Elastic 安全分析领域应用

杰瑞朱 = Jerry 朱杰
Elastic 架构师

挑战 一

安全数据暴增

Elastic从一开始就是为大数据设计的

- 横向扩展
- 分布式
- 近实时

挑战 二

安全威胁一直在变化

Elastic致力于从大数据中自动发现

- 一切都被索引记录
- 应对未知威胁
- 机器学习

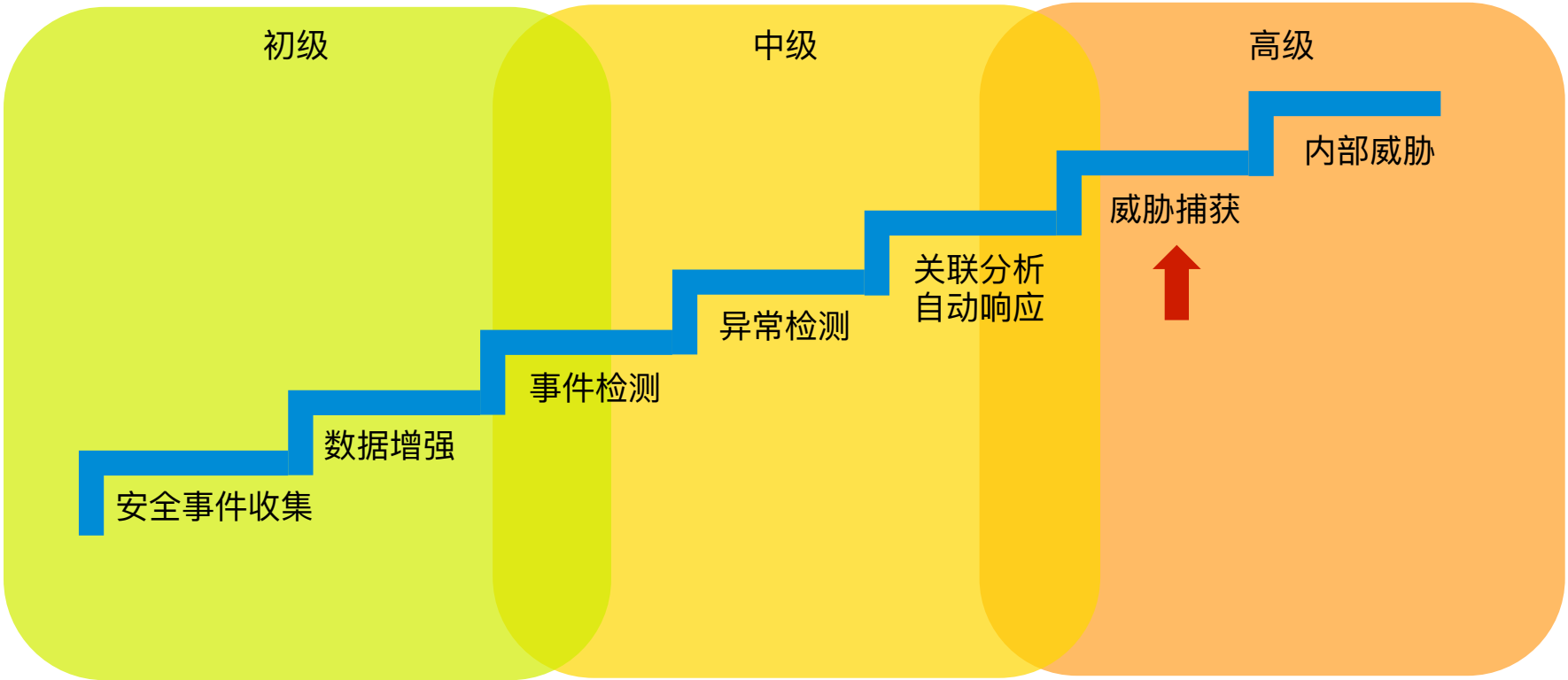
挑战 三

无意义的告警

Elastic 聚焦于

- 最相关的告警
- 明显的异常行为

企业安全成熟度阶梯



Elastic助力实现初级阶段目标

收集 从各种数据源采集数据完成拼图

整理 从各种数据源聚合和整理相关性

增强 为分析预先计算更多属性

索引 为快速搜索索引数据

Beats

Logstash

Elasticsearch

elastic

日志、指标采集 Beats生态

libbeat

插件

FILEBEAT
日志文件

插件

METRICBEAT
指标数据

PACKETBEAT
网络数据

FUNCTIONBEAT
云服务器监控

WINLOGBEAT
Window日志

HEARTBEAT
服务可用性监控

AUDITBEAT
Linux审核框架事件

httpbeat | apachebeat | nginxbeat | pingbeat

execbeat | dockerbeat | elasticbeat | 70+ 社区制造

elastic

日志、指标采集 Logstash生态

Logstash

200+ 插件

azure event hub	cloudwatch	couchdb	elasticsearch	exec
file	websocket	tcp	upd	graphite
http	http poller	imap	irc	java generator
java stdin	jdbc	jms	jmx	kafka
log4j	xmpp	redis	rss	s3
snmp	sqlite	stdin	syslog	github

更多
社区制造

elastic

开放生态 第三方重磅工具

elastic

Elastic更致力于实现中高级目标

机器学习 自动构建模型 异常检测 预测

关联分析 用图来展示数据关联

告警 检测变化 告警

Machine Learning

Graph

Alerting

elastic

告警

对任何的查询结果设置告警

ES集群提供功能

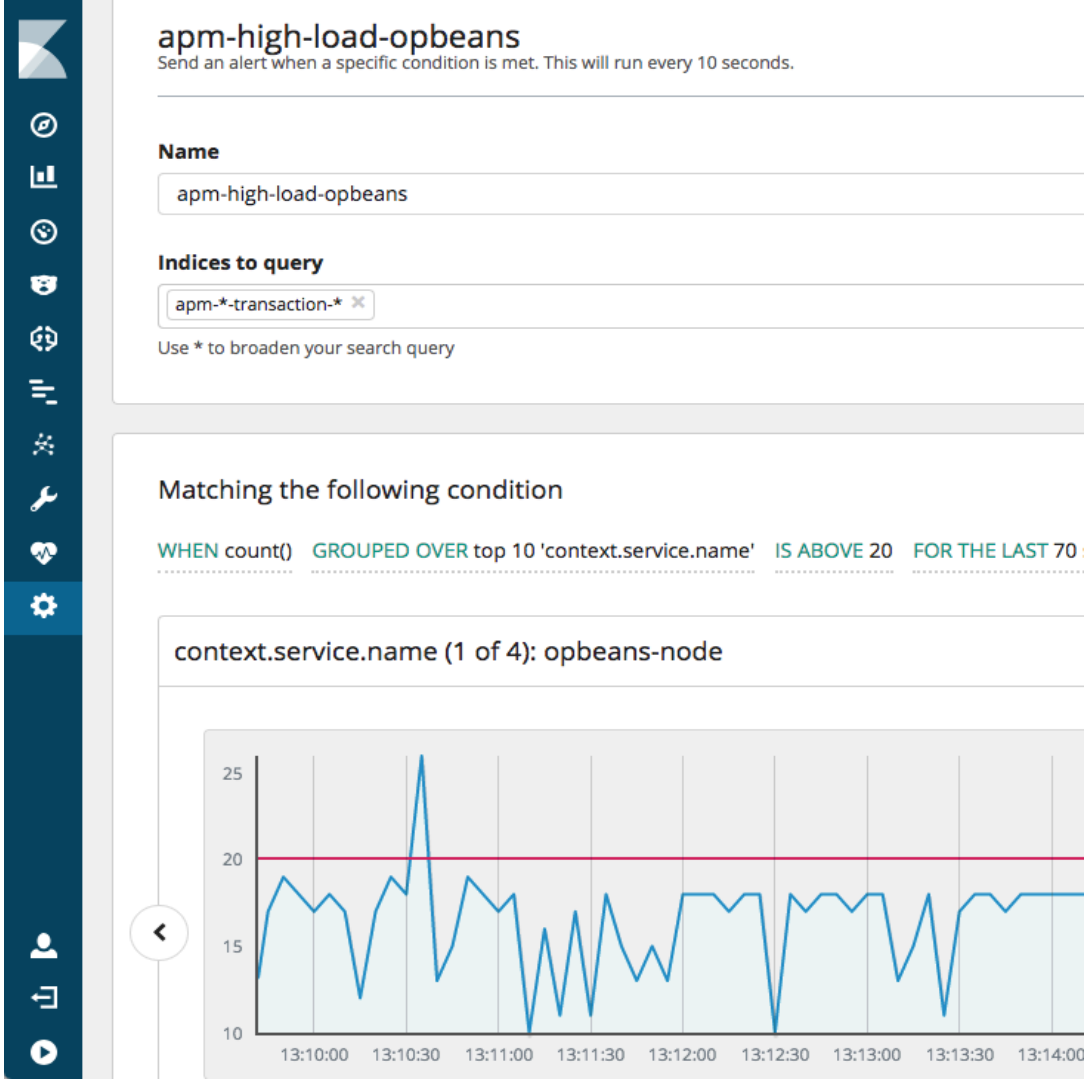
Elasticsearch查询结果设置告警
分布式执行，支持大量告警规则
高可用
定时
级联检测
告警抑制功能
API批量设定

