elastic | 中国开发者大会

Elastic for Security Analytics
安全分析

Andy Karandikar
Elastic Senior Director, Solutions Architecture



战略级赞助商 HUAWEI | 钻石级赞助商 普翔 | 白金级赞助商 华夏博格 SINO BIG DATA 神州数码 Digital China | 金牌级赞助商 iDataAPI

合作伙伴 开源中国 oschina.net 掘金 谱时 IT大咖说 otpub Broadview www.broadview.com.cn 百格活动 bagevent.com MAXHUB


elastic
ELASTIC for
SECURITY ANALYTICS
安全分析
Andy Karandikar / 安迪 卡兰迪卡
Sr Director, Solutions Architecture
架构部高级总监

Attacks are INEVITABLE

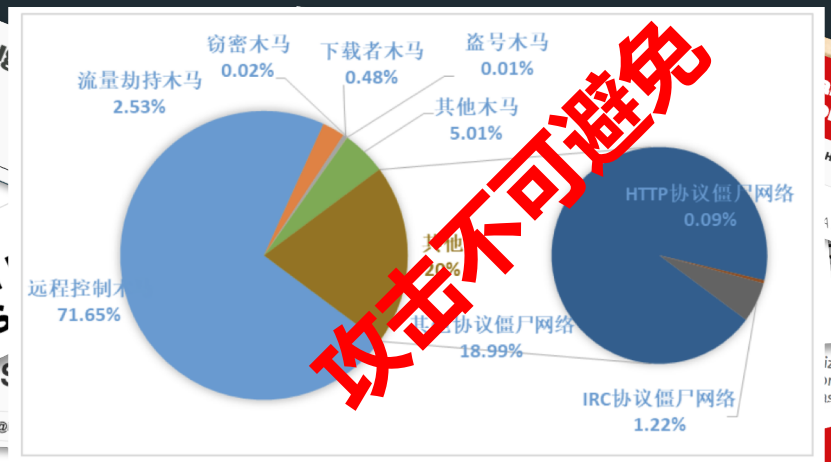


图 1 2017 年我国计算机感染恶意程序类型及分布

Uber data breach "raises hug
watchdog

Up to 100,0
in Fafsa Tool Breac

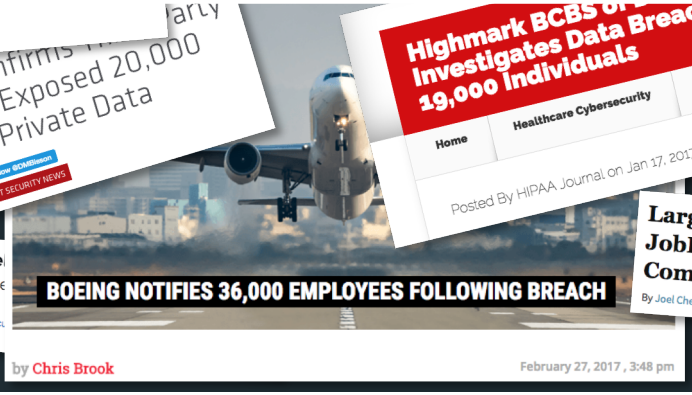
By ALAN RAPPEPORT APRIL 6, 2017

NBCNEWS
TECH > SECURITY
Massive Equifax Data
Affect Half of the U.S

Data Breaches on Track to
1,500 in 2017

Scottrade Confirms
Data Breach Exposed 20,000
Customers' Private Data

A huge trove of patient data le
The data of almost a million patients with diabetes and othe



Highmark BCBS
Investigates Data Breach
19,000 Individuals

Home
Healthcare Cybersecurity
Highmark BCBS of Delaware Investigates Data Breach Affecting 19,000 Individuals
Posted By HIPAA Journal on Jan 17, 2017

Large-Scale Breach Of America's
JobLink Alliance Potentially
Compromised Millions Of Job Seekers
By Joel Cheesman March 29, 2017 ERE

nd Women's Health Reports
nware Attack
Healthcare Cybersecurity
Ashland Women's Health Reports Ransomware Attack
Journal on Apr 13, 2017

es notifies 22
s of data brea

HIPAA AND COMPLIANCE NEWS
Patient data breach at Washington University School of Medicine

amily Services

Family service rochester

ABCD Pediatrics Breached and Hit with Ransomware
April 5, 2017 Kayla Thrailkill

North Carolina data breaches expose internal documents, personal records
Two unrelated breaches exposed both official working documents and the social security numbers of agency customers.
By Colin Wood



Traditional SIEM

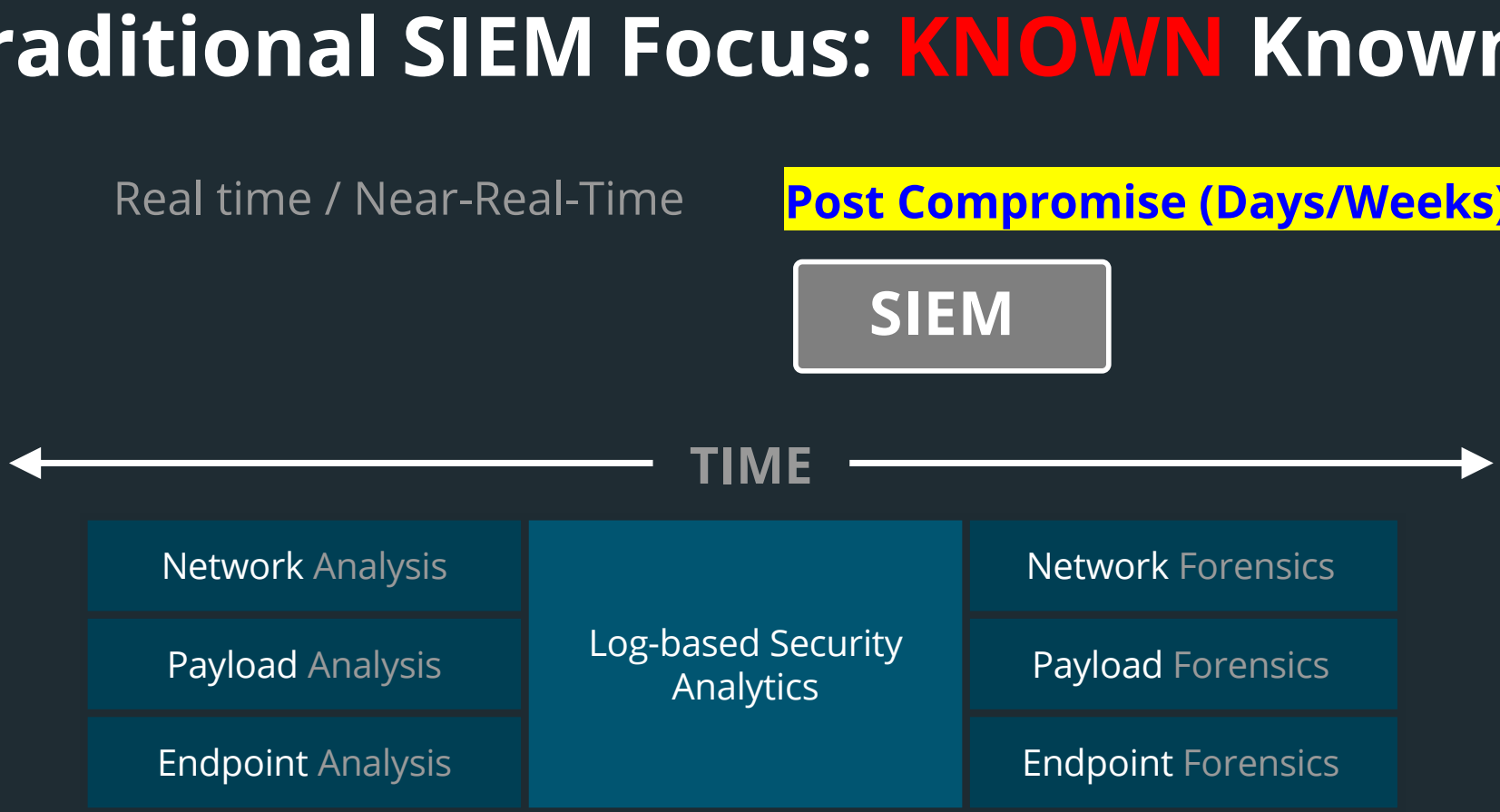
(Security Incident & Event Management)

