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

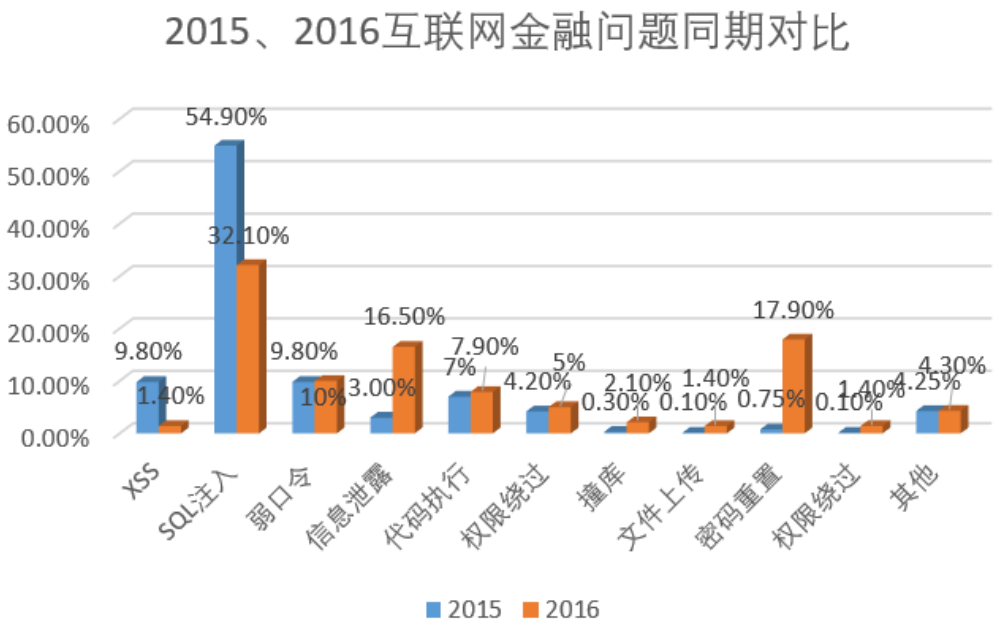
从攻击者视角看待互联网金融安全

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



- 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
- 漏洞类型朝着多元化方向发展

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

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

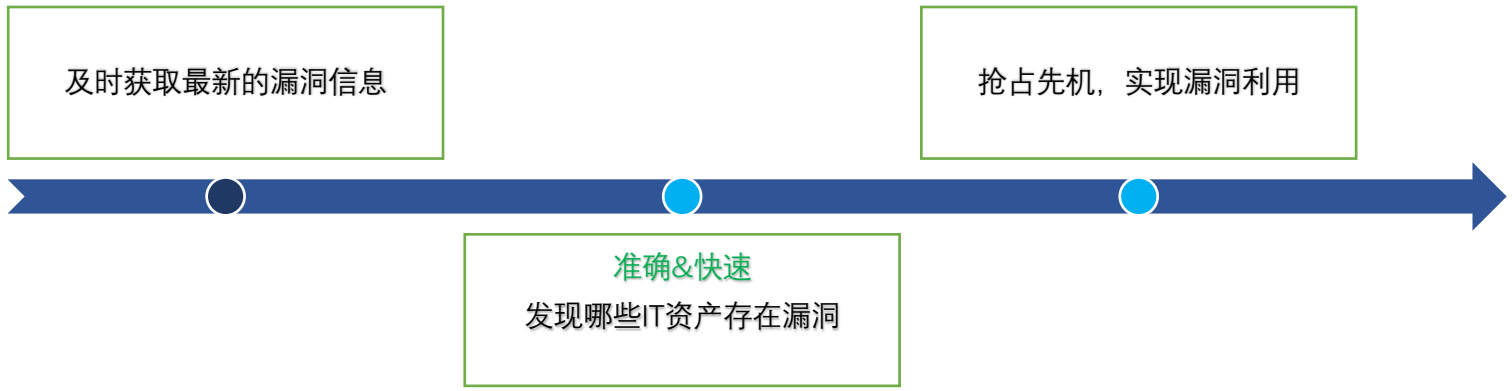
传统漏洞扫描或安全检测产品大多是以合规为导向
企业安全建设与运营大多以被动式防御为主

