



Elastic 安全分析领域应用

杰瑞朱 = Jerry 朱杰
Elastic 架构师

挑战 —

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

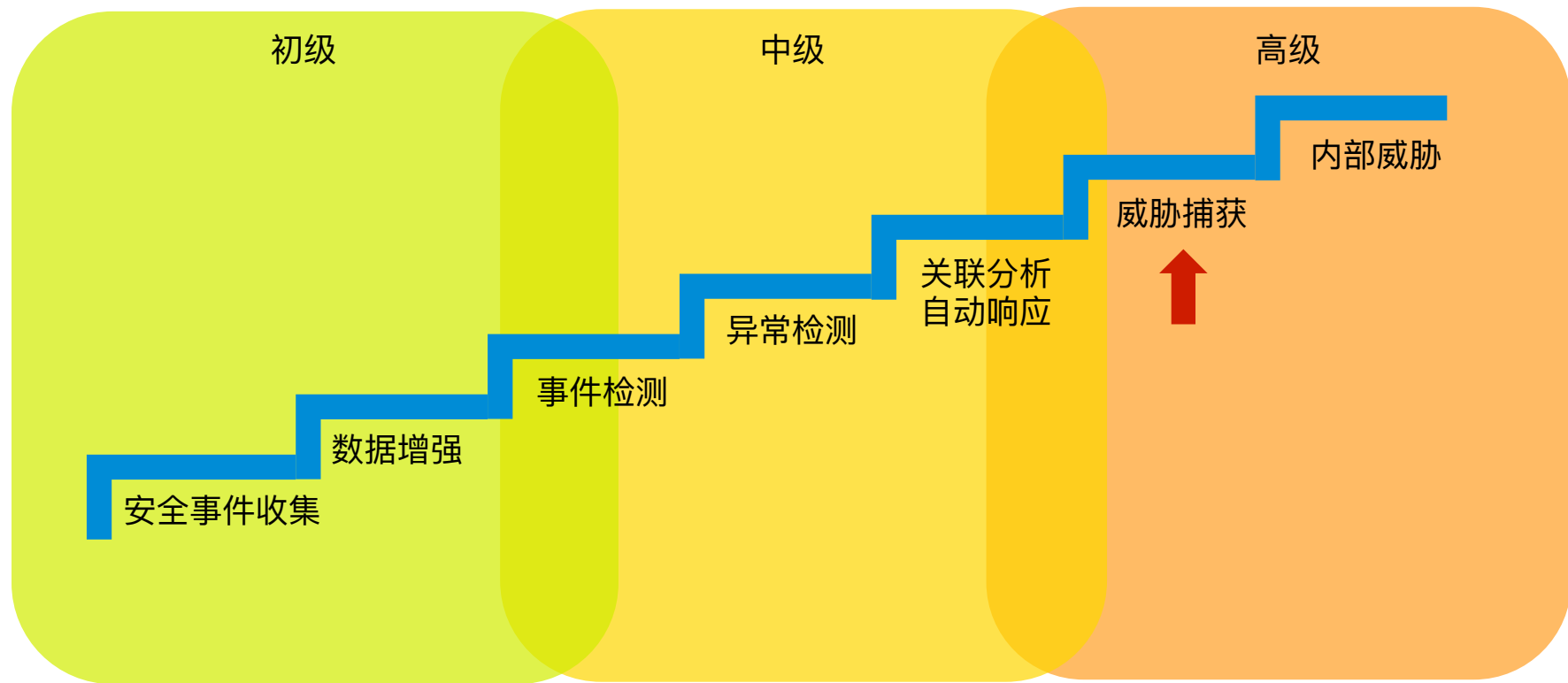
挑战 三

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

日志、指标采集 Beats生态

libbeat



30+ 插件

FILEBEAT
日志文件



WINLOGBEAT
Window日志



40+ 插件

METRICBEAT
指标数据



HEARTBEAT
服务可用性监控



PACKETBEAT
网络数据



AUDITBEAT
Linux审核框架事件



FUNCTIONBEAT
云服务器监控

httpbeat

apachebeat

nginxbeat

pingbeat

execbeat

dockerbeat

elasticbeat

70+
社区制造

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

开放生态 第三方重磅工具



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

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



apm-high-load-opbeans

Send an alert when a specific condition is met. This will run every 10 seconds.

Name

apm-high-load-opbeans

Indices to query

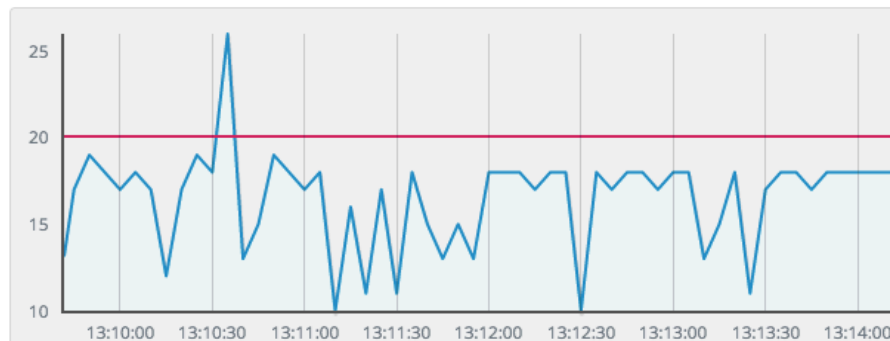
apm-*transaction-*

Use * to broaden your search query

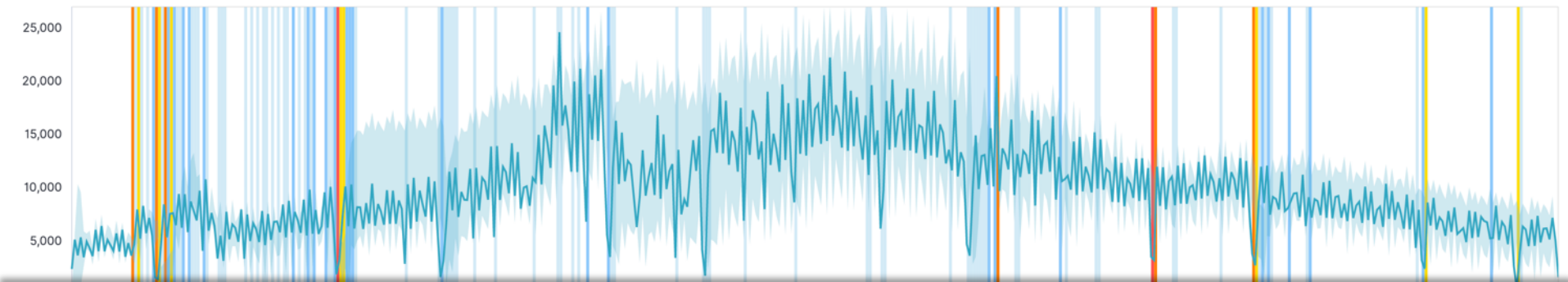
Matching the following condition

WHEN count() GROUPED OVER top 10 'context.service.name' IS ABOVE 20 FOR THE LAST 70

