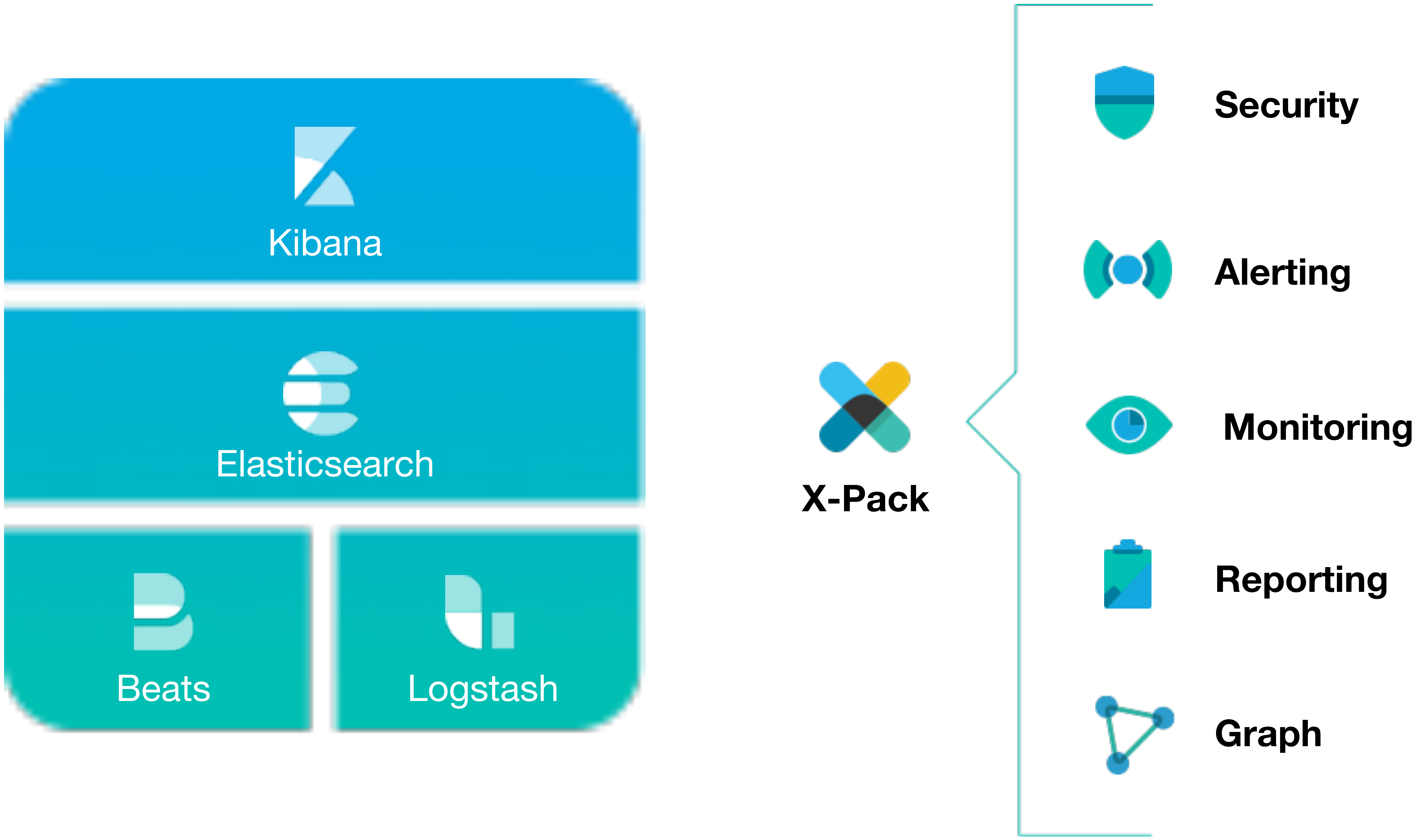
X-Pack 5.0:
Extending the Elastic Stack

William Wong
Support Engineer

elastic

We loved extensions

X-Pack: One Pack. Many Features.



