打造自适应攻击验证系统

携程信息安全部　　凌霄

2017携程信息安全沙龙

目录

CONTENTS

ENTER YOUR COMPANY NAME

攻击来源

如何处理

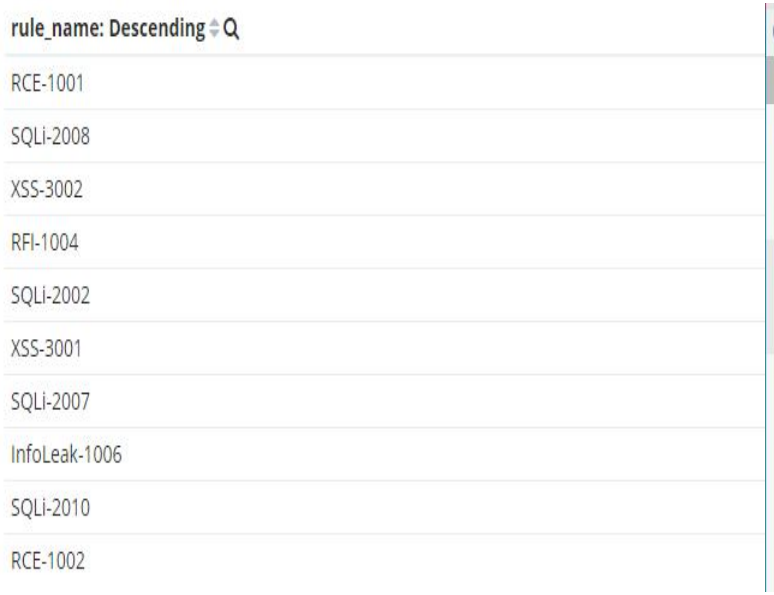
遇到的问题

持续改进

攻击来源

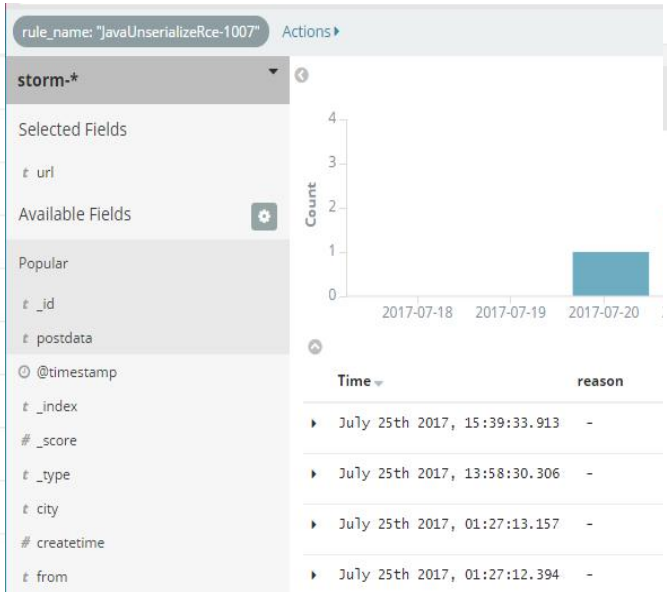
常见安全漏洞巡查

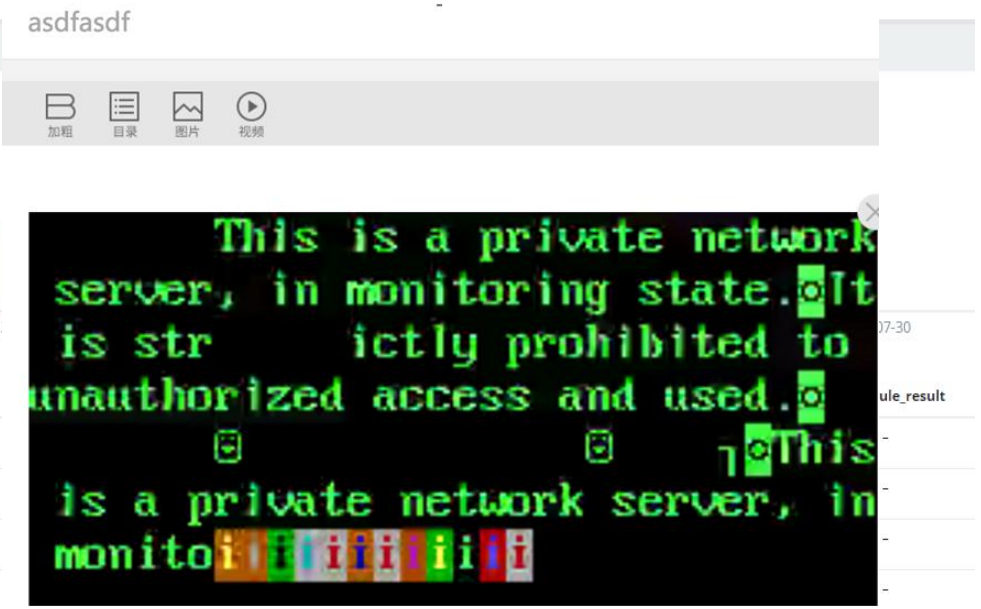
1



突发安全漏洞利用

2

