基于威胁情报的数据分析和自动决策

黄凯

证通股份有限公司

关于我

8 年安全从业经验 证通公司安全技术负责人

负责

信息安全技术体系管理

安全监控系统运营

安全技术调研 等

关于证通

证券机构

互联网企业

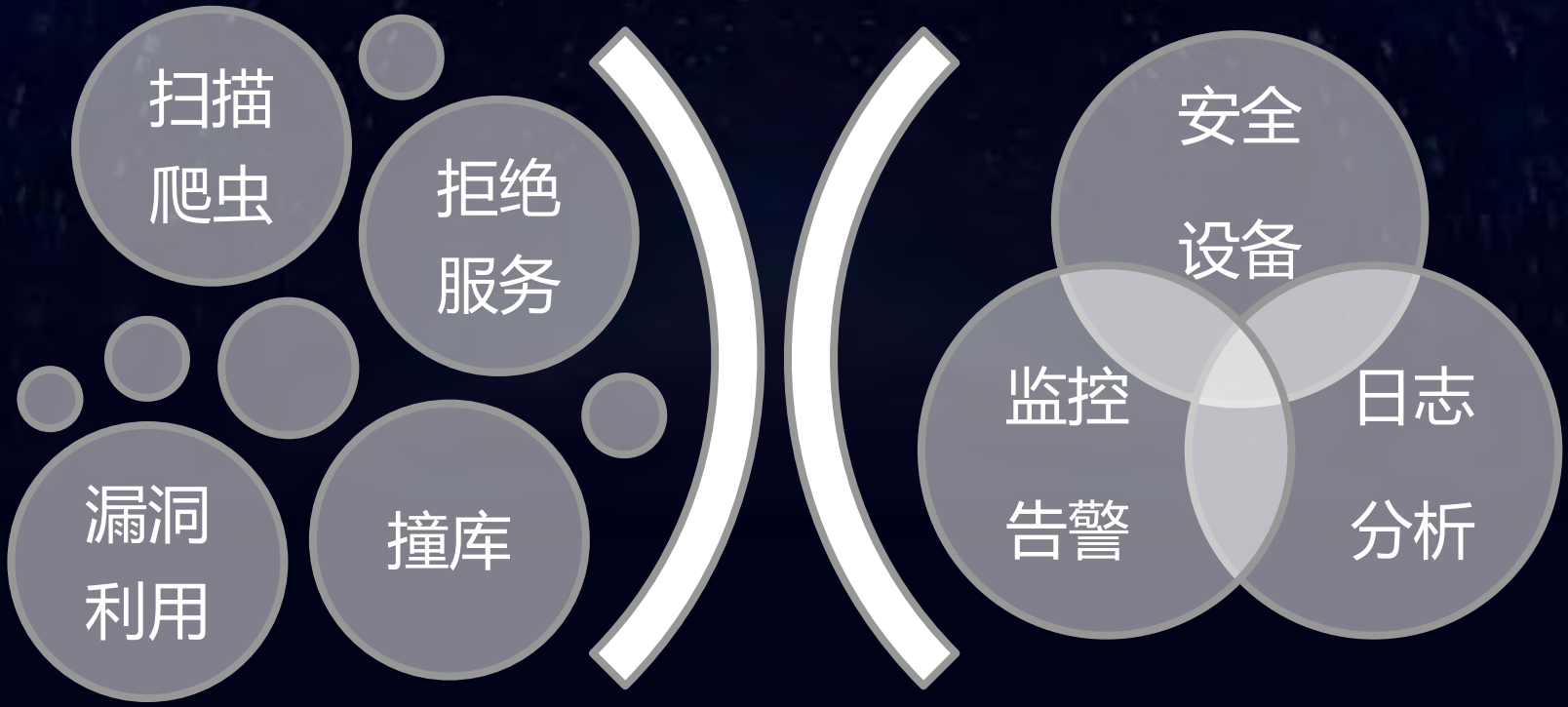
金融服务机构

金融机构（证券业为主）

互联网企业

安全需求

安全挑战



安全挑战

监控对象	告警级别	告警状态	告警内容
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	WAF检测到11.22.33.44正在扫描
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]