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

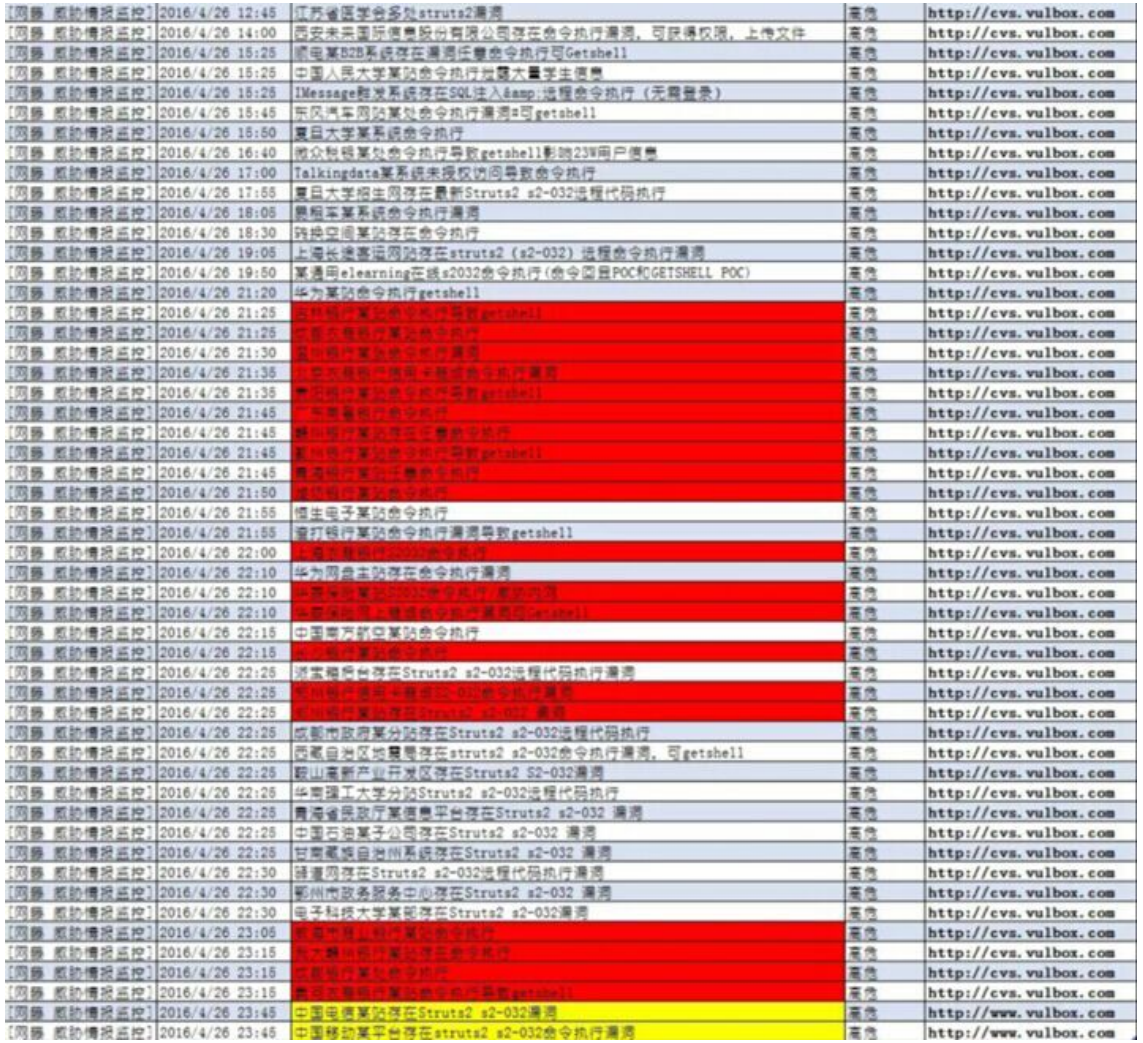
攻击者如何思考？以一个0-Day举例



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
[redacted]某处struts漏洞 标记：struts2	高危	互联网漏洞与威胁情报（互联网漏洞）
[redacted]存在struts-s2-032漏洞	高危	互联网漏洞与威胁情报（互联网漏洞）
[redacted]struts2直播命令执行 [redacted] 标记：struts2	高危	互联网漏洞与威胁情报（互联网漏洞）
[redacted]存在struts远程执行命令 标记：struts2	高危	互联网漏洞与威胁情报（互联网漏洞）
[redacted]存在struts2S2032命令执行 标记：struts2	高危	互联网漏洞与威胁情报（互联网漏洞）
[redacted]分站存在struts2命令执行 标记：struts2	高危	互联网漏洞与威胁情报（互联网漏洞）
[redacted]系统存在struts2命令执行 标记：struts2	高危	互联网漏洞与威胁情报（互联网漏洞）
[redacted]限公司存在struts2命令执行 标记：struts2	高危	互联网漏洞与威胁情报（互联网漏洞）
[redacted]际存在struts2命令执行 跨邦国际	高危	互联网漏洞与威胁情报（互联网漏洞）
[redacted]存在struts2命令执行漏洞 标记：struts2	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 – 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）	
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）	
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）	
在zabbix注入	高危	互联网漏洞与威胁情报（互联网漏洞）	
ZABBIX v2.2.x, 3.0.0-3.0.3 jsrpc 参数profi	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）	