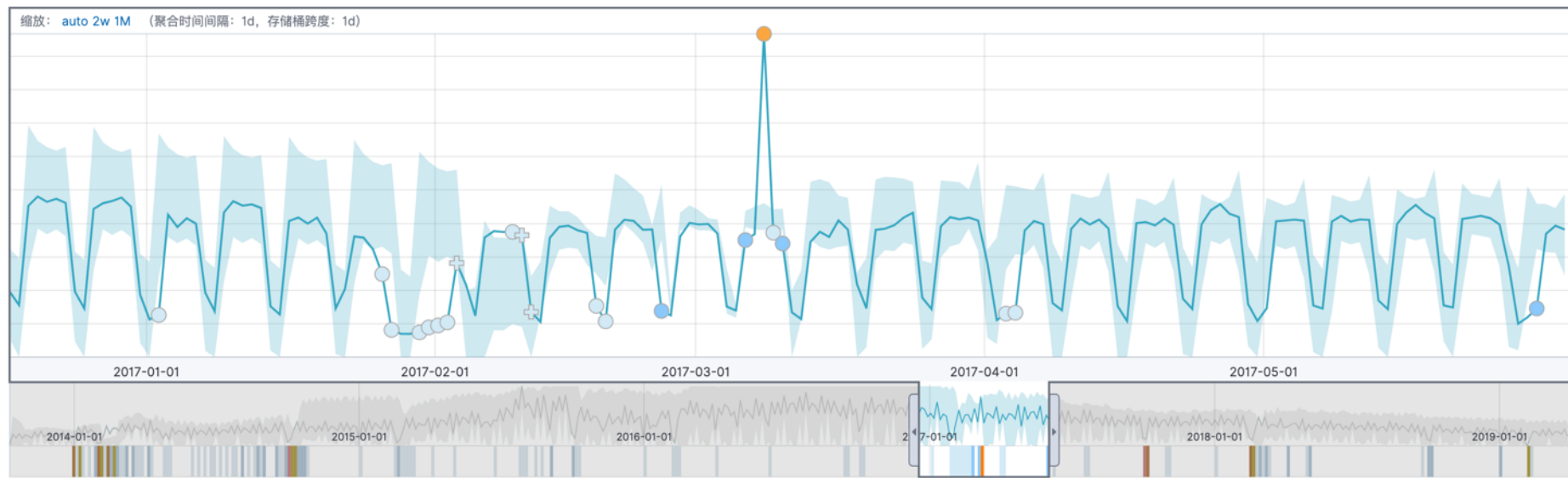
context.service.name (1 of 4): opbeans-node



机器学习- 更加智能的检测和告警



☒ 显示模型边界 ☒ 注释



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

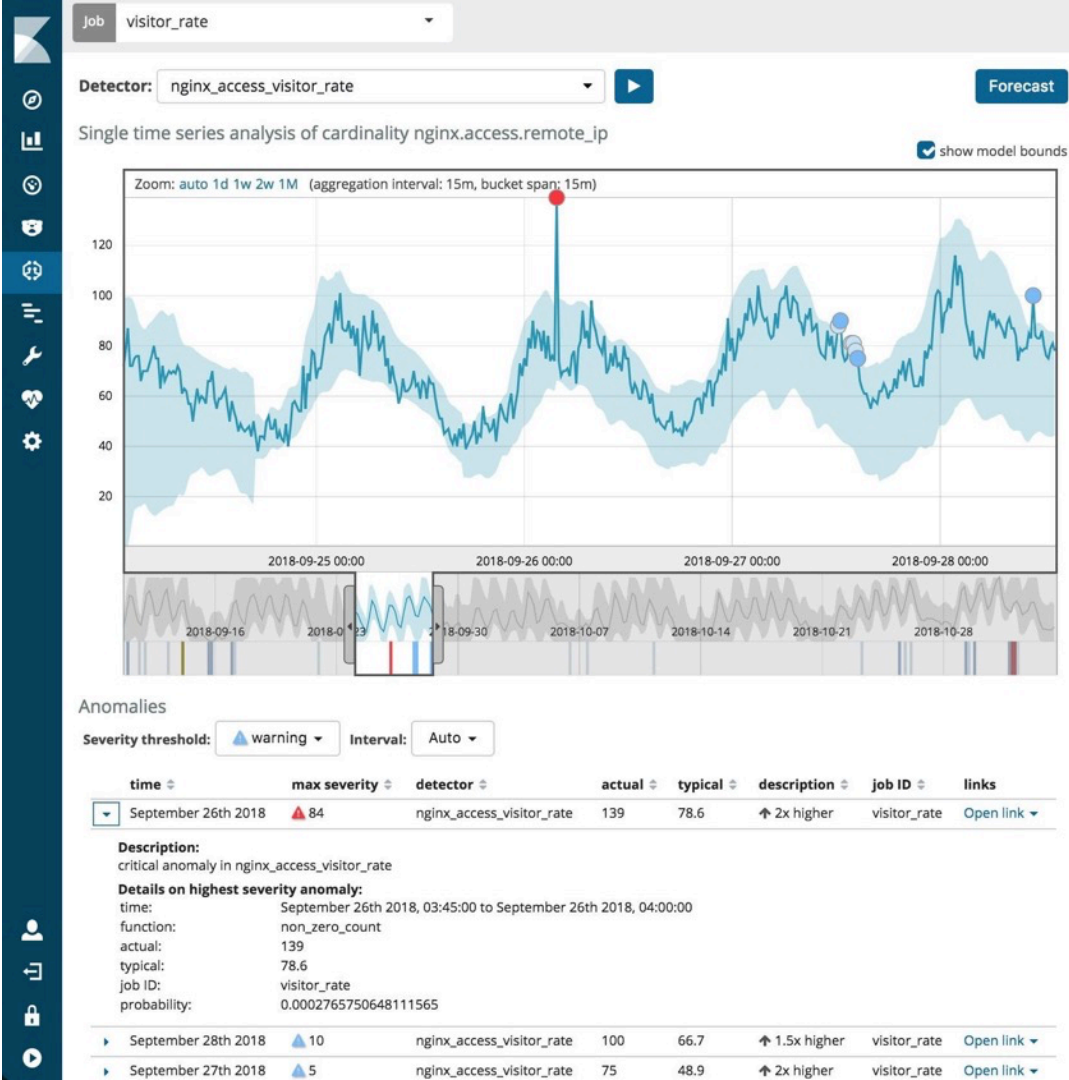
预测

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

Job Management [Anomaly Explorer](#) Single Metric Viewer Data Visualizer Settings

