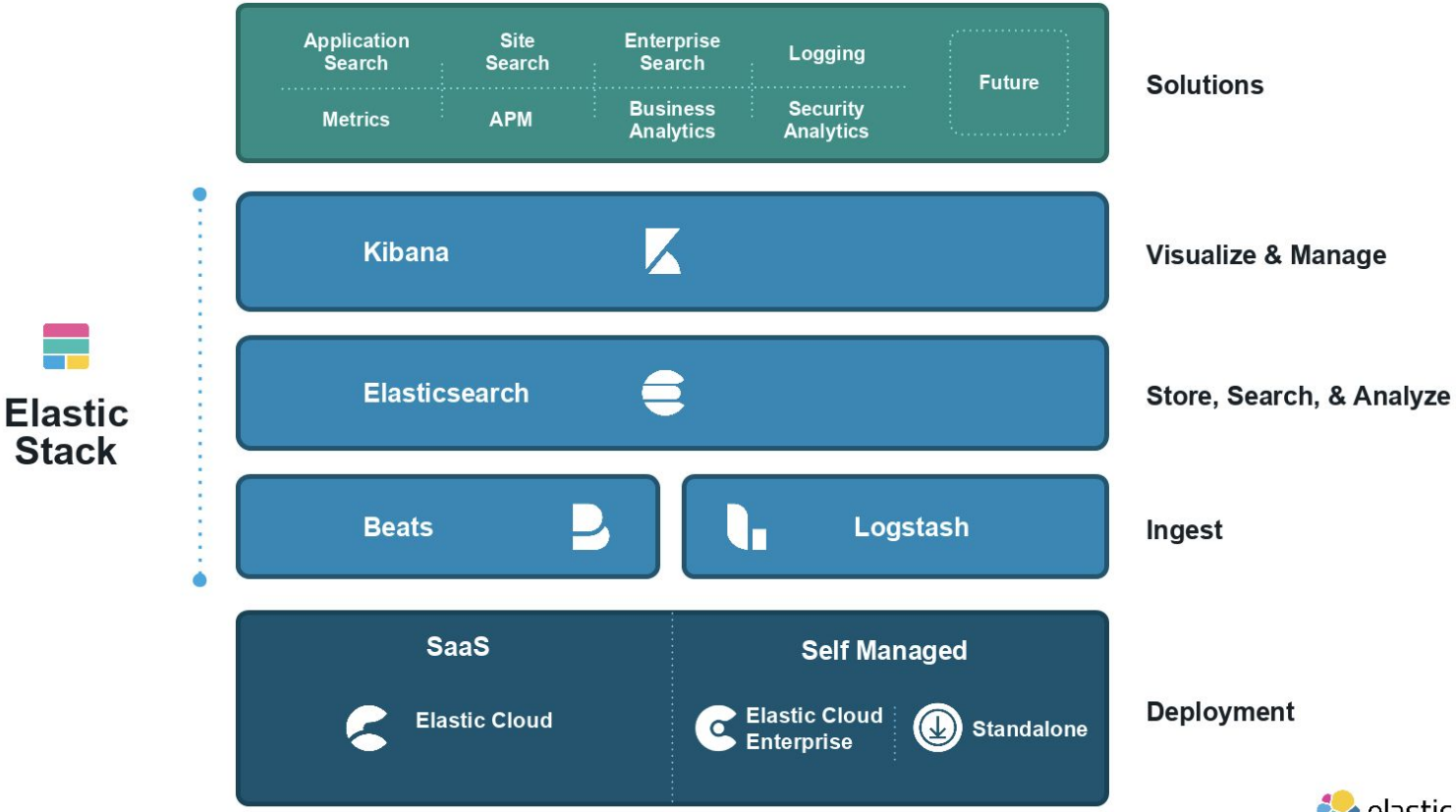
Machine Learning & more for the Elastic Stack

