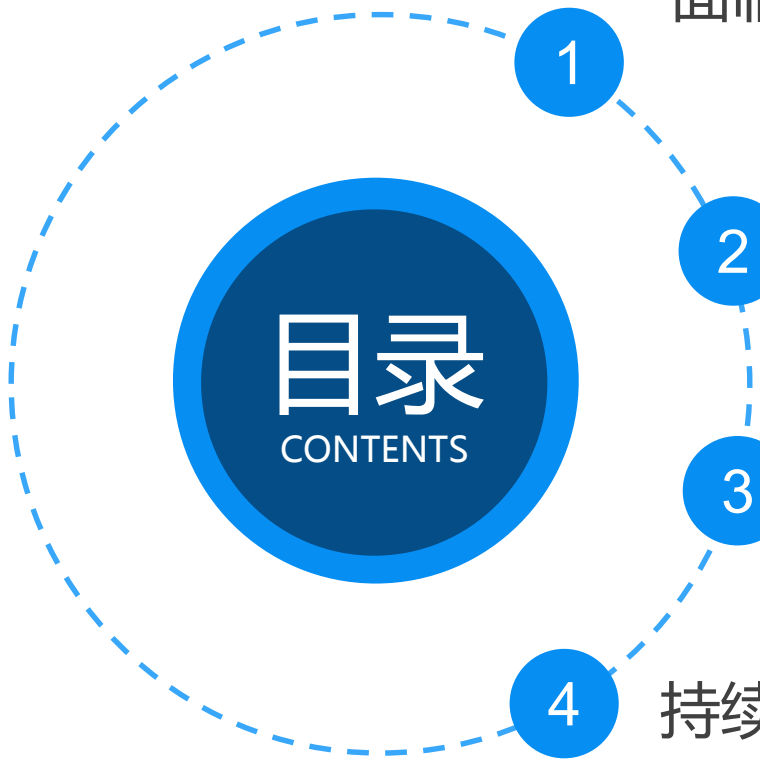
招联金融
MUCFC.COM

WWW.MUCFC.COM

基于Splunk的安全监控系统

企业SIEM经验之谈



/01

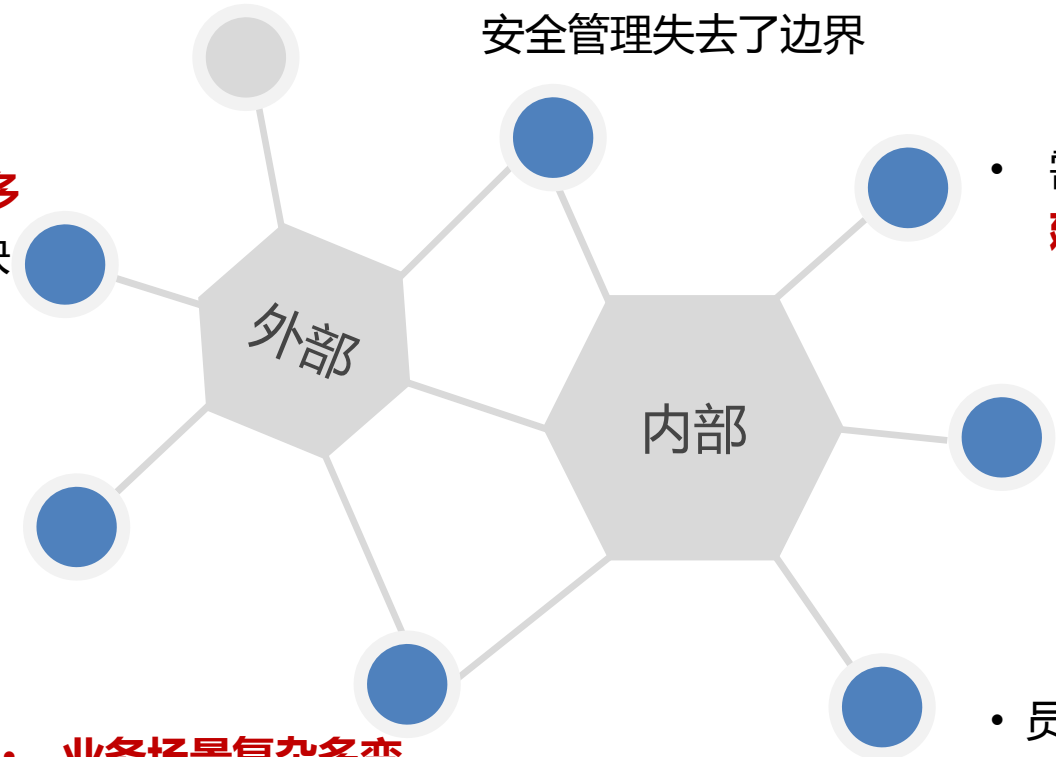
面临哪些问题

面临的核心问题

- **网络边界逐渐消失**
  安全管理失去了边界

- **攻击类型越来越多**
  攻击方法传播更快

- 需加快**自身安全体系的建设**



- 持续的互联网化
  攻击面不断扩大

- **混乱的资产管理**

- **业务场景复杂多变**
  安全控制要随需而变

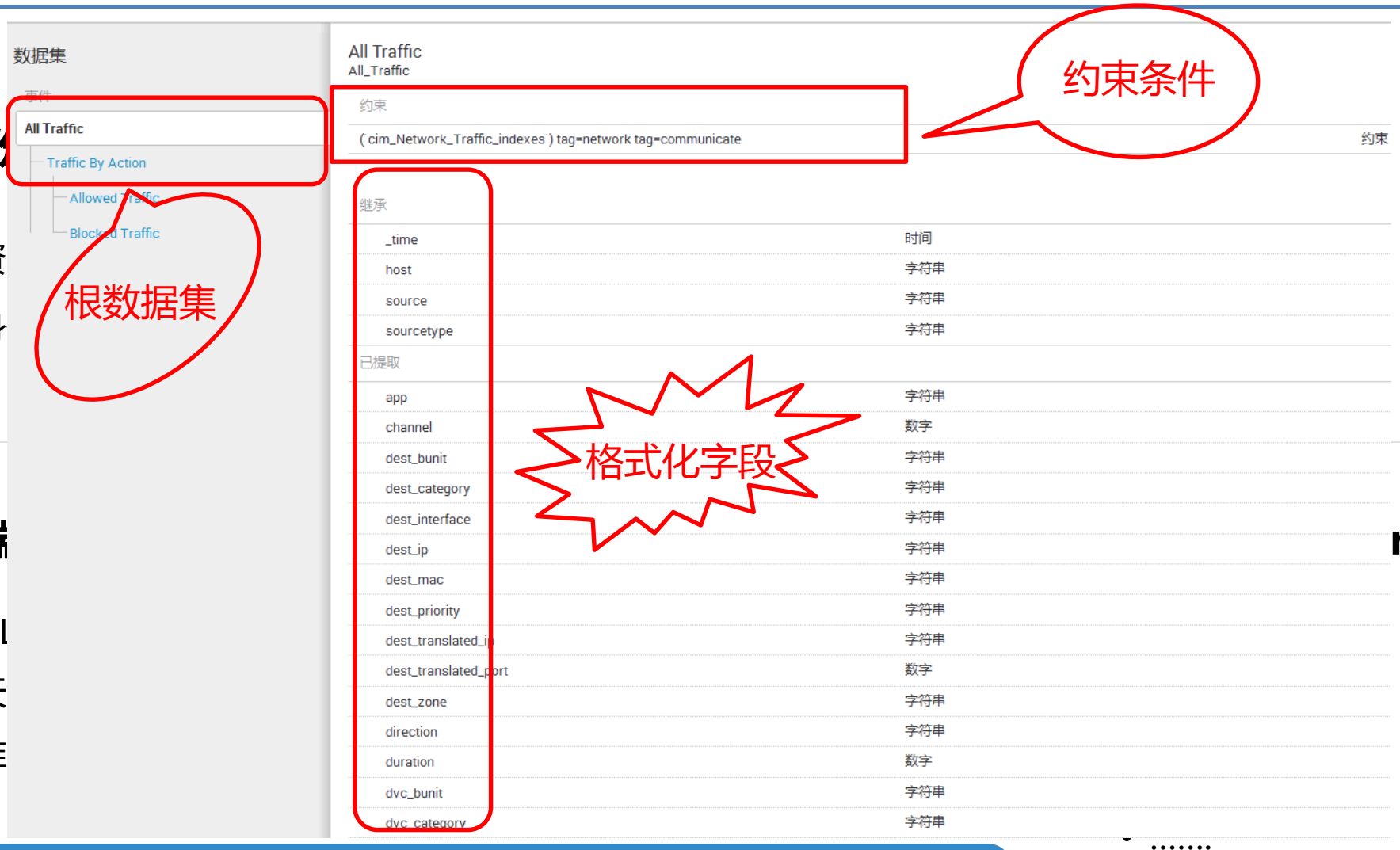
- 员工**行为不可控**

信息不确定	• IP干嘛，不知道 • 服务器啥业务，不知道 • 看到的信息永远都是IP
难以快速实现安全自检	• 跨网络边界 • 海量告警信息 • 多渠道环境
失控的数据信息	• 四通八达的内部环境 • 花样式的数据传输方式

/02 如何解决

- 数据模型
  - 分布式部署

数据模型介绍



身份

- 资
- 身

终端

- DI
- 天
- 准

rk)

.....

