



点融秋季安全沙龙

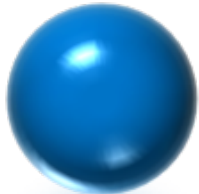
# 从攻击者视角看待互联网金融安全

徐钟豪 斗象科技

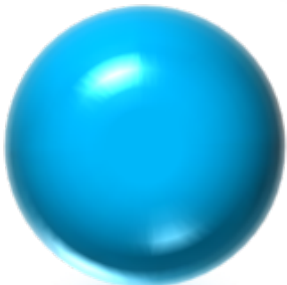


# 提纲

---



互联网金融安全事件分析



从攻击者视角看待互联网金融安全



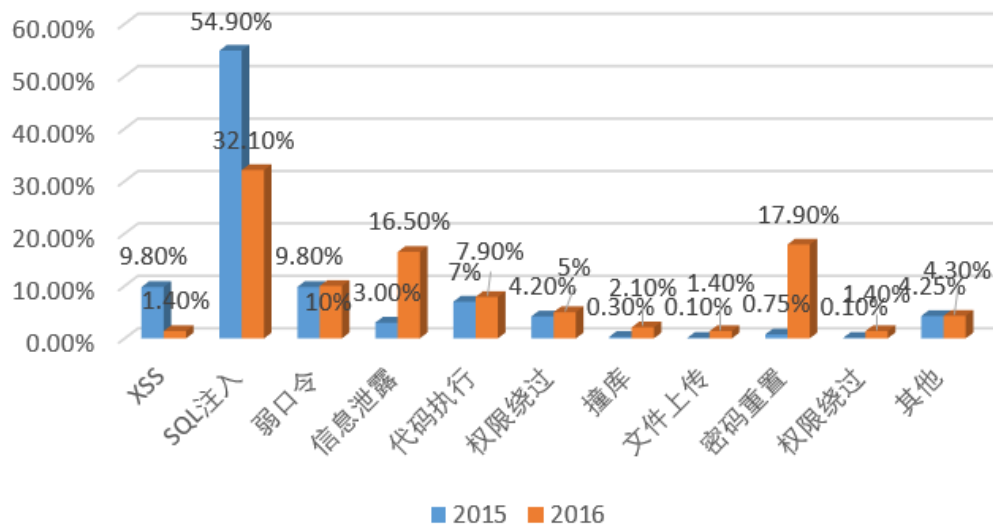
以资产为核心---CRS

互联网金融是一种普惠金融，正是因为它的亲民，让它承受了更多的未知风险。

因此，**互联网金融安全**也被推倒了一个**新的高度**。

# 互联网金融安全事件分析

2015、2016互联网金融问题同期对比



- SQL注入是互联网金融的最大威胁
- 弱口令、信息泄露等也是常见高危问题
- 漏洞类型朝着多元化方向发展

# 互联网金融安全事件分析

The screenshot displays the '漏洞盒子' (Vulnerability Box) website interface. The top navigation bar includes links for '首页' (Home), '黑板报' (Blackboard), '项目' (Projects), '排行榜' (Ranking), '企业服务' (Enterprise Services), '常见问题' (FAQ), '商城' (Marketplace), and '产品' (Products). The main content area is titled '盒子黑板报' (Blackboard) and features a search bar with '互联网金融' (Internet Finance) entered. Below the search bar, a list of security events is displayed, each with a home icon, a title, a description, a user profile, a medal count, and a rank.

漏洞标题	漏洞描述	发现者	奖励	排名
理财平台, 存储型XSS漏洞, 以及信息越权访问	理财平台, 存储型XSS漏洞, 以及信息越权访问	seoicc	2 Rank	2 Rank
网站存在储存型XSS漏洞	网站存在储存型XSS漏洞	seoicc	+2	2 Rank
安卓客户端脱壳后通信数据加密可被...	安卓客户端脱壳后通信数据加密可被...	大头鬼Love大花猫	50	8 Rank
SQL注入, 泄露全部用户数据	SQL注入, 泄露全部用户数据	匿名者	+2	3 Rank
SQL注入可泄露投资者泄露	SQL注入可泄露投资者泄露	匿名者	+3	4 Rank
主站源码信息泄露	主站源码信息泄露	匿名者		3 Rank
平台sql注入可获 470万公司信息+两万会员详...	平台sql注入可获 470万公司信息+两万会员详...	hkcs	500	12 Rank