通知

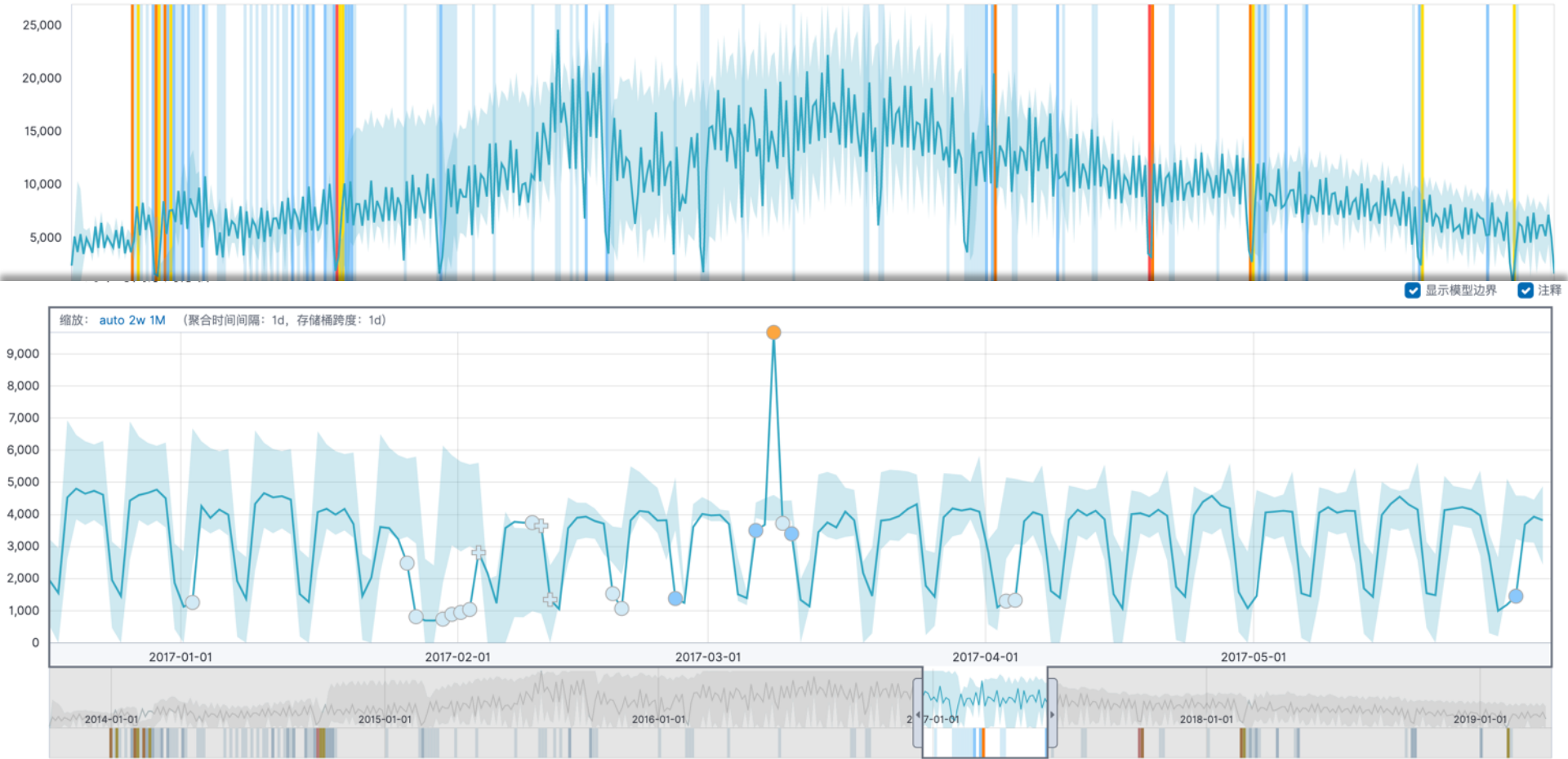
Email, Slack, PagerDuty，Jira，Log，Index，webhook

和ES原生功能的集成

机器学习，ES集群监控，报表



机器学习- 更加智能的检测和告警



机器学习

发现不正常的数据

自动异常检测

非监督机器学习

增量生成模型

单个 & 多个时间序列

检测出异常点

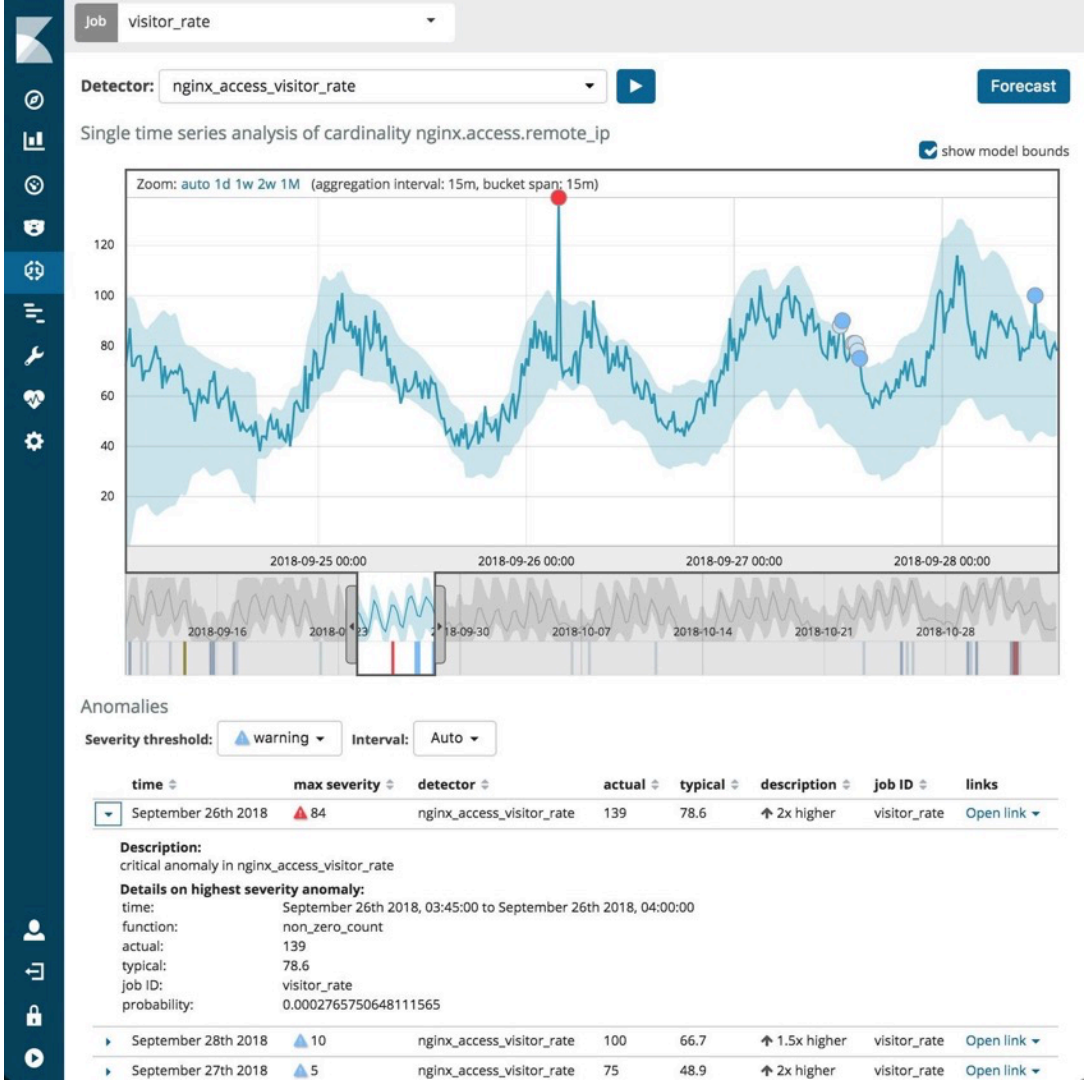
预测

还能回答什么问题?