Job 1a-dns_exfiltration and 5 others

Top Influencers

dest.ip

10.10.10.110 99 2157

192.168.128.86 99 394

11.39.90.115 98 148

34.253.76.153 96 192

172.16.1.108 95 278

10.10.10.109 77 413

172.20.10.8 67 79

172.20.12.85 48 150

10.10.10.1 45 45

192.168.1.204 41 152

beat.name

desktop_102 99 3425

desktop_201 96 1297

Anomaly timeline

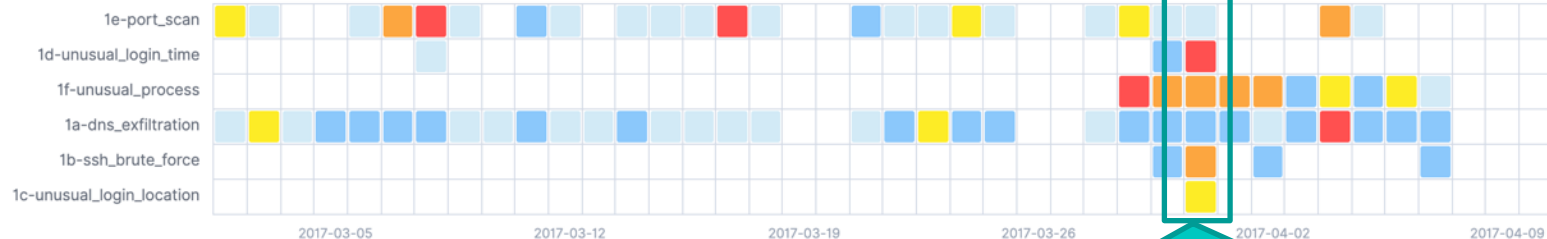


View by

job ID

Limit

10



Anomalies

Severity threshold

warning

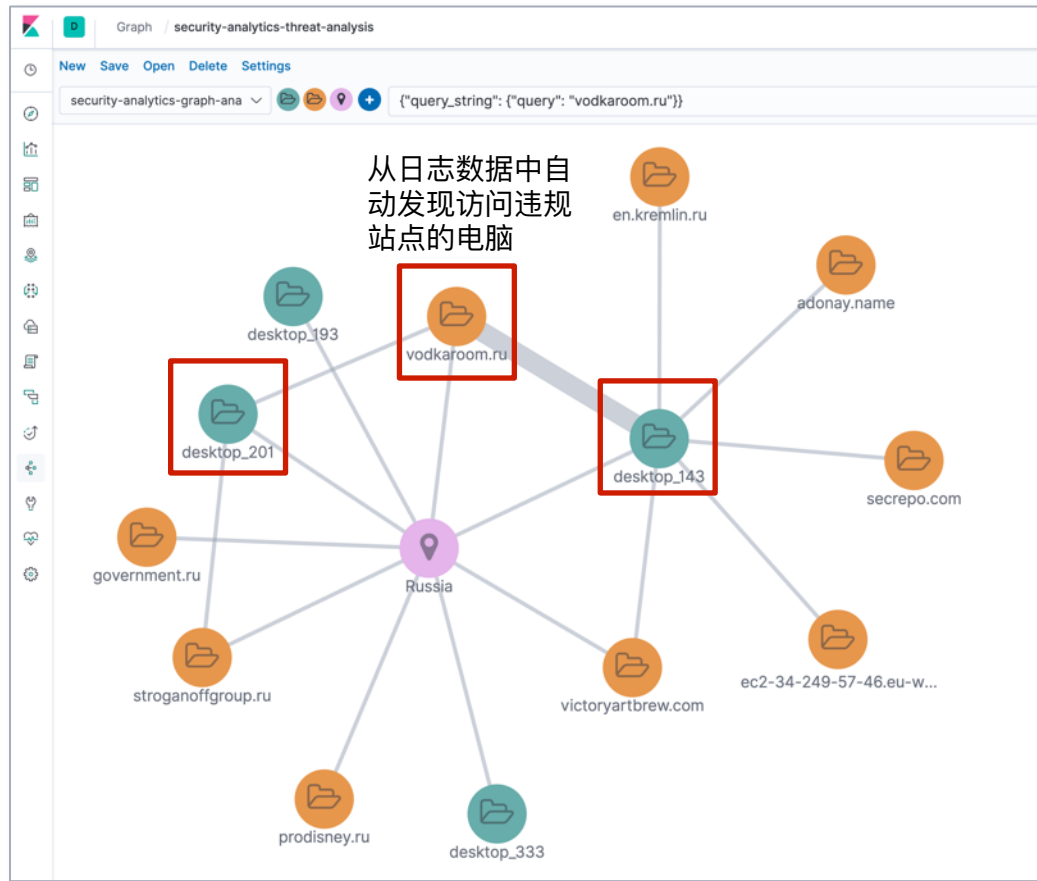
Interval

Auto

time	max severity ↓	detector	found for	influenced by	actual	actions
> March 17th 2017	99	high_distinct_count("dest.port") partitionfield="beat.name"	desktop_102	beat.name: desktop_102 dest.ip: 10.10.10.110	1052	
> March 31st 2017	96	time_of_day by "system.auth.user"	elastic_user_0	beat.name: server_101 system.auth.ssh.ip: 24.154.102.17	00:01 21:33 ↑ 1.2x higher	

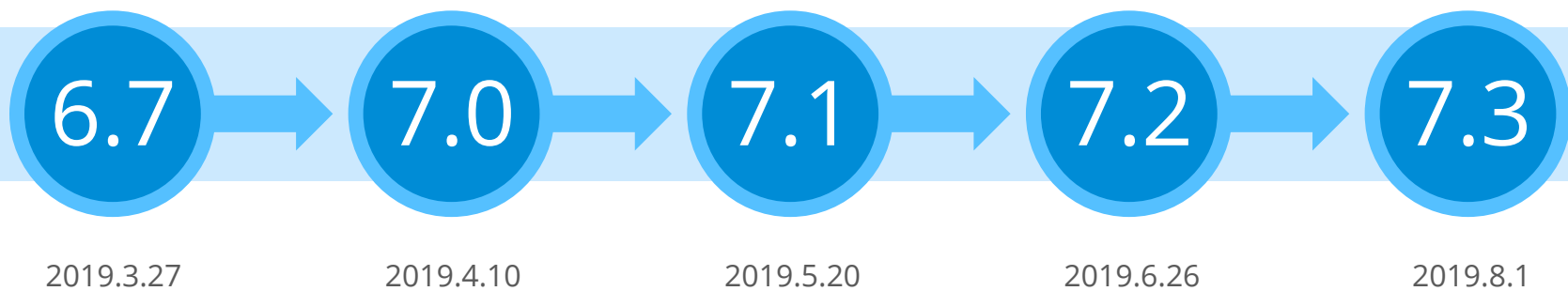
- 端口扫描异常
- 在罕见的时间登陆
- 在罕见的地点登陆
- 服务器罕见的进程
- DNS流量异常
- SSH暴力攻击

