

# 顺丰在安全领域的实践与探索

胡泽柱  
顺丰



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

 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

 众语时

 IT大咖说

 otpub

 Broadview  
www.broadview.com.cn

 百格活动  
bagevent.com

 MAXHUB  
高效会议平台

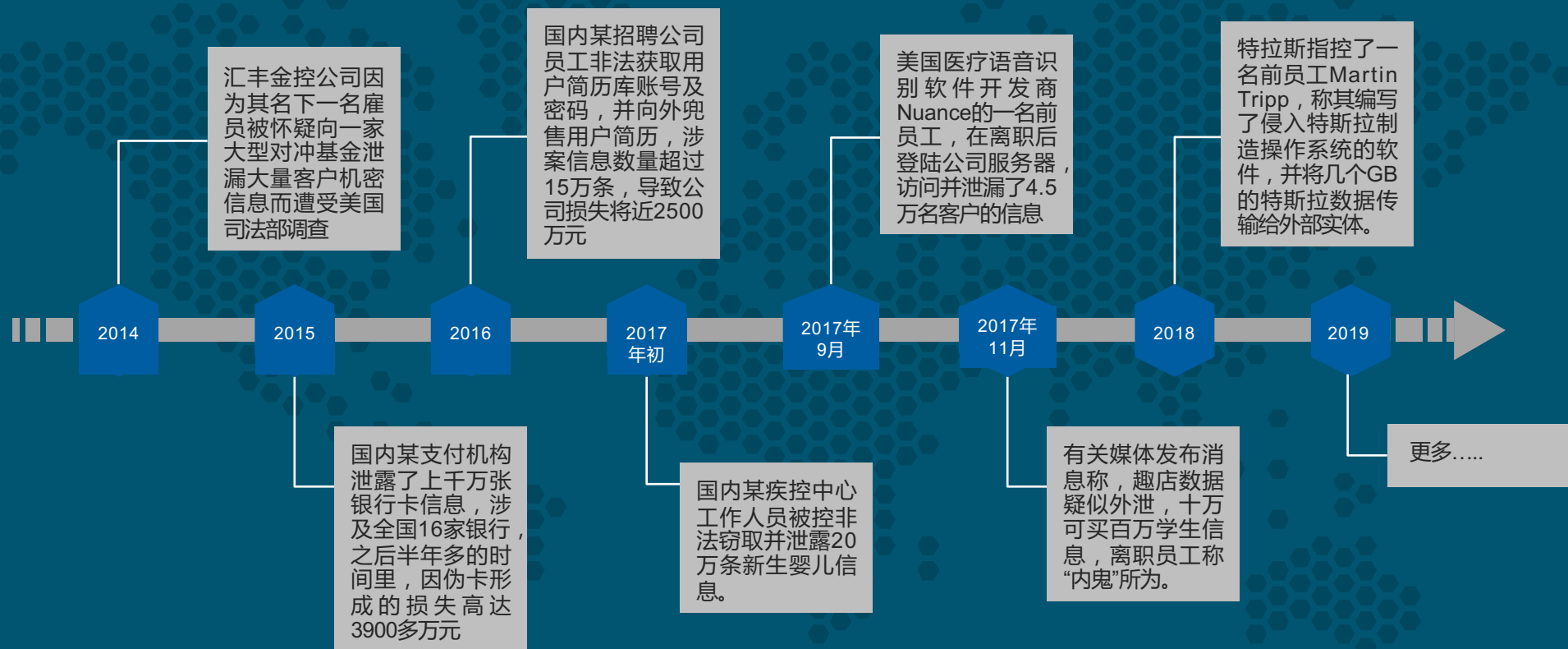
# 概要

- 安全形势
- 挑战
- 解决方案
- 实践



Security

## 安全形势



## 挑战 - 内部威胁

“无知型”内鬼

”利益型”内鬼