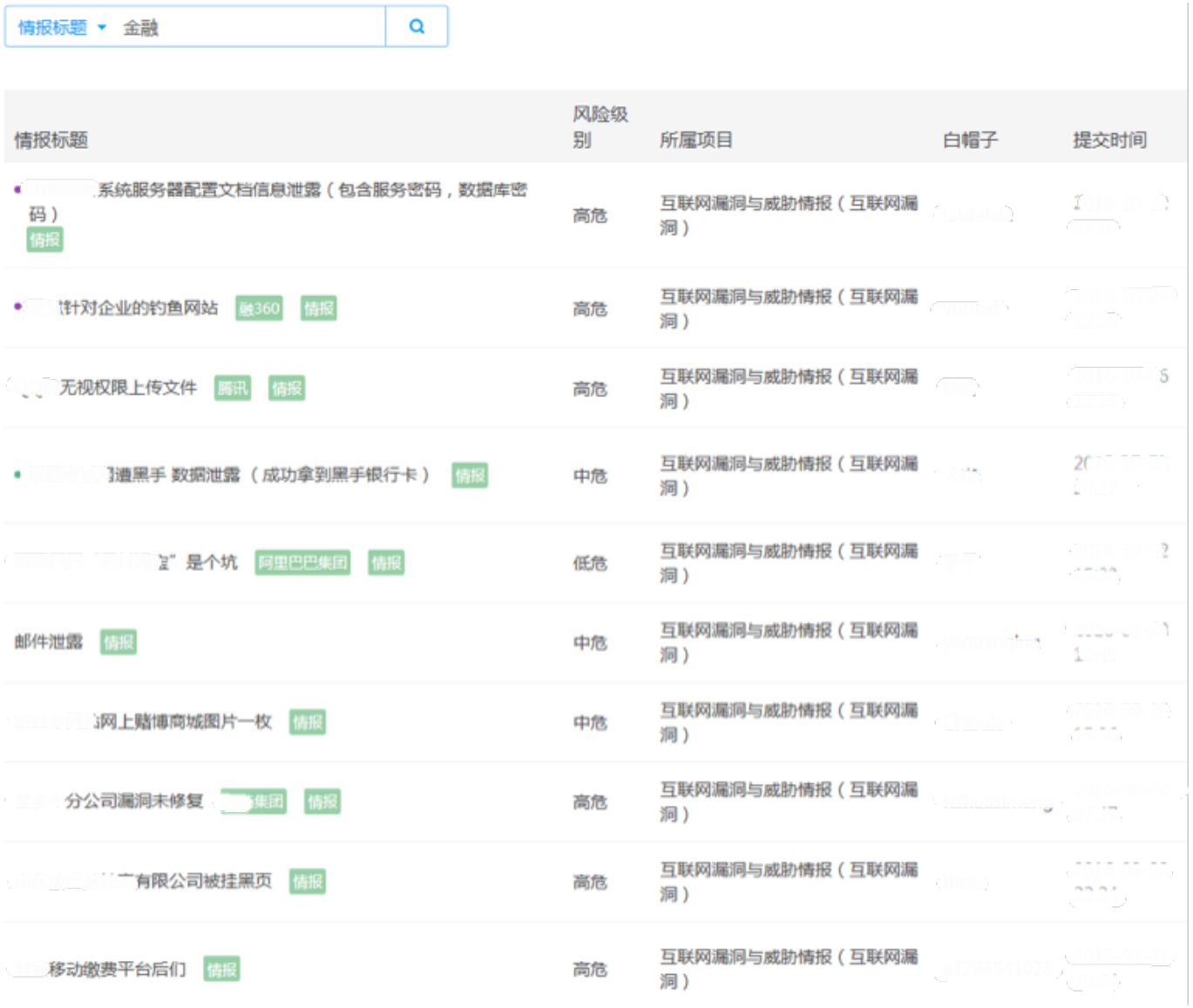
从攻击者视角看待互联网金融安全 – 绕过防护设备

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

从攻击者视角看待互联网金融安全 – 威胁情报



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