CHALLENGES

Traditional SIEM Focus: KNOWN Knowns

Real time / Near-Real-Time

Post Compromise (Days/Weeks)

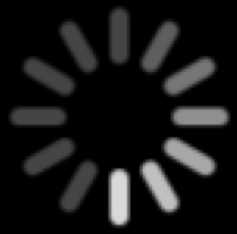


1

Security data exploding

ad hoc exploration suffers at scale

Poor speed @ scale



2

New threats every day

SIEM correlations and rules fall short


Limited visibility

3

Too Expensive & Rigid

Forced to drop data

NEXT-GEN Threat Hunting needs...

Data collection **Visualizations**
Machine Learning Aggregation
Query language *Drill down* **Centralized Logging**
Enrichment Fast **Real-time** **Alerting**
Anomaly Detection Reports Normalization
Indexing **Search** Advanced Analytics **Dashboards**

Next gen CyberSecurity w/ Smart DevOps



Horizontal Scale



Real-Time Data Availability



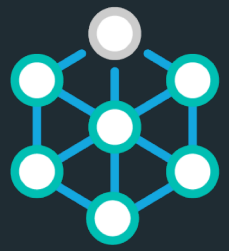
Flexible Data Model



Rapid Query Execution



Sophisticated Query Language



Schemaless

SIEM Augmentation: Threat HUNTING

Real time / Near-Real-Time

Post Compromise (Days/Weeks)



TIME

Network Analysis	Log-based Security Analytics	Network Forensics
Payload Analysis		Payload Forensics
Endpoint Analysis		Endpoint Forensics

FORRESTER®

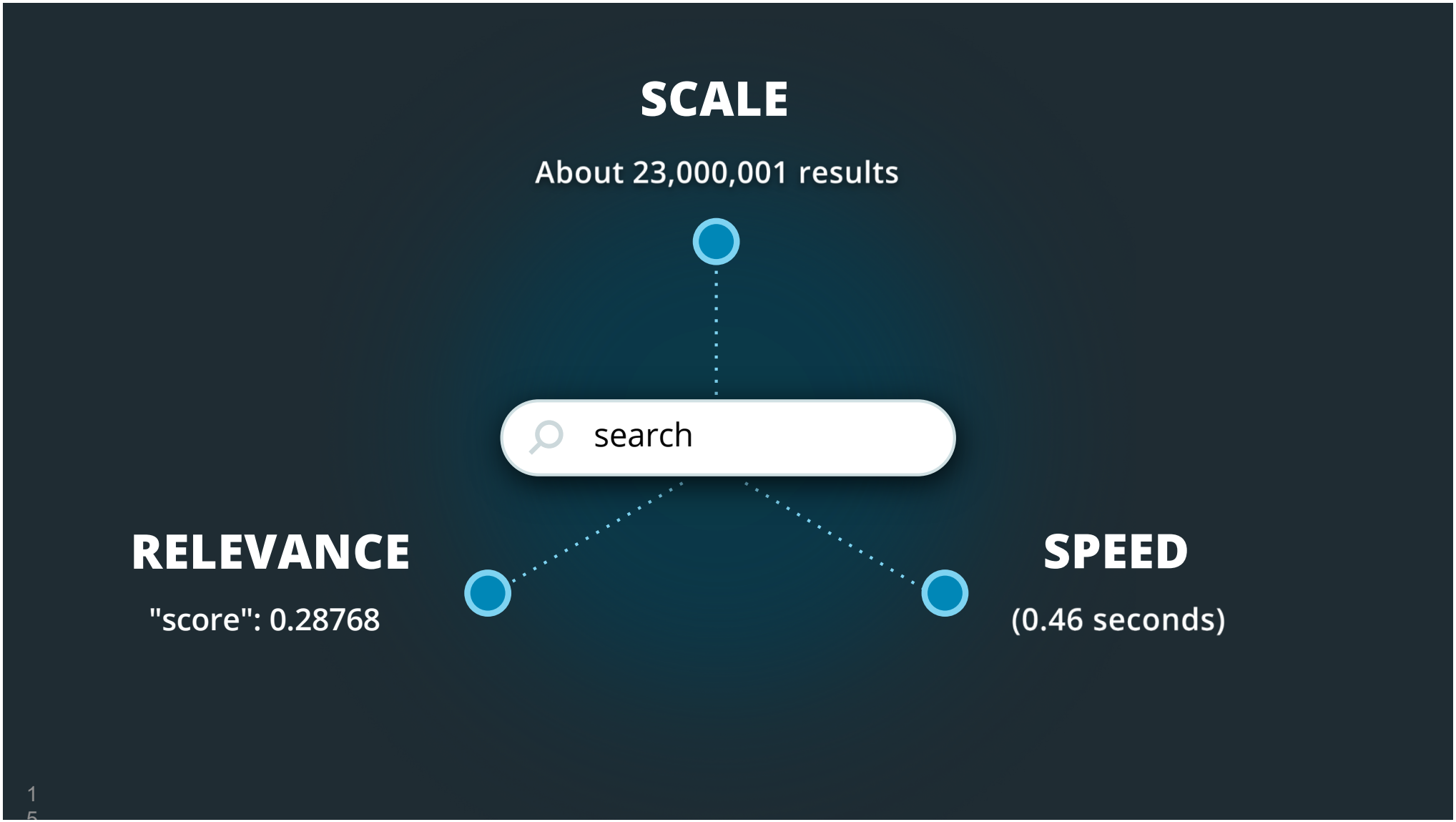
Many security teams are choosing to store logs outside of traditional log management tools. Open source options like the **Elasticsearch, Logstash, and Kibana (ELK) stack** and Graylog are becoming increasingly common.