WAF检测到11.22.33.44正在扫描

知己知彼

知己

- 代码检测
- 漏洞扫描
- 资产识别

知彼

- 威胁情报

系统架构

步骤1：日志字段提取

发生时间/2016-12-02 17:59:04,威胁/低,事件/缺失报头,请求方法/GET,URL地址//,POST数据/,服务器IP/x.x.x.x,主机名/,服务器端口/xxxxx,客户端IP/222.x.x.130,客户端端口/55756,客户端环境/,标签/缺失报头,动作/告警,HTTP/S响应码/403,攻击特征串/,触发规则/11030002,访问唯一编号/WEFF6H8AAAEAAWpgNTQAACwP,国家/中国,省/四川,市/成都

```
... | rex field=some_field "(?<capture_name>.*)"
```

步骤1：日志字段提取

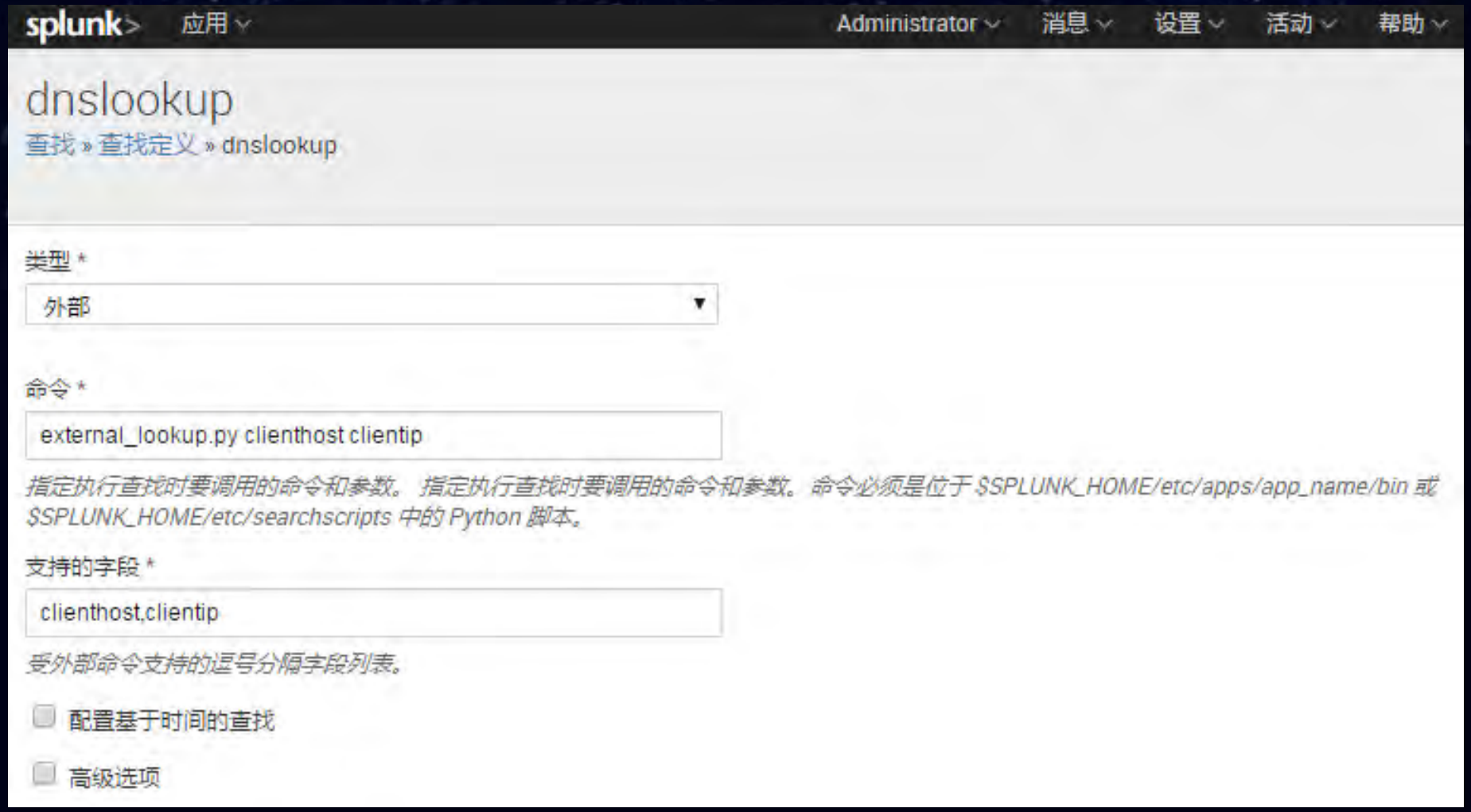
事件 | threat_level | rule_name | request_method | request_host | request_uri | post_data | server_ip | hostname | server_port | client_ip | client_port | user_agent
attack_payload | rule_id | request_id | country | province | city