# 从攻击者视角看待互联网金融安全

做了这么多的合规、基线、补丁稽查、购买了多种安全防护产品，却仍然做不好安全？

投入成本低？

安全团队消极怠工？

安全防护设备功能不够？

# 从攻击者视角看待互联网金融安全

---

因为视角

传统漏洞扫描或安全检测产品大多是以合规为导向  
企业安全建设与运营大多以被动式防御为主

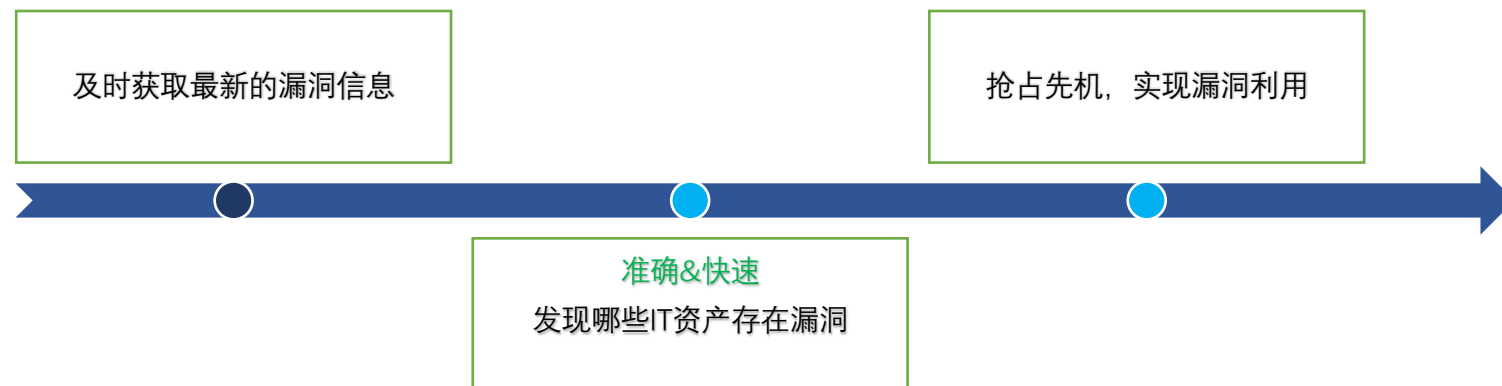
# 从攻击者视角看待互联网金融安全

	攻击者	企业
方向	攻击	防守
定位	全职做攻击	兼职做安全
信息获取	社工库、社会工程学、各种信息渠道等	大众媒体网站等
资讯获取速度	迅速	有延迟
成本	有明确目标, 各种绕过, 成本低	需要做到面面聚到, 成本高
动力	收益明确, 主动性强	工作被动, 有侥幸、懒惰心态



# 从攻击者视角看待互联网金融安全

攻击者如何思考？以一个0-Day举例



# 从攻击者视角看待互联网金融安全 – 0Day

## Struts2-032, 0-Day集中式爆发一瞥

漏洞标题	风险级别	所属项目
某处struts漏洞	高危	互联网漏洞与威胁情报 (互联网漏洞)
存在struts-s2-032漏洞	高危	互联网漏洞与威胁情报 (互联网漏洞)
struts2直播命令执行	高危	互联网漏洞与威胁情报 (互联网漏洞)
字在struts远程执行命令	高危	互联网漏洞与威胁情报 (互联网漏洞)
字在struts2S2032命令执行	高危	互联网漏洞与威胁情报 (互联网漏洞)
分站存在struts2命令执行	高危	互联网漏洞与威胁情报 (互联网漏洞)
系统存在struts2命令执行	高危	互联网漏洞与威胁情报 (互联网漏洞)
有限公司存在struts2命令执行	高危	互联网漏洞与威胁情报 (互联网漏洞)
国际存在struts2命令执行	高危	互联网漏洞与威胁情报 (互联网漏洞)
存在struts2命令执行漏洞	高危	互联网漏洞与威胁情报 (互联网漏洞)