”愤怒型”内鬼



## 挑战 - 内部威胁 - “无知型”内鬼

指的是我们心地善良的员工，由于信息安全意识薄弱，容易通过邮件、电话、网络等手段，被利用人性弱点，受到欺骗，无意间把公司信息泄露出去。

嘿嘿，弄到了，又可以抢一批客户啦



黑产

你好，xx快递，我是运单号33xxxx9寄件人小王的朋友，他电话是139xxx，他让我查一下收件人是谁，帮我查一下好么？

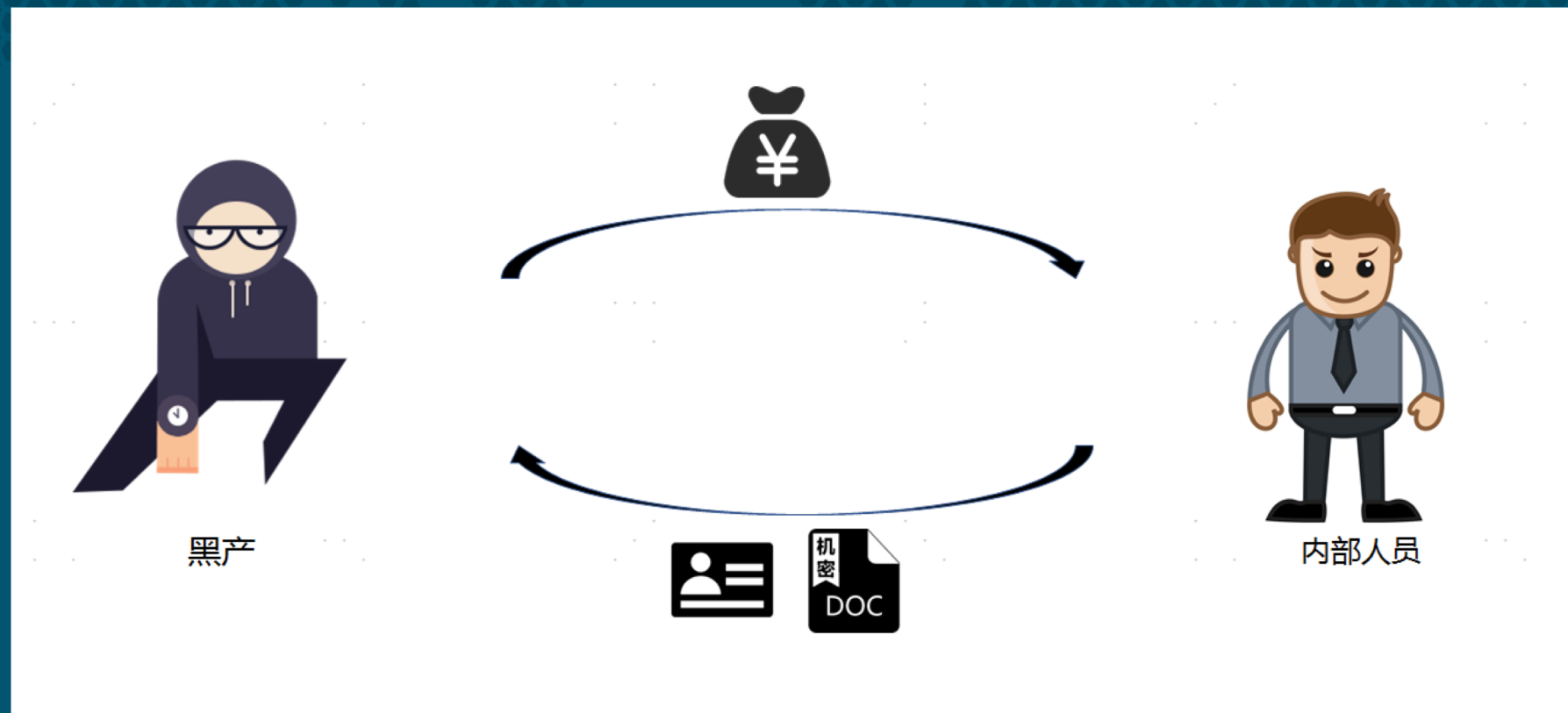
好嘞，这个单子收件人电话是158xxx，收件人是李xx。



内部人员

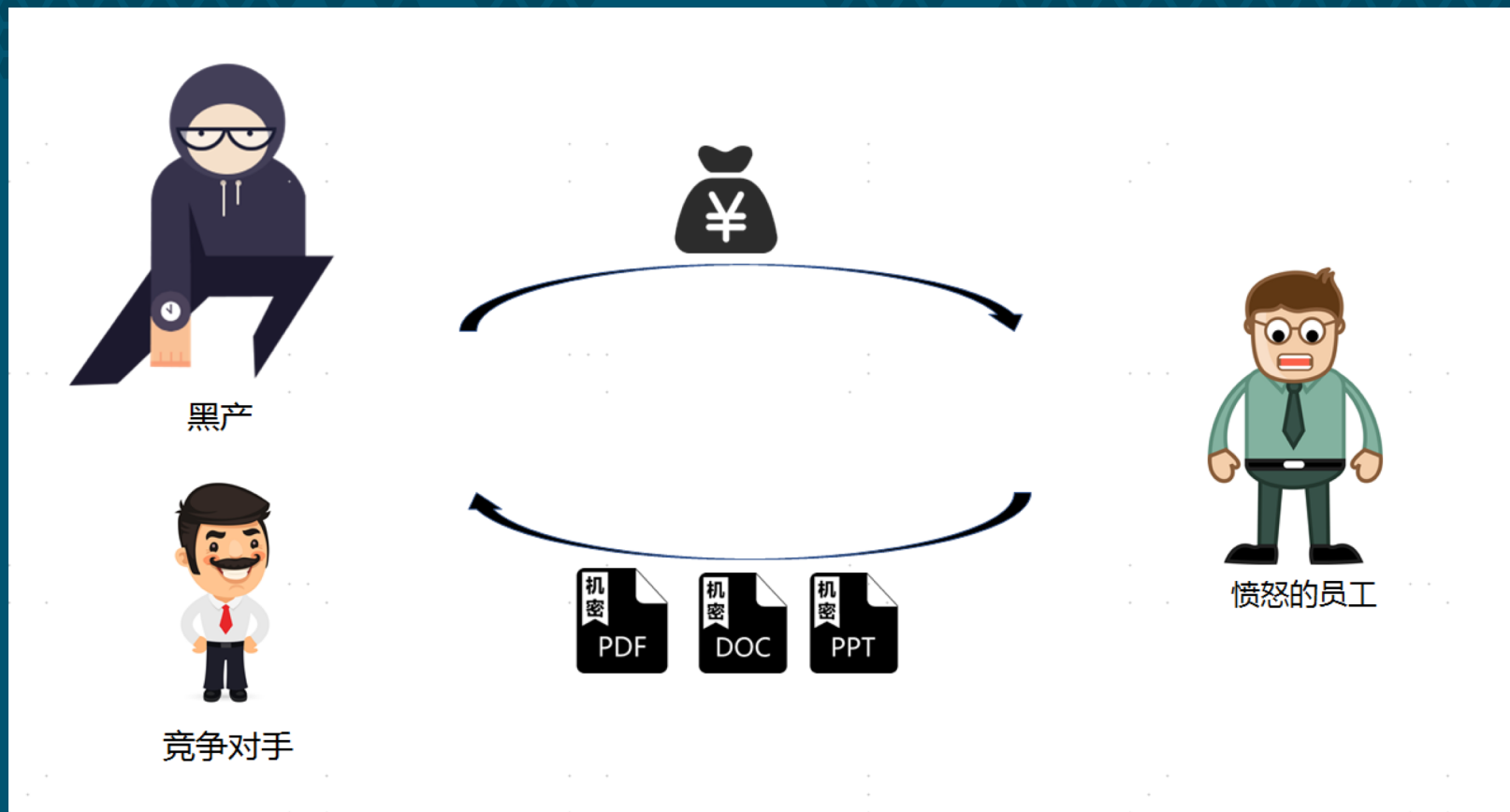
## 挑战 - 内部威胁 - “利益型”内鬼

指的是那些知法犯法，被黑产利诱，利用工作权限获取大量公司机密信息，通过贩卖获取利益的人。