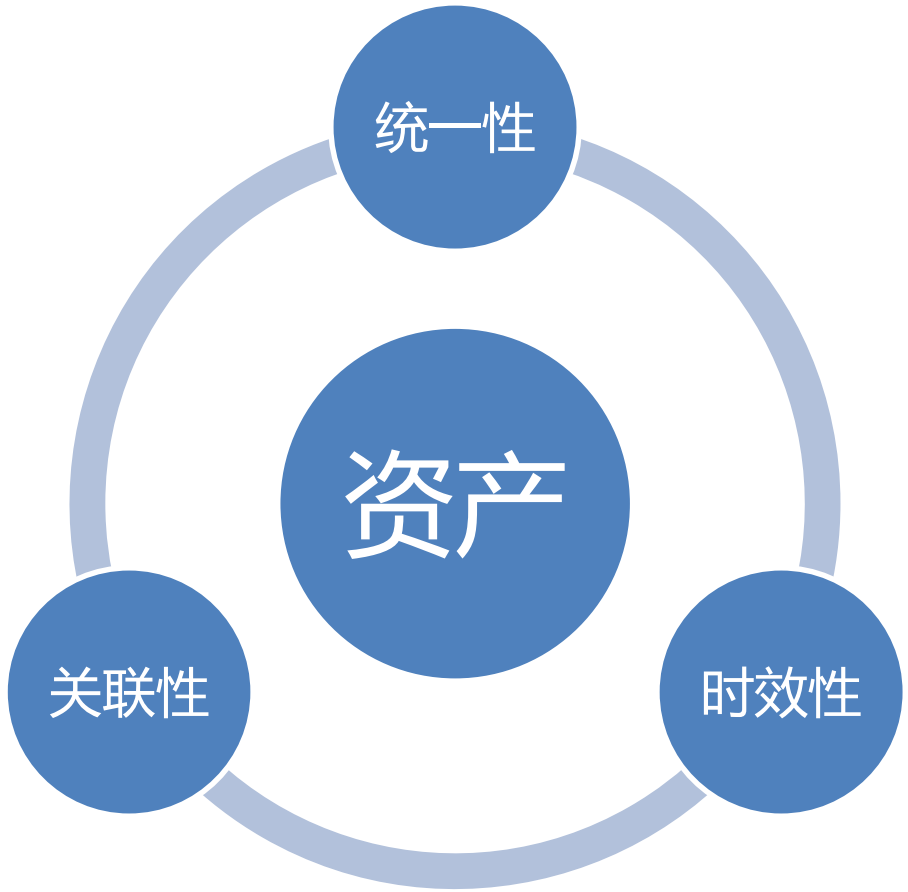
数据模型的优势

- 加速定义的数据模型的数据
- 关联同一数据模型不同来源类型的数据
- 格式化数据

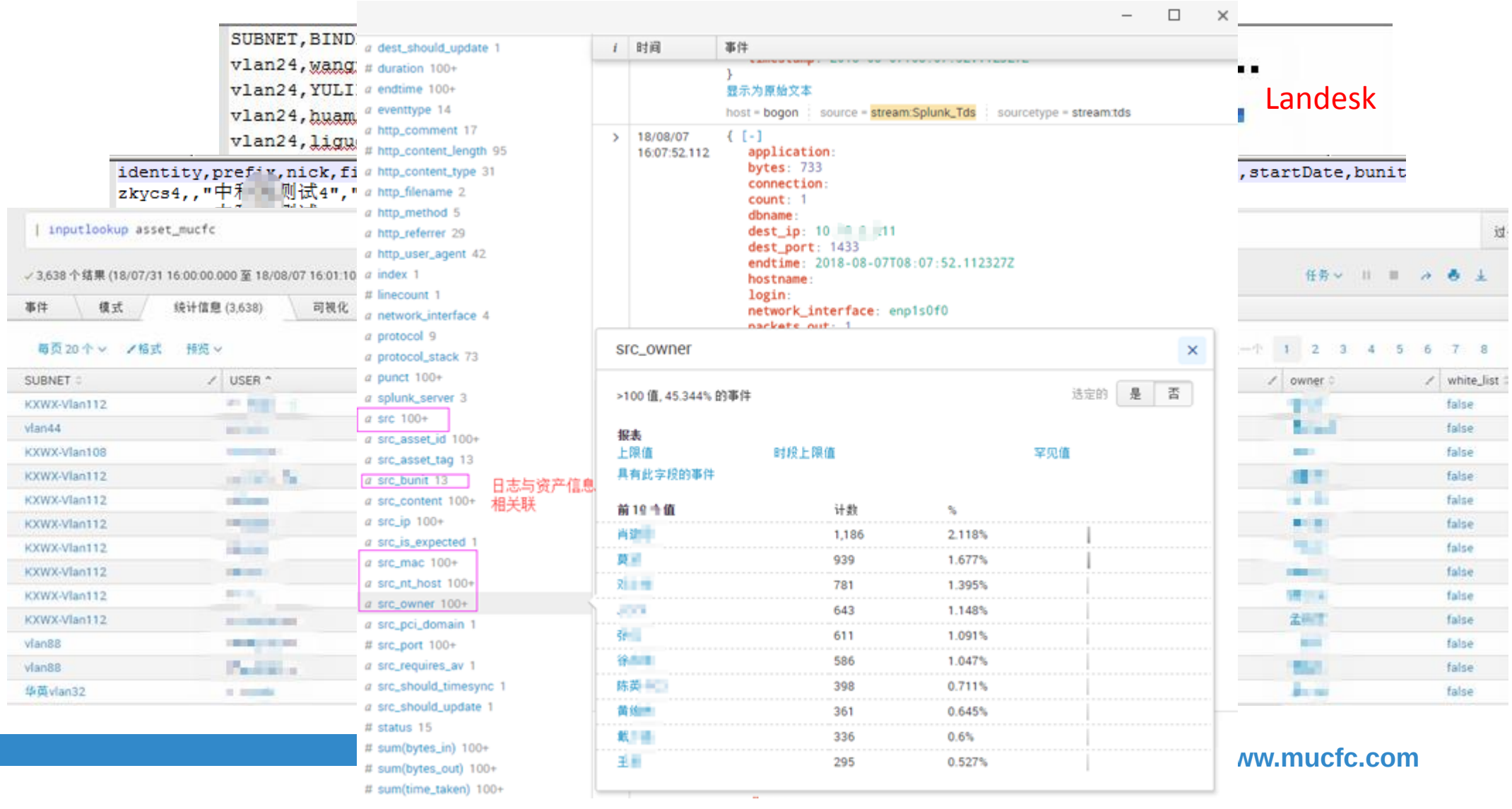
数据模型效果


时间
今天
职场
所有
操作人员
所有
隐藏过滤器
催收系统敏感接口访问趋势
新搜索
另存为
关闭
| pivot Mucfc_dcs All_User_Action dc(post_data) AS post_data SPLITROW _time AS _time PERIOD auto SPLITCOL url_explain FILTER url_explain in ("外包文件发送","查看主借款人单位信息"
,"查看借款人银行卡信息","查看借款人手机号码","查看借款人地址信息","查看借款人网络信息") FILTER post_data isNotNull SORT 0 _time ROWSUMMARY 0 COLSUMMARY 0 NUMCOLS 100 SHOWOTHER 1
今天
搜索任务查看器 | Splunk 7.0.0 - Google Chrome
新搜索
另存为
关闭
index=data_base sourcetype=dcs-web
今天
3,899,647 个事件 (18/08/07 0:00:00.000 至 18/08/07 18:14:34.000 的部分结果)
无事件采样
任务
详细模式
事件 (3,899,647)
模式
统计信息
可视化
设定时间线的格式
缩小
缩放到所选区域
取消选择
每列 1 小时
2018/08/07
2018/08/07 19:00
列表
格式
隐藏字段
所有字段
选定字段
host 2
source 1
sourcetype 1
感兴趣的字段
时间
18/08/07 18:05:42.854
18/08/07
搜索任务查看器 | Splunk 7.0.0 - Google Chrome
https://10.75.224.11:8000/zh-CN/manager/SplunkEnterpriseSecuritySuite/job_inspector?sid=1533636874.45756
搜索任务查看器
This search has completed and has returned 1,000 结果 by scanning 3,899,647 事件 in 328.702 seconds
搜索子系统返回了下面消息:
info : Search finalized.
(SID: 1533636874.45756) search.log
执行成本
持续时间 (秒)
组件
调用
输入计数
输出计数
0.27
command.fields
331
3,899,647
3,899,647
上一个 1 2 3 4 5 6 7 8 9 ... 下一步
cess():49|[][][153.37.178.170][application/json, text/p
[/dcs-web/new_work/ajaxActionSelectOptions.do]
"content-type":["application/json;charset=UTF-
application/json, text/plain, */*"],"origin":
(KHTML, like Gecko) Chrome/66.0.3359.139
content-length":["0"],"x-real-ip":["153.37.178.170"],"r
/]
ess():49|[][][153.37.178.170][application/json, text/pl

