中小企业公有云的安全挑战及威胁情报的结合

轻松筹 韩晋

国内主流公有云安全防护的优缺点

中小互联网企业特点

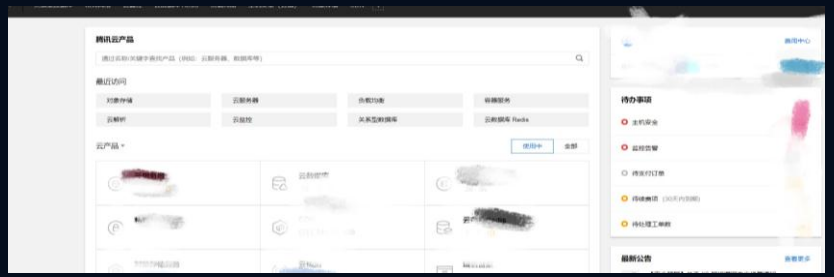
专职安全人员少
预算有限

公有云上安全优点

资产管理成本降低，api获取及配置资产
故障恢复相对快速
部分基础设施风险可降低及转移

公有云上安全缺点

大多数管理操作都要走公网
大部分公有云的账户审计功能较弱
子账户及AK的访问控制粒度不足



公有云中安全防护重点

子账号访问控制

角色：
开发、测试、运维、安全、
大数据
市场、运营、产品
甚至客服

公网访问，无法限制登陆地
点

公有云中安全防护重点

操作审计&报警

AccessKey:
AccessKey ID+Secret可直接访问，大多数功能无ip白名单限制

```
-rwxrwxrwx 1 root root 612 Jan  1  2018 Actiontrail_cn-hangzhou_20171231225153_1002_7_612
-rwxrwxrwx 1 root root 613 Jan  1  2018 Actiontrail_cn-hangzhou_20171231225153_1002_7_613
-rwxrwxrwx 1 root root 643 Jan  1  2018 Actiontrail_cn-hangzhou_20171231225153_1002_8_643
-rwxrwxrwx 1 root root 378 Jan  1  2018 Actiontrail_cn-hangzhou_20171231225155_1002_1_378
-rwxrwxrwx 1 root root 376 Jan  1  2018 Actiontrail_cn-hangzhou_20171231230018_1002_1_376
-rwxrwxrwx 1 root root 380 Jan  1  2018 Actiontrail_cn-hangzhou_20171231230056_1002_1_380
-rwxrwxrwx 1 root root 422 Jan  1  2018 Actiontrail_cn-hangzhou_20171231230056_1002_2_422
-rwxrwxrwx 1 root root 425 Jan  1  2018 Actiontrail_cn-hangzhou_20171231230056_1002_2_425
-rwxrwxrwx 1 root root 466 Jan  1  2018 Actiontrail_cn-hangzhou_20171231230056_1002_3_466
-rwxrwxrwx 1 root root 374 Jan  1  2018 Actiontrail_cn-hangzhou_20171231230057_1002_1_374
-rwxrwxrwx 1 root root 379 Jan  1  2018 Actiontrail_cn-hangzhou_20171231230057_1002_1_379
-rwxrwxrwx 1 root root 378 Jan  1  2018 Actiontrail_cn-hangzhou_20171231230404_1002_1_378
-rwxrwxrwx 1 root root 375 Jan  1  2018 Actiontrail_cn-hangzhou_20171231230635_1002_1_375
-rwxrwxrwx 1 root root 376 Jan  1  2018 Actiontrail_cn-hangzhou_20171231231249_1002_1_376
-rwxrwxrwx 1 root root 421 Jan  1  2018 Actiontrail_cn-hangzhou_20171231231923_1002_2_421