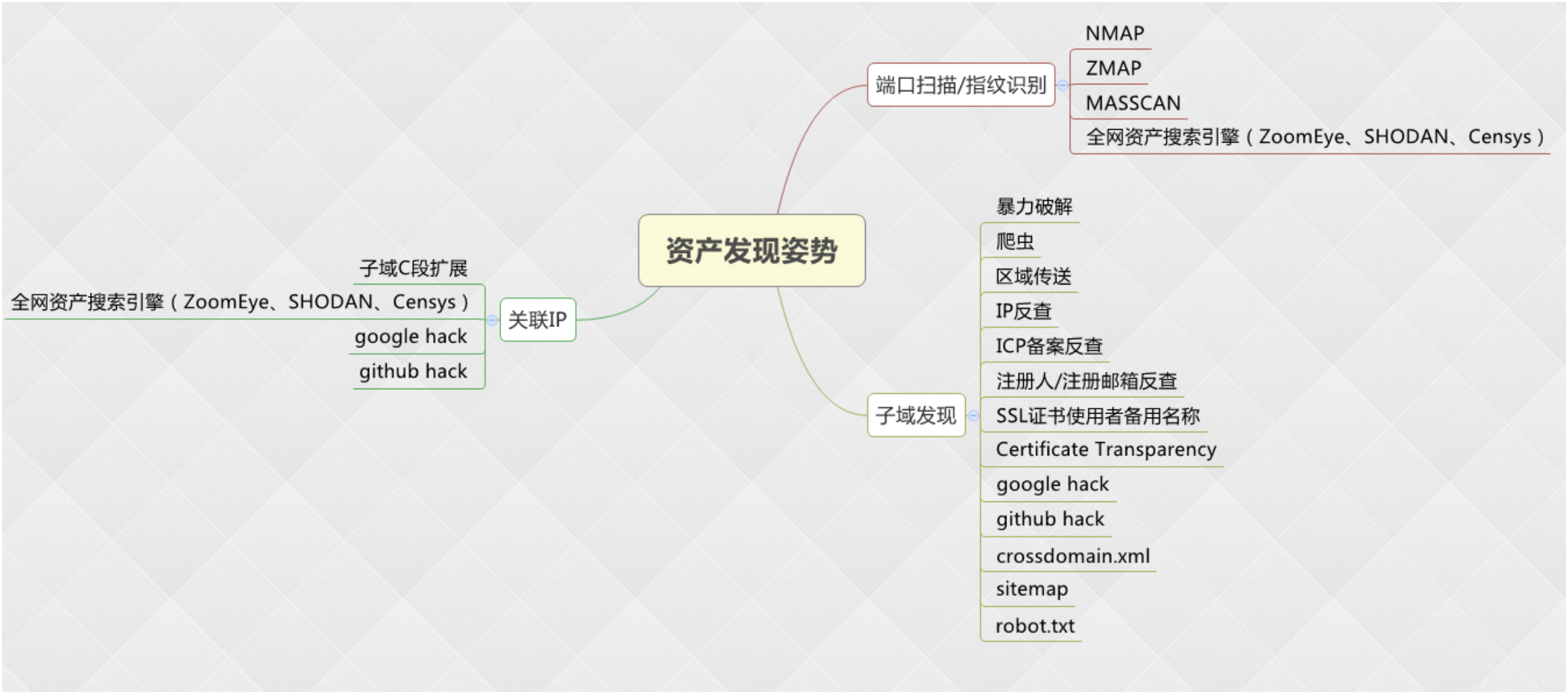
域名 IP 端口 服务 类别 用途 指纹

关联度

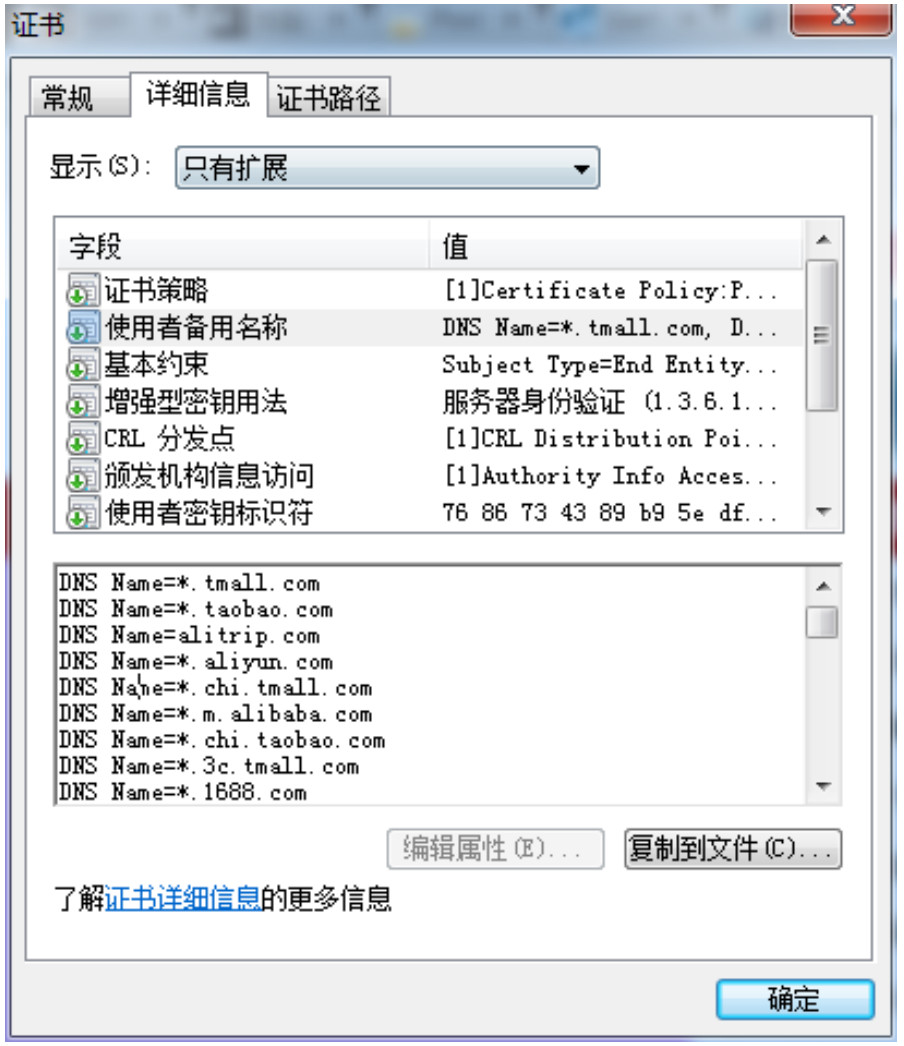
- 域名
- 网站标题
- Headers
- Meta, Keyword, Desc
- SSL证书信息
- ……