[网警 威胁情报监控]	2016/4/26 12:45	江苏省医学会儿科struts2漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 14:00	西安未来国际俱乐部股份有限公司存在命令执行漏洞, 可获取权限, 上传文件	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 15:25	顺电某B2B系统存在漏洞任意命令执行可getshell	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 15:25	中国人民大学某院命令执行漏洞大量学生受害	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 15:25	!Message对象系统在SQL注入&mp;远程命令执行 (无需登录)	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 15:45	东风汽车网站某处命令执行漏洞可getshell	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 15:50	复旦大学某系统命令执行	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 16:40	德众数据某系统未授权访问导致命令执行	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 17:00	Talkingdata某系统未授权访问导致命令执行	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 17:55	复旦大学招生网存在最新Struts2 s2-032远程代码执行	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 18:05	携程某系统命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 18:30	跨境电商某系统存在命令执行	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 19:05	上海长途客运网站存在struts2 (s2-032) 远程命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 19:50	某清明eLearning在线S2032命令执行 (命令回显POC和GETSHELL POC)	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 21:20	华为某命令执行getshell	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 21:25	某网站某系统存在命令执行getshell	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 21:25	某系统存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 21:30	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 21:35	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 21:35	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 21:45	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 21:45	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 21:45	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 21:45	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 21:50	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 21:55	恒生电子某系统命令执行	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 21:55	渣打银行某系统命令执行漏洞导致getshell	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:00	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:10	华为网盘主站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:10	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:10	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:15	中国南方航空某系统命令执行	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:15	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:25	浙商银行存在Struts2 s2-032远程代码执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:25	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:25	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:25	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:25	成都市政府某分站存在Struts2 s2-032远程代码执行	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:25	西藏自治区地震局存在struts2 s2-032命令执行漏洞, 可getshell	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:25	鞍山高新技术产业园区存在Struts2 S2-032漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:25	华南理工大学分站Struts2 s2-032远程代码执行	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:25	青海省公安厅某系统平台存在Struts2 s2-032 漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:25	中国石油某子公司存在Struts2 s2-032 漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:25	甘肃某地州系统存在Struts2 s2-032 漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:30	陕西四喜存在Struts2 s2-032远程代码执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:30	郑州市政务服务中心存在Struts2 s2-032 漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 22:30	电子科技大学某系统存在Struts2 s2-032漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 23:05	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 23:15	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 23:15	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 23:15	某网站存在命令执行漏洞	高危	http://cvs.vulbox.com
[网警 威胁情报监控]	2016/4/26 23:45	中国电商某系统存在Struts2 s2-032漏洞	高危	http://www.vulbox.com
[网警 威胁情报监控]	2016/4/26 23:45	中国移动某系统存在struts2 s2-032命令执行漏洞	高危	http://www.vulbox.com

# 从攻击者视角看待互联网金融安全 - 运维组件

攻击者不再仅钟情于企业的业务网络，如边缘网络、测试服务器、C段、运维网等其他非核心业务网的渗透也可以造成不可估量的损失。

案例：2016年8月曝出zabbix工具存在sql注入漏洞，漏洞盒子仅一个月时间就搜集了大量此漏洞，超过1000+。

企业的安全不能仅聚焦重点业务，需要更全面的考虑

漏洞标题	风险级别	所属项目	白帽子
abbix注入 可命令执行	高危	互联网漏洞与威胁情报 (互联网漏洞)	
公司 zabbix注入可命令执行	高危	互联网漏洞与威胁情报 (互联网漏洞)	
zabbix注入	高危	互联网漏洞与威胁情报 (互联网漏洞)	
有限公司 zabbix注入可命令执行	高危	互联网漏洞与威胁情报 (互联网漏洞)	
网络科技有限公司 zabbix注入 可命令执行	高危	互联网漏洞与威胁情报 (互联网漏洞)	
有限公司 zabbix注入可命令执行	高危	互联网漏洞与威胁情报 (互联网漏洞)	
zabbix注入	高危	互联网漏洞与威胁情报 (互联网漏洞)	
存在zabbix注入	高危	互联网漏洞与威胁情报 (互联网漏洞)	
<a href="#">ZABBIX v2.2.x, 3.0.0-3.0.3 jsrpc 参数profi</a>	高危	互联网漏洞与威胁情报 (互联网漏洞)	
有限公司Zabbix SQL Injection	高危	互联网漏洞与威胁情报 (互联网漏洞)	

