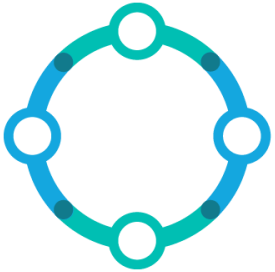
Elastic for Security Analytics (SIEM)

The world’s most popular enterprise open source products for real-time search, logging, analytics, and more

March 2017

80,000+
Community Members

100M+
Product Downloads



3,000+
Subscription Customers

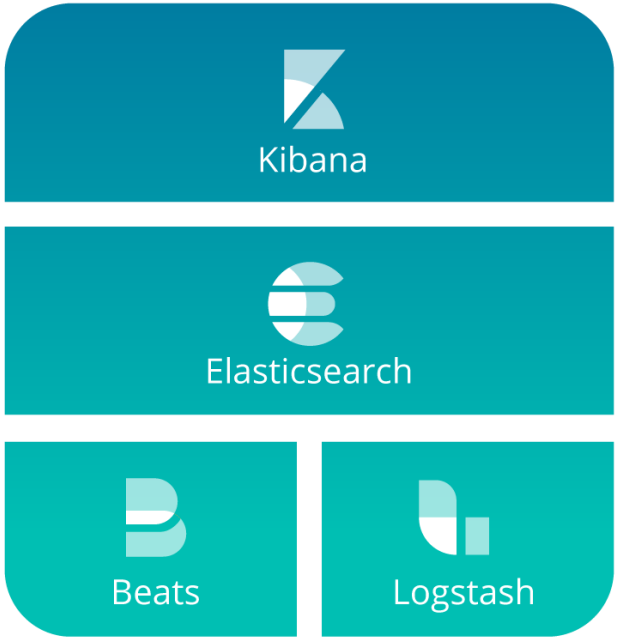
Statistics since 2012, founding of Elastic

Tech	Adobe	hp	salesforce	Microsoft	CISCO	DELL
Finance	SwissLife	Scottrade	Goldman Sachs	HSBC	E*TRADE	ZURICH
Telco	verizon	COX COMMUNICATIONS	orange	ROGERS	Alcatel·Lucent	Sprint
Consumer	Audi	UBER	GROUPON	Columbia Sportswear Company	DHL	ebay

Enterprise Customers in Every Industry

Elastic Stack

100% open source
No enterprise edition



X-Pack

Single install
Extensions for the Elastic Stack
Subscription pricing

Security

Alerting

Monitoring

Reporting

Graph

Machine Learning*

* Currently in Beta – GA expected Spring 2017 (5.4)

Elastic Stack

X-Pack

Elastic Cloud

Application Search	**Enterprise Search**	**Business Analytics**
Log Analytics	**Metrics Analytics**	**Security Analytics**

Solving many diverse & complex use cases

Sniff sniff sniff, find the bad actors in your data

200% YoY growth in security use cases with our products

What is a SIEM ?

- SIEM = Security Information & Event Management
  - Software tool for managing and monitoring security logs for:
    - Regulatory Compliance
    - Threat Detection
  - Teams include Security Operations (SOC), Cyber Threat Operations (CTOC)
    - Users often referred to as security analysts, security engineers
  - Well-defined software segment
    - Gartner Magic Quadrant has been around for many years
  - Usually sold as a turnkey solution
    - However, deployments take months or years
    - High-level of dissatisfaction with SIEM users
    - Can be very expensive $$$
  - Leading solutions include
    - HP ArcSight, Splunk ES app, IBM QRadar, etc.

