打赢
企业信息安全
这场仗

A NEW WAR IS COMING SOON

距离开战仅剩0天0小时0分0秒

by：姚威（p0tt1）

关于我

凌晨网络科技

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

曾今，带领一支只知道挖漏洞和钻研最新攻击手法的团队，

后来，别人觉得可能攻防已经不对等了，有点“打女人”。

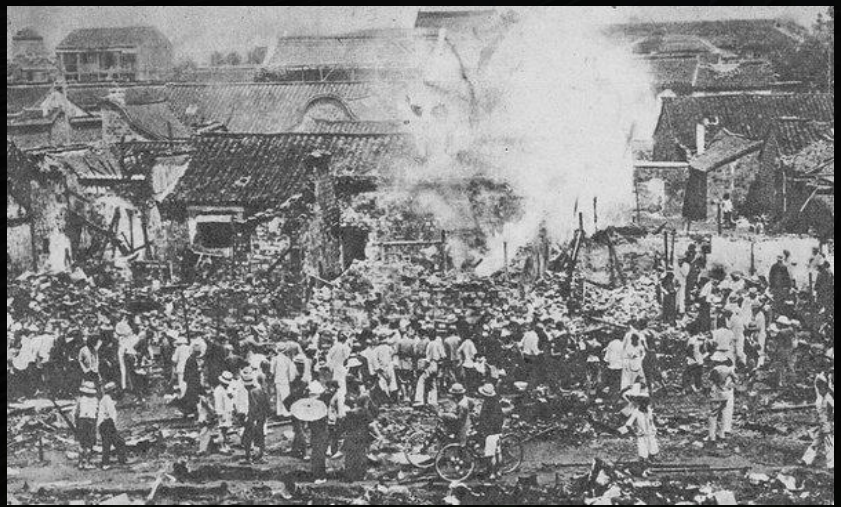
对企业安全，纯攻击思维能带来什么？幼稚？无知？

我们被问住了，然后高傲的“怂”了！

目录

曾经的我们 攻者无界

有种攻击叫“无差别 ”



