2012

第一届
全国网络与信息安全防护峰会

对话·交流·合作

CONVERSATION · COMMUNICATION · COOPERATION

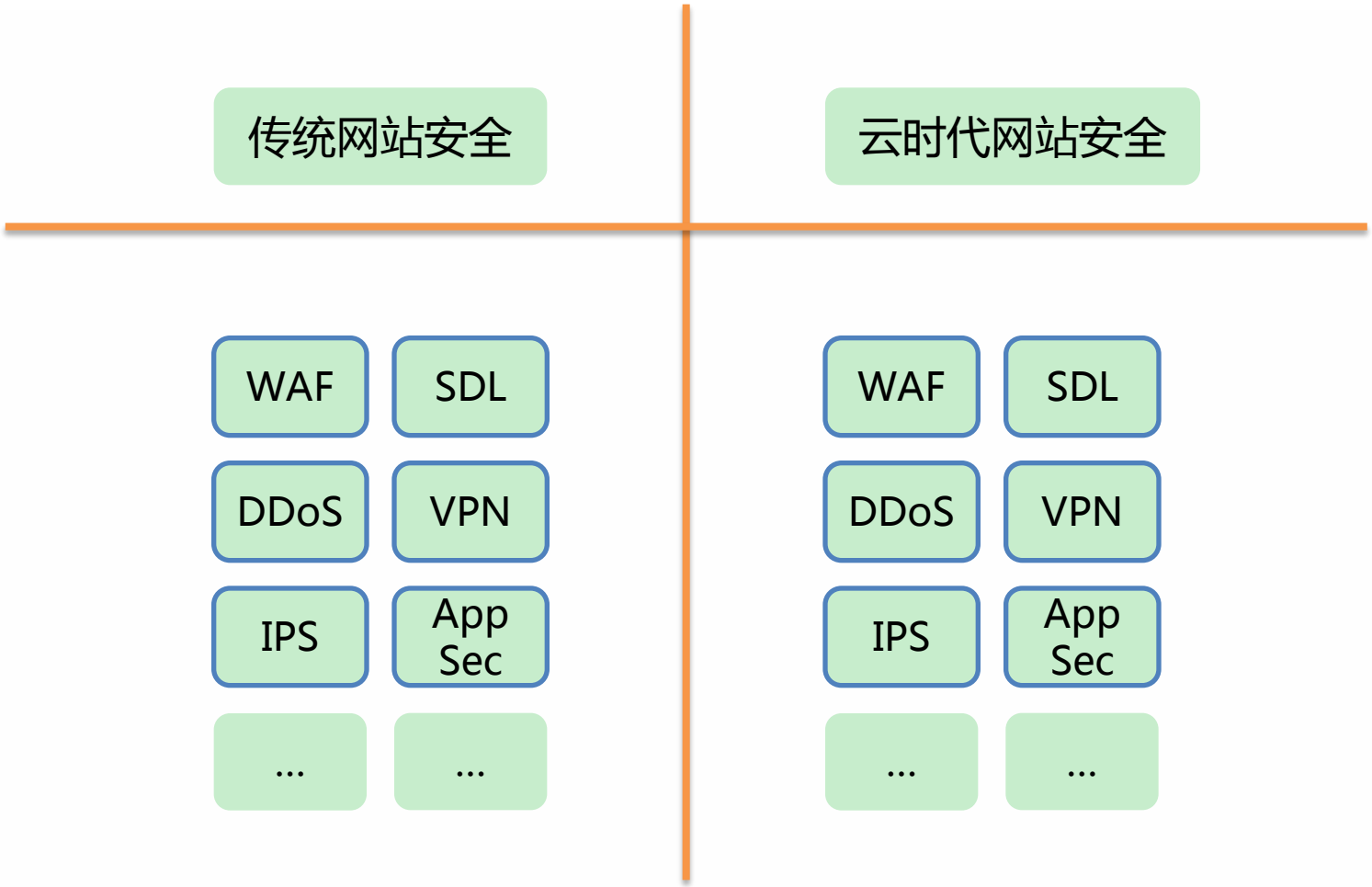
XDef 2012
对话·交流·合作

云时代下的安全思考

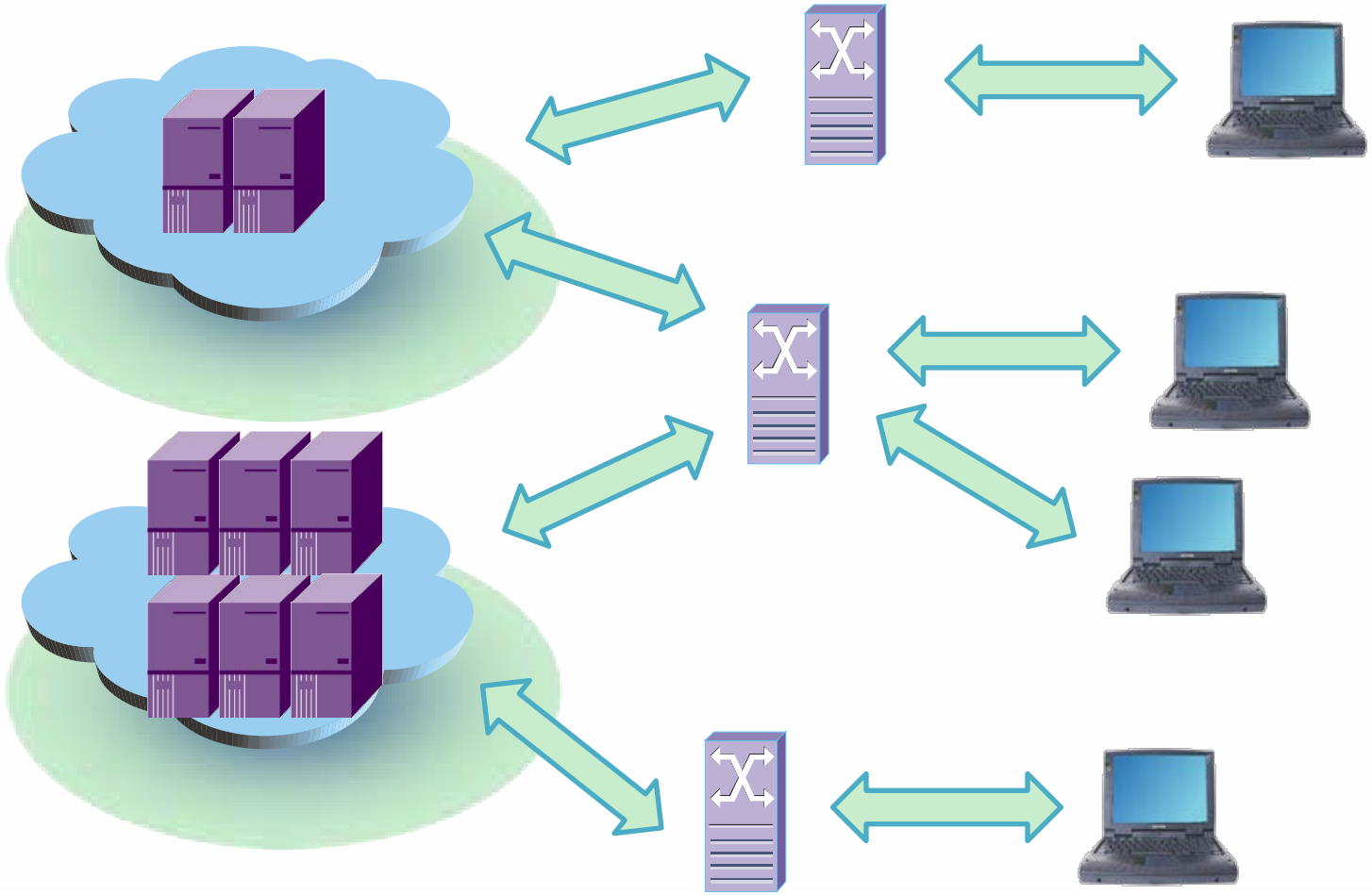
----聪明的应用层安全防护体系

李诚
安全宝

云时代下的网站安全

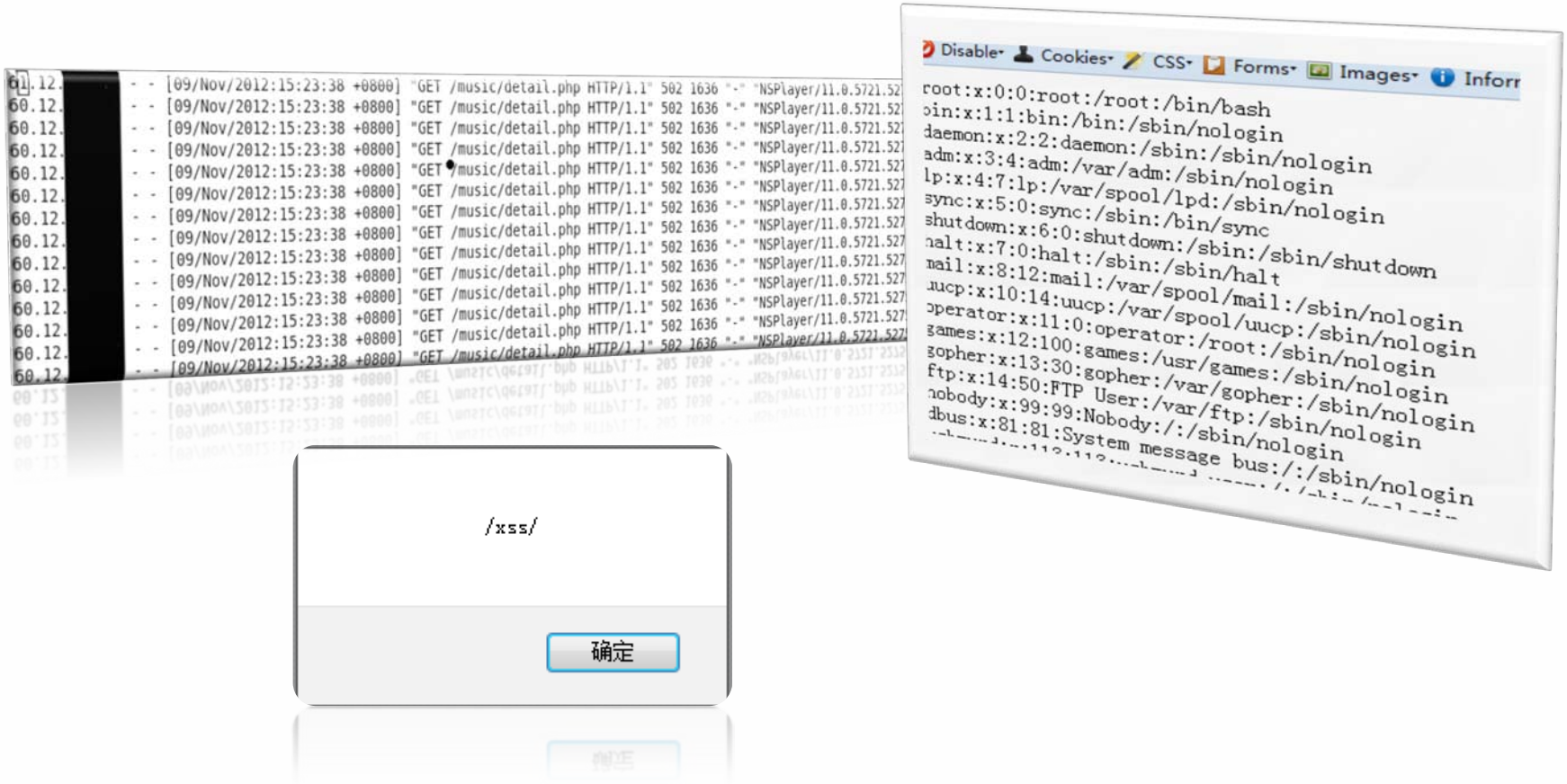

传统网站安全
WAF
SDL
DDoS
VPN
IPS
App Sec
…
…
云时代网站安全
WAF
SDL
