ELK 安全监控中心踩坑和实践

去哪儿网安全工程师　周军

2016携程信息安全沙龙

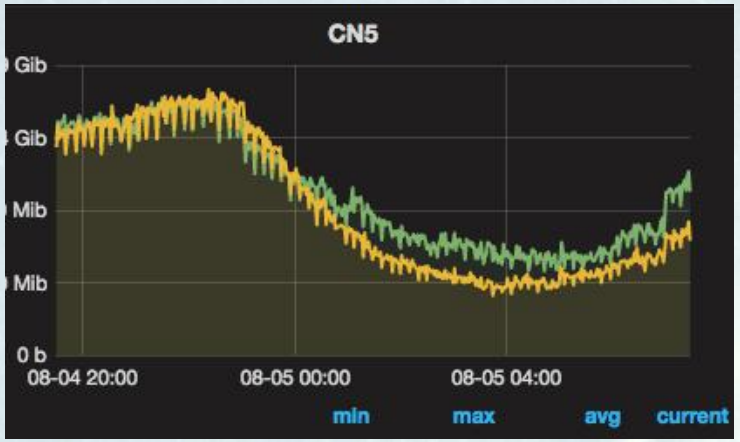
关于我

* 去哪儿网

* 主要负责漏洞分析、运维安全、日志分析相关工作

安全监控涉及到的场景

传统监控方案



利用 Watcher 监控分析网络流量

Suricata IDS

利用 Suricata 监控网络行为

传统监控方案

利用 Ossec 分析主机日志

tomcat log

+

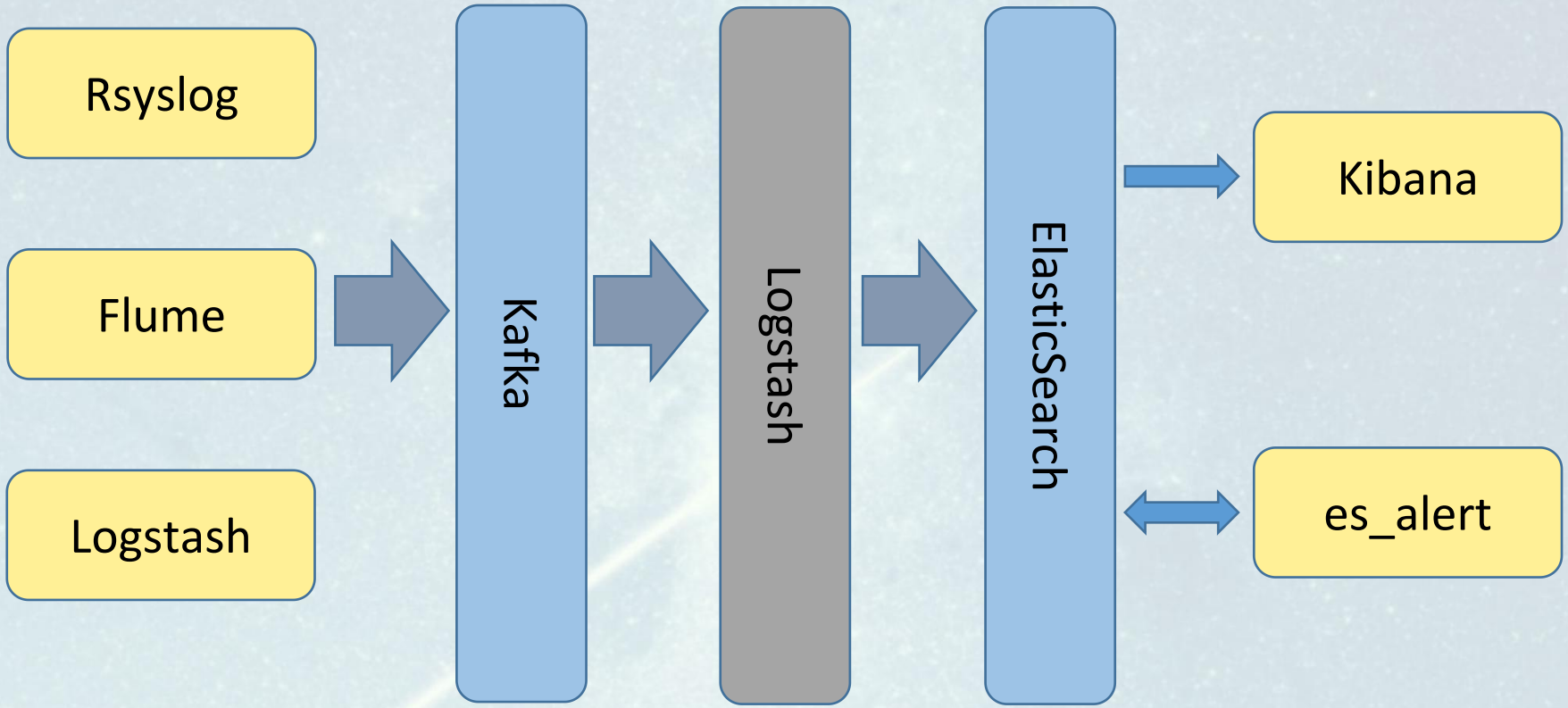
python

利用 Python 分析 Web 日志

传统解决方案的问题和坑

- 监控分散，各部分独立
- 难以扩展，无法复用
- 历史数据保存问题
- 缺少可视化分析
- 人工成本高

基于 ELK 的解决方案



使用 ELK（Elasticsearch、Logstash、Kibana）搭建日志平台

数据源


日志丢失？
缺少字段？
日志埋点？
数据量过大？
……
Bash
MySQL
Auditd
VPN
QSSO
Gitlab
SVN
Wiki
Sflow
Qwaf
IDS
Jira

数据采集


Bash
MySQL
Auditd
VPN
Wiki
Jira
Sflow
IDS
.history 内容？No, patch 埋点
字段混乱？ Rsyslog 日志重组
资源文件干扰？Logstash 收集过滤
数据量过大？本地先聚合

Logstash

```
input {
    kafka { }
}

filter {
    if [type] == "xxxx" {
        grok {
            match =>["message","%{IPV4:server_ip}.* .... (%{IPV4:cl
        }
    }
    mutate { remove_field => [""] }
}

output {
    #stdout { codec => rubydebug }
    if [type] == "xxxx" {
        elasticsearch {
            host => ["xxx.xxx.xxx.xxx", "..."]
            cluster => "elasticsearch"
            protocol => "http"
            index => "%{type}-%{+YYYY.MM}"
            template_overwrite => true
            workers => 5
        }
```