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！

把威胁和漏洞，证明给你看！然后？

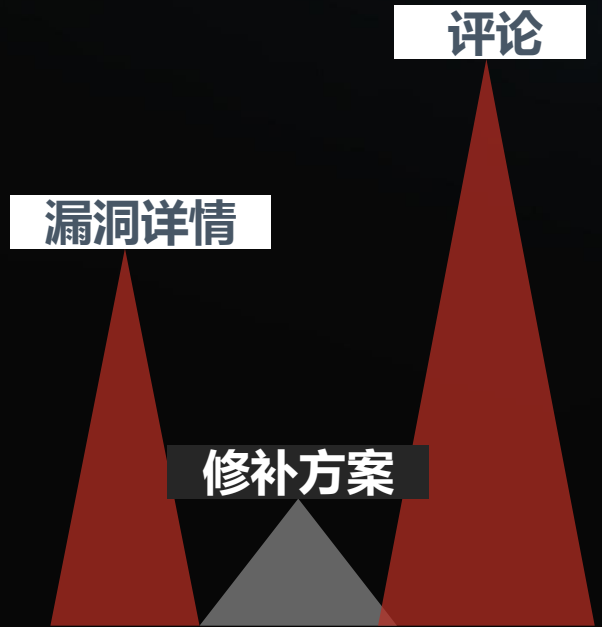
冷眼旁观

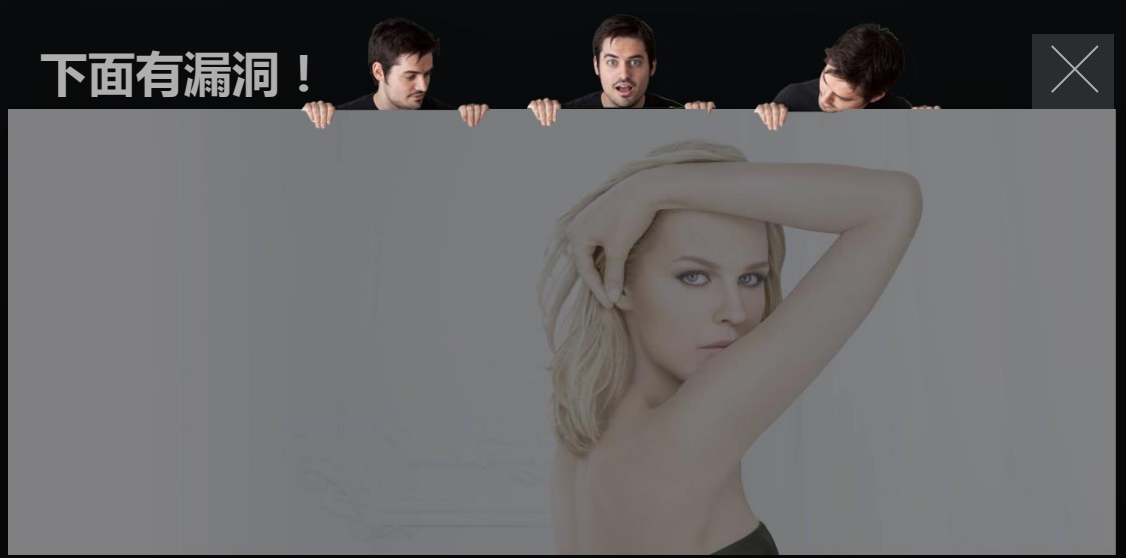
lěng yǎn páng guān

一个无聊的统计

我们找了各大漏洞平台和个人博客，将每个漏洞分成：漏洞详情，修补方案和评论三块！并统计图文长度！

然后发现比例是下图这样的：





我们究竟做了些什么？
有用的…… …

当时的
他们 措手不及


漏洞
泄露数据
舆论
嘴炮
勒索
撞库
代码泄露
业务风险
类APT
SRC
防火墙
安全能力
资产管理
自检扫描
等保
… …

请随意感受下企业负责防御的相关部门的心情

也谈测试

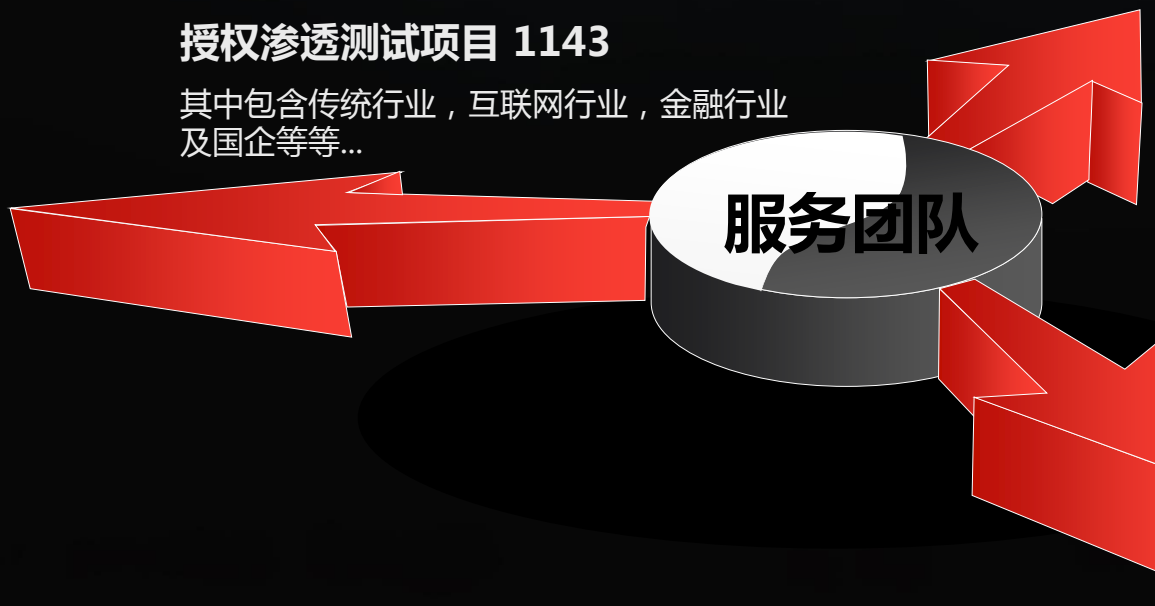
安全测试几乎和检查式扫描几乎占据了安全服务的半壁江山
然而我方团队统计的数据是这样的