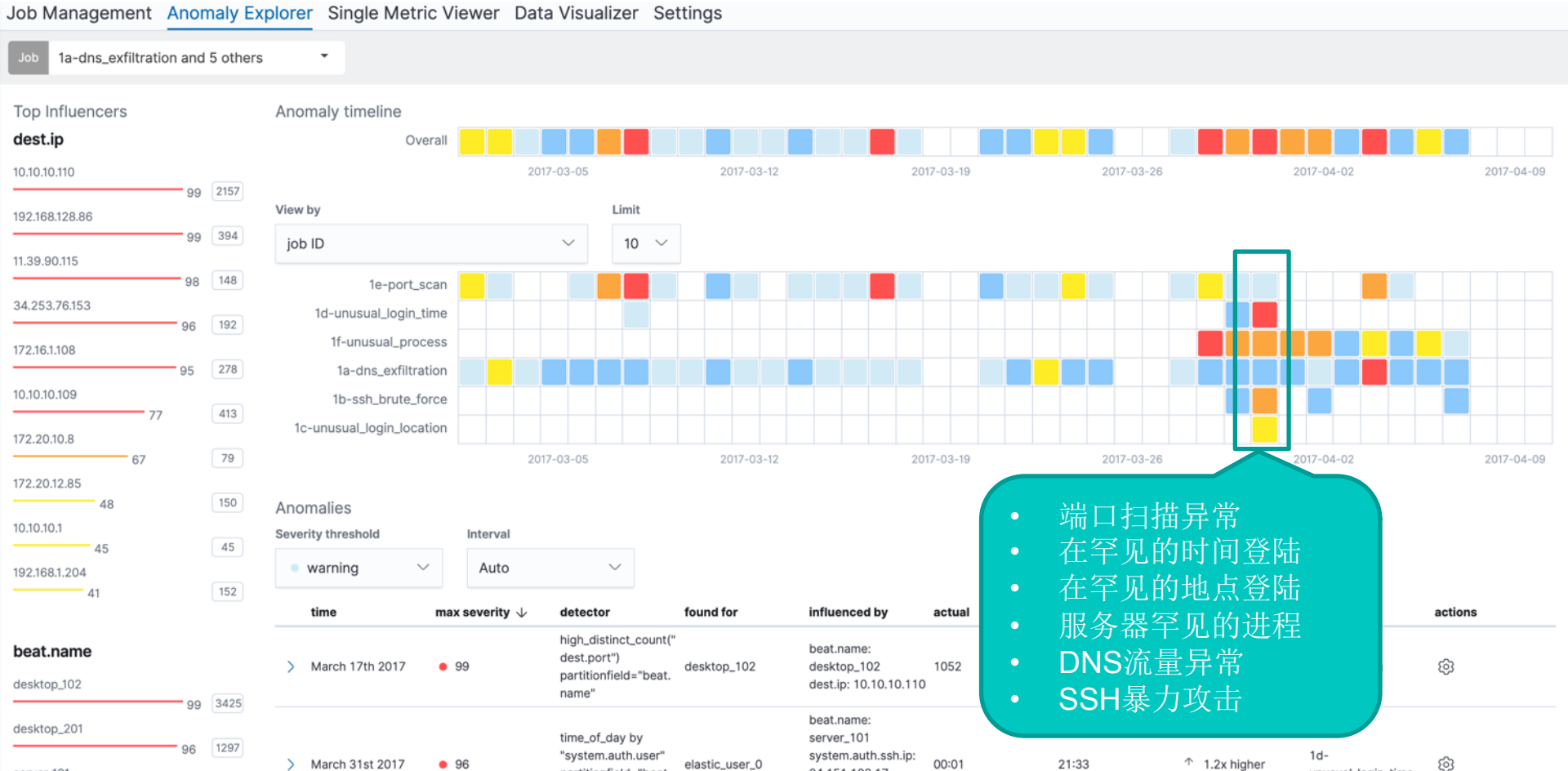
在不通常的时间登陆

在不通常的地点登陆

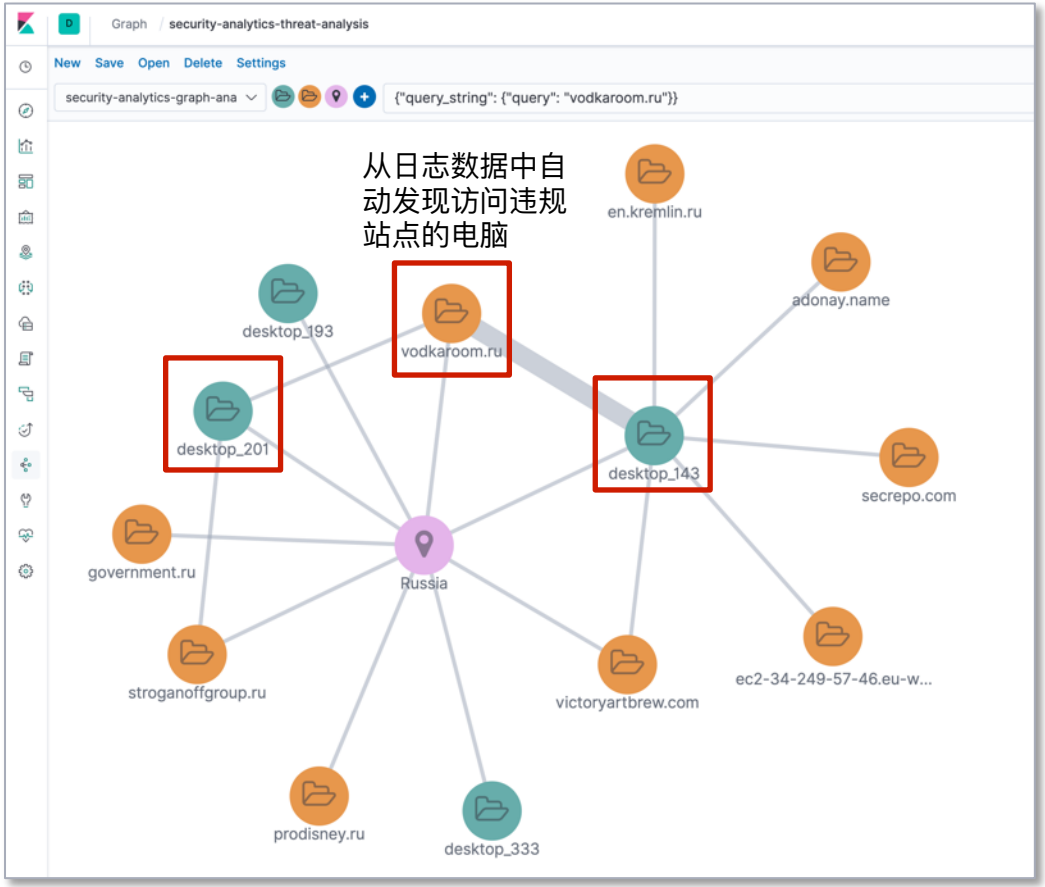
找出稀有的命令行



机器学习- 创建任务检测各种异常联合分析



数据关联分析 – 从大数据中自动发现



- 推荐
- 行为分析
- 威胁分析
- 关联关系

elastic

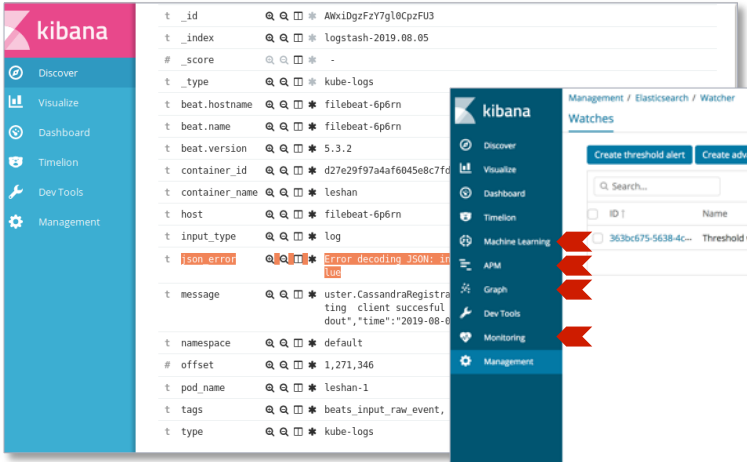
产品快速迭代

2019.3.27　2019.4.10　2019.5.20　2019.6.26　2019.8.1

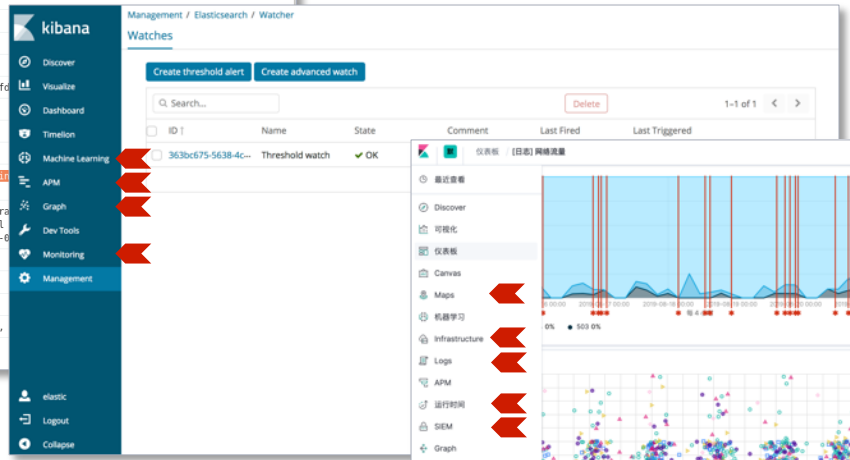
elastic

客户可以享受到更多功能

Kibana 5.5



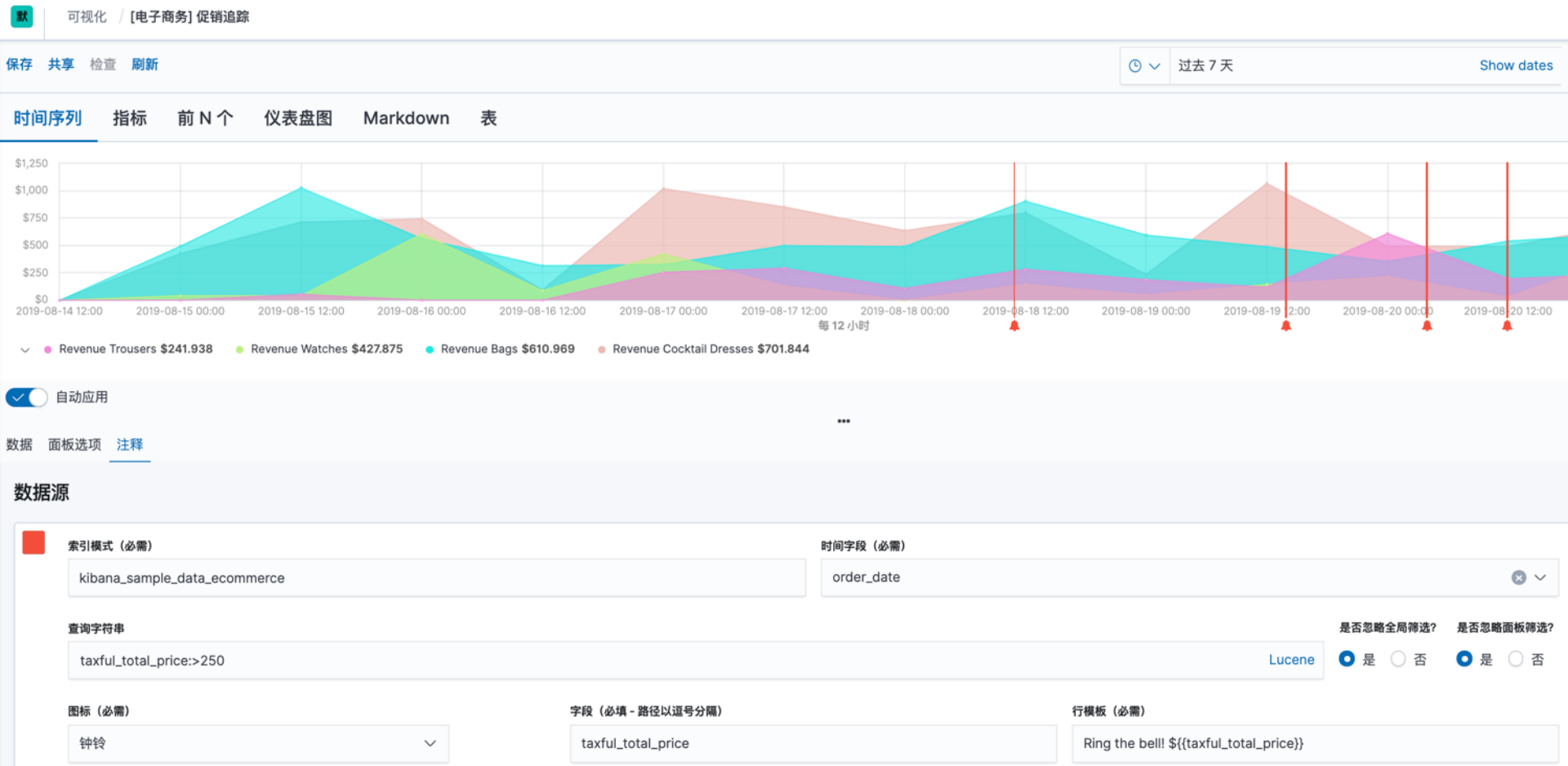
Kibana 6.5



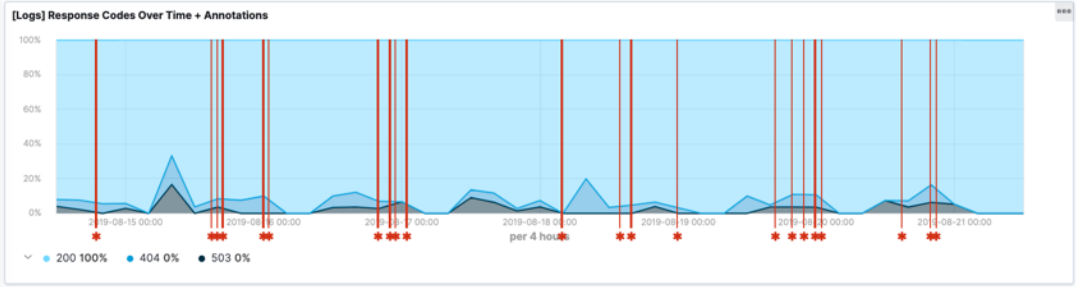