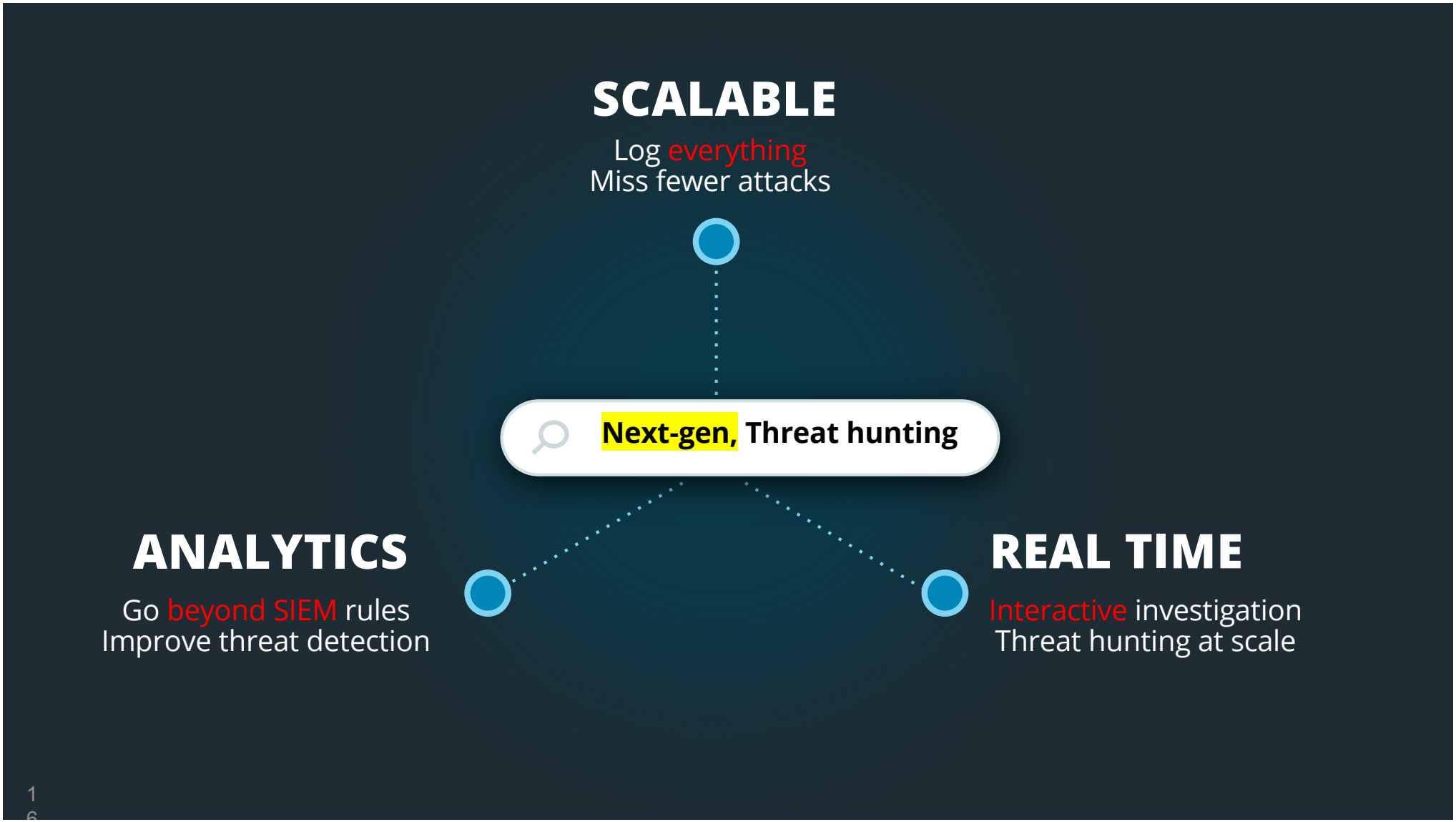
elastic

Gartner®

Consider open-source tools, like the **Elastic Stack (also known as the ELK stack)** when your organization has the resources and expertise to dedicate to implementing, customizing and administering these tools.

elastic


SCALE
About 23,000,001 results
search
RELEVANCE
"score": 0.28768
SPEED
(0.46 seconds)


SCALABLE
Log everything
Miss fewer attacks
Next-gen, Threat hunting
ANALYTICS
Go beyond SIEM rules
Improve threat detection
REAL TIME
Interactive investigation
Threat hunting at scale



> We were able to convert 80% of our SIEM rules into Watcher alerts. We will tackle the remaining 20% in the future.

Neelsen “Nelly” Cyrus, Senior Security Analyst

https://www.elastic.co/elasticon/conf/2016/sf/all-quiet-digital-front-security-analytics-usaa

elastic

Users across all segment































Many use cases

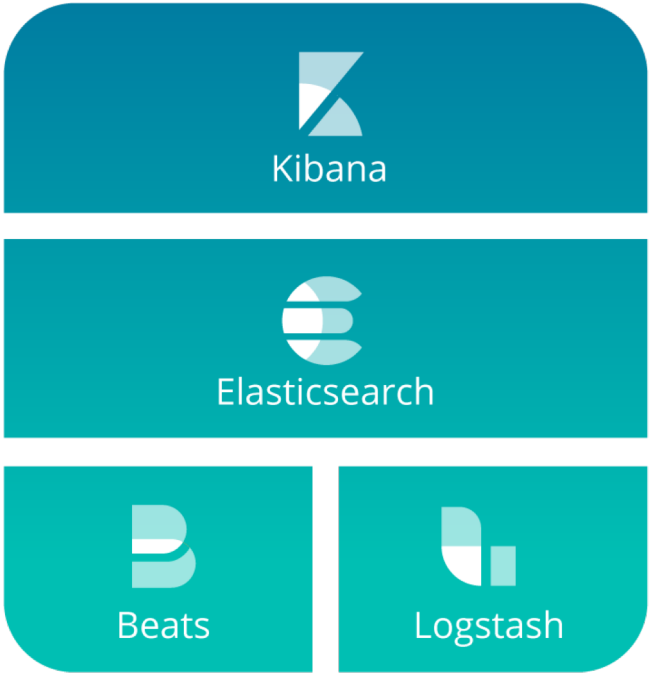
SIEM Alternative *(internal)*	Security Ops team **No SIEM in place**	slack
SIEM Augmentation *(internal)*	Security Ops teams **Existing SIEM hitting limits**	BARCLAYS
Custom Security App *(internal)*	In house dev team **Creates special security projects/apps**	Goldman Sachs
MSSP *(external)*	Service provider business **Creates managed SIEM solution**	Nessus® cloud
Vertical Security Solution *(end user)*	Security vendor / OEMs **Builds an end solution**	FireEye elastic

