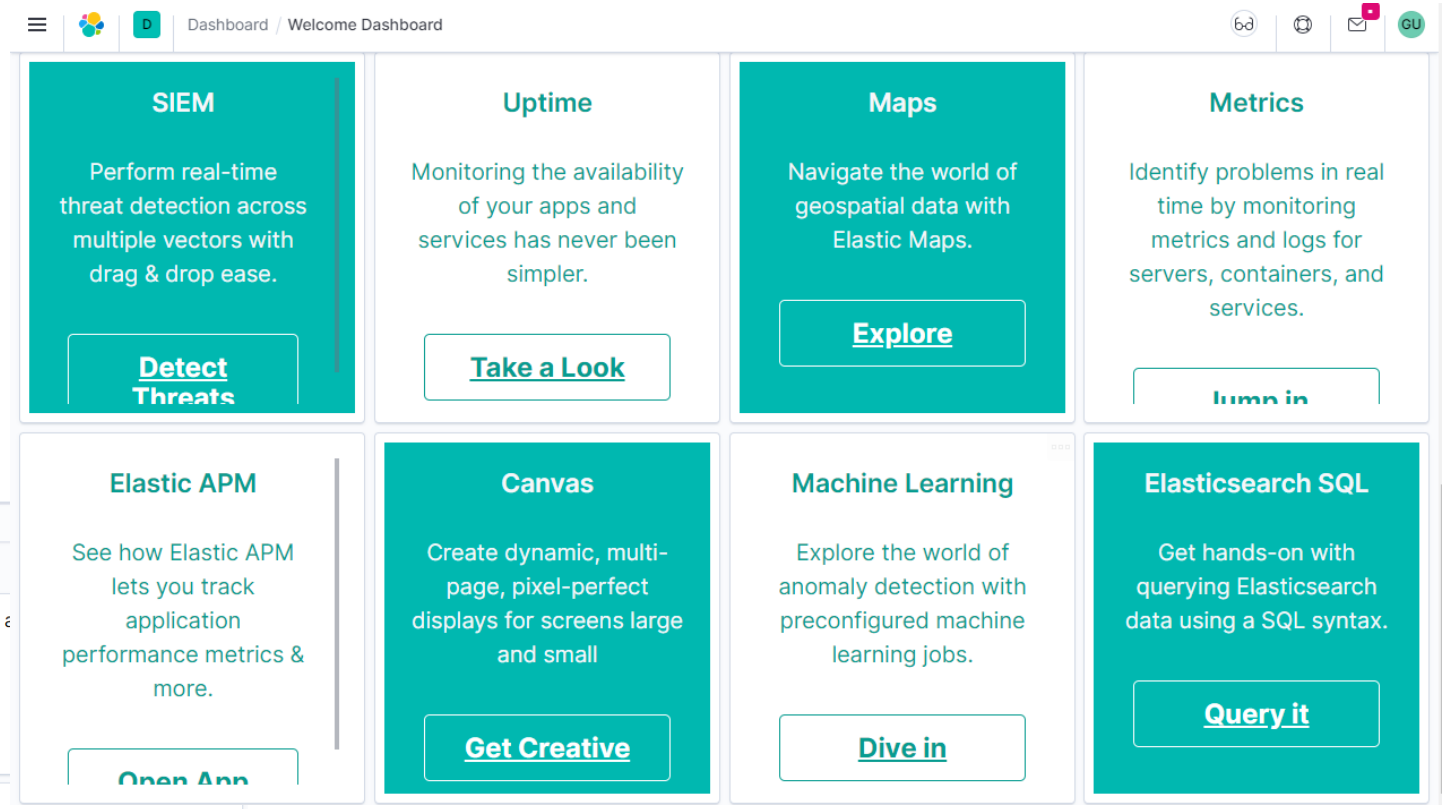
Semantix

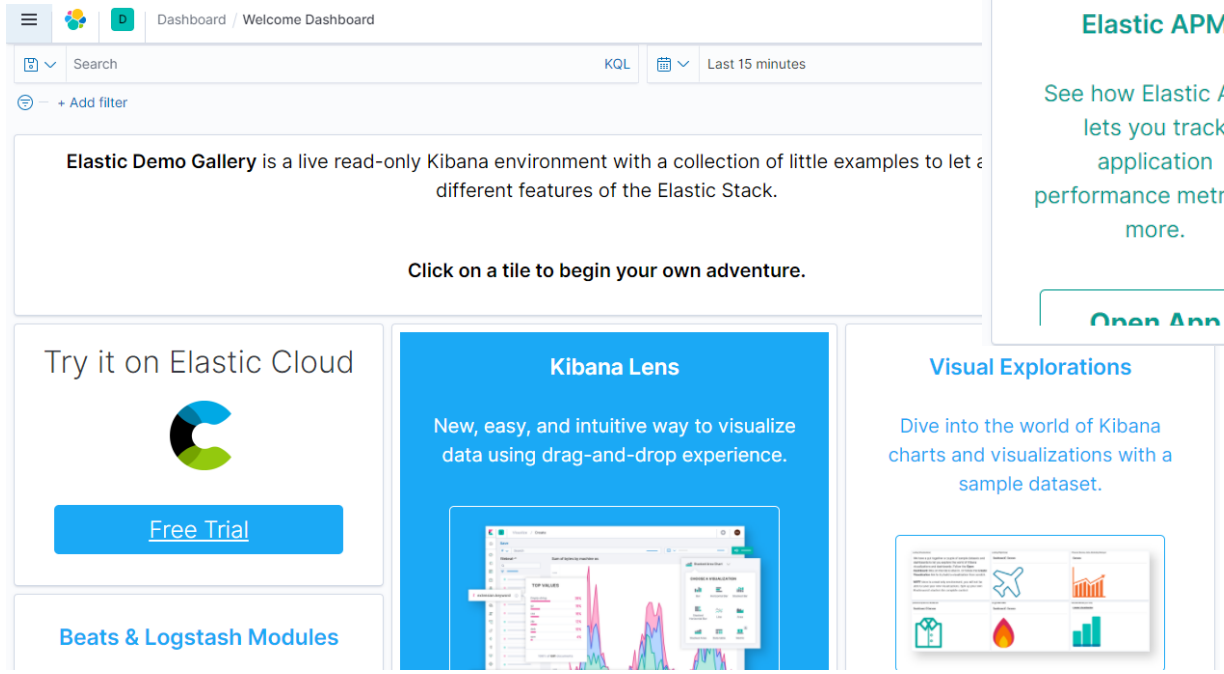
Bônus

Semantix

Treinar Features do Elastic

- https://demo.elastic.co/





Semantix

Semantix

Obrigado!

Alguma pergunta?

Você pode me encontrar em:

rodrigo.augusto@semantix.com.br

GET SMARTER