## 挑战 - 内部威胁 - “愤怒型”内鬼

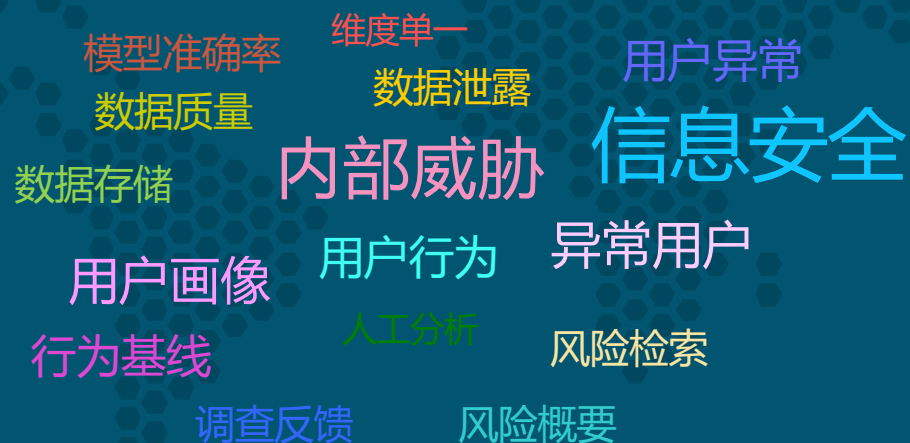
指的是那些出于报复的犯罪动机的员工，故意破坏或盗窃公司的知识产权，并对外或向竞争公司出售商业机密。



## 挑战

我们面临的问题或难点：

- (1) 内部威胁动态变化，并没有一种万能的方法可以减轻所有类别的内部威胁及风险；
- (2) 有了模型，但准确率不高，预警结果还需辅助大量人工分析；
- (3) 调查时难以上下文进行追溯，调查反馈用时长；
- (4) 没有统一的用户画像数据存储；
- (5) 难以全面了解用户的异常行为和风险概况；
- (6) 标签缺乏，数据质量不高；
- (7) 单一事件建模，较难定位真正的异常用户；
- (8) ....



