RED HAT
OPEN SOURCE DAY
Europe, Middle East & Africa

redhat.

BigData alla velocità della luce. Search, Analytics & Discovery

Stefano Pampaloni
CEO/Seacom srl

#redhatosd

SEACOM
the leading open source architects

Chi è Seacom

zimbra
A SYNACOR PRODUCT

Distributore italiano

Authorized Zimbra Training Center

Aggregator (mercato ISP)

Fondatore di…

RIOS RETE ITALIANA OPEN SOURCE

Gli altri prodotti a listino

confluent

from the creators of Kafka

ProcessMaker®

Workflow Simplified

redhat.

Seacom Premium partner Elastic

Elastic Overview

Statistics since 2012, start of the company

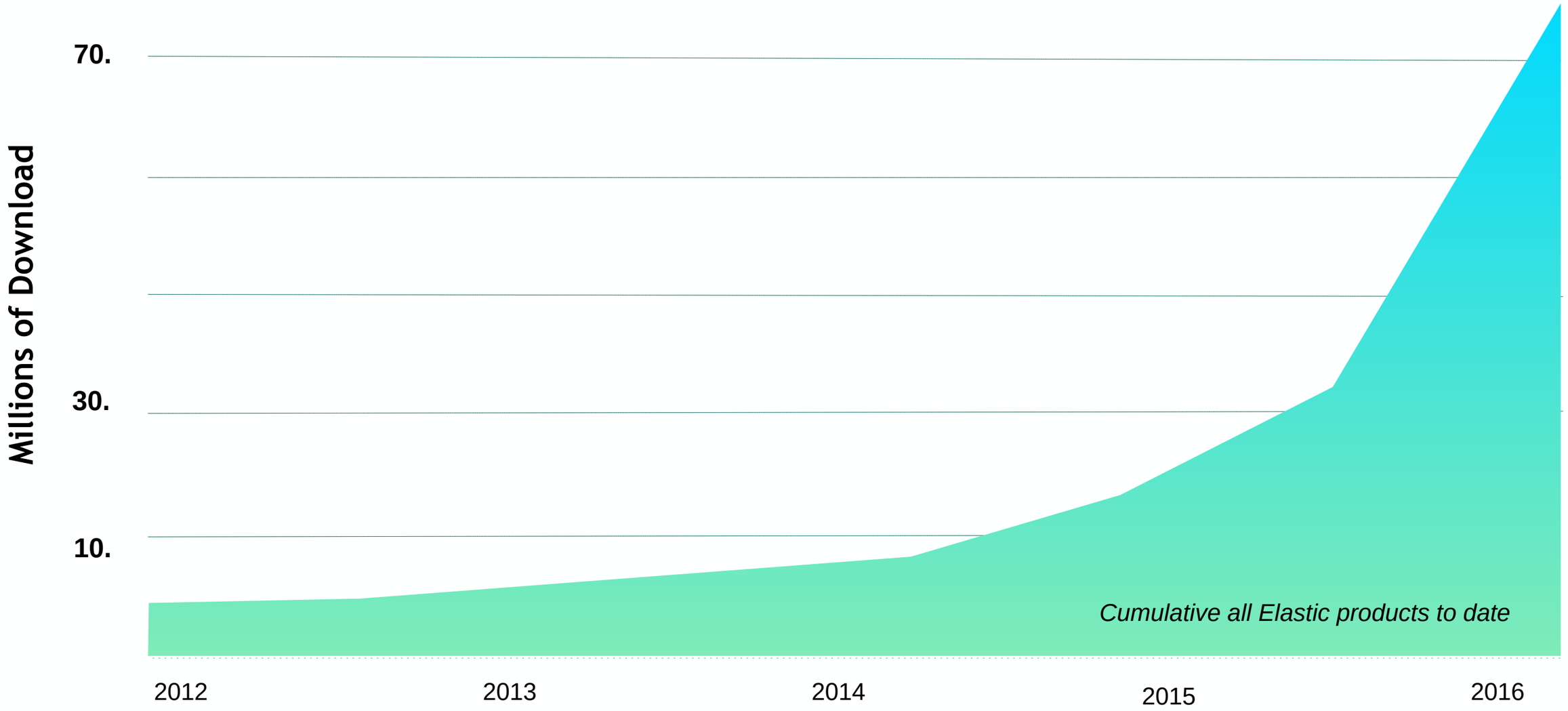
70,000+
Community Members

70M+
Product Downloads

2,400+
Subscription Customers

Il nostro obiettivo è di aiutare a rendere i dati fruibili in tempo reale per risolvere i problemi reali di oggi

70 Million Lifetime Product Downloads



Solving Problems Beyond ‘Search’

“Migliora la cura dei pazienti aiutando a prendere le decisioni in tempo reale.”

“Aiuta a combattere il traffico di esseri umani.”

“Analisi di 3-4 miliardi di eventi al giorno per la security intelligence.”

“Trovare la camera giusta non è mai semplice (senza Elastic).”

“Molti ambiti di utilizzo: ottimizzazione del trading, analisi dei log, reclutamento del personale.”

A Solution for *Every Use Case* and *Everyone*

IT Operations
Application Management
Security Analytics

Marketing Insights
Business Development
Customer Sentiment

Website/App Search
Internal/Intranet Search
URL Search

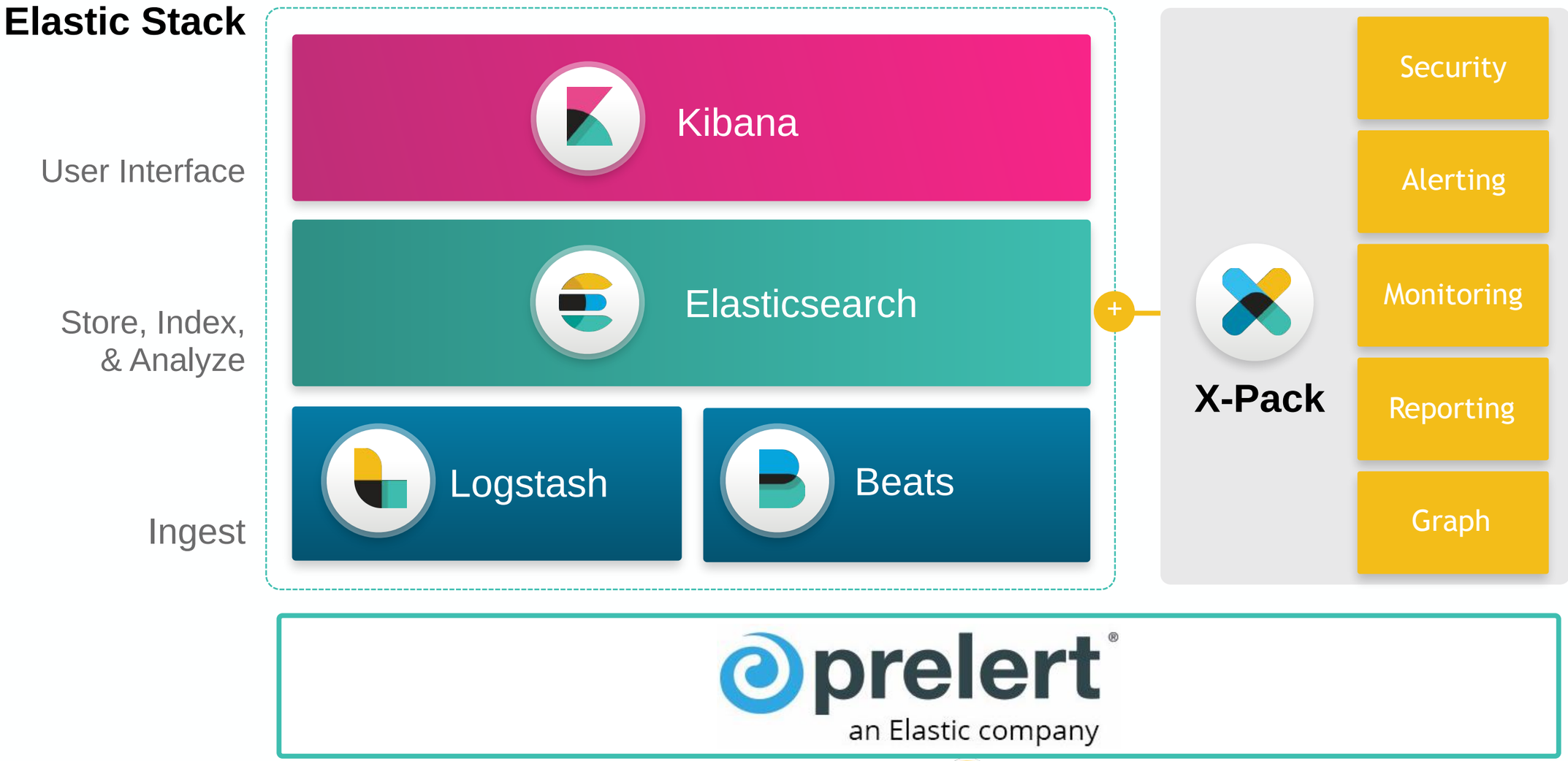
Security Analytics | Log Analytics | Metrics Analytics | Operational Analytics | Embedded Search | Application Search