资产信息要求



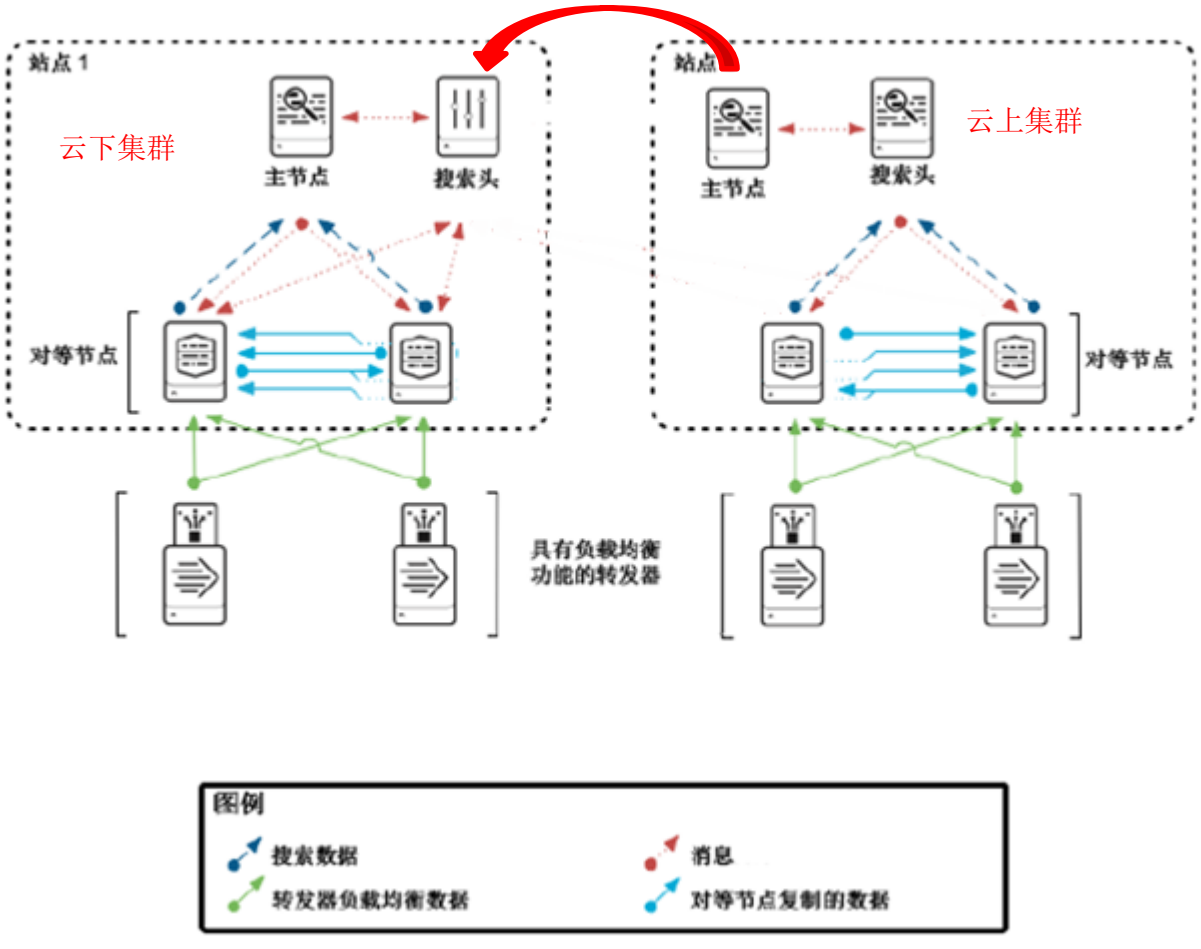
资产统一管理


SUBNET,BIND
vlan24,wang
vlan24,YULI
vlan24,huam
vlan24,ligu
identity,prefix,nick,fi
zkycs4,,"中和 测试4","
Landesk
,startDate,bunit
| inputlookup asset_mucfc
✓3,638 个结果 (18/07/31 16:00:00.000 至 18/08/07 16:01:10
事件
模式
统计信息 (3,638)
可视化
每页 20 个
格式
预览
SUBNET
USER
KXWX-Vlan112
vlan44
KXWX-Vlan108
KXWX-Vlan112
KXWX-Vlan112
KXWX-Vlan112
KXWX-Vlan112
KXWX-Vlan112
KXWX-Vlan112
KXWX-Vlan112
vlan88
vlan88
华茵vlan32
a dest_should_update 1
duration 100+
a endtime 100+
a eventtype 14
a http_comment 17
http_content_length 95
a http_content_type 31
a http_filename 2
a http_method 5
a http_referrer 29
a http_user_agent 42
a index 1
linecount 1
a network_interface 4
a protocol 9
a protocol_stack 73
a punct 100+
a splunk_server 3
a src 100+
a src_asset_id 100+
a src_asset_tag 13
a src_bunit 13
a src_content 100+
a src_ip 100+
a src_is_expected 1
a src_mac 100+
a src_nt_host 100+
a src_owner 100+
a src_pci_domain 1
src_port 100+
a src_requires_av 1
a src_should_timesync 1
a src_should_update 1
status 15
sum(bytes_in) 100+
sum(bytes_out) 100+
sum(time_taken) 100+
日志与资产信息
相关联
i
时间
事件
}
显示为原始文本
host = bogon
source = stream:Splunk_Tds
sourcetype = stream:tds
18/08/07
16:07:52.112
{ [-]
application:
bytes: 733
connection:
count: 1
dbname:
dest_ip: 10
:11
dest_port: 1433
endtime: 2018-08-07T08:07:52.112327Z
hostname:
login:
network_interface: enp1s0f0
src_owner
>100 值, 45.344% 的事件
选定的
是
否
报表
上限值
时段上限值
罕见值
具有此字段的事件
前 10 个值
计数
%
1,186
2.118%
939
1.677%
781
1.395%
643
1.148%
611
1.091%
586
1.047%
398
0.711%
361
0.645%
336
0.6%
295
0.527%
owner
white_list
false