Kibana

Elasticsearch

Beats

Logstash

X-Pack

- Security
- Alerting
- Monitoring
- Reporting
- Graph

Simplified Getting Started Experience

```
$ bin/elasticsearch-plugin install x-pack
```

```
$ bin/kibana-plugin install x-pack
```

Demo: X-Pack

Prelert:
Behavioral Analytics for the Elastic Stack

IT Operations

- How do I know my systems are behaving normally?
- Where to set thresholds for good alerting?
- How to find the root cause of problems when I don’t know what to look for?

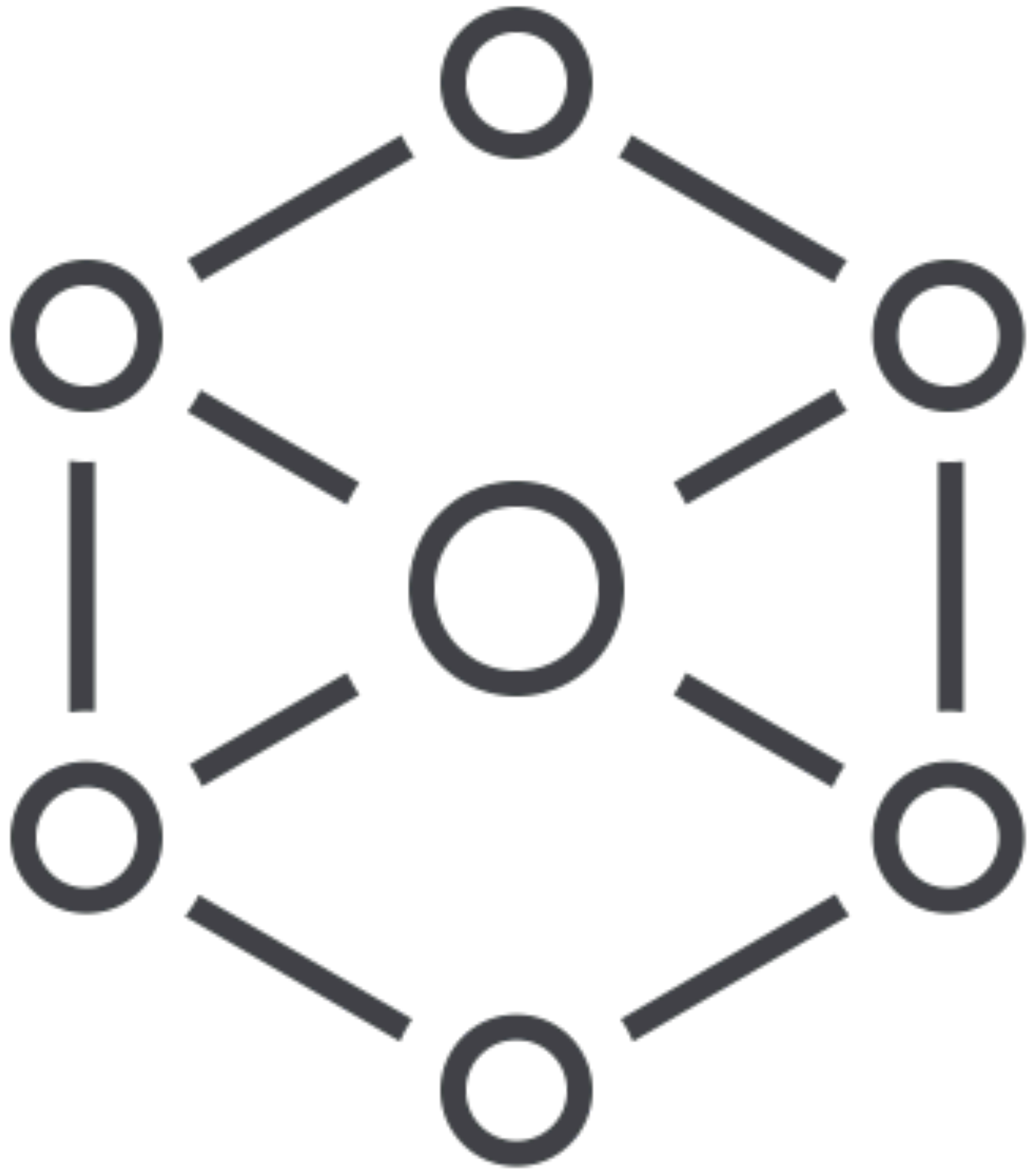
IT Security

- **Do I have systems that are compromised with malware?**

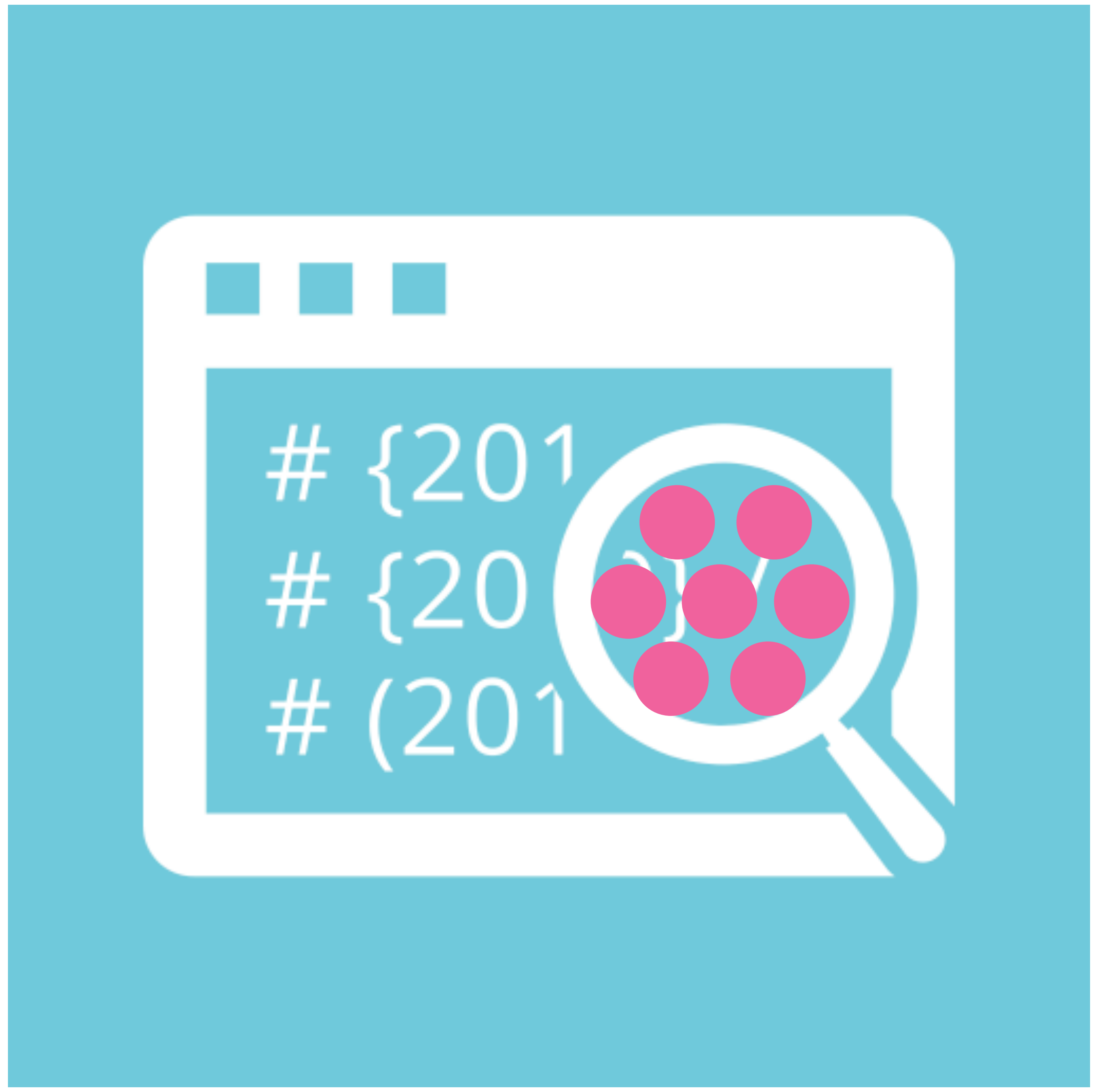
- **Which users could be an insider threat?**