-rwxrwxrwx 1 root root 378 Jan  1  2018 Actiontrail_cn-hangzhou_20171231231929_1002_1_378
-rwxrwxrwx 1 root root 377 Jan  1  2018 Actiontrail_cn-hangzhou_20171231232048_1002_1_377
-rwxrwxrwx 1 root root 375 Jan  1  2018 Actiontrail_cn-hangzhou_20171231232058_1002_1_375
-rwxrwxrwx 1 root root 427 Jan  1  2018 Actiontrail_cn-hangzhou_20171231232309_1002_2_427
-rwxrwxrwx 1 root root 379 Jan  1  2018 Actiontrail_cn-hangzhou_20171231232327_1002_1_379
-rwxrwxrwx 1 root root 379 Jan  1  2018 Actiontrail_cn-hangzhou_20171231232334_1002_1_379
-rwxrwxrwx 1 root root 379 Jan  1  2018 Actiontrail_cn-hangzhou_20171231232355_1002_1_379
-rwxrwxrwx 1 root root 377 Jan  1  2018 Actiontrail_cn-hangzhou_20171231232546_1002_1_377
-rwxrwxrwx 1 root root 379 Jan  1  2018 Actiontrail_cn-hangzhou_20171231232546_1002_1_379
-rwxrwxrwx 1 root root 380 Jan  1  2018 Actiontrail_cn-hangzhou_20171231233000_1002_1_380
-rwxrwxrwx 1 root root 375 Jan  1  2018 Actiontrail_cn-hangzhou_20171231233101_1002_1_375
-rwxrwxrwx 1 root root 375 Jan  1  2018 Actiontrail_cn-hangzhou_20171231233101_1002_1_375
-rwxrwxrwx 1 root root 425 Jan  1  2018 Actiontrail_cn-hangzhou_20171231233101_1002_2_425
-rwxrwxrwx 1 root root 380 Jan  1  2018 Actiontrail_cn-hangzhou_20171231233418_1002_1_380
-rwxrwxrwx 1 root root 375 Jan  1  2018 Actiontrail_cn-hangzhou_20171231233423_1002_1_375
-rwxrwxrwx 1 root root 379 Jan  1  2018 Actiontrail_cn-hangzhou_20171231233513_1002_1_379
-rwxrwxrwx 1 root root 378 Jan  1  2018 Actiontrail_cn-hangzhou_20171231234555_1002_1_378
-rwxrwxrwx 1 root root 379 Jan  1  2018 Actiontrail_cn-hangzhou_20171231235155_1002_1_379
-rwxrwxrwx 1 root root 377 Jan  1  2018 Actiontrail_cn-hangzhou_20171231235233_1002_1_377
-rwxrwxrwx 1 root root 378 Jan  1  2018 Actiontrail_cn-hangzhou_20171231235938_1002_1_378
```