权重

资产发现姿势

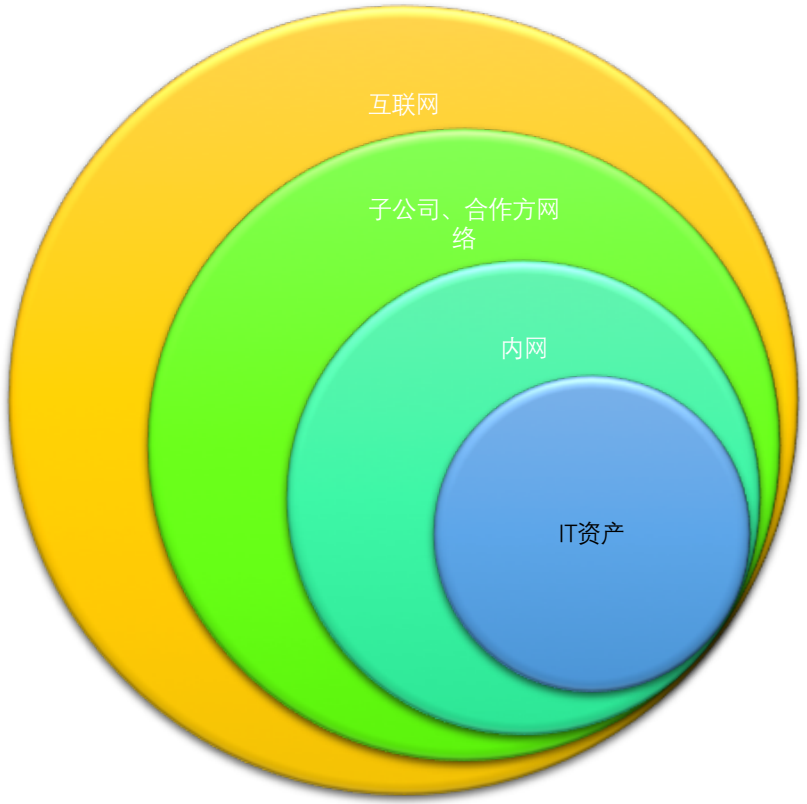

资产发现姿势
端口扫描/指纹识别
NMAP
ZMAP
MASSCAN
全网资产搜索引擎（ZoomEye、SHODAN、Censys）
子域发现
暴力破解
爬虫
区域传送
IP反查
ICP备案反查
注册人/注册邮箱反查
SSL证书使用者备用名称
Certificate Transparency
google hack
github hack
crossdomain.xml
sitemap
robot.txt
关联IP
子域C段扩展
全网资产搜索引擎（ZoomEye、SHODAN、Censys）
google hack
github hack

使用者备用名称


证书
常规
详细信息
证书路径
显示(S): 只有扩展
字段
值
证书策略
[1]Certificate Policy:P...
使用者备用名称
DNS Name=*.tmall.com, D...
基本约束
Subject Type=End Entity...
增强型密钥用法
服务器身份验证 (1.3.6.1...
CRL 分发点
[1]CRL Distribution Poi...
颁发机构信息访问
[1]Authority Info Acces...
使用者密钥标识符
76 86 73 43 89 b9 5e df...
DNS Name=*.tmall.com
DNS Name=*.taobao.com
DNS Name=alitrip.com
DNS Name=*.aliyun.com
DNS Name=*.chi.tmall.com
DNS Name=*.m.alibaba.com
DNS Name=*.chi.taobao.com
DNS Name=*.3c.tmall.com
DNS Name=*.1688.com
编辑属性(E)...
复制到文件(C)...
了解证书详细信息的更多信息
确定

