ELK自身安全与安全领域应用

分享者：张坤(中邮速递易)

2019-04-20

需求

安全要做到对攻击可感知、
可溯源。

老板

安全工程师：小强

需求分析

可感知 == 入侵检测

可追溯 == 溯源分析

谁 时间 对象 操作 结果

五要素

产品调研

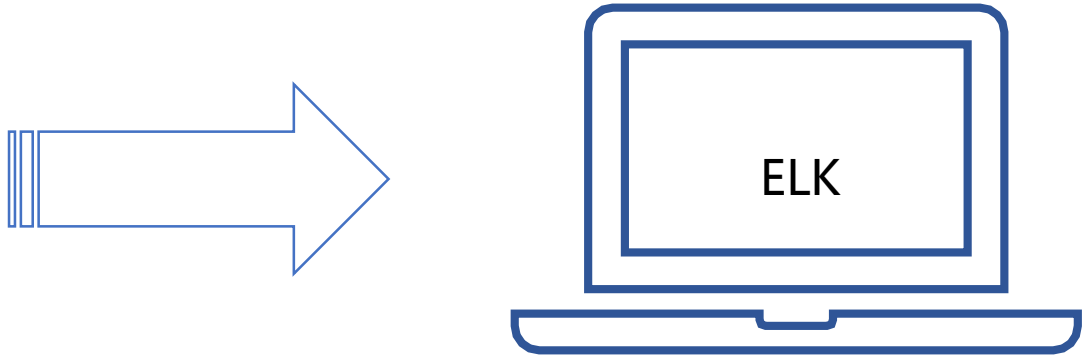
SIEM：安全信息与事件管理

SOC：安全运营中心

日志分析

IDS：入侵检测系统

WAF：Web应用防火墙



产品隐患

漏洞（产品的副产物）

配置（看似合理的需求）

产品隐患

关键字【elasticsearch】的搜索结果共39记录

提交时间	标题	漏洞类型	提交者
2016-04-27	暴风某站Elasticsearch未授权访问&Hadoop未授权访问	应用配置错误	路人甲
2016-04-19	360手机一处Elasticsearch未授权访问	应用配置错误	milkwort。
2016-03-19	新华网某频道服务器一处Elasticsearch配置不当/可任意操作/涉及被采访人员信息	未授权访问/权限绕过	路人甲
2016-03-16	上海某服务器一处Elasticsearch配置不当/可任意操作/涉及大量敏感信息(790多W用户姓名\身份证号\民族\开房时间\退房时间\房间号等)	应用配置错误	路人甲
2016-03-15	广西移动一处Elasticsearch配置不当/可任意操作/涉及大量敏感信息(用户手机号码/IMEI/IMSI/上网时间/地点等)		路人甲
2016-03-15	疑似奇虎360手机助手一处Elasticsearch低风险信息泄露(可任意操作\可执行sql)	应用配置错误	路人甲
2015-10-01	风行某站Elasticsearch配置不当（任意文件读取）	未授权访问/权限绕过	null_z
2015-09-11	神器而已证券系列之九州证券某站Elasticsearch远程代码执行漏洞	命令执行	举起手来
2015-05-27	芒果某服务Elasticsearch Groovy命令执行	命令执行	路人甲
2015-05-16	36kr某站点Elasticsearch远程代码执行	命令执行	lijiejie
2015-04-27	elasticsearch某内置功能缺陷利用可能导致getshell风险	命令执行	园长
2015-04-18	安智网某站Elasticsearch Groovy 命令执行 & ActiveMQ 弱口令	命令执行	几何黑店
2015-03-13	广州多玩某站Elasticsearch Groovy未授权访问	未授权访问/权限绕过	路人甲
2015-03-06	货运人某服务器Elasticsearch Groovy命令执行	命令执行	路人甲
2015-03-06	ACT阿里云服务器存在ElasticSearch Groovy远程代码执行（ROOT权限）	命令执行	Alen

产品隐患

@ShawberH228 你好，

当你为你的 Twitter 帐号设置密码时，我们使用掩码处理技术，没有工作人员能够看到密码。 我们近期发现了密码未经掩码处理保存在内部日志中的问题。 我们已经修复了这个问题，而且我们的调查未显示出任何人的泄露或滥用迹象。