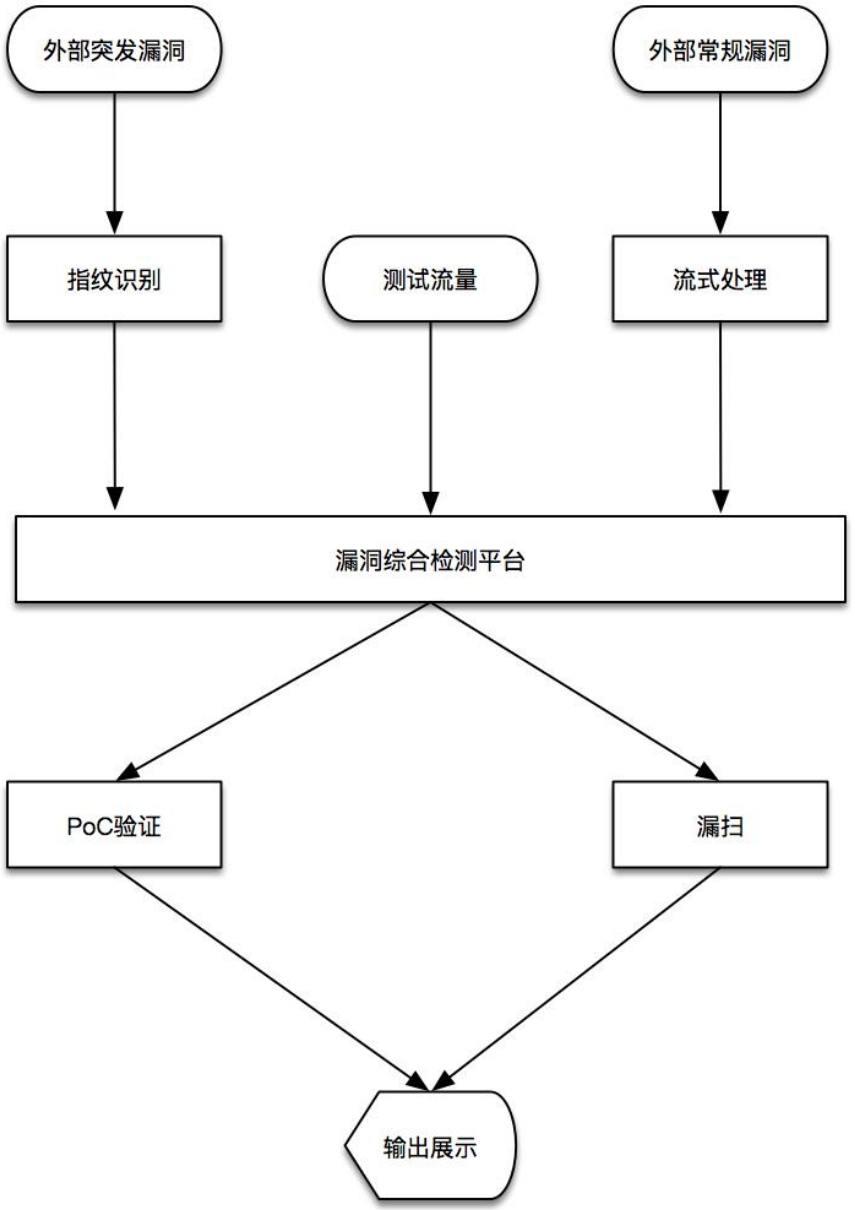




整体架构

1，基于指纹的资产信息整理
2，基于外部攻击的接口捕获
3，基于攻击数据的流式验证
4，高度自定义的验证方式

站在攻击者的肩膀上



处理海量告警 -- Webshell

初级告警 -- Webshell

Time	reason	srcip	url	ml_result	rule_result
July 31st 2017, 14:02:16.795	-	-	ct.ctrip.com//admin/error.asp	-	-

