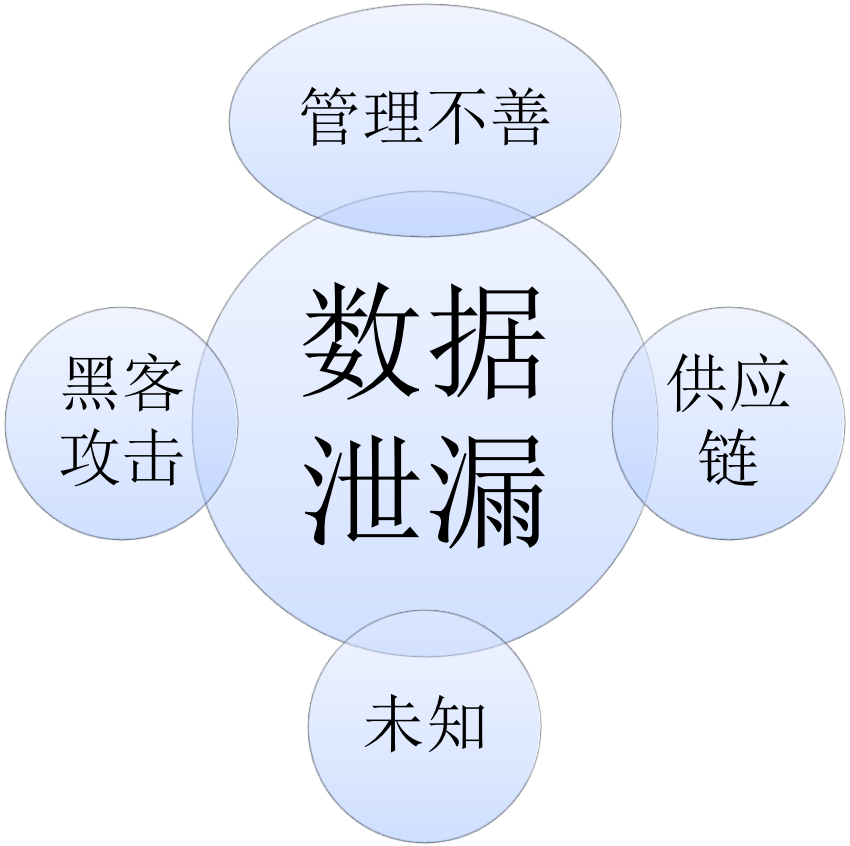
企业运营后台之数据安全

挖土

目录


管理不善
数据泄漏
黑客攻击
供应链
未知

快递内鬼和不法电商沆瀣一气

竟把公司电脑搬来窃取公民信息

经查，郑州某科技公司法人郑某早些年一直从事电商推广业务，并通过知名网络平台的“推送和植入”推广公司产品。郑某苦心钻营，一次与长期合作而熟识的快递业务员刘某、卫某闲谈时，忽然计上心来。

“你们快递公司内部系统不是能查到所有客户信息吗？你提供给我，我按照货到付款的方式广撒网，这样我能省掉广告运营的成本，你的发件量上去了，绩效工资不就来了？赚到的钱我年底再分你5个点。”郑某跟快递员如此商量道。

『雅虎前工程师访问了大约6000个年轻女子的电子邮件账号』

一名前雅虎软件工程师近日在法庭上供认不讳，承认自己通过雅虎系统非法访问了6000多个雅虎用户的个人账号，以寻找年轻女性的个人私密图片和视频，从而下载到硬盘。

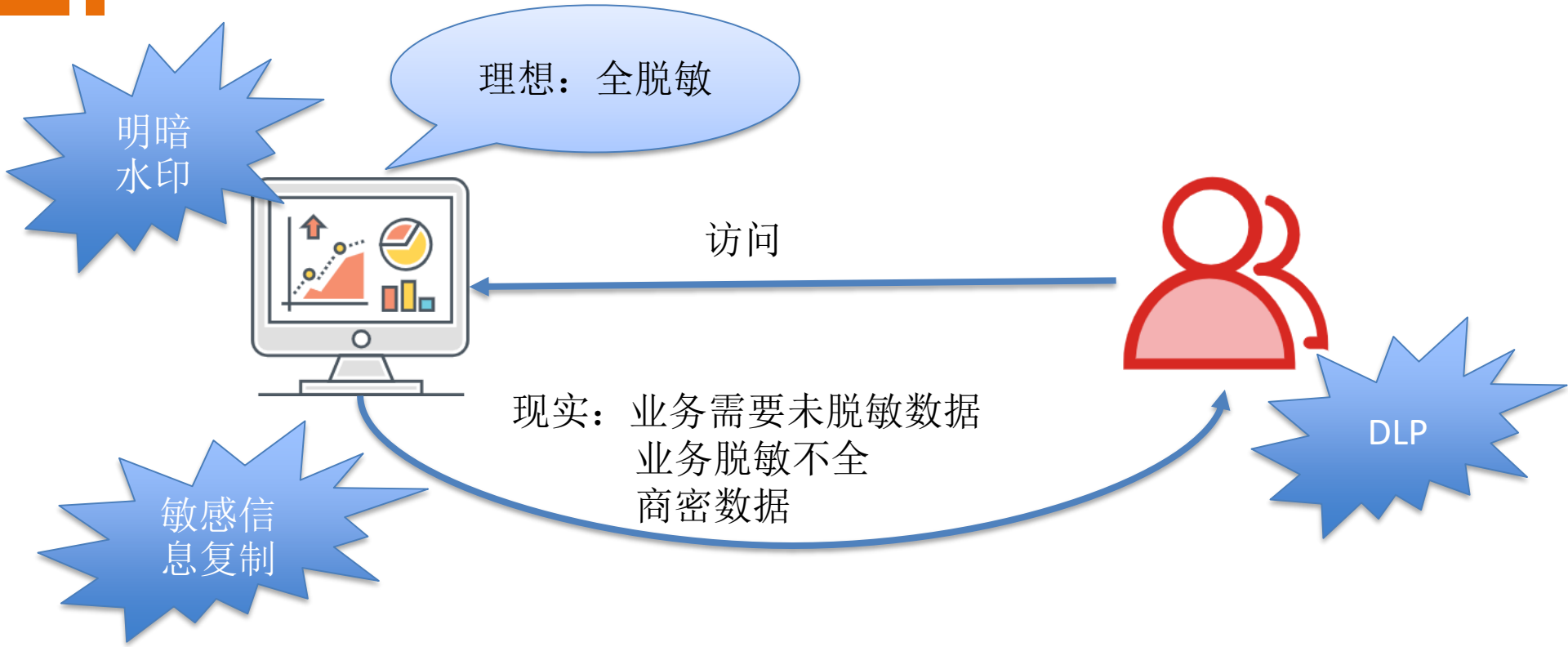
这个34岁的名为Reyes Daniel Ruiz的跟踪者来自美国加利福尼亚州，他在雅虎工作了十多年，他在该公司主要担任雅虎邮件@yahoo.com服务的可靠性工程师。其于2018年7月停止了其在雅虎的工作，目前受雇于一家专门从事单点登录（SSO）解决方案的硅谷科技公司。

