



边界网络安全风险分析 攻击手段识别

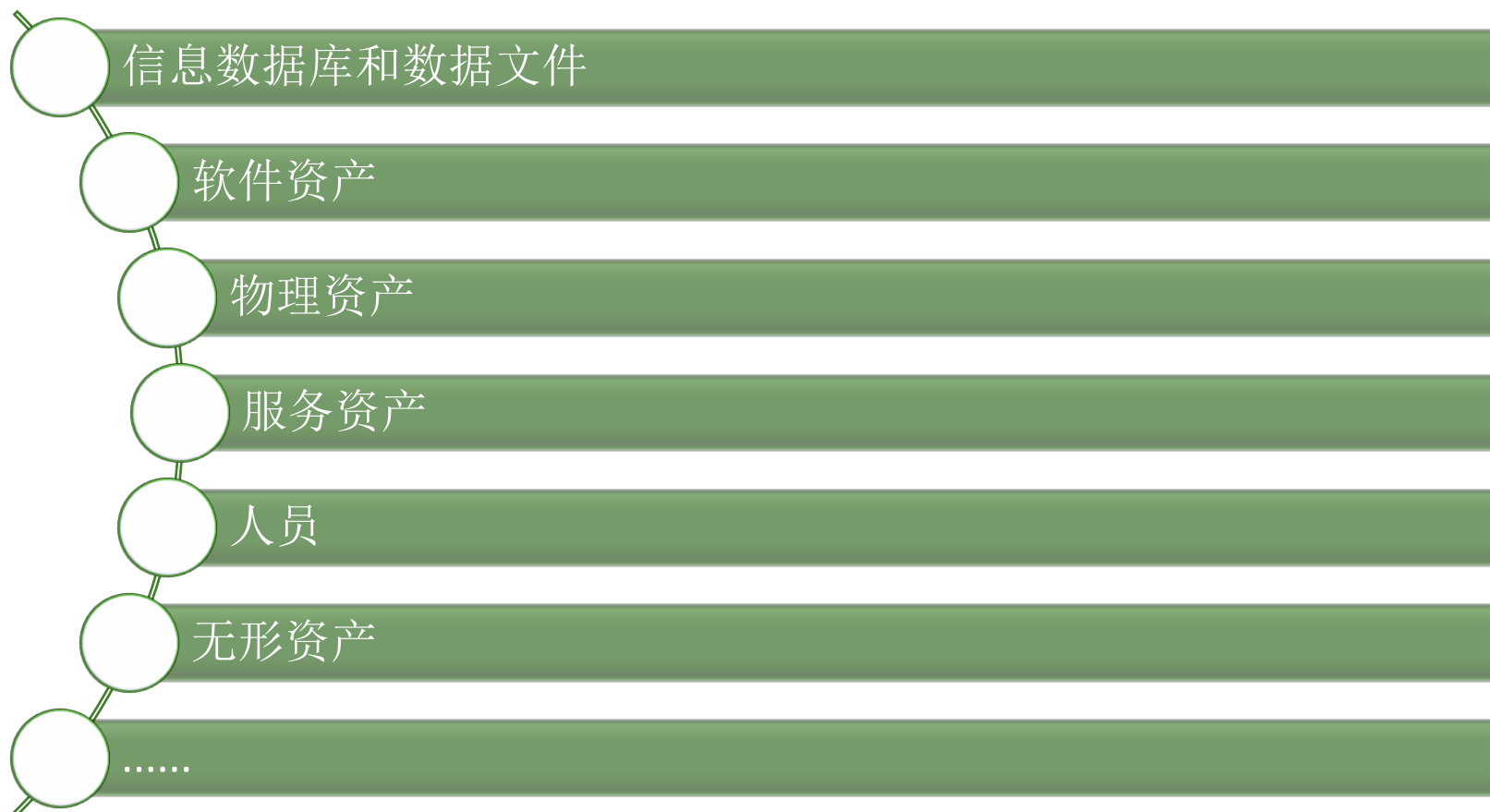
崔勤@长亭科技

资产管理

风险分析

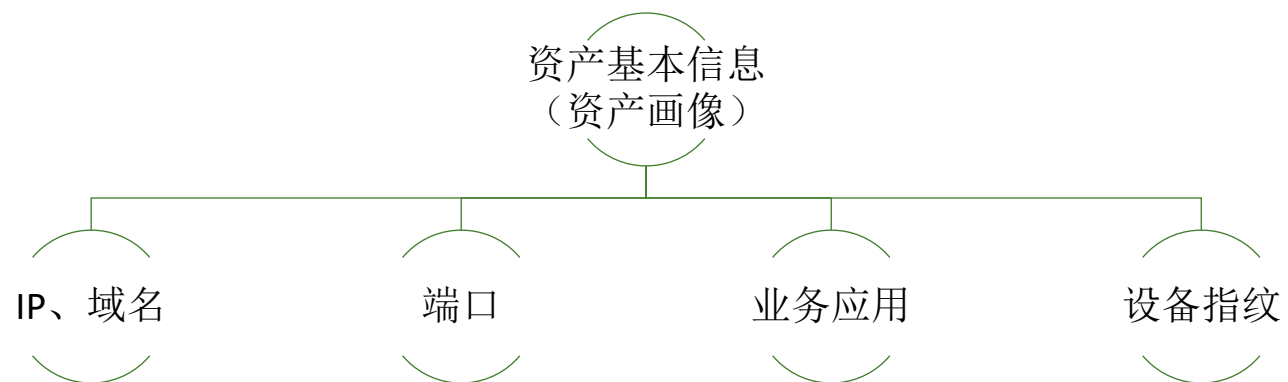
数据监控

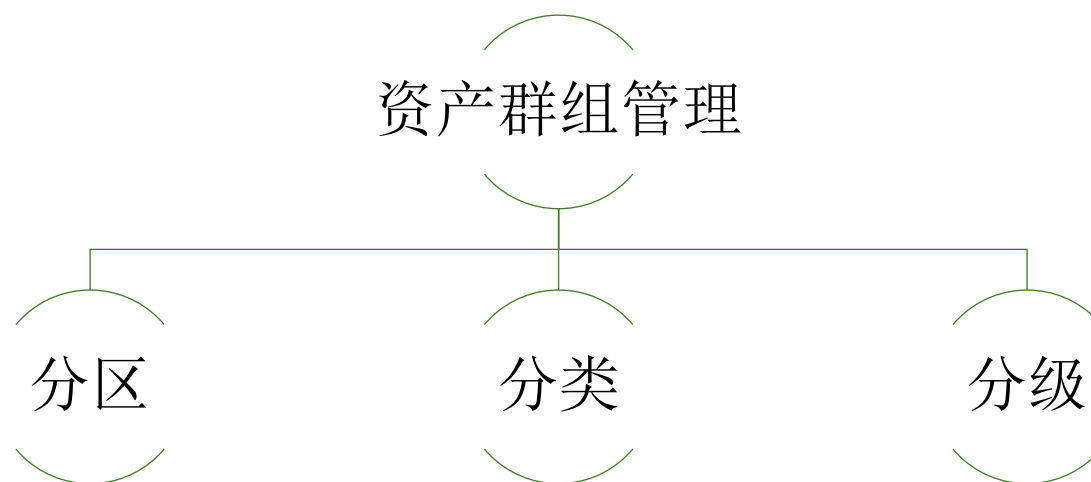
资产



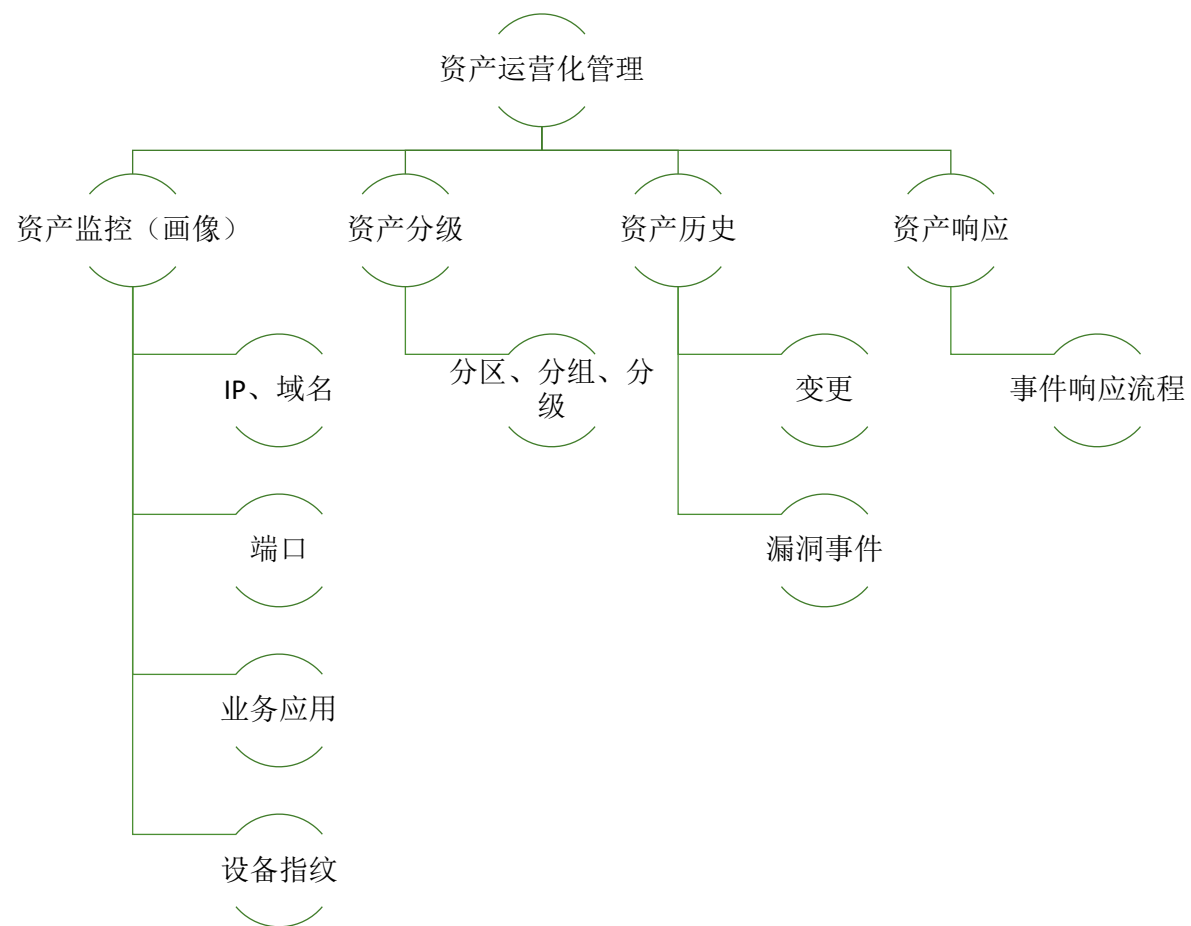
全量的安全风险分析，前提是做到完全的自知。

资产管理（Level 1）





资产管理（Level 3）



企业



- ☐ 数据库
- ☐ 代码
- ☐ 敏感文件

员工



- ☐ 邮件
- ☐ OA、CRM
- ☐ 员工权限

用户



- ☐ 资金
- ☐ 账户
- ☐ 个人信息

核心资产受到威胁的后果

雅虎5亿数据泄露后续：Verizon或放弃48亿美元收购计划

雅虎命运多舛，最终能否嫁入豪门又成谜团。

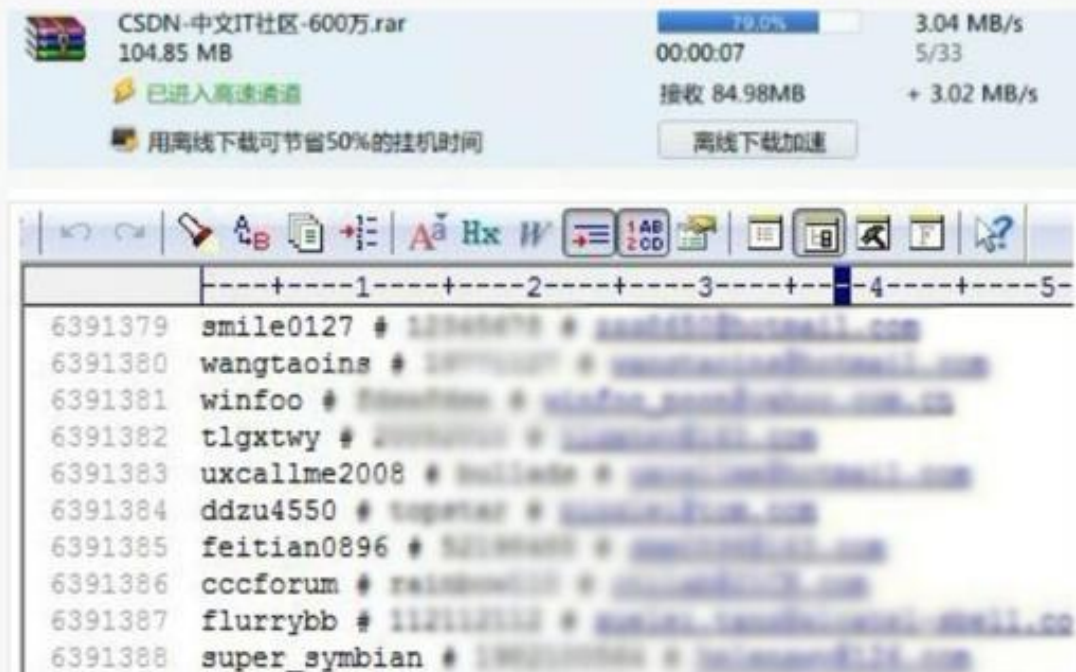
美国电信运营商 Verizon 在今年7月启动对雅虎的收购，预计花费48亿美元，明年完成收购。但雅虎自曝2014年遭黑客窃取 5 亿用户数据后，计划搁浅。Verizon 昨天公开向媒体表示，黑客事件严重影响到雅虎的估值，他们正考虑放弃对雅虎的收购。

「我认为我们已经有了充分理由相信，这次事件的影响是巨大的，」Verizon 法律顾问 Craig Silliman 在小型的圆桌会议上向多家媒体表示，这样的事情已经严重影响到雅虎的财务价值，使得收购雅虎显得不那么有吸引力。