Kibana 7.3

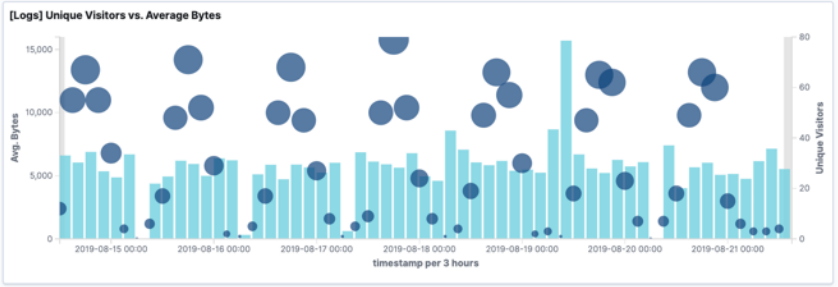
elastic

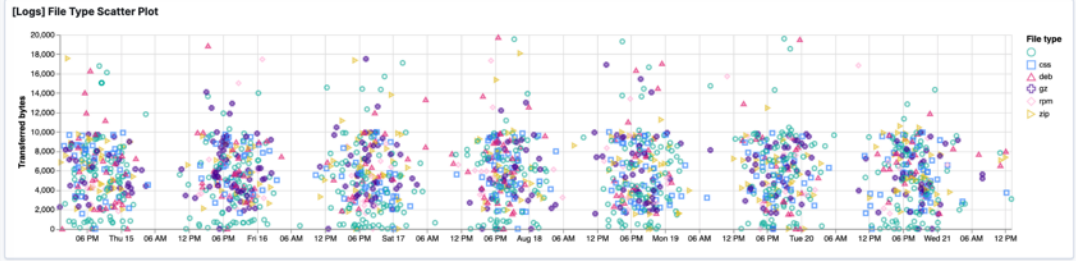
数据展现 - 时序数据分析器



数据展现 – 丰富的图表

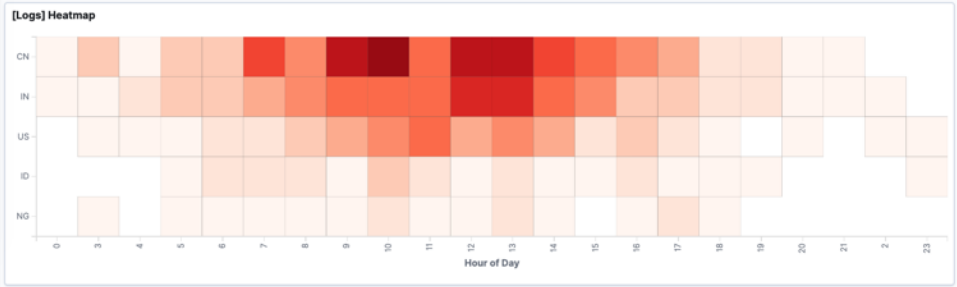


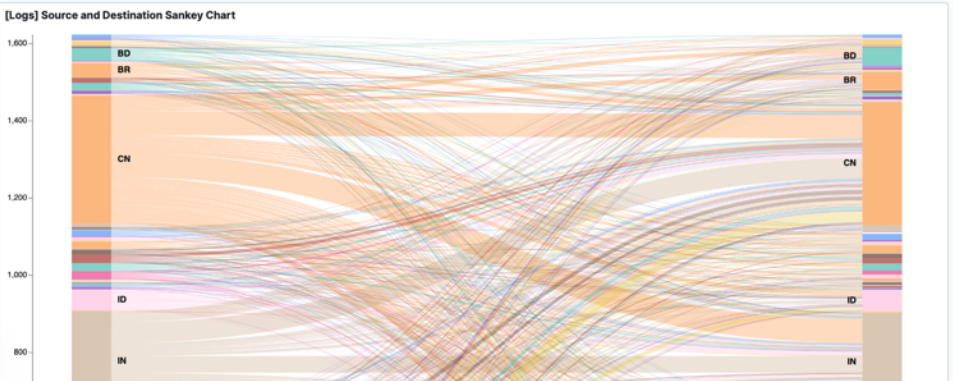




[Logs] Host, Visits and Bytes Table

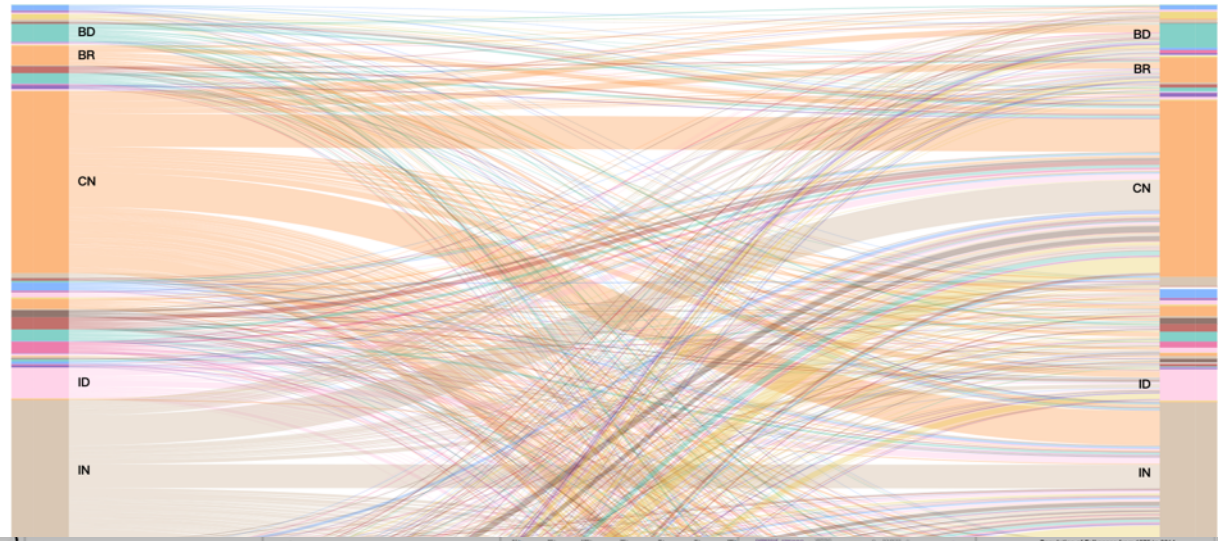
Type	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
	0B	0B	0	0
gz	0B	0B	0	0
css	0B	3.634KB	0	1
zip	0B	7.195KB	0	1
deb	0B	7.793KB	0	1
rpm	0B	0B	0	0