据法庭文件显示，其利用其工作岗位提供的访问雅虎内部网络的权限，破解了用户的密码，进而非法闯入了电子邮件账号。

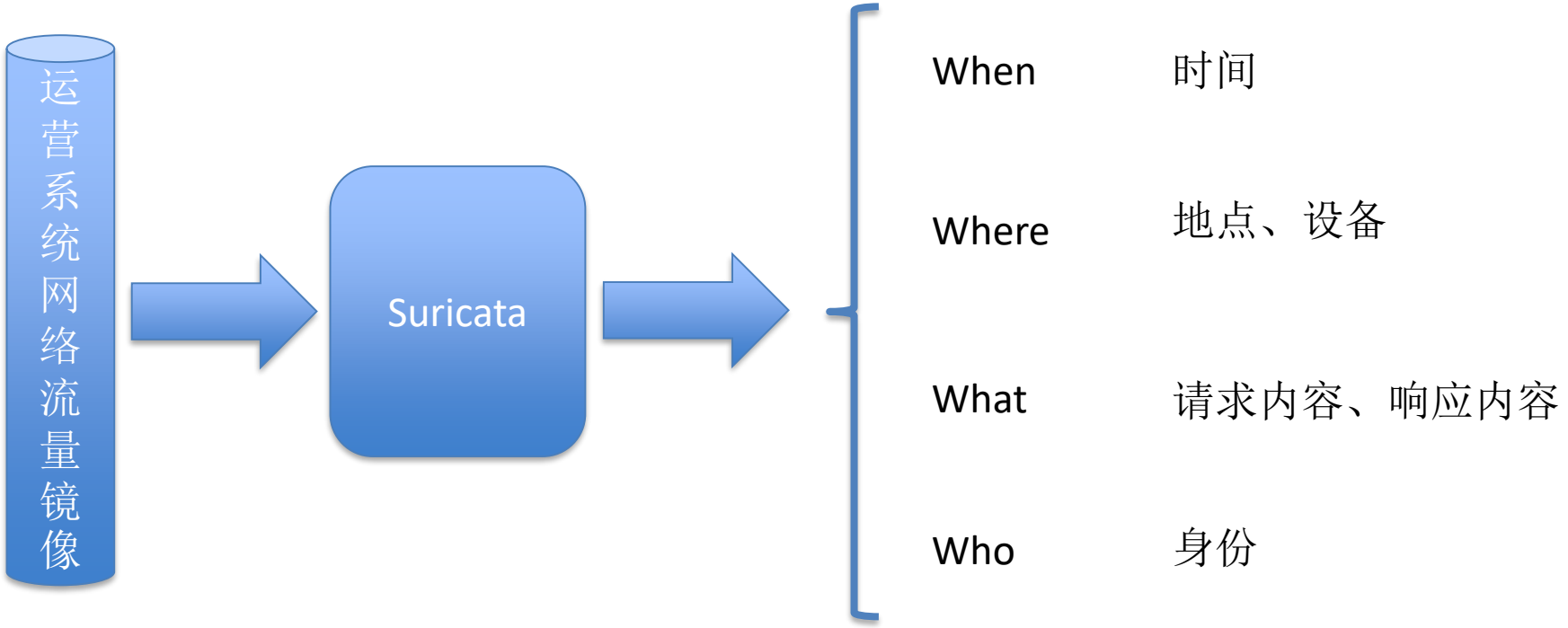
目录

02 运营后台溯源/分析系统

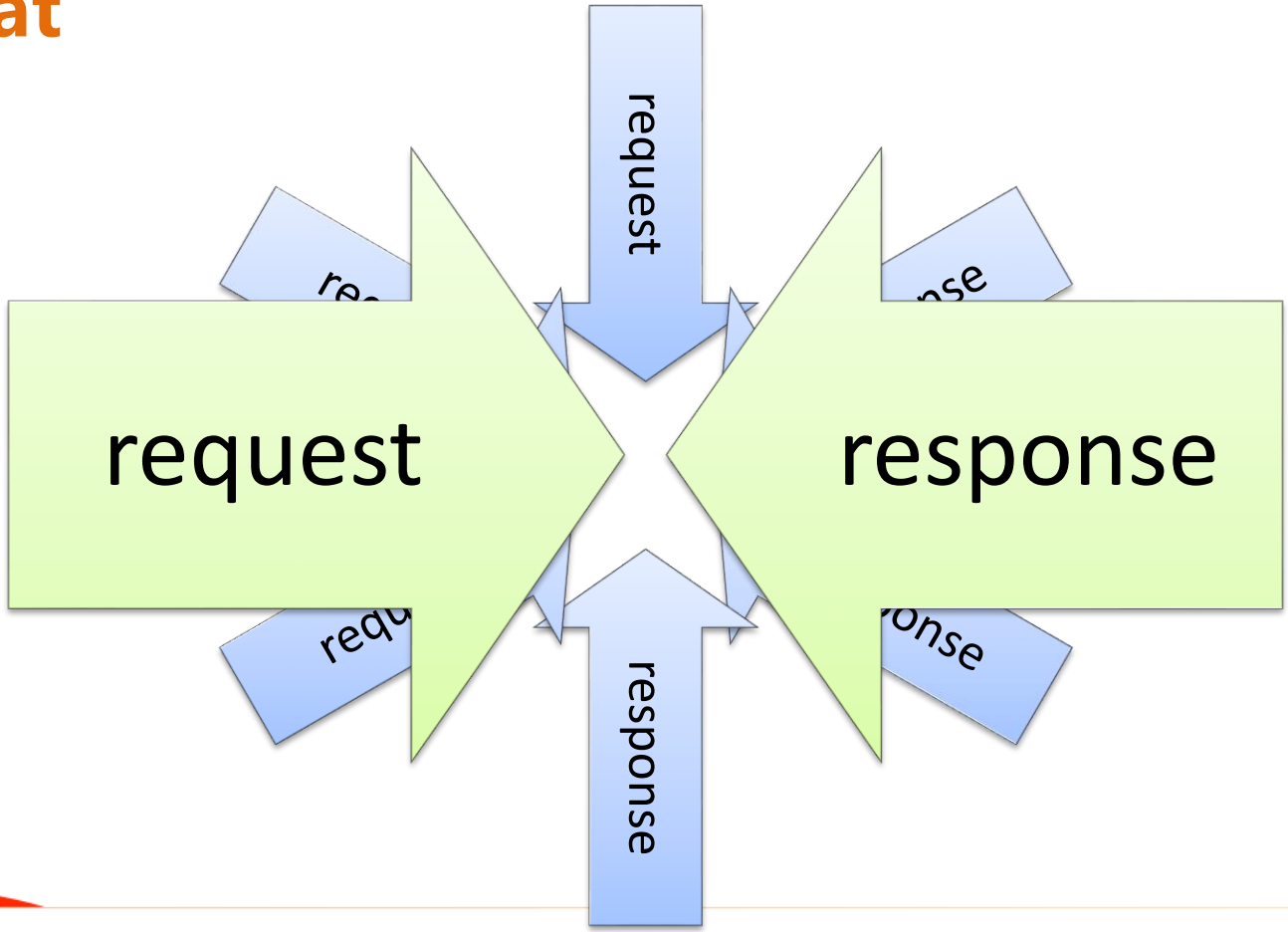
运营后台现状



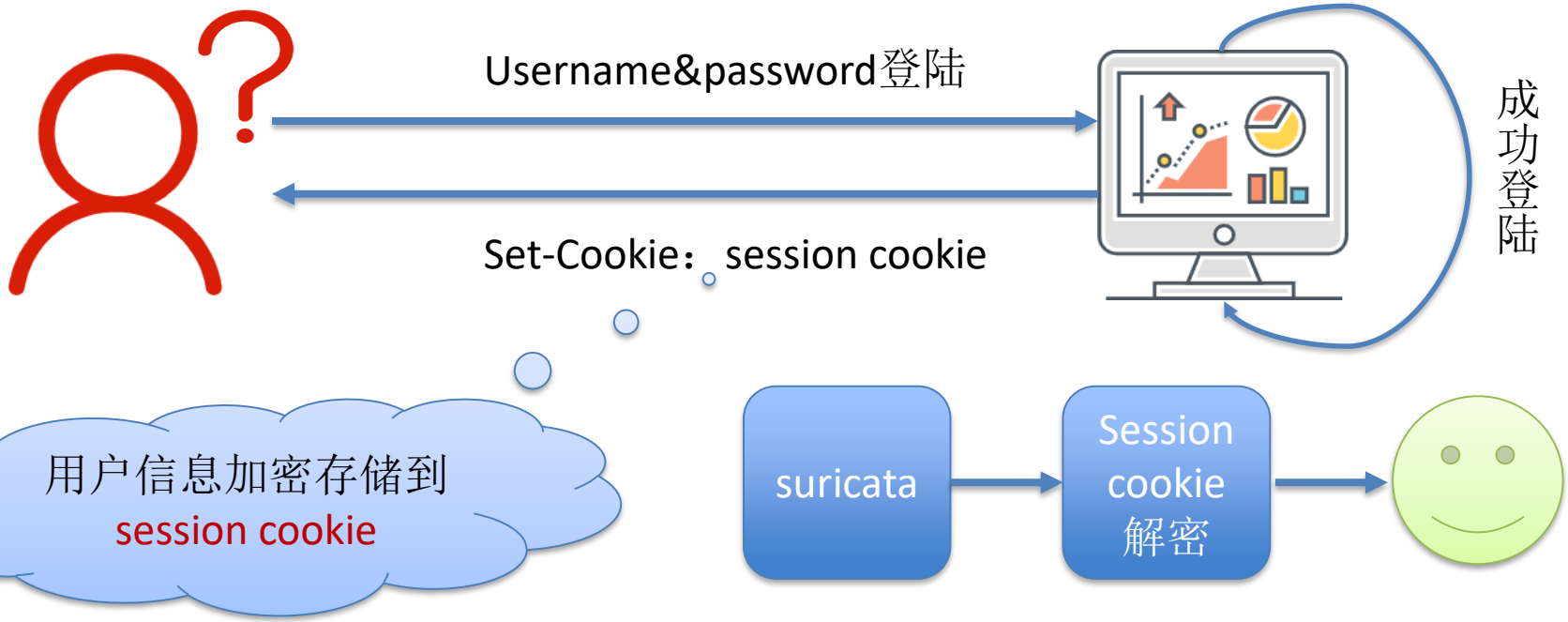
分析/溯源要素


运营系统网络流量镜像
Suricata
When
时间
Where
地点、设备
What
请求内容、响应内容
Who
身份

What



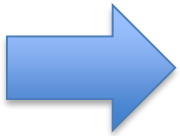
Who


Username&password登陆
Set-Cookie：session cookie
成功登陆
用户信息加密存储到
session cookie
suricata
Session cookie 解密

轻量级落地

- Suricata
- Luajit

运营系统网络流量镜像



Suricata

- 14.2.3. http
  - 14.2.3.1. HttpGetReque
  - 14.2.3.2. HttpGetReque
  - 14.2.3.3. HttpGetReque
  - 14.2.3.4. HttpGetRespo
  - 14.2.3.5. HttpGetReque
  - 14.2.3.6. HttpGetRespo
  - 14.2.3.7. HttpGetRawR
  - 14.2.3.8. HttpGetRawR
  - 14.2.3.9. HttpGetRequestUriRaw
  - 14.2.3.10. HttpGetRe
  - 14.2.3.11. HttpGetR
  - 14.2.3.12. HttpGetR

```
# Lua Output Support - execute lua script to generate alert and event
# output.
# Documented at:
# https://suricata.readthedocs.io/en/latest/output/lua-output.html
- lua:
    enabled: yes
    scripts-dir: /opt/suricata/etc/suricata/lua-output/
    scripts:
      - http.lua
```

