塔防模型落地之运维大战情报

[黑客叔叔p0tt1@凌晨网络科技]

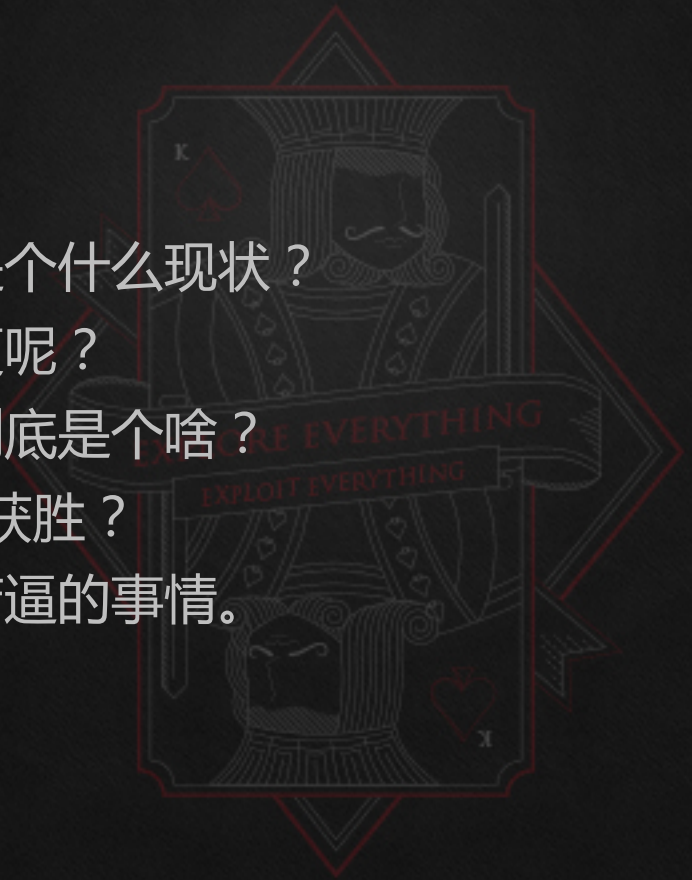
About Me

姚威
ID:黑客叔叔p0tt1
大家口中的“大炮”
广州凌晨网络科技有限公司 CEO
RainRaid Crew 信息安全团队负责人
3.A.M Lab 凌晨三点安全实验室负责人

凌晨网络科技

非典型双子座的信息安全创业者

目录



1.说点实话，针对企业的攻击是个什么现状？
2.讲点废话，漏洞到底谁在修复呢？
3.谈点老话，纵深防御和塔防到底是个啥？
4.放点狠话，运维VS情报 谁将获胜？
5.来点笑话，总结下企业安全苦逼的事情。

Part. 01

说点实话，针对企业的攻击是个什么现状？

为什么这张图火了呢？

那些年，醉人的“三字经”

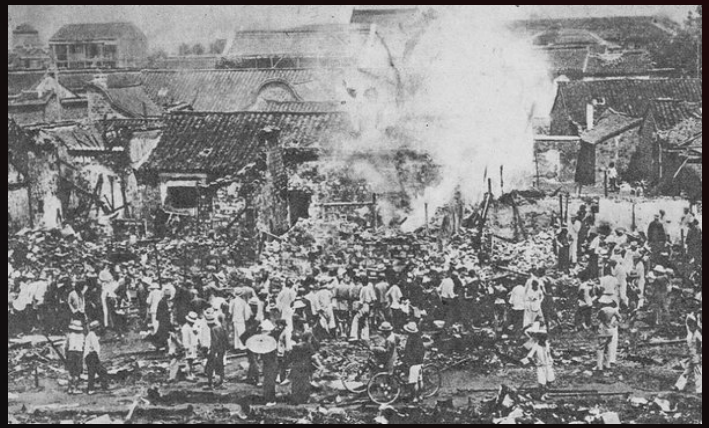
网站渗透娱乐版：

进谷歌	找注入
没注入	就旁注
没旁注	用Oday
没Oday	猜目录
没目录	就嗅探
爆账户	找后台
传小马	放大马
拿权限	挂页面
放暗链	清数据

针对企业的实战版→

搞企业	先扫描
扫描器	商业好
默认密	都知道
社工库	找一找
邮箱号	先列好
九头蛇	跑一跑
搞不定	放大招
发邮件	凭伪造
没邮箱	搞网站
二级域	皆可爆
老漏洞	没修好
新漏洞	刷一票
干研发	Git 找
源代码	全都要
C D N	可以跳
防火墙	可以撬
堡垒机	可以绕
云防护	可以秒
是企业	没有哪家搞不了！