谨慎起见，我们请你考虑在所有使用过此密码的服务上更改密码。 你可以在密码设置 页随时更改你的 Twitter 密码。

解决隐患

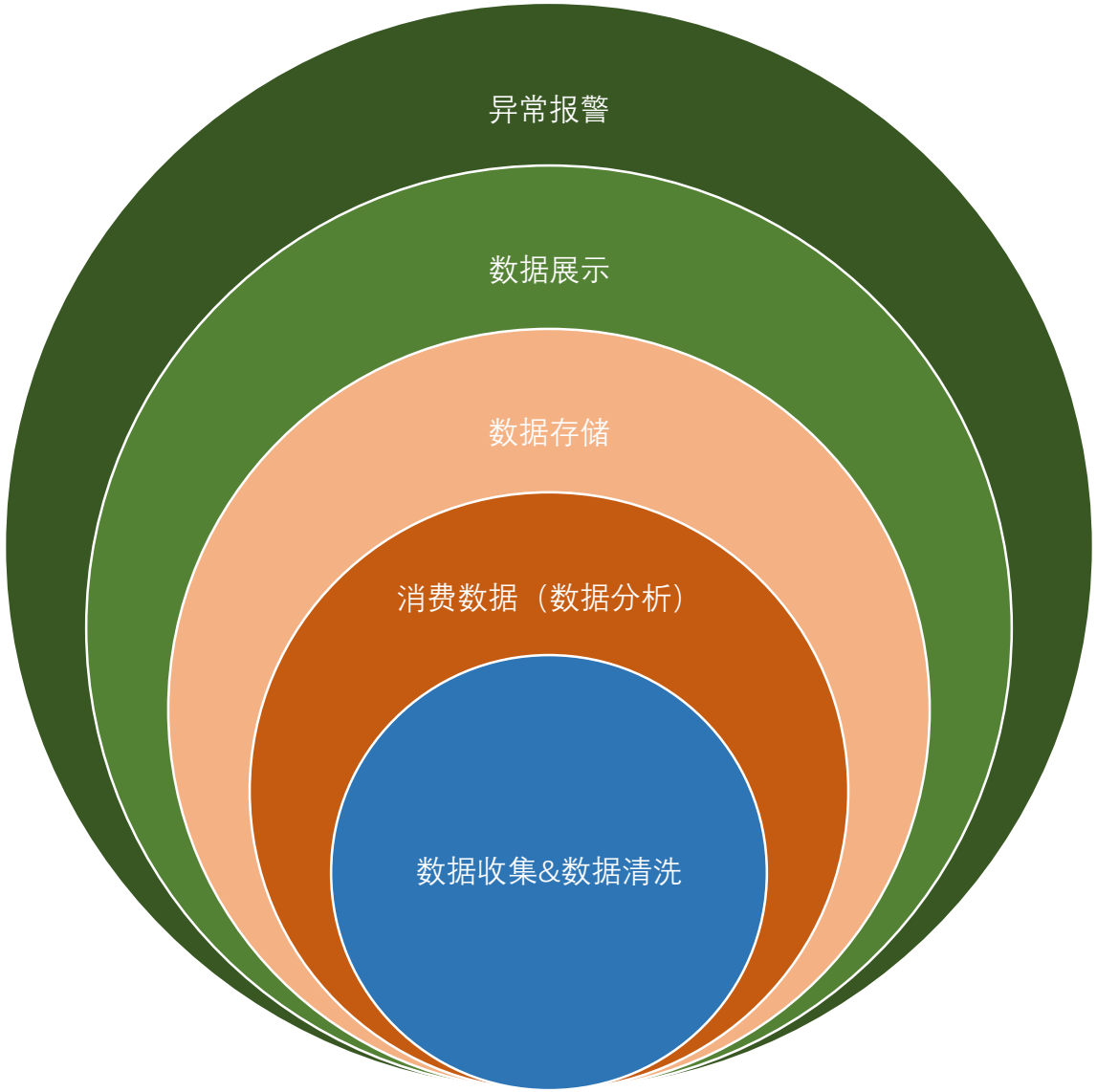
补丁管理：资产监控、情报监控

加密传输：SSL

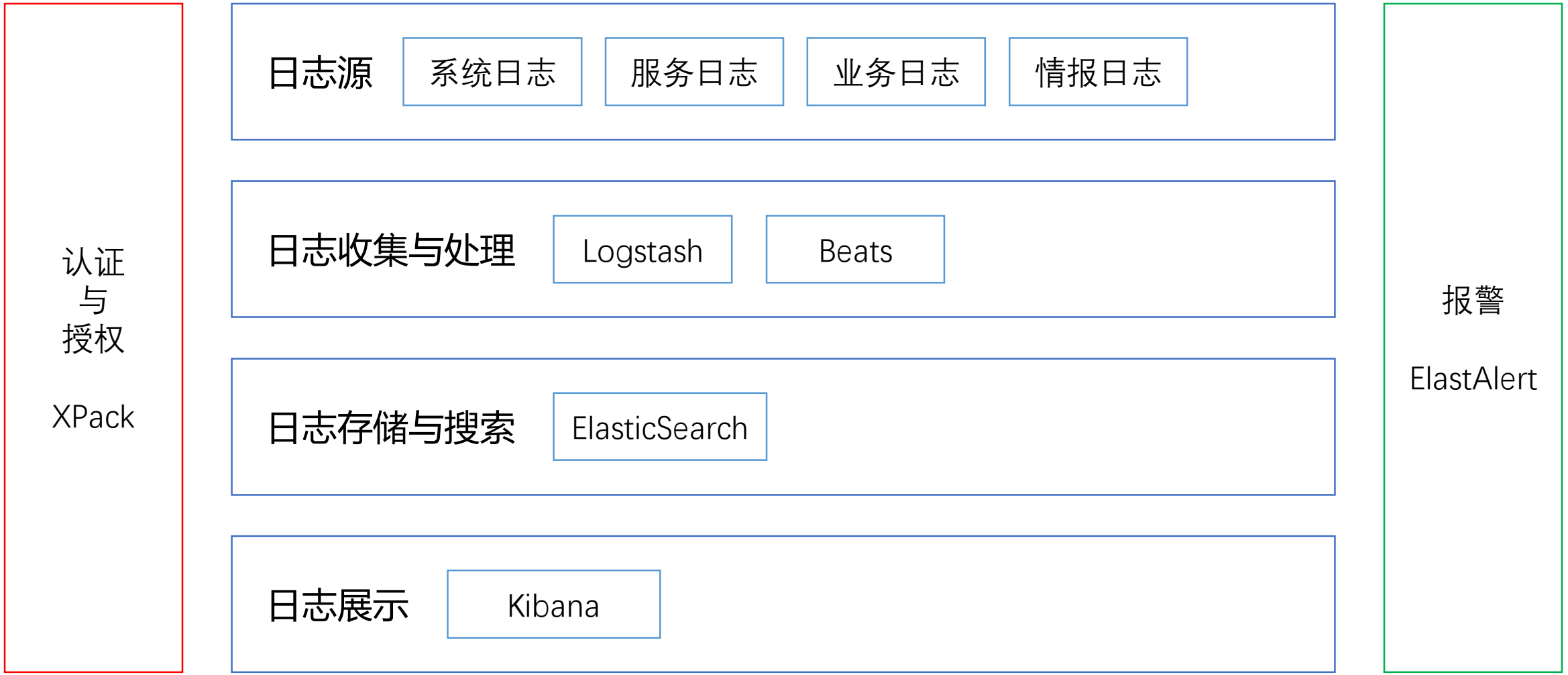