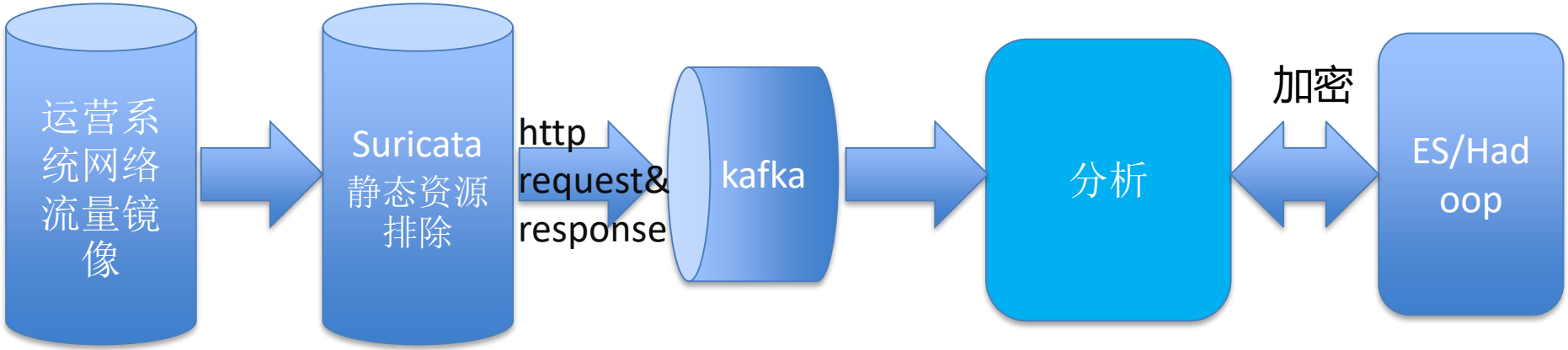
正则匹配关心的敏感信息，解密身份信息，记录4W

https://suricata.readthedocs.io/en/suricata-4.1.5/lua/index.html

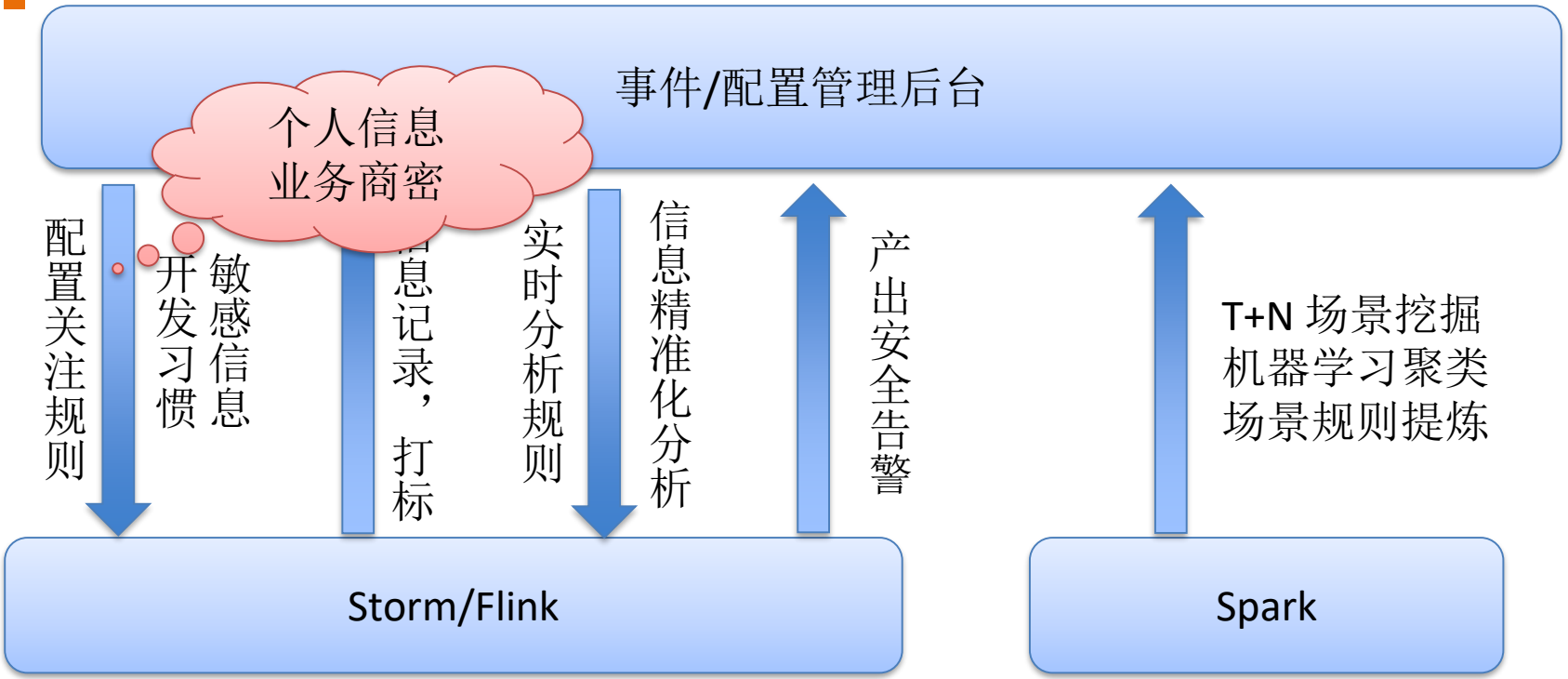
复杂化落地

- Suricata
- Luajit
- librdkafka/Cjson

- Kafka
- Storm/Flink/Spark
- ES/Hadoop



分析


事件/配置管理后台
个人信息
业务商密
配置关注规则
开发习惯
敏感信息
息记录，打标
实时分析规则
信息精准化分析
产出安全告警
T+N 场景挖掘
机器学习聚类
场景规则提炼
Storm/Flink
Spark

风险捕获

YOOZOO GAMES

风险概览

风险概览

风险概览

开始日期 至 结束日期 | 接口访问频次异常 | 已处理 | 搜索

ID	策略名称	聚合主体	事件内容	发生时间	生成时间	处理时间	备注	状态	操作
20584	接口访问频次异常	[redacted]	接口 http://cr[redacted]tr av[redacted]/Cust o[redacted] m[redacted]m p[redacted]g ement[redacted]Co [redacted] [redacted]x 被账号 x [redacted]频繁访问	2019-07-28 20:44:28	2019-07-28 20:44:29	2019-07-29 16:35:26	爬虫，制作报表用。	已处理	处理