The Product Stack



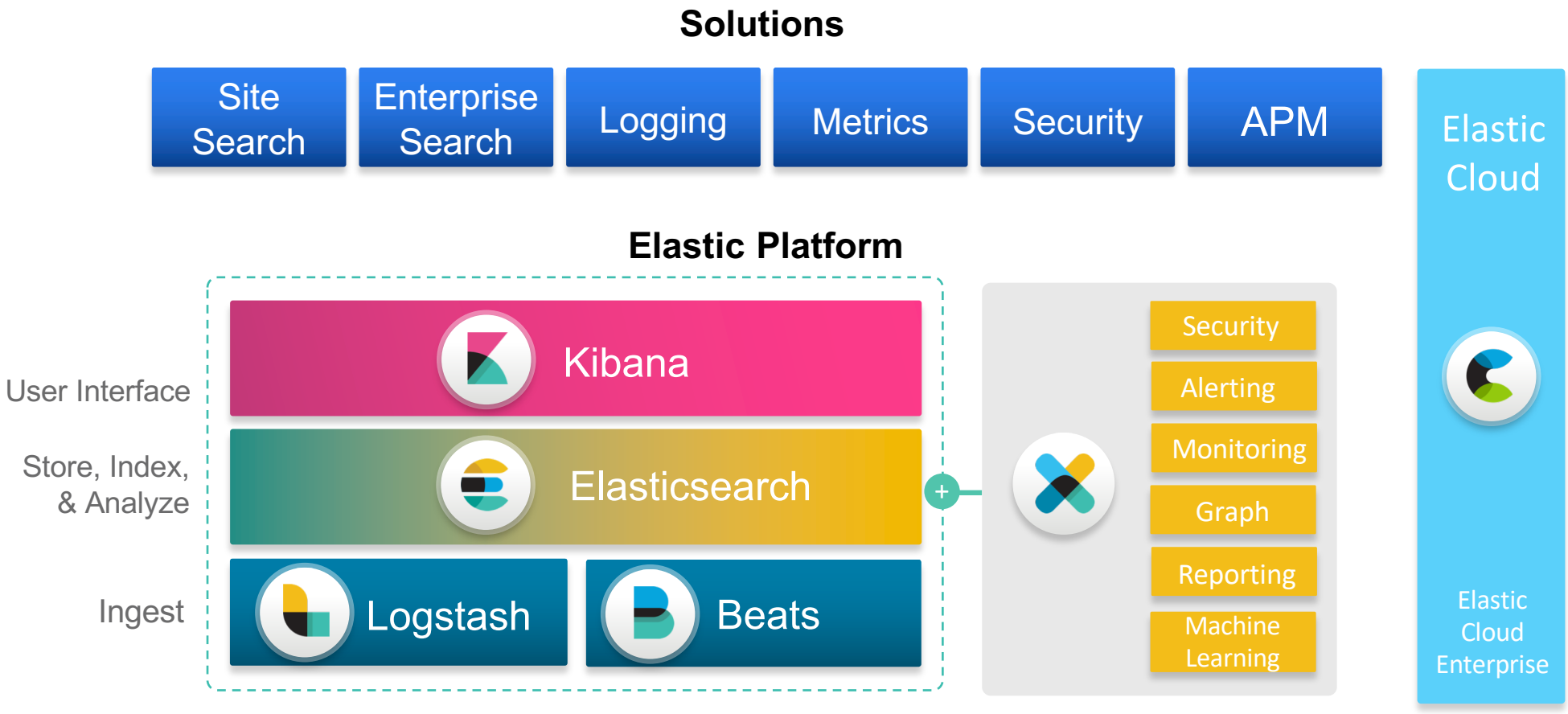
Elastic Stack

100% open source



elastic

Our Product Portfolio





Security

Protect Data Access

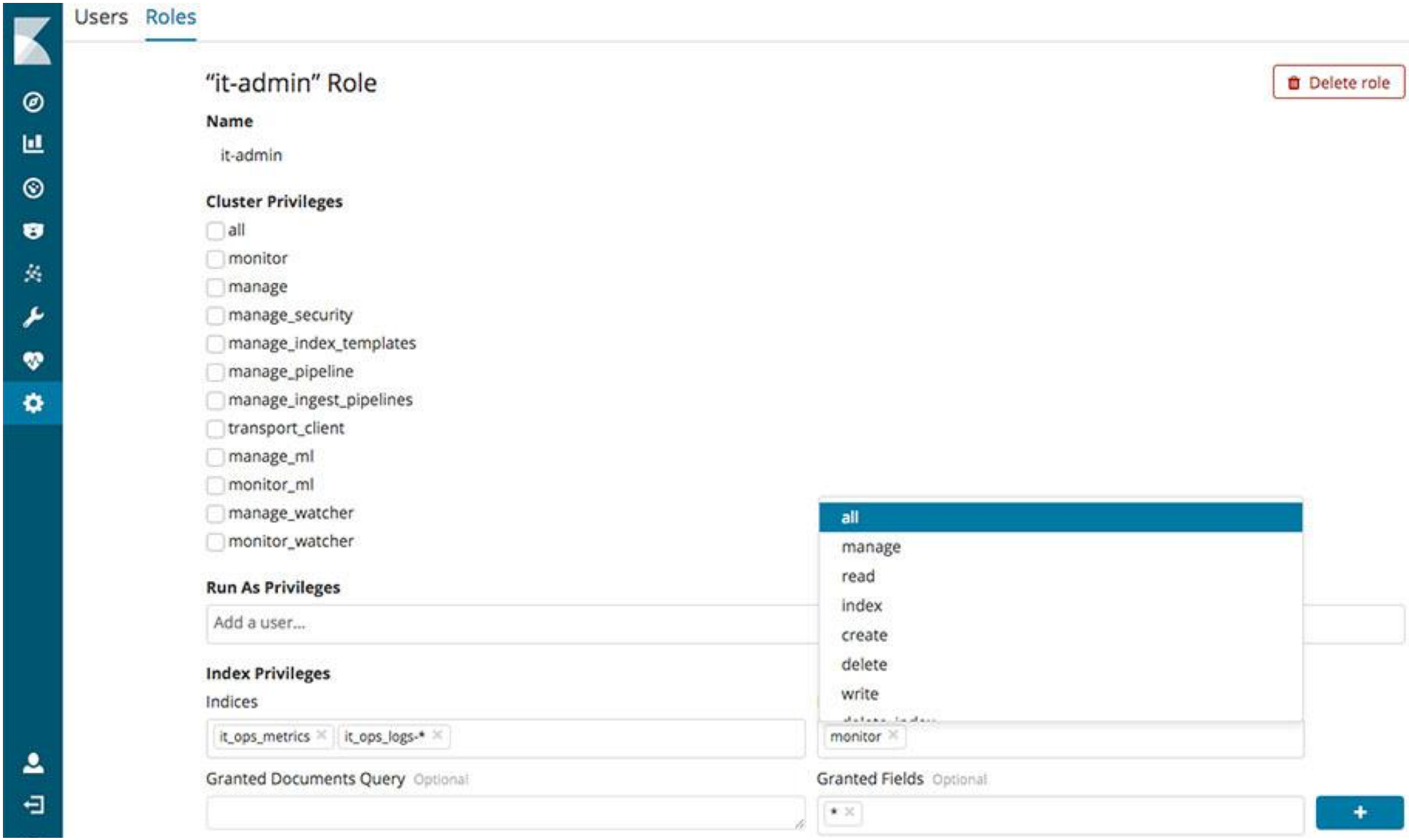
- Username and password
- Role-based access control
- Field & document level security
- Integrate with authentication systems

Encrypt Data

- SSL/TLS encryption

Provide Accountability

- Audit logging


Users
Roles
"it-admin" Role
Delete role
Name
it-admin
Cluster Privileges
all
monitor
manage
manage_security
manage_index_templates
manage_pipeline
manage_ingest_pipelines
transport_client
manage_ml
monitor_ml
manage_watcher
monitor_watcher
Run As Privileges
Add a user...
Index Privileges
Indices
it_ops_metrics
it_ops_logs-*
Granted Documents Query Optional
Granted Fields Optional
*
all
manage
read
index
create
delete
write
monitor



