

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



* 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

异常
流量

异常
行为

数据
查删

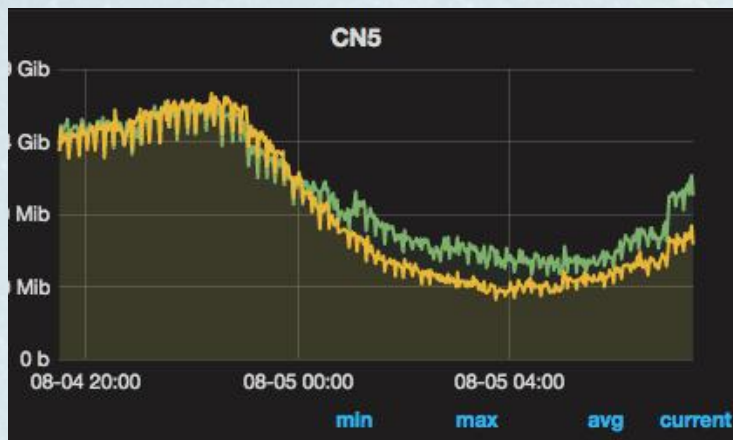
系统
状态

DNS
解析

登录
注册

安全
事件

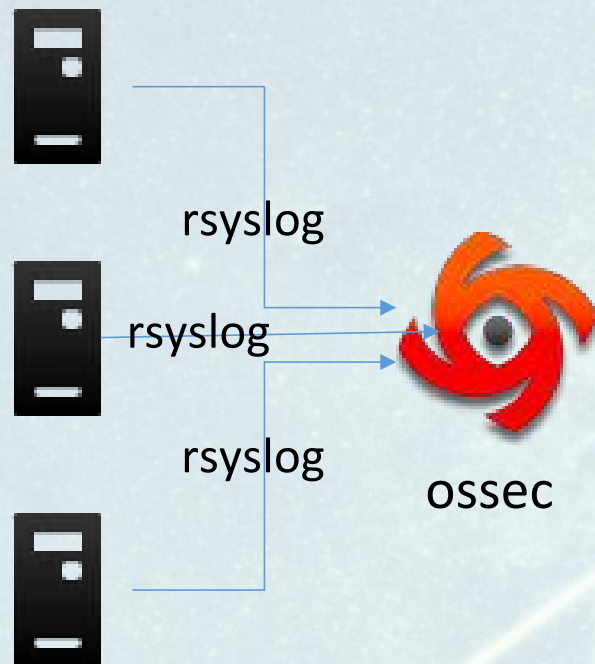
....