数据关联分析 - 从大数据中自动发现



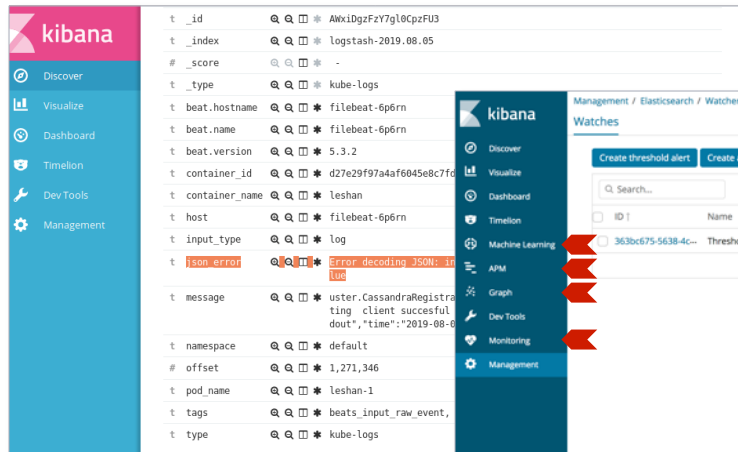
- 推荐
- 行为分析
- 威胁分析
- 关联关系

产品快速迭代

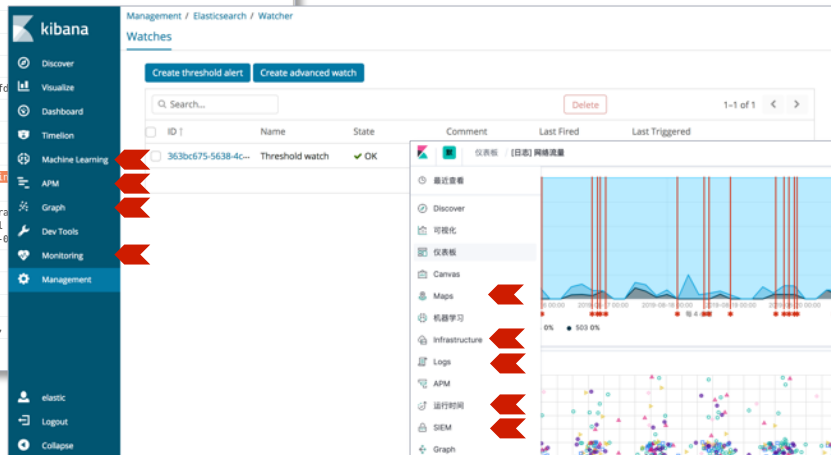


客户可以享受到更多功能

Kibana 5.5



Kibana 6.5



Kibana 7.3



数据展现 - 时序数据分析器

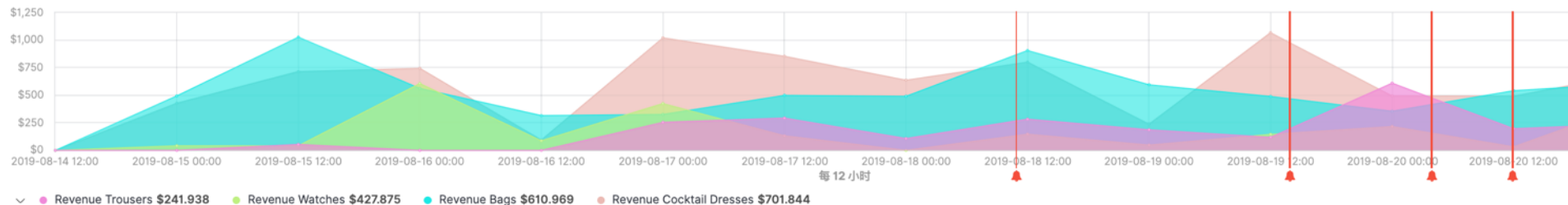
可视化 / [电子商务] 促销追踪

保存 共享 检查 刷新

过去 7 天

Show dates

时间序列 指标 前 N 个 仪表盘图 Markdown 表



自动应用

数据 面板选项 注释

数据源

索引模式 (必需)

kibana_sample_data_ecommerce

时间字段 (必需)

order_date

查询字符串

taxful_total_price:>250

Lucene

是否忽略全局筛选?

☒ 是 ☐ 否

是否忽略面板筛选?

☒ 是 ☐ 否

图标 (必需)

钟铃

字段 (必填 - 路径以逗号分隔)

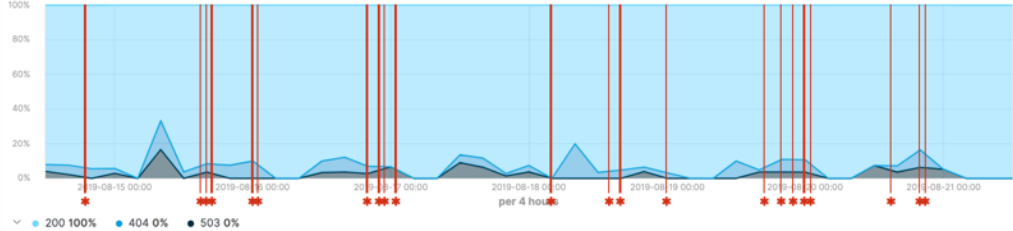
taxful_total_price

行模板 (必需)

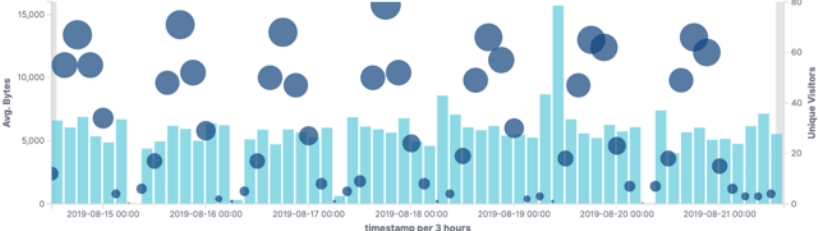
Ring the bell! \${{taxful_total_price}}

数据展现 - 丰富的图表

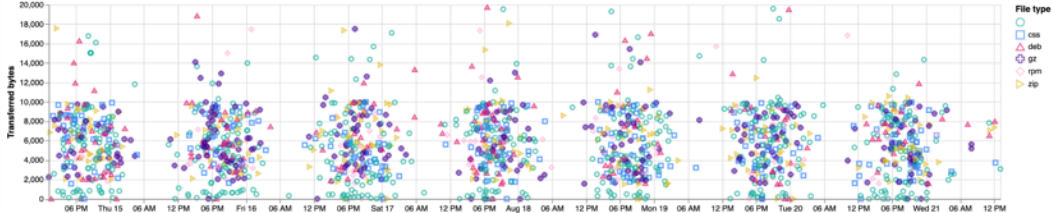
[Logs] Response Codes Over Time + Annotations



[Logs] Unique Visitors vs. Average Bytes



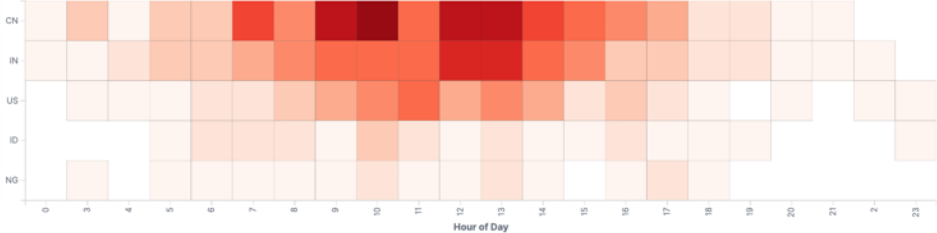
[Logs] File Type Scatter Plot



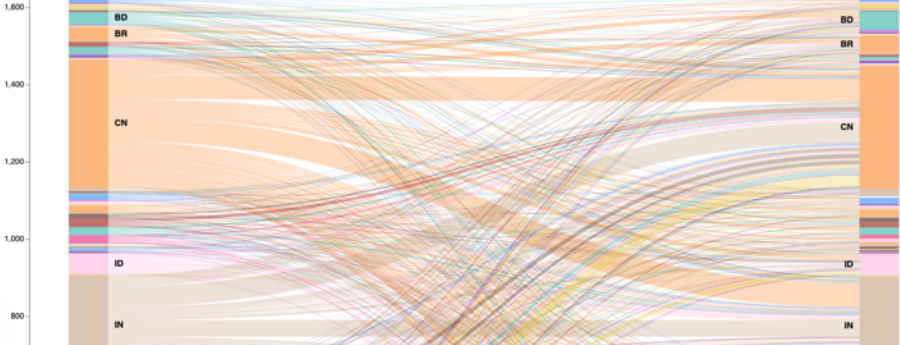
[Logs] Host, Visits and Bytes Table

Type ↑	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
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 ↓