用户认证：HTTP Base、Xpack、SSO

合理授权：Xpack

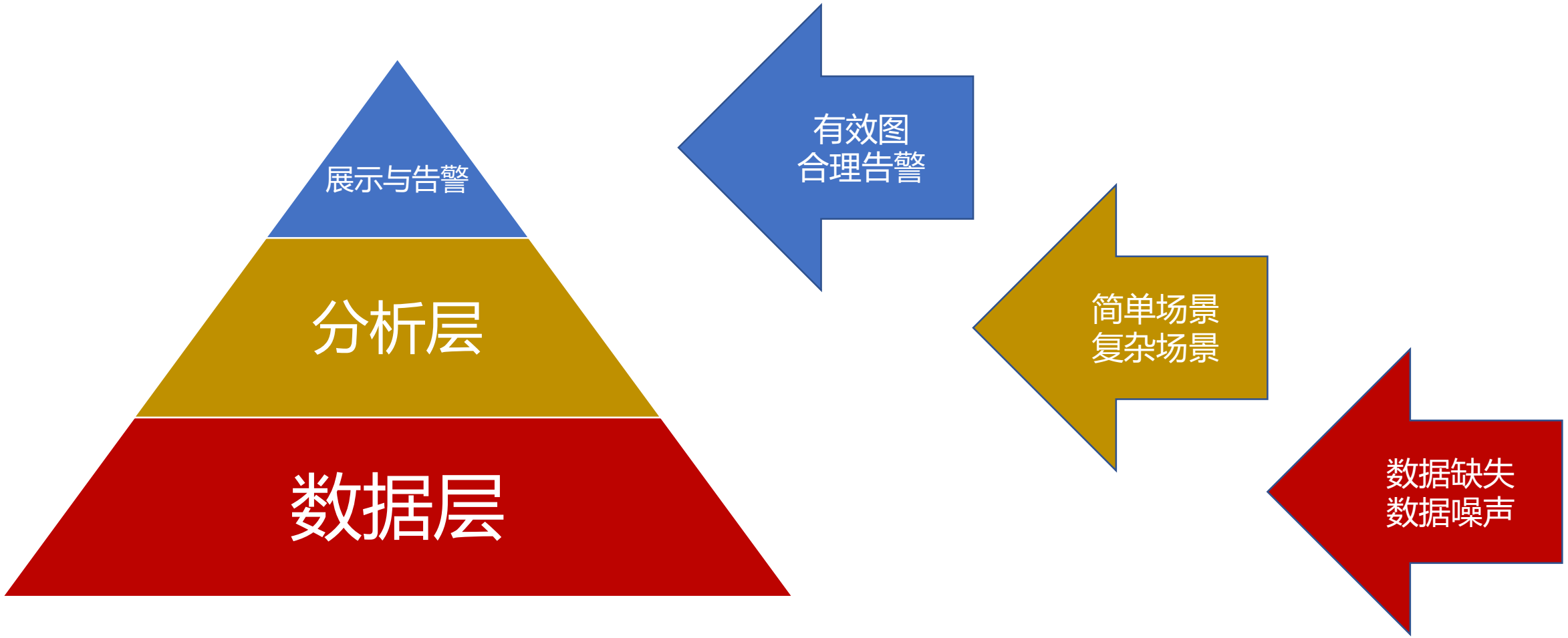
撸起袖子加油干



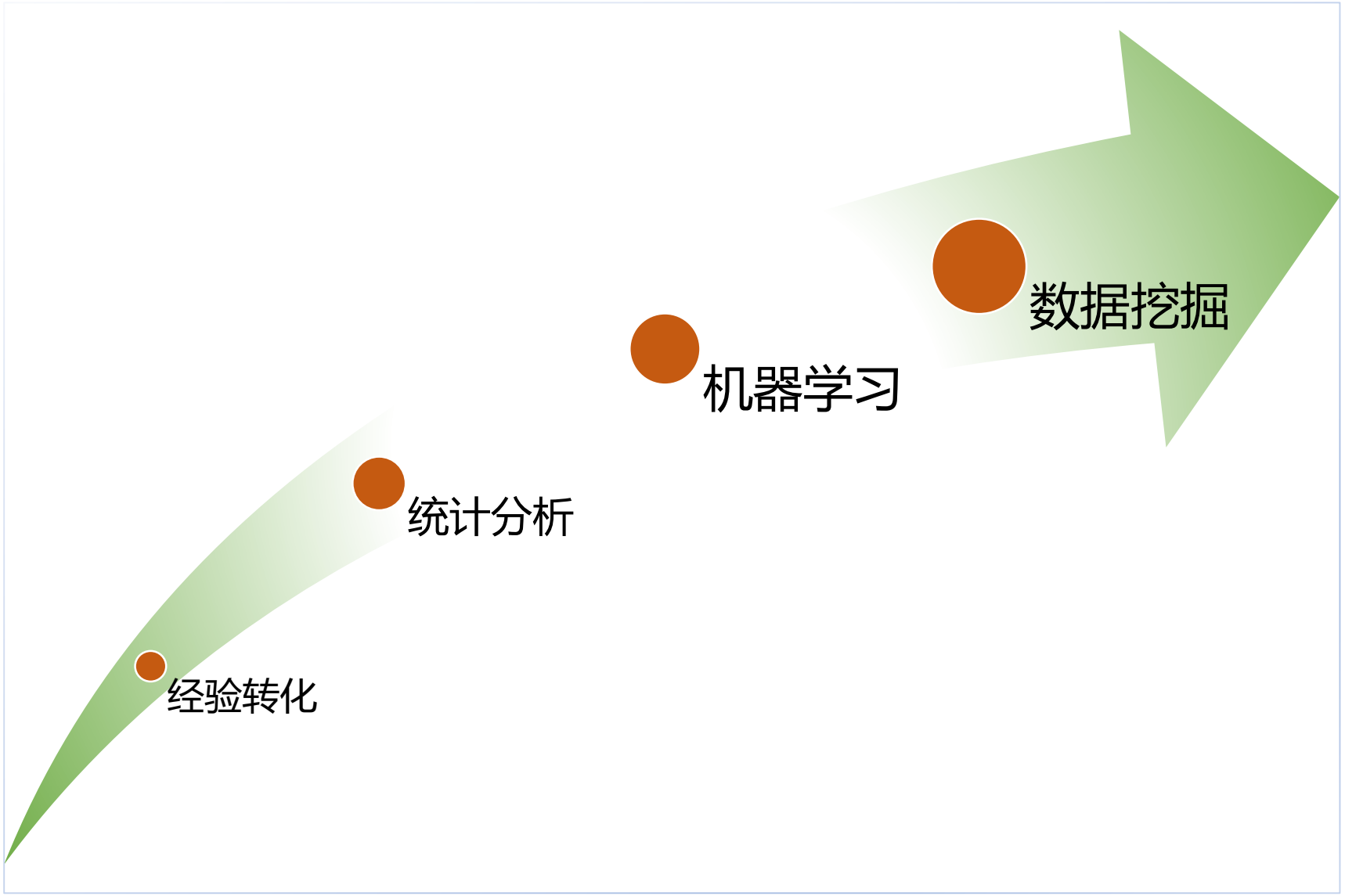
实现方案架构


认证
与
授权
XPack
日志源
系统日志
服务日志
业务日志
情报日志
日志收集与处理
Logstash
Beats
日志存储与搜索
ElasticSearch
日志展示
Kibana
报警
ElastAlert

架构逐层分析



分析手段



落地基本需求：目标

1.威胁时序图
2.疑似威胁分析
3.疑似威胁漏报分析
4.威胁访问流量
5.威胁流量占比
6.境外威胁来源国家(地区)统计
7.境内威胁来源城市统计
8.威胁严重度
9.威胁响应分析
10.恶意IP
11.恶意URL分析
12.威胁类型分析
13.威胁类型分布
14.威胁分类计数
15.威胁来源热力图
16.威胁总数
17.威胁日志占比

来源IP分布

独立IP访问趋势

访问路径排行

用户信息分布(UA/Cookie)