## ==::: 解决方案



数据



方法



工具



人员



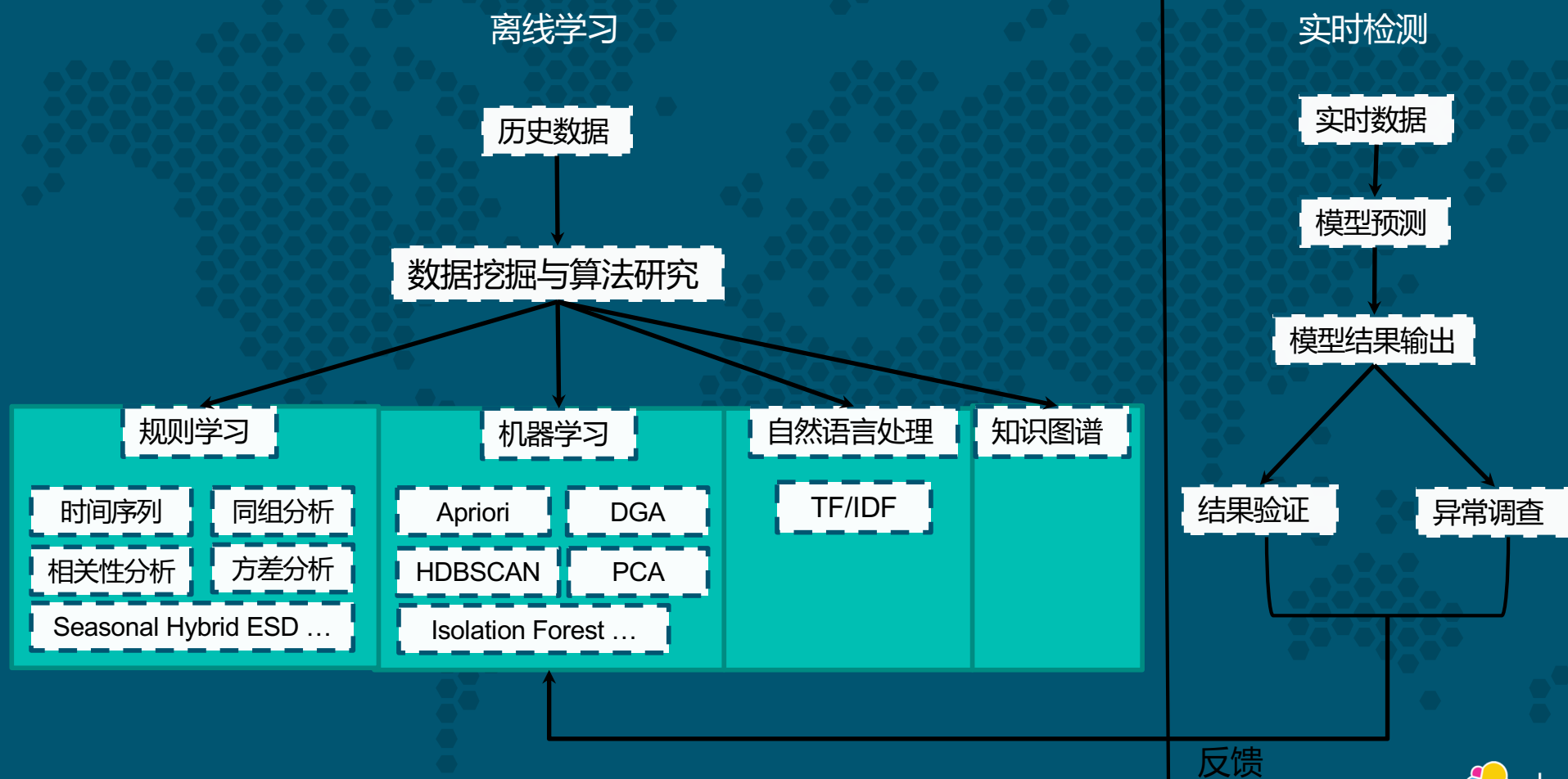
## 思路 – 行为分析思路