[Logs] Heatmap



[Logs] Source and Destination Sankey Chart

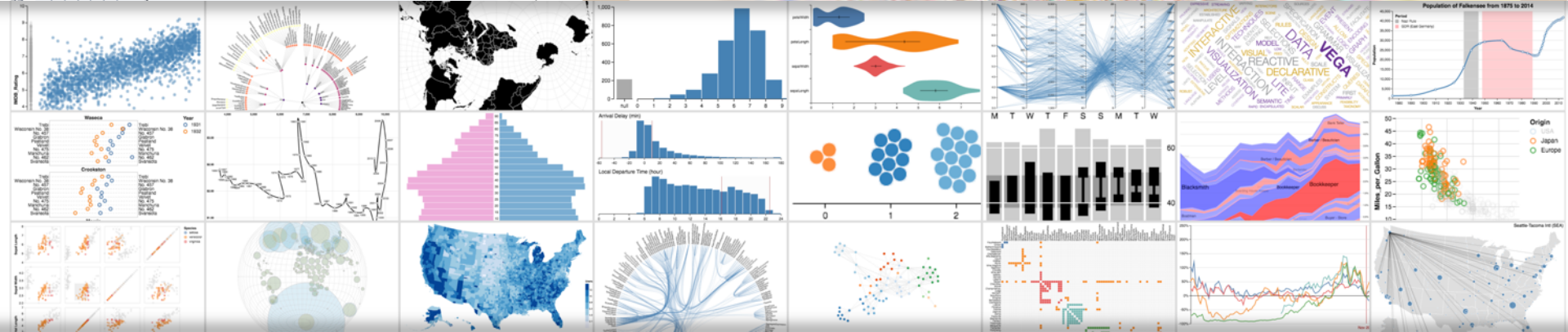
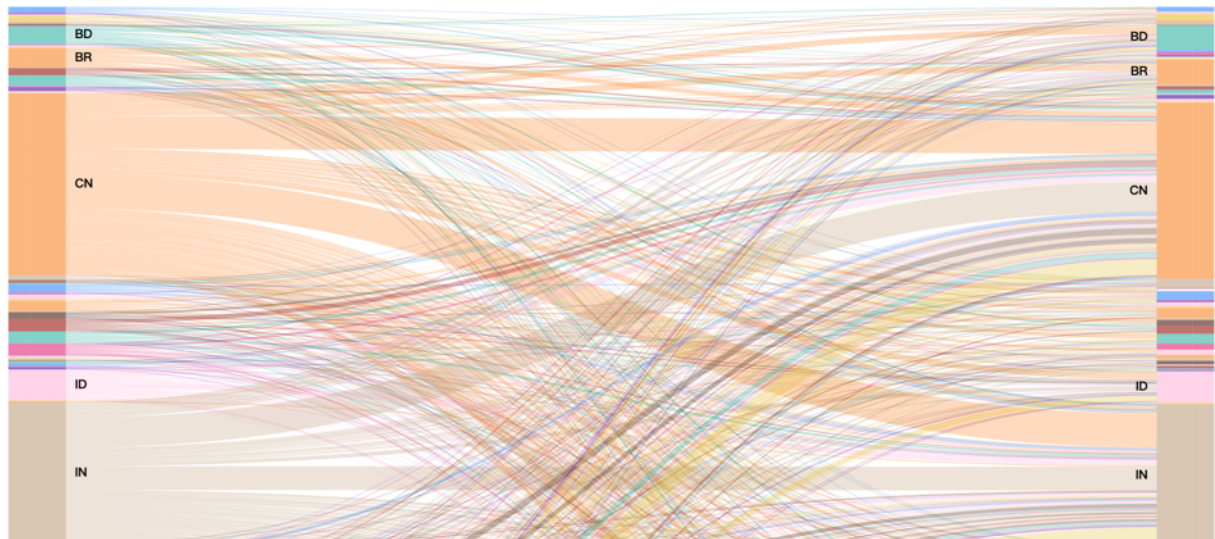


[Logs] Total Requests and Bytes

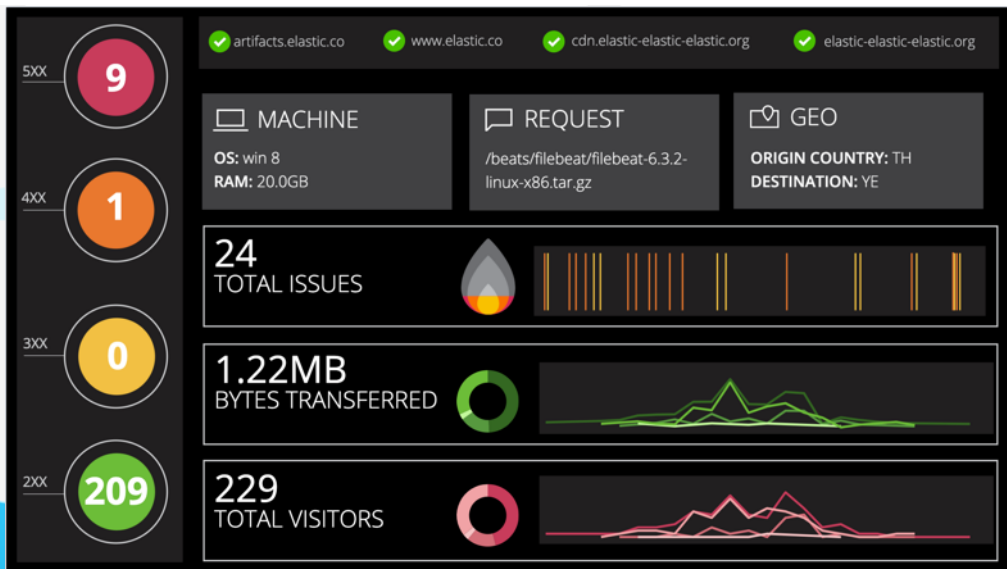


数据展现 - 丰富的开放生态，支持开源Vega图表组件

```
1 {  
2   $schema: https://vega.github.io/schema/vega/v3.0.json  
3   data: [  
4     {  
5       // query ES based on the currently selected time range and  
6       // filter string  
7       name: rawData  
8       url: {  
9         %context%: true  
10        %timefield%: timestamp  
11        index: kibana_sample_data_logs  
12        body: {  
13          size: 0  
14          aggs: {  
15            table: {  
16              composite: {  
17                size: 10000  
18                sources: [  
19                  {  
20                    stk1: {  
21                      terms: {field: "geo.src"}  
22                    }  
23                  }  
24                  {  
25                    stk2: {  
26                      terms: {field: "geo.dest"}  
27                    }  
28                  }  
29                ]  
30              }  
31            }  
32          }  
33        }  
34      }  
35    ]  
36  }
```