网络要求

- 各个边界的日志单独存储
- 各个边界的日志能关联分析
- 各个边界节点的日志转发器能统一管理

分布式群集部署



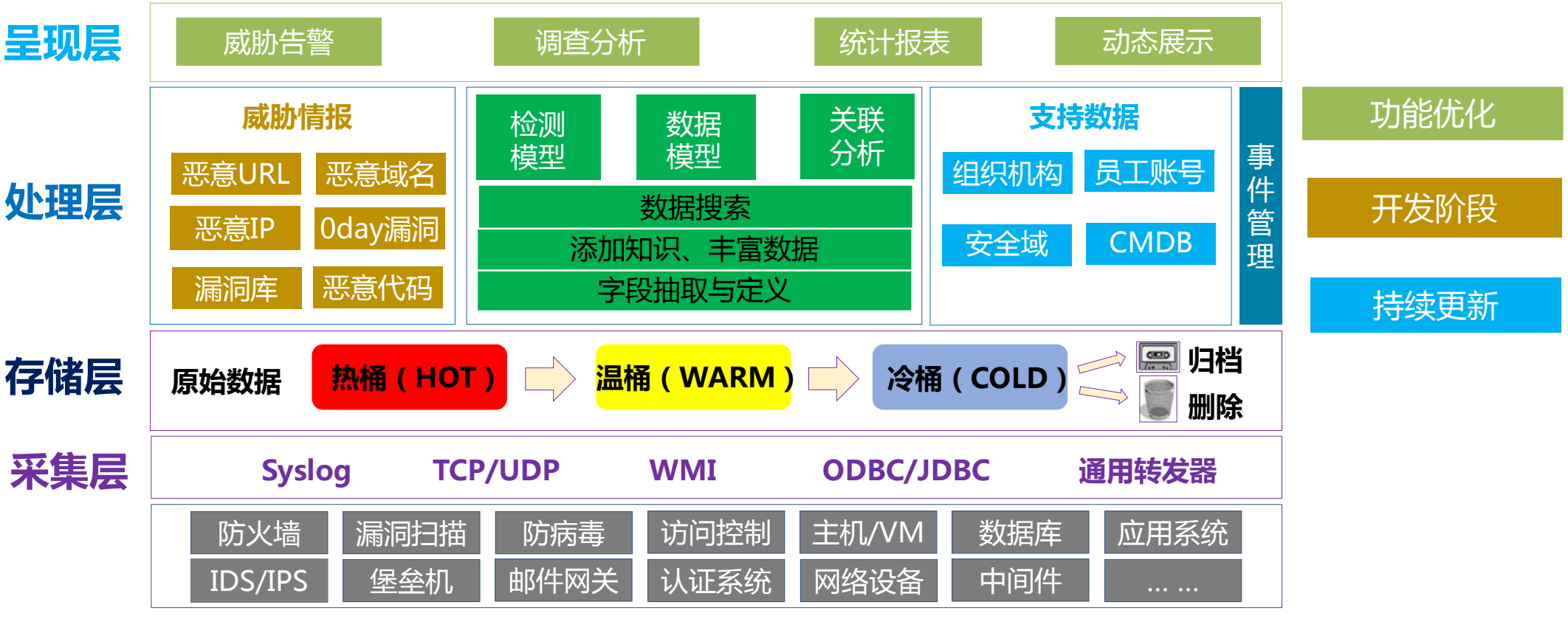
- 搜索头：建立任务，处理数据，展示结果
- 主节点：管理节点，下发任务
- 对等节点：索引日志
- 转发器：收集数据，过滤数据

/03

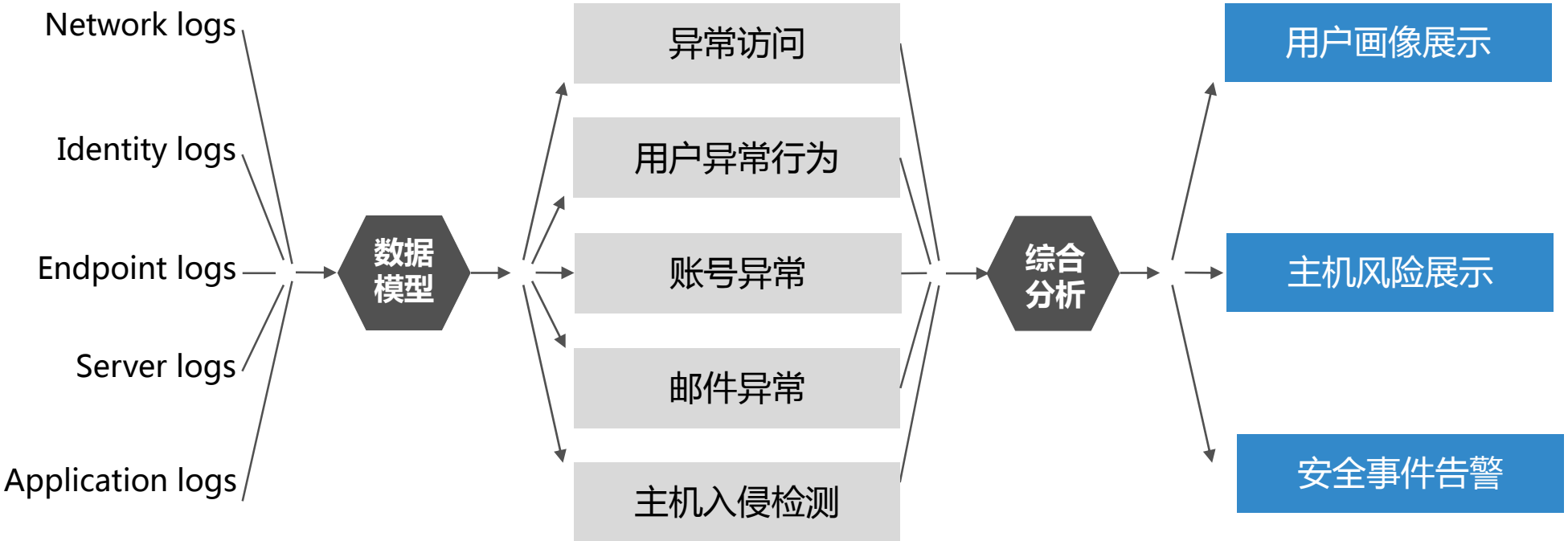
安全监控系统架构

- 系统架构
  - 关联分析

安全监控平台架构


呈现层
威胁告警
调查分析
统计报表
动态展示
处理层
威胁情报
恶意URL
恶意域名
恶意IP
0day漏洞
漏洞库
恶意代码
检测模型
数据模型
关联分析
数据搜索
添加知识、丰富数据
字段抽取与定义
支持数据
组织机构
员工账号
安全域
CMDB
事件管理
存储层
原始数据
热桶（HOT）
温桶（WARM）
冷桶（COLD）
归档
删除
采集层
Syslog
TCP/UDP
WMI
ODBC/JDBC
通用转发器
防火墙
漏洞扫描
防病毒
访问控制
主机/VM
数据库
应用系统
IDS/IPS
堡垒机
邮件网关
认证系统
网络设备
中间件
... ...
功能优化
开发阶段
持续更新