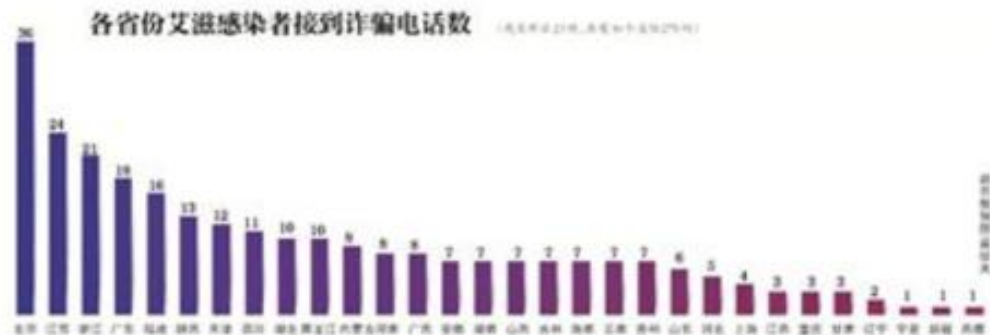
之前曾有传闻 Verizon 希望降价 10 亿美元收购雅虎，但没有得到双方的证实。昨天 Verizon 首次就雅虎数据泄露事件表态，并且当即否认欲降价 10 亿美元收购雅虎。就 Verizon 目前的态度看，其认为雅虎的品牌价值贬值严重，对网民的吸引力不再那么强，双方需要回到谈判桌，重新商量收购问题。

核心资产受到威胁的后果

有网友爆料称，昨天有黑客在网上公开了知名网站CSDN的用户数据库，这是一次严重的暴库泄密事件，涉及到的账户总量高达600万个，我们部分同事确实也在泄漏的库里发现了自己的帐号。又到了修改密码的时候了：



核心资产受到威胁的后果



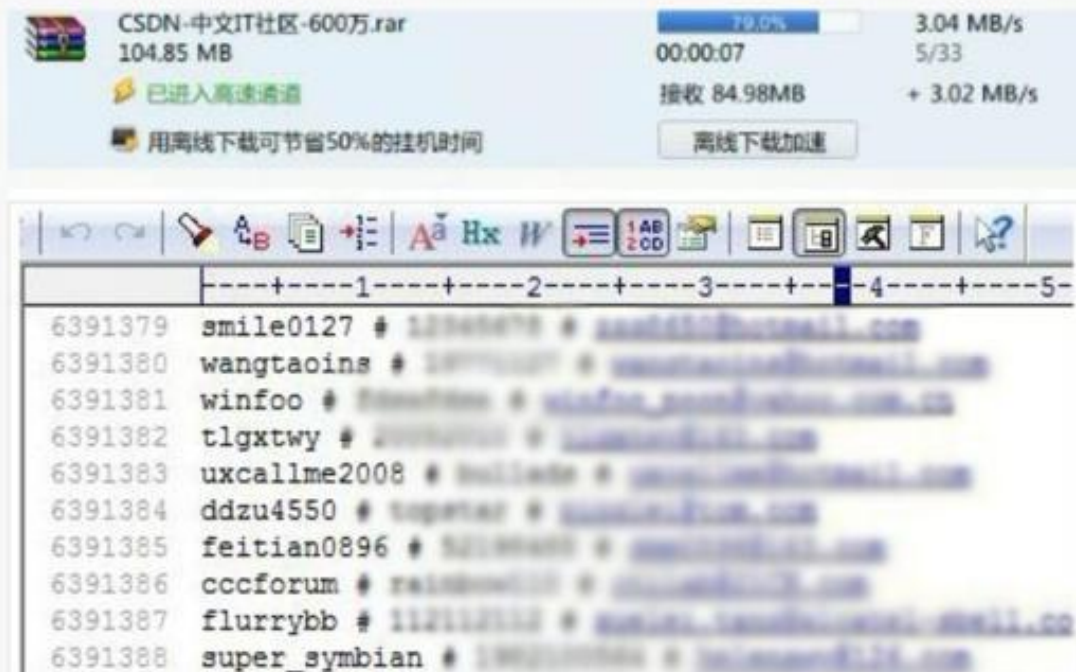
艾滋病感染者个人信息疑遭大面积泄露；中疾控称已报请公安部门立案侦查

新京报讯（记者李丹丹 戴轩）近日，全国30省份275位艾滋病感染者称接到了诈骗电话，艾滋病感染者的个人信息疑似被大面积泄露。昨日，中国疾病预防控制中心相关负责人表示，已经报案，将积极配合公安部门尽快破案。

诈骗者掌握病人姓名、确诊时间等信息

核心资产受到威胁的后果

有网友爆料称，昨天有黑客在网上公开了知名网站CSDN的用户数据库，这是一次严重的暴库泄密事件，涉及到的账户总量高达600万个，我们部分同事确实也在泄漏的库里发现了自己的帐号。又到了修改密码的时候了：