# 从攻击者视角看待互联网金融安全 – 绕过防护设备

单一的防御方案如：WAF，IPS等已经防不住当今的高级黑客。

案例：漏洞盒子查到的白帽子绕过企业WAF，实现获取企业敏感信息的案例。

不能单单只是依附于安全产品，构建更完善的纵深防御体系

• [redacted] 存在存储性xss漏洞，可绕过waf进行跨站脚本攻击	中危	[redacted]	[redacted]
• [redacted] 冷链在线搜索处绕过: [redacted] WAF反射xss	低危	[redacted]	[redacted]
• [redacted] 结合后端数据库特性waf完全绕过	高危	[redacted]	[redacted]
• [redacted] 存在SQL注入漏洞，有waf 标记：Q3报告-廖文	中危	[redacted]	[redacted]
• [redacted] 后台存在注入，已绕过waf进入后台	高危	[redacted]	[redacted]
<a href="#">SQL绕过 [redacted] waf获取70万人信息(包括名字身份证号工作单位等)</a>	百度 Google 高危	互联网漏洞与威胁情报 (互联网漏洞)	[redacted]
• [redacted] 某站用的waf服务器远程命令执行	高危	互联网漏洞与威胁情报 (互联网漏洞)	[redacted]
• [redacted] 站点SQL注入 (绕过waf)	迅雷 已反馈 高危	互联网漏洞与威胁情报 (互联网漏洞)	[redacted]

# 从攻击者视角看待互联网金融安全 – 威胁情报

情报标题	风险级别	所属项目	白帽子	提交时间
系统服务器配置文档信息泄露 (包含服务密码, 数据库密码) <span>情报</span>	高危	互联网漏洞与威胁情报 (互联网漏洞)		2017-07-11 10:00:00
针对企业的钓鱼网站 <span>腾讯360</span> <span>情报</span>	高危	互联网漏洞与威胁情报 (互联网漏洞)		2017-07-11 10:00:00
无视权限上传文件 <span>腾讯</span> <span>情报</span>	高危	互联网漏洞与威胁情报 (互联网漏洞)		2017-07-11 10:00:00 5
遭黑手 数据泄露 (成功拿到黑手银行卡) <span>情报</span>	中危	互联网漏洞与威胁情报 (互联网漏洞)		2017-07-11 10:00:00
“是个坑” <span>阿里巴巴集团</span> <span>情报</span>	低危	互联网漏洞与威胁情报 (互联网漏洞)		2017-07-11 10:00:00 2
邮件泄露 <span>情报</span>	中危	互联网漏洞与威胁情报 (互联网漏洞)		2017-07-11 10:00:00
网上赌博商城图片一枚 <span>情报</span>	中危	互联网漏洞与威胁情报 (互联网漏洞)		2017-07-11 10:00:00
分公司漏洞未修复 <span>集团</span> <span>情报</span>	高危	互联网漏洞与威胁情报 (互联网漏洞)		2017-07-11 10:00:00
有限公司被挂黑页 <span>情报</span>	高危	互联网漏洞与威胁情报 (互联网漏洞)		2017-07-11 10:00:00
移动缴费平台后门 <span>情报</span>	高危	互联网漏洞与威胁情报 (互联网漏洞)		2017-07-11 10:00:00

# 从攻击者视角看待互联网金融安全 – 威胁情报

有防护的地方没人攻击  
攻击的地方没有人防护

## 企业方

- 企业方防火墙, IDS, IPS部署完毕
- 企业方WEB端云WAF准备就绪
- 企业方SRC正在接收漏洞提交
- 企业方威胁情报接受中
- 企业方成功抵御攻击, 正在自检
- 企业方资产梳理完成, 正在自检

## 攻击方

- 攻击方获得**泄露数据**, 进行数据分析
- 攻击方于**GIT**上获取敏感**源代码**
- 攻击方开始使用**社工库撞库**攻击
- 攻击方开始使用Nday循环攻击边缘资产, OWASP TOP 10、**逻辑漏洞**
- 攻击方获取对方资产分布, 攻击准备

# 从攻击者视角看待互联网金融安全

---

作为企业，就0Day如何快速有效的解决问题？

# 从攻击者视角看待互联网金融安全

---

第一时间获取威胁情报

及时梳理，哪些资产上存在问题？

缓解措施 & 修复方案



# 从攻击者视角看待互联网金融安全

---

然而，道理都懂，说起来容易，做起来难。

**HOW?**

有多少资产？哪些资产上存在漏洞？检测工具、修复方案？安全预警渠道？

以**资产**为核心，管理企业资产

# 资产画像



关联度

- 域名
- 网站标题
- Headers
- Meta, Keyword, Desc
- SSL证书信息
- .....