正则出错？使用正则模板

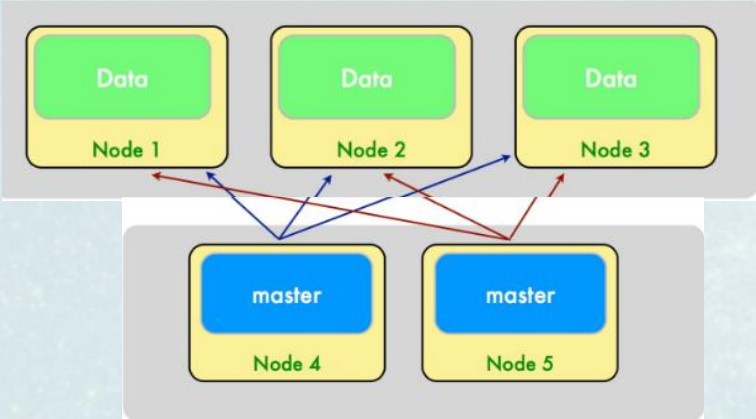
冗余字段？删除冗余干扰字段

输出错误？rubydebug 调试

Logstash 假死？简单心跳检测

数据混杂？按字段生成索引

ES 集群搭建

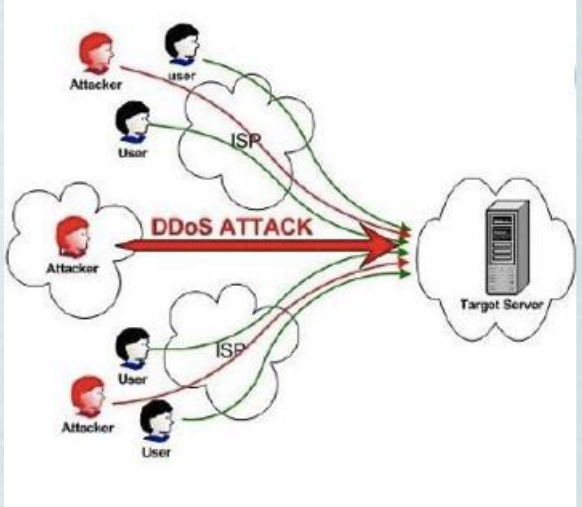


- 应用部署？data 和 log 目录独立
- 访问控制？Shield？Searchguard