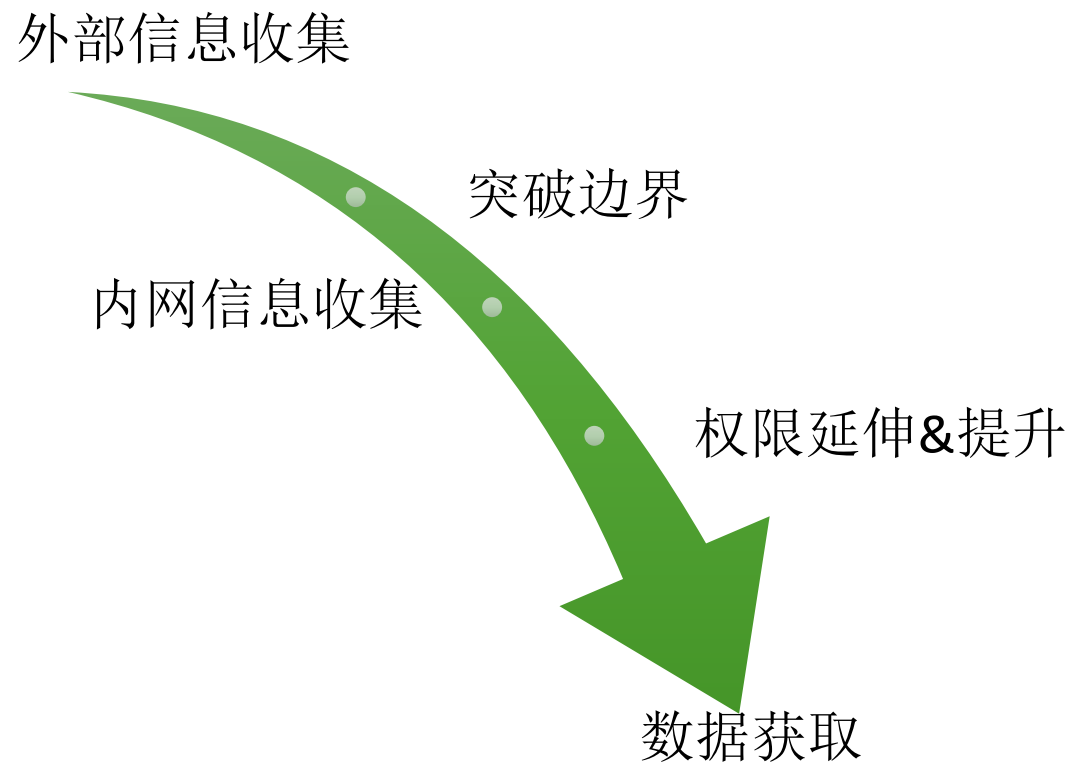
核心资产受到威胁的后果

孟加拉央行被黑客盗转1.01亿美元

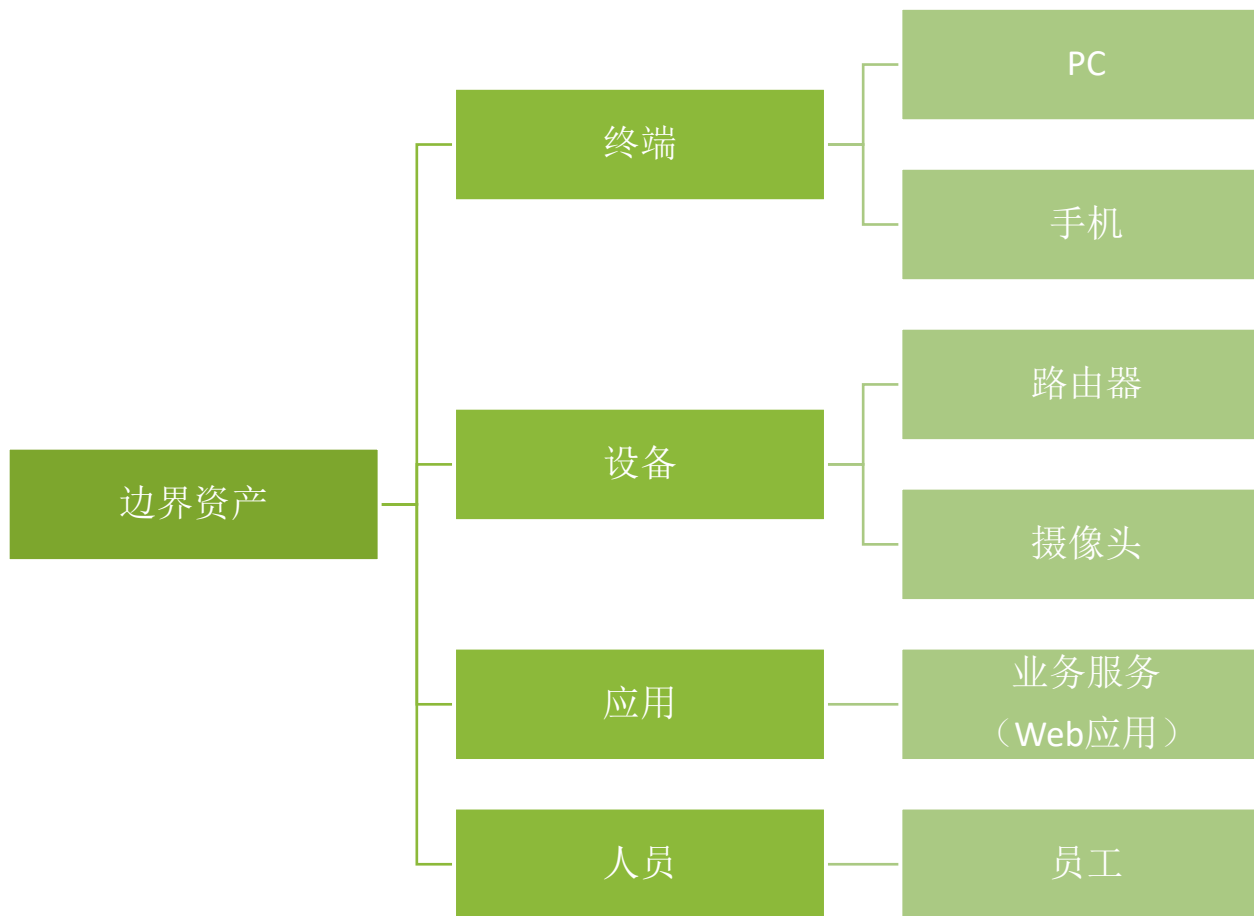
据悉，黑客入侵该国央行安全系统后，伪装成孟加拉官员，要求纽约联储转账



攻击过程



“边界”突破口举例



不知攻 焉知防

简单

员工

运维漏洞

应用漏洞

设备漏洞

钓鱼

复杂

员工信息

- 搜索引擎



[全部](#) [视频](#) [新闻](#) [图片](#) [地图](#) [更多 ▾](#) [搜索工具](#)

找到约 328,000 条结果 (用时 0.46 秒)

[PDF] Baidu Search - wsdm-conference.org
www.wsdm-conference.org/2015/wp-content/.../02/WSDM-Talk-Baidu-Search.pdf ▾
<http://www.baidu.com>. 2012年2月月. Baidu Search: ... zhukaihua@[baidu.com](mailto:zhukaihua@baidu.com). Architect of Baidu Search
..... Visiting opportunity. • [Mailto: wuxiaohui@baidu.com](mailto:wuxiaohui@baidu.com).

mailto://www.baidu.com/是什么意思_百度知道
zhidao.baidu.com/question/100280313.html
2009年10月5日 - <mailto://www.baidu.com/>是什么意思. 2009-06-06 11:06 匿名 | 分类: 网站使用. 我有更好的答案. 分享到: . 按默认排序 | 按时间排序 ...

| | |
|------------------------------|------------|
| html插入邮件链接_百度知道 | 2014年1月15日 |
| FLASH CS5 中使用mailto发送邮件_百度知道 | 2011年5月4日 |
| Dreamweaver 邮件连接怎么写_百度知道 | 2010年5月27日 |
| 我想知道URL和URI的区别! 请大 ... | 2007年11月2日 |


zhidao.baidu.com站内的其它相关信息

发邮件到news@baidu.com的邮箱,结果未送达_新闻搜索吧_百度贴吧
tieba.baidu.com/p/875820465 ▾
2010年8月30日 - 如题! 退信内容如下: 向这些收件人或通讯组列表传递邮件失败: zhangning@baidu.com
[com<mailto:zhangning@baidu.com>](mailto:zhangning@baidu.com) 现在, 收件人的邮箱已满, ...


'[Beowulf] HPC system administrator position at Baidu USA in ...
marc.info/?l=beowulf&m=143027973603363&w=2 ▾ 翻译此页
2015年4月29日 - ... or contact me at patricklegresley@baidu.com \ <<mailto:patricklegresley@baidu.com>> for more information. Cheers, Patrick [Attachment #5 ...

员工信息


- Github

 **surlymo/SedaFramework – config.properties** INI
Showing the top 12 matches. Last indexed on 25 Mar.

```
2 # mail config #
3 #####
4 mail.smtp.host=mail-fengchao.baidu.com
5 mail.smtp.auth=false
6 mail.from=deimos-satellite@baidu.com
7 mail.to=chenchao03@baidu.com
8 mail.cc=chenchao03@baidu.com
```

 **qxiong133/tools – process.conf**
Showing the top seven matches. Last indexed on 27 Mar.

```
1 [map_wap_wapmap]
2 mail_list=huangyixin@baidu.com,zhuangqunxiong@baidu.com,lili15@baidu.com,wangrui06@baidu.com
```

 **qxiong133/tools – process.conf.online**
Showing the top seven matches. Last indexed on 27 Mar.

```
1 [map_wap_wapmap]
2 mail_list=huangyixin@baidu.com,zhuangqunxiong@baidu.com,lili15@baidu.com,wangrui06@baidu.com
```

员工信息

- 社交平台

“不仅仅有个人信息，还可能泄漏更多有意思的东西”

见当天培训内容

- 社工库



员工信息

- 网站业务

重置密码

重置密码

帐号:



很遗憾，您未设置任何密码保护措施，无法通过系统重置密码。
请联系贵公司邮箱的维护人员重置密码。

返回登录页

员工信息

- 社工字典

%username% = 用户名

%domain% = 公司域名

%username%%domain%

%username%@%domain%

%username%1

%username%12

%username%123

%username%1234

%username%12345

%username%123456

%username%@123

%username%8

%username%88

%username%888

%username%999

%username%666

%username%2013

%username%2014

%username%2013

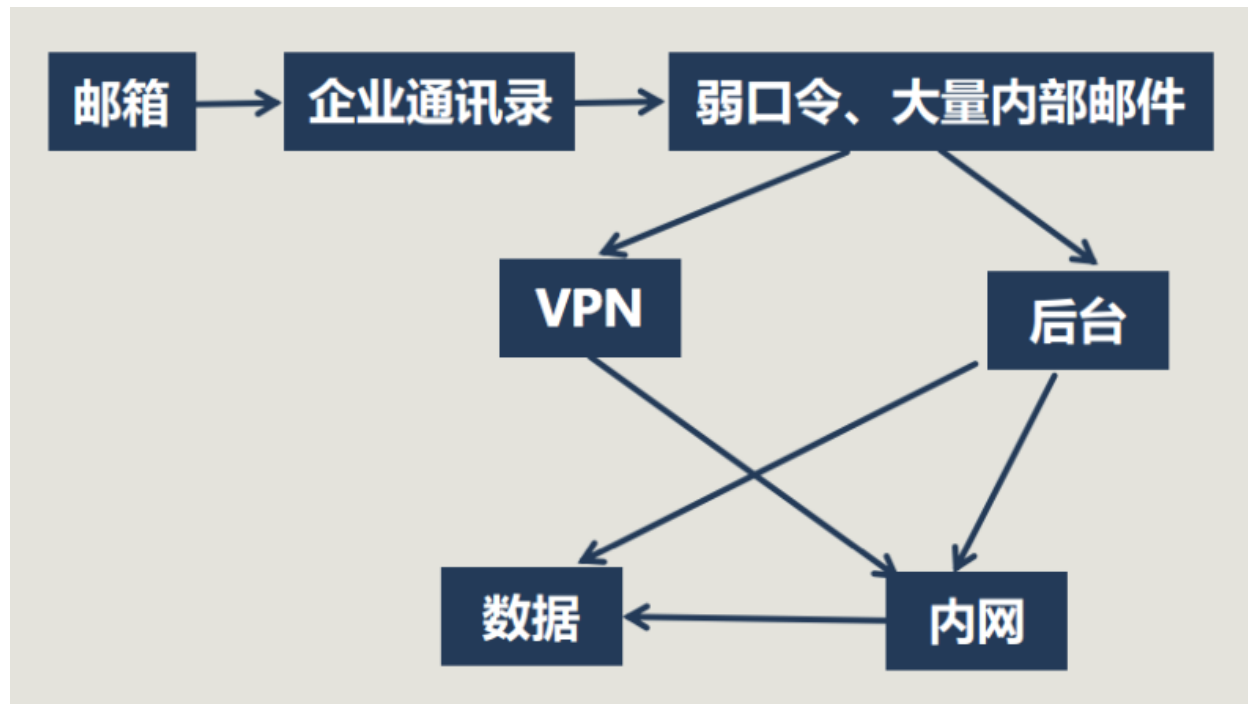
%username%@2013

%username%@2014

%username%@2015

%username%!@#

攻击思路



社工&钓鱼案例

现场分享

社工&钓鱼案例

现场分享

现场分享

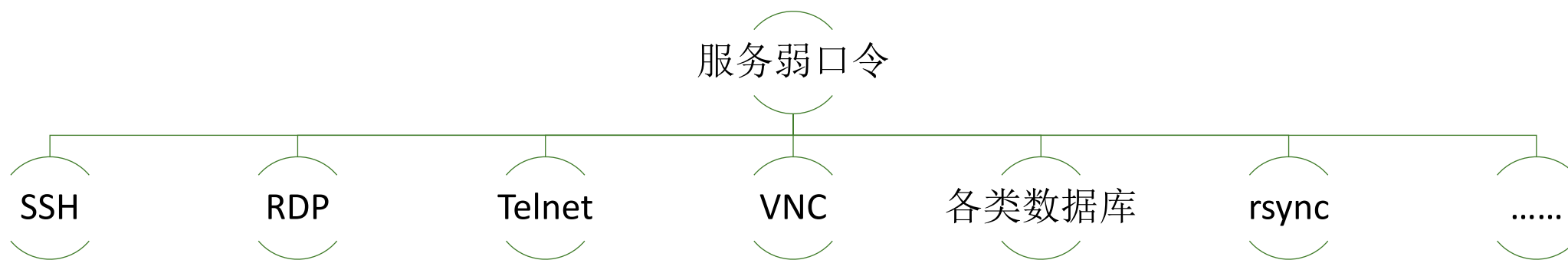
社工&钓鱼案例

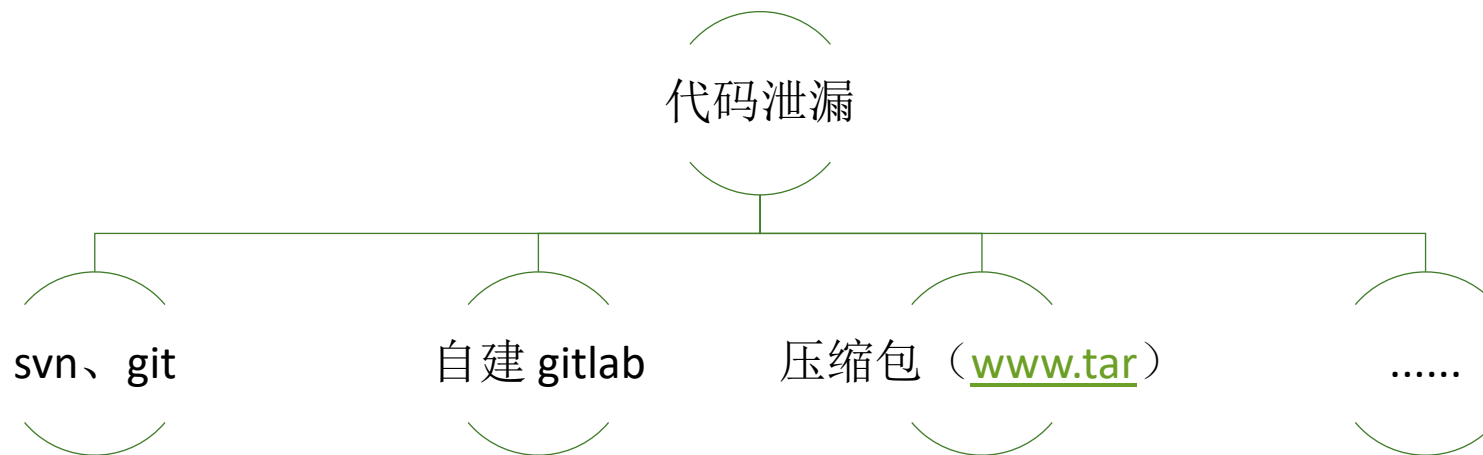
现场分享

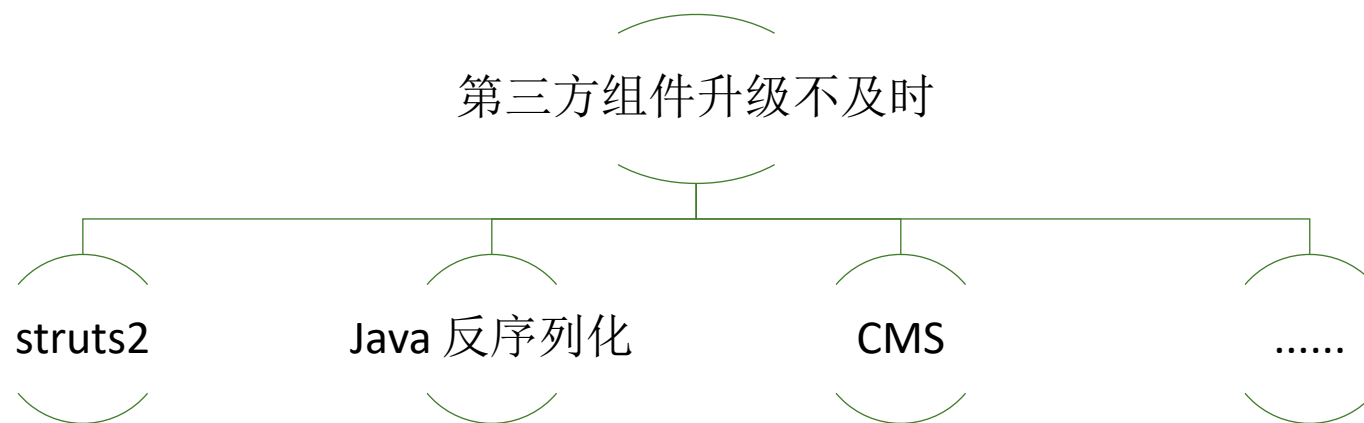
社工&钓鱼案例

现场分享

现场分享











运维漏洞举例

网站备份泄漏

http://192.168.1.174:8088/web.rar

http://192.168.1.174:8088/www.rar

| | | | |
|---|----------------|-------------|-----------|
|  www.rar | 2017/4/7 11:10 | WinRAR 压缩文件 | 48,396 KB |
|  web.rar | 2017/4/7 11:06 | WinRAR 压缩文件 | 3 KB |
|  www | 2017/4/7 11:10 | 文件夹 | |
|  web | 2017/4/7 11:06 | 文件夹 | |

```
name="zh-cn_databaseConnectionString" connectionString="packet size=4096;user id=able; PWD='able_shjdyxy2012'; data source=202.120.1.1"
name="databaseConnectionString_RM" connectionString="packet size=4096;user id=able; PWD='able_shjdyxy2012'; data source=202.120.1.1"
name="databaseConnectionString_QE" connectionString="packet size=4096;user id=able; PWD='able_shjdyxy2012'; data source=202.120.1.1"
ctionStrings>
```

运维漏洞举例

- 业务无关代码未及时删除
 - JS 泄漏敏感信息

```
<title> 电子签约平台 </title>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<script type="text/javascript" src="http://172.20.1.146/_component/jquery/jquery-1.11.0.min.js"></script>
<script type="text/javascript" src="http://172.20.1.146/_component/jquery/form/jquery.form.js"></script>
<script type="text/javascript" src="http://172.20.1.146/_component/jquery/boxy/jscripts/jquery.boxy.js"></script>
<script type="text/javascript" src="http://172.20.1.146/_component/jquery/jquery-validate/jquery.validate.js"></script>
<script type="text/javascript" src="http://172.20.1.146/_component/jquery/jquery-validate/lib/jquery.metadata.js"></script>
<script type="text/javascript" src="http://172.20.1.146/_component/jquery/jquery-validate/localization/messages_cn.js"></script>
<script type="text/javascript" src="http://172.20.1.146/_component/ancun/core.js"></script>
<script type="text/javascript" src="http://172.20.1.146/_component/ancun/core.validate.js"></script>
<link href="http://172.20.1.146/didi_online/css/global.css" rel="stylesheet" type="text/css" />
```

- 测试账号未删除

```
<?php
//=====*/
/* 测试帐号 */
/* 2838975848 123456789 */
/* 1953024456 robot123 */
/* 2838572550 robot123 */
define("USERNAME",""); // qq帐号
define("PASSWORD",""); // qq密码
define("REPLY","parse.ini"); // 相关回复解析
define("temp_dir","tmp/"); // cookie, 日志等信息的临时存放目录
```

- 备份文件

```
→ ~ curl http://test.php.com:9900/common.php
page is working

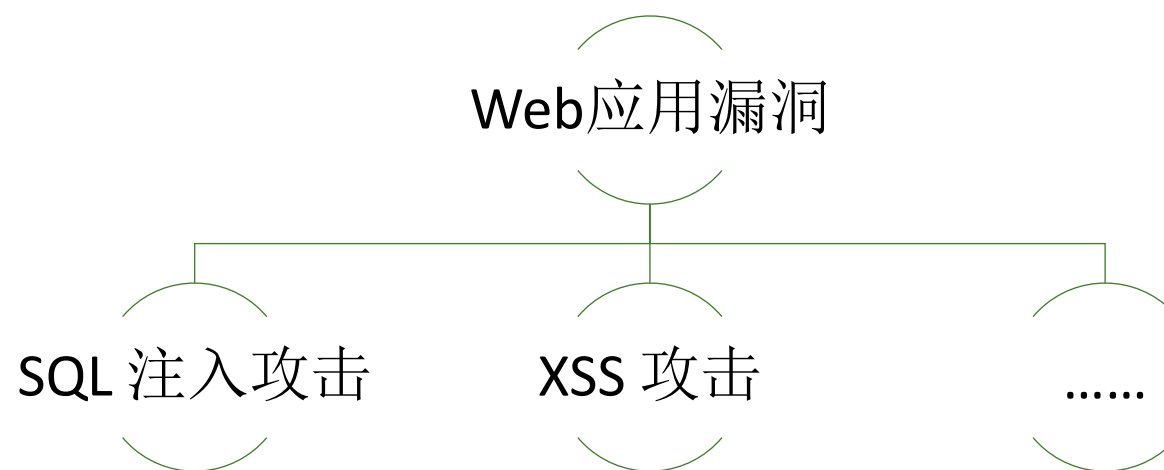
→ ~ curl http://test.php.com:9900/common.php.bak
<?php
echo 'page is working';
$myuser = 'admin';
$myPwd = 'YP9KEMgD!8';
?>
```

运维漏洞举例

- 配置文件未及时删除

| | |
|--------------------------|----------------------------|
| System | Linux php2-g5.priv.free.fr |
| _SERVER["REMOTE_ADDR"] | 222.128.2.10X |
| _SERVER["DOCUMENT_ROOT"] | /mnt/102/sda/3/9/leserged |

一切有交互的地方都可能存在漏洞



应用漏洞

| OWASP Top 10 – 2013 (Previous) | OWASP Top 10 – 2017 (New) |
|---|---|
| A1 – Injection | A1 – Injection |
| A2 – Broken Authentication and Session Management | A2 – Broken Authentication and Session Management |
| A3 – Cross-Site Scripting (XSS) | A3 – Cross-Site Scripting (XSS) |
| A4 – Insecure Direct Object References - Merged with A7 | A4 – Broken Access Control (Original category in 2003/2004) |
| A5 – Security Misconfiguration | A5 – Security Misconfiguration |
| A6 – Sensitive Data Exposure | A6 – Sensitive Data Exposure |
| A7 – Missing Function Level Access Control - Merged with A4 | A7 – Insufficient Attack Protection (NEW) |
| A8 – Cross-Site Request Forgery (CSRF) | A8 – Cross-Site Request Forgery (CSRF) |
| A9 – Using Components with Known Vulnerabilities | A9 – Using Components with Known Vulnerabilities |
| A10 – Unvalidated Redirects and Forwards - Dropped | A10 – Underprotected APIs (NEW) |