Changes in the industry

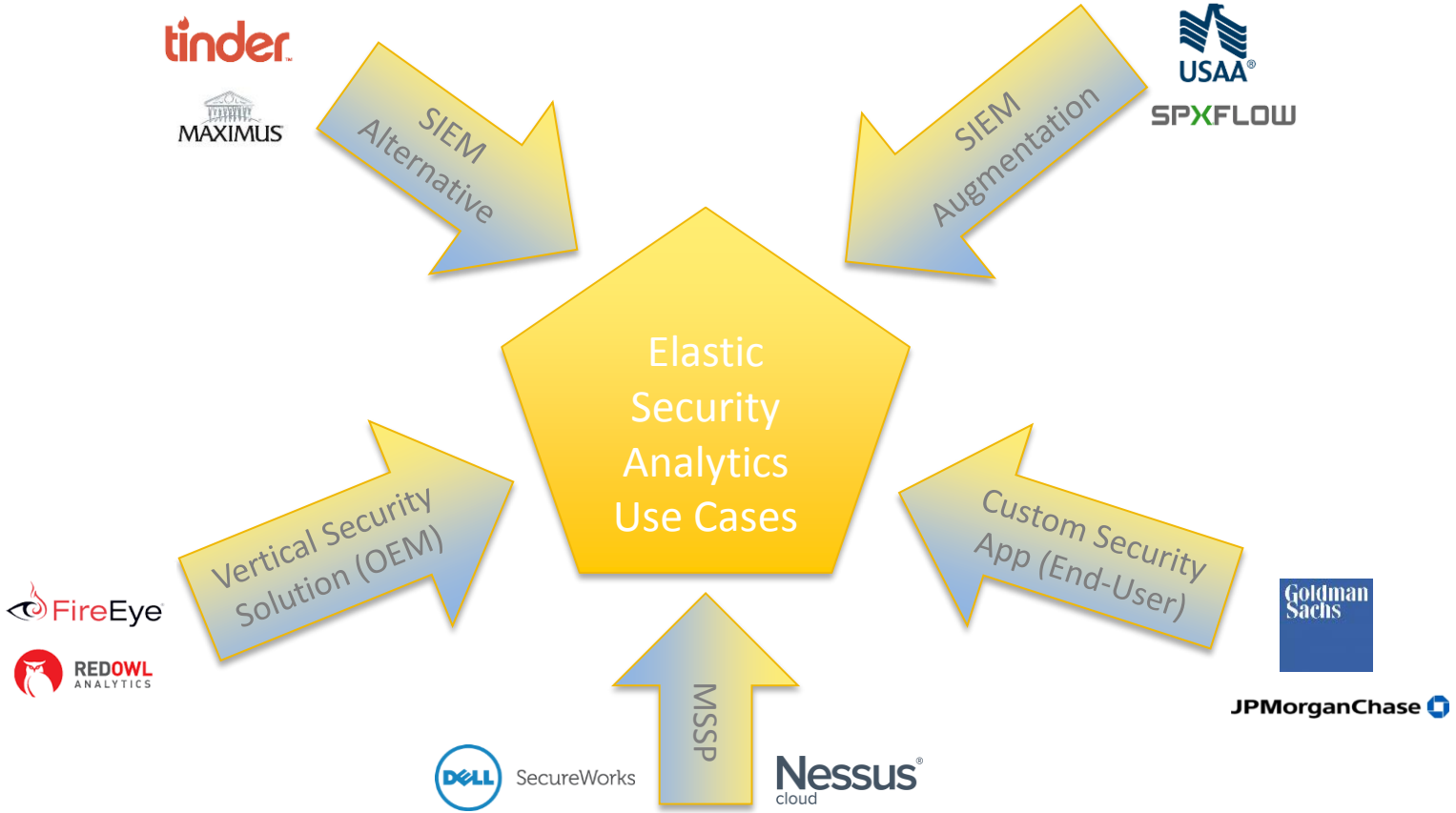
- Scale
  - Massive increase in amount of data to analyze
  - Monitoring your key # number of devices/apps bad practice
  - Massive increase in # of bad actors (internal / external)
  - Disregarding log files gets you fired
- Flexibility
  - Security team’s need open data
  - Slice & Dice in different ways

What is Security Analytics?

- Highly scalable collection, aggregation and real-time advanced analysis of diverse set of data:
  - Event data from security technologies
  - Event data from other related IT log sources
  - Threat intelligence
  - Asset information
  - User information
- To support security-related use cases:
  - Real-time monitoring
  - Threat detection
  - Incident response
  - Custom security-related applications

We mine and analyze **4 billion** events every day to detect security hacks and threats.

Who's using the Elastic for Security Analytics?