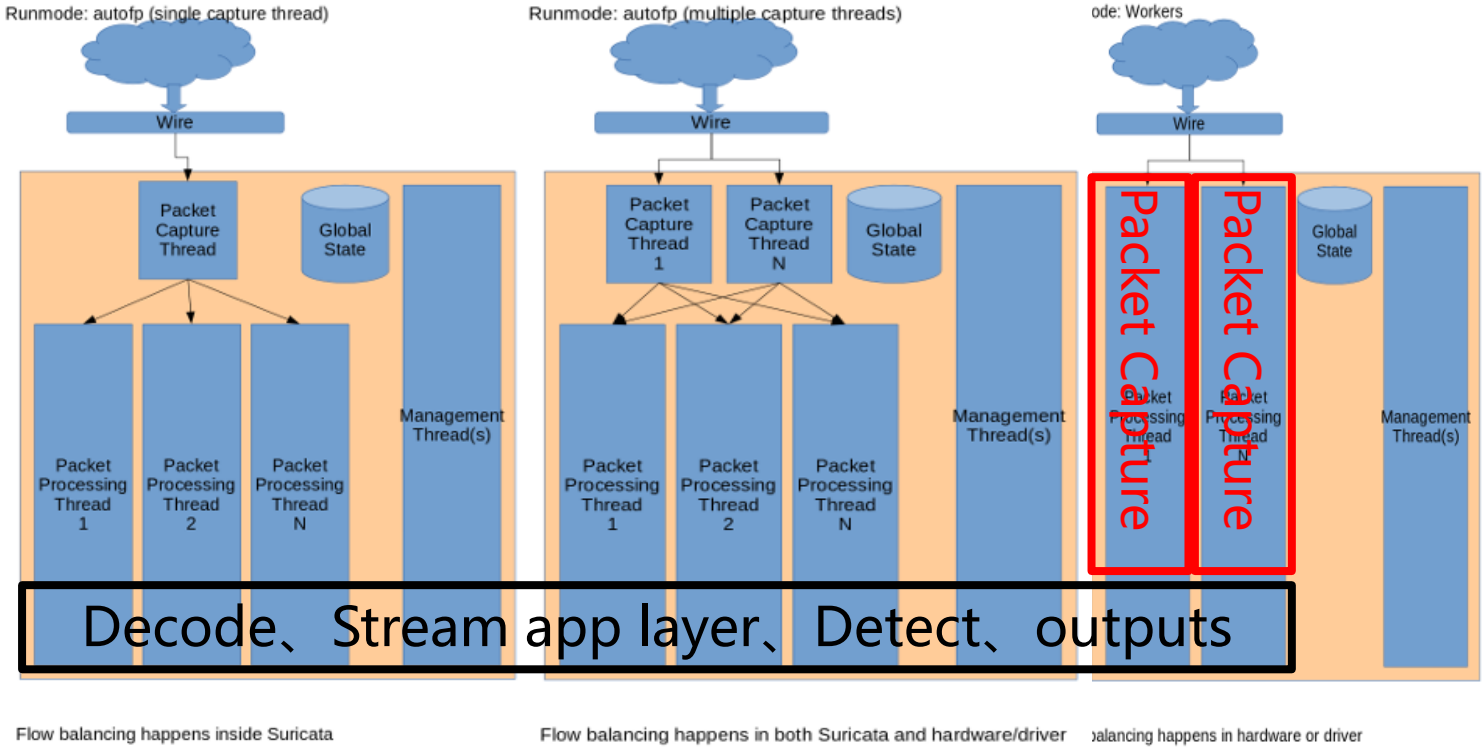
挑战

- 事件关联分析（DLP、VPN、考勤、排班）
- 事件运营，反推业务脱敏，问题定性较难
- 场景覆盖率，过多依赖于经验和事后挖掘
- 有据，未知理，why？？
- UEBA
- 加密流量

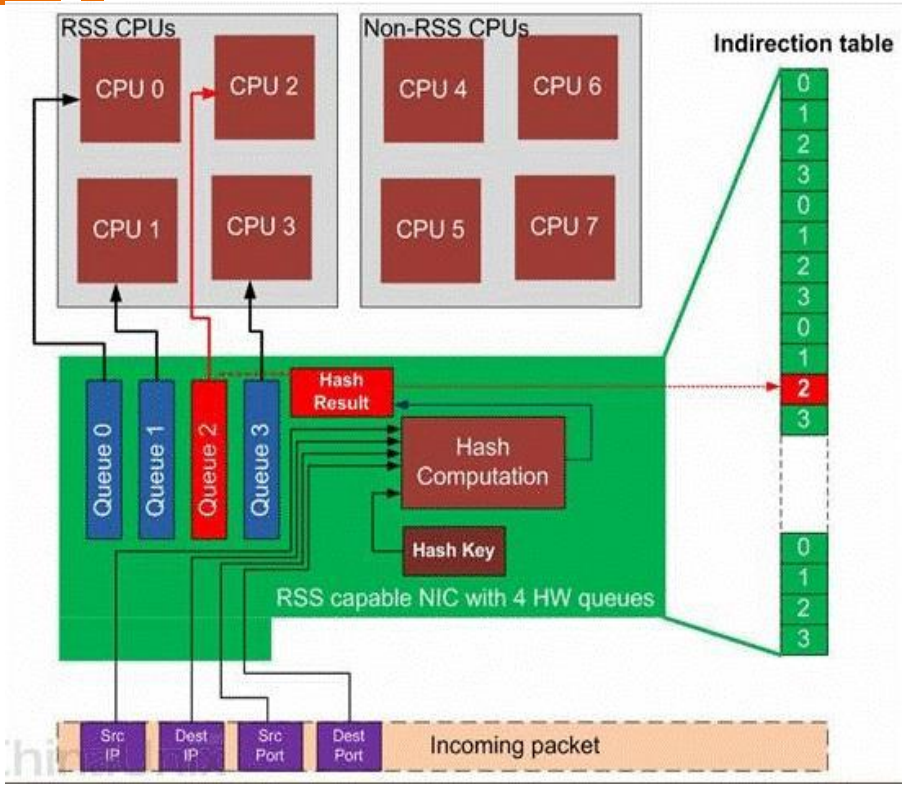
目录

Runmodes

- single
- autofp
- workers



RSS (Receive Side Scaling)