DDoS
VPN
IPS
App Sec
…
…

云时代下的安全



从数据挖据看应用层安全

老生常谈


- - [09/Nov/2012:15:23:38 +0800] "GET /music/detail.php HTTP/1.1" 502 1636 "-" "NSPlayer/11.0.5721.527
Disable Cookies CSS Forms Images Inforr
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
/xss/
确定

几组数据

2012年：

- http GET DDOS攻击约占所有DDOS攻击的24.30%

  并且http GET DDOS呈逐年上升趋势
- XSS（cross site script）约占web漏洞的31.60%
- SQL injection约占web漏洞的3.70%
- ……

- 攻击行为从网络层转向应用层是一种趋势

经验，能告诉我们

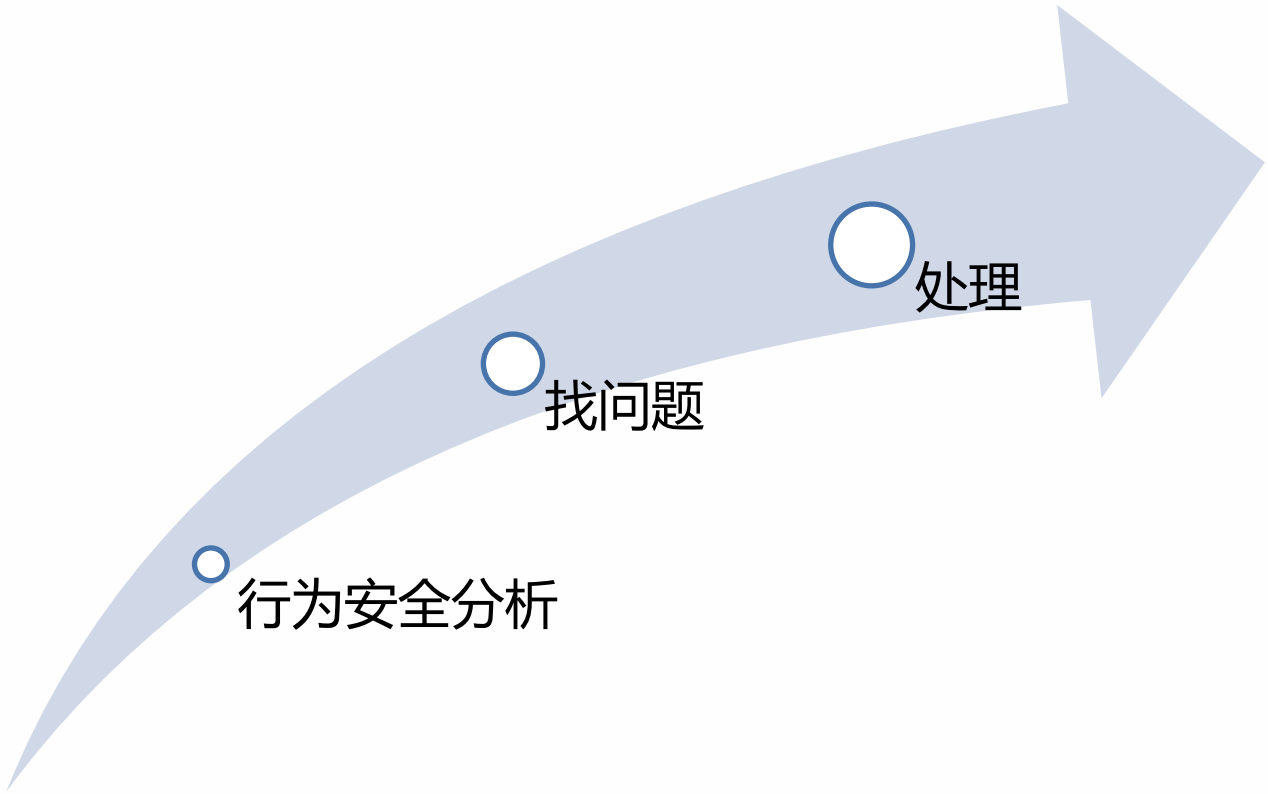
- 阈值
  - 单IP每秒请求30次 = 攻击？ 单IP每秒请求20次 = 攻击？
  - 登陆密码连续错误3次 = 暴力破解？
- 特征
  - http://www.test.com?test=<script>alert(1)</script>
  - POSTDATA： cmd=adduser helloworld;
  - ……