- 数据备份？设置复制分片
- 负载均衡？master和data 独立
- 频繁 GC？调整 cache/buffer 参数

异常流量监控案例

网络流量

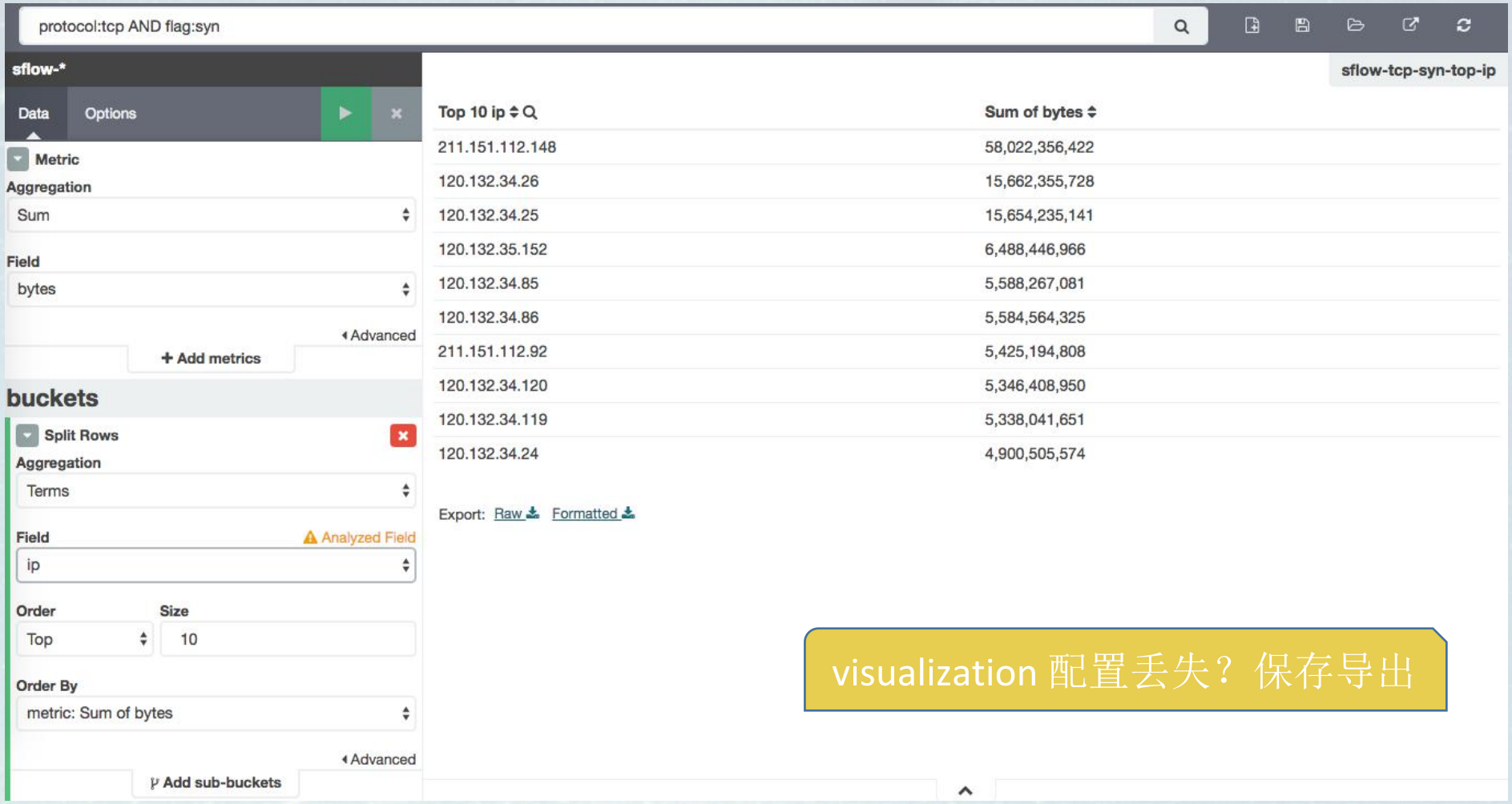
- 流量总量是否在正常范围
- TCP/syn 类流量总量
- UDP 类流量总量
- TCP/syn 类流量数据包总量
- ICMP 类流量
- ……