Internal Systems/Applications ⟷ External Systems/Applications

Developers | Architects | IT/Ops | Business Analysts | CTO/CIO/CDO

redhat.

Introducing the Elastic Stack, X-Pack, and Prelert



Store, Index, and Analyze

Distributed & Scalable

- Designed for scale-out
- High availability; multitenancy
- Structured & unstructured data

Developer Friendly

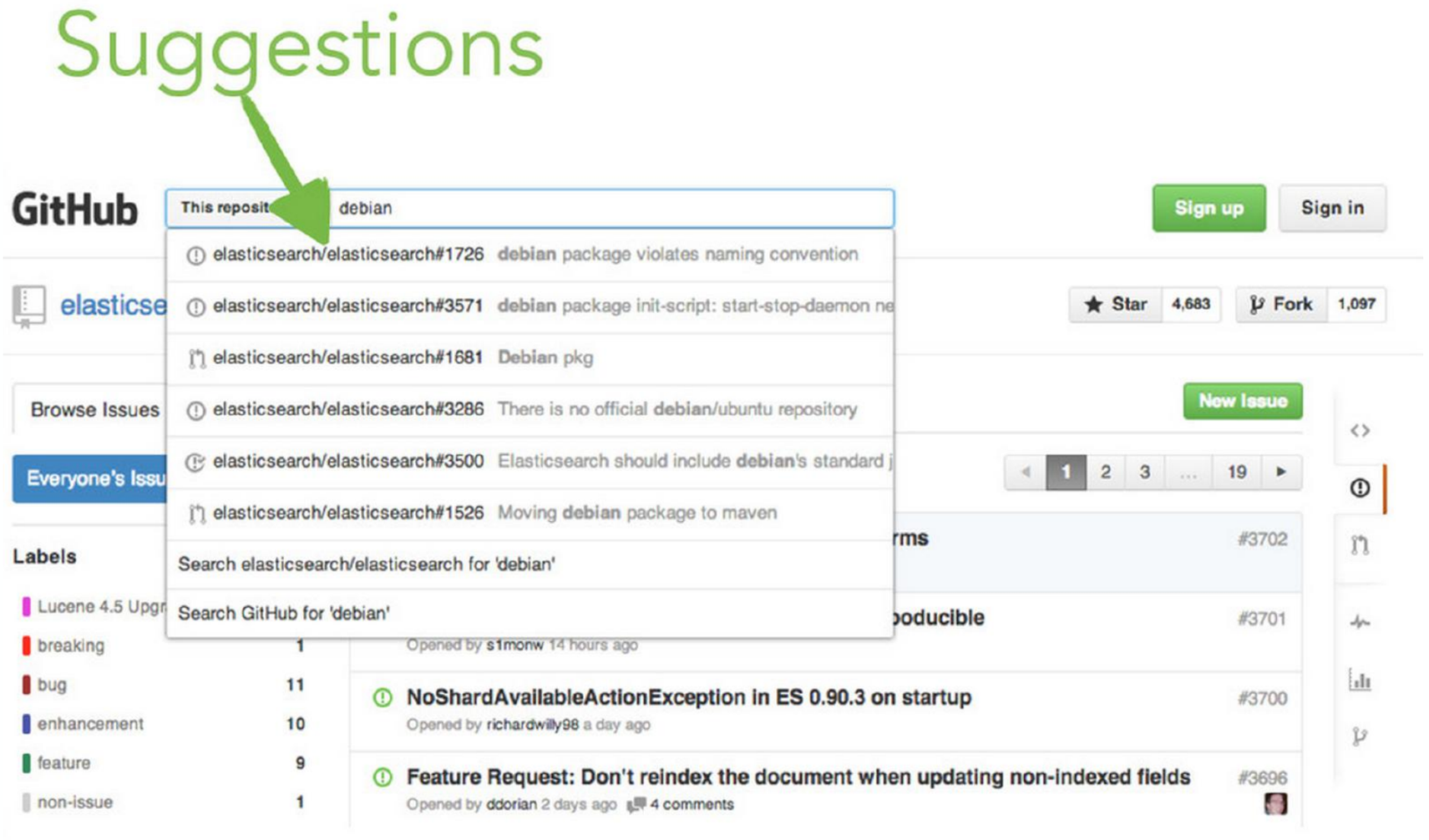
- Schemaless
- Native JSON
- Client libraries
- Apache Lucene

Search & Analytics

- Real-time
- Full-text search
- Aggregations
- Geospatial
- Multilingual

redhat.

Google Like Experience



Visualize and Explore

Discover Insights

- Explore and analyze patterns in data; drill down to any level
- Leverage powerful analytical capabilities in Elasticsearch

Customize & Share

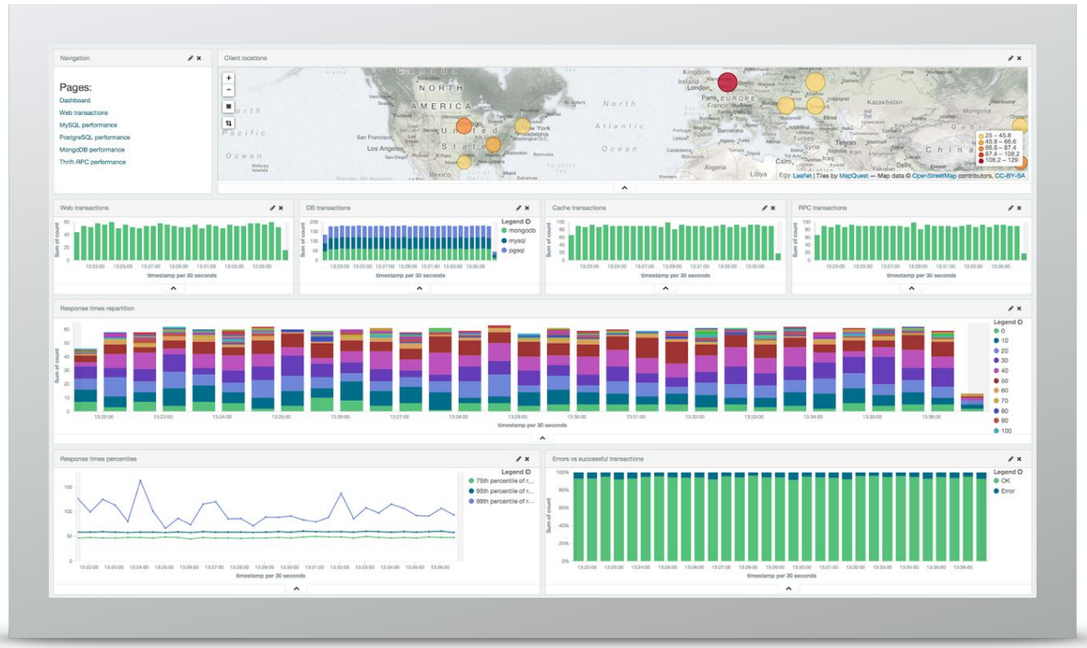
- Create bar charts, line and scatter plots, maps and histograms
- Share and embed dashboards into operational workflows