有种攻击叫做“无差别”



还有种攻击叫做“见缝插针”

防护的地方没人打
打的地方没人防护

请随意感受下企业负责防御的相关部门的心情

针对企业或组织的攻击现状

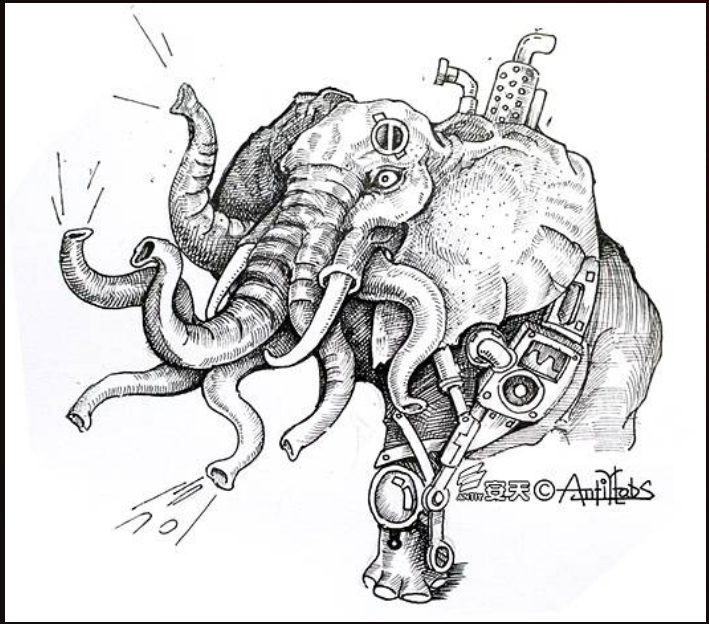
[!] 防守方IDS，IPS部署完毕
[!] 防守方WEB端云WAF准备就绪
[!] 防守方SRC正在接收漏洞提交
[!] 防守方威胁情报接受中
[!] 防守方成功抵御攻击，正在自检
[!] 防守方资产梳理完成，正在自检
...
.....

[!] 攻击方获得泄露数据
[!] 攻击方于GIT上获取敏感源代码
[!] 攻击方开始使用撞库攻击
[!] 攻击方开始使用Nday循环攻击
[!] 攻击方获取对方资产分布，攻击准备
[!] 攻击方放弃使用0day，任务胜利
...
.....

最后插一嘴

0day固然可怕
然而你还不配

白象舞步的思考



第二攻击波普遍使用了具有极高社工构造技巧的鱼叉式钓鱼邮件进行定向投放，至少使用了CVE-2014-4114和CVE-2015-1641等三个漏洞;其在传播层上不再单纯采用附件而转为下载链接、部分漏洞利用采取了反检测技术对抗;其相关载荷的HASH数量则明显减少，其中使用了通过Autoit脚本语言和疑似由商业攻击平台MSF生成的ShellCode;同时其初步具备了更为清晰的远程控制的指令体系。