Alerting

Detect Changes in Your Data

- If you can query it, you can alert on it
- Store & track alert history

Get notified your way

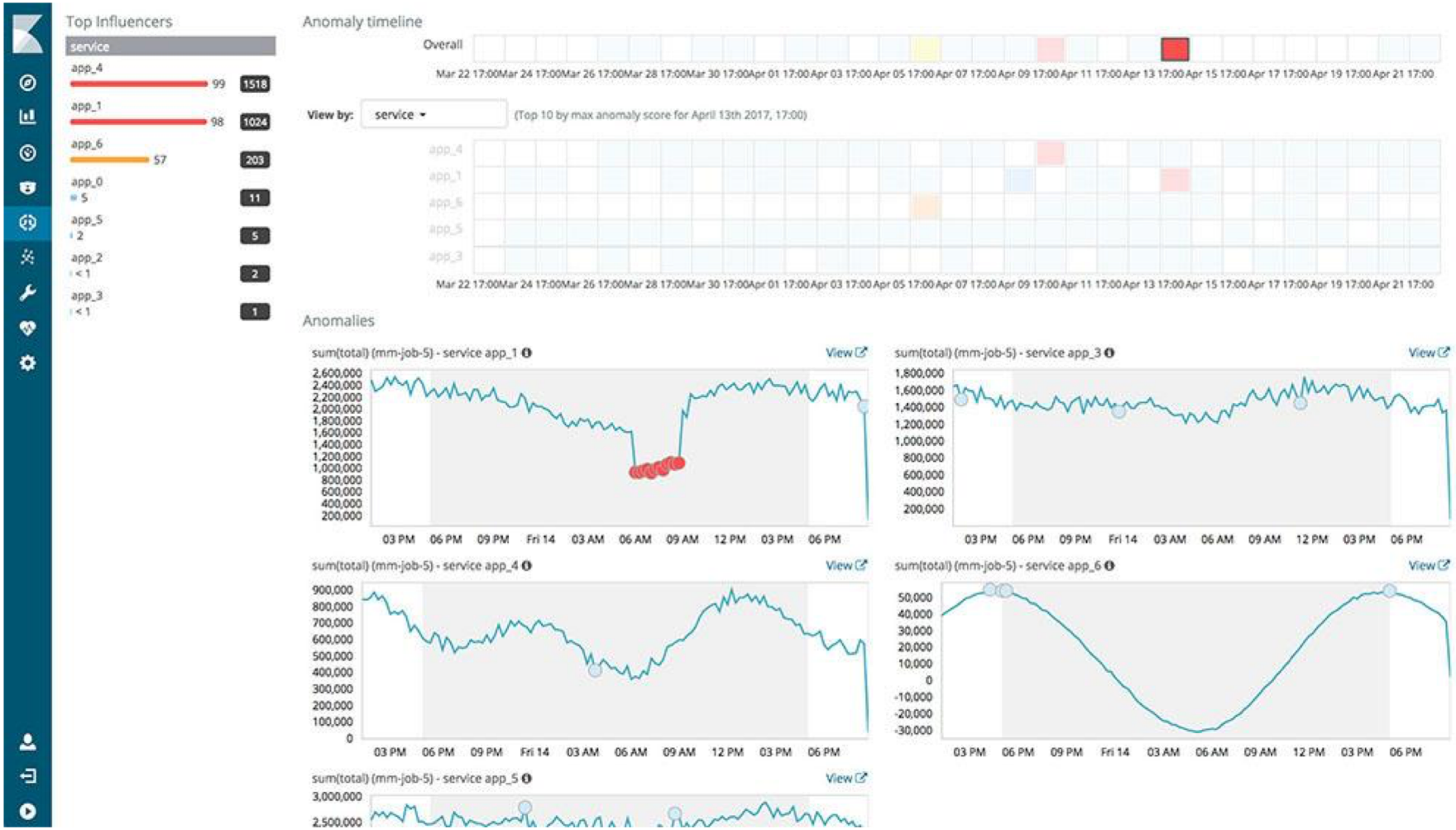
- Email, Slack, PagerDuty, HipChat or JIRA
- Custom integration via webhooks