公有云中安全防护重点

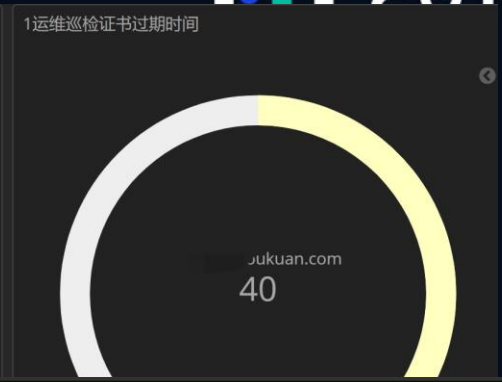
操作审计

日志收集：
Elk+beats

近实时报警：
elasticalert+脚本

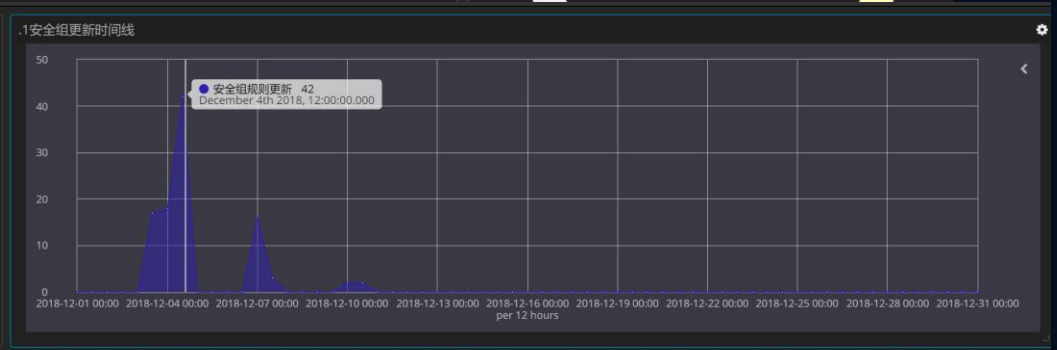
可视化：
Kibana

公有云中安全防护重点



通过公有云厂商的api直接获取：
- 资源变动
- 安全组配置等

自己写代码爬：
- 证书有效期等

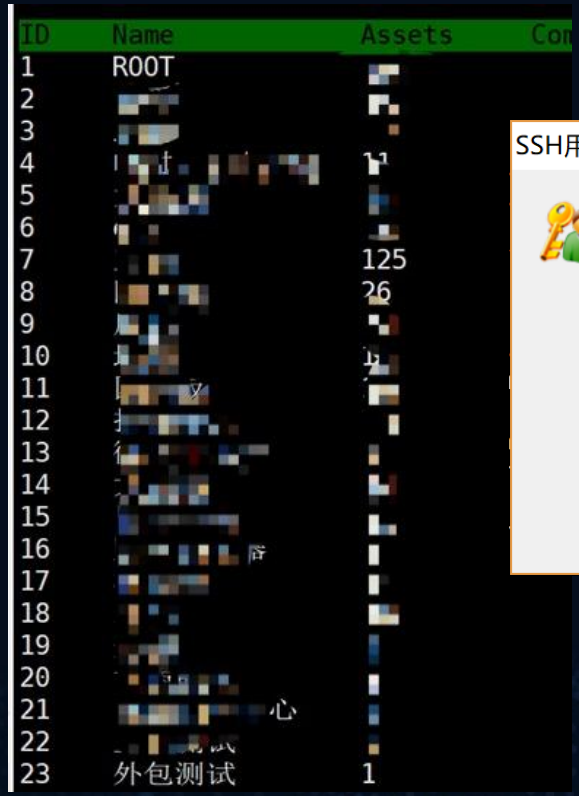


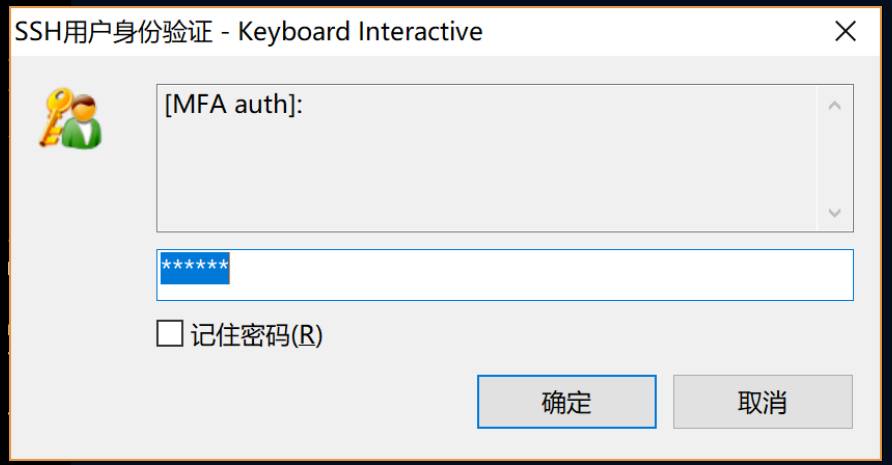
.1安全组入方向风险

对外开放风险地址	所在区域	安全组名称	规则说明	端口	命中数量
0.0.0.0/0	cn-[redacted]	[redacted]安全组	邮件465	30001/30001	8
0.0.0.0/0	cn-[redacted]	[redacted]安全组	邮件465	465/465	8
0.0.0.0/0	cn-[redacted]	[redacted]安全组	22	22/22	8
0.0.0.0/0	cn-[redacted]	[redacted]安全组	邮件110	110/110	8
0.0.0.0/0	cn-[redacted]	[redacted]安全组	邮件测试	-1/-1	8