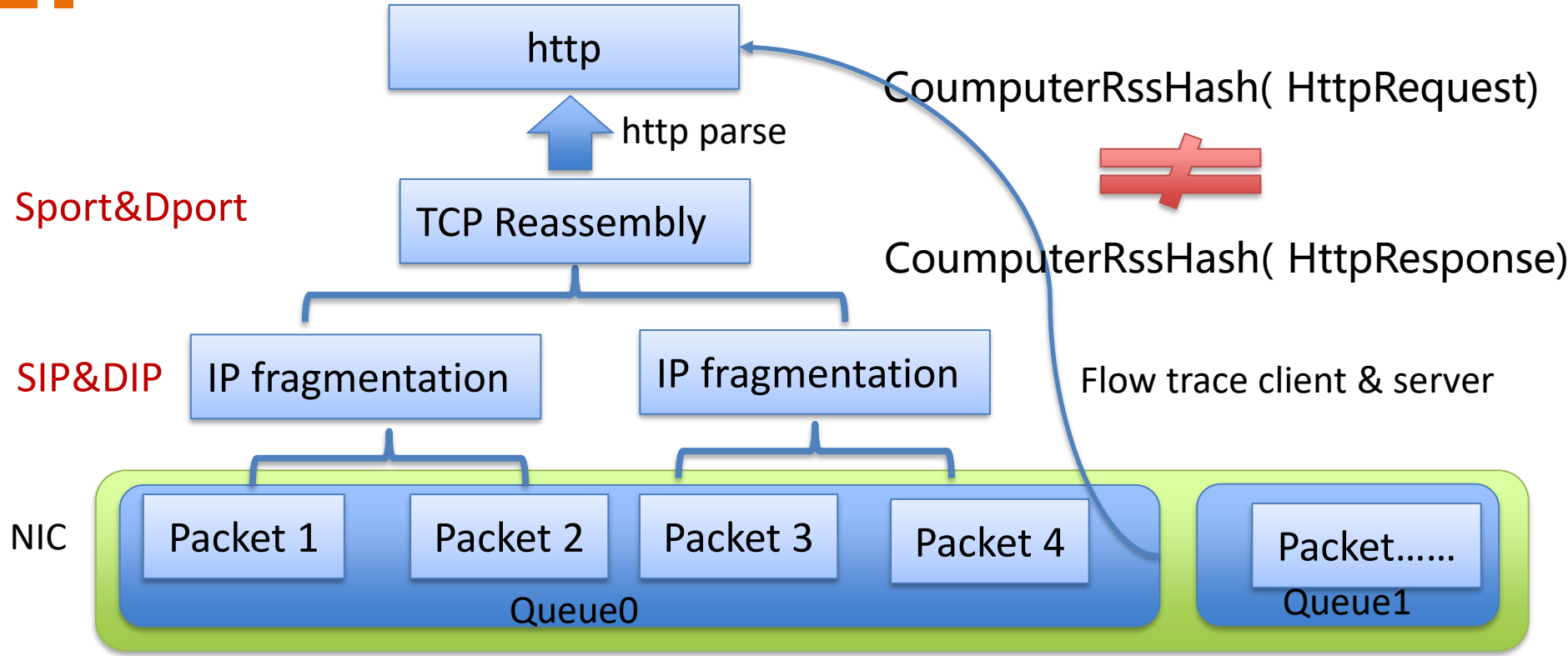



```
[ ... ~]$ ethtool -l eth6
Channel parameters for eth6:
Pre-set maximums:
RX:             0
TX:             0
Other:          1
Combined:       63
Current hardware settings:
RX:             0
TX:             0
Other:          1
Combined:       20
```