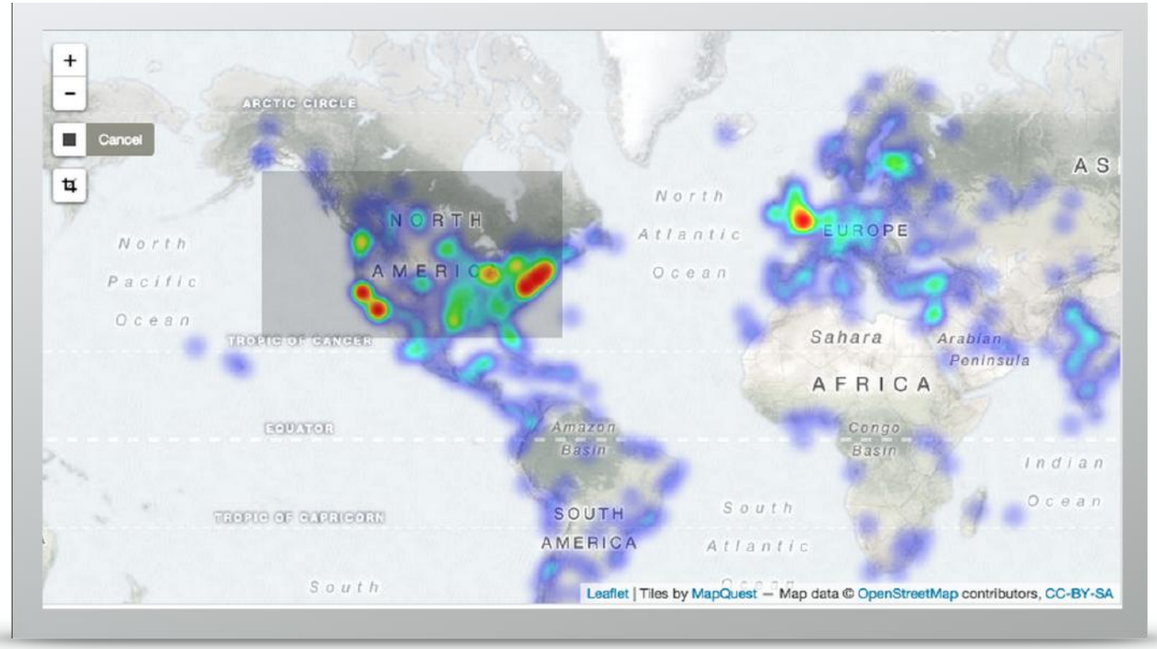
Window into Elastic Stack

- Unified user interface for data visualization
- Administration and management for the Elastic Stack
- Pluggable architecture to create custom visualizations and applications

Visualize and Explore

kibana





Ingest

logstash

- Data collection and enrichment; 200+ plugins
- Next generation data pipeline; micro-batches, process groups of events

beats

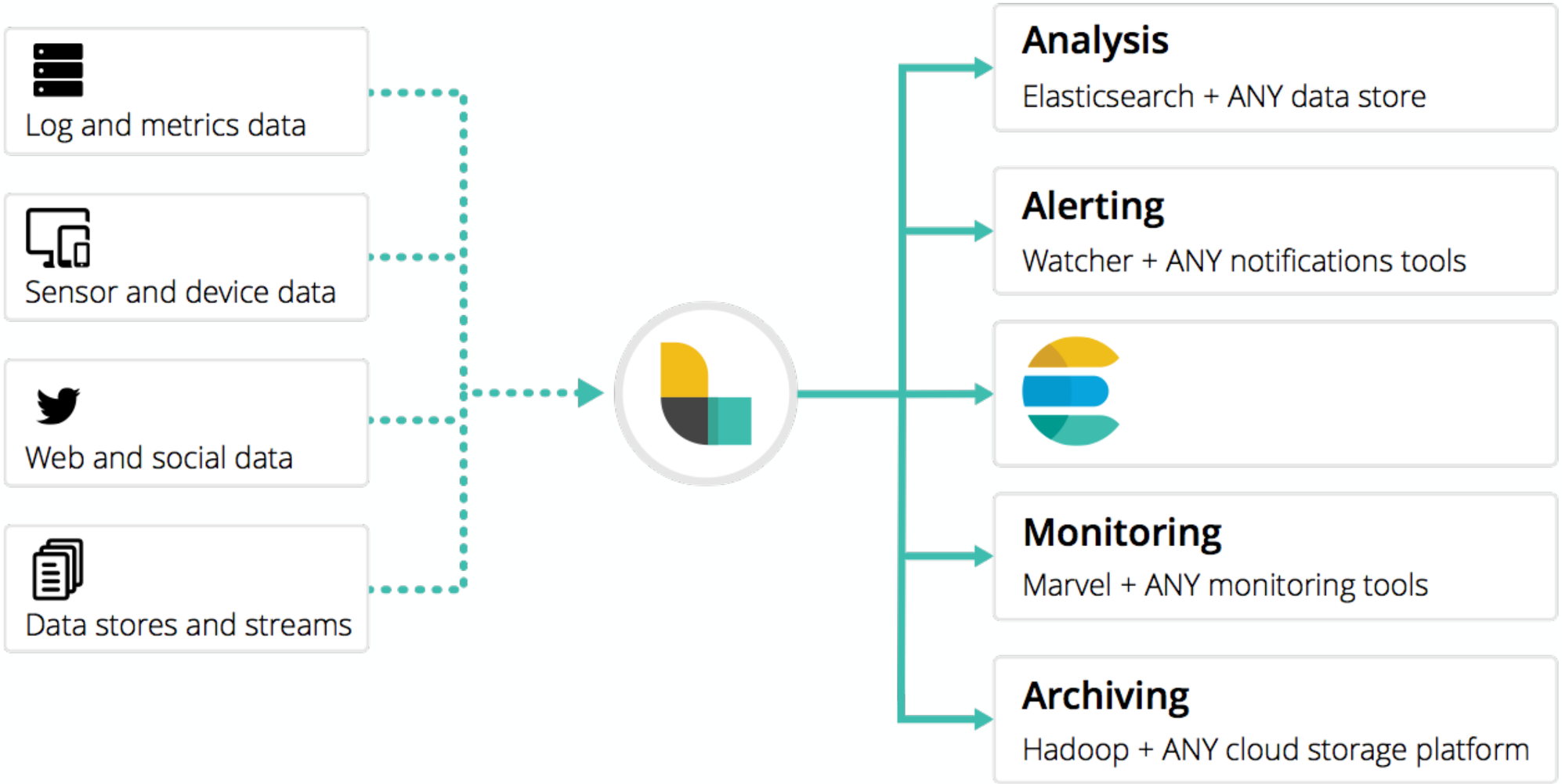
- Platform to build lightweight, data shippers
- Forward host-based metrics and any data to Elasticsearch

ES-Hadoop

- Two-way connector to integrate with HDFS, Spark, MapReduce, etc.
- Enable real-time search queries on Hadoop data

redhat.