公有云中安全防护重点

堡垒机：
vpn+Ip白名单
多云跨域
账号接入统一登陆
多因素验证
操作审计（输入输出）





公有云中安全防护重点

堡垒机dashboard：

- 命令活跃度
- 用户活跃度
- 命令top
- 最新命令
- 高危命令

公有云各种日志收集

统一登陆的必要性

各系统操作审计日志、访问日志

Git泄露、代码审计、构建日志

EDR日志

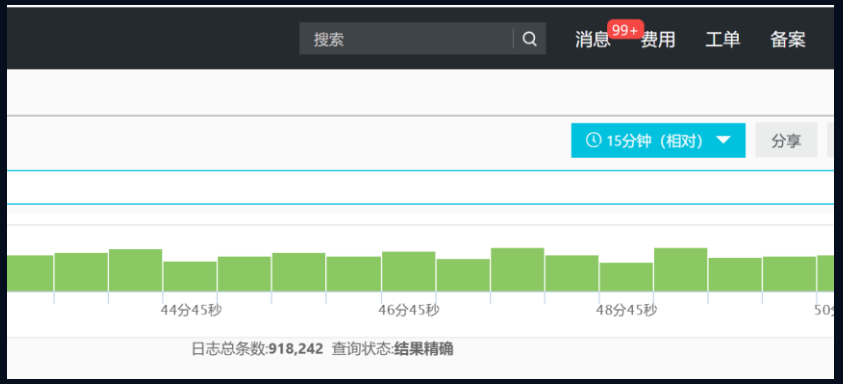
网络流量 with 威胁情报日志

办公网登陆、访问日志

公有云各种日志收集

满足日常查询、可视化需求，可以用公有云日志服务

日志不仅用来查询，可自建
如安装额外插件、精细化配置、自定义冷热节点，update已有数据等

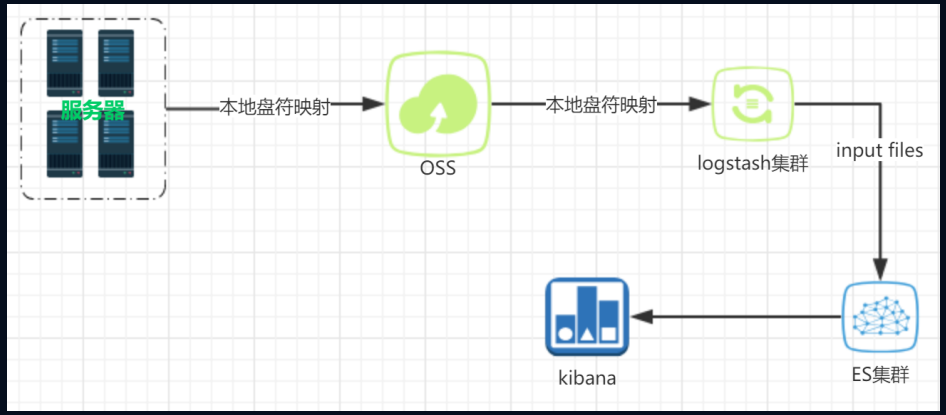


一种公有云日志集中收集的姿势

自建ELK，一种公有云日志集中收集的姿势：

1.所有终端做相应oss bucket盘符映射
2.日志输入映射文件夹
3.创建一台日志服务器映射所有的bucket
4.日志收集在一台服务器配置

不适合高并发读/写的场景，如nginx



- 随机或者追加写文件会导致整个文件的重写。
- 元数据操作，例如list directory，因需要远程访问OSS服务器，因此性能较差。
- 重命名文件/文件夹不属于原子操作。
- 多个客户端挂载同一个OSS bucket时，依赖用户自行协调各个客户端的行为。例如避免多个客户端写同一个文件等。
- 不支持hard link。
- 不适合高并发读/写的场景，这样会让系统的负载升高。