应用漏洞

WooYun.org  加关注 16.3万

首页 | 厂商列表 | 白帽子 | 乌云榜 | 团队 | 漏洞列表 | 提交漏洞 | 社区 | 公告

当前位置: 首页 >> 检索结果

搜索关键字: **sql注入 (共 17564 条记录)**

[兴业银行某站存在SQL注入](#)
提交日期: 2016-07-12 08:29 作者: by:安全者

[天天果园某分站存在SQL注入](#)
提交日期: 2016-07-08 08:46 作者: xiao晓威

[温州大学某站sql注入 \(113库\)](#)
提交日期: 2016-07-06 16:53 作者: 路人甲

SQL 注入 危害

窃取数据库敏感信息

对数据进行恶意的增删改

造成拒绝服务攻击

获取服务器权限

数字型

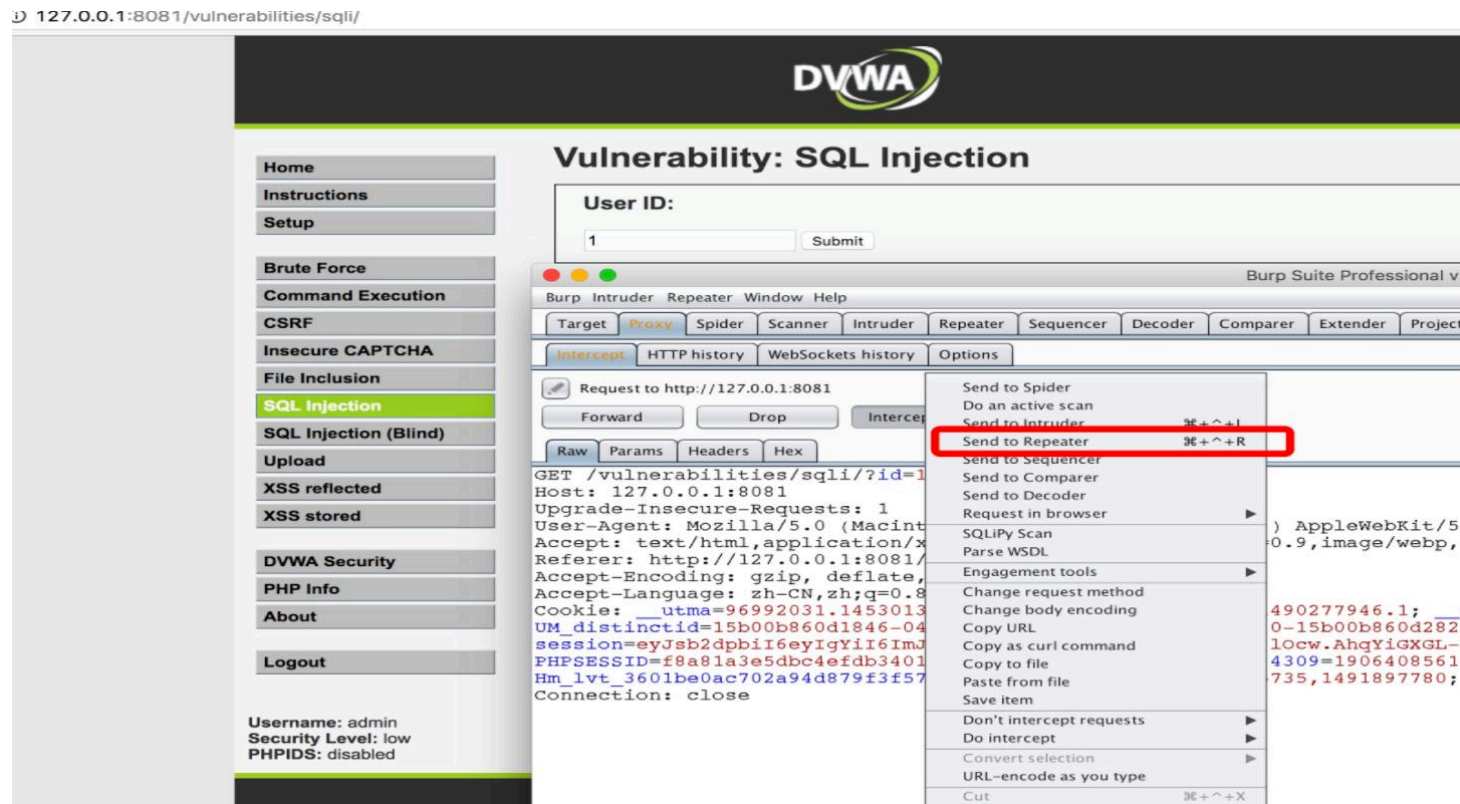
“select * from product where id =”. \$_GET['id']

字符型

“select * from person_info where username=”. \$_GET['name'].“”

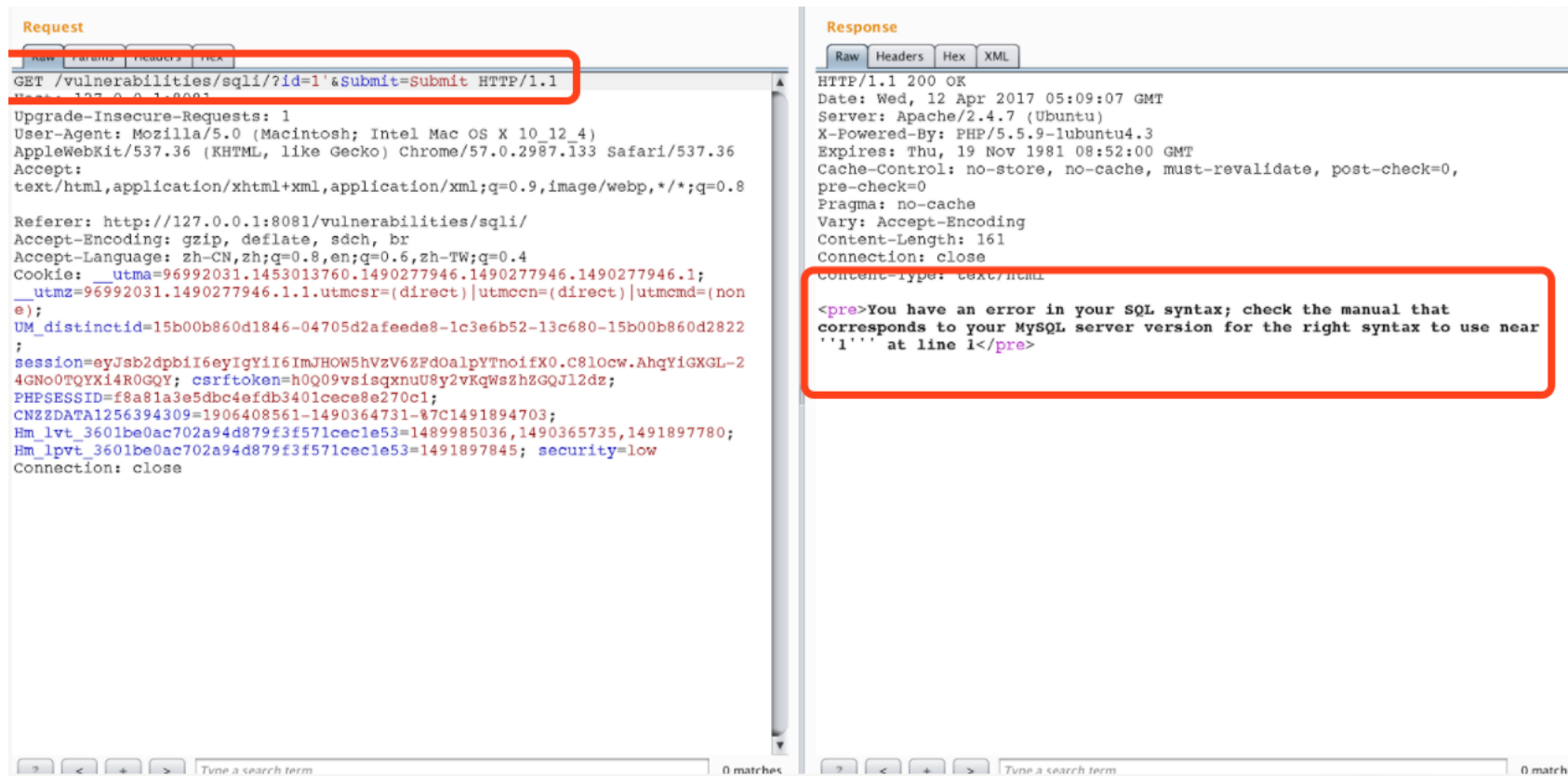
应用漏洞举例

- 测试环境



应用漏洞举例

- 测试环境



Request

Raw Params Headers Text

```
GET /vulnerabilities/sqli/?id=1'&Submit=Submit HTTP/1.1
Host: 127.0.0.1:8081
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://127.0.0.1:8081/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: zh-CN,zh;q=0.8,en;q=0.6,zh-TW;q=0.4
Cookie: __utma=96992031.1453013760.1490277946.1490277946.1490277946.1; __utmsr=(direct)|utmccn=(direct)|utmcmd=(none); UM_distinctid=15b00b860d1846-04705d2afeede8-1c3e6b52-13c680-15b00b860d2822; session=eyJsb2dpbiI6eyIyI6ImJHOW5hVzV6ZFdoalpyTnoifX0.C8lOcw.AhqYiGXGL-24GN0TQYXi4R0GQY; csrftoken=h0Q09vsisqxnuU8y2vKqWszh2GQJl2dz; PHPSESSID=f8a81a3e5dbc4efdb3401cece8e270c1; CNZZDATA1256394309=1906408561-1490364731-87C1491894703; Hm_lvt_3601be0ac702a94d879f3f571cecle53=1489985036,1490365735,1491897780; Hm_lpvt_3601be0ac702a94d879f3f571cecle53=1491897845; security=low
Connection: close
```

Response

Raw Headers Hex XML

```
HTTP/1.1 200 OK
Date: Wed, 12 Apr 2017 05:09:07 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-lubuntu4.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 161
Connection: close
Content-Type: text/html

<pre>You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near
''1'' at line 1</pre>
```

应用漏洞举例

• 测试环境

The screenshot displays a web browser window with two tabs: 'Request' and 'Response'. The 'Request' tab shows the raw HTTP request, which includes a payload for a SQL injection attack. The 'Response' tab shows the raw HTTP response, which includes the injected SQL query and its results.