Collect, enrich and transport



Lightweight Data Shippers

Libbeat

Library for forwarding host-based metrics to Elasticsearch

Packetbeat

Real-time network packet analytics for web, database, and any network protocols

Topbeat

Gather resource utilization data such as CPU, memory, and other pre-process/system data

Filebeat

Next-generation Logstash forwarder to collect, pre-process, and forward log files.

Winlogbeat

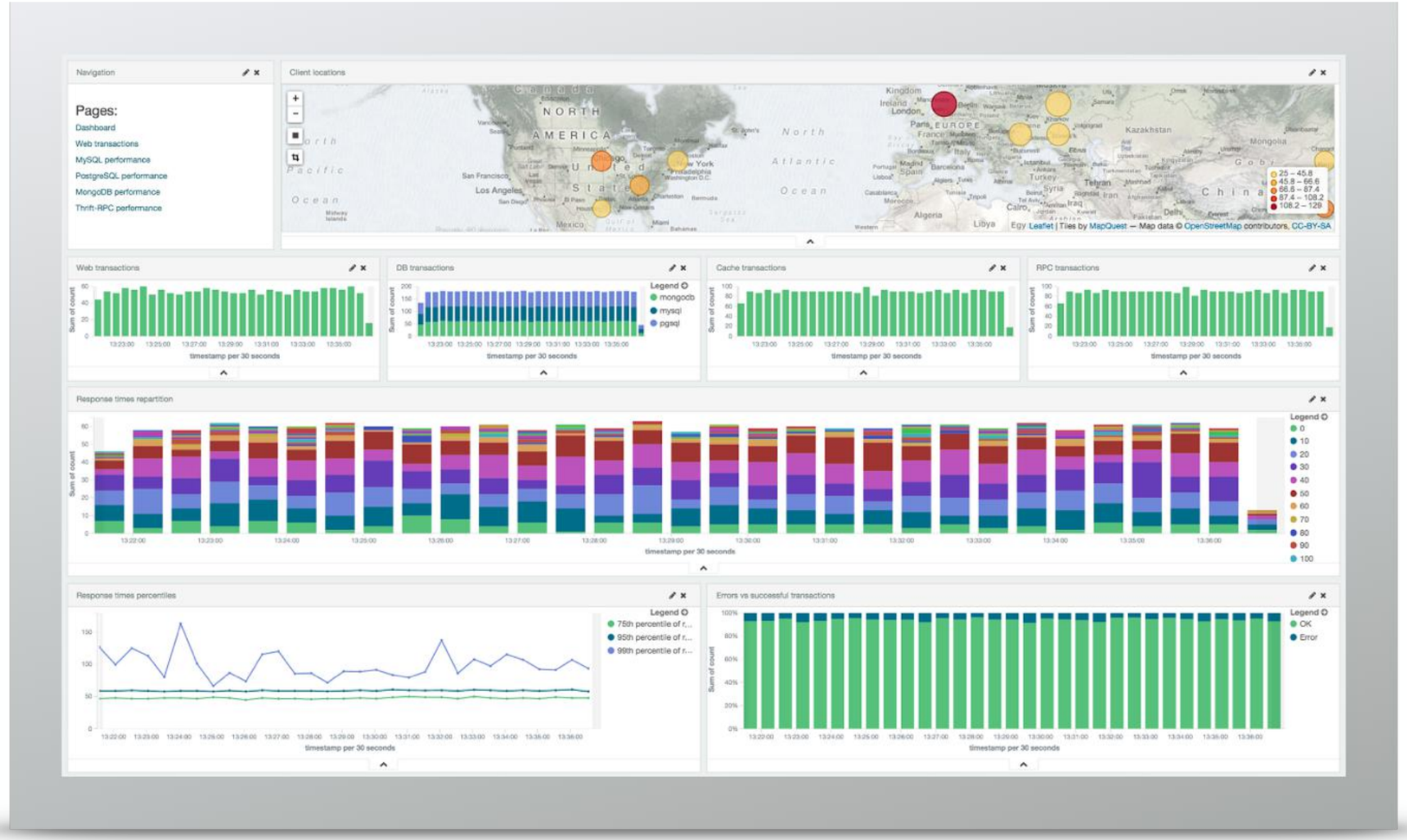
System, application, and security information from Window event logs

{Future}beats

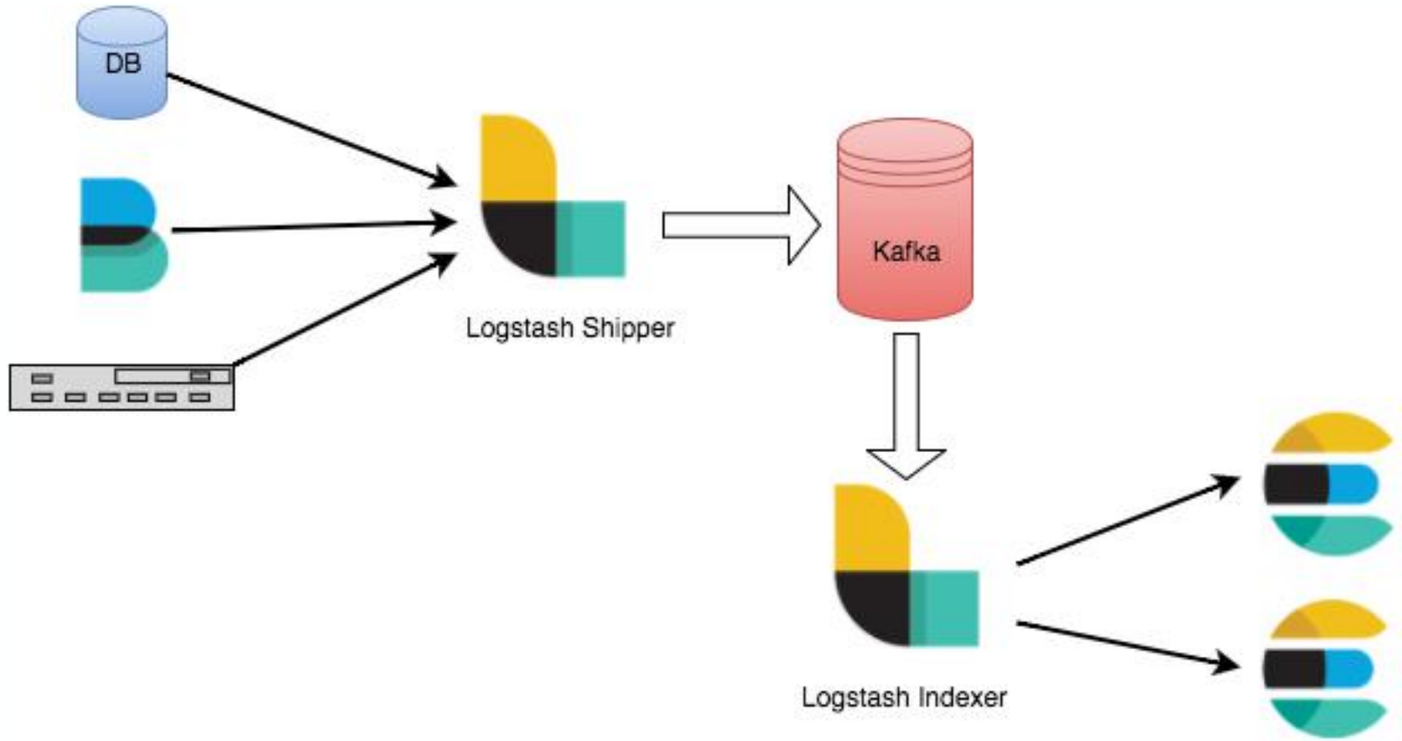
Growing list of beats from the community including http, Redis, Nginx, Docker, Twitter, etc