数据展现 - 像PPT一样的全动态大屏报表



19
MINS

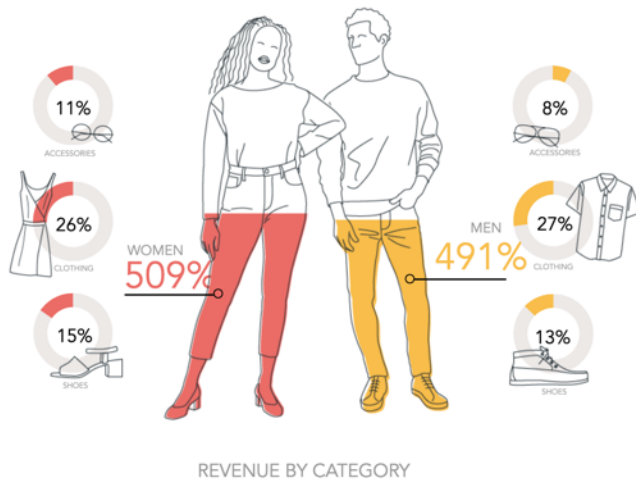
FLIGHTS

12.5
MILES

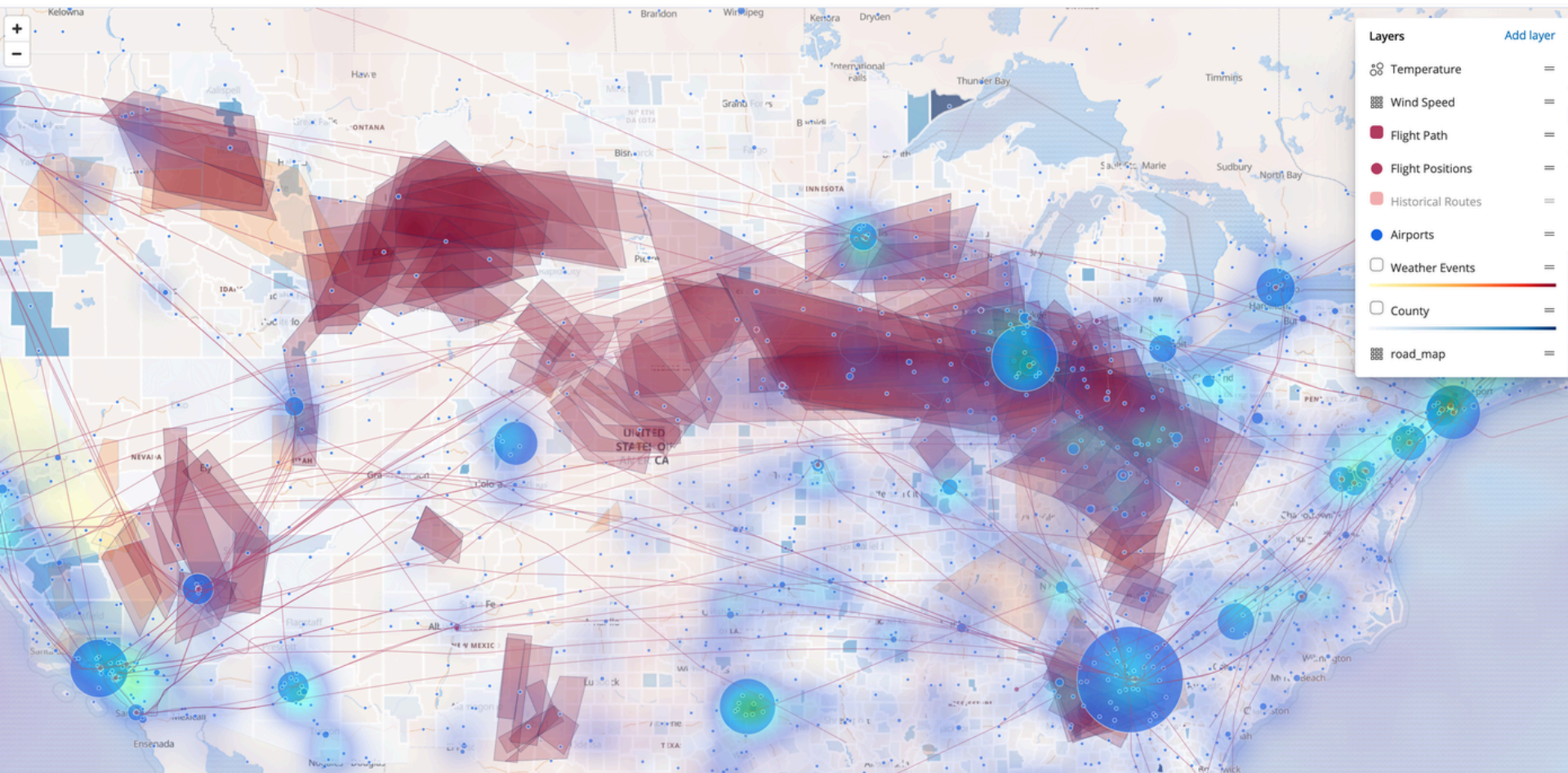
AIRPORTS

10.6k
MILES

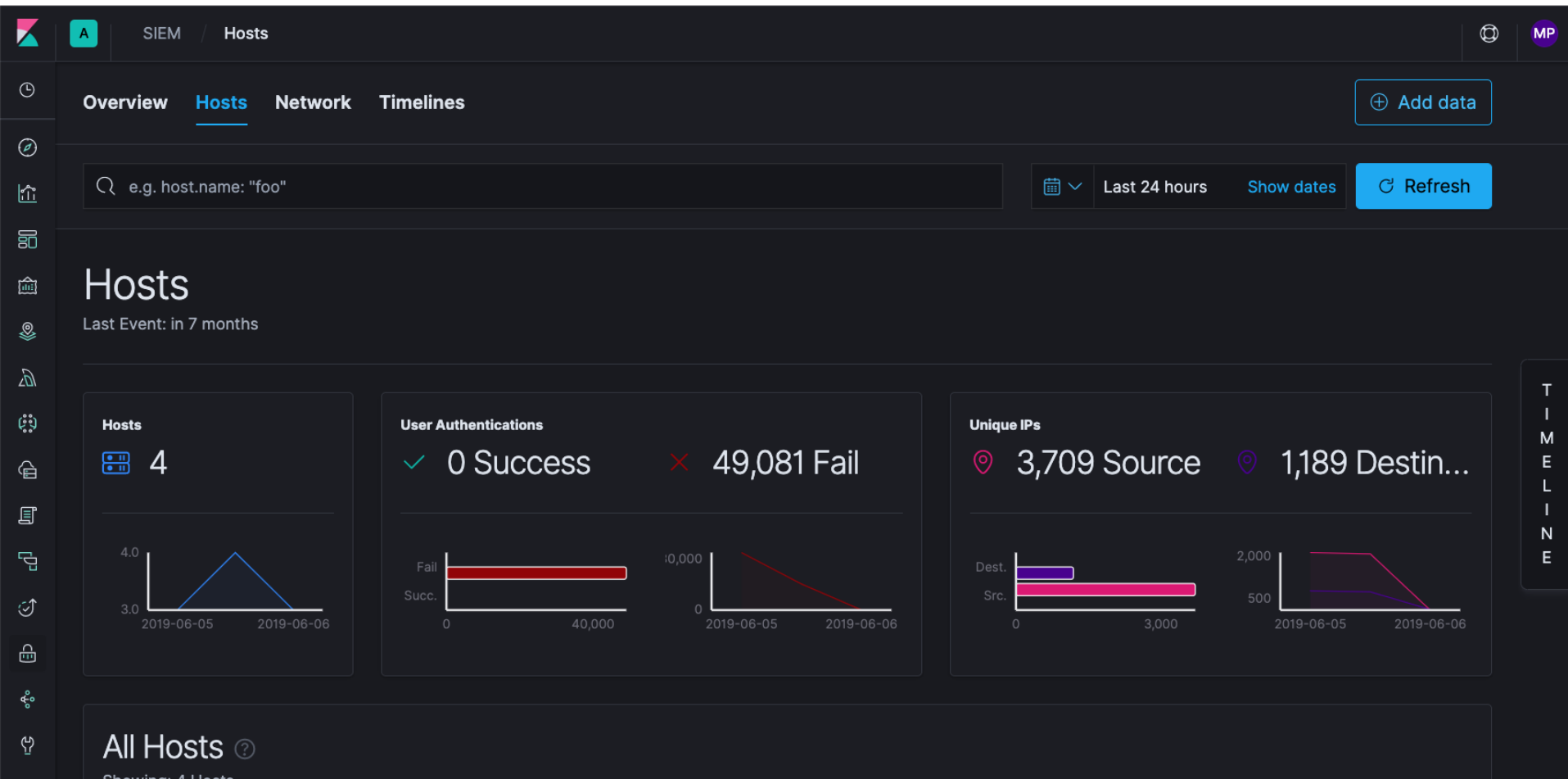
LONGEST FLIGHT



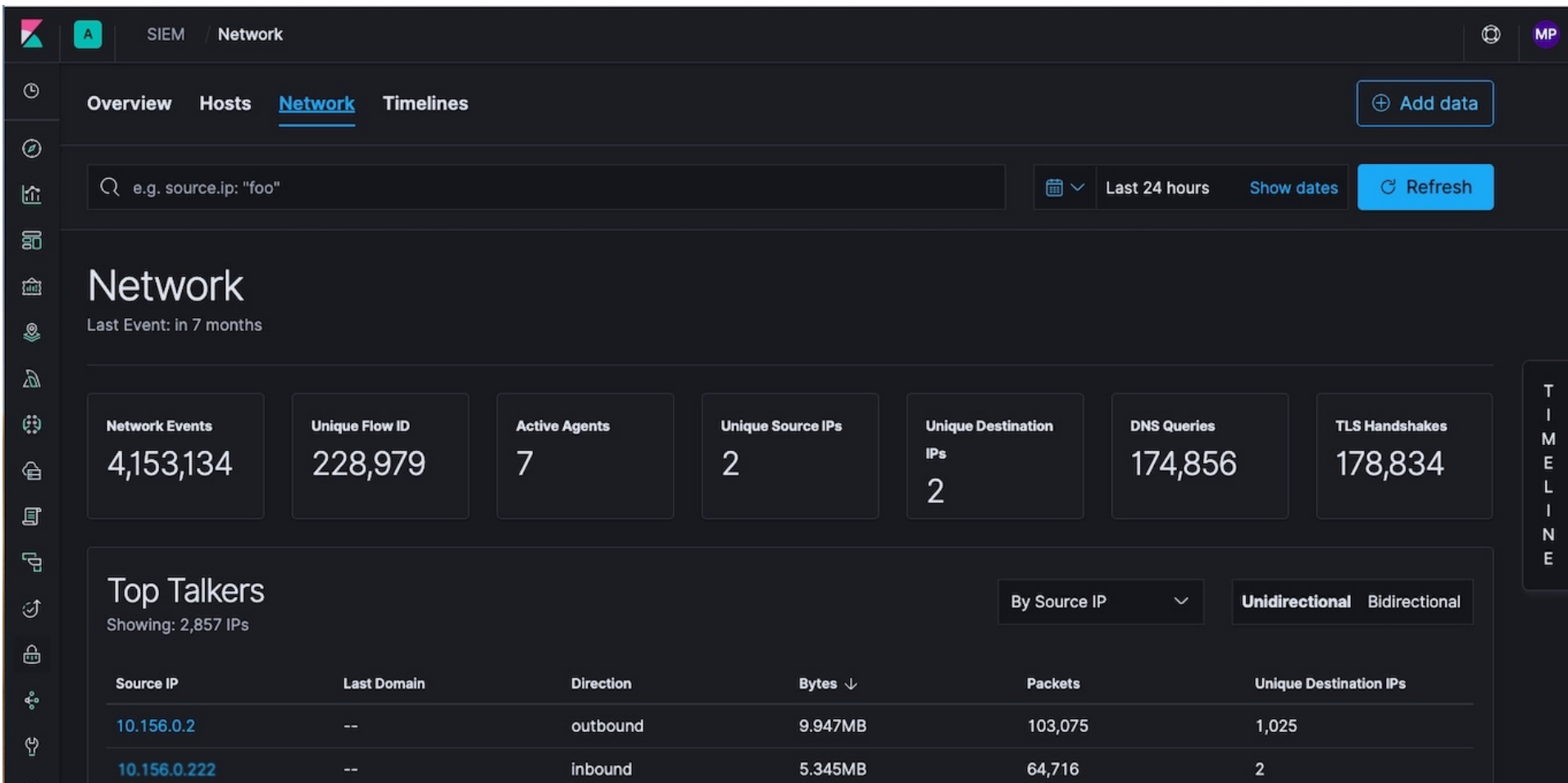
数据展现 - 在地图上分析数据



SIEM APP - 主机安全事件分析



SIEM APP - 网络安全事件分析



Network

Last Event: in 7 months

Network Events

4,153,134

Unique Flow ID

228,979

Active Agents

7

Unique Source IPs

2

Unique Destination
IPs

2

DNS Queries

174,856

TLS Handshakes

178,834

Top Talkers

Showing: 2,857 IPs


By Source IP


Unidirectional

Bidirectional