Request:

```
GET /vulnerabilities/sqli/?id=1'+union+select+user(),2--+&Submit=Submit HTTP/1.1
Host: 127.0.0.1:8081
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://127.0.0.1:8081/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: zh-CN,zh;q=0.8,en;q=0.6,zh-TW;q=0.4
Cookie: __utma=96992031.1453013760.1490277946.1490277946.1490277946.1; __utmz=96992031.1490277946.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); M_distinctid=15b00b860d1846-04705d2afeede8-1c3e6b52-13c680-15b00b860d2822
session=eyJsb2dpbiI6eyIyI6ImJHbW5hVzV6ZFdOalpYTnoifX0.C8l0cw.AhQYiGXGL-2GNo0TQYXi4R0GQY; csrftoken=h0Q09vsisqxnuU8y2vKqWszhZGQJl2dz; HFSESSID=f8a81a3e5dbc4efdb340lcece8e270cl; NZZDATA1256394309=1906408561-1490364731-87C1491894703; m_lvt_3601be0ac702a94d879f3f571cecle53=1489985036,1490365735,1491897780; m_lpv_3601be0ac702a94d879f3f571cecle53=1491897845; security=low
Connection: close
```

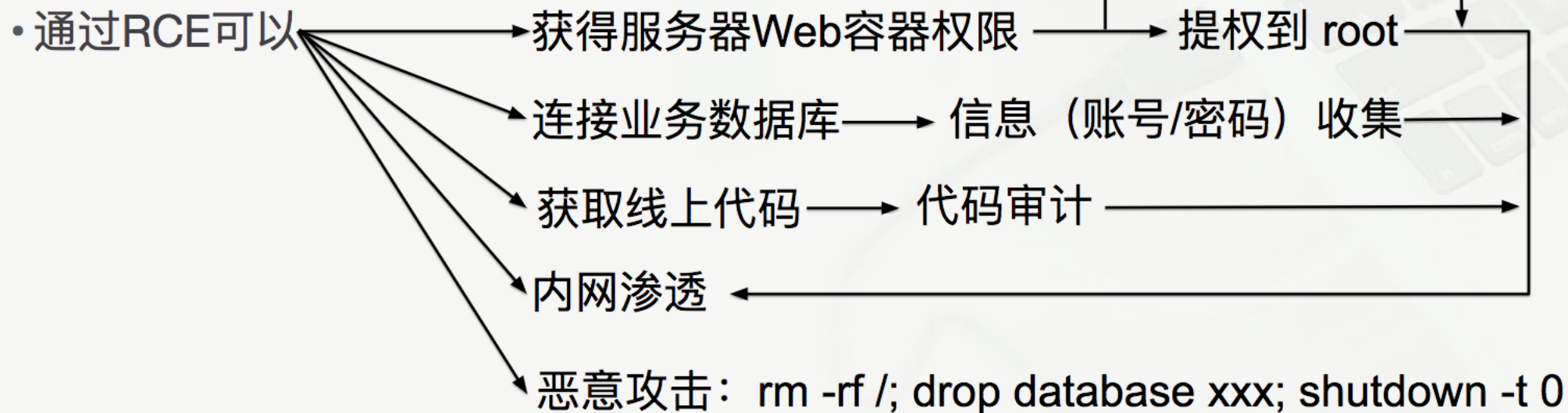
Response:

```
</div>
<div id="main_body">
<div class="body_padded">
  <h1>Vulnerability: SQL Injection</h1>
  <div class="vulnerable_code_area">
    <h3>User ID:</h3>
    <form action="#" method="GET">
      <input type="text" name="id">
      <input type="submit" name="Submit"
value="Submit">
    </form>
    <pre>ID: 1' union select user(),2-- <br>First name:
admin<br>Surname: admin</pre><pre>ID: 1' union select user(),2--
<br>First name: admin@localhost<br>Surname: 2</pre>
  </div>
  <h2>More info</h2>
  <ul>
    <li><a
href="http://hiderefer.com/?http://www.securiteam.com/securityreviews/5DP0N1P76E.html"
target="_blank">http://www.securiteam.com/securityreviews/5DP0N1P76E.html</a></li>
    <li><a
href="http://hiderefer.com/?http://en.wikipedia.org/wiki/SQL_injection"
target="_blank">http://en.wikipedia.org/wiki/SQL_injection</a></li>
    <li><a
href="http://hiderefer.com/?http://ferruh.mavituna.com/sql-injection-cheat
```

应用漏洞举例

- RCE 远程代码执行

- 危害程度：★★★★★



设备漏洞



海康威视
HIKVISION

海康威视
旗舰店

全国联保

200万网络高清套装
— H.264编码 / POE供电 / 红外30米 —



送

螺丝刀 网线钳 卷尺20米 VGA线

< >



设备漏洞

10月24日，由KEEN主办的GeekPwn 2015（极棒）安全极客嘉年华正式举行。在这场倍受人们关注的“黑客奥运会”上，众多智能软硬件被安全极客们攻破，并在现场做了技术展示。

当天上午，长亭科技的参赛选手一次性攻破7款智能摄像头，引发现场一片哗然。试想，原本用于实时监控，承担安全防护作用的智能摄像头遭破解，并被黑客远程控制，进而变成偷窥隐私的犯罪工具，这是一件多么可怕的事情。



设备漏洞

【IT168 资讯】日前，全球首个关注智能生活的安全极客大赛GeekPwn2016澳门站正式落下帷幕。其中，在备受关注的路由器和摄像头破解大赛中，国内新兴的网络安全公司长亭科技在杨坤的带领下表现技惊四座，团队选手一口气攻破了市面上销售10款主流品牌路由器和1款摄像头，当之无愧的问鼎本届大赛一等奖，并独揽42万元奖金。据悉，在极客圈，“42”代表了宇宙中一切终极答案。



▲ 长亭科技团队成员比赛现场

前提：攻击面

攻击表面 [编辑]

维基百科，自由的百科全书

攻击表面（英语：**attack surface**），也称**攻击面**、**攻击层面**，它是指**软件**环境中可以被未授权用户（**攻击者**）输入或提取数据而受到攻击的点位（**攻击矢量**）。^{[1][2]}

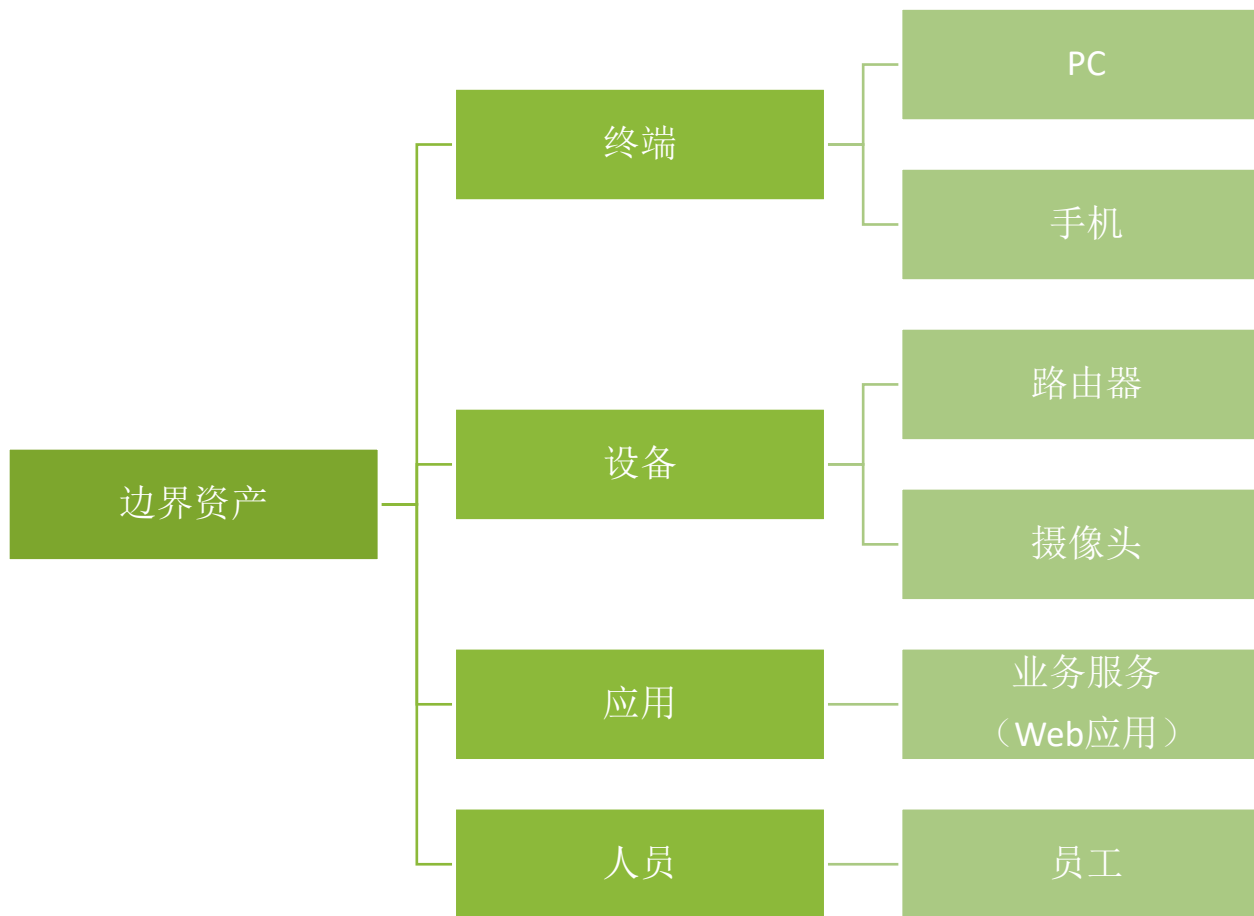
目录 [隐藏]

- 1 [攻击矢量例子](#)
- 2 [减少表面](#)
- 3 [参见](#)
- 4 [参考资料](#)

攻击矢量例子 [编辑]