利用 Watcher 监控分析网络流量



利用 Suricata 监控网络行为



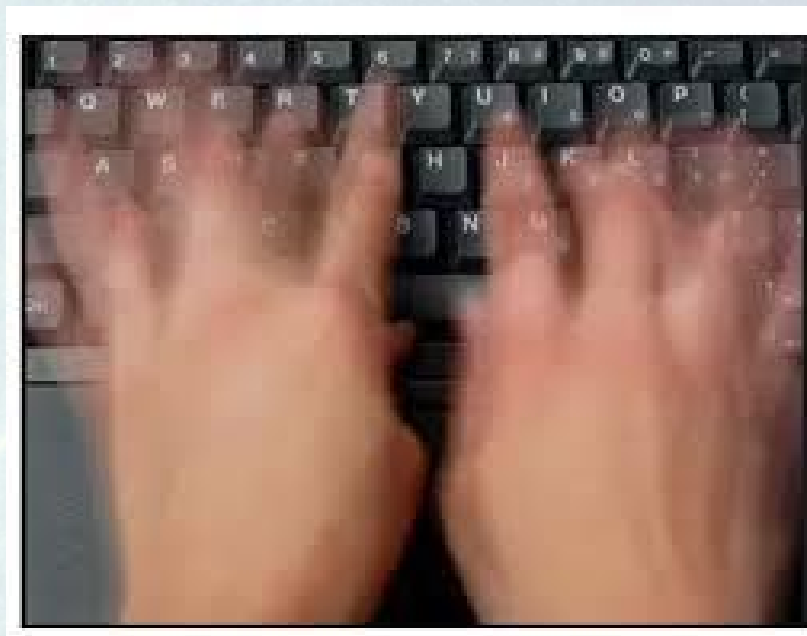
利用 Ossec 分析主机日志

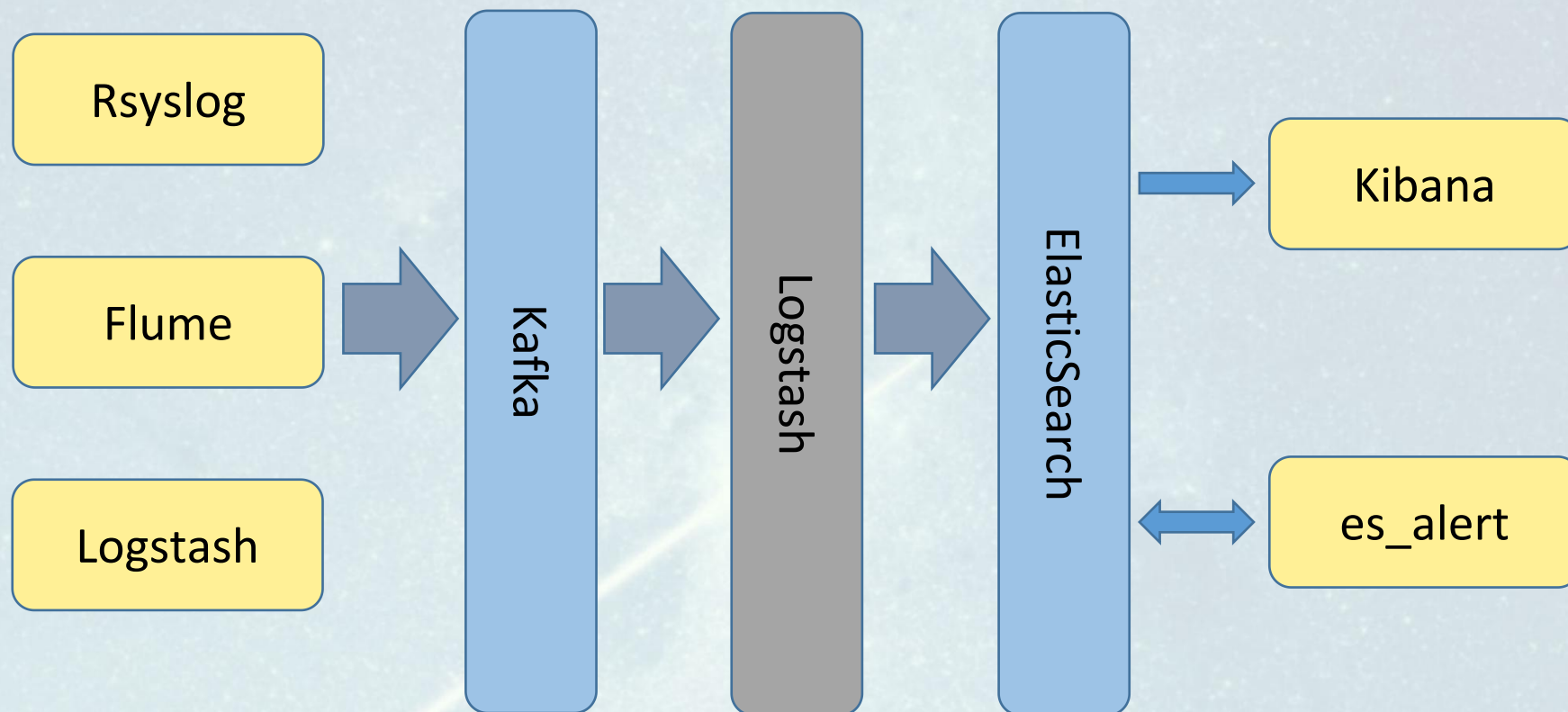


利用 Python 分析 Web 日志

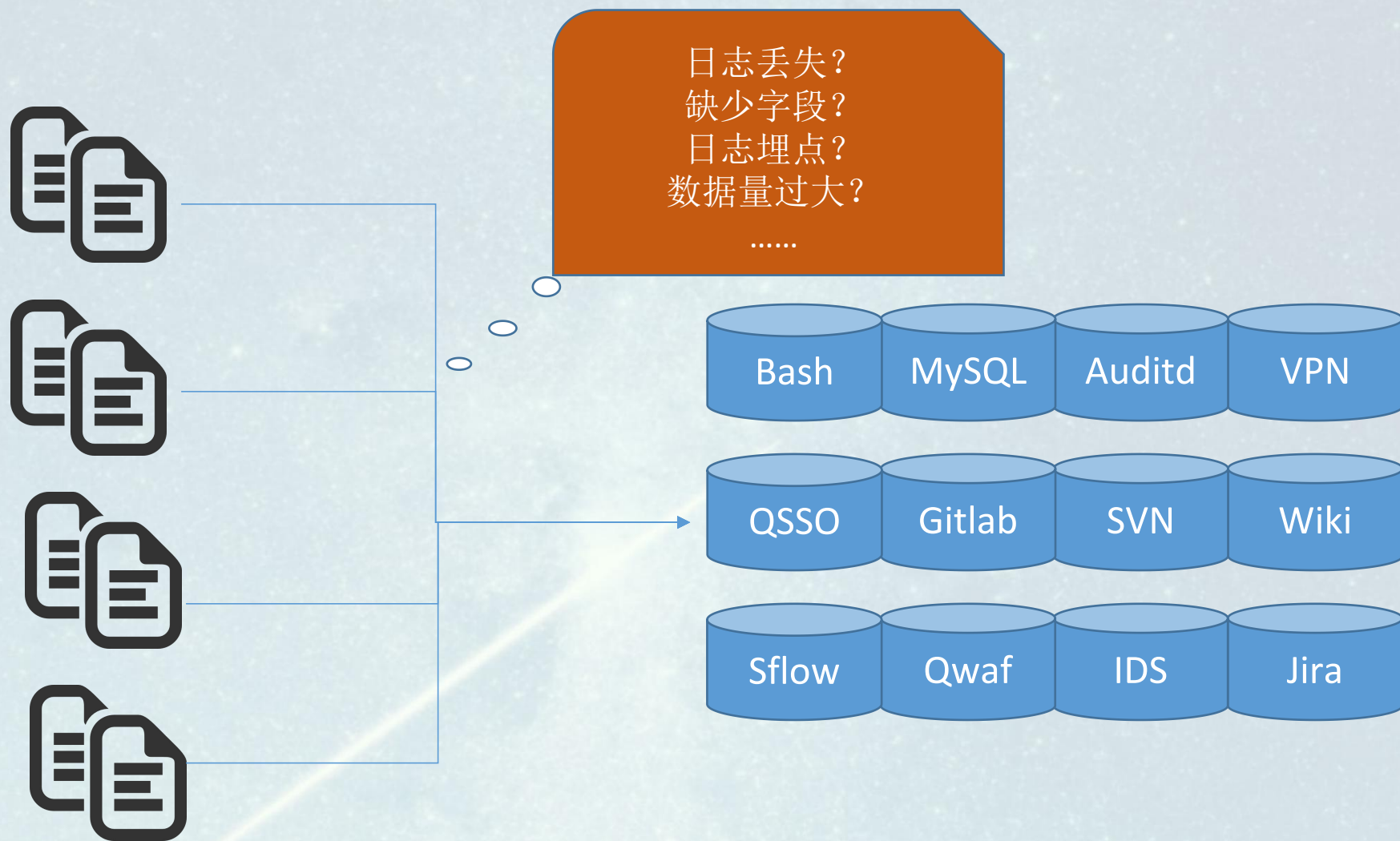


- 监控分散，各部分独立
- 难以扩展，无法复用