Gabriel Moskovicz - Michael Yuan
Solutions Architects - US & LATAM
October 2018

Elastic Stack



elastic

Machine Learning

Image Classification **Recommendations**

Autonomous cars Voice Recognition Predictive Medicine

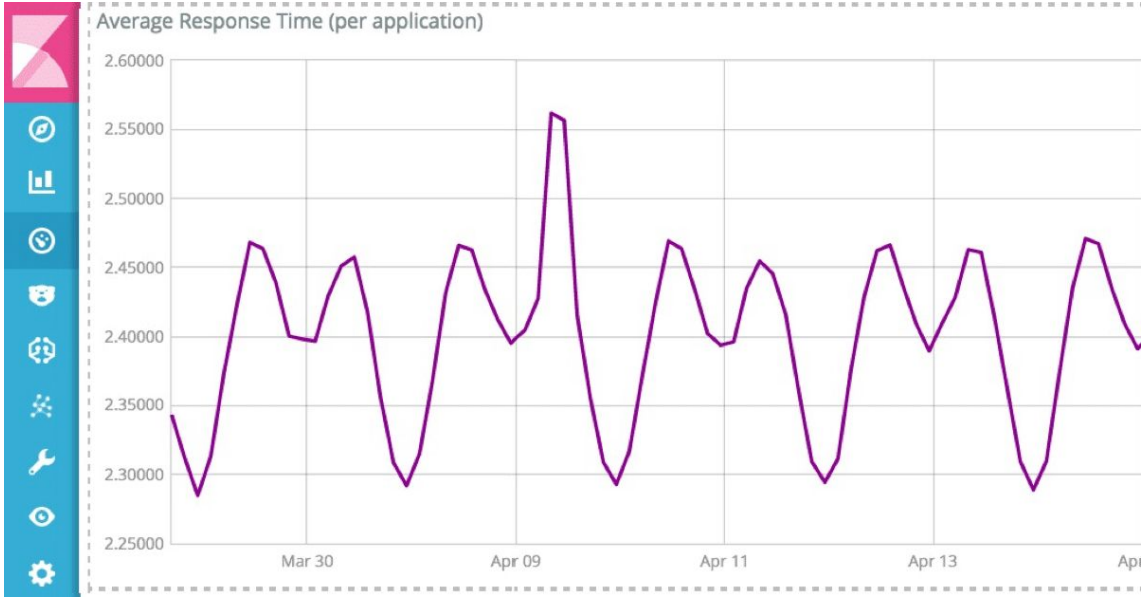
Fraud detection **Anomaly Detection**

Learn to Rank Speech Recognition

Language Translation **Entity Resolution**

Detecting (noteworthy) anomalies is hard!

- Data is complex, high dimensional, fast moving
- Human inspection is not practical
- Easy to miss things



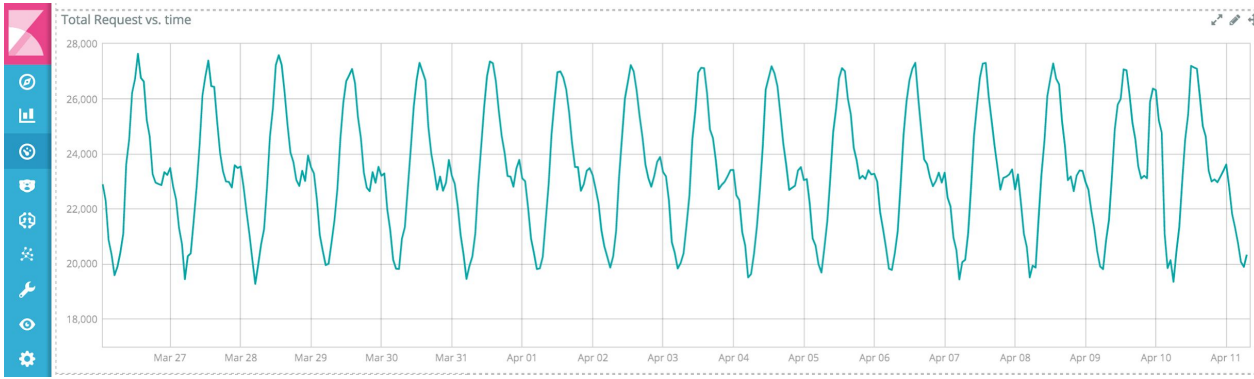
Visual inspection is not practical

Rule-based alerts are insufficient

Detecting (noteworthy) anomalies is hard!

- Defining “normal” via static thresholds is hard
- Rules don’t evolve with data / infrastructure
- Rules can be bypassed

What’s the right threshold ?