攻击矢量的示例包括：用户输入字段、[协议](#)、[接口](#)和[服务](#)等。

“边界”突破口举例



风险分析

合理的资产管理

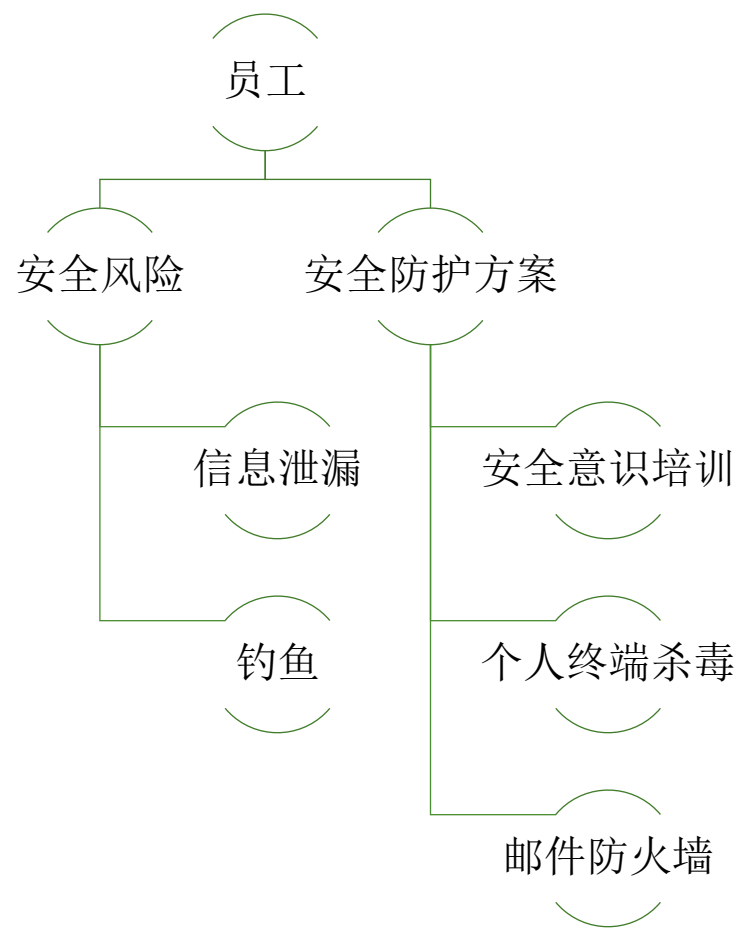
寻找脆弱点

梳理攻击面

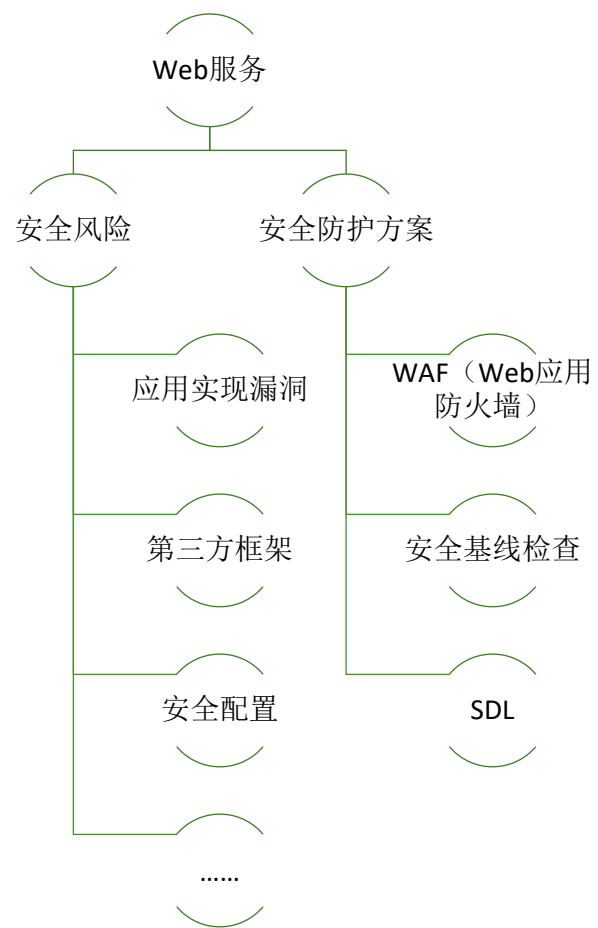
安全防护办法



风险分析举例



风险分析举例




WAF 的作用？

针对HTTP访问的Web防护（拦截攻击，放行正常流量）

- SQL注入、XSS跨站脚本、PHP远程代码执行、Java反序列化（攻击千变万化、花样繁多）
- Web攻击门槛低，下载一款扫描器即可开始攻击
- 绝大多数的入侵事件都从Web端（网站、API等）作为入口进入

风险分析案例

 SAFELINE

统计信息

站点管理

入侵检测

防护策略管理

入侵检测日志

扩展插件管理

检测参数配置

访问控制

系统设置

用户管理

个人中心

入侵检测 / 检测日志详情

有效期至 2026-12-02 © 北京长亭科技有限公司

功能搜索

qin.cui

检测错误? 一键报告给长亭

| | | | | | |
|------|----------------|----------|----------------------------------|------|--------------------------|
| ID | 68781 | Event ID | a9775e1bbdbc4d61897c5e9dca0fc436 | | |
| 节点 | detector-srv | 时间 | 2017-09-11 14:17:01 | 风险等级 | 高危 |
| 执行动作 | 拦截 | 攻击类型 | SQL注入 | 请求域名 | safeline-demo.chaitin.cn |
| 源IP | 180.173.35.248 | 地理位置 | 上海 | 模块 | SQL 注入检测模块 |
| 原因 | 发现 SQL 注入 攻击 | | | | |

Decode Path

urlpath : url_parse

Payload

category-1) AND (SELECT 4037 FROM(SELECT COUNT(*),CONCAT(CHAR(58,100,114,108,58),(SELECT (CASE WHEN (4037

Method + URLpath

GET /resume/?/home/explore/category-1)%20AND%20(SELECT%204037%20FROM(SELECT%20COUNT(*),CONCAT(CHAR(58,100,114,108,58),(SELECT%20(CASE%20WHE
N%20(4037=4037)%20THEN%201%20ELSE%200%20END)),CHAR(58,122,103,111,58),FLOOR(RAND(0)*2))x%20FROM%20information_schema.tables%20GROUP%20BY%20
x)a)%20AND%20(9909=9909 HTTP/1.1

UserAgent

Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322)

原始请求头

GET /resume/?/home/explore/category-1)%20AND%20(SELECT%204037%20FROM(SELECT%20COUNT(*),CONCAT(CHAR(58,100,114,108,58),(SELECT%20(CASE%20WHE
N%20(4037=4037)%20THEN%201%20ELSE%200%20END)),CHAR(58,122,103,111,58),FLOOR(RAND(0)*2))x%20FROM%20information_schema.tables%20GROUP%20BY%20
x)a)%20AND%20(9909=9909 HTTP/1.1
Host: safeline-demo.chaitin.cn
Accept-Encoding: identity
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322)

请求重放

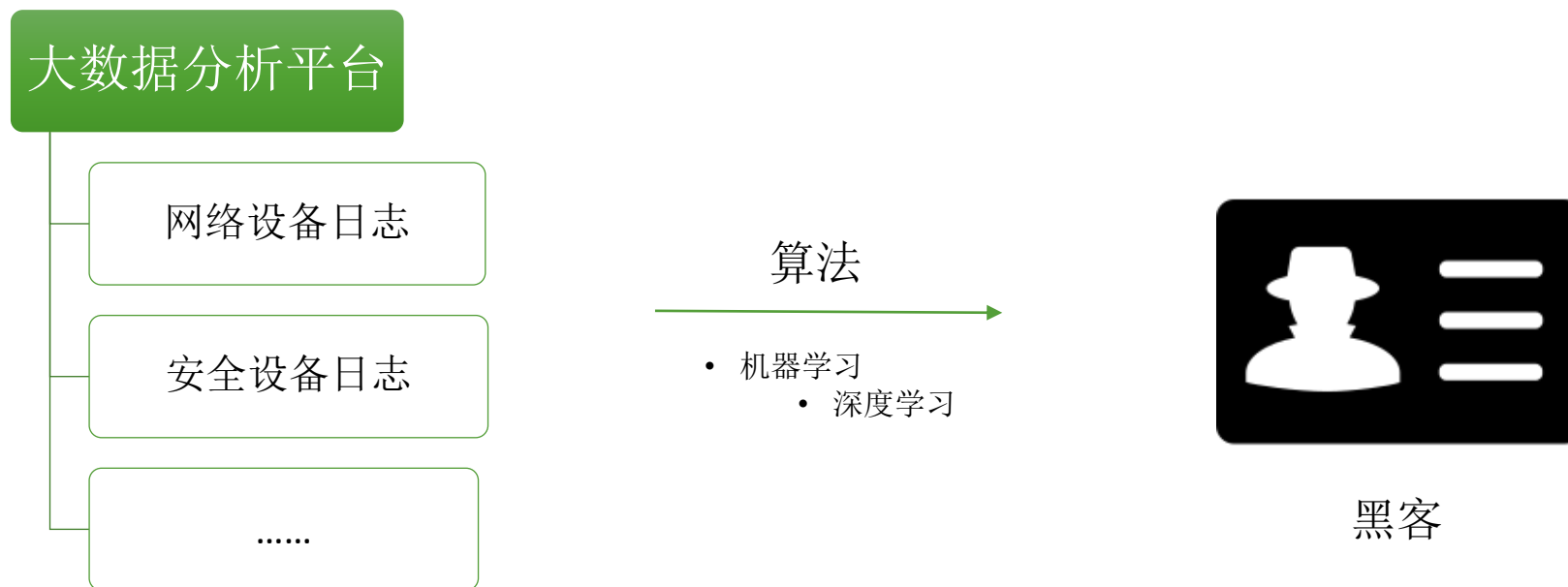
下载 删除 返回

Safeline SL-S10-20170907-092cb © 2017 Chaitin Tech.

被动防御的劣势愈加明显

- Struts2 应用漏洞
- WannaCry 蠕虫传播

“治疗”和“预防”的区别



理想状态

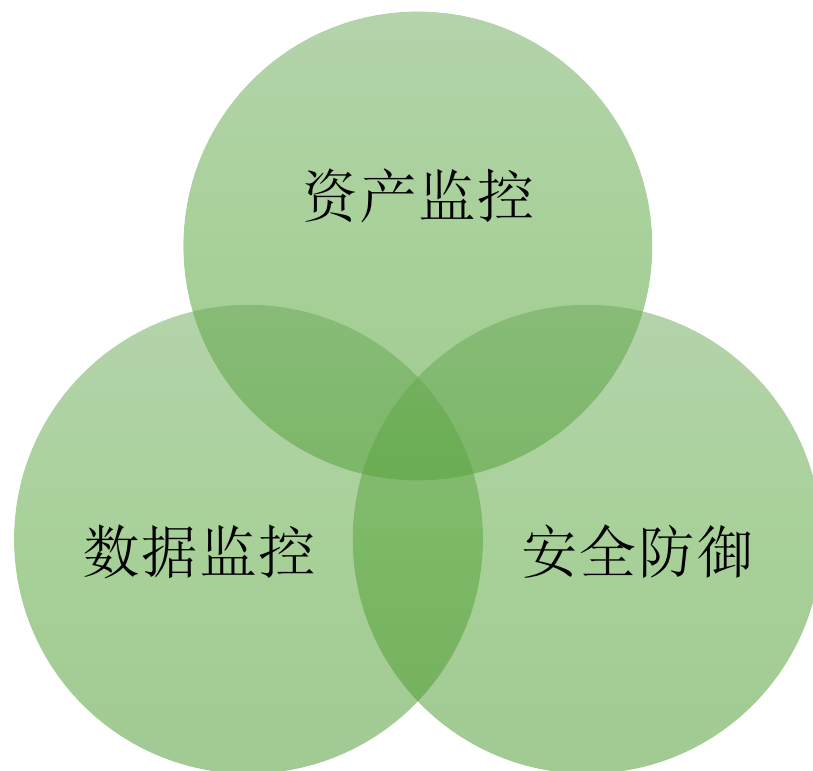
通过数据的异常发现“所有攻击”