摘自安天发布的《白象的舞步——来自南亚次大陆的网络攻击》分析报告

Part. 02

讲点废话，漏洞到底谁在修复呢？

企业安全的各种角色

企业安全相关负责人

企业安全部门人员

企业运维人员

企业研发人员

一个真实案例

企业安全相关负责人

你们赶紧修复呀

企业安全部门人员

SRC收到一个弱密码漏洞
我们自己的人又检测出一个
SQL注入漏洞

企业运维人员

企业研发人员

一个真实的现状

企业安全相关负责人

看来漏洞永远补不完
甚至不可能减少

企业安全部门人员

漏洞类别没有增加
漏洞数量还在增加

企业运维人员

下次设置密码
还是qaz@123

企业研发人员

下次写数据库查询还
是不带过滤的

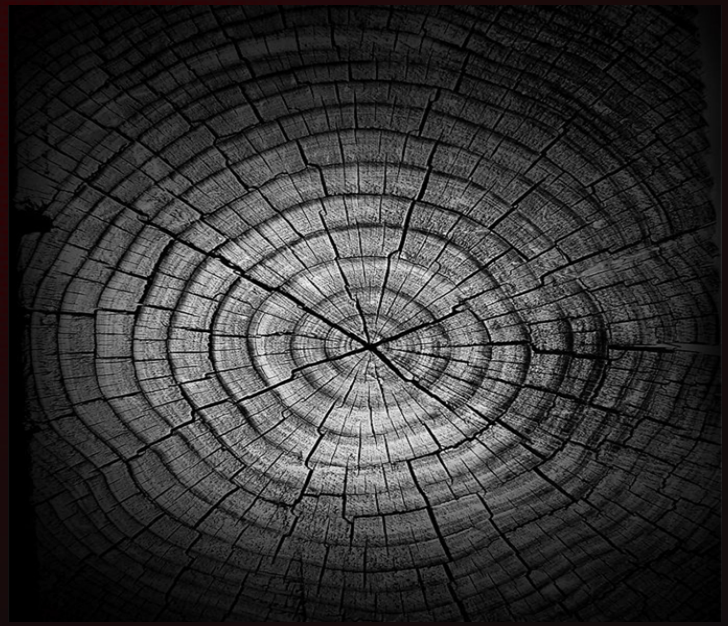
补洞的人不懂安全
懂安全的插不上手

Part. 03

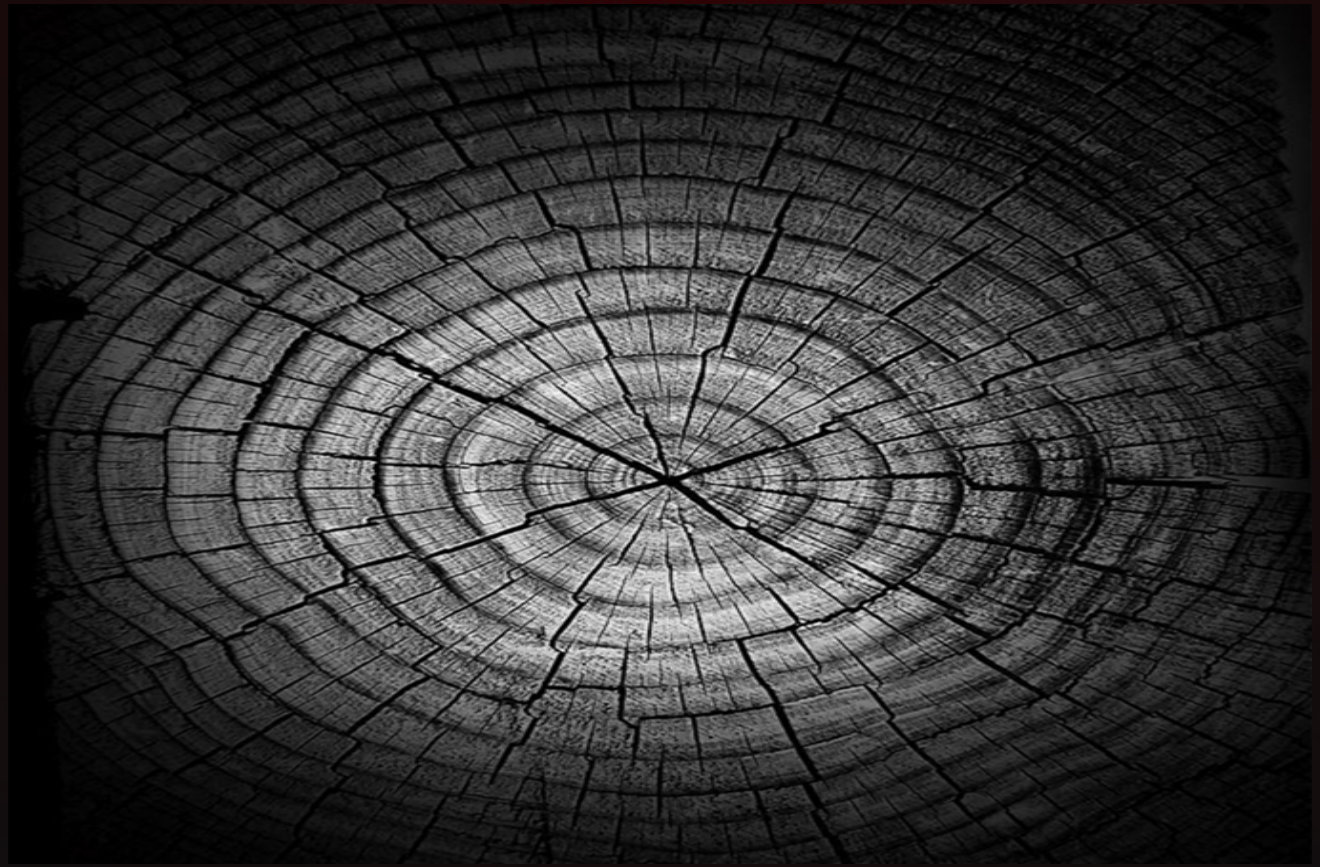
谈点老话，纵深防御和塔防到底是个啥？

纵深防御和塔防到底是个啥？

纵深防御和塔防到底是个啥？



我知道你们都是这么干的！



说好的边界防御设备呢？

我们的防御是坚不可摧的！

事实上成了攻击的跳板- -！

关于纵深防御的两个浅显误区

IPS,IDS等等安全设备的堆叠并没有纵深

有足够纵深的却没有限制攻击路线等于没有防御

为了便于理解我只能选择“放毒”