权重

# 资产发现姿势

## 资产发现姿势

### 端口扫描/指纹识别

NMAP

ZMAP

MASSCAN

全网资产搜索引擎 (ZoomEye、SHODAN、Censys)

### 关联IP

子域C段扩展

全网资产搜索引擎 (ZoomEye、SHODAN、Censys)

google hack

github hack

### 子域发现

暴力破解

爬虫

区域传送

IP反查

ICP备案反查

注册人/注册邮箱反查

SSL证书使用者备用名称

Certificate Transparency

google hack

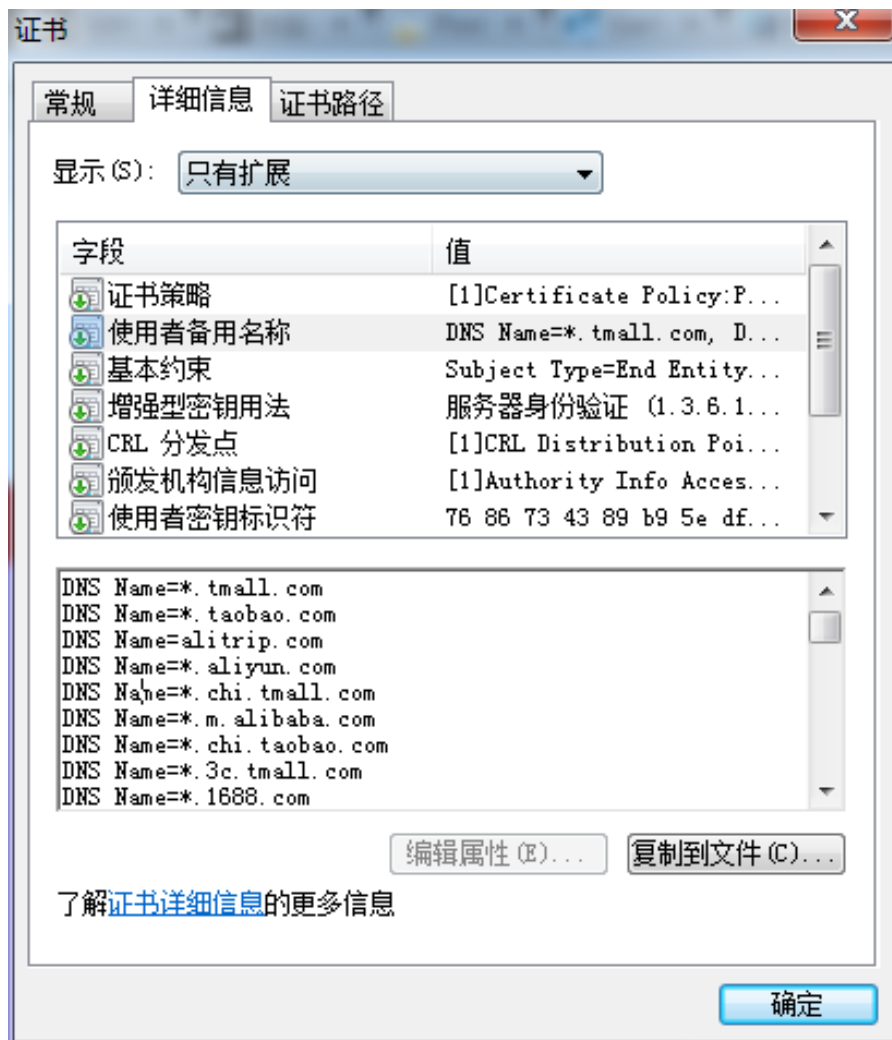
github hack

crossdomain.xml

sitemap