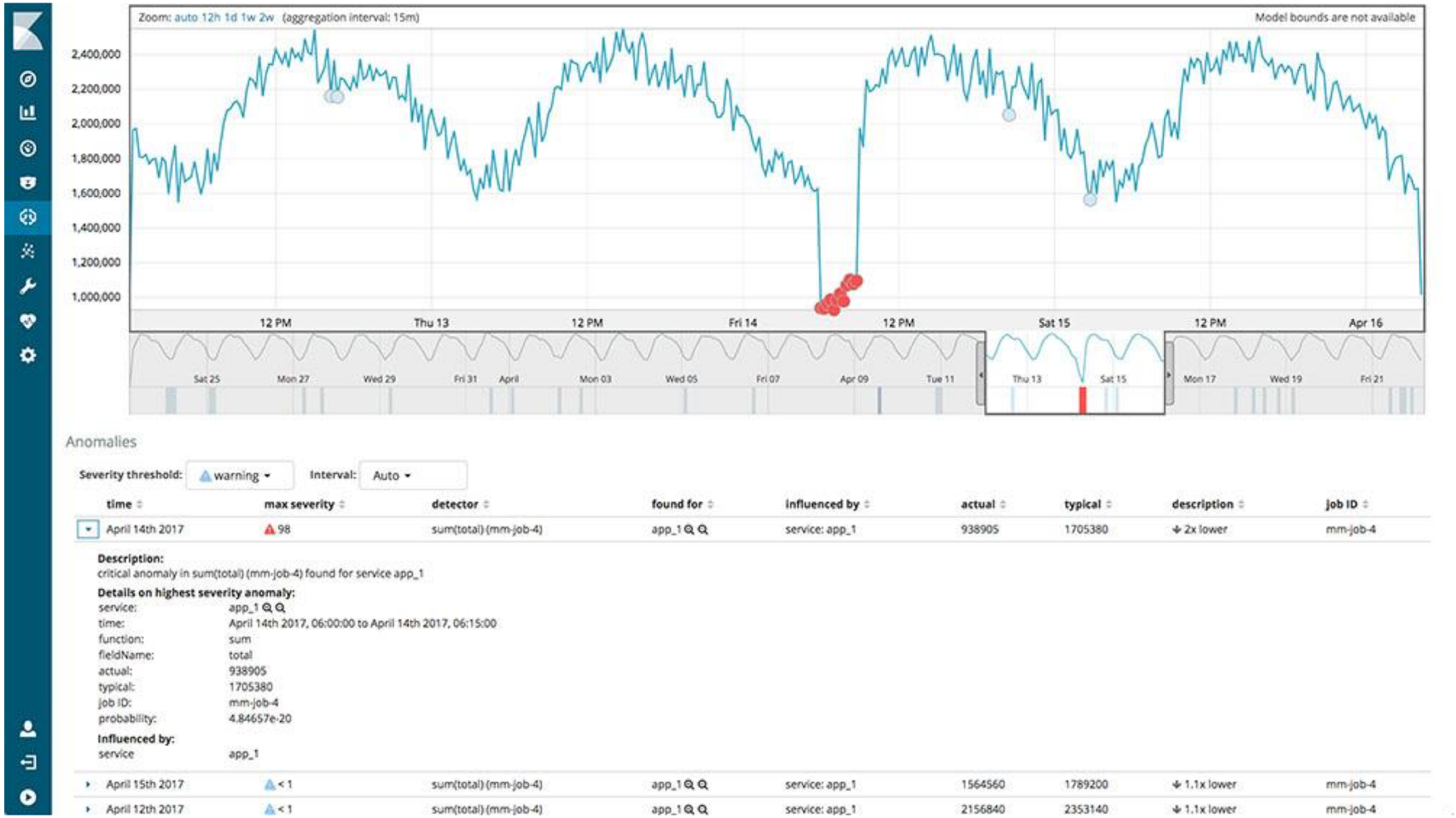


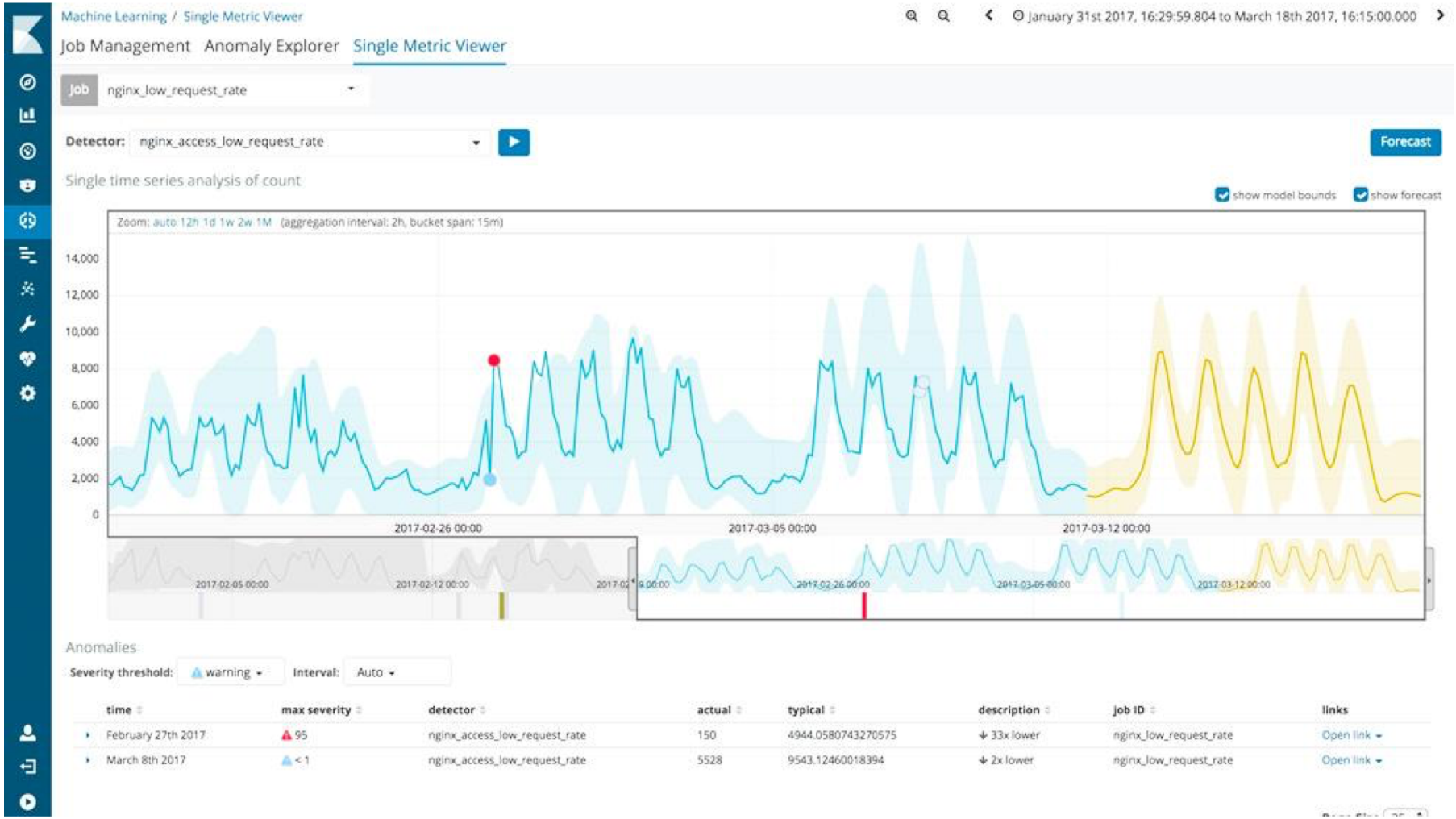
Machine Learning

Unsupervised Machine Learning

- Automate anomaly detection
- Accelerate root cause analysis
- Go beyond SIEM rules
- Reduce false positives


Top Influencers
service
app_4 99 1518
app_1 98 1024
app_6 57 203
app_0 5 11
app_5 2 5
app_2 < 1 2
app_3 < 1 1
Anomaly timeline
Overall
Mar 22 17:00Mar 24 17:00Mar 26 17:00Mar 28 17:00Mar 30 17:00Apr 01 17:00 Apr 03 17:00 Apr 05 17:00 Apr 07 17:00 Apr 09 17:00 Apr 11 17:00 Apr 13 17:00 Apr 15 17:00 Apr 17 17:00 Apr 19 17:00 Apr 21 17:00
View by: service
(Top 10 by max anomaly score for April 13th 2017, 17:00)
app_4
app_1
app_6
app_5
app_3
Anomalies
sum(total) (mm-job-5) - service app_1
View
sum(total) (mm-job-5) - service app_3
sum(total) (mm-job-5) - service app_4
sum(total) (mm-job-5) - service app_6
sum(total) (mm-job-5) - service app_5
03 PM 06 PM 09 PM Fri 14 03 AM 06 AM 09 AM 12 PM 03 PM 06 PM


Zoom: auto 12h 1d 1w 2w (aggregation interval: 15m)
Model bounds are not available
2,400,000
2,200,000
2,000,000
1,800,000
1,600,000
1,400,000
1,200,000
1,000,000
12 PM
Thu 13
12 PM
Fri 14
12 PM
Sat 15
12 PM
Apr 16
Sat 25
Mon 27
Wed 29
Fri 31
April
Mon 03
Wed 05
Fri 07
Apr 09
Tue 11
Thu 13
Sat 15
Mon 17
Wed 19
Fri 21
Anomalies
Severity threshold: warning
Interval: Auto
time
max severity
detector
found for
influenced by
actual
typical
description
job ID
April 14th 2017
98
sum(total) (mm-job-4)
app_1
service: app_1
938905
1705380
2x lower
mm-job-4
Description:
critical anomaly in sum(total) (mm-job-4) found for service app_1
Details on highest severity anomaly:
service: app_1
time: April 14th 2017, 06:00:00 to April 14th 2017, 06:15:00
function: sum
fieldName: total
actual: 938905
typical: 1705380
job ID: mm-job-4
probability: 4.84657e-20
Influenced by:
service app_1
April 15th 2017
< 1
sum(total) (mm-job-4)
app_1
service: app_1
1564560
1789200
1.1x lower
mm-job-4
April 12th 2017
< 1
sum(total) (mm-job-4)
app_1
service: app_1
2156840
2353140
1.1x lower
mm-job-4