Other

- **Is my factory working normally?**
- **What do I do with thousands of time-series data?**
- **Which traffic incidents are causing the most delay?**



Extracting useful, valuable information is hard



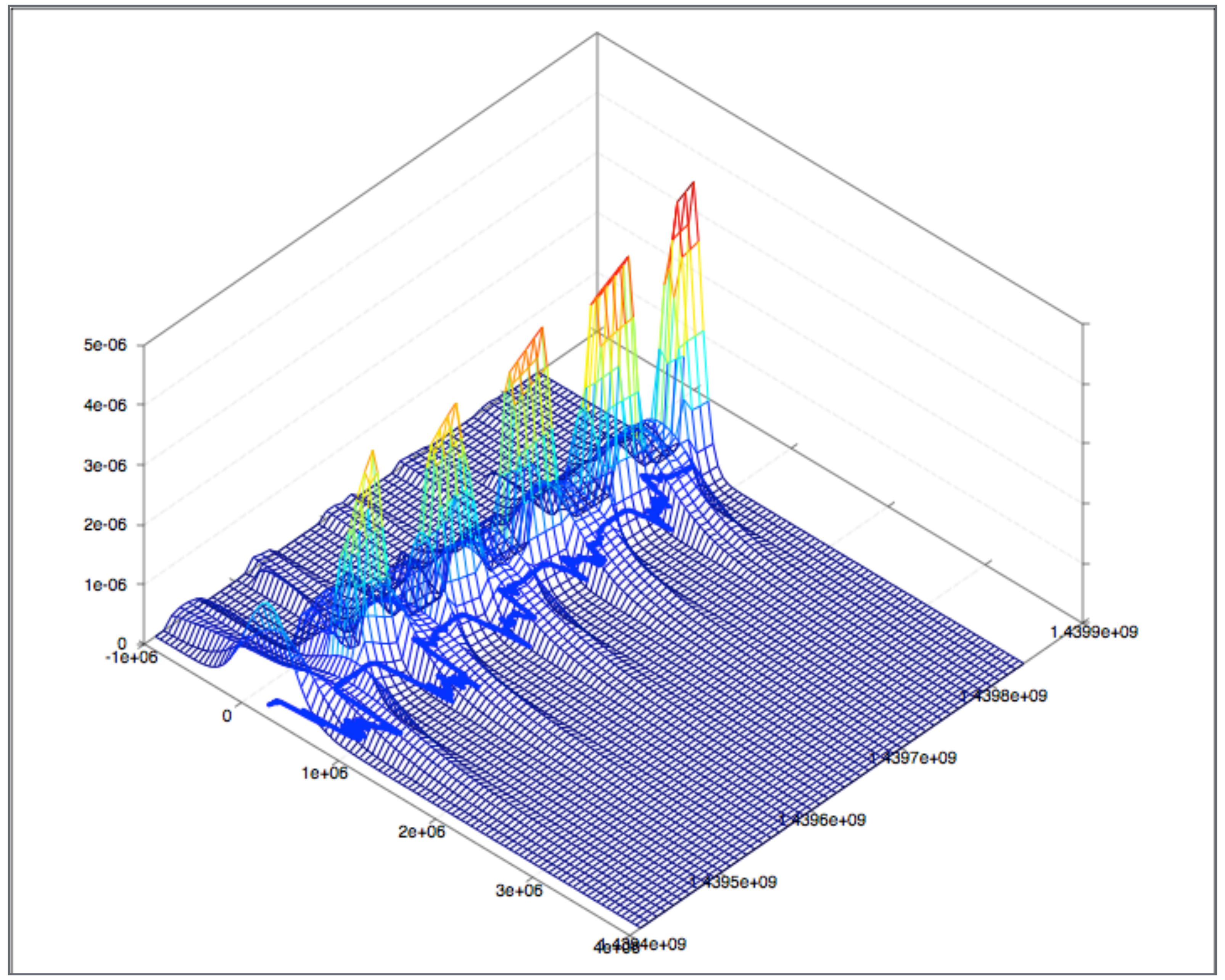
Search

Aggregations

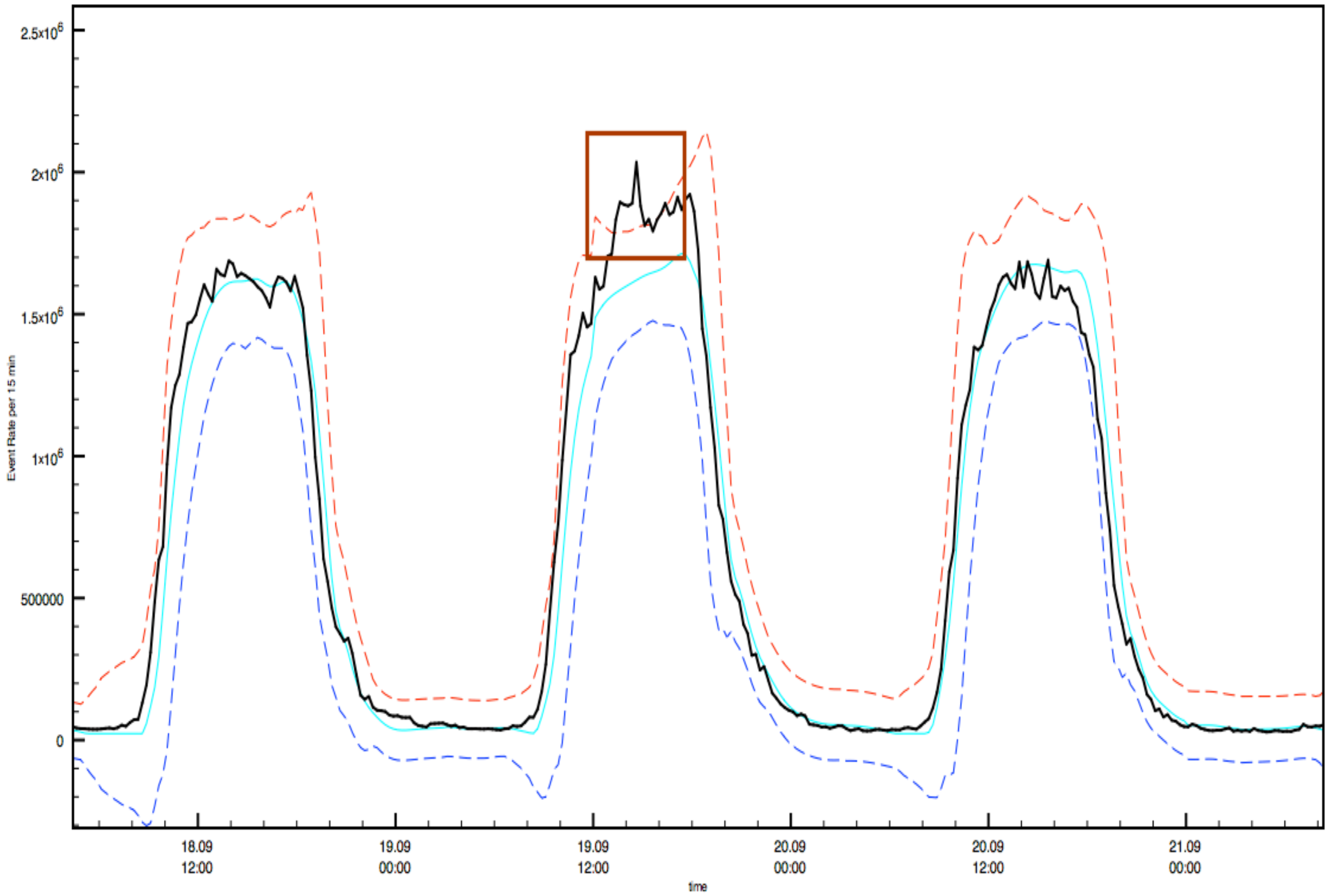
Visualization

Machine Learning

Example: Detecting anomalies in data



Unsupervised machine learning automatically models behaviors in data



Notify when current behavior deviates significantly from the predictive model

Demo: Prelert

Coming Soon

- Beta available for download now
- Working on tighter integration into the Elastic Stack
- GA targeted in first half of 2017

elastic

www.elastic.co