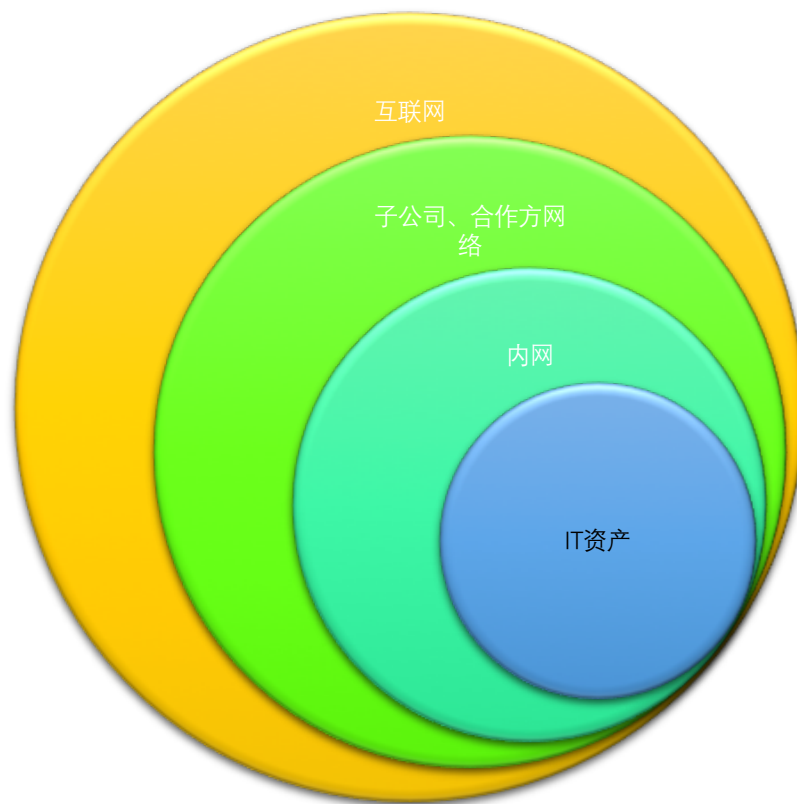
robot.txt

# 使用者备用名称



# 信任边界

## 资产信任边界划分



# 以资产为核心

企业做安全，决策者需要把最多的资源和精力投入到最值得的资产上。

**Q:** 那么问题来了，如何判定“最值得的资产”？

**A:** 资产档案库



# 以资产为核心

回到主题，这样能降低企业的风险吗？

威胁情报，可从乙方获得

针对0-Day，第一时间提供最新安全漏洞预警

资产建模功能

精确定位，哪些资产特征符合0-Day指纹信息

自动化检测 + 解决方案

快速自动化检测并提供完整的修复方案、专家协查



但企业安全管理何止是0Day

# 总结

---

第一、给懂安全的人一扇门

WHY?