短木板

经验=指导!=结论

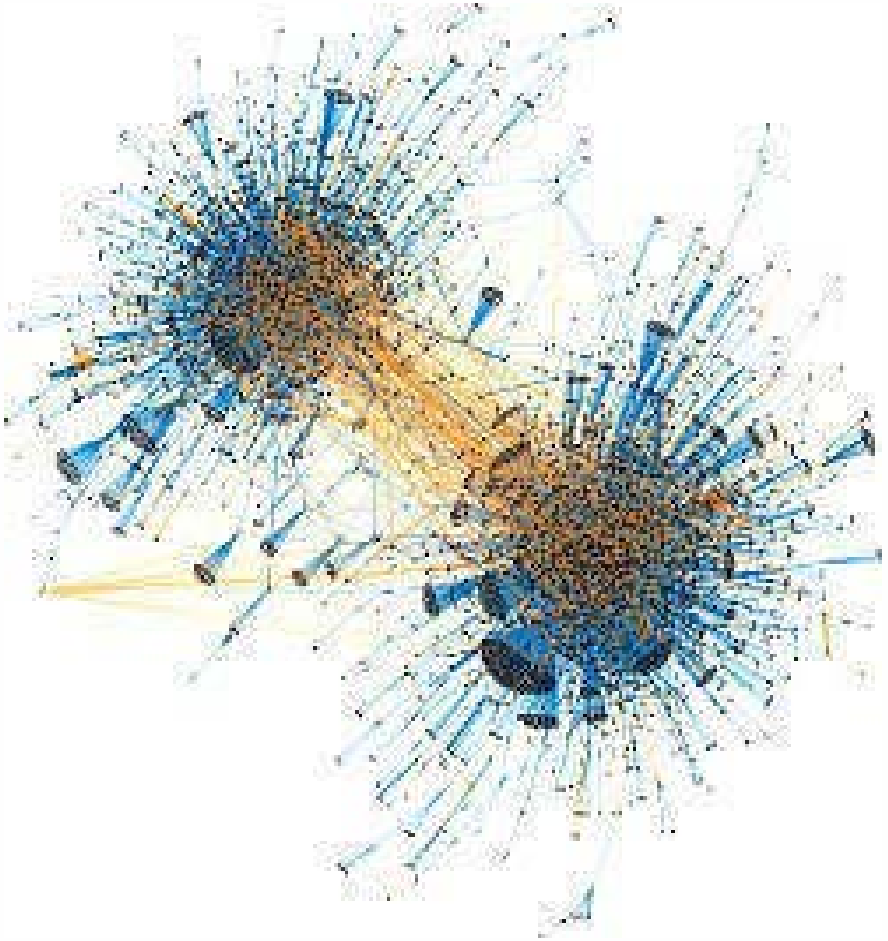
- 阈值：紧了怕误伤，松了怕无效。
- 情况天天在变！
- Bypass！

数据，行为安全分析

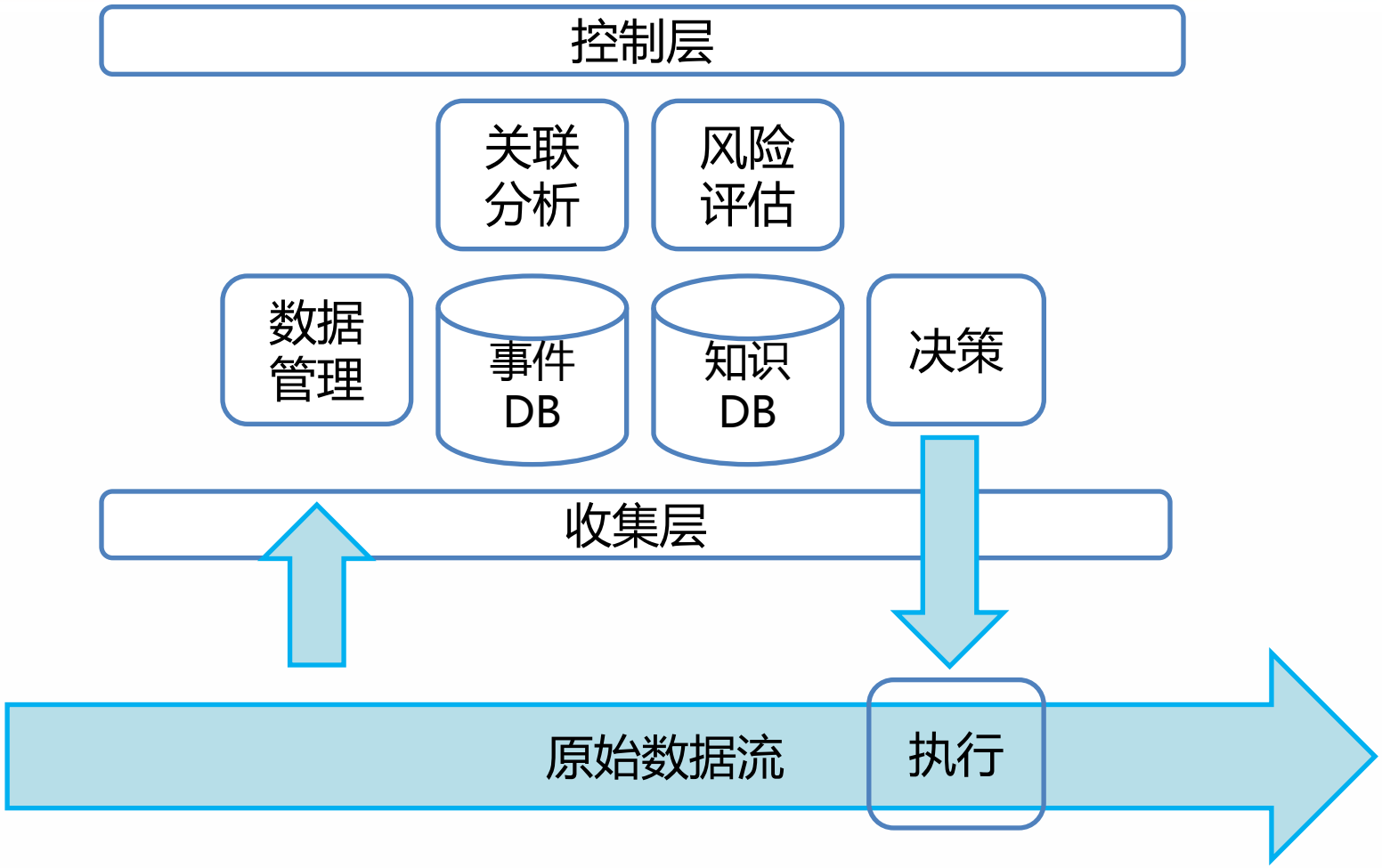


分析什么？怎么分析？

- 找异常的思想：
  - 整理
  - 关联
- 个体的异常：
  - 不合群
    - 行为重复
    - 周期频率
    - 个体特征
- 全局的异常：
  - 变化趋势
- 抽象一般化模型



功能结构



Why

- 实时数据分析
  - 有限的数据
  - 简单的计算
  - 逻辑的耦合
  - 实时性高
- 离线数据分析
  - 实时性不高
  - 更复杂的计算
  - 更大的数据量
  - 逻辑的隔离