关联分析



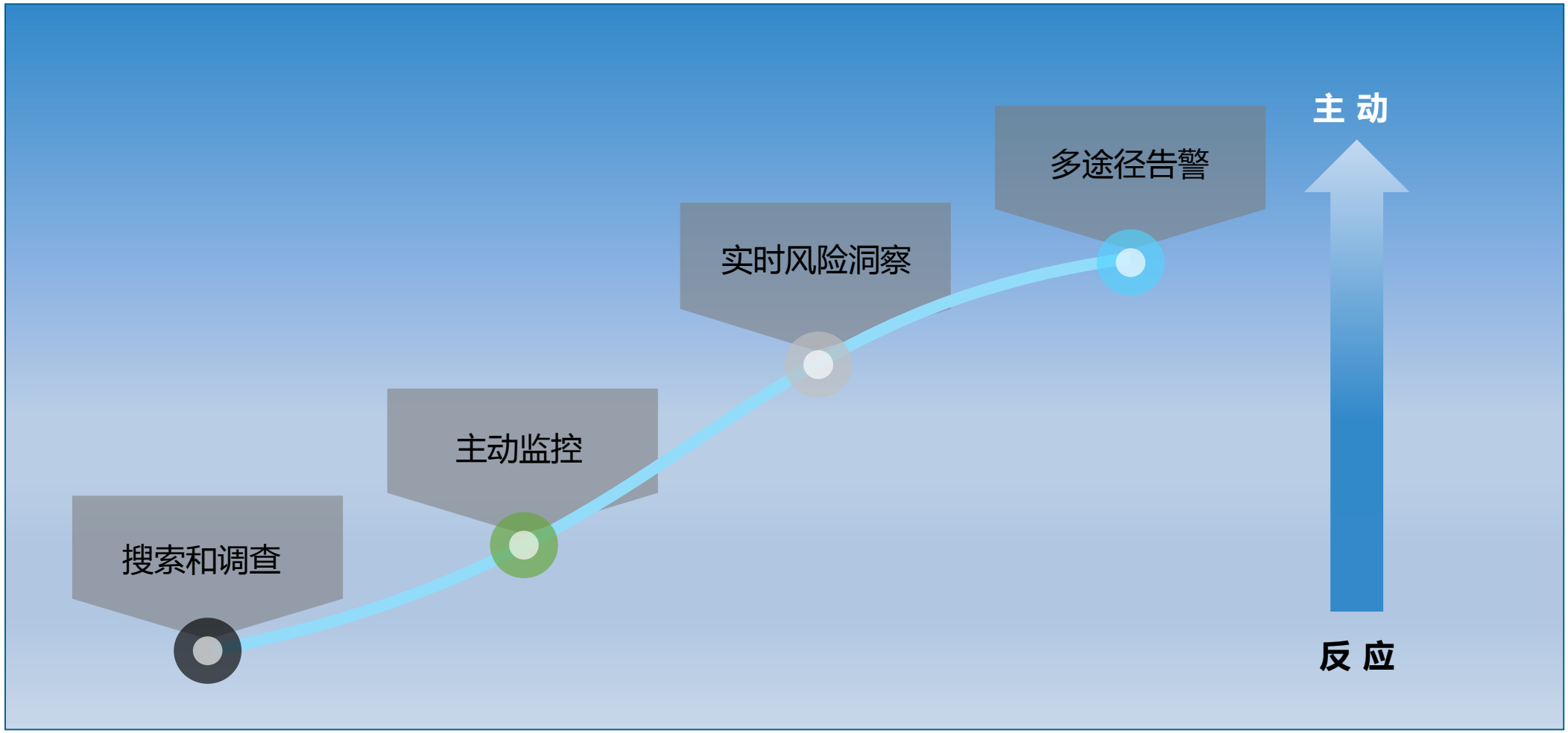
异常检测模型

统一展示

招联金融
MUCFC.COM

举个栗子（邮件日志）

预期效果



/04 持续监控

- 云主机安全监控
  - 个人用户行为分析
    - 一个响应案例

云主机的安全监控总览


编辑
风险主机
总数量
3
-1
风险操作
总数量
8
-5
风险系数
风险评分
70分
-200
WEBSHELL计数
总数量
0
提权操作
操作计数
0
异常登录
总次数
0
0
整体的安全指标
云主机风险分布(过去7天)
消费金融系统(
01.82)
监控系统(10
0.19)
会计系统
31.11)
运维管理系统(
00.3)
sever_name: 监控系统(10
0.19)
risk: 40
risk%: 14.286%
风险系数主机分布
运维管理系统(
0.81)
监控系统(
.0.23)
59
MongoDB明文密码登录
MySQL明文密码登录
Mysql明文密码登录
nc rule
nmap端口扫描
rsync外传服务器数据文件
scp外传服务器数据文件
tcpdump
wget下载黑客工具
查看或修改host key
查看系统版本
敏感目录或文件危险权限
60