**解决方案：**基于用户24小时的行为分析，识别内网异常用户和 用户异常。

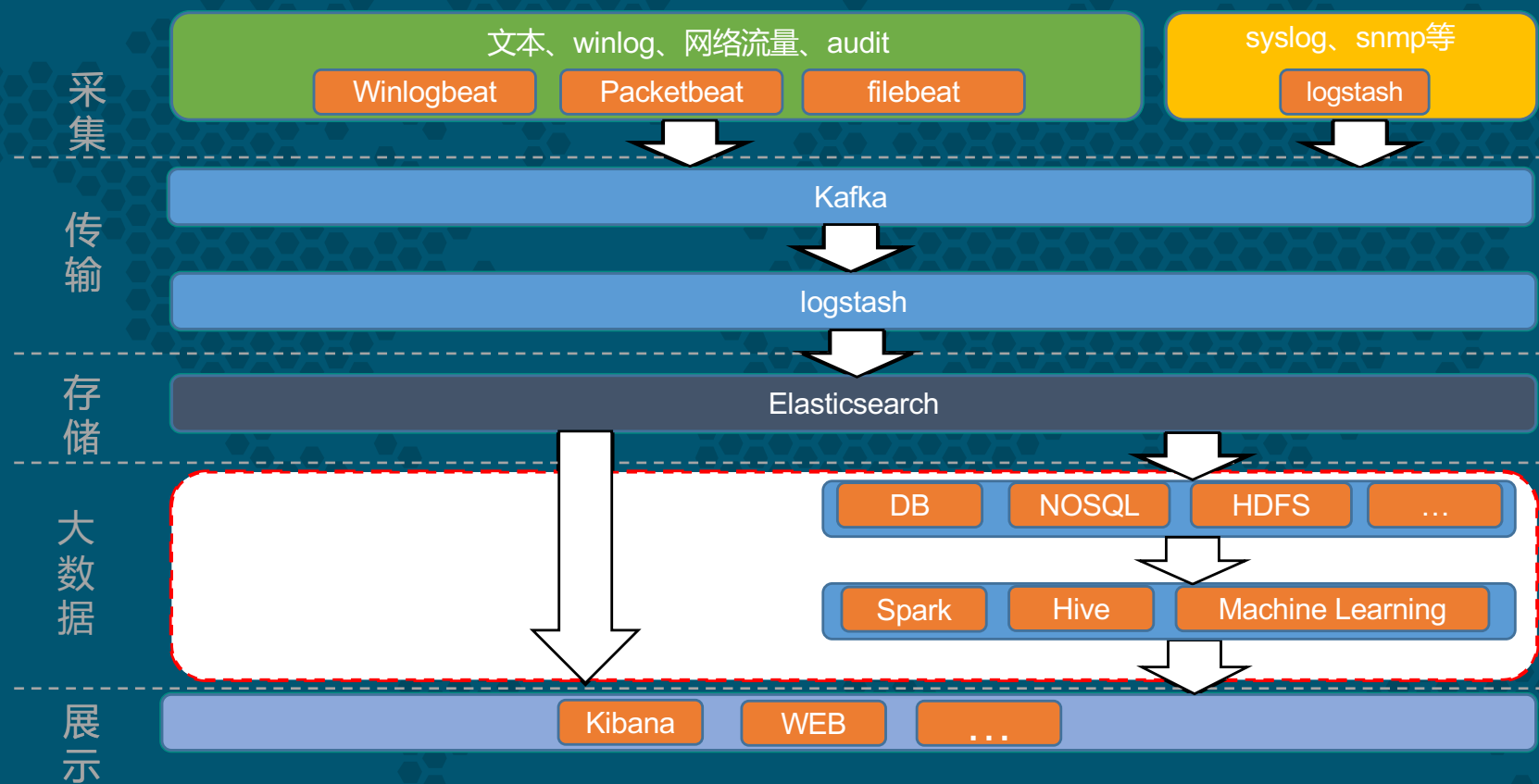
**重点：**建立用户正常行为模式基线，充分利用终端以及基础安全数据信息发现用户异常。