✓ 1,000 个事件 (17/06/27 17:25:48.000 之前)　每页 20 个　〈预览　1

过滤器　应用　示例: 前 1,000 个事件　所有事件　所有事件　匹配　不匹配

_raw	threat_level	rule_name	request_method	request_ho
✓ Jun 27 16:07:40 10.63.0.45 Jun 27 16:07:40 . 发生时间/2017-06-27 16:07:37,威胁/高,事件/漏洞防护,请求方法/GET,URL地址/ ,2/validate.php/ n=discover&proto=http&ip= ?&port=80&t=1498550856868&h=< %cip= xff= &loc=1156310000,POST数据/ ,服务器IP/ ,主机名/ 2,服务器端口/10000,客户端IP/ 客户端端口/28670,客户端环境/python-requests/2.17.3,标签/漏洞防护,动作/告警,HTTP/S响应码/404,攻击特征串/python-requests/,触发规则/18010042,访问唯一编号/WVISSX8AAAEAAHKHSsMAADyA,国家/加拿大,省/NIL,市/NIL	高	漏洞防护	GET	
✓ Jun 27 16:07:40 10.63.0.45 Jun 27 16:07:40 发生时间/2017-06-27 16:07:37,威胁/高,事件/漏洞防护,请求方法/GET,URL地址/ /validate.php? n=discover&proto=http&ip= &port=80&t=1498550856868&h= &cip= xff= &loc=1156310000,POST数据/ ,服务器IP/ ,主机名/ ,服务器端口/10000,客户端IP/ ,客户端端口/28670,客户端环境/python-requests/2.17.3,标签/漏洞防护,动作/告警,HTTP/S响应码/404,攻击特征串/python-requests/,触发规则/18010042,访问唯一编号/WVISSX8AAAEAAHKHSsMAADyA,国家/加拿大,省/NIL,市/NIL	高	漏洞防护	GET	
✓ Jun 27 16:07:40 10.63.0.45 Jun 27 16:07:40 发生时间/2017-06-27 16:07:37,威胁/高,事件/漏洞防护,请求方法/GET,URL地址/ /validate.php? n=discover&proto=http&ip= &port=80&t=1498550856868&h= &cip= &loc=1156310000,POST数据/ ,服务器IP/ ,主机名/ ,服务器端口/10000,客户端IP/ ,客户端端口/28670,客户端环境/python-requests/2.17.3,标签/漏洞防护,动作/告警,HTTP/S响应码/404,攻击特征串/python-requests/,触发规则/18010042,访问唯一编号/WVISSX8AAAEAAHKHSsMAADyA,国家/加拿大,省/NIL,市/NIL	高	漏洞防护	GET	
✓ Jun 27 16:07:23 10.127.0.45 Jun 27 16:07:23 发生时间/2017-06-27 16:07:23,威胁/高,事件/漏洞防护,请求方法/GET,URL地址/ idate.php? n=discover&proto=http&ip= &port=80&t=1498550841617&h= &cip= %xff=1 loc=1156310000,POST数据/ ,服务器IP/ ,主机名/ ,服务器端口/10000,客户端IP/ ,客户端端口/12676,客户端环境/python-requests/2.17.3,标签/漏洞防护,动作/告警,HTTP/S响应码/404,攻击特征串/python-requests/,触发规则/18010042,访问唯一编号/WVISOn8AAAEAAEq8nCYAAAKY,国家/加拿大,省/NIL,市/NIL	高	漏洞防护	GET	
✓ Jun 27 16:07:23 10.127.0.45 Jun 27 16:07:23 发生时间/2017-06-27 16:07:19,威胁/高,事件/漏洞防护,请求方法/GET,URL地址/ /validate.php/ n=discover&proto=http&ip= 2&port=80&t=1498550837917&h= &cin=1 ff= &loc=1156310000,POST数据/ ,服务器IP/ ,主机名/ ,服务器端口/10000,客户端IP/ ,客户端端口/13460,客户端环境/python-requests/2.17.3,标签/漏洞防护,动作/告警,HTTP/S响应码/404,攻击特征串/python-requests/,触发规则/18010042,访问唯一编	高	漏洞防护	GET	