Source IP	Last Domain	Direction	Bytes ↓	Packets	Unique Destination IPs
10.156.0.2	--	outbound	9.947MB	103,075	1,025
10.156.0.222	--	inbound	5.345MB	64,716	2

T
I
M
E
L
I
N
E




 e.g. host.name: "foo"











































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

  Untitled Timeline   Last 24 hours  Show dates  Refresh 

Drop anything **highlighted** here to build an **OR** query

AND Filter   Filter events

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

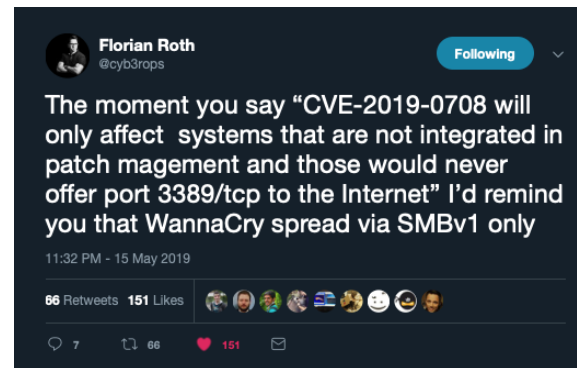
Group 2 (Must be populated to the max extent practical where event message contains relevant fields.)