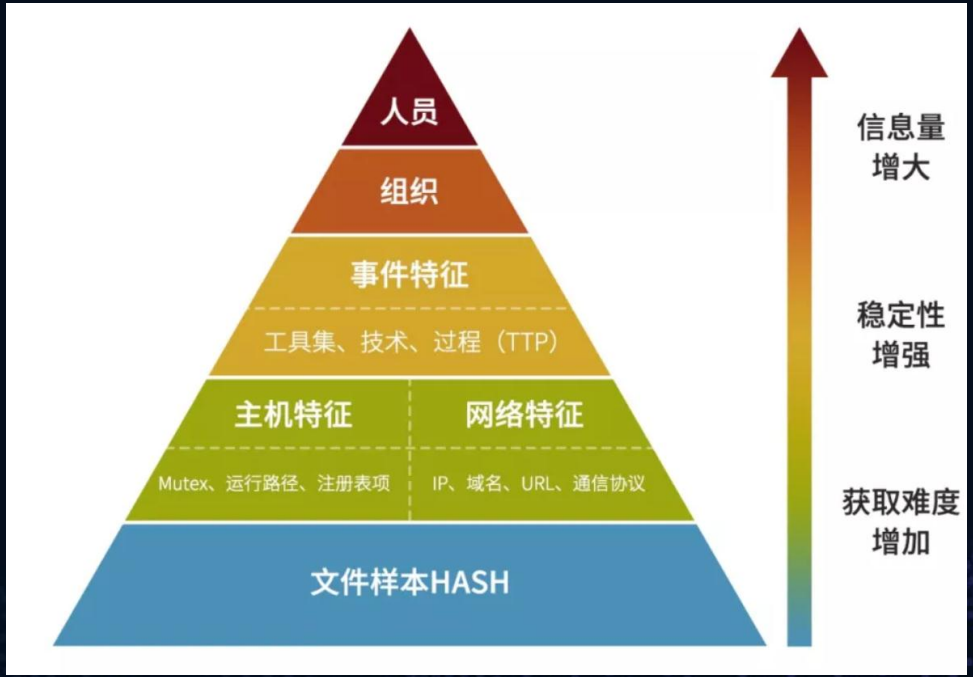
威胁情报在公有云中的使用

定义：

Threat intelligence is evidence-basedknowledge, including context, mechanisms, indicators, implications andactionable advice, about an existing or emerging menace or hazard to assetsthat can be used to inform decisions regarding the subject's response to thatmenace or hazard.

威胁情报是某种基于证据的知识，包括上下文、机制、标示、含义和能够执行的建议，这些知识与资产所面临已有的或酝酿中的威胁或危害相关，可用于对这些威胁或危害进行响应的相关决策提供信息支持。

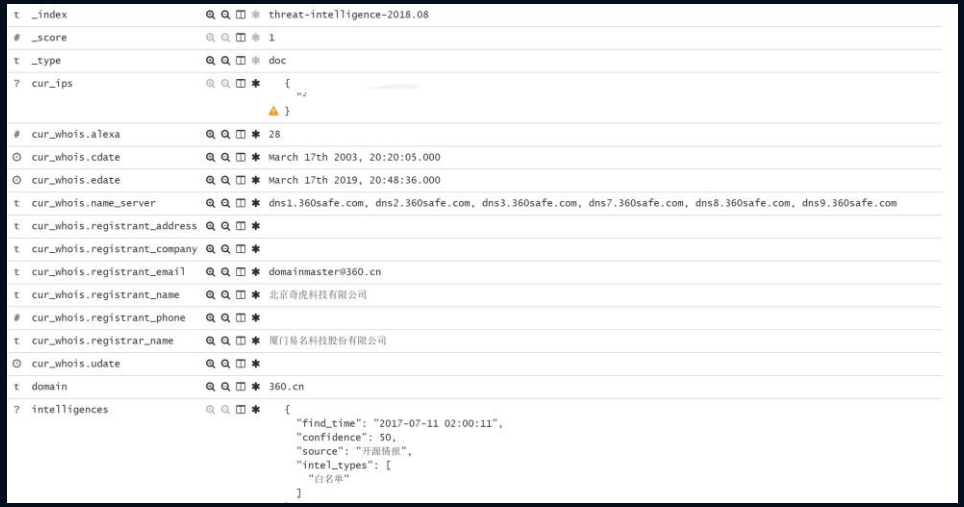
主要关注底部两层



威胁情报在公有云中的使用

威胁情报网络流量采集，2个环境：

- 公有云端
- 办公网



t	_index	threat-intelligence-2018.08
#	_score	1
t	_type	doc
?	cur_ips	{ "2 ⚠ }
#	cur_whois.alexa	28
⊙	cur_whois.cdate	March 17th 2003, 20:20:05.000
⊙	cur_whois.edate	March 17th 2019, 20:48:36.000
t	cur_whois.name_server	dns1.360safe.com, dns2.360safe.com, dns3.360safe.com, dns7.360safe.com, dns8.360safe.com, dns9.360safe.com
t	cur_whois.registrant_address	
t	cur_whois.registrant_company	
t	cur_whois.registrant_email	domainmaster@360.cn
t	cur_whois.registrant_name	北京奇虎科技有限公司
#	cur_whois.registrant_phone	
t	cur_whois.registrar_name	厦门易名科技股份有限公司
⊙	cur_whois.udate	
t	domain	360.cn
?	intelligences	{ "find_time": "2017-07-11 02:00:11", "confidence": 50, "source": "开源情报", "intel_types": ["白名单"]