Packetbeat

Real-time network packet analytics for web, database, and any network protocols



Elastic & Kafka



BigData Architecture

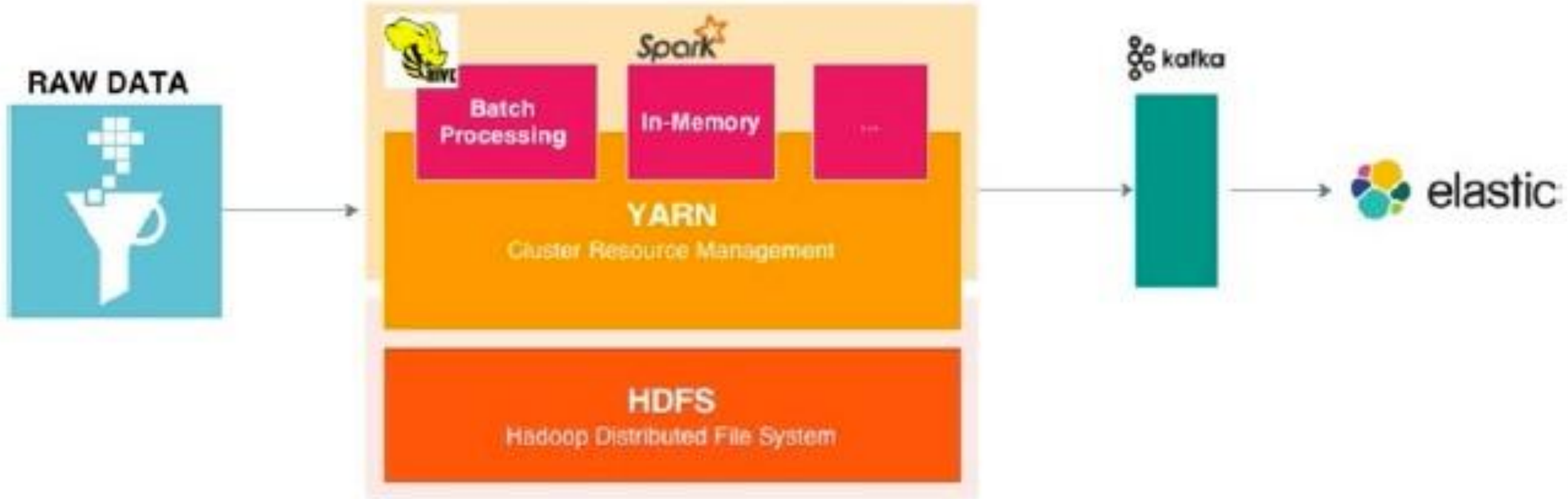
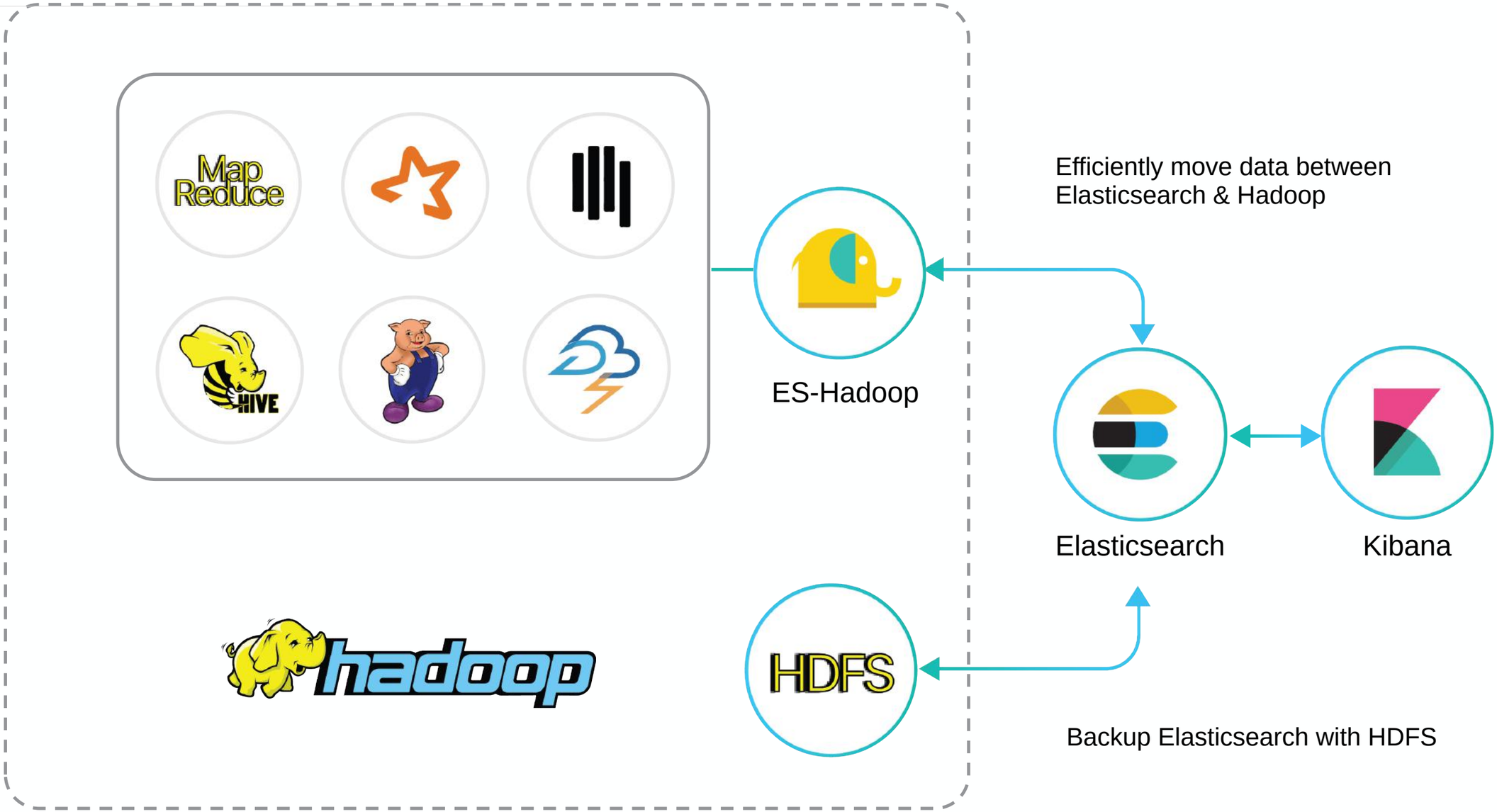


Figure 4 Processing engine

Elasticsearch for Hadoop



A Single Extension

x-pack

Security

Security for the Elastic Stack (Shield)

Alerting

Notifications for the Elastic Stack (Watcher)

Monitoring

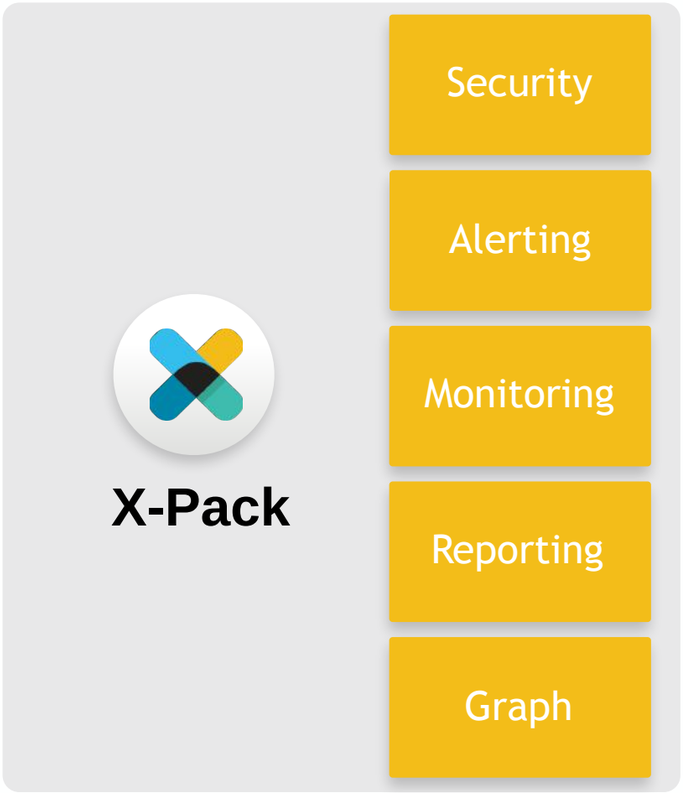
Monitoring for the Elastic Stack (Marvel)

Reporting

Automated reporting for the Elastic Stack

Graph

Real-time graph analytics for the Elastic Stack



redhat.