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

安全分析实例



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



规则来拯救

```
1 title: Suspicious Outbound RDP Connections
2 status: experimental
3 description: Detects Non-Standard Tools Connecting to TCP port 3389 indicating possible lateral movement
4 references:
5   - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
6 author: Markus Neis ~ Swisscom
7 date: 2019/05/15
8 tags:
9   - attack.lateral_movement
10  - attack.t1210
11 logsource:
12   product: windows
13   service: sysmon
14 detection:
15   selection:
16     EventID: 3
17     DestinationPort: 3389
18   filter:
19     Image:
20       - '%\mstsc.exe'
21       - '%\RTSApp.exe'
22       - '%\RTSApp.exe'
23       - '%\RDCMan.exe'
24       - '%\ws_TunnelService.exe'
25       - '%\RSSensor.exe'
26       - '%\RemoteDesktopManagerFree.exe'
27       - '%\RemoteDesktopManager.exe'
28       - '%\RemoteDesktopManager64.exe'
29       - '%\mRemoteNG.exe'
30       - '%\mRemote.exe'
31       - '%\Terminals.exe'
32       - '%\spiceworks-finder.exe'
33       - '%\FSDiscovery.exe'
34       - '%\FSAssessment.exe'
35       - '%\MobaRTE.exe'
36       - '%\chrome.exe'
37   condition: selection and not filter
38 falsepositives:
39   - Other Remote Desktop RDP tools
40 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也支持传统的规则检测

The image shows the Sigma rule interface in Elasticsearch. The rule is titled "CVE-2019-0708 A Critical 'Worm' Remote Code Execution". The description states: "Detects connection to port 3389 from non-MS binaries, like mstsc.exe and possible defence evasion via masquerading technique (hiding worm activity under fake mstsc binary)".

The rule is categorized as "Sigma" and "Elasticsearch". The "CONTENT: .YML" section shows the rule configuration:

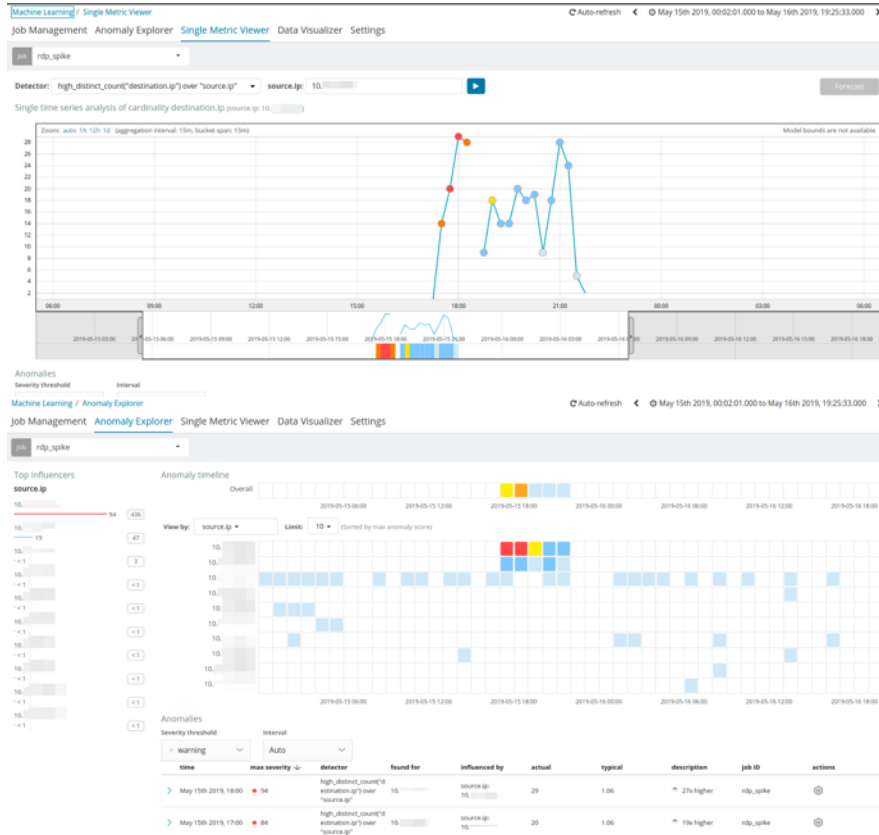
```
title: Possible MS RDP Worm activity aka "BlueKeep"
description: Detects connection to port 3389 from non-MS binaries, like mstsc.exe and possible defence evasion via masquerading technique (hiding worm activity under fake mstsc binary).
author: Roman Ranskyi
references:
- https://krebsonsecurity.com/2019/05/microsoft-patent-bluekeep/
- https://portal.msrmc.microsoft.com/en-US/security-advisories/default.aspx?advisory=CVE-2019-0708
- https://blogs.technet.microsoft.com/msrc/2019/05/14/bluekeep-remote-code-execution-vulnerability-in-rdp/
- https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/bluekeep-remote-code-execution-vulnerability-in-rdp/
status: stable
date: 2019/05/15
logsource:
  product: windows
```

The "CONTENT: ELASTICSEARCH QUERY" section shows the query:

```
((event_id:"3" AND event_data.DestinationPort("3389")) AND NOT (event_id:"3" AND event_data.Protocol("udp")) AND NOT (event_id:"3" AND event_data.Image("C:\\Windows\\System32\\mstsc.exe"))) OR ((exists:("event_data.Description" "event_data.FileVersion" "event_data.Product" "event_data.Company")) AND (event_data.Image:"mstsc.exe") AND (event_data.Description.keyword:"?" OR event_data.FileVersion.keyword:"?" OR event_data.Product.keyword:"?" OR event_data.Company.keyword:"?")) OR ((event_id:"1" AND event_data.ParentImage("svchost.exe") AND event_data.ParentCommandLine("termsvc") AND NOT (event_data.Image("C:\\Windows\\System32\\rdpclip.exe"))
```

The interface also includes a "Suggest Update" button, a "Copy" button, and a "Search in Kibana" button. The bottom of the interface shows a navigation bar with links to "Exploitation of Remote Service...", "Masquerading", "Network Service Scanning", and "Threat Hunting".

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, 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 Bezverkhyyi


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.

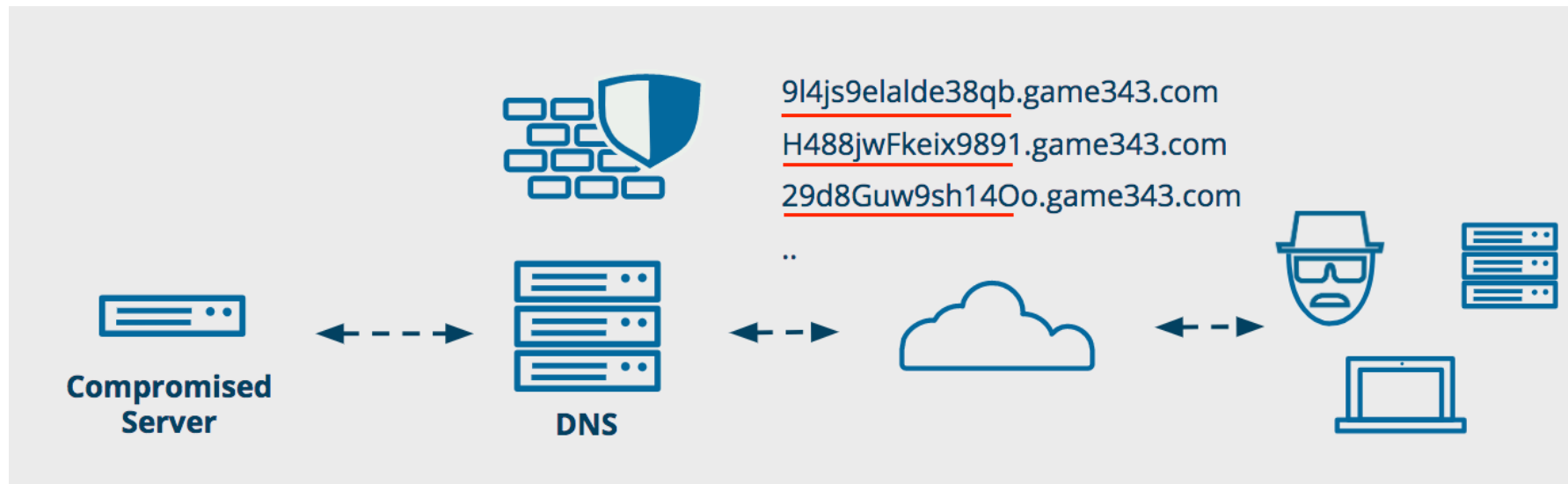
**WATCH NOW**

The background of the hero section is a dark blue field filled with a network of glowing orange lines and dots, resembling a digital or neural network. Small green squares are scattered throughout the background.

Security education, consulting, and support

DEMO

通过DNS隧道进行数据渗透



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/>