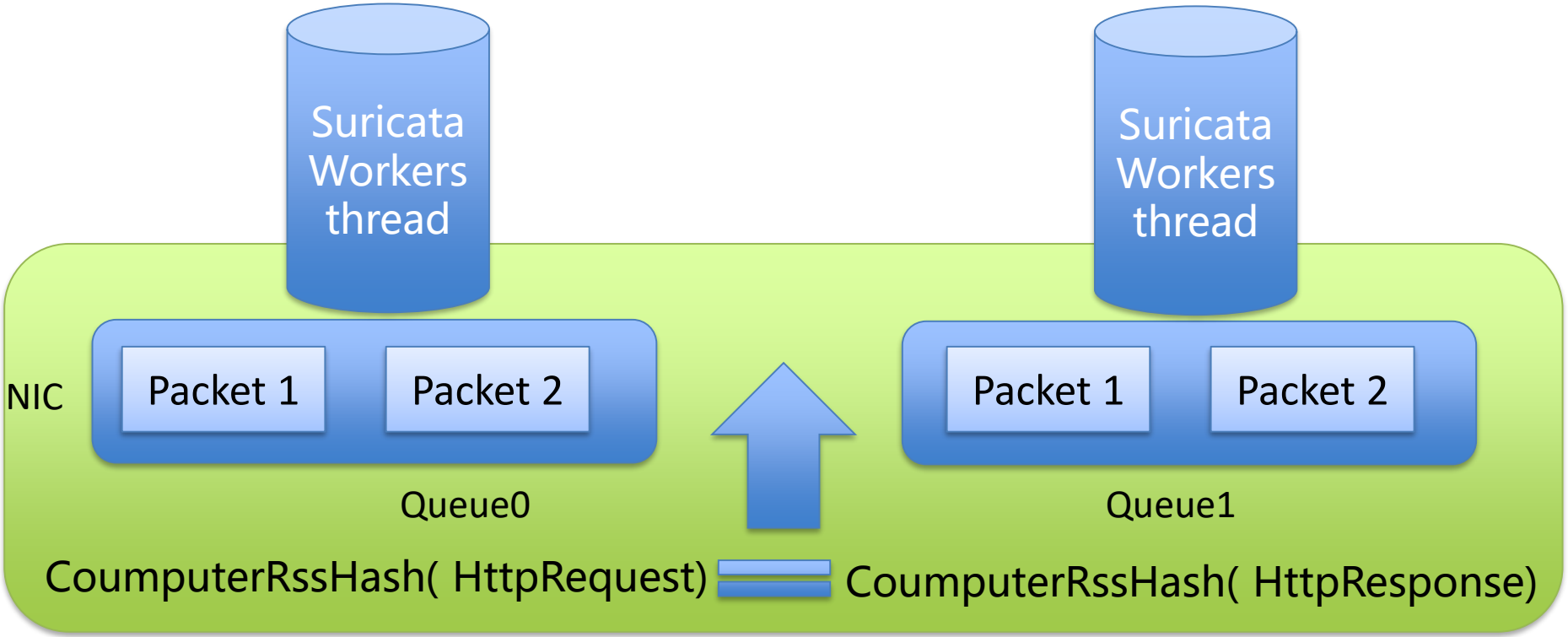
Algorithm 1 RSS Hash Computation Algorithm

function COMPUTERSSHASH($Input[]$, RSK)
  $ret = 0$;
  for each bit b in Input[] **do**
    if $b == 1$ **then**
      $ret \hat{}= $ (left-most 32 bits of RSK);
    end if
    shift RSK left 1 bit position;
  end for
end function