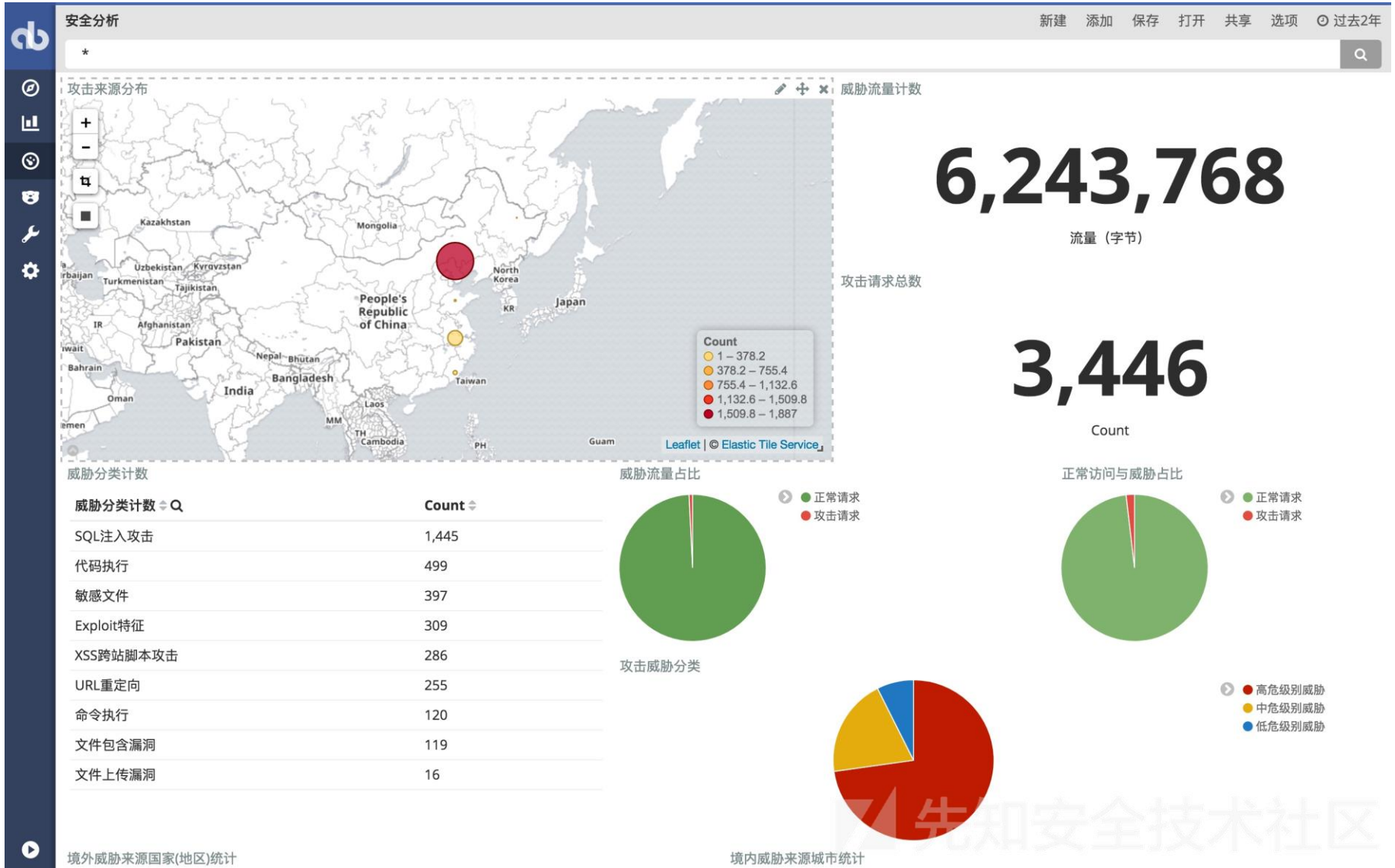
攻击事件类型排行

历史攻击事件

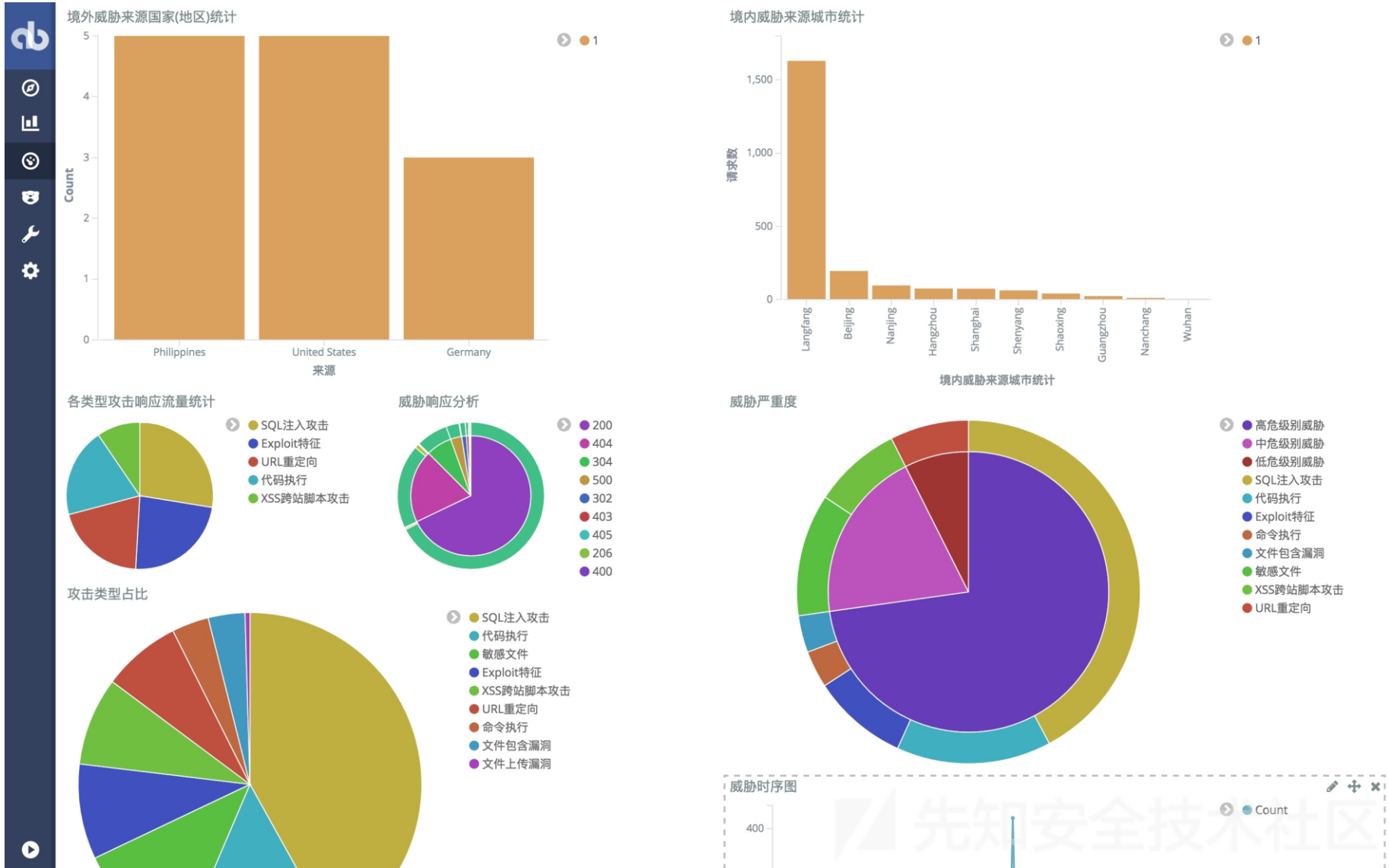
落地基本需求：采集

```
input {
    file {
        path => ["/var/log/httpd/access_log"]
        type => "httpd"
    }
}

filter {
    grok {
        match => { "message" => "%{COMBINEDAPACHELOG}" }
    }
}

output {
    elasticsearch {
        hosts => ["127.0.0.1:9200"]
        index => "logstash-httpd-%{+YYYY.MM.dd}"
    }
}
```

落地基本需求：展示


安全分析
新建
添加
保存
打开
共享
选项
过去2年
*
攻击来源分布
威胁流量计数
6,243,768
流量（字节）
攻击请求总数
3,446
Count
Count
1 – 378.2
378.2 – 755.4
755.4 – 1,132.6
1,132.6 – 1,509.8
1,509.8 – 1,887
Leaflet | © Elastic Tile Service
威胁分类计数
威胁分类计数
Count
SQL注入攻击 1,445
代码执行 499
敏感文件 397
Exploit特征 309
XSS跨站脚本攻击 286
URL重定向 255
命令执行 120
文件包含漏洞 119
文件上传漏洞 16
威胁流量占比
正常请求
攻击请求
正常访问与威胁占比
正常请求
攻击请求
攻击威胁分类
高危级别威胁
中危级别威胁
低危级别威胁
境外威胁来源国家(地区)统计
境内威胁来源城市统计