步骤2：威胁情报接口调用



步骤3：数据整合

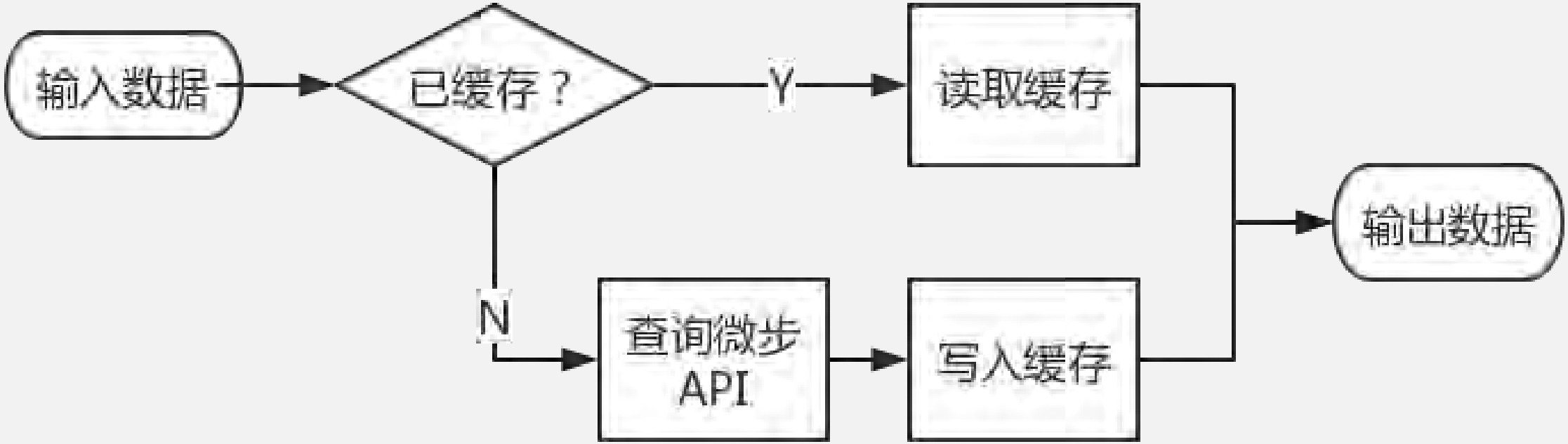

```
{"response_code":0,"hit":{"expired":false,"detected":
true,"info":["zombie","idc","compromised","spam"]},"i
p":{"carrier":"1and1.com","ip":"82.165.37.26","locati
on":{"country":"德国","province":"德国
","lng":"10.454150","city":"","lat":"51.164181"}}}
```


```
...  | stats count by client_ip server_ip | lookup iplookup
ip as client_ip OUTPUT info as _TI | spath input=_TI
```

步骤3：数据整合

hit.detected	hit.expired	hit.info{}	intelligences{}.confidence	intelligences{}.find_time	intelligences{}.intel_types{}	intelligences{}.source	ip.carrier
true	false	idc	90	2016-07-08 23:18:13	IDC服务器	ThreatBook Labs	
		compromised	70	2016-05-17 20:17:47	IDC服务器	ThreatBook Labs	
		spam	85	2016-04-19 08:00:53	垃圾邮件	ThreatBook Labs	
			75	2016-04-19 07:04:04	垃圾邮件	ThreatBook Labs	
			75	2016-04-16 14:53:53	垃圾邮件	ThreatBook Labs	
			75	2016-02-19 12:16:51	垃圾邮件	ThreatBook Labs	
false	false	dynamic_ip	80	2016-05-17 12:06:53	动态IP	ThreatBook Labs	电信
true	false	idc	90	2016-07-08 23:18:13	IDC服务器	ThreatBook Labs	
		compromised	70	2016-05-17 20:16:19	IDC服务器	ThreatBook Labs	
		spam	75	2016-02-19 12:16:51	垃圾邮件	ThreatBook Labs	
true	false	idc	90	2016-05-11 17:21:01	IDC服务器	ThreatBook Labs	阿里云/电信/联通/移动/铁通/教育网
			90	2016-05-11 17:21:01	IDC服务器	ThreatBook Labs	
true	false	idc	90	2016-07-08 23:18:06	IDC服务器	ThreatBook Labs	
		compromised	75	2016-06-21 10:26:41	扫描	开源情报	
		spam	70	2016-05-17 20:15:45	IDC服务器	ThreatBook Labs	
			75	2016-02-19 12:16:51	垃圾邮件	ThreatBook Labs	