识别 → 预警 → 防护 → 溯源

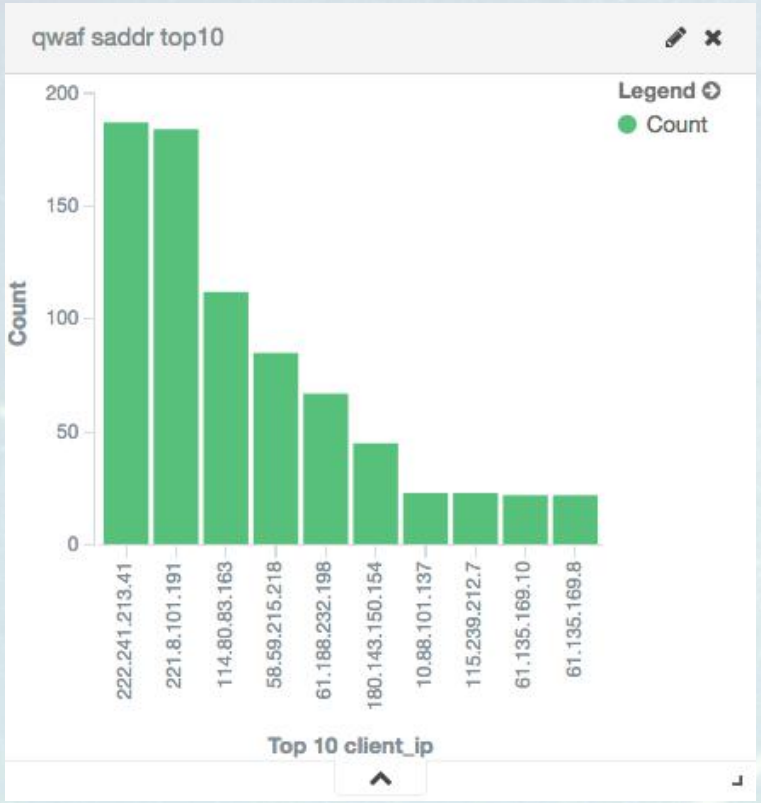
异常流量监控案例

kibana

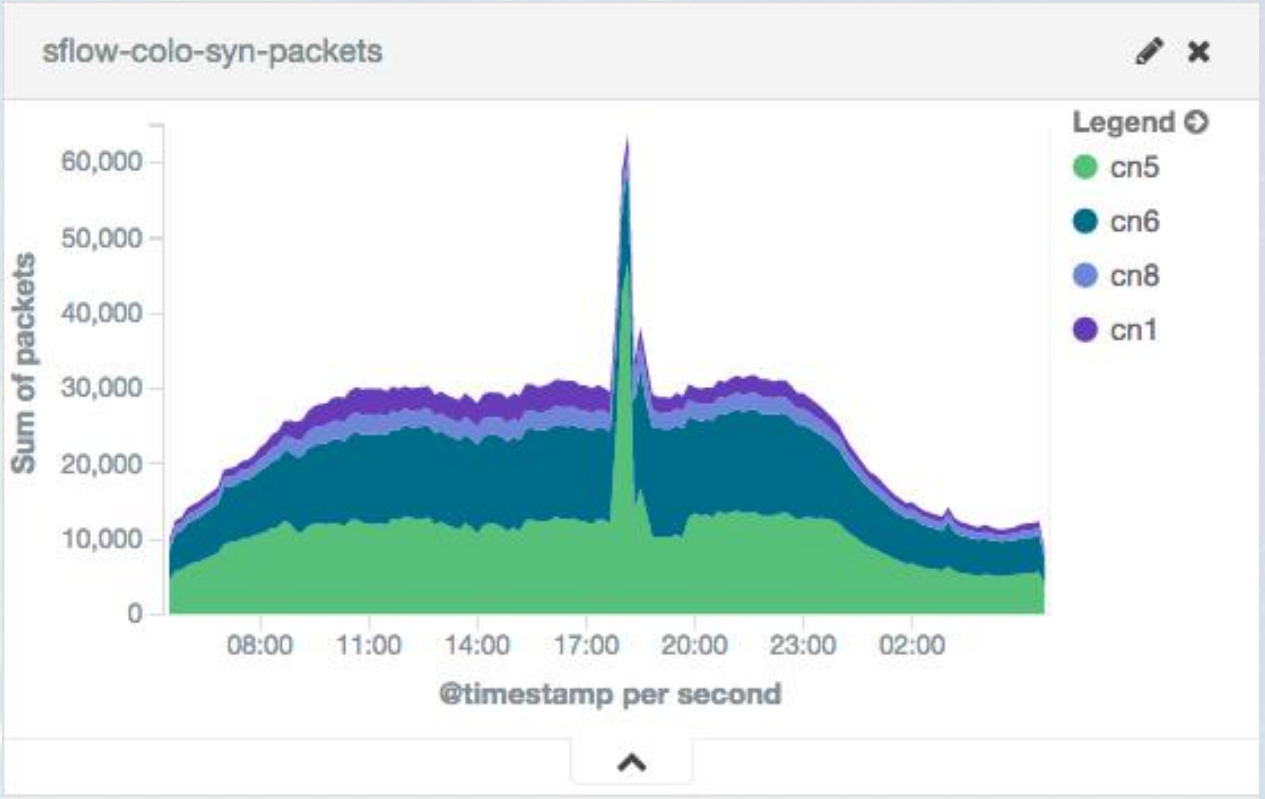


异常流量监控案例

kibana



Qwaf top 10 saddr evil ip



Sflow 检测到 syn flood DDOS

异常行为监控案例

网络行为

- 内网渗透行为
- 内网漏洞扫描行为
- 内网信息探测行为
- 检测无线路由器
- ……

- 进入内网
- 主机发现
- 端口扫描
- 漏洞检测

异常行为监控案例

分词失效？设置成空白字符

Table JSON Bash

@timestamp	July 7th 2016, 15:49:48.000
@version	1
_id	AVXEVY5TZ-gCpHI4V9NP
_index	bash-2016.07
_type	bash
cmd	sudo chmod a+x testtesttest.sh
execuser	xiangcen.bao
hostname	l-fangzhen18.f.dev.cn0
pid	25604
pwd	/home/q/tools/bin/publisher
sid	25604
tty	/dev/pts/2
type	bash
username	xiangcen.bao