云端收集关注点：

- 数据流向
- 关键文件hash
- 端口与进程关系
- 公有云控制台操作审计源ip

威胁情报收集在公有云中的阻碍及缓解

公有云无法硬采集流量镜像

几个选择：

- Packet beat
- Xcpoy
- Iptables tee

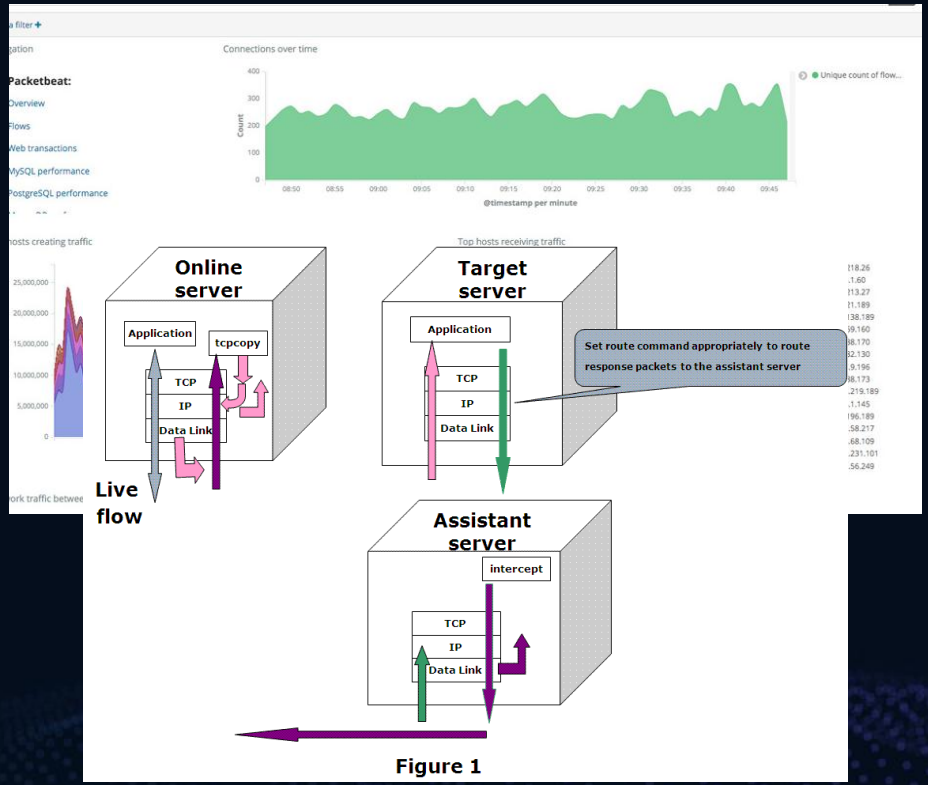


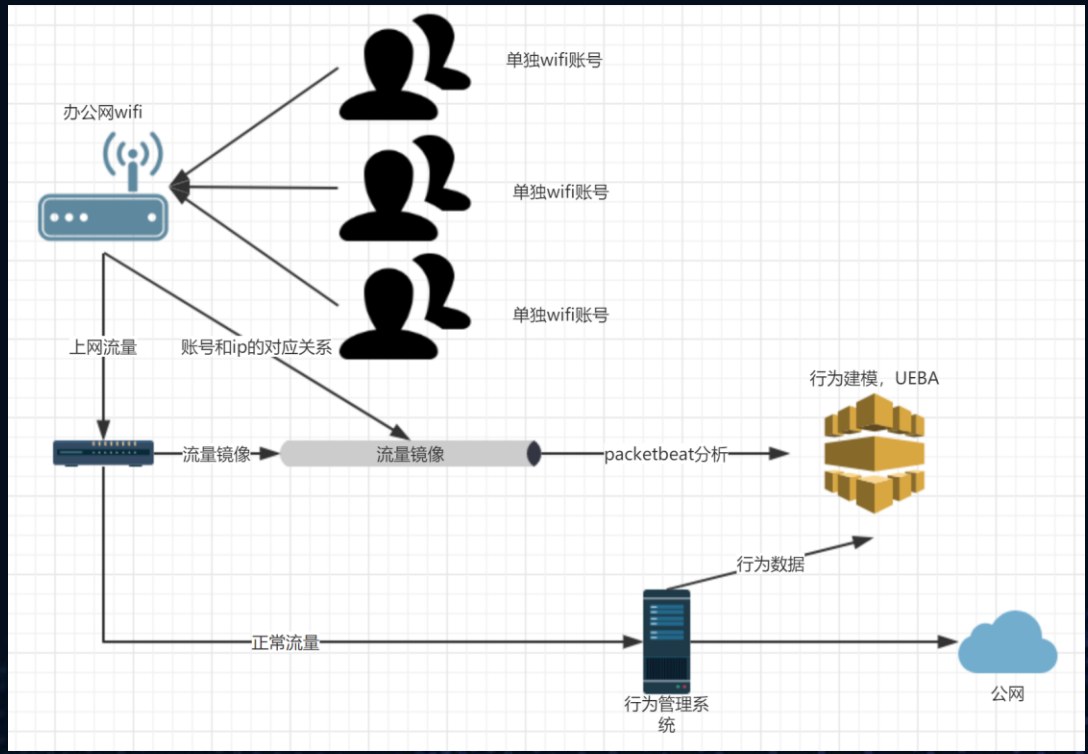
Figure 1

威胁情报在公有云中的使用

威胁情报办公网流量收集：