云主机监控详情

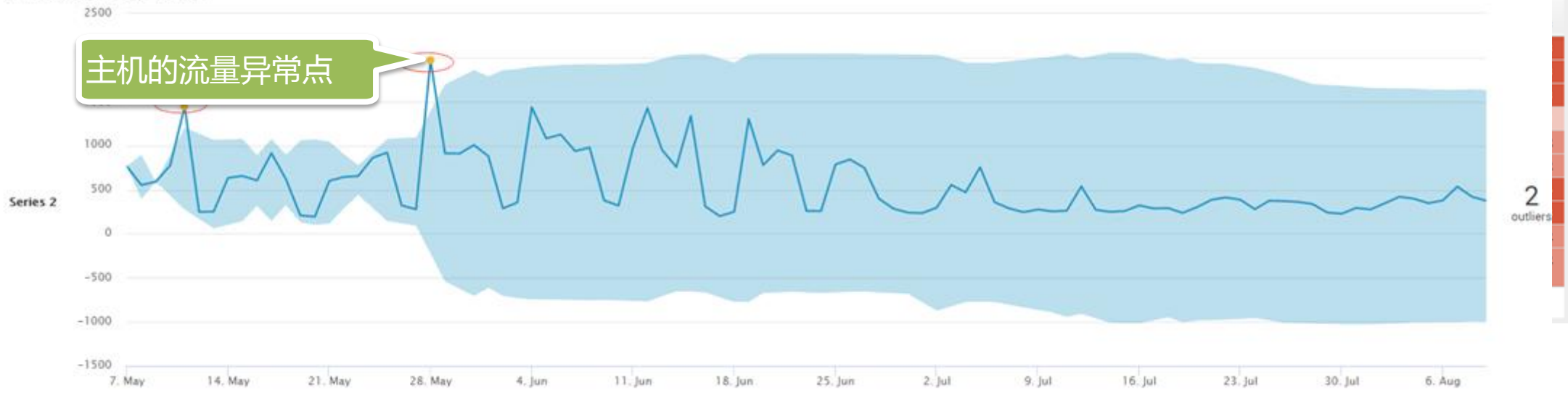
过去7天风险事件审计

client_ip	client_name	serve_ip	serve_name	rule	sparkline	count
			商户业务系统:资金能力系统	wget下载黑客工具		8
	堡垒机		运维管理系统	rsync外传服务器数据文件 查看或修改host key		3
			hadoop开发集群机器	查看系统版本		2
				Mysql明文密码显示		2