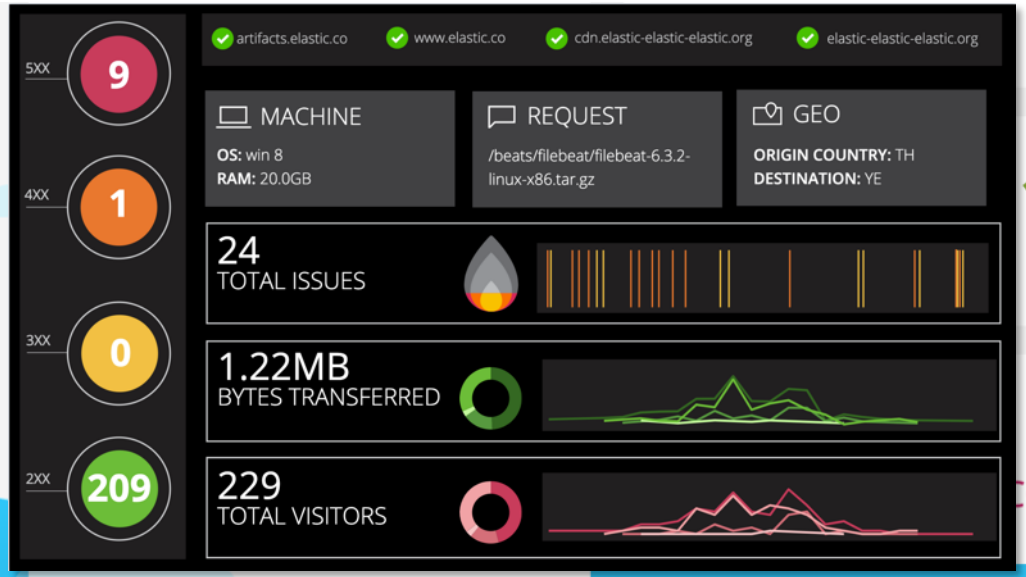


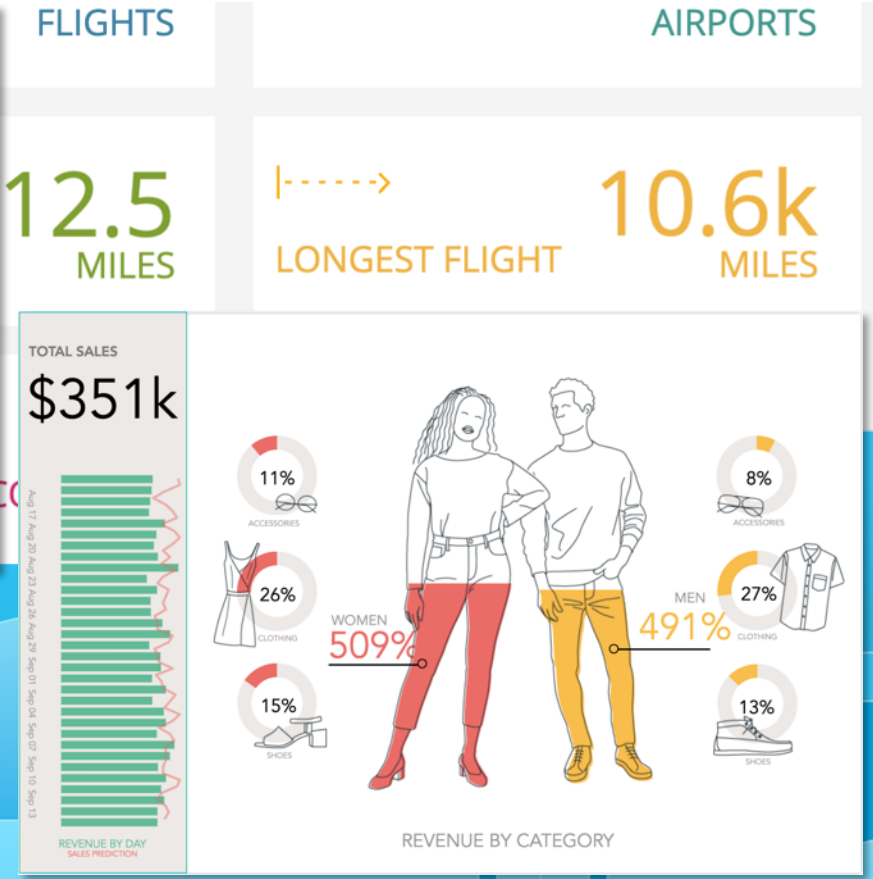
数据展现 – 丰富的开放生态，支持开源Vega图表组件

```
{
  $schema: https://vega.github.io/schema/vega/v3.0.json
  data: [
  {
    // query ES based on the currently selected time range and
       filter string
    name: rawData
    url: {
      %context%: true
      %timefield%: timestamp
      index: kibana_sample_data_logs
      body: {
        size: 0
        aggs: {
          table: {
            composite: {
              size: 10000
              sources: [
                {
                  stk1: {
                    terms: {field: "geo.src"}
                  }
                }
                {
                  stk2: {
                    terms: {field: "geo.dest"}
                  }
```