Table JSON

Link to /stormshell-2017.07/webshell/AV2XPOVw3_D_nh6WcIQ6

@timestamp	July 31st 2017, 14:02:16.795
_id	AV2XPOVw3_D_nh6WcIQ6
_index	stormshell-2017.07
_score	-
_type	webshell
city	重庆
created_at	July 31st 2017, 22:02:16.795
host	ct.ctrip.com
latitude	29.533155
longitude	106.504962
method	POST
port	80
postdata	niyade=Execute++++++++++++++++++++++++++++++("++++++++++++++++++++++++++++++Execute++++++++++++++++++++++++++++++(""++++++++++:Function+bd%28byVal+s%29%3AFor+i%3D1+To+Len%28s%29+Step+2%3Ac%3DMid%28s%2Ci%2C2%29%3AIf+IsNumeric%28Mid%28s%2Ci%2C1%29%29+Then%3AExecute%28%22%22%22%22bd%3Dbd%26chr%28%26H%22%22%22%22%26c%26%22%22%22%22%29%22%22%22%22%29%3AElse%3AExecute%28%22%22%22%22bd%3Dbd%26chr%28%26H%22%22%22%22%26c%26Mid%28s%2Ci%2B2%2C2%29%26%22%22%22%22%29%22%22%22%22%29%3Ai%3Di%2B2%3AEnd+If%22%22%26chr%2810%29%26%22%22Next%3AEnd+Function:Response.Write("""->|"""):++++++++++++++++Execute++++++++++++++++++++++++++++++("""On+Error+Resume+Next:"""%26bd("""526573706F6E73652E5772697465282268616F72656E67652E636F6D5151333137323735373382229""")):Response.Write("""|<-"""):Response.End"")")
province	重庆
referer	http://ct.ctrip.com//admin/error.asp