Why Elastic for Security Analytics

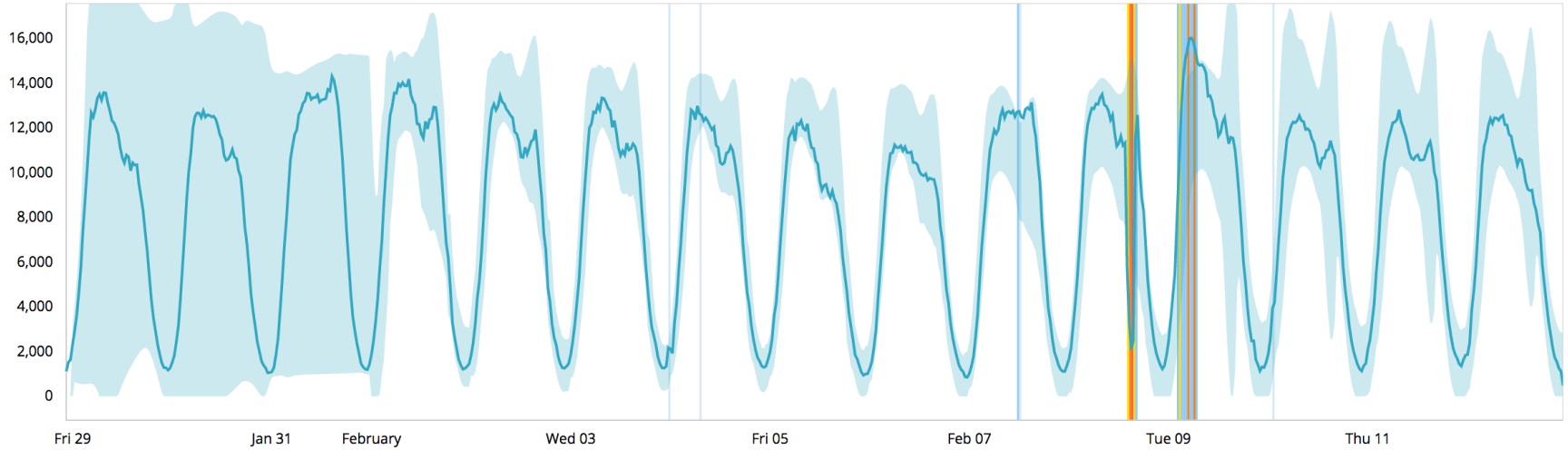
- Harness the speed and scale of Elasticsearch
  - Powerful alerting and correlation based on elastic searches
  - Machine learning automated anomaly detection finds unusual, rare events, attack behaviors
  - Graph helps to find relationships in security data to uncover threat activity
  - Role-based access controls help SOC teams allocate tasks to analysts

Chart interval: 30m Use full it_ops-kpi data

New job from index pattern it_ops-kpi

Aggregation **Field** **Bucket span**

Count 5m



Job it_ops-kpi created

Reset View Results

Job: it_ops-kpi and 2 others

Top Influencers

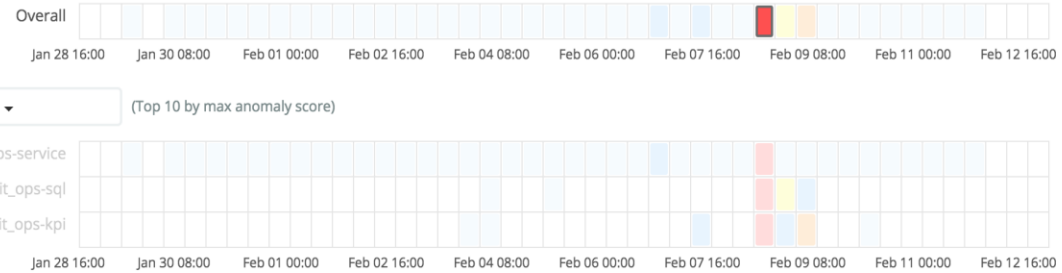
service

inventory-us-east-1-34	94	97
auth-us-west-1-1e	7	51
test-srv-02	5	29
elasticsearch-22	3	16
elasticsearch-77	2	11
payment-srv-21	2	6
payment-srv-11	1	5
backup-srv-13	1	9
test-srv-01	1	7
inventory-us-west-1-4e	1	7