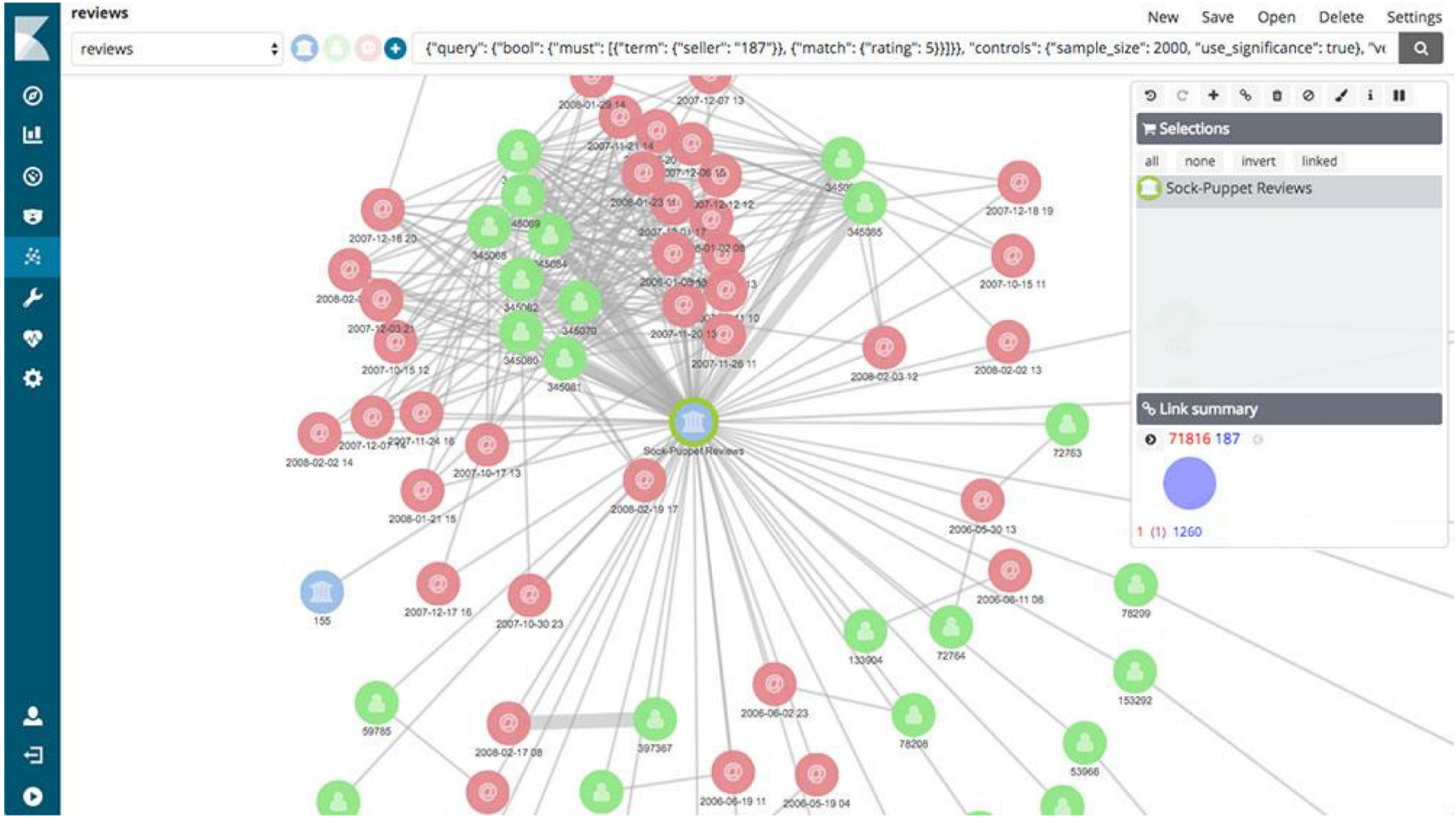

Machine Learning / Single Metric Viewer
January 31st 2017, 16:29:59.804 to March 18th 2017, 16:15:00.000
Job Management
Anomaly Explorer
Single Metric Viewer
Job
nginx_low_request_rate
Detector:
nginx_access_low_request_rate
Forecast
Single time series analysis of count
show model bounds
show forecast
Zoom: auto 12h 1d 1w 2w 1M (aggregation interval: 2h, bucket span: 15m)
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
2017-02-26 00:00
2017-03-05 00:00
2017-03-12 00:00
Anomalies
Severity threshold:
warning
Interval:
Auto
time
max severity
detector
actual
typical
description
job ID
links
February 27th 2017
95
nginx_access_low_request_rate
150
4944.0580743270575
33x lower
nginx_low_request_rate
Open link
March 8th 2017
< 1
nginx_access_low_request_rate
5528
9543.12460018394
2x lower
nginx_low_request_rate
Open link