高危漏洞数量3946个

其中不包含0day漏洞
只统计通用漏洞与Nday

授权渗透测试项目 1143

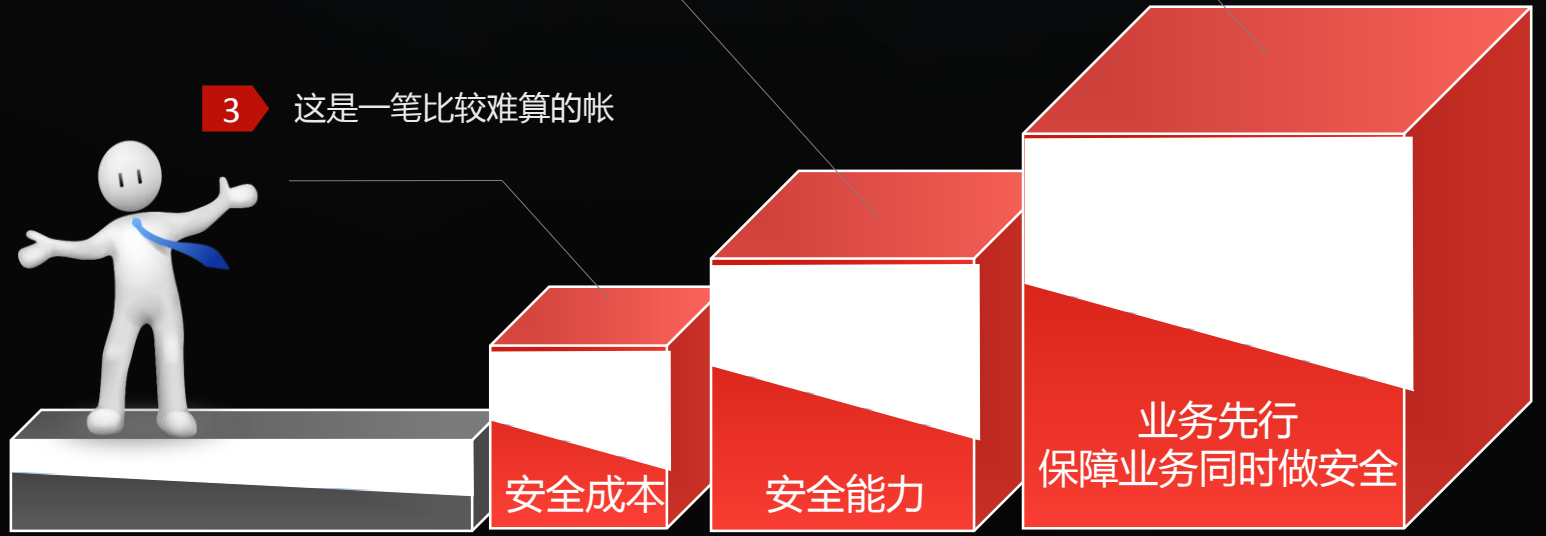
其中包含传统行业，互联网行业，金融行业
及国企等等...