HTTP流量还原


http
http parse
TCP Reassembly
IP fragmentation
IP fragmentation
Sport&Dport
SIP&DIP
NIC
Packet 1
Packet 2
Packet 3
Packet 4
Queue0
Packet……
Queue1
CoumputerRssHash(HttpRequest)
≠
CoumputerRssHash(HttpResponse)
Flow trace client & server

Symmetric RSS



http://www.ndsl.kaist.edu/~kyoungsoo/papers/TR-symRSS.pdf

- Suricata runmode：workers
- RSS queues >= workers threads
- Symmetric RSS
- Suricata worker cpu affinity & priority
- Stop irqbalance & irq cpu affinity

```
[root@[redacted] ~]# mpstat -P ALL
Linux [redacted]                    10/21/2019      _x86_64_        (32 CPU)

04:55:13 PM  CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice   %idle
04:55:13 PM  all   25.70    0.00    1.46    0.00    0.00    1.77    0.00    0.00    0.00   71.07
04:55:13 PM    0    2.08    0.00    3.07    0.00    0.00    0.18    0.00    0.00    0.00   94.66
04:55:13 PM    1    3.01    0.00    4.05    0.00    0.00   24.46    0.00    0.00    0.00   68.47
04:55:13 PM    2    1.64    0.00    2.29    0.00    0.00   15.34    0.00    0.00    0.00   80.73
04:55:13 PM    3    3.13    0.00    2.26    0.00    0.00   10.29    0.00    0.00    0.00   84.31
04:55:13 PM    4    2.79    0.00    1.72    0.00    0.00    0.00    0.00    0.00    0.00   95.49
04:55:13 PM    5    2.75    0.00    1.64    0.00    0.00    0.00    0.00    0.00    0.00   95.61
04:55:13 PM    6    2.64    0.00    1.46    0.00    0.00    0.00    0.00    0.00    0.00   95.90
04:55:13 PM    7    2.77    0.00    1.75    0.00    0.00    0.00    0.00    0.00    0.00   95.48
04:55:13 PM    8    0.95    0.00    1.56    0.00    0.00    9.76    0.00    0.00    0.00   87.74
04:55:13 PM    9    5.21    0.00    2.02    0.00    0.00   13.45    0.00    0.00    0.00   79.32
04:55:13 PM   10    4.69    0.00    1.92    0.00    0.00    5.40    0.00    0.00    0.00   87.98
04:55:13 PM   11    2.85    0.00    1.32    0.00    0.00    0.00    0.00    0.00    0.00   95.83
04:55:13 PM   12    2.76    0.00    1.15    0.00    0.00    0.00    0.00    0.00    0.00   96.09
04:55:13 PM   13    2.74    0.00    1.12    0.00    0.00    0.00    0.00    0.00    0.00   96.14
04:55:13 PM   14    0.66    0.00    1.09    0.00    0.00    0.00    0.00    0.00    0.00   98.25
04:55:13 PM   15    0.59    0.00    1.00    0.00    0.00    0.00    0.00    0.00    0.00   98.41
04:55:13 PM   16   44.16    0.00    0.96    0.00    0.00    0.84    0.00    0.00    0.00   54.03
04:55:13 PM   17   54.74    0.00    1.39    0.00    0.00    0.56    0.00    0.00    0.00   43.31
04:55:13 PM   18   56.04    0.00    1.52    0.00    0.00    1.58    0.00    0.00    0.00   40.87
04:55:13 PM   19   53.10    0.00    1.25    0.00    0.00    0.51    0.00    0.00    0.00   45.14
04:55:13 PM   20   42.60    0.00    1.11    0.00    0.00    0.20    0.00    0.00    0.00   56.10
04:55:13 PM   21   41.77    0.00    0.90    0.00    0.00    0.66    0.00    0.00    0.00   56.67
04:55:13 PM   22   43.89    0.00    1.69    0.00    0.00    1.35    0.00    0.00    0.00   53.06
04:55:13 PM   23   42.25    0.00    1.64    0.00    0.00    1.18    0.00    0.00    0.00   54.93
04:55:13 PM   24   51.22    0.00    1.29    0.00    0.00    0.00    0.00    0.00    0.00   47.49
04:55:13 PM   25   50.81    0.00    1.28    0.00    0.00    0.00    0.00    0.00    0.00   47.91
04:55:13 PM   26   50.94    0.00    1.27    0.00    0.00    0.00    0.00    0.00    0.00   47.79
04:55:13 PM   27   37.79    0.00    1.04    0.00    0.00    0.00    0.00    0.00    0.00   61.18
04:55:13 PM   28   39.37    0.00    1.06    0.00    0.00    0.00    0.00    0.00    0.00   59.57
04:55:13 PM   29   37.78    0.00    1.03    0.00    0.00    0.00    0.00    0.00    0.00   61.20
04:55:13 PM   30   39.21    0.00    1.05    0.00    0.00    0.00    0.00    0.00    0.00   59.74
04:55:13 PM   31   37.66    0.00    1.02    0.00    0.00    0.00    0.00    0.00    0.00   61.32
```

YOOZOO GAMES

Thanks

招数据安全