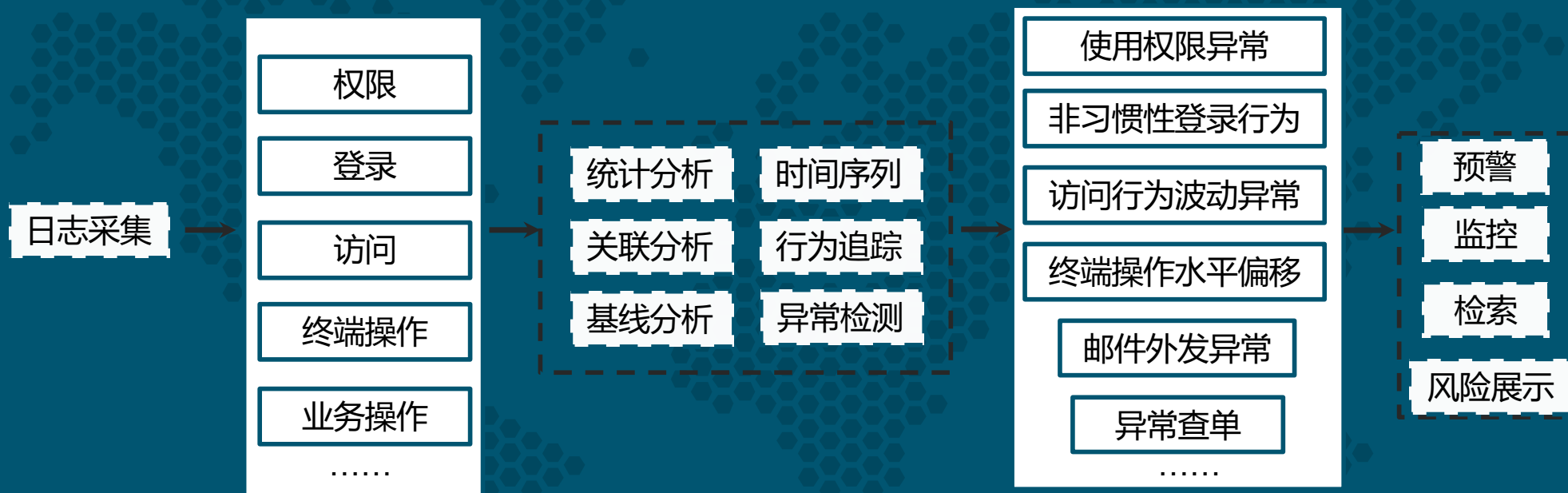
## 方法 – 大数据分析



## 工具--日志平台架构图



## 行为日志探索案例（基于ELK）



统一存储

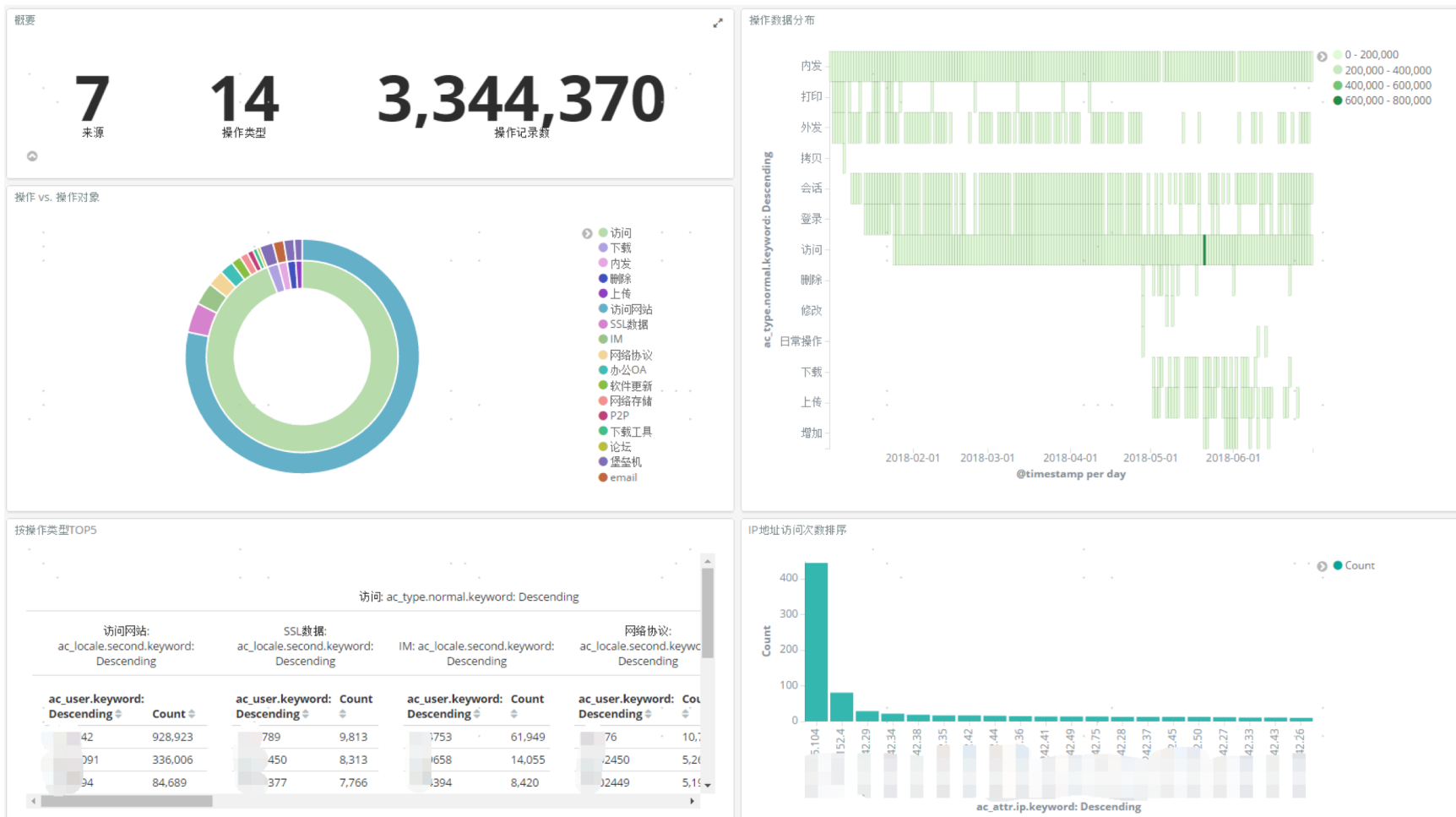
异常分析

异常行为

快速定位



## 统计分析

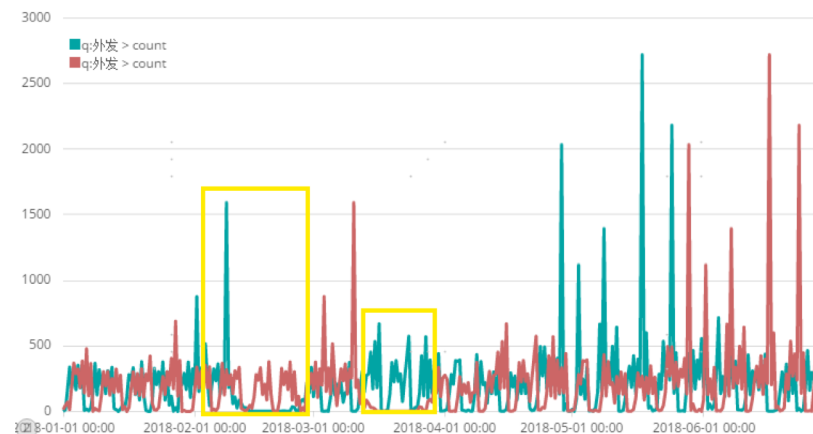




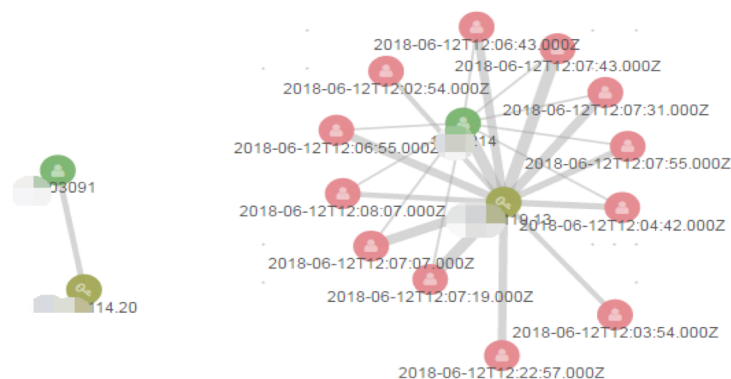
## 时间序列 & 关联分析



波动性分析