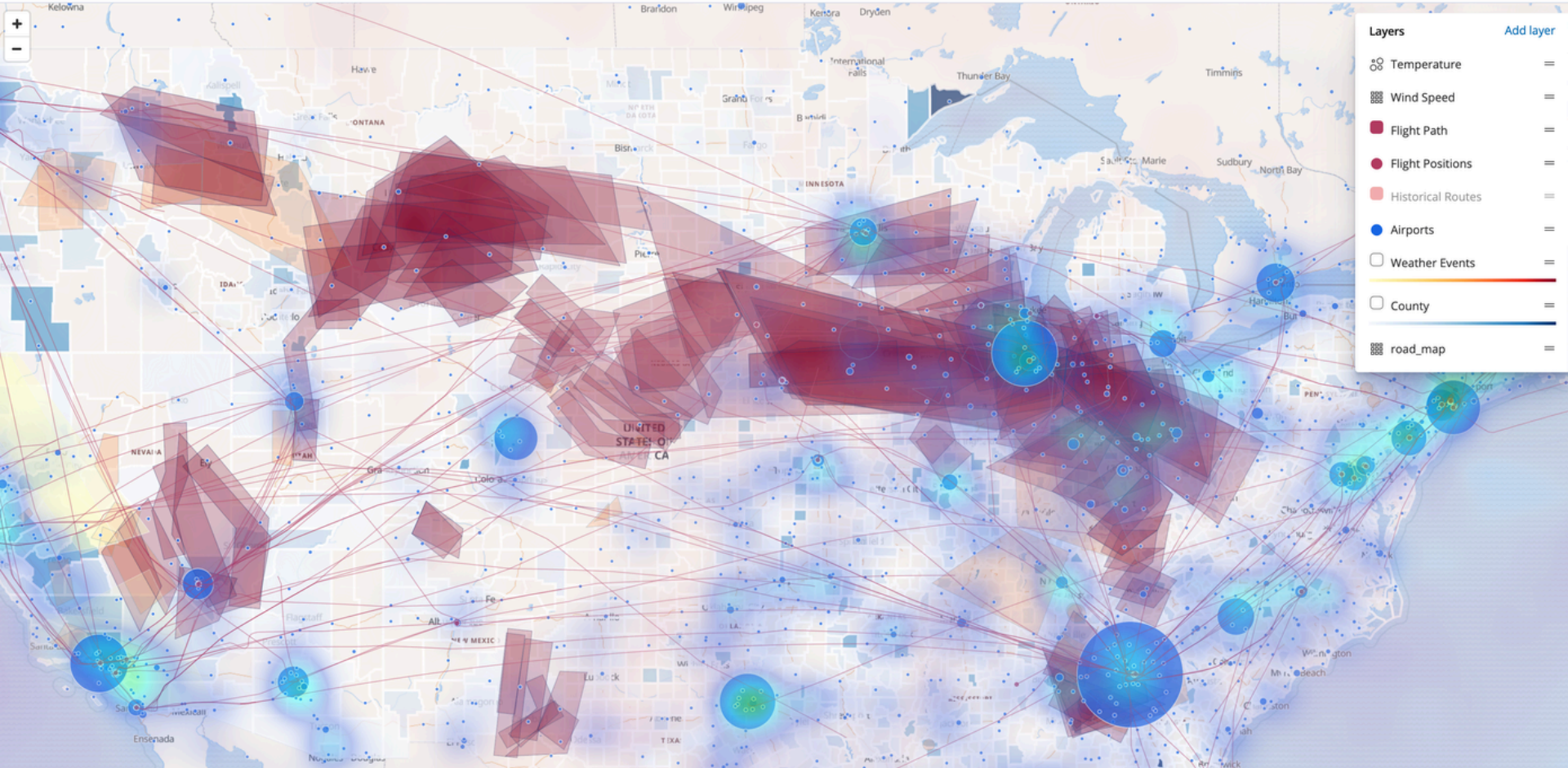


数据展现 – 像PPT一样的全动态大屏报表

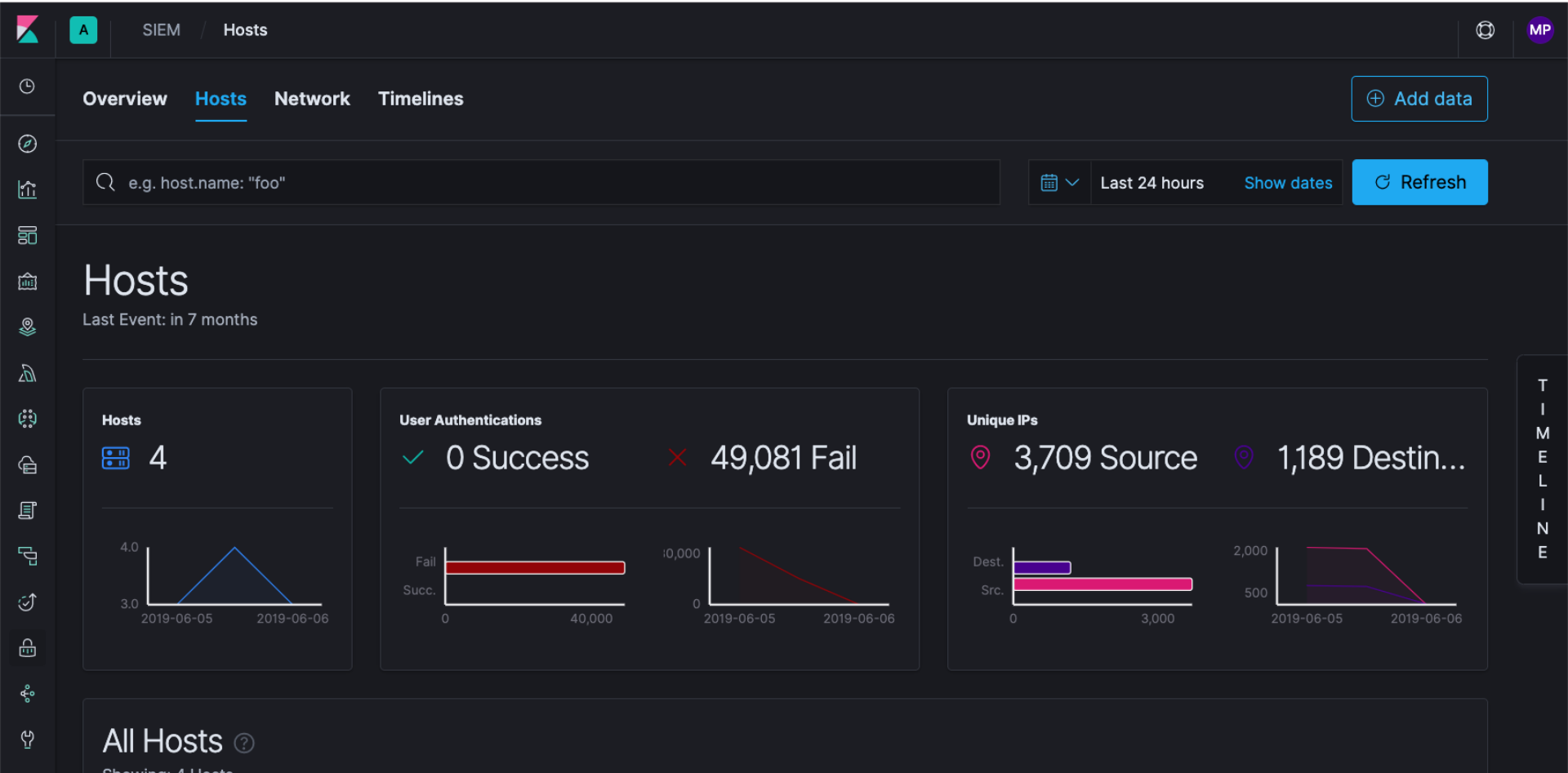




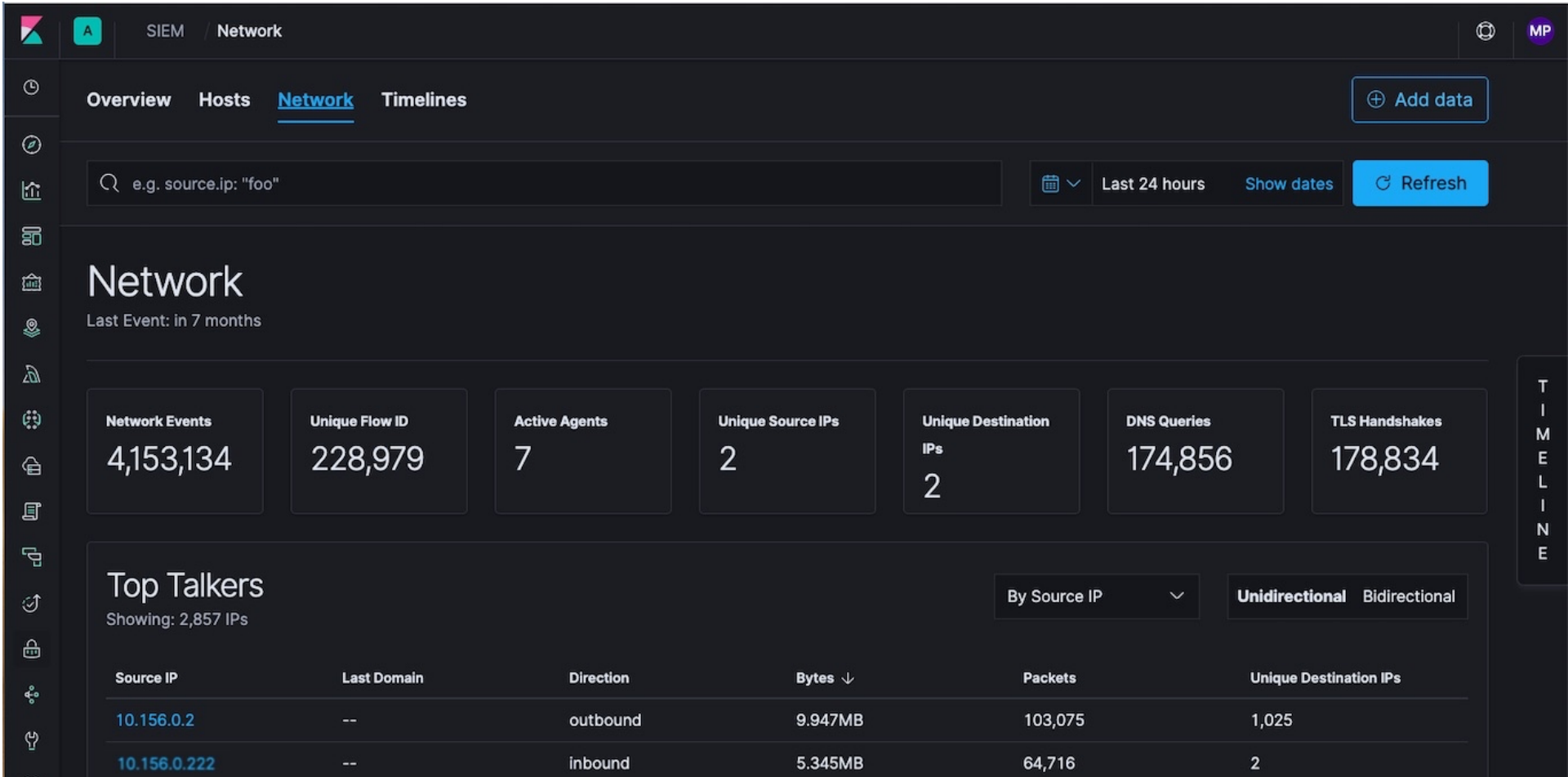
数据展现 – 在地图上分析数据

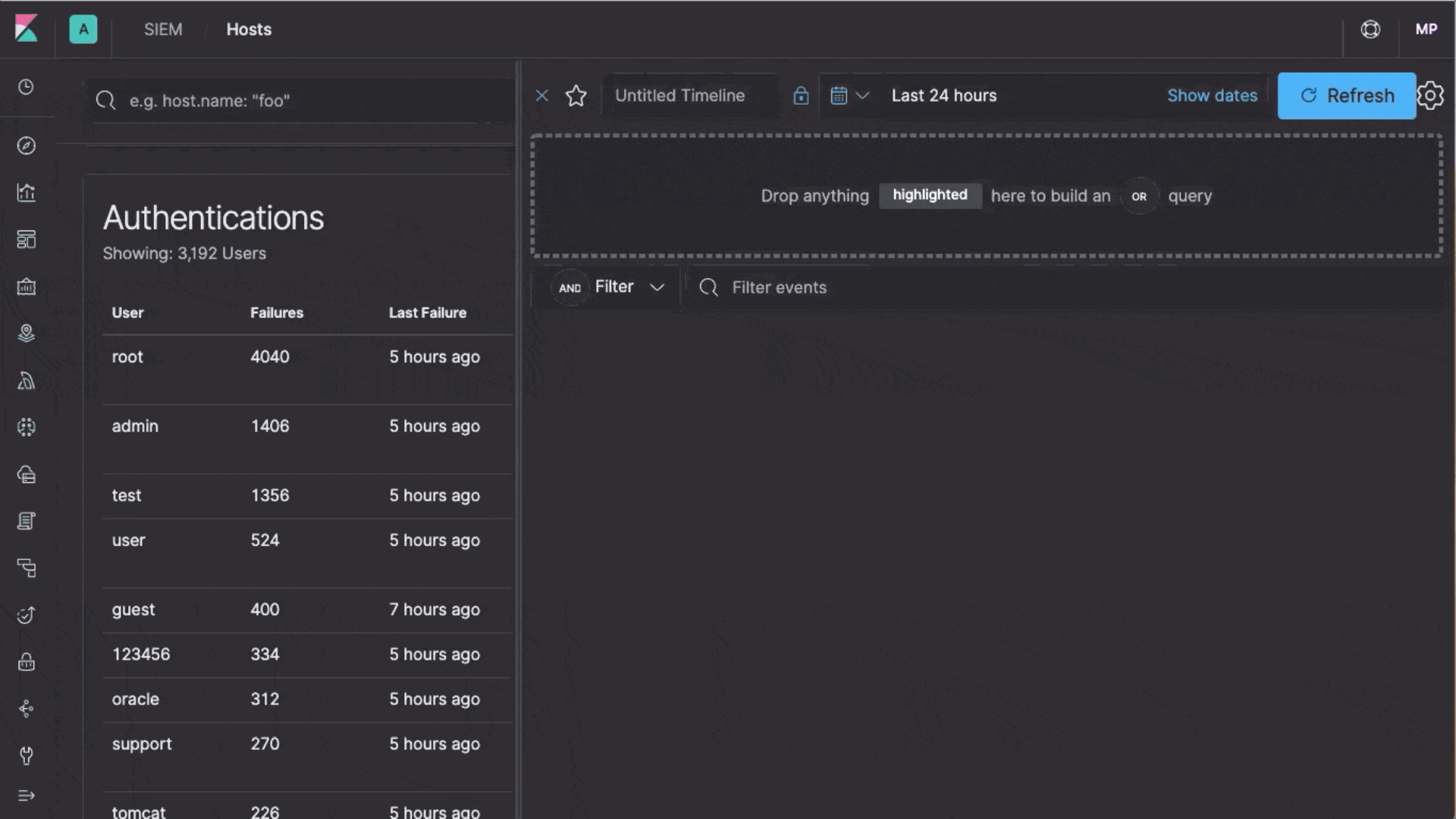


SIEM APP – 主机安全事件分析



SIEM APP – 网络安全事件分析




A
SIEM
Hosts
MP
e.g. host.name: "foo"
Untitled Timeline
Last 24 hours
Show dates
Refresh
Drop anything
highlighted
here to build an
OR
query
AND
Filter
Filter events
Authentications
Showing: 3,192 Users
User
Failures
Last Failure
root
4040
5 hours ago
admin
1406
5 hours ago
test
1356
5 hours ago
user
524
5 hours ago
guest
400
7 hours ago
123456
334
5 hours ago
oracle
312
5 hours ago
support
270
5 hours ago
tomcat
226
5 hours ago

ECS – Elastic Common Schema

优势

在不同的多个数据源中做关联分析
能够复用分析内容
能够复用Elastic所提供的内容

状态

github.com/elastic/ecs
内部多个工作组进行验证
非常欢迎来自社区的反馈!

ECS Revision: 0.992 Group 1 Fields: 3 Group 2 Fields: 81

Group 1 (Must be populated)

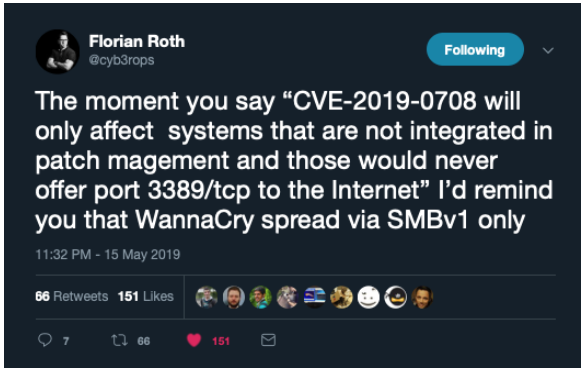
@timestamp
ecs_version
message

Group 2 (Must be populated to the max extent practical where event message contains relevant fields.)

Event	Device	Host	Agent	Network	Source	Destination	Service	Resource
event.category	device.mac	host.mac	agent.id	network.protocol	source.mac	destination.mac	service.id	resource.type
event.type	device.timezone_offset	host.timezone_offset	agent.name	network.forwarded_ip	source.ip	destination.ip	service.name	resource.id
event.data_source_id	device.ip	host.ip	agent.version	network.inbound_bytes	source.hostname	destination.hostname	service.version	resource.file_name
event.module	device.network_interface	host.network_interface		network.inbound_packets	source.domain	destination.domain	service.type	resource.uri
event.organization_name	device.hostname	host.hostname		network.outbound_bytes	source.port	destination.subdomain	service.state	resource.url
event.organization_id	device.type	host.id		network.outbound_packets		destination.port	service.query	resource.path