Adds value across all use cases

x-pack

SECURITY ANALYTICS	LOG ANALYTICS	METRICS ANALYTICS	BUSINESS ANALYTICS	ENTERPRISE SEARCH	APPLICATION SEARCH

lock down your data and monitor access

get notified when something changes in your data

monitor the health of your Elasticsearch cluster(s)

explore meaningful relationships in your data

generate PDF reports to share your insights

redhat.

Security (Shield)

x-pack

Simply Secure the Elastic Stack

Username/password protection

Advanced Security When Needed

LDAP/AD integration

Role-based access control

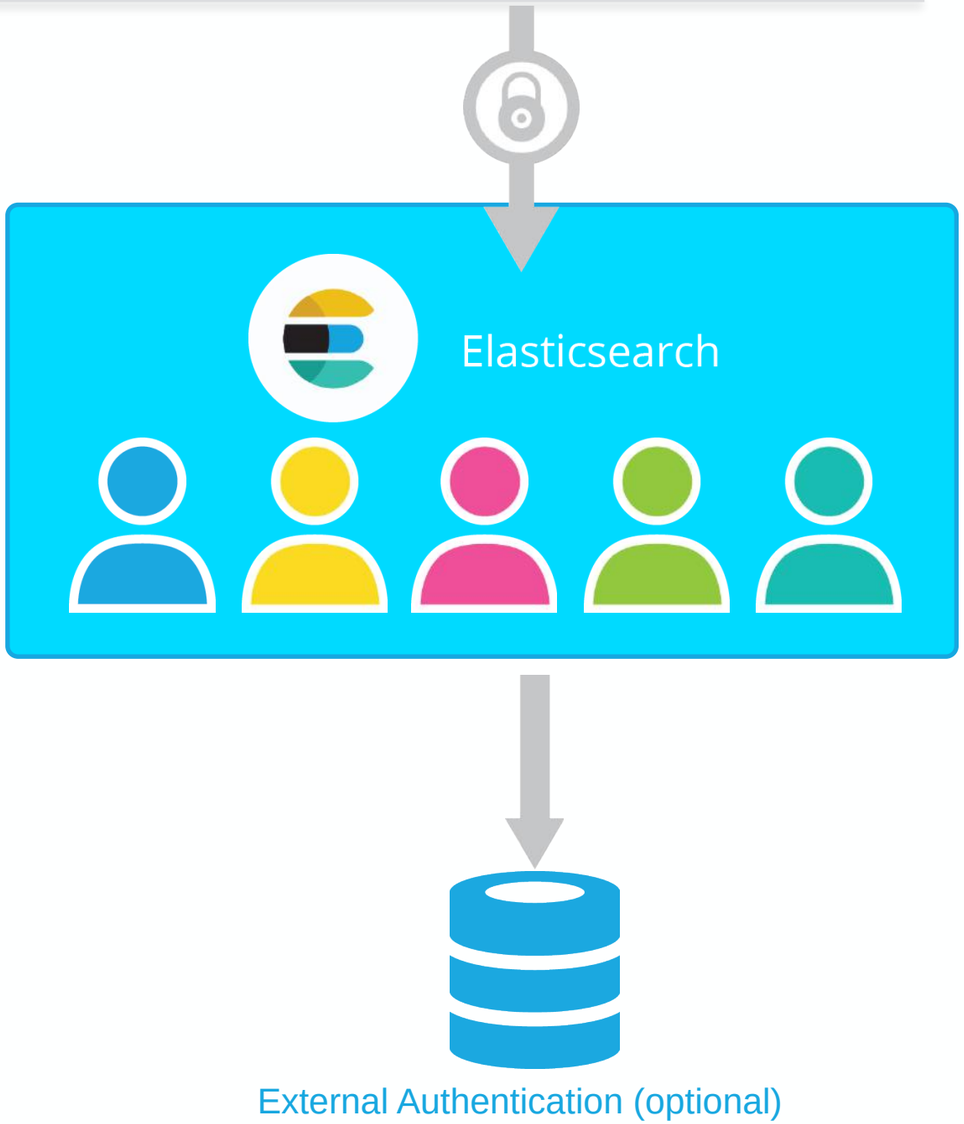
IP filtering

Field and document level security

Encrypted communications

Audit logging

Kibana plugin for login and session management



Alerting (Watcher)

x-pack

Setup Alerts

- Create Watches based on data
- Trigger automatic notifications
- Setup chained inputs

Notify and Integrate

- Slack, Hipchat, JIRA, Pagerduty
- Email
- Elastic Monitoring (Marvel)
- Other

redhat.

Monitoring (Marvel)

Monitor Elasticsearch

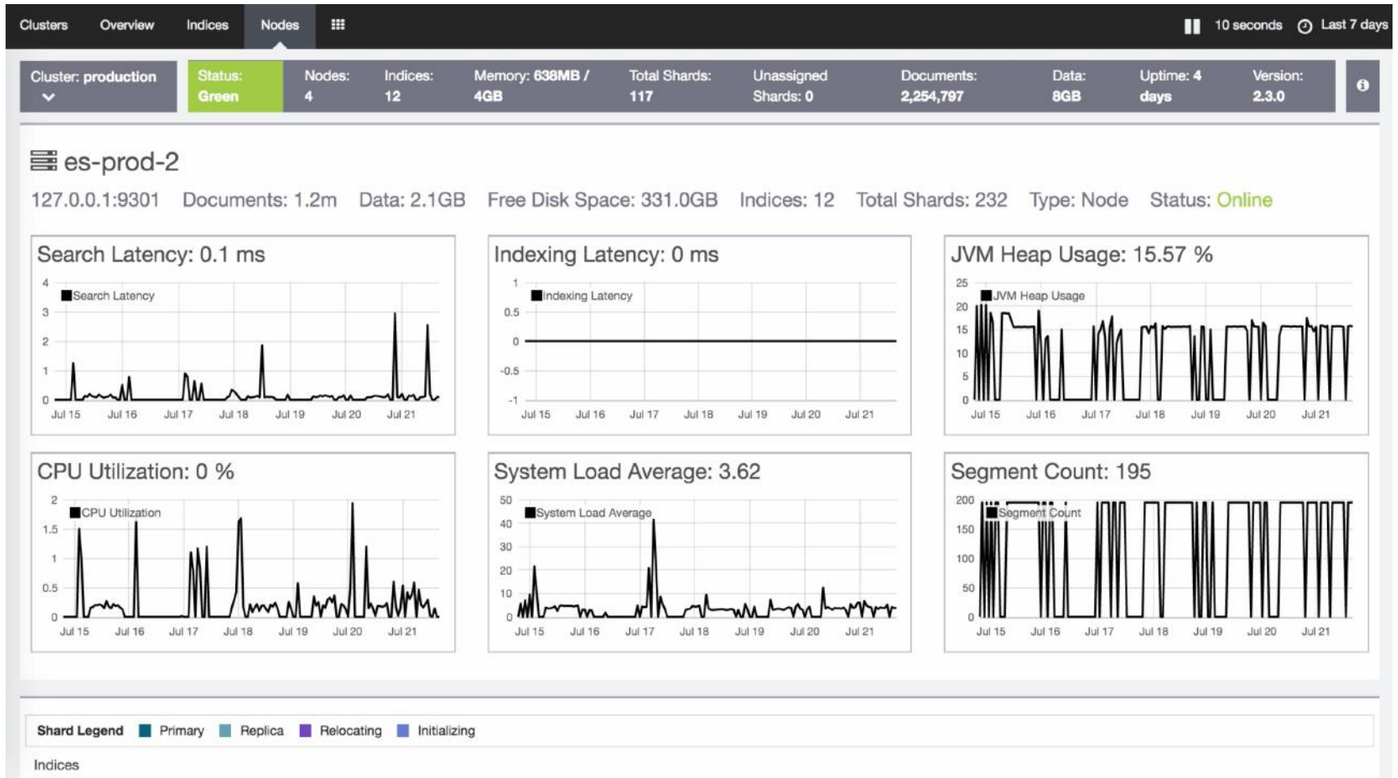
Real-time statistics and metrics for all clusters and nodes