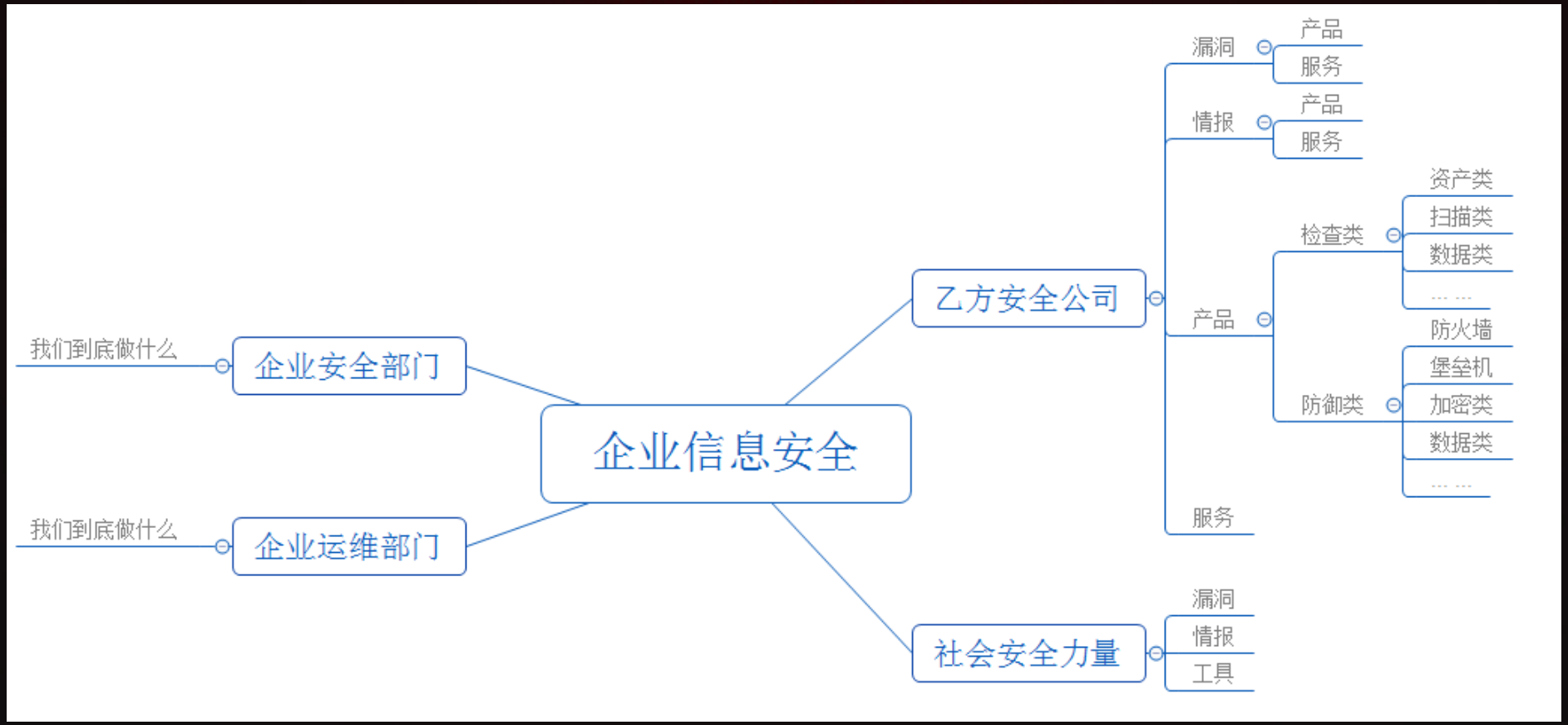
一个按照攻击路线的攻击者
你的防御体系和设备才有用

一个允许攻击者自由瞬移的防御谈不上纵深防御或塔防

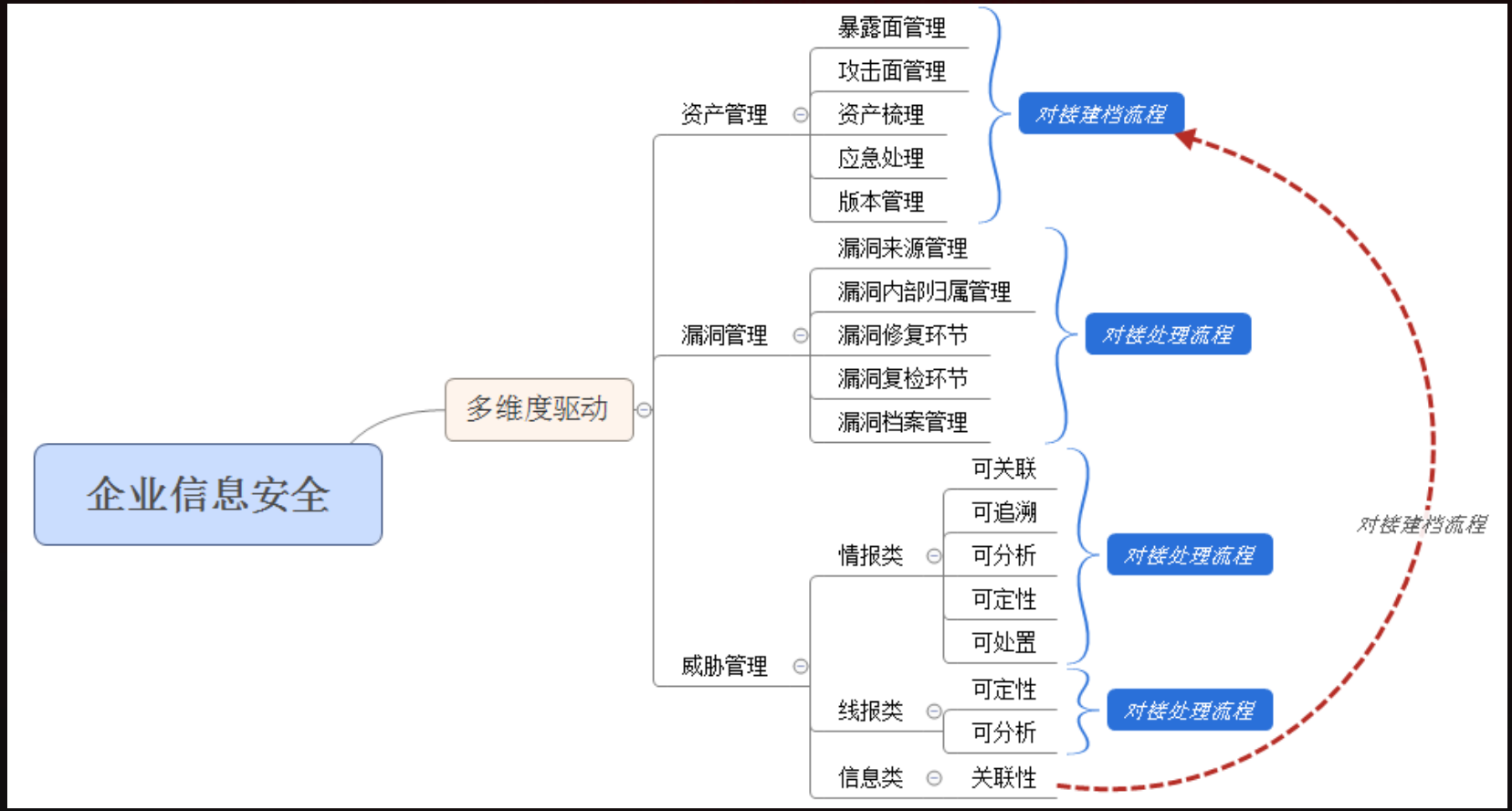
Part. 04

放点狠话，运维VS情报 谁将获胜？

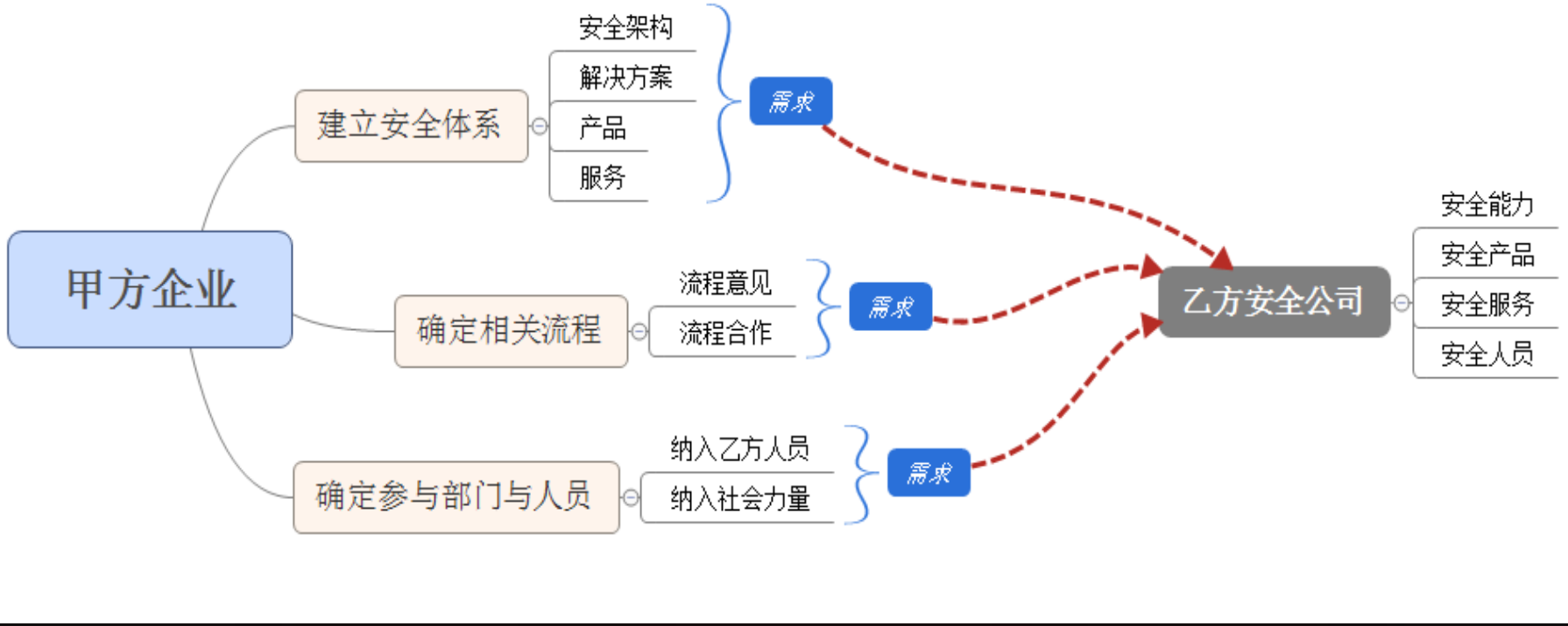