主端口流量镜像至分析服务器
分析服务器网卡开启混杂模式
运行流量分析工具

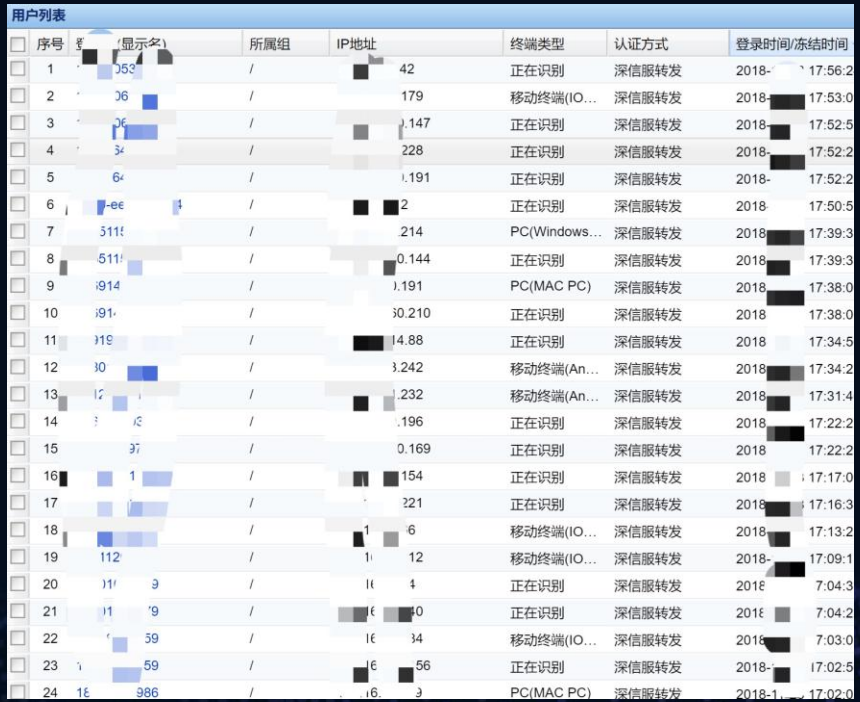
关注点：
访问源ip、目标ip、域名(DN)



威胁情报收集在公有云中的阻碍及缓解

办公网采集的账号与行为记录的问题:

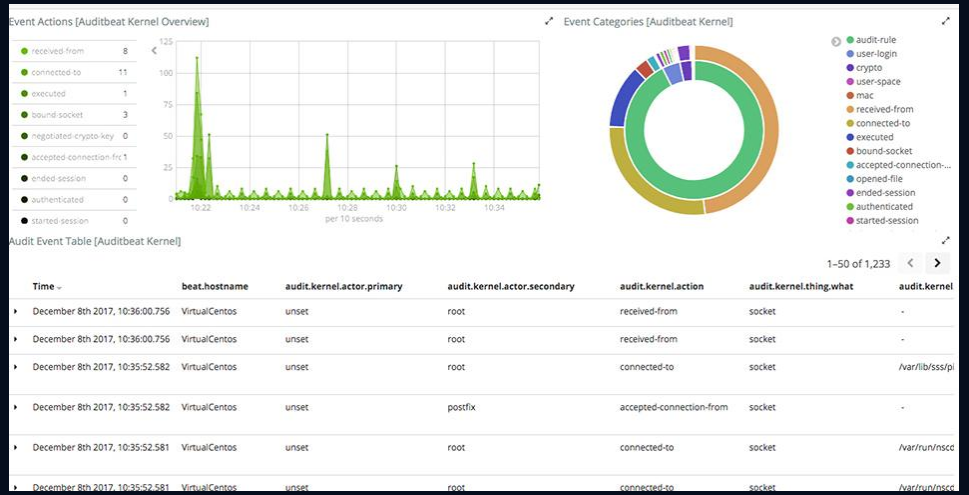
- 需要内网IP和员工的对应关系
- WPA2 企业版 with ldap
- 路由器中对相应用户名分配ip的API
- 上网行为管理数据库（ mysql ）