Diagnose Issues

Analyze historical or real-time data for root cause analyses

Optimize Performance

Utilize in-depth analyses to improve cluster performance



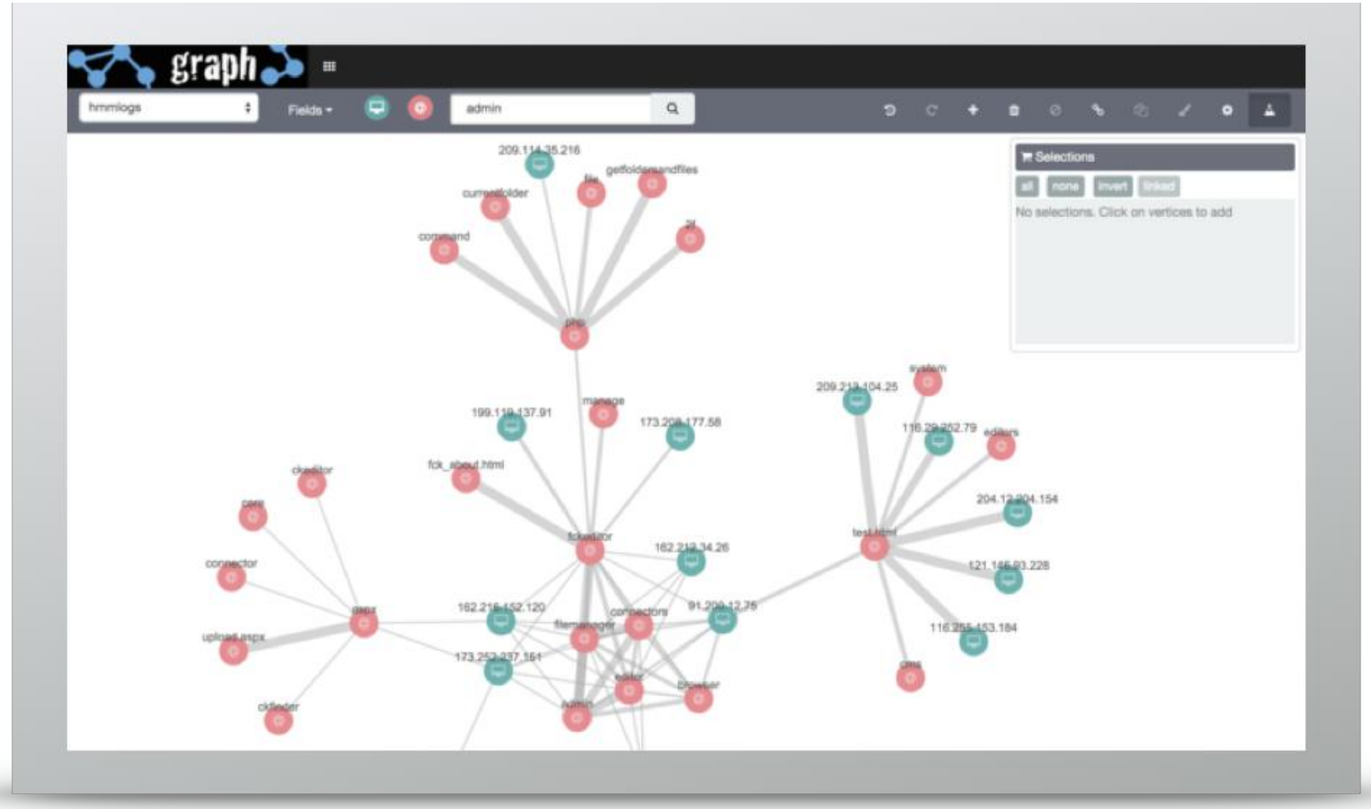
Graph Analytics

Query and Visualize Relationships

Use relevance as a guide to uncover and explore new relationships in all your data stored in Elasticsearch

Interact with Graph via a Kibana plugin or use the Graph API to integrate with your applications

Enable new use cases – behavioral analysis, fraud, cybersecurity, drug discovery, and recommendations