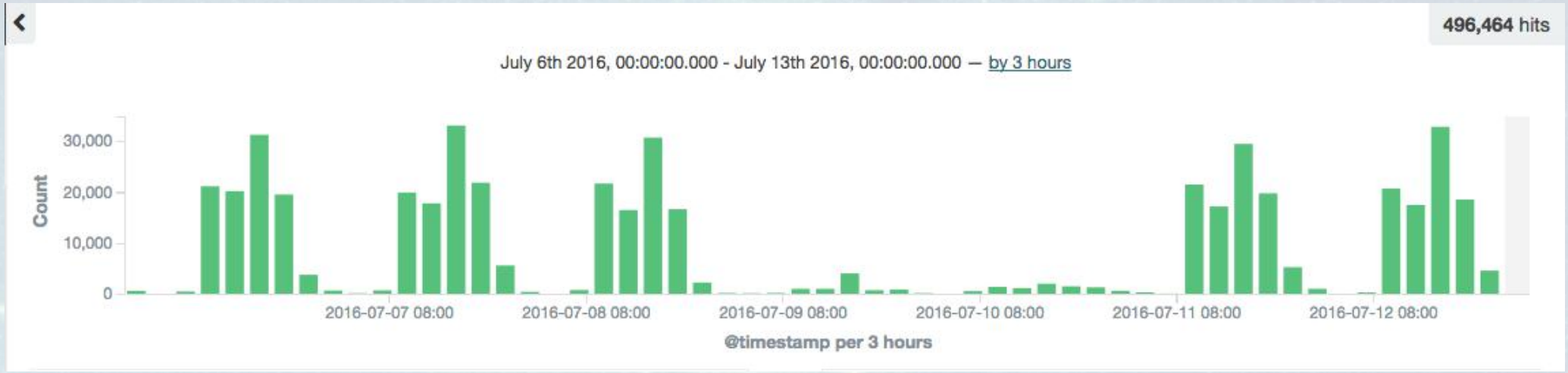
字段类型不匹配？设置 mapping

Table JSON IDS

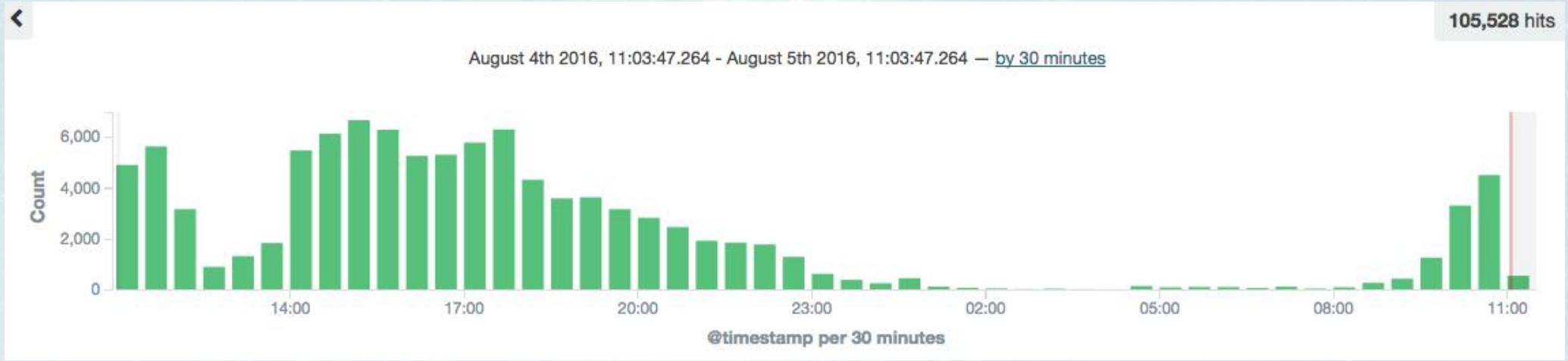
@timestamp	July 7th 2016, 15:49:49.972
@version	1
_id	AVXEVZeRBpz4ULTljhJH
_index	ids-2016.07.07
_type	ids
dest_ip	192.168.224.43
dest_port	80
src_ip	10.89.131.60
src_port	58,842
ttl	60
type	ids