不对等的不仅仅是攻防，还有“甲乙”



不对等的不仅仅是攻防，还有“甲乙”

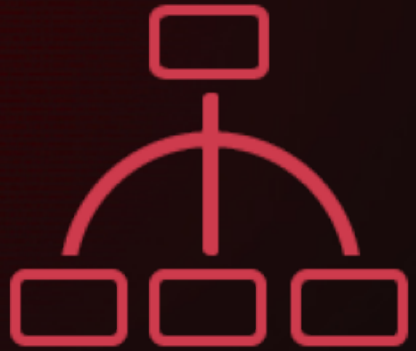


不对等的不仅仅是攻防，还有“甲乙”



说到产品和服务了，我们就看下

威胁情报



资产管理

就算结合产品与服务，结果依然很明显

Part. 05

来点笑话，总结下企业安全苦逼的事情

其实是个总结

1. 纵深防御在企业中是可行的，也是必要的，但要结合资产状况
2. 纵深是限制攻击线路的手法，而不是安全产品的堆叠
3. 威胁情报是有用的，但是要消化成至少在运维与研发侧能够落地的
4. 运维安全和安全运维是两码事，虽然都非常重要
5. 企业安全做再多事情，最后还是要量化和亮化

真实的笑话

不会写代码的运维进不了企业安全部

T H A N K S

[黑客叔叔p0tt1@凌晨网络科技]