Reporting

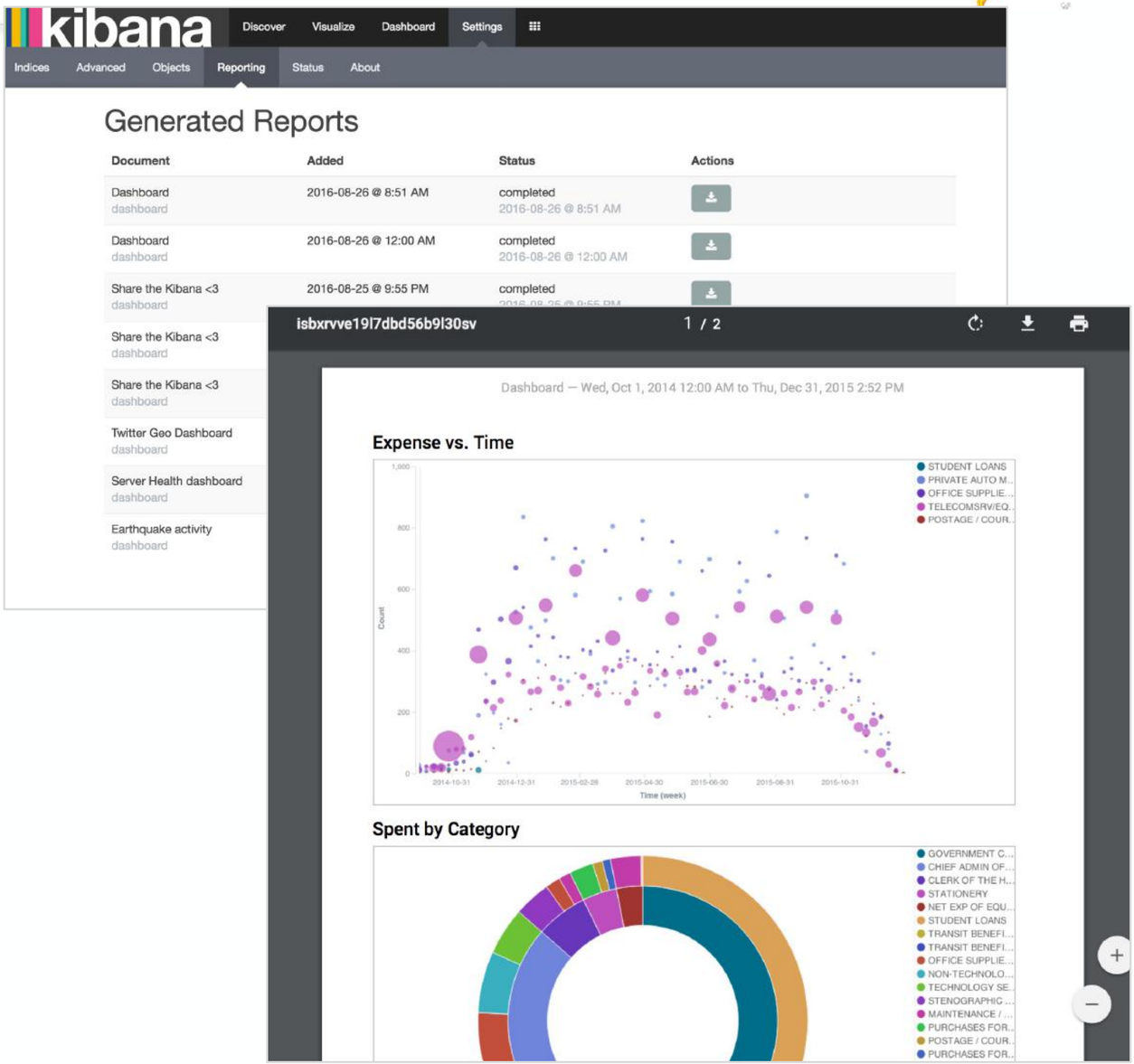
Generate and share reports

Export PDFs of reports of dashboards and visualizations with a single click

Use Alerting features to:

email reports on a time-based interval

schedule event-based reports (example: when X event occurs, send Y report)

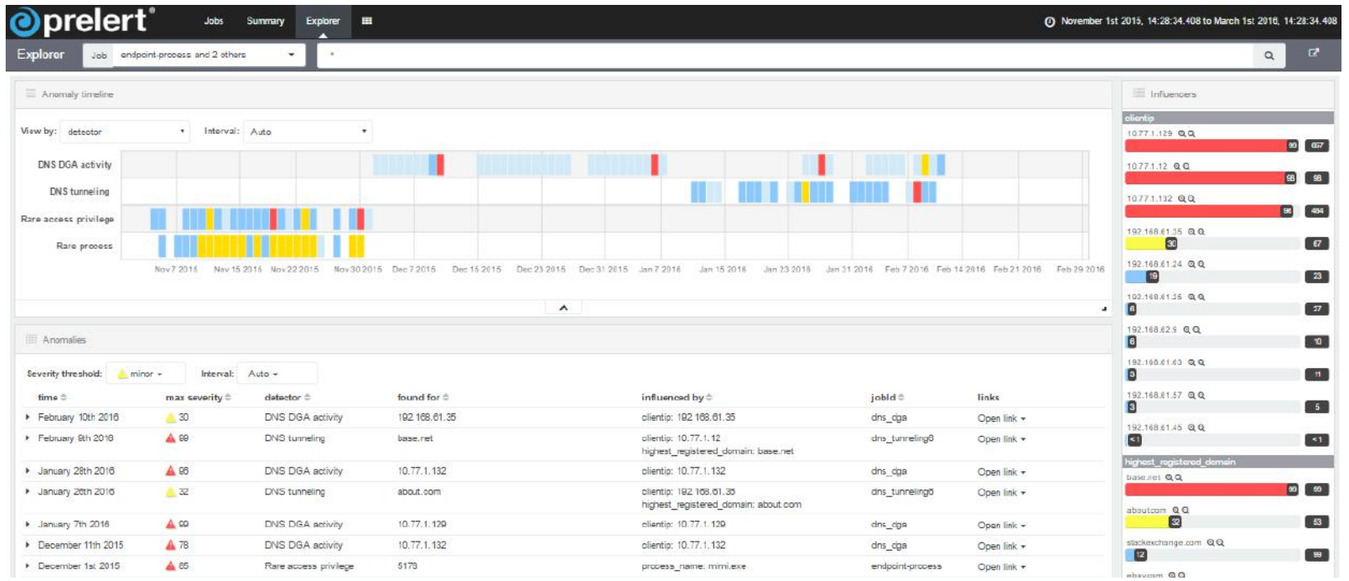


redhat.

Behavioral Analytics

Unsupervised machine learning

- Automatically detect anomalies
- Advanced correlation and categorization
- Identify root cause(s) and expose early warning signs

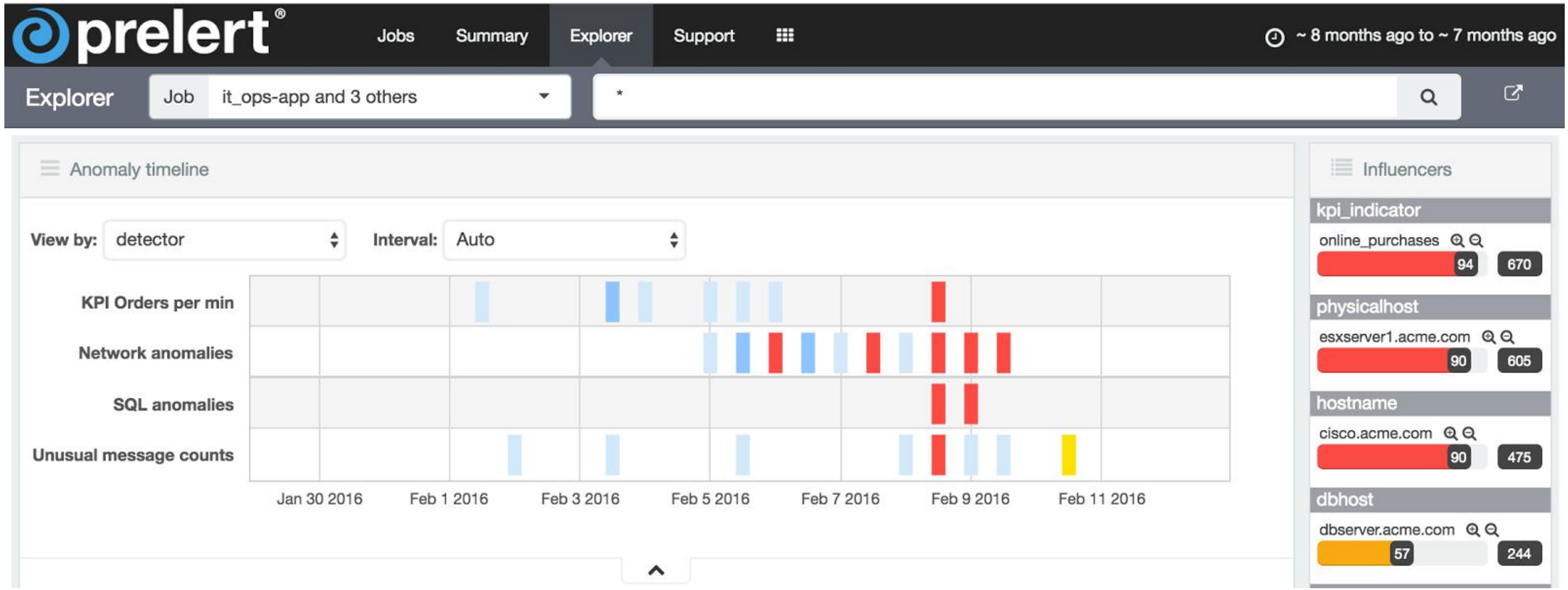


Analyze time series data

- Use cases span security, IT ops, fraud, finance and many more
- Currently in beta; building native integration with the Elastic Stack

redhat.

Anomaly Detection



RED HAT
OPEN SOURCE DAY
Europe, Middle East & Africa

redhat.

Grazie

Stefano Pampaloni
CEO/Seacom srl

#redhatosd

SEACOM
the leading open source architects