- 到底需要什么？
  - 既实时的数据分析
  - 也需要离线数据分析
  - 或者是两者的均衡

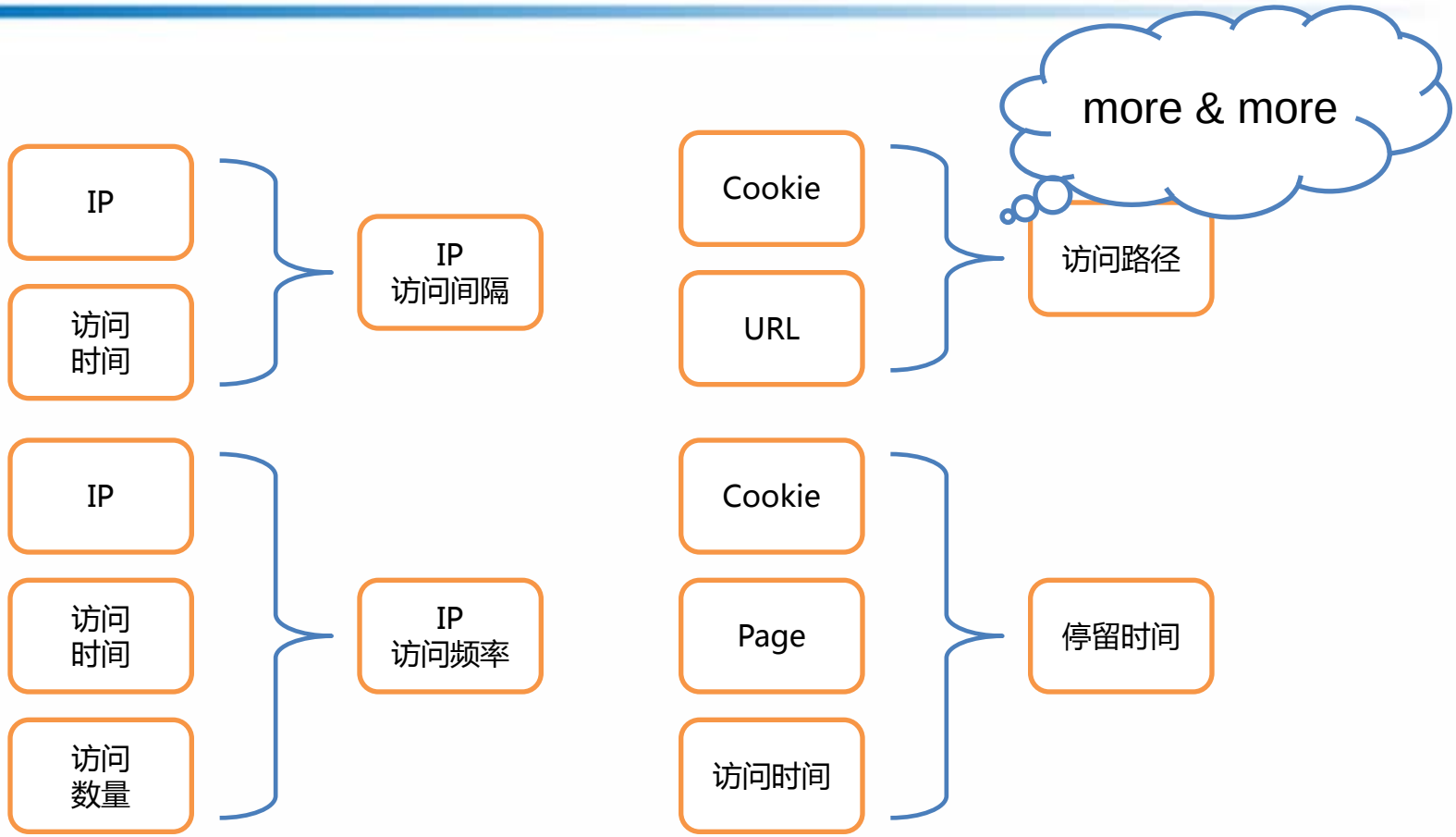
原材料

能够获取的原料：

- IP
- Cookie
- URL
- 参数
- 访问时间
- 响应时长
- 返回状态

……

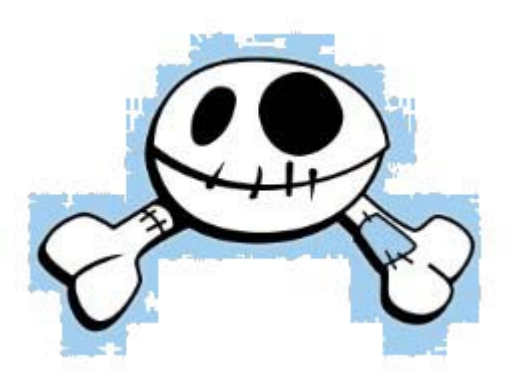
加工


more & more
IP
访问时间
IP
访问间隔
Cookie
URL
访问路径
IP
访问时间
访问数量
IP
访问频率
Cookie
Page
访问时间
停留时间