落地基本需求：展示

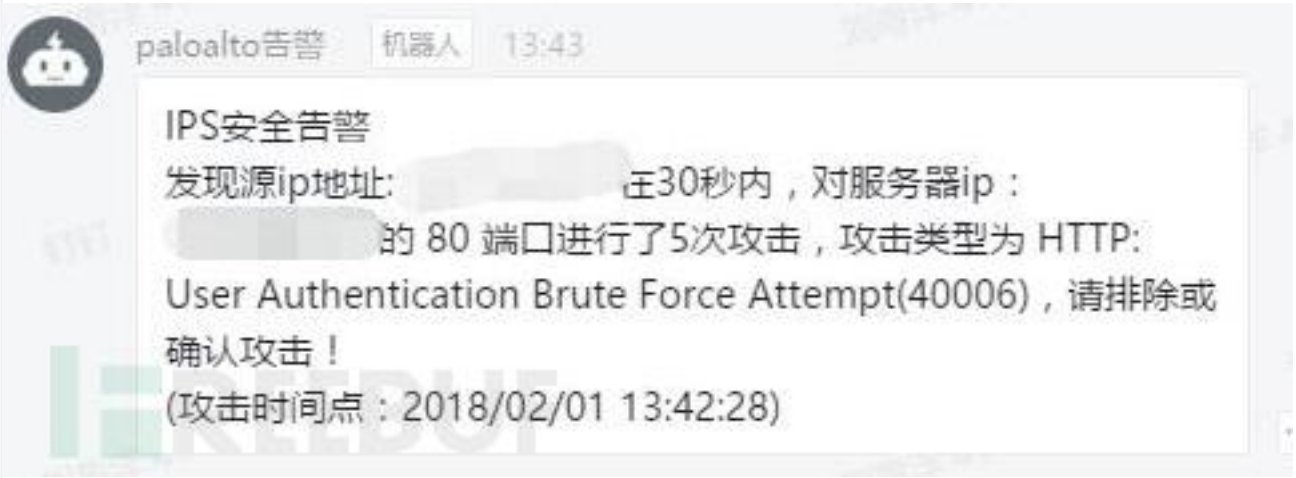

境外威胁来源国家(地区)统计
Count
来源
Philippines
United States
Germany
境内威胁来源城市统计
请求数
境内威胁来源城市统计
Langfang
Beijing
Nanjing
Hangzhou
Shanghai
Shenyang
Shaoxing
Guangzhou
Nanchang
Wuhan
各类型攻击响应流量统计
SQL注入攻击
Exploit特征
URL重定向
代码执行
XSS跨站脚本攻击
威胁响应分析
威胁严重度
高危级别威胁
中危级别威胁
低危级别威胁
SQL注入攻击
代码执行
Exploit特征
命令执行
文件包含漏洞
敏感文件
XSS跨站脚本攻击
URL重定向
攻击类型占比
SQL注入攻击
代码执行
敏感文件
Exploit特征
XSS跨站脚本攻击
URL重定向
命令执行
文件包含漏洞
文件上传漏洞
威胁时序图
Count

落地基本需求：报警

```
es_host: 127.0.0.1
es_port: 9200
name: security
type: any
index: logstash

# 查询模式
filter:
- query:
        query_string:
                query: "message:test"

# 报警模式
alert:
- "elastalert_modules.dingtalk_alert.DingTalkAlerter"

# 钉钉的webhook接口
dingtalk_webhook: ""
dingtalk_msgtype: "text"
```

落地基本需求：报警

```
security

@timestamp: 2018-11-07T11:40:56.739Z
@version: 1
_id: ncb57WYBPCWMEgXKtFSQ
_index: logstash-httpd-2018.11.07
_type: doc
host: bloodzer0
message: test
num_hits: 27
num_matches: 27
path: /var/log/httpd/access_log
tags: [
    "_grokparsefailure"
]
type: httpd
```



展望

老板

嗯，很好！

安全工程师：小强

对外我们可以感知所有的攻击；
对内我们可以对所有用户行为实施分析；

谢谢
Q&A

专业、垂直、纯粹的 Elastic 开源技术交流社区

https://elasticsearch.cn/