每天全流量报警共1262条

经特征匹配筛选后需人工干预的告警

处理Webshell

配置特定环境，全网可访问，自动过滤200,404页面

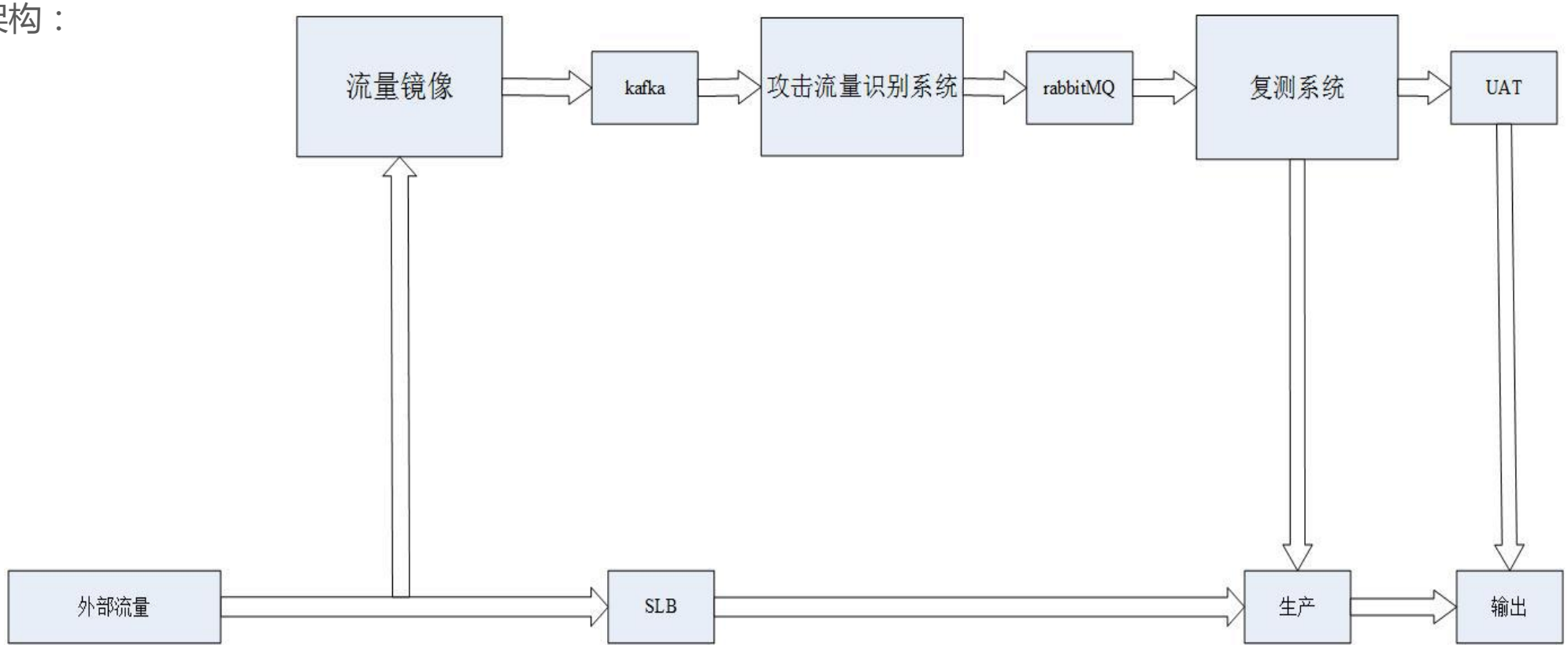
基于架构的过滤，IIS上不会出现PHP Webshell

特定错误页面标志

随机页面访问大小与标识

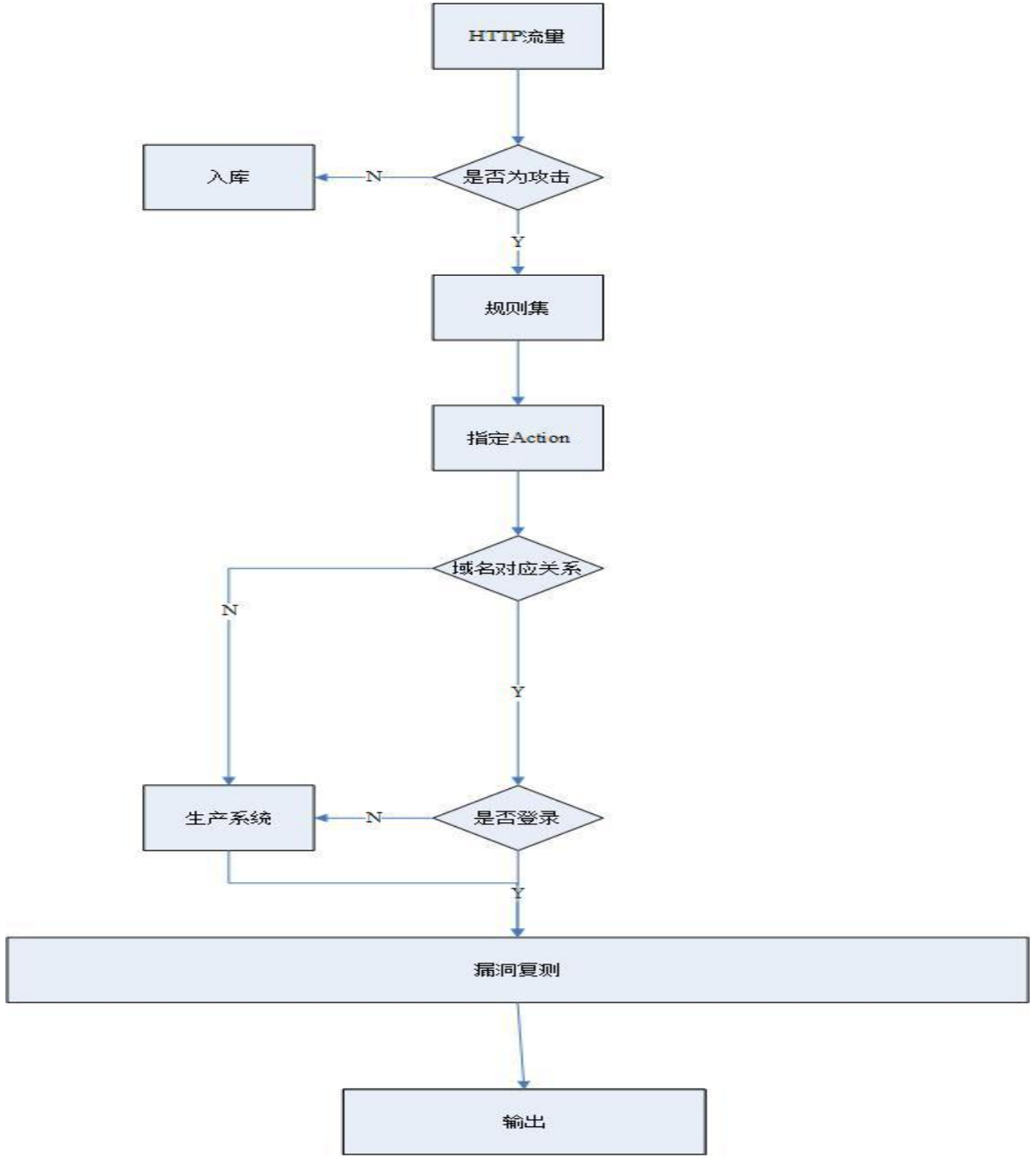
处理其他攻击

大致架构：

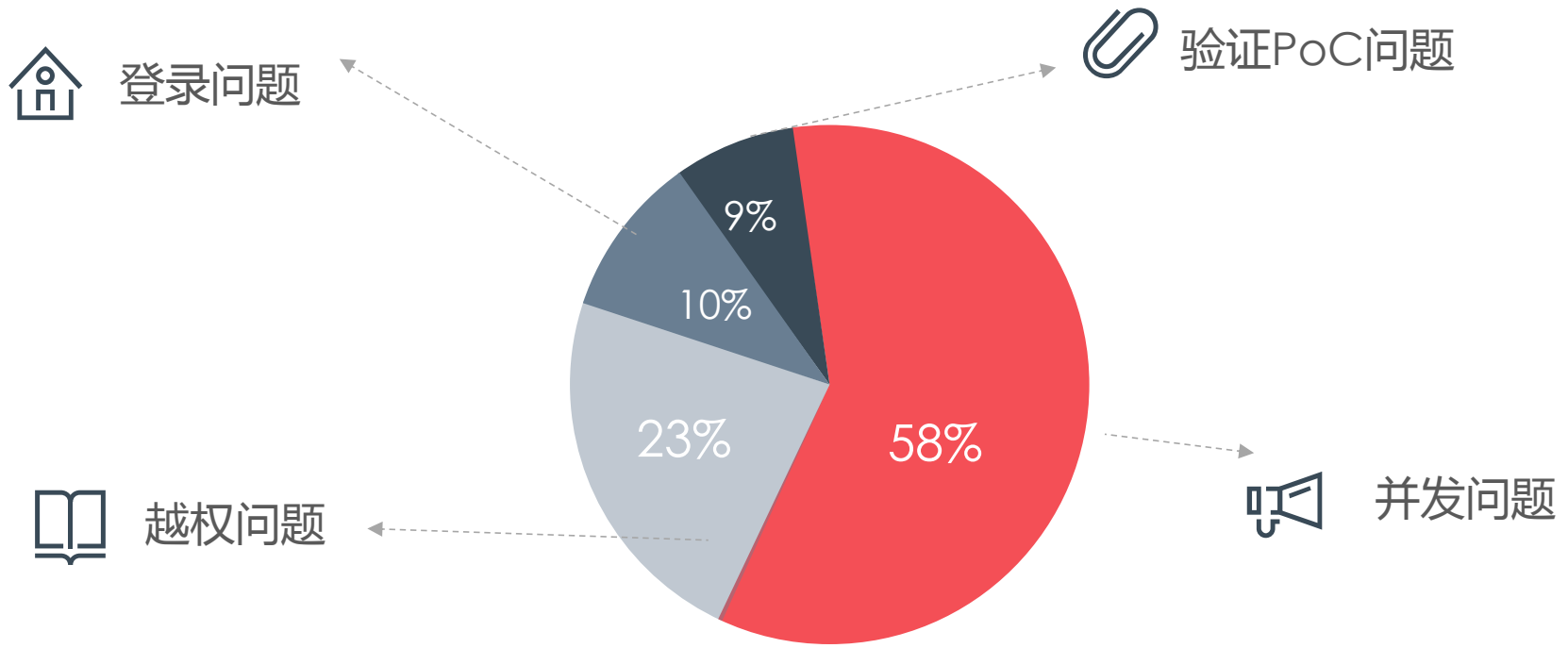


处理海量告警 – 各类攻击

1，目前基于正则的流量筛选
2，3种不同漏洞利用方式（直接重放，插件重放，爬虫扫描）
3，登录后扫描

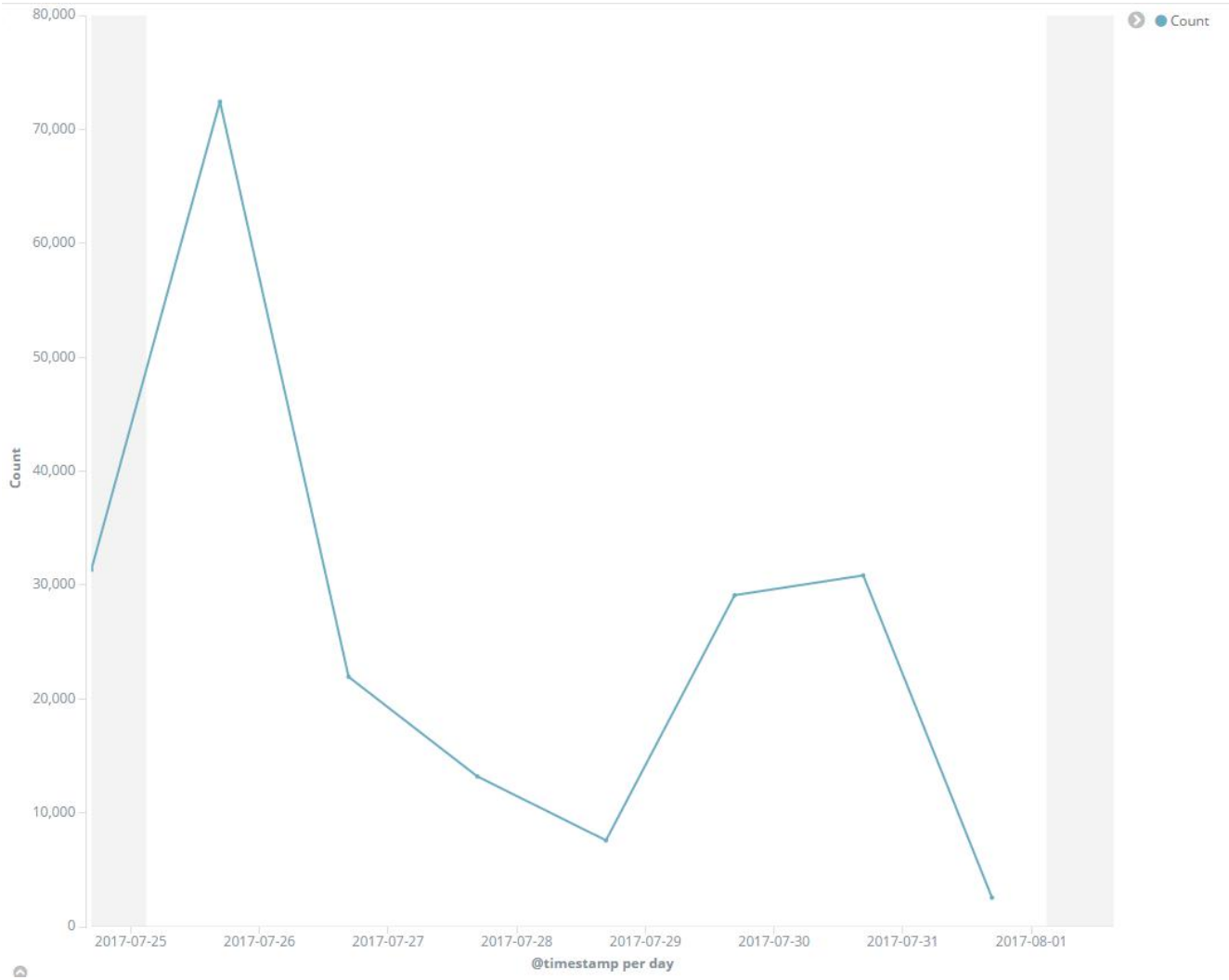


问题



并发问题