信任边界

资产信任边界划分

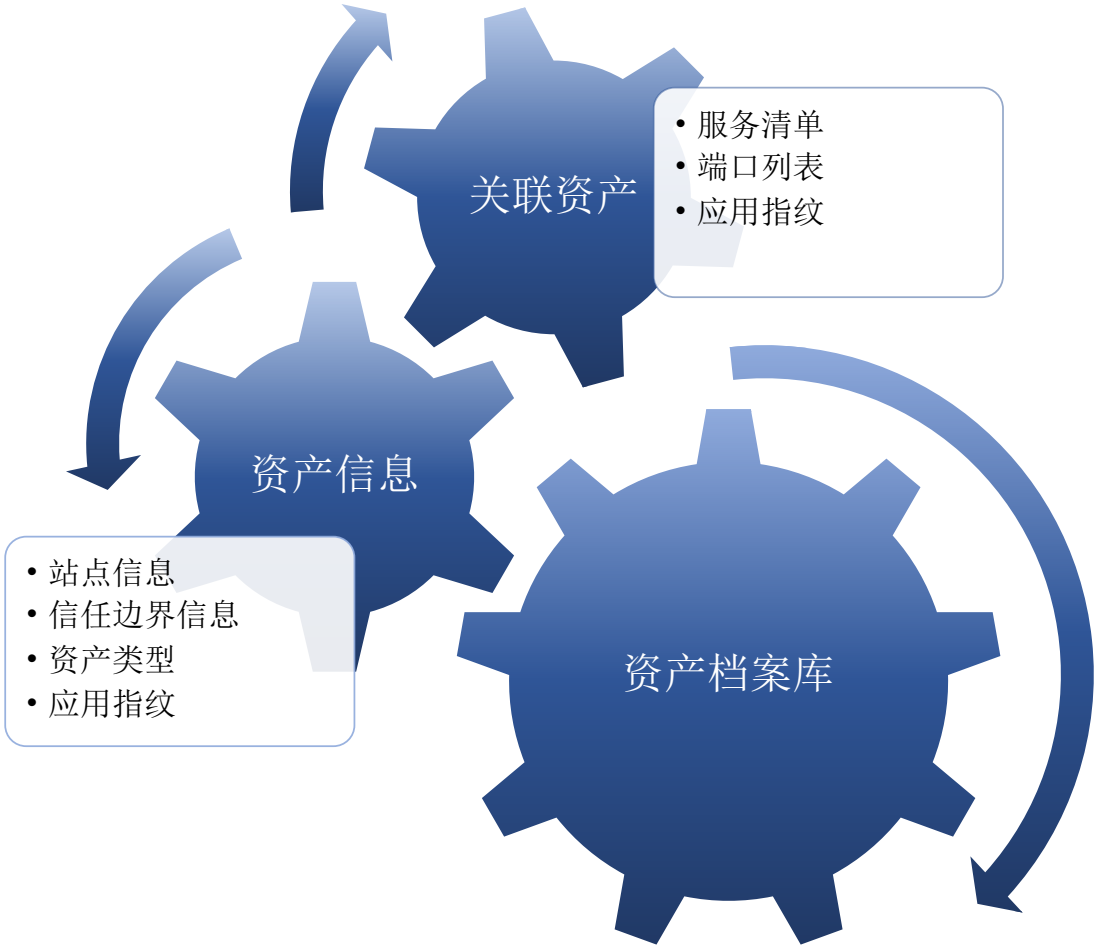


以资产为核心

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?