从数据中获得指导

- 获得并修正经验曲线
  - 记录数据，分析走势，同比，环比
  - 训练，根据实际情况调整经验曲线和波动范围

  - 有对比才能知道不同



图一

对话·交流·合作

```
CCAP> show site bbs.[redacted]
NOW:2012-11-10 18:13:46
Site: bbs[redacted]      Last Request: 2012-11-10 18:13:45
Current  QPS:      18
Last 60s QPS:      18       5      27      41       6       4      10       0      47      13
                   23      67       9      46       8       4       5       8      13      15
                    6      19      19      74      57      36      82      82      13       9
                    0       7       3      39       1       6      11      10       4       1
                    3       5      14      43       9       4       2       5      13       4
                    4       9      17      57      35      63      77      48      64      15
Last 60m QPM:    1616    1309    1245    1288    1203    1304    1456    1569    1138     714
                  939    1121    1407     971    1645    1190    1282    1265    1544    2097
                 1699    1710    1447    1496    1476    1957    1728    2336    1589    1483
                 1599    1834    1520    1459    1644    1428    1416    1495    1191    1502
                 1550    1133    1284    1557    1299    1286    1074    1357    1391    1455
                 1779    1201    1378    1606    1533    1533    1560    1853    1451    1636
Last 24h QPH:   91842  100798   17603       0       0       0       0       0       0       0
                    0       0       0       0       0       0       0       0       0       0
                    0       0       0       0
Current  DELAY:   0.419
Last 60s DELAY:   0.106   0.000   0.166   0.215   0.145   0.307   0.097   0.000   0.122   0.285
                  0.129   0.109   0.220   0.129   0.248   0.311   0.181   0.103   0.281   0.190
                  0.148   0.399   0.152   0.371   0.244   0.205   0.368   0.147   0.000   0.418
                  0.000   0.666   0.532   0.500   0.101   0.492   0.645   0.696   0.166   0.134
                  0.299   0.686   0.445   0.425   0.374   1.533   0.000   0.341   0.452   0.377
                  0.272   0.383   0.167   0.413   0.189   0.208   0.153   0.154   0.454   0.264
5s  Avg  DELAY:   0.155   0.179   0.158   0.154   0.128   0.170   0.157   0.155   0.159   0.160
                  0.152   0.175   0.201   0.176   0.212   0.196   0.176   0.218   0.230   0.231
                  0.250   0.248   0.238   0.234   0.224   0.249   0.269   0.312   0.525   0.518
                  0.516   0.514   0.541   0.566   0.489   0.491   0.453   0.415   0.379   0.437
                  0.443   0.661   0.656   0.656   0.705   0.706   0.355   0.365   0.330   0.349
                  0.312   0.280   0.230   0.225   0.225
Req  Status Code:    rate all_reqs   400   499   4xx   500   502   5xx
Last Second Code: 100.0%       18     0     0     0     0     0     0
Curr Minite Code: 100.0%      926     0     0     0     0     0     0
Curr  Hour  Code:  99.9%    16309     0     0     9     0     0     0

CCAP>
```

图二

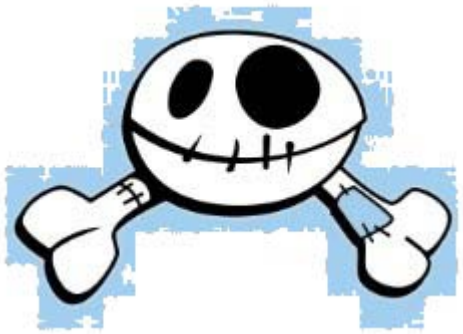
对话·交流·合作

```
CCAP> show page [redacted]/sendgift.htm
NOW:2012-11-17 18:10:54
Site: [redacted]      Last Request: 2012-11-17 17:27:14

Today All Request:
[11/Nov/2012:07:03:18 +0800] "GET /bbs/sendgift.htm?uid=10123&gift=rose&to=977[redacted]"
[11/Nov/2012:09:11:23 +0800] "GET /bbs/sendgift.htm?uid=83[redacted]6&gift=cake&to=1[redacted]34"
[11/Nov/2012:09:12:51 +0800] "GET /bbs/sendgift.htm?uid=1[redacted]2&gift=rose&to=3[redacted]03"
[11/Nov/2012:10:07:10 +0800] "GET /bbs/sendgift.htm?uid=5[redacted]6&gift=rose&to=9[redacted]2"
[11/Nov/2012:13:21:33 +0800] "GET /bbs/sendgift.htm?uid=1[redacted]6&gift=apple&to=[redacted]084"
[11/Nov/2012:13:27:14 +0800] "GET /bbs/sendgift.htm?uid=4[redacted]6&gift=rose&to=8[redacted]5"
[11/Nov/2012:13:30:16 +0800] "GET /bbs/sendgift.htm?uid=9[redacted]&gift=apple&to=6[redacted]76"
[11/Nov/2012:13:31:19 +0800] "GET /bbs/sendgift.htm?uid=9[redacted]&gift=rose&to=1[redacted]5"
[11/Nov/2012:14:03:18 +0800] "GET /bbs/sendgift.htm?uid=21[redacted]&gift=rose&to=39[redacted]4"
[11/Nov/2012:15:11:23 +0800] "GET /bbs/sendgift.htm?uid=83[redacted]&gift=cake&to=11[redacted]4"
[11/Nov/2012:16:12:51 +0800] "GET /bbs/sendgift.htm?uid=17[redacted]&gift=rose&to=45[redacted]3"
[11/Nov/2012:16:27:10 +0800] "GET /bbs/sendgift.htm?uid=5[redacted]6&gift=rose&to=90[redacted]"
[11/Nov/2012:16:27:13 +0800] "GET /bbs/sendgift.htm?uid=5[redacted]6&gift=rose&to=90[redacted]"
[11/Nov/2012:16:27:21 +0800] "GET /bbs/sendgift.htm?uid=5[redacted]6&gift=gold&to=80[redacted]"
[11/Nov/2012:16:31:19 +0800] "GET /bbs/sendgift.htm?uid=1[redacted]2&gift=rose&to=1[redacted]5"
[11/Nov/2012:16:33:18 +0800] "GET /bbs/sendgift.htm?uid=3[redacted]33&gift=rose&to=97[redacted]4"
[11/Nov/2012:16:41:23 +0800] "GET /bbs/sendgift.htm?uid=8[redacted]36&gift=cake&to=1[redacted]34"
[11/Nov/2012:16:52:51 +0800] "GET /bbs/sendgift.htm?uid=1[redacted]2&gift=rose&to=59[redacted]"
[11/Nov/2012:17:27:10 +0800] "GET /bbs/sendgift.htm?uid=5[redacted]6&gift=rose&to=90[redacted]2"
[11/Nov/2012:17:27:13 +0800] "GET /bbs/sendgift.htm?uid=5[redacted]6&gift=rose&to=19[redacted]34"
[11/Nov/2012:17:27:14 +0800] "GET /bbs/sendgift.htm?uid=5976&gift=gold&to=8[redacted]5"

Type identification:  Parameter      Type      Matchrate
Type identification:        uid  interage           100%
Type identification:       gift   no sure              -
Type identification:         to   no sure              -

CCAP>
```