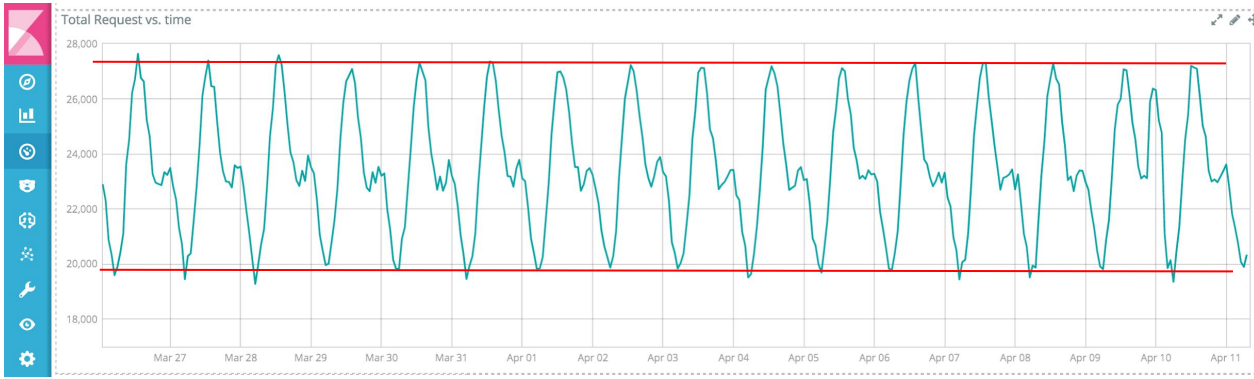


Rule-based alerts are insufficient

Detecting (noteworthy) anomalies is hard!

- Defining “normal” via static thresholds is hard
- Rules don’t evolve with data / infrastructure
- Rules can be bypassed

What’s the right threshold ?



Anomalies in your data could indicate trouble

Operational Analytics

Spiked 404 errors

Web attack

Security Analytics

Unusual DNS activity

Data exfiltration

Business Analytics

Rare log messages

Failing sensor

Use Case

Operational Analytics

- Is my website seeing unusual traffic volume?

Use Case

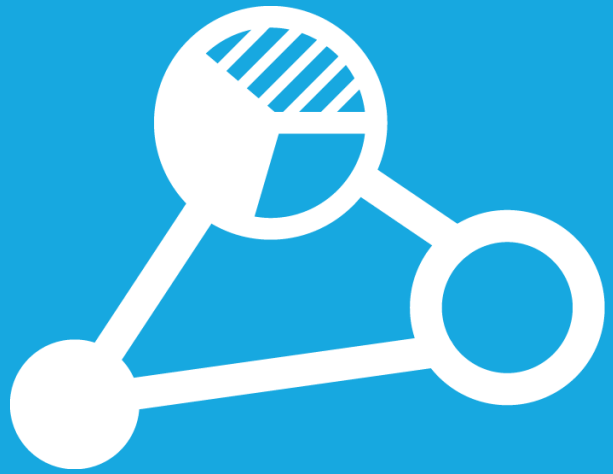
Security Analytics

- Is there indication of data theft in my DNS logs?

Use Case

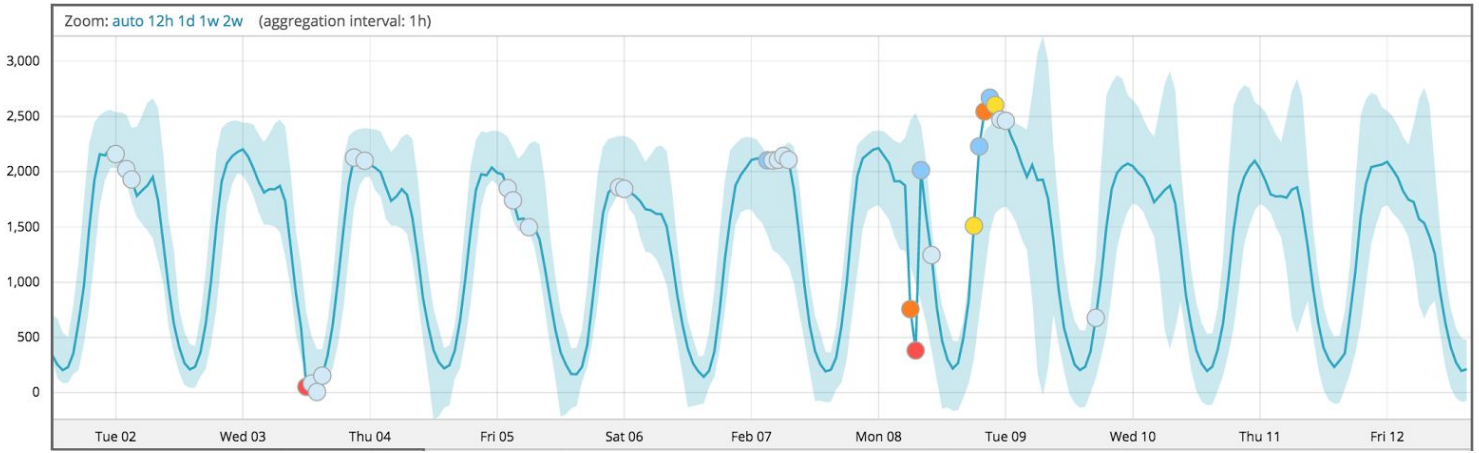
Telemetry / Sensors

- Which trucks in my fleet show unusual driving pattern?