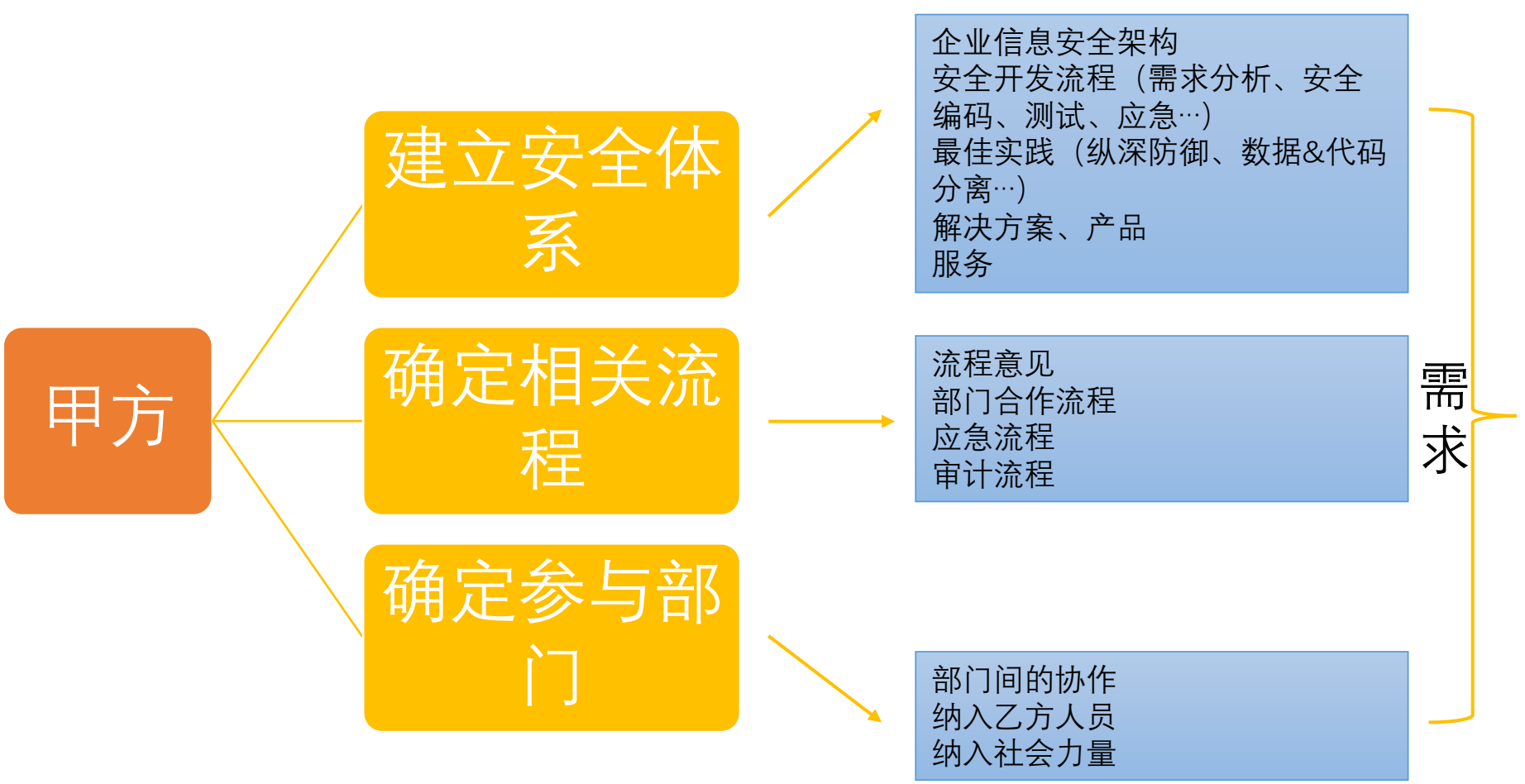
专业的事情留给专业的人

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

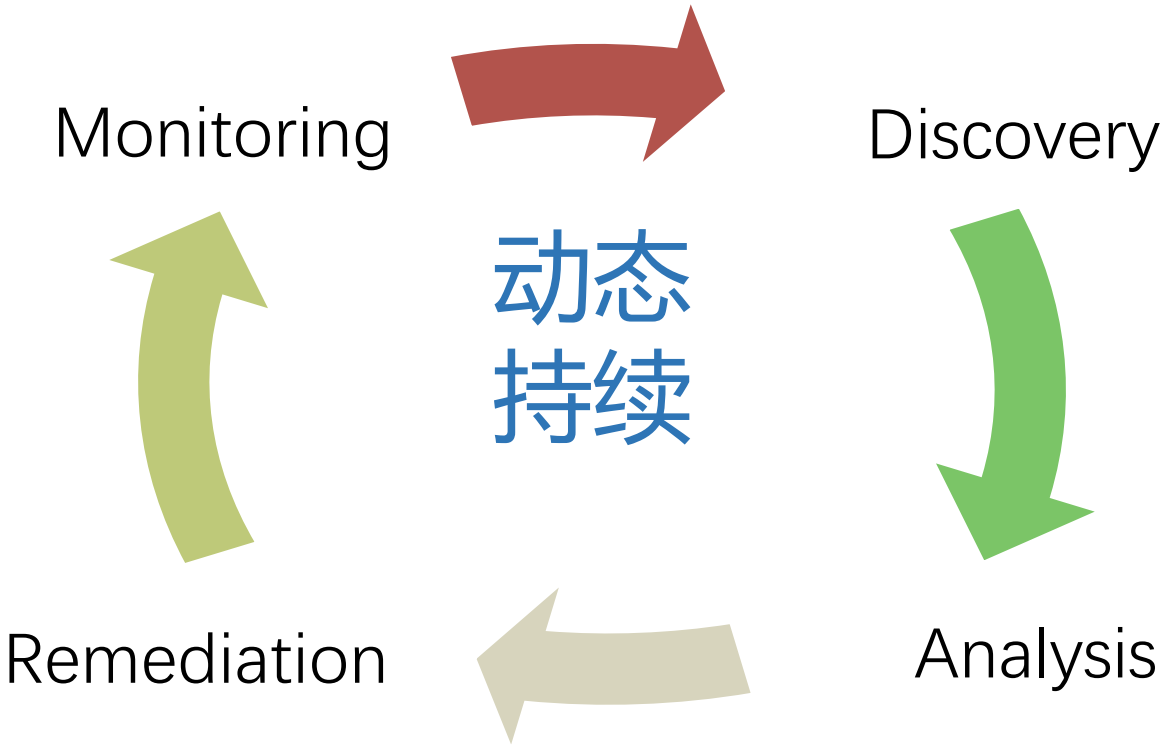


乙方

能力、产品、服务、人员

- 能力：开发培训、测试培训、安全意识教育…
- 服务：安全评估、代码审计、渗透、社工测试…
- 产品：检查类、防御类…
- 情报：攻击事件、泄露数据、社工库、最新漏洞预警…

理念



点融秋季安全沙龙

谢谢