专业的事情留给专业的人

# 企业安全多维度

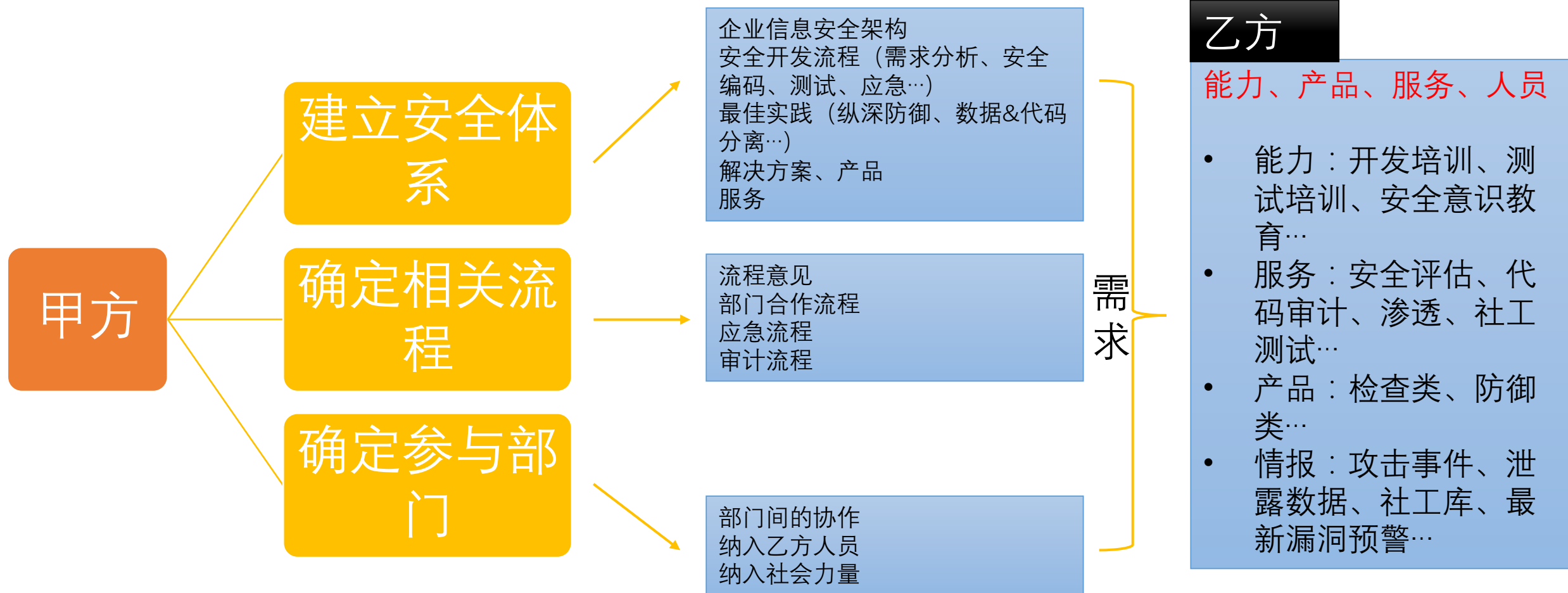
企业信息安  
全多维度驱  
动

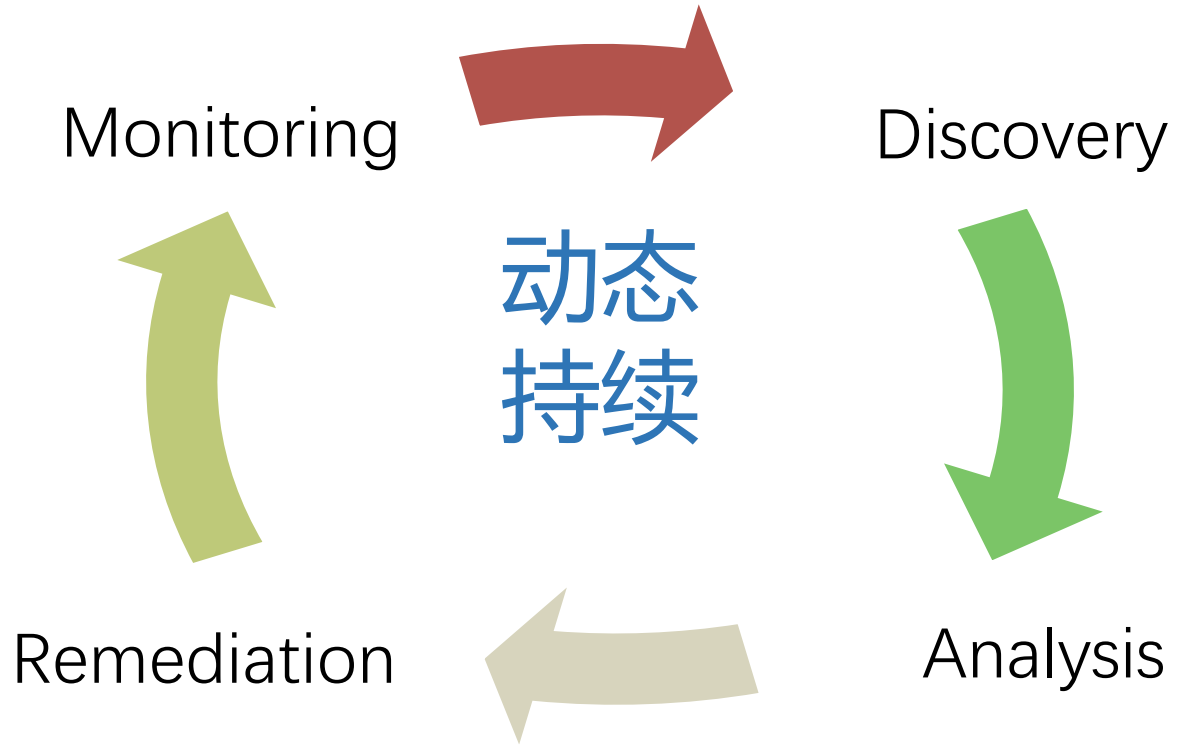
资产管理：资产识别、梳理&分类（服务、版本、类型、用途），  
构建资产矩阵

威胁管理：威胁建模、暴露面管理、攻击面分析、威胁情报

漏洞管理：漏洞归属、定期检测、修复、补丁、复测、存档

# 甲方需求&乙方供给







# 点融秋季安全沙龙

谢谢