- 历史数据保存问题
- 缺少可视化分析
- 人工成本高





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

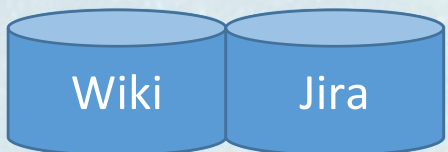




.history 内容? No, patch 埋点



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

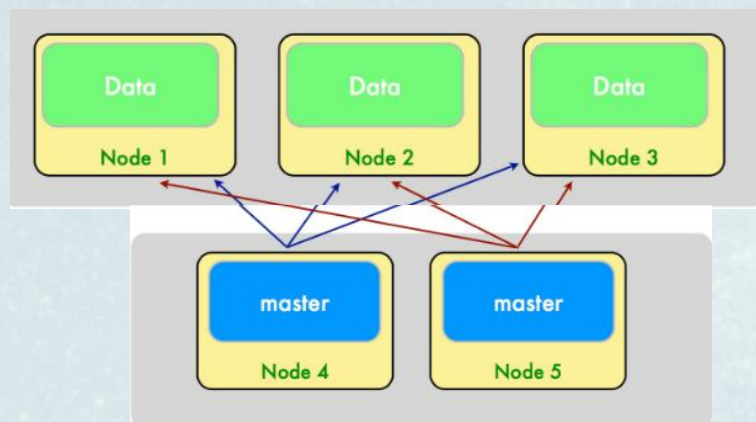
输出错误？rubydebug 调试

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

网络
流量

流量总量是否在正常范围

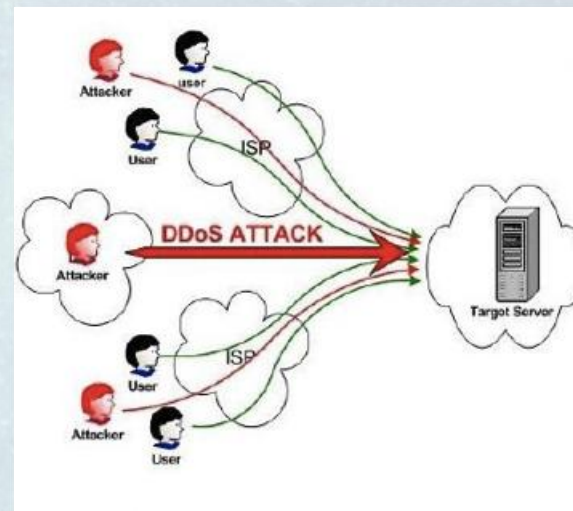
TCP/syn 类流量总量

UDP 类流量总量

TCP/syn 类流量数据包总量

ICMP 类流量

.....