来源

目标

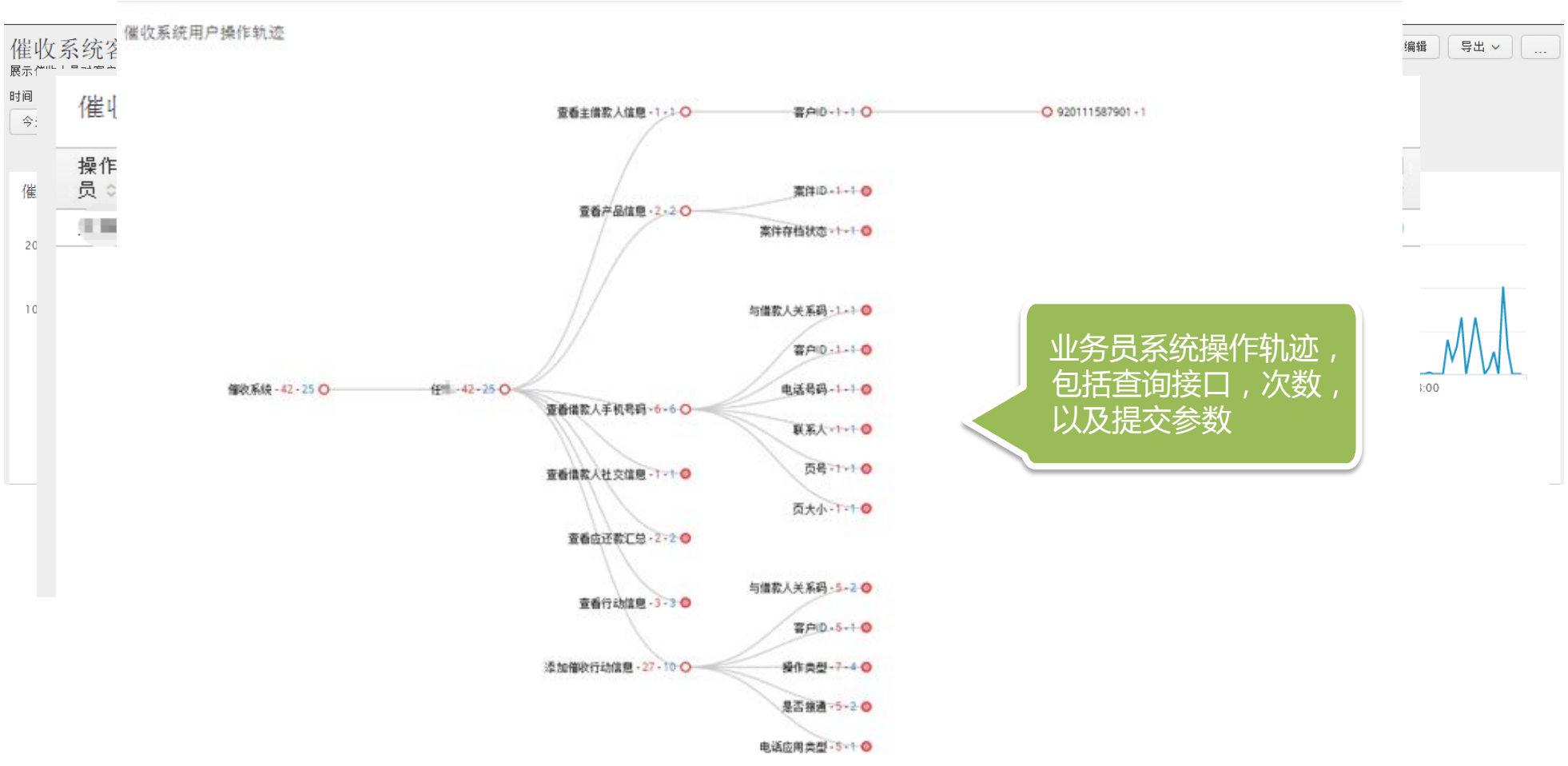
SFTP服务器下载流量波动图



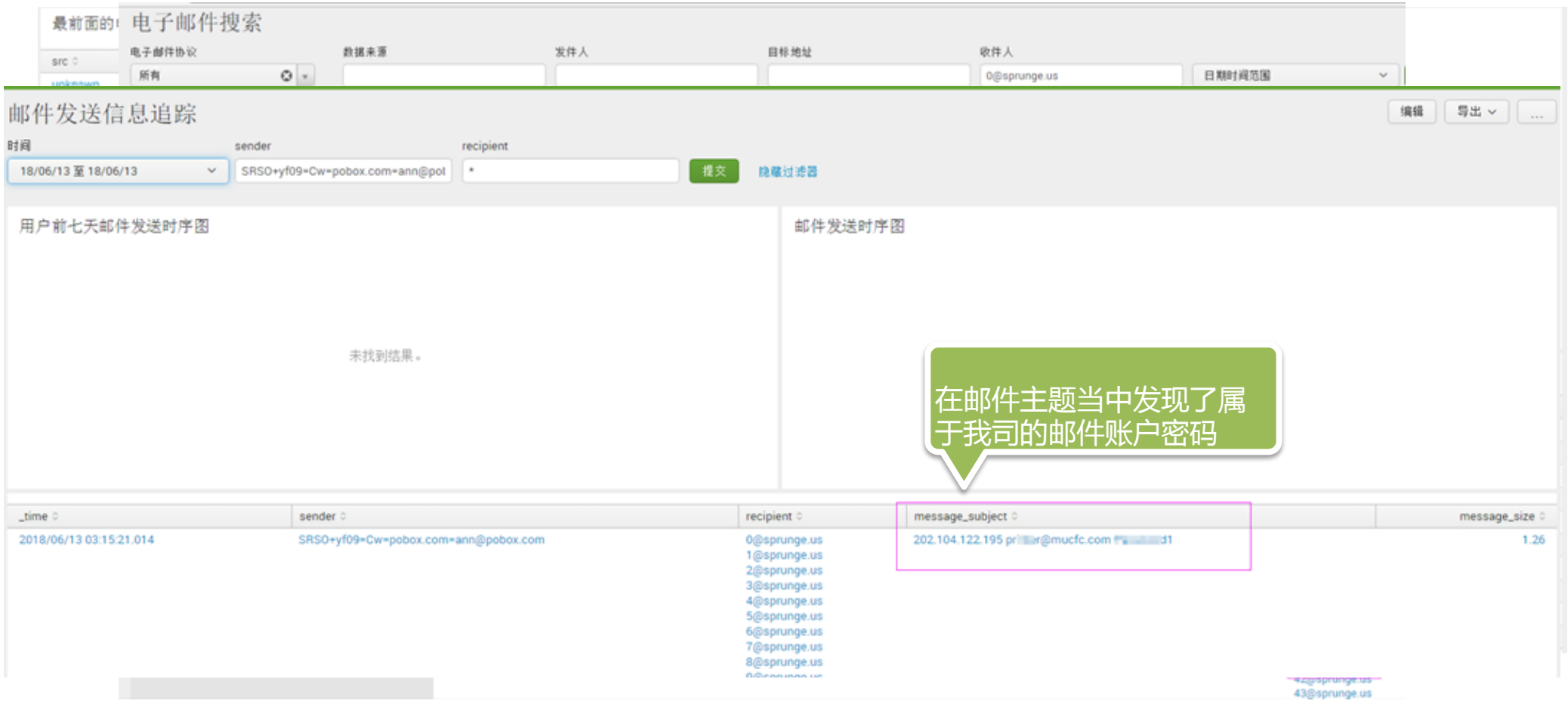
用户行为画像


搜索
用户的详细信息
is_expected: false
bunit: 研发中心
_time: 2018-08-10T11:49:28+0800
should_timesync: false
should_update: false
owner:
pci_domain: untrust
ip: 10.75.2
requires_av: false
mac: 4c:cc:6a:ef:36:24
编辑
2018-08-04
2018-08-05
2018-08-06
2018-08-07
2018-08-08
2018-08-09
2018-08-10
所有更改
威胁列表活动
非企业邮件发送
文件拷贝
身份验证
文件打印
风险调节器
重要事件
恶意软件攻击
过去 7 天
用户行为以及安全事件
搜索未返回结果
搜索未返回结果
2018年8月9日 早上8点34 - 2018年8月9日 上午10点22
247 事件
文件拷贝 (247)
2018年8月9日 早上8点34
2018年8月9日 上午10点22
GMT+0800
dest_ip
10.75.25.112
事件发生的详细情况以及可处理操作，含有触发的规则说明，点击搜索可查看原始事件
以时间为横轴，标志行为发生的时间点，颜色越深，表明次数越多
查看: 7天 38分钟
08/03
08/10

业务系统的访问分析


催收系统用户操作轨迹
催收系统 - 42 - 25
查看主借款人信息 - 1 - 1
客户ID - 1 - 1
920111587901 - 1
查看产品信息 - 2 - 2
案件ID - 1 - 1
案件存档状态 - 1 - 1