异常行为监控案例

kibana

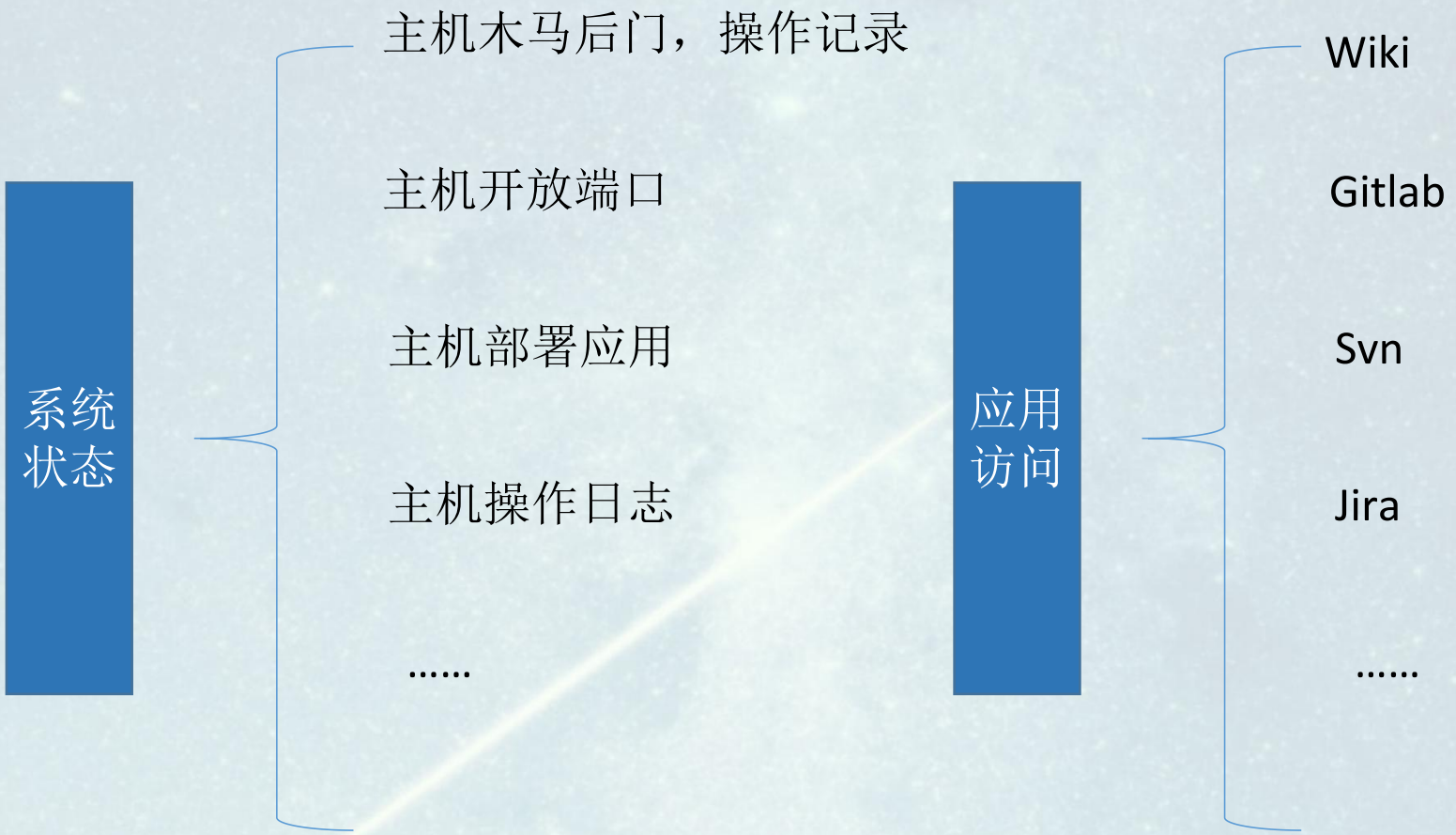


主机操作周记录统计



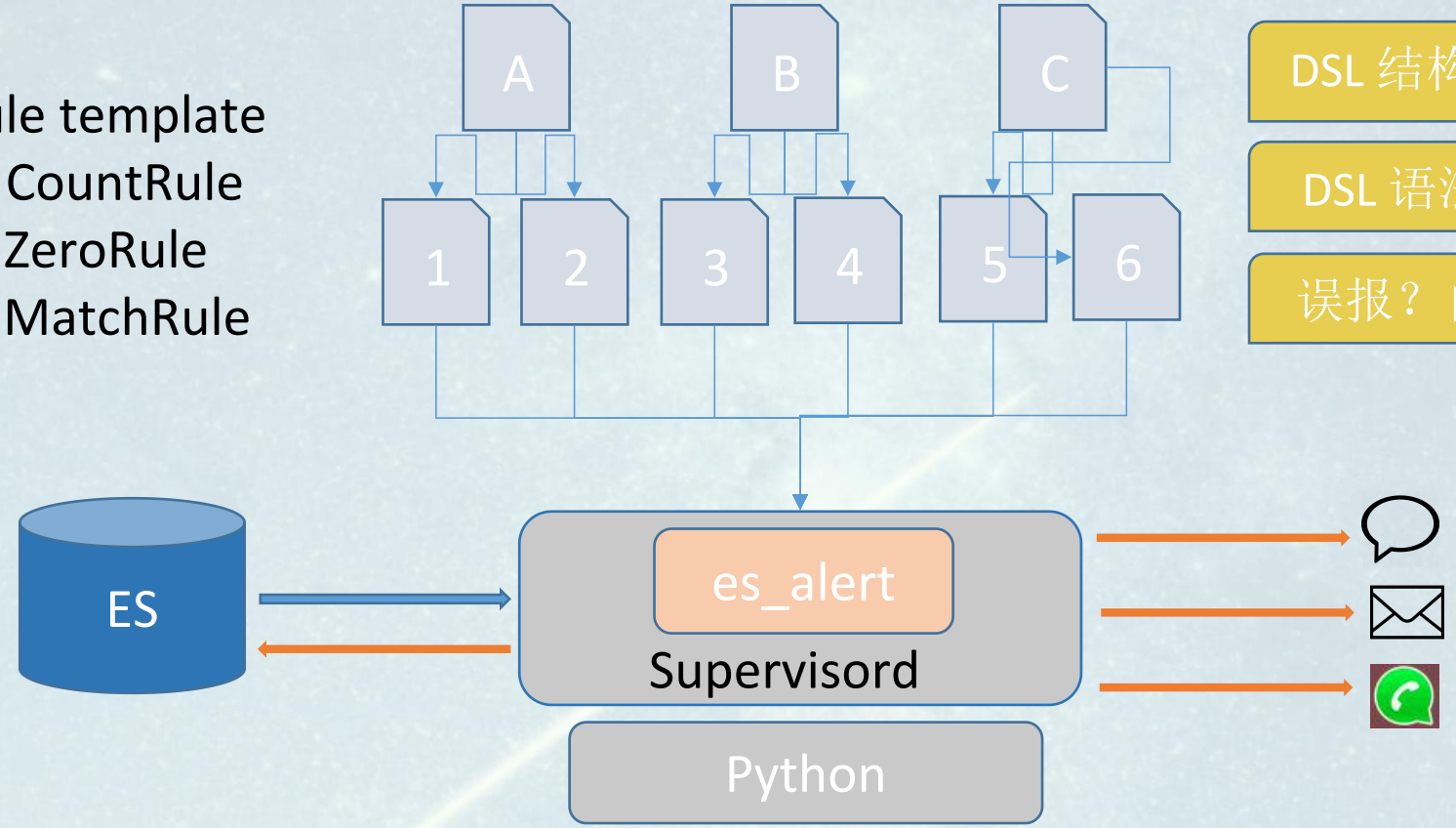
主机操作日记录统计

其他安全监控场景


系统状态
主机木马后门，操作记录
主机开放端口
主机部署应用
主机操作日志
……
应用访问
Wiki
Gitlab
Svn
Jira
……

监控告警实现

Rule template
A: CountRule
B: ZeroRule
C: MatchRule



DSL 结构？对应 json 格式

DSL 语法？注意版本差异

误报？白名单，调整阈值

监控告警实现

CountRule 时序统计告警规则

MatchRule 匹配触发告警规则

ZeroRule 索引异常告警规则

```
type: count

name: syn_flow

index: sflow-*

query: colo

count: bytes

filter:
    flag: syn

thresholds:
    default: 40 * 1024 * 1024 / 8

unit: 1024 * 1024

alert_to:
    - xxx.xxx
    - xxx.xxx

alert_type:
    - qtalk
    - mail
    - mobile

# {0} is query value, {1} is count(default is doc_count) sum
alert_content: syn flow in {0} over {1}MB/s
```

Syn flow count rule

新方案优势

- 数据接入统一
- 扩展能力增强
- 集中监控，统一告警
- 可视化，便于人工分析
- 监控独立，告警事件
- 数据备份，可用于审计


THANKS
Q&A