步骤4：威胁查询优化



步骤5：事件联动接口调用

```
for ads in ADS_LIST:
    one_result = {}
    one_result['ads_host'] = ads
    one_result['param'] = p
    try:
        r = urllib2.urlopen('https://%s/facade/unifiedInterface.php?%s' % \
            (ads, urlencode(p)), timeout=5)
        if r.getcode() == 200:
            success = True
        else:
            success = False

        one_result['success'] = success
        one_result['info'] = r.read()
        success_flag = success_flag * 0

    except Exception as e:
        success_flag = success_flag * 0
        one_result['success'] = False
        one_result['info'] = e
        #return False, e
    result_list.append(one_result)
```

实现1：分析评估

112.2	.182[中国山东临沂联通(垃圾邮件、僵尸网络、动态IP)]正在对 送验证码页面进行异常访问11次
117.62	8[中国江苏苏州电信(垃圾邮件、僵尸网络、动态IP)]正在对 送验证码页面进行异常访问11次
112.23	.182[中国山东临沂联通(垃圾邮件、僵尸网络、动态IP)]正在对 送验证码页面进行异常访问23次
114.24	215[中国北京北京联通]正在对 发送验证码页面进行异常访问21次
115.15	46[中国江西上饶电信(动态IP)]正在对 发送验证码页面进行异常访问14次
117.62	3[中国江苏苏州电信(垃圾邮件、僵尸网络、动态IP)]正在对 发送验证码页面进行异常访问18次
117.90	30[中国江苏镇江电信(僵尸网络、垃圾邮件、动态IP)]正在对 发送验证码页面进行异常访问13次

实现2：本地威胁情报库

IP、域名 分析

基本信息

IP地址	
地理位置	中国,上海,上海(联通)
标签	[僵尸主机, 受控主机, 垃圾邮件]

威胁情报

显示 5 项结果 搜索:

序号	情报源	发现时间	情报类型
1	开源情报	2016-08-02 04:37:13	僵尸网络
2	开源情报	2016-08-01 21:15:20	垃圾邮件 僵尸网络

显示第 1 至 2 项结果，共 2 项 上页 1 下页

攻击信息

显示 10 项结果 搜索:

序号	时间	源IP	目的IP	系统名称	攻击类型	风险
1	2017-06-21 23:36:21			网络系统	扫描踩点	低

显示第 1 至 1 项结果，共 1 项 上页 1 下页

实现3：分析模型优化


各安全域运行指数
200
0
陕西
江苏
上海
广东
最新威胁
时间
资产名称
攻击者画像
攻击阶段
威胁等级
02-16 16:43
02-16 16:41
02-16 16:29
02-16 16:16
02-16 16:09
手机网络
扫描跳点
中
近30天威胁趋势

实现4：自适应决策

211. 193[中国四川电信(IDC服务器)]正在对. 进行漏洞扫描 总计207次 (200响应0次 404响应207次 500响应0次 其它响应0次)

221. 105[中国江苏徐州电信(撞库、垃圾邮件、僵尸网络、可疑、扫描、IDC服务器)]扫描ZTP证通官网(, 已被阻断。（ 分钟后解封，仅保持持续关注）

119. 227[中国广东深圳电信(垃圾邮件、僵尸网络、动态IP)]正在对 进行跨站攻击，经智能漏洞验证确认目标URL不存在漏洞，仅保持关注

使用威胁情报的收益

- 安全事件评估的有力参考，安全威胁态势一目了然
- 过滤无效告警，人工介入减少90%+
- 为安全运营提供全新安全视角和更广视野

探索

kafka

elasticsearch

资产信息库
漏洞历史库
微步威胁情报

Spark Streaming


谢谢！