hostname

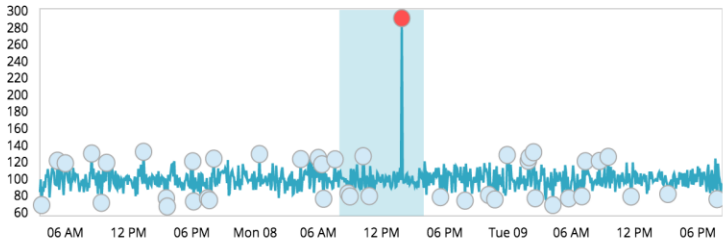
MSSQL-0783E4076	94	1237

Anomaly timeline

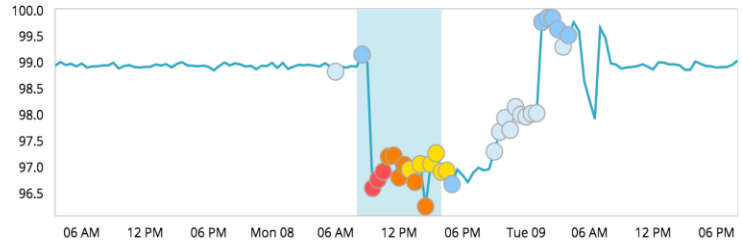


Anomalies

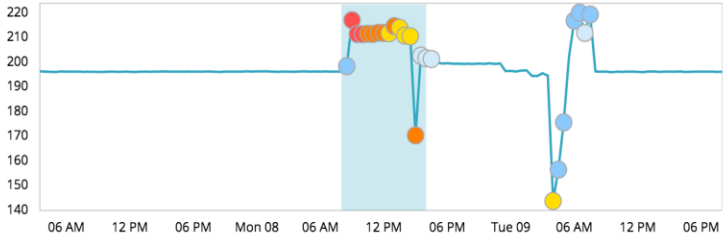
mean responsetime service inventory-us-east-1-34