event.id	device.vendor	host.type		network.total_bytes			service.response_code	resource.version
event.raw	device.product	host.sub_type		network.total_packets				resource.hash_value
event.hash	device.version	host.operating_system		network.direction				resource.hash_type
event.tags	device.serial_number	host.operating_system_version						
event.labels	device.action	host.provider						
event.duration	device.rule_set	host.availability_zone						
event.severity	device.event_id	host.region						
event.risk_score								

安全分析实例

[Proactive detection content: CVE-2019–0708 vs MITRE ATT&CK, Sigma, Elastic and ArcSight]



elastic

规则来拯救

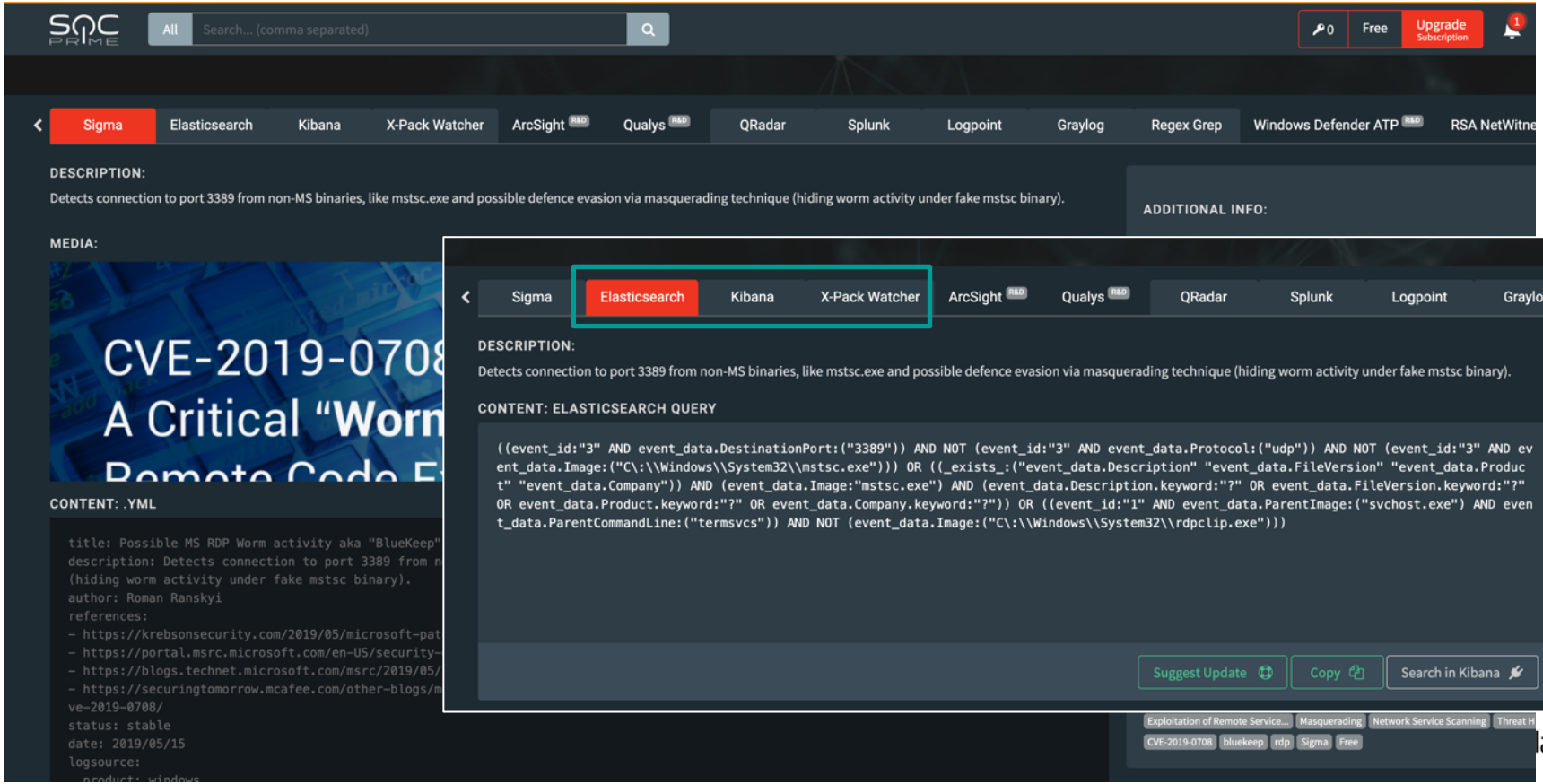
```
title: Suspicious Outbound RDP Connections
status: experimental
description: Detects Non-Standard Tools Connecting to TCP port 3389 indicating possible lateral movement
references:
    - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
author: Markus Neis - Swisscom
date: 2019/05/15
tags:
    - attack.lateral_movement
    - attack.t1210
logsource:
    product: windows
    service: sysmon
detection:
    selection:
        EventID: 3
        DestinationPort: 3389
    filter:
        Image:
            - '*\mstsc.exe'
            - '*\RTSApp.exe'
            - '*\RTS2App.exe'
            - '*\RDCMan.exe'
            - '*\ws_TunnelService.exe'
            - '*\RSSensor.exe'
            - '*\RemoteDesktopManagerFree.exe'
            - '*\RemoteDesktopManager.exe'
            - '*\RemoteDesktopManager64.exe'
            - '*\mRemoteNG.exe'
            - '*\mRemote.exe'
            - '*\Terminals.exe'
            - '*\spiceworks-finder.exe'
            - '*\FSDiscovery.exe'
            - '*\FSAssessment.exe'
            - '*\MobaRTE.exe'
            - '*\chrome.exe'
    condition: selection and not filter
falsepositives:
    - Other Remote Desktop RDP tools
level: high
```