威胁情报收集、清洗、分析概要

网络端口、进程、文件等信息的采集：

- ossec
- auditbeat
- osquery
- 甚至ansible等



威胁情报收集、清洗、分析概要

收集后统一格式化处理：
Logstash等

处理包括去掉无用信息、精确拆分字段、格式化数据（如转为纯数字0、1、2、3）
最后统一经过kafka进入es集群

后续用途：
作为机器学习的输入维度

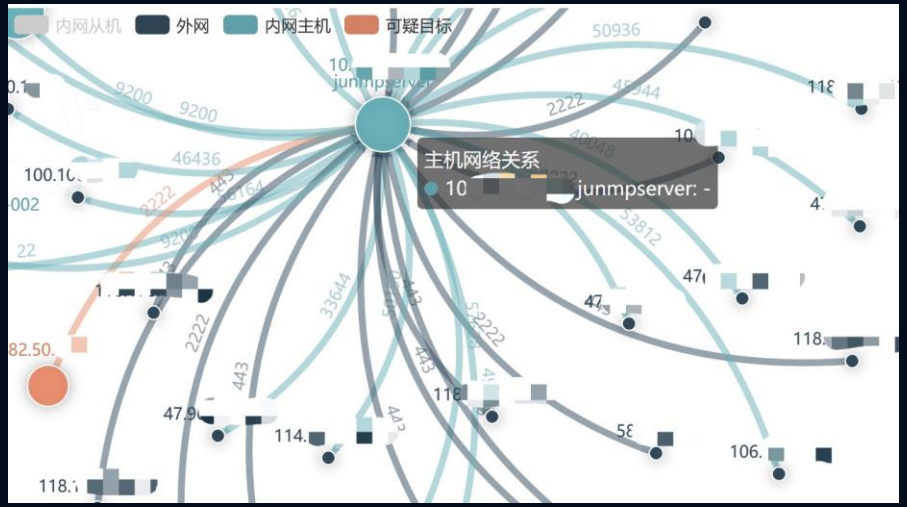
```
    }
    mutate{
       split=>["index_time_tem","T"]
           add_field => {
                   "index_time" =>  ["%{index_time_tem}"]
           }
           remove_field => ["index_time_tem"]
    }
}
if[log_type] == "nginx"{
    grok{
       match => {"messages" => '%{IPORHOST:nginx[remote_addr]} - (%{USER:nginx[remote_user]}|-) \[%{HTTPDATE:ng
 HTTP/%{NUMBER:nginx[httpversion]})" (%{NUMBER:nginx[status]}|-) (%{NUMBER:nginx[body_bytes_sent]}|-) "(%{NOTSPA
o_x_forwarded_for]}|-)"'}
    }
    date{
       match => [ "nginx[time_local]","dd/MMM/yyyy:HH:mm:ss Z" ]
       add_field => { "index_time_tem" => "%{@timestamp}" }
    }
    mutate{
       gsub=> ["index_time_tem","Z","-08:00"]
    }
```

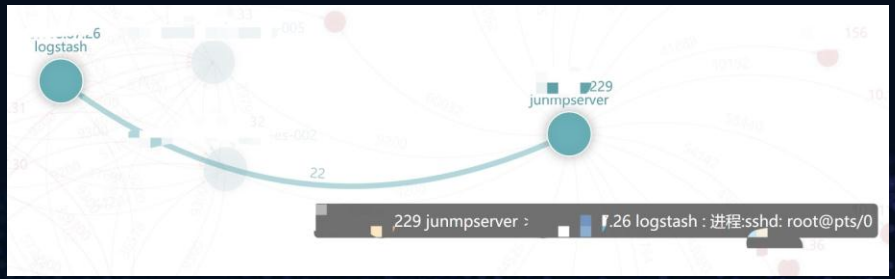
威胁情报收集、清洗、分析概要

公有云网络关系图

基于已完成的功能结合威胁情报制作进程与网络关系图谱

可疑目标高亮可视化筛查





FREEBUF | FIT

THANKS