查看借款人手机号码 - 6 - 6
与借款人关系码 - 1 - 1
客户ID - 1 - 1
电话号码 - 1 - 1
联系人 - 1 - 1
页号 - 1 - 1
页大小 - 1 - 1
查看借款人社交信息 - 1 - 1
查看应还款汇总 - 2 - 2
查看行动信息 - 3 - 3
添加催收行动信息 - 27 - 10
与借款人关系码 - 5 - 2
客户ID - 5 - 1
操作类型 - 7 - 4
是否接通 - 5 - 2
电话应用类型 - 5 - 1
业务员系统操作轨迹，包括查询接口，次数，以及提交参数

一个事件调查


电子邮件搜索
电子邮件协议
所有
数据来源
发件人
目标地址
收件人
0@sprunge.us
日期时间范围
邮件发送信息追踪
编辑
导出
时间
18/06/13 至 18/06/13
sender
SRSO=yf09=Cw=pobox.com=ann@pol
recipient
*
提交
隐藏过滤器
用户前七天邮件发送时序图
未找到结果。
邮件发送时序图
在邮件主题当中发现了属于我司的邮件账户密码
_time
sender
recipient
message_subject
message_size
2018/06/13 03:15:21.014
SRSO=yf09=Cw=pobox.com=ann@pobox.com
0@sprunge.us
1@sprunge.us
2@sprunge.us
3@sprunge.us
4@sprunge.us
5@sprunge.us
6@sprunge.us
7@sprunge.us
8@sprunge.us
202.104.122.195
@mucfc.com
1.26
43@sprunge.us

作个总结

- 资产是前提
- 数据需规划与预估
- 行为需要关联
- 不断提到效率和自动化
- 严谨很重要

Q&A

THANKS

招联金融
MUCFC.COM