mean SQLServer_Buffer_Manager_Buffer_cache_hit_ratio hostname MSSQL-0783E4076



mean SQLServer_General_Statistics_User_Connections hostname MSSQL-0783E4076



mean SQLServer_SQL_Statistics_Batch_Requests_sec hostname MSSQL-0783E4076

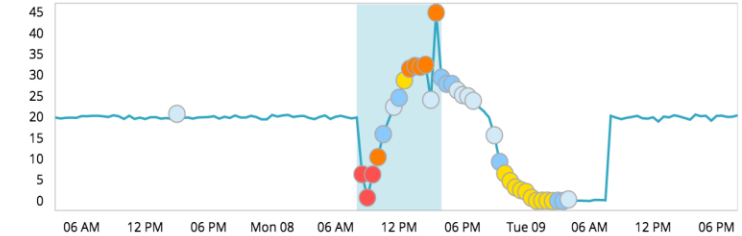


Chart interval: 1h Use full it_ops-services data

New job from index pattern it_ops-services

Fields

responsetime Average

Bucket span

5m

Split Data

service

Key Fields

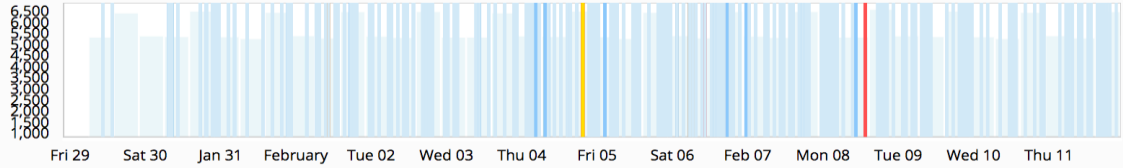
service

Job Details

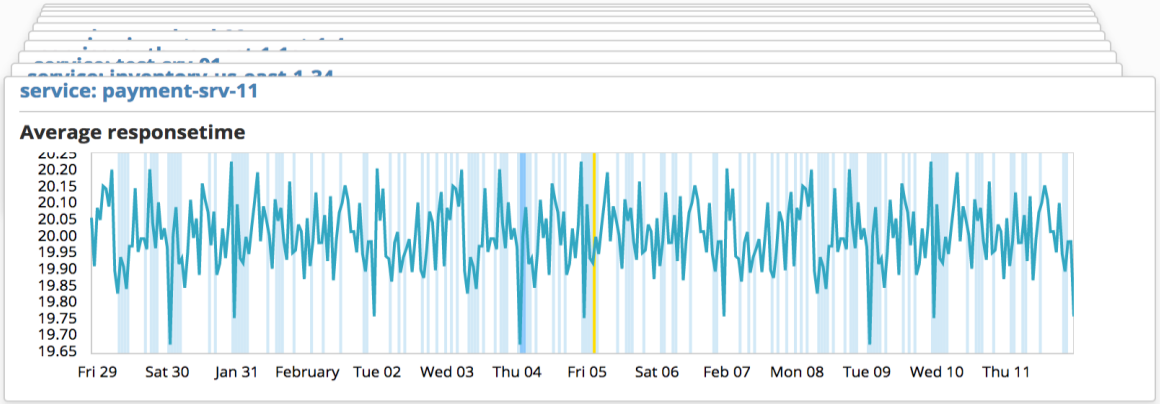
Job it_ops-service created

Reset View Results

Document count

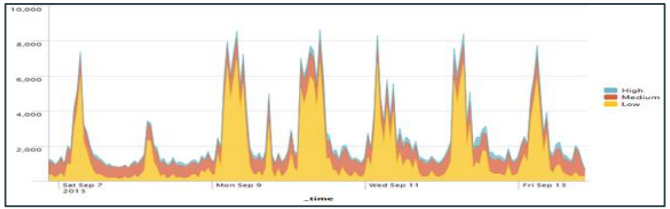


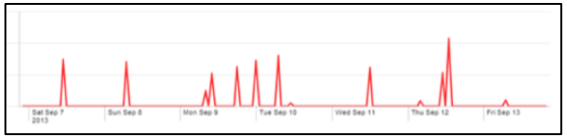
Data split by service

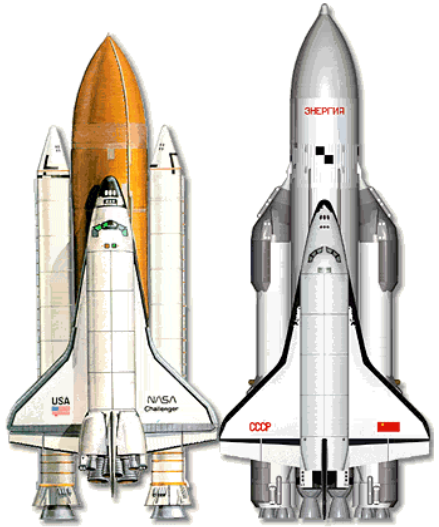


Customer Example Machine Learning

- Security and protection of intellectual property critical to business
- Current intrusion detection systems (IDS) generating 1000s alerts per day
  - ML reduced this to a handful of alerts per week







- Other use cases
  - Identifying web site scanners and snoopers
  - Identifying users that were abusing of internet privileges
  - Identifying unusual data exfiltration

Summary

- Elastic provides a scalable, flexible, extensible, performant, cost-effective platform that improve the security-related threat detection and incident response capabilities
  - As **alternative** to SIEM to establish basic security analytics capabilities
  - To **augment** their existing SIEM to build an effective security analytics solution
  - To build a **custom security-related app**

We analyze piles of data:

13B AMP queries/day

600B emails/day

16B web requests/day

Security Analytics Success Stories

https://www.elastic.co/content-pack?id=1463729261240613

Security Analytics with the Elastic Stack

Watch the Recording

Watch the Recording

Watch the Recording (47:49)

Watch the Recording

Securing Elasticsearch

Watch the Recording

Watch the Recording

Watch the Recording

Watch the Recording

Read the Post

THANK YOU

hans@elastic.co
www.elastic.co