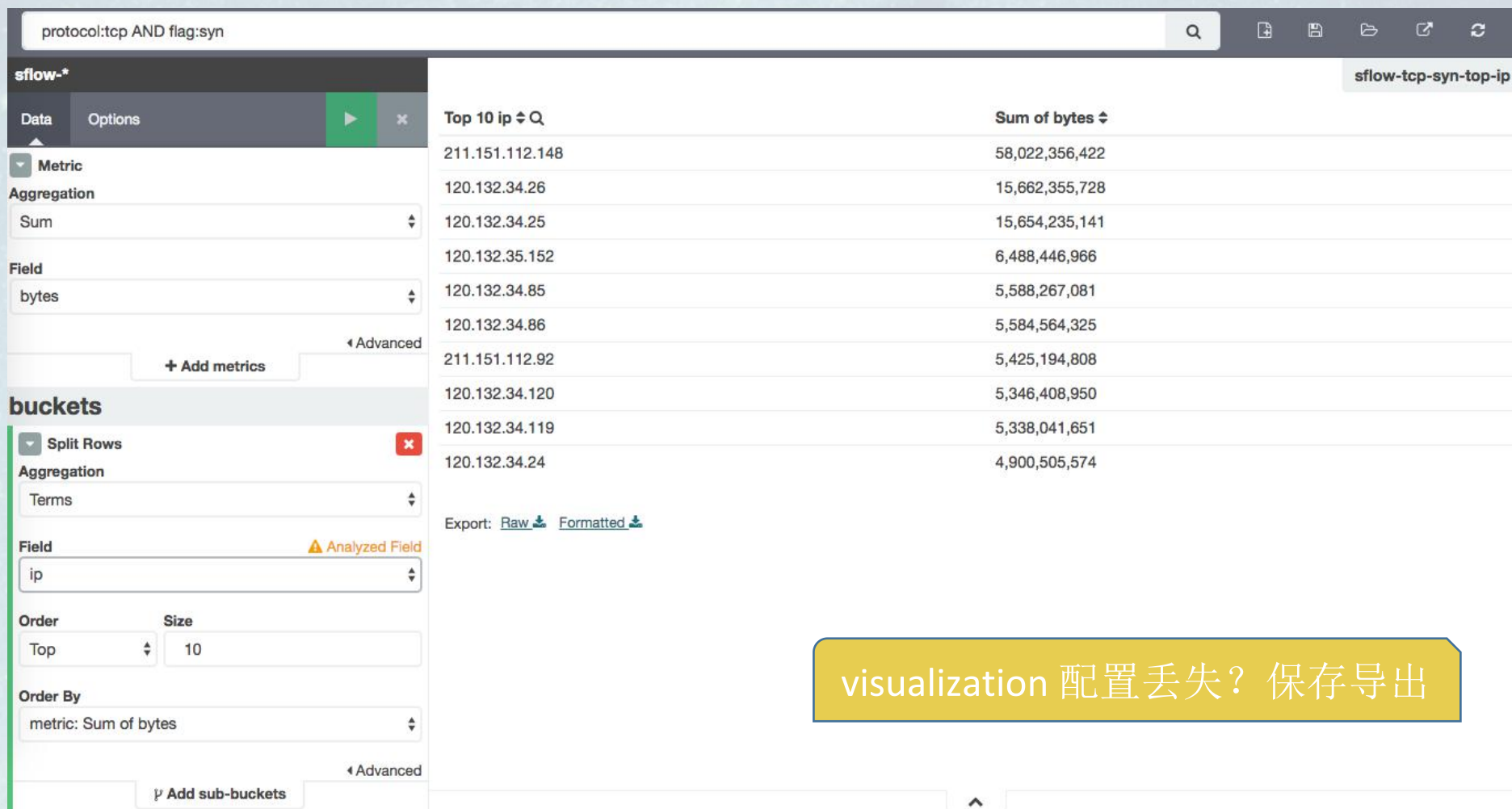


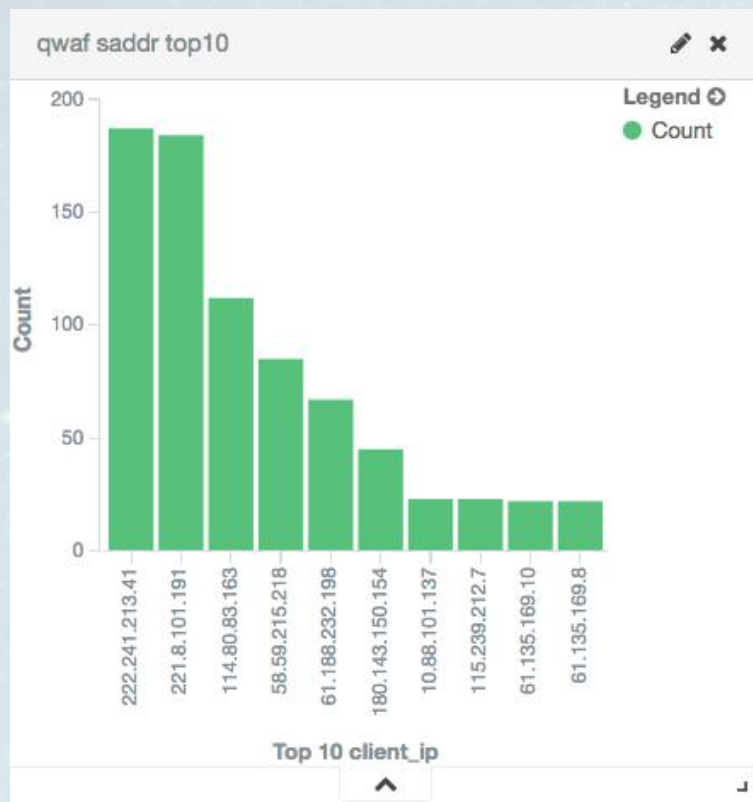
识别

预警

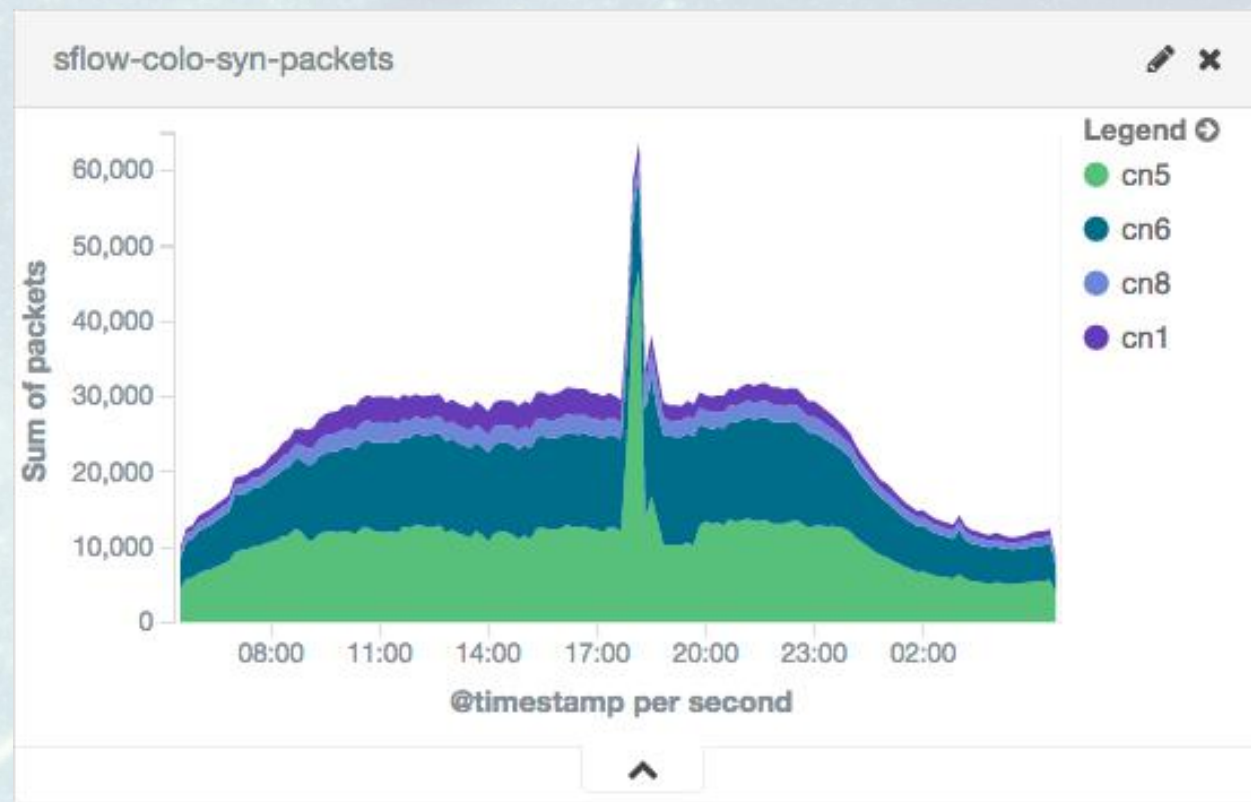
防护

溯源





Qwaf top 10 saddr evil ip



Sflow 检测到 syn flood DDOS

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