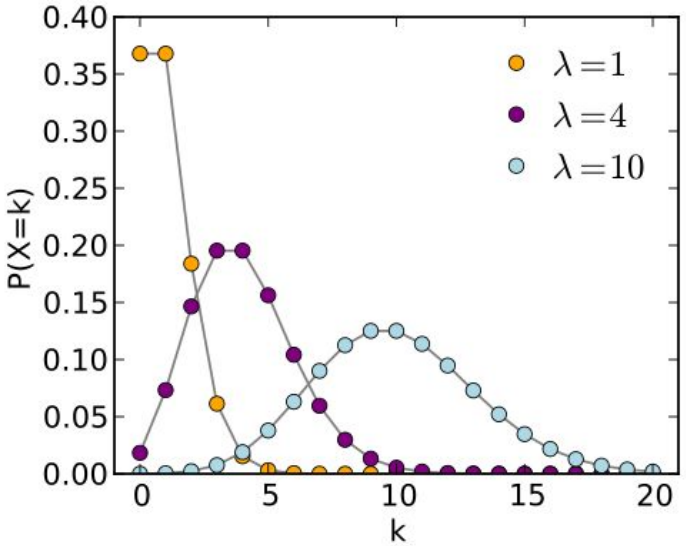
X-Pack solves this with automated anomaly detection

- Uses unsupervised machine learning techniques to
  - Learn what's "normal" by modeling historic behavior
  - Detect anomalies when data falls outside expected bounds

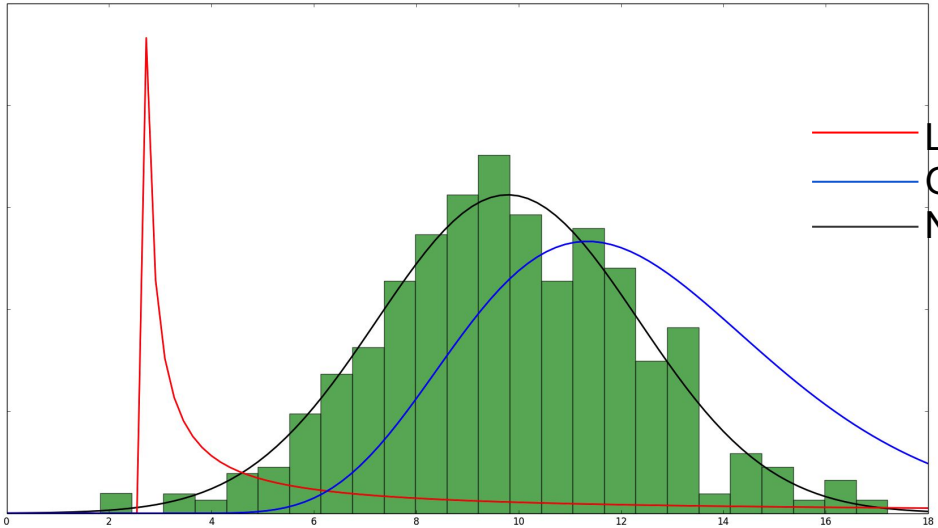


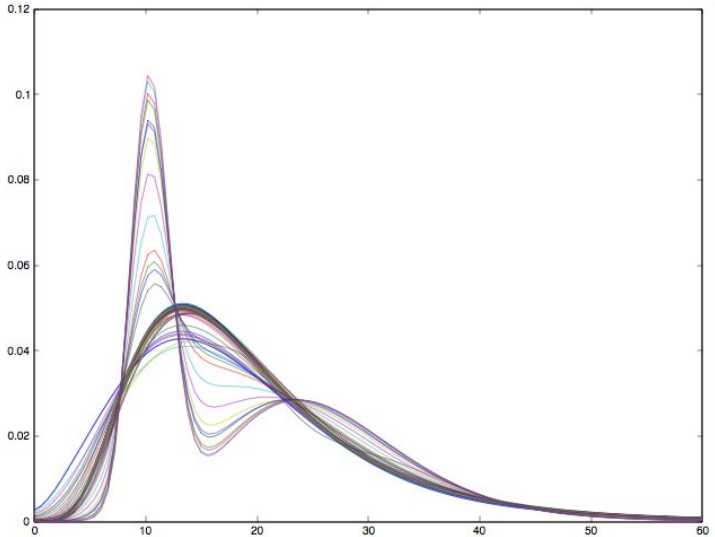
X-Pack solves this with automated anomaly detection

- How to construct a model?
  - Observations!
  - e.g. How do I learn how much mail do I get daily and how do I predict how much will I get in the future?
  - Bayesian Algorithms



Machine Learning picks the model for you





DEMO

Thank you

Gabriel Moskovicz - @gmoskovicz
Engineer - LATAM