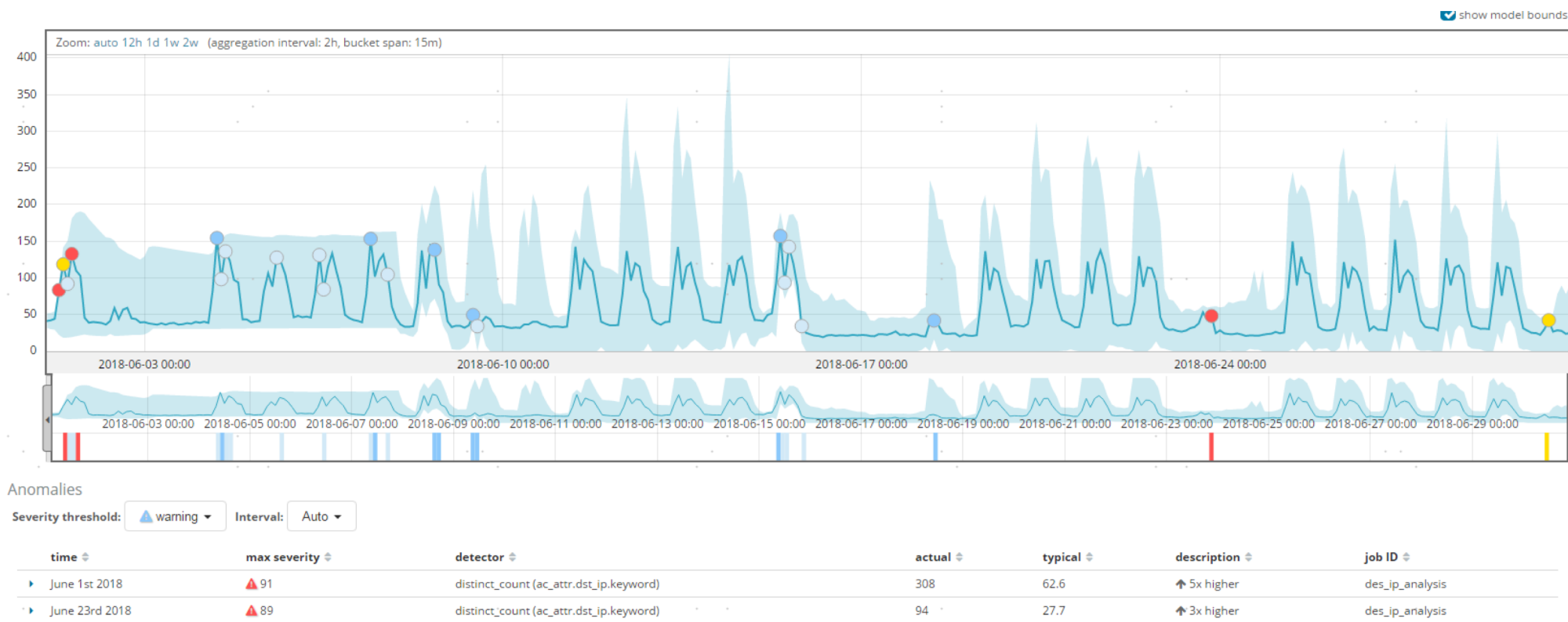
与上月同期对比



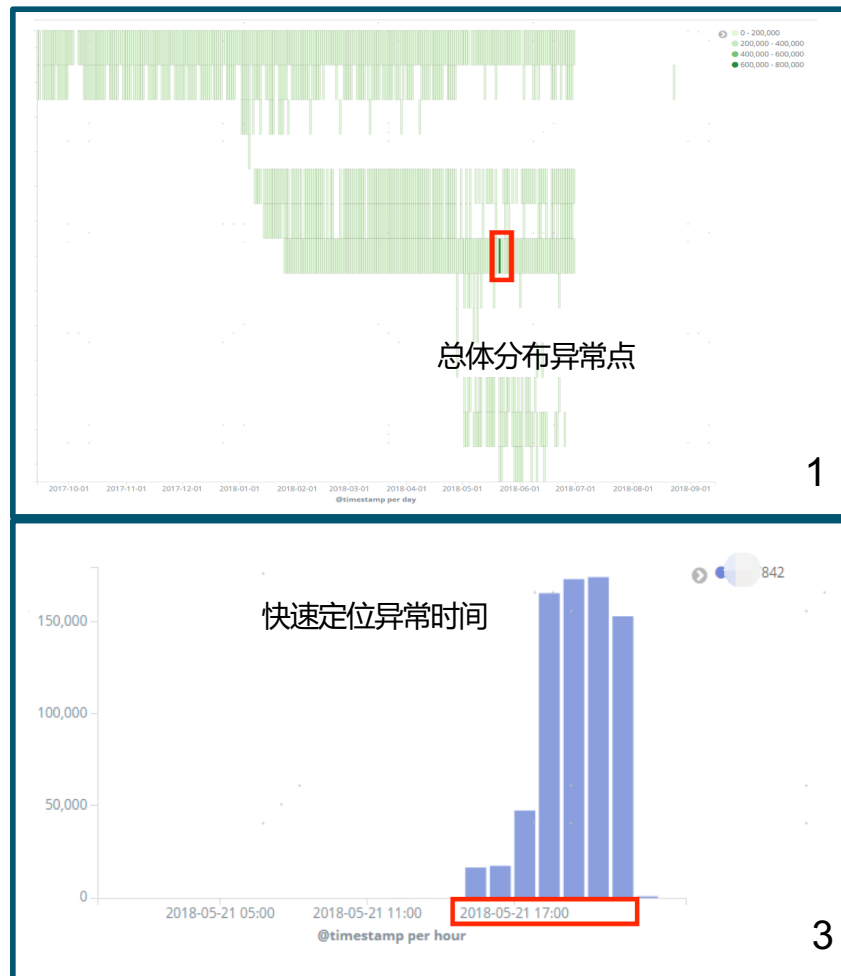
用户与ip的关联分析

## 机器学习

### 快速定位IP使用异常



## 行为追踪



数据筛选

数据筛选

数据筛选



## 总结

- ES提供了一个集中化存储中心
- 可关联用户不同行为进行分析，了解用户整体风险
- 快速检索功能，提高了日志检索、行为追踪的效率
- 可视化让分析人员更为直观地了解总体和各关注点的风险情况
- 通过时间序列分析能快速观察到随着时间的变化，用户行为的正常模式和异常点
- 利用关联分析，分析人员能挖掘出数据间较为隐藏的关联性
- 数据接入、存储、分析、检索、展示天然集成，让分析和调查人员所想及所得

☰ :: 下一步

其他分析工具与ELK分析结合

基于ELK集成更多的算法



## 最后我想说

解决问题是目的、数据是基础、**人才是关键**，欢迎加入！



THANK!



# elastic 中文社区

专业、垂直、纯粹的 Elastic 开源技术交流社区

<https://elasticsearch.cn/>