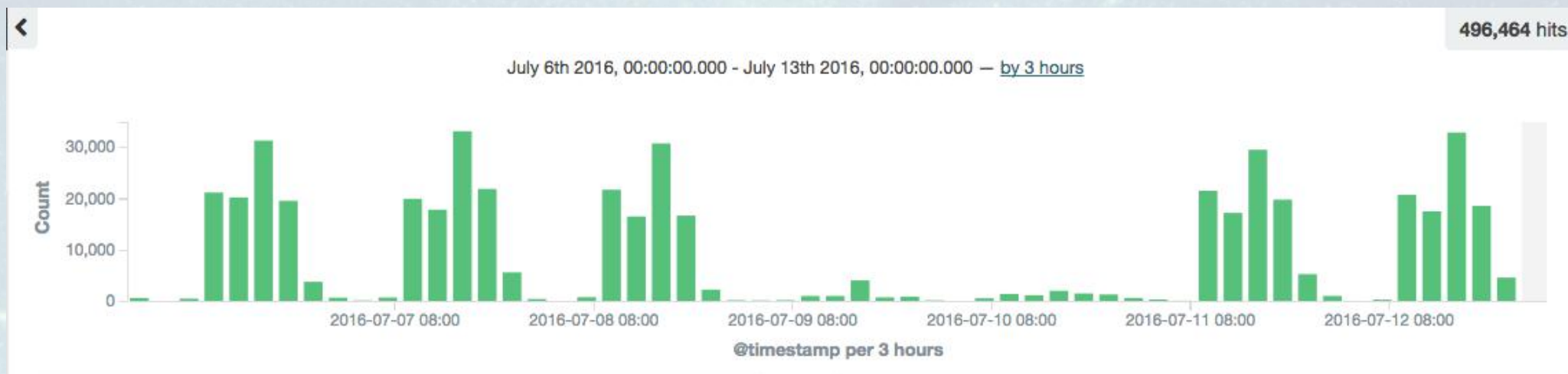
漏洞检测

分词失效？设置成空白字符

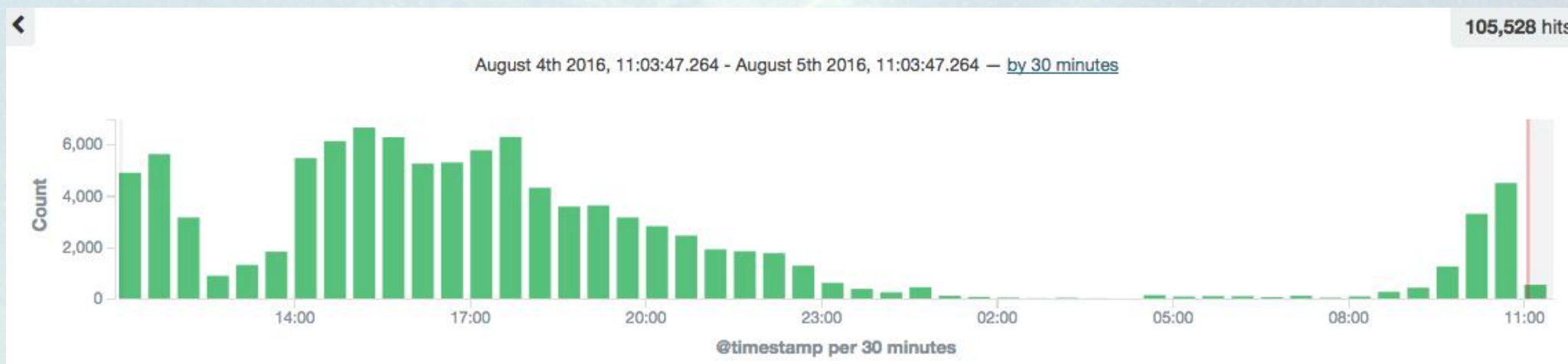
Table	JSON	Bash
@timestamp	🔍 🔍 📅	July 7th 2016, 15:49:48.000
t @version	🔍 🔍 📅	1
t _id	🔍 🔍 📅	AVXEY5TZ-gCpHI4V9NP
t _index	🔍 🔍 📅	bash-2016.07
t _type	🔍 🔍 📅	bash
t cmd	🔍 🔍 📅	sudo chmod a+x testtesttest.sh
t execuser	🔍 🔍 📅	xiangcen.bao
t hostname	🔍 🔍 📅	l-fangzhen18.f.dev.cn0
t pid	🔍 🔍 📅	25604
t pwd	🔍 🔍 📅	/home/q/tools/bin/publisher
t sid	🔍 🔍 📅	25604
t tty	🔍 🔍 📅	/dev/pts/2
t type	🔍 🔍 📅	bash
t username	🔍 🔍 📅	xiangcen.bao