- WEB攻击
- 钓鱼软件
- 木马病毒
-

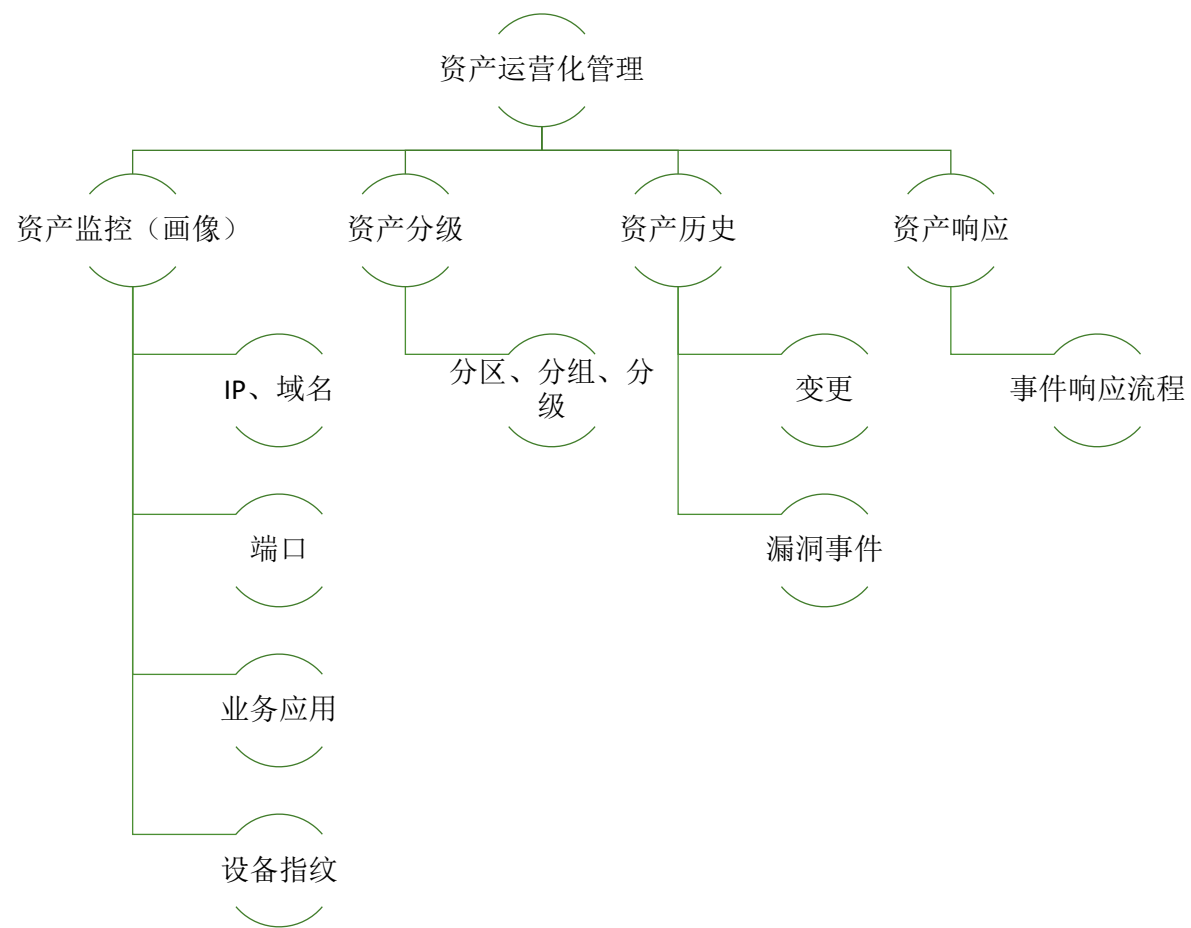
现实情况

无法100%覆盖所有的安全场景

安全体系架构

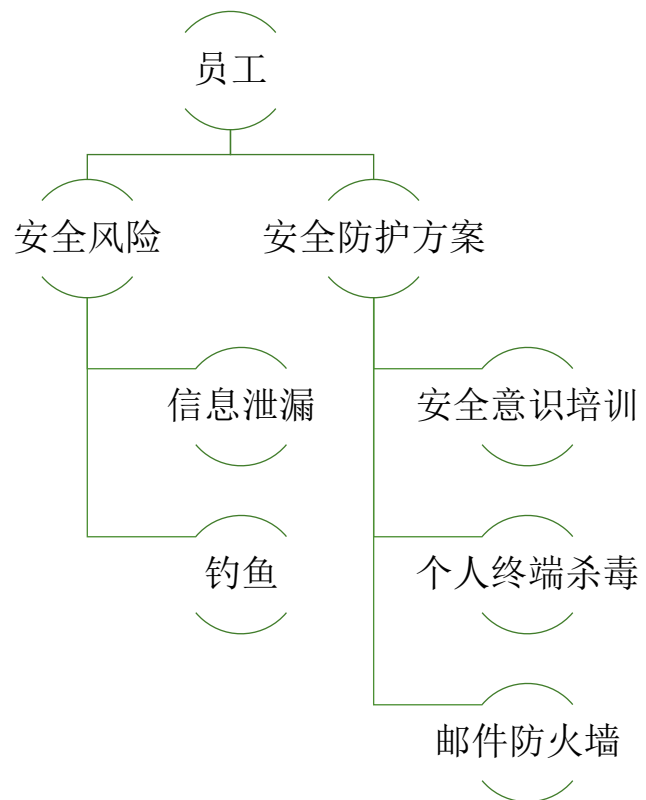
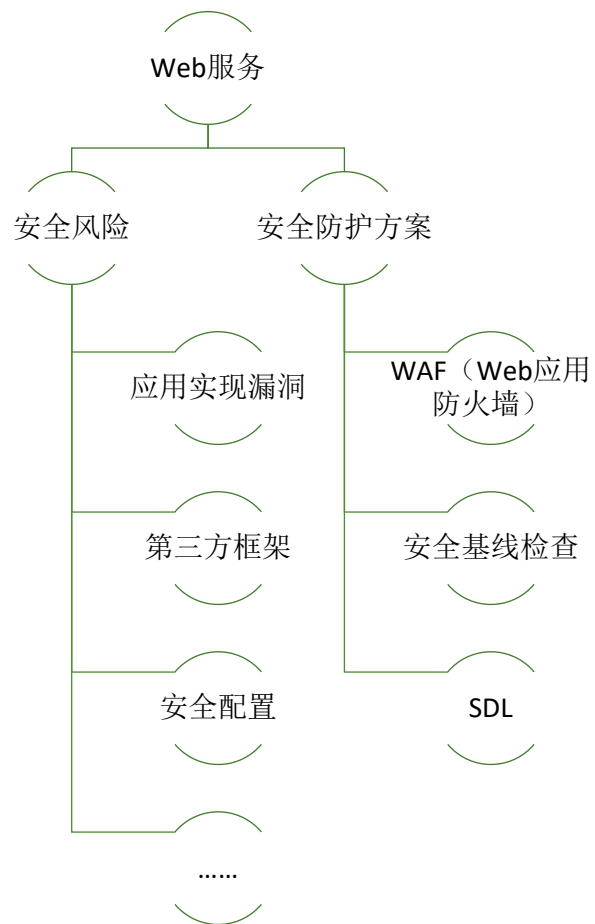


资产监控

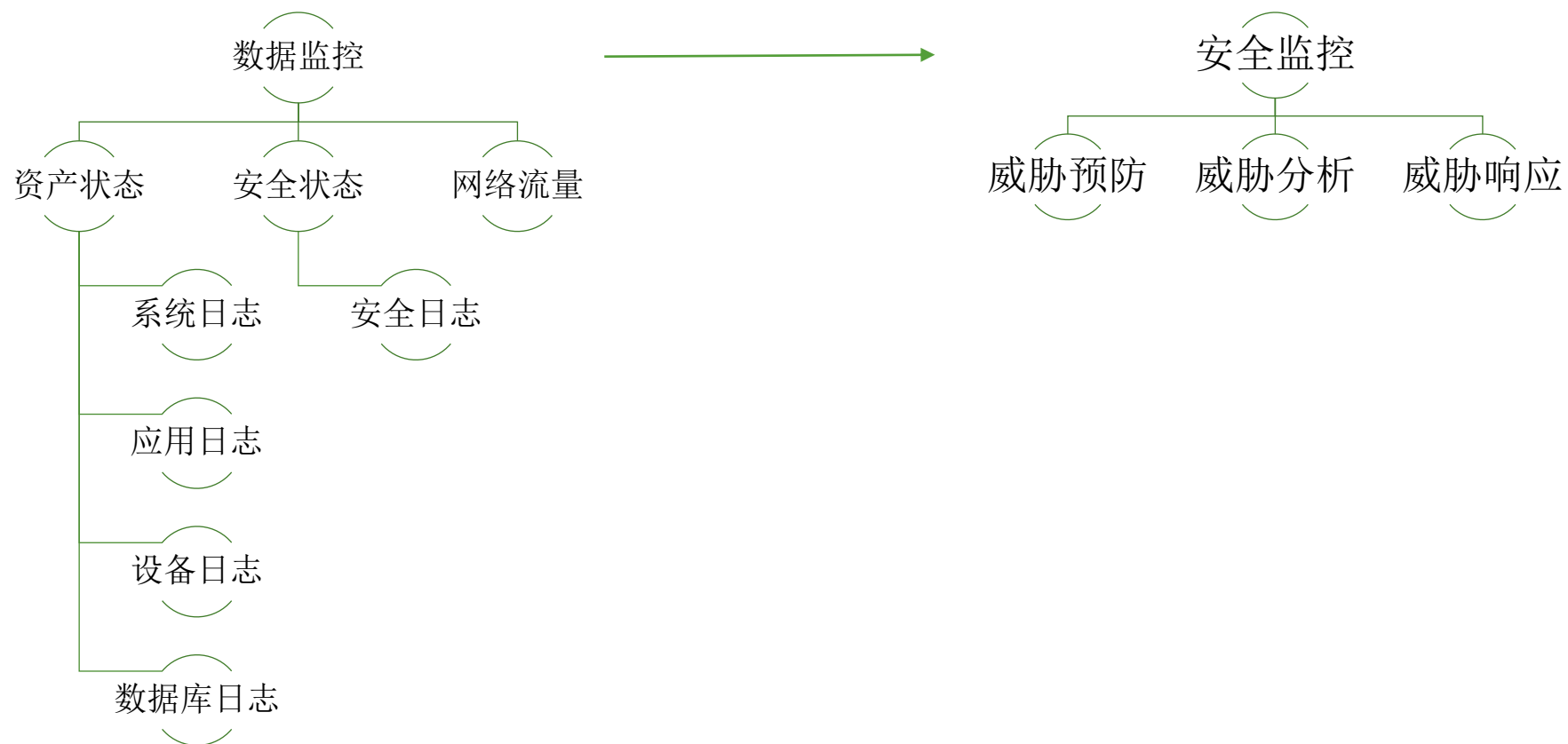




安全防御方案

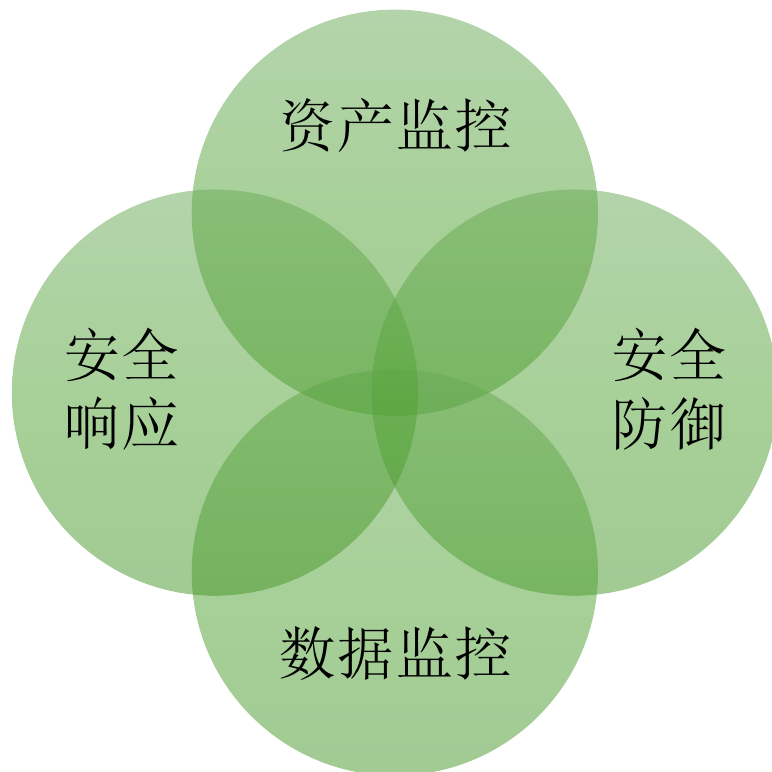


数据监控



安全体系架构

管理流程办法





Thanks

宁波长亭科技有限公司

张昌斌：13777292838