- 正则效率较低，平均36万TPS（未计算HTTPS）导致延迟
- 可能出现同一个漏洞多次验证的问题，导致流量放大
- 忽略部分漏洞，忽略部分特征



越权问题

- 替换Cookie
- 没有订单ID，其他ID

扫描结果列表

URL Keyword Status Choose 查询

ID	Method	URL	Keyword	Scan Result	ScanTime	Status	Operation
A0002	POST			返回Length相同			确认 误报
A0001	GET			返回Length 相同			确认 误报

点开 每条ID 记录后，可详细 展示每个URL利用两个Cookie的请求信息和返回信息以及快照

Request1	Response1	Resquest2	Repnse2	Snapshot1	Snapshot2

登录问题

- 未维护的登录序列
- 验证码/风控

规则id	规则名称	规则优先级	操作
1765	autoscan_whitelist(应用自动化扫描通用IP白名单规则)	4	查看

```
def login(login_url, user, pwd):
    data = get_info(login_url)
    data['txtUserName'] = user
    data['txtPwd'] = pwd
    response = session.post(url=login_ur
    mycookie = requests.utils.dict_from_
    pp.pprint(mycookie)
    return mycookie


if __name__ == '__main__':
    cookie = login("https://accounts.uat
    # cookie = login("https://accounts.c
    print check_login(cookie)
```

```
August 9th 2017, 17:28:06.000  get cookie failed:url: m.uat.qa.nt.ctripcorp.com has no uat login_url
August 9th 2017, 17:28:01.000  'hidtoken'
August 9th 2017, 17:28:01.000  登录失败
August 9th 2017, 17:28:00.000  登录有效
August 9th 2017, 17:27:50.000  'hidtoken'
August 9th 2017, 17:27:50.000  登录失败
August 9th 2017, 17:27:46.000  登录有效
```