字段类型不匹配？设置 mapping

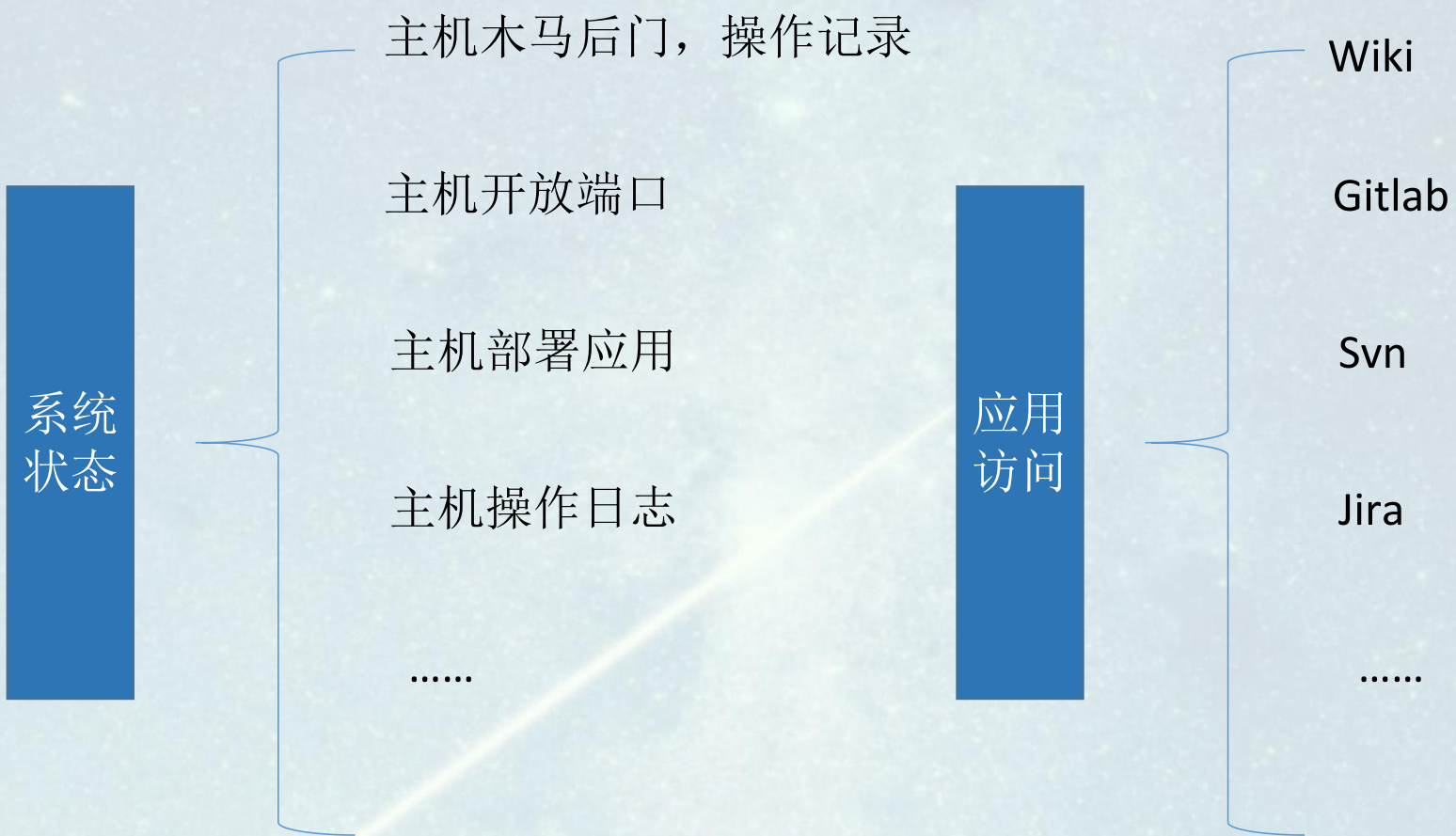
Table	JSON	IDS
@timestamp	🔍 🔍 📅	July 7th 2016, 15:49:49.972
t @version	🔍 🔍 📅	1
t _id	🔍 🔍 📅	AVXEVZeRBpz4ULTljhJH
t _index	🔍 🔍 📅	ids-2016.07.07
t _type	🔍 🔍 📅	ids
t dest_ip	🔍 🔍 📅	192.168.224.43
# dest_port	🔍 🔍 📅	80
t src_ip	🔍 🔍 📅	10.89.131.60
# src_port	🔍 🔍 📅	58,842
# ttl	🔍 🔍 📅	60
t type	🔍 🔍 📅	ids



主机操作周记录统计



主机操作日记录统计



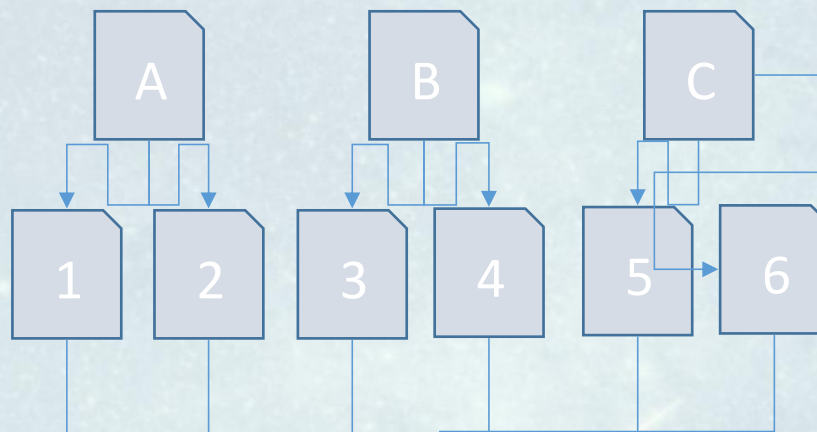


Rule template

A: CountRule

B: ZeroRule

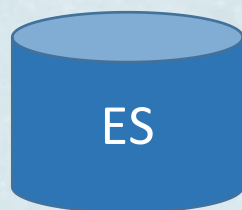
C: MatchRule



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



es_alert
Supervisord

Python





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



- 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



The background is a deep teal and blue space scene. It is filled with numerous small, bright white stars of varying sizes. A prominent, bright yellow-green comet streak with a long tail enters from the bottom left, moving towards the center. The overall texture is grainy, resembling a high-quality astronomical photograph.

THANKS
Q&A