Graph

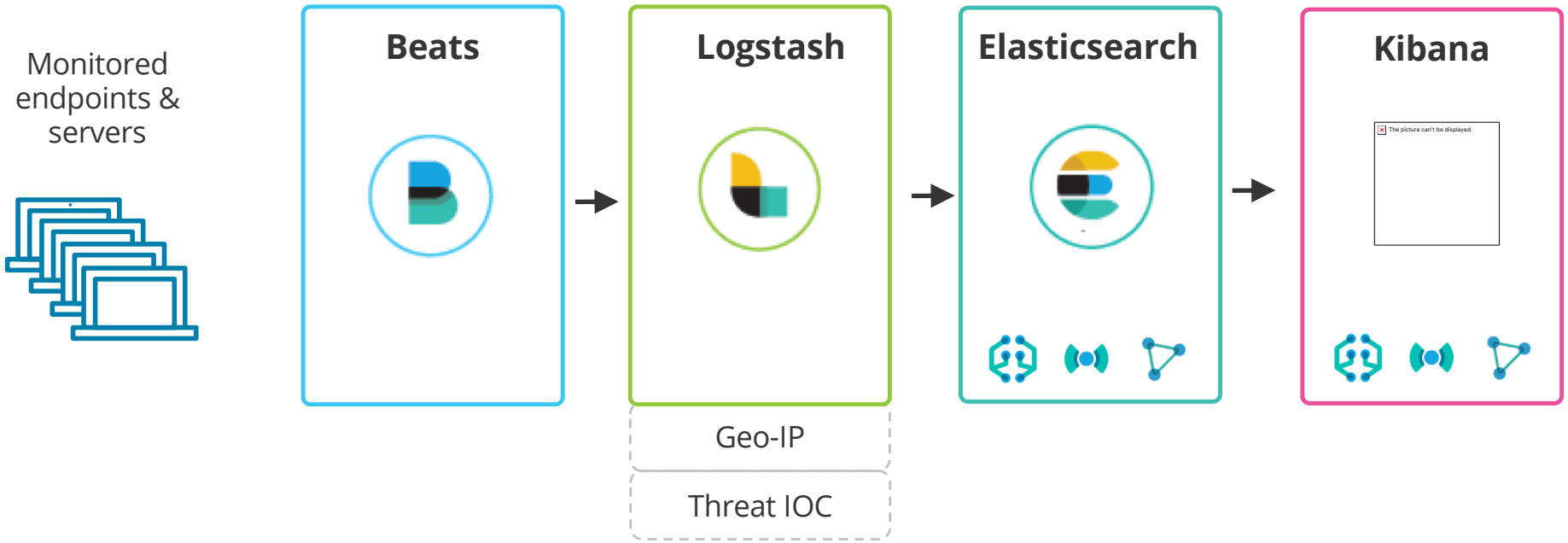
Find Connections in Your Data

- Uses relevance capabilities of Elasticsearch
- Leverage API and UI-drive tool


reviews
New
Save
Open
Delete
Settings
reviews
{"query": {"bool": {"must": [{"term": {"seller": "187"}}, {"match": {"rating": 5}}]}}}, "controls": {"sample_size": 2000, "use_significance": true}, "v
Selections
all
none
invert
linked
Sock-Puppet Reviews
Link summary
71816 187
1 (1) 1260
Sock-Puppet Reviews

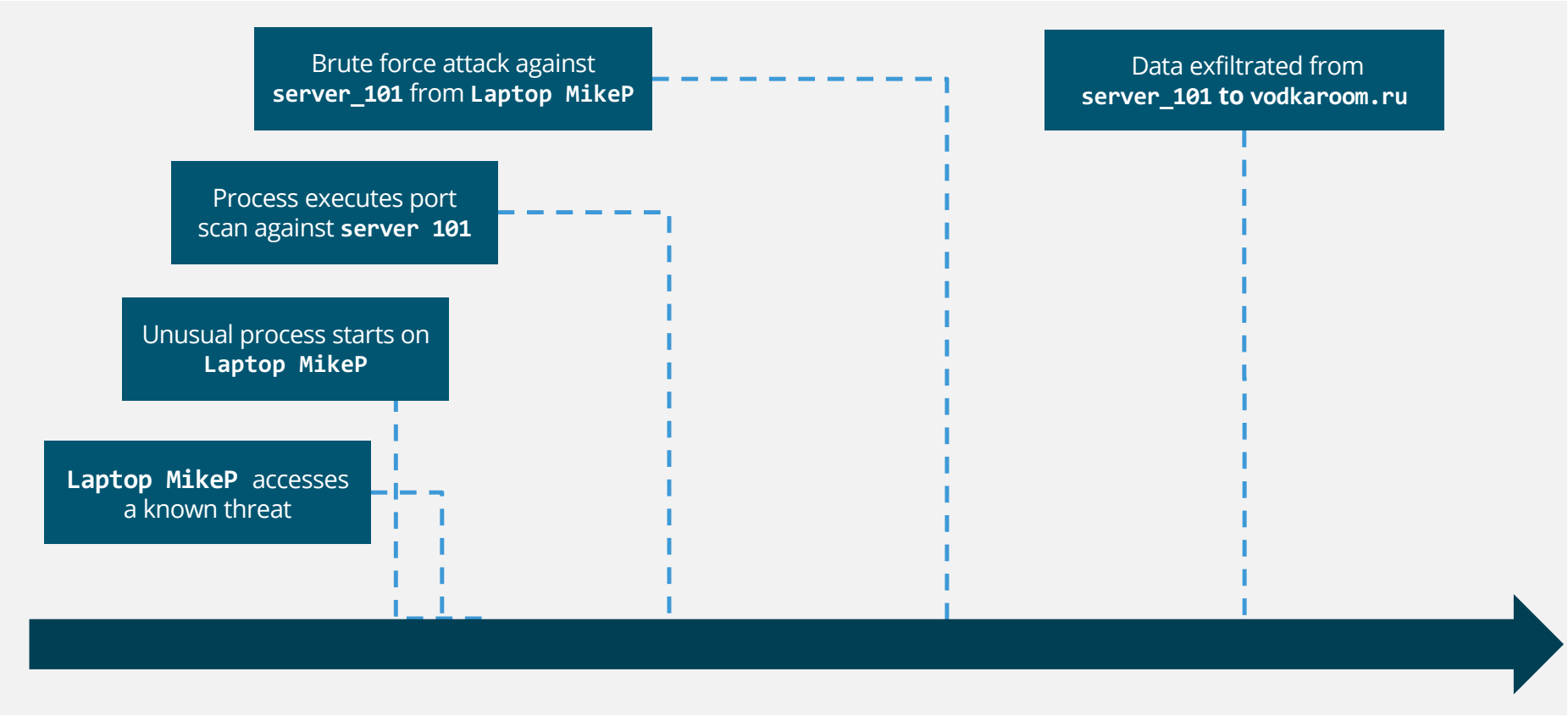
Demo

Security Analytics Demo - Environment



elastic

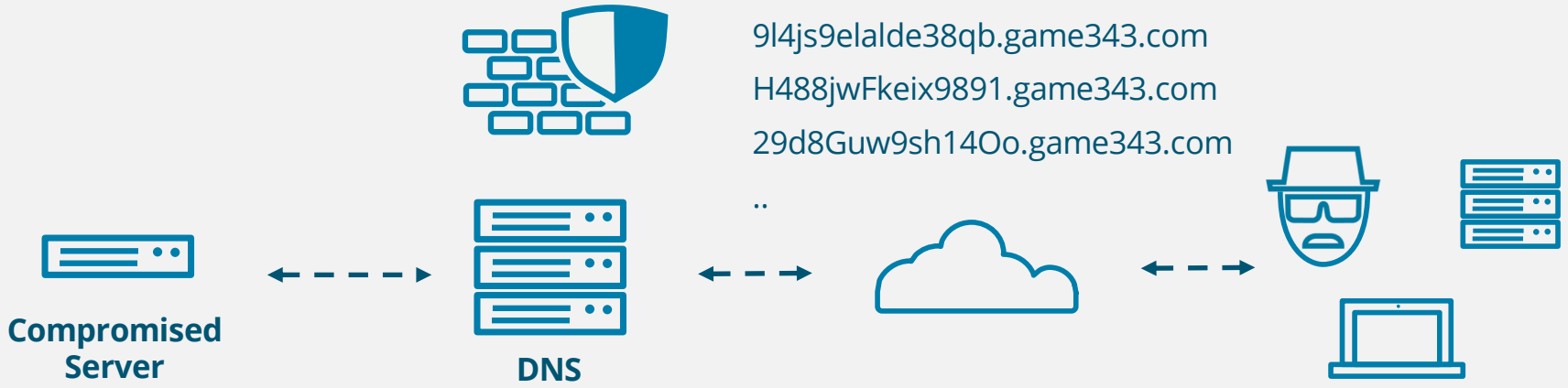
Security Analytics Demo - Attack Progression



Skip Recipe

elastic

Elementary Attack Behavior – DNS Tunneling



- Encrypted messages disguised as subdomains can contain control or data payloads
- Insufficient monitoring of DNS for ‘tunneling’ activity poses a significant risk

elastic



elastic
中文社区

专业、垂直、纯粹的 Elastic 开源技术交流社区
https://elasticsearch.cn/

elastic