聪明

找问题找特征

- 分析特征
  - 找到被攻击点
  - 事件的聚合
  - 从关联的结果中寻找出相同点，抓出提取特征



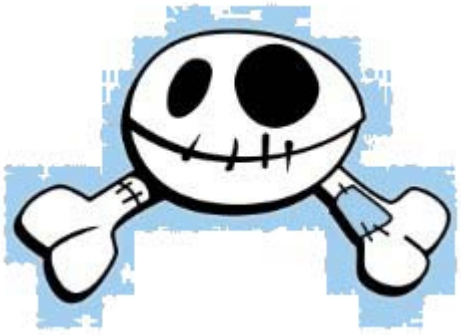
图三

对话·交流·合作

```
CCAP> show site url v[redacted].com
url_num = 525
 seq times v_times  r_time ip_num url
   1  1244    1244   0.049      5 [1214663415]/download.asp
   2   335     335   0.420      0 [ 266597082]not attention
   3   123     123   0.200      0 [  77967832]not attention
   4   102     102   0.135      0 [2176651233]not attention
   5    71       1   0.173      0 [ 896668193]not attention
   6    70       1   0.183      0 [1471714855]not attention
   7    70       1   0.069      0 [3219899057]not attention
   8    68       1   0.137      0 [3535444837]not attention
   9    62       1   0.041      0 [ 964155012]not attention
  10    59       1   0.073      0 [3331217586]not attention
  11    55       0   0.000      0 [3152095566]not attention
  12    49       0   0.000      0 [2426865740]not attention
  13    49       0   0.000      0 [4013634169]not attention
  14    48       0   0.000      0 [2219634953]not attention
  15    48       0   0.000      0 [ 367184396]not attention
  16    48       0   0.000      0 [3643928850]not attention
  17    48       0   0.000      0 [ 719925318]not attention
  18    48       0   0.000      0 [2186777683]not attention
  19    48       0   0.000      0 [3608767833]not attention
  20    48       0   0.000      0 [2890455949]not attention

CCAP> show site url ip [redacted] 1214663415
ip_num = 5
 seq          ip       times LastRequestTime
   1   98.229.[redacted]     2 2012-11-19 13:16:36
   2    59.33.[redacted]     2 2012-11-19 13:16:20
   3  113.107.[redacted]     1 2012-11-19 13:16:24
   4    59.33.[redacted]     1 2012-11-19 13:16:30
   5    59.33.[redacted]     1 2012-11-19 13:16:29

CCAP>
```

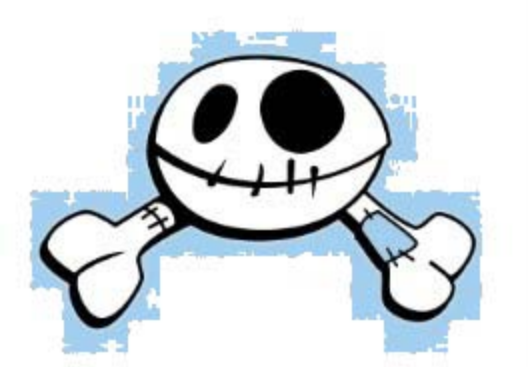
风险评估

- 可用性评估
  - 当前的行为是不是会引起服务器资源的持续恶化
- 恶意性评估
  - 具备确认的攻击特征
  - 攻击类型评估
- 不同的评估结果对应不同的处理方式



降低风险

- 策略确认
  - 策略增强
    - 分析过程是不断持续的过程，更多的特征被分析出来
    - 转移
  - 策略退化
    - 资源的好转
    - 可能出现的高误杀率



展望未来

- 更聪明
- 更定制
- 更准确
- 更有效

国际惯例

对话·交流·合作

谢谢！

Email: Cheng.li@unlun.com