Sigma #1 by Markus Neis
https://github.com/Neo23x0/sigma/blob/master/rules/windows/sysmon/sysmon_susp_rdp.yml
Lateral Movement; T1210;
log sources: microsoft sysmon.
https://attack.mitre.org/techniques/T1210/

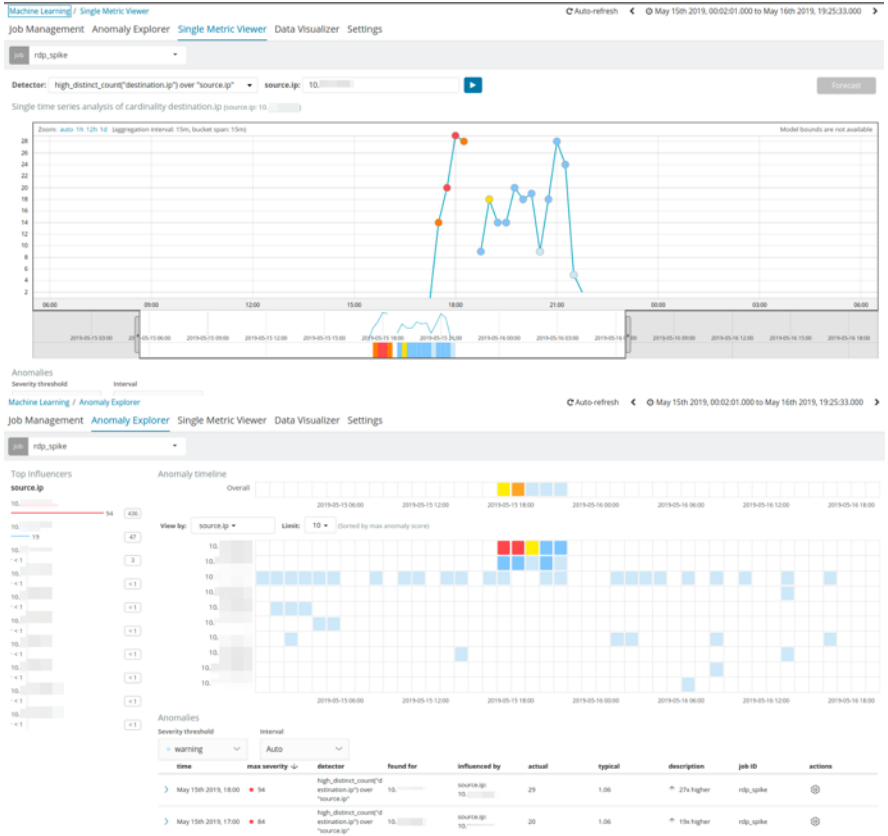
Sigma #2 by Roman Ranskyi
https://tdm.socprime.com/tdm/info/2159/
Lateral Movement, Defense Evasion, Discovery; T1210, T1036, T1046;
log sources: microsoft sysmon.
https://attack.mitre.org/techniques/T1036/

elastic

Elastic也支持传统的规则检测



Elastic机器学习主动防御未知威胁



对RDP连接，对每一个source ip，统计不同的destination ip个数，根据它的历史数据来检测异常

Example Elasticsearch Index Patterns:
ecs-netflow*

Example Elasticsearch Query:
“query”: {“term”: {“destination.port”: {“value”: 3389",”boost”: 1}}}

Machine Learning Analysis / Detector Config:
Detector(s): high_distinct_count(destination.ip) over source.ip
Bucketspan: 15m
Influencer(s): source.ip

elastic

Elastic, ArcSight or Sigma?

If we just use ATT&CK as a benchmark, Elastic is the winner being 1 technique ahead. The main advantage of the Elastic stack is its ability to combine both Machine Learning and modern Threat Hunting queries based on Sigma. Remember that the re-factor of Sigma rules to real-time correlation queries does not find Masquerading / T1036 on ArcSight.

Andrii Bezverkhyi

持续投资
安全分析领域

WHY ENDGAME?

Reimagine Endpoint Protection

Endpoint protection platform replacing AV, NGAV, anti-exploit prevention, IOC search, and IR reducing cost and complexity of your endpoint environment.

WATCH NOW

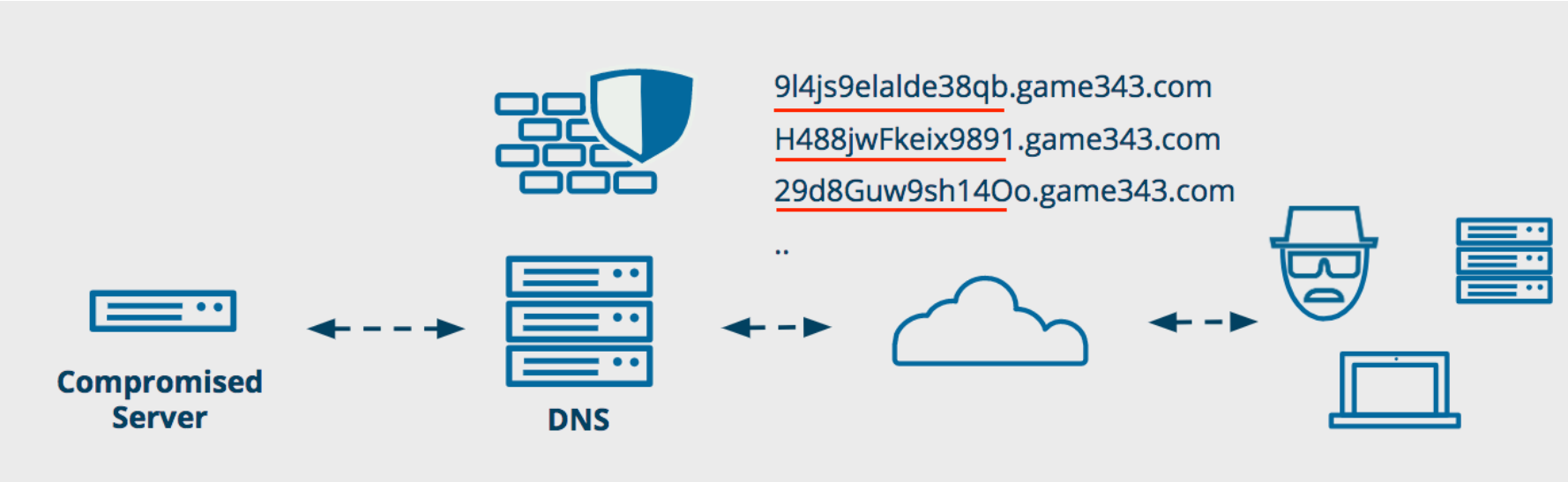
WHY ENDGAME

perched

Education Consulting Support Blog Contact

DEMO

通过DNS隧道进行数据渗透



elastic

部署机器学习任务全方位监控

网络数据机器学习任务	主机日志机器学习任务
dns exfiltration	ssh brute force
port scan	unusual login location
	unusual login time
	unusual process

elastic
中文社区

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