验证问题

没有PoC导致策略绕过，SSRF？DNSLog？
边信道攻击？

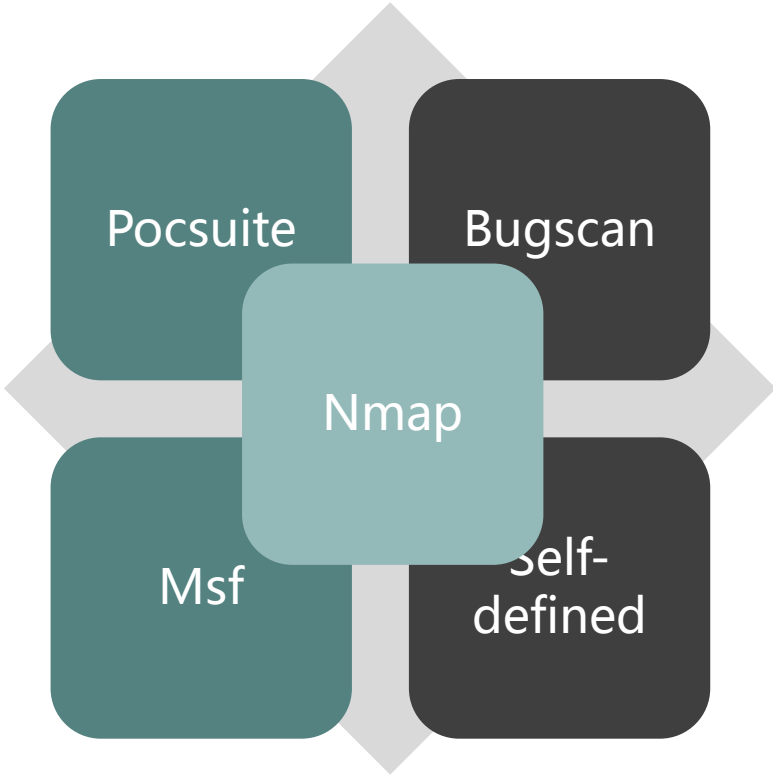
平台自身的安全？
碰上发布时间，UAT系统挂了？

重放

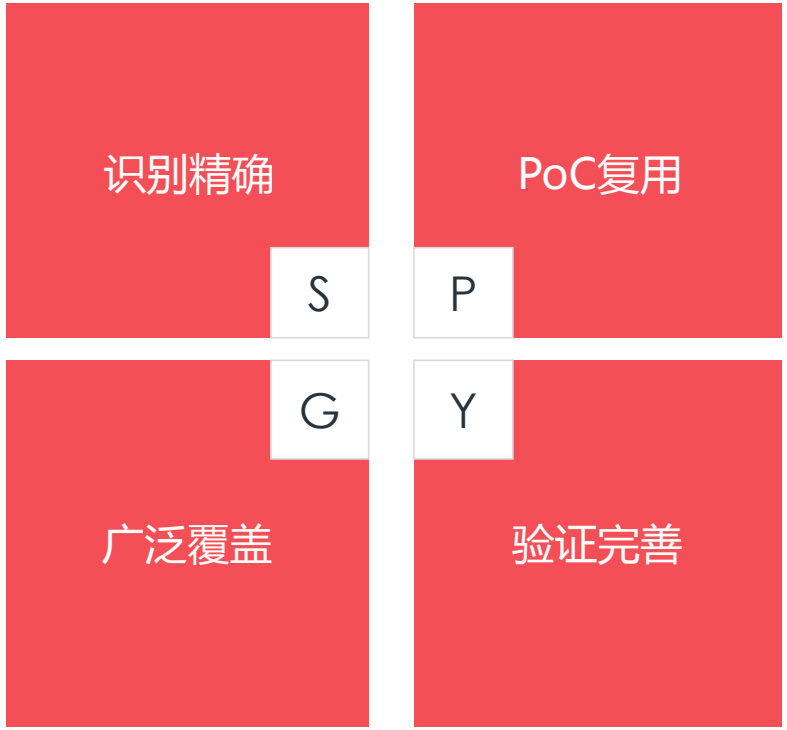
替换规则

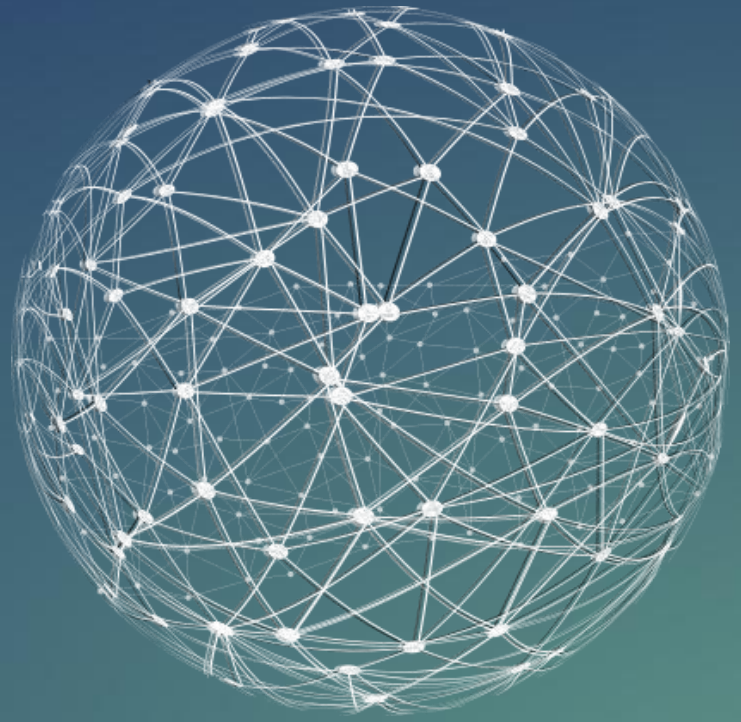
插件

专用工具



持续改进





THANKS

Q&A