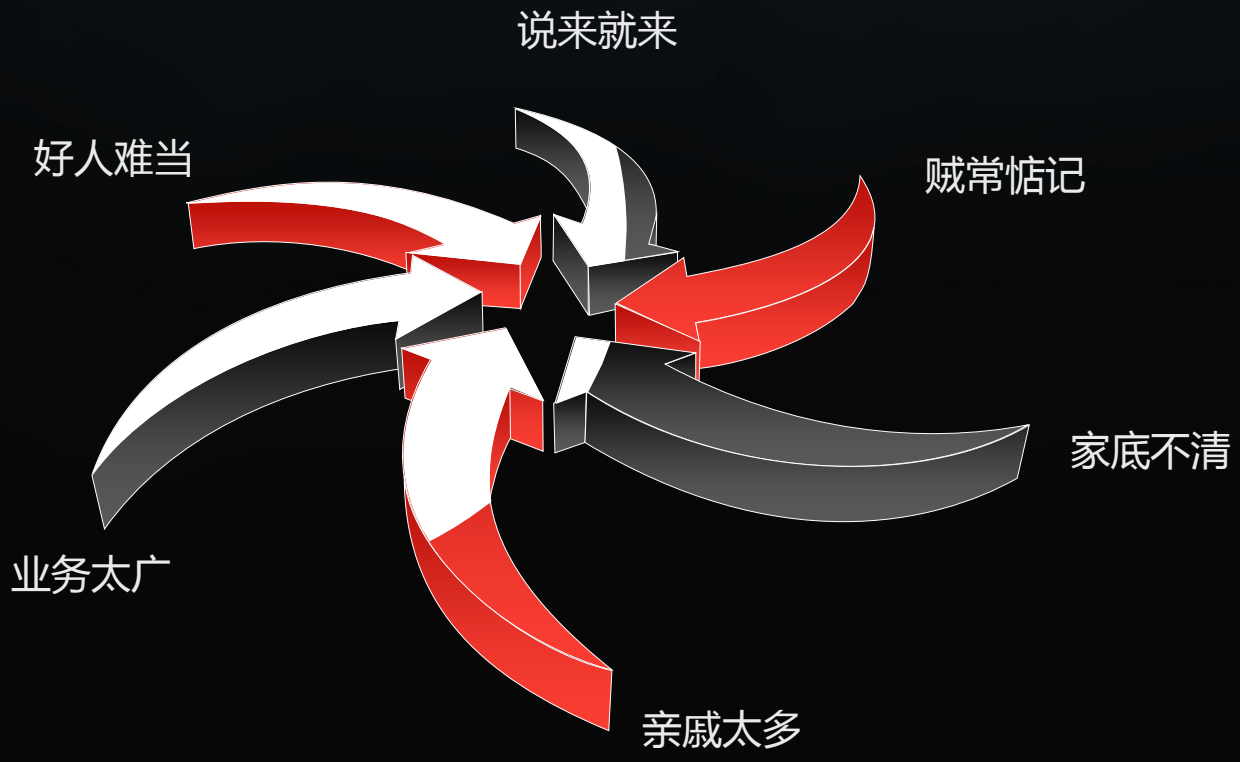
厂商三个月后修复率28.9%

何为措手不及

1. 安全的切入点：切得太深，不行；切得太狠，不行，切得太广，还是不行。
2. 有安全相关软硬件却不能代表安全能力的提升
3. 这是一笔比较难算的帐



为何措手不及

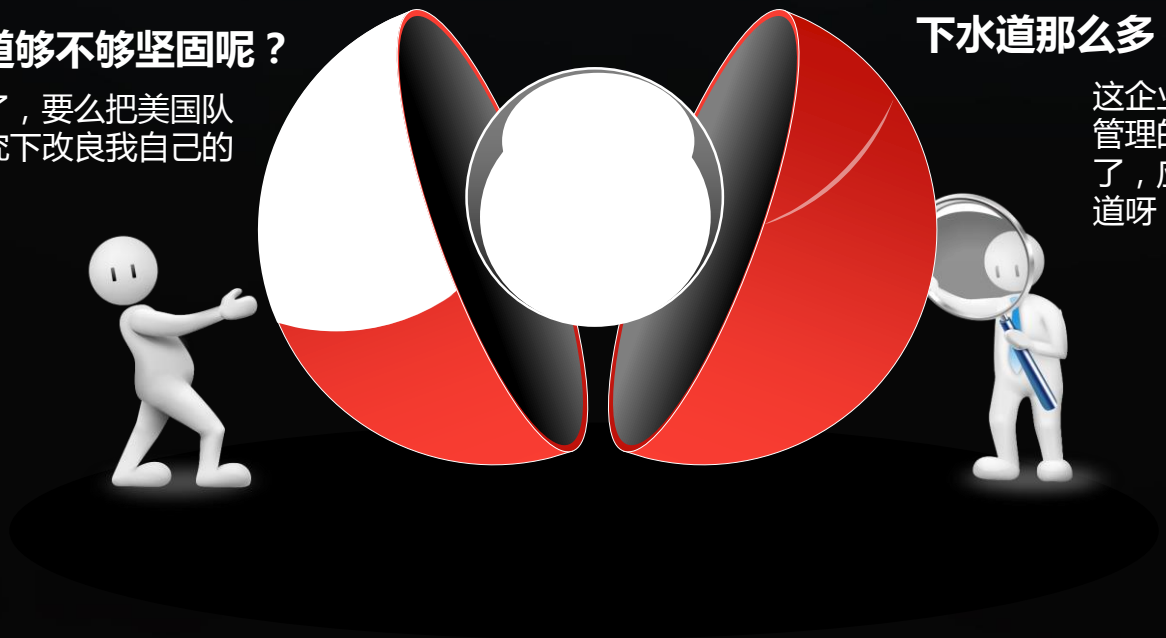


奇葩现象

原来表面上都在谈的一些高大上的 A B C
实际干起来都是南辕北辙的 3 6 9 ...

我的护盾不知道够不够坚固呢？

感觉已经挺厚实了，要么把美国队长的盾牌拿来研究下改良我自己的护盾？



下水道那么多，走那条才好呢？

这企业真二，下水道都不管理的么，宽度能开坦克了，应该填水泥！缩小管道呀！

注意：下面不是段子

还搞SRC呢，老板都不重视安全！

XXX公司程序员脑袋有坑！

XXX公司的洞这么久还不补！

XXX公司安全部门白养了都！

XXX公司的安全真弱智！so easy!

真希望你是我老板！

没坑都当黑客去了！

脑洞还没填平呢！再等等！

KPI每次都过关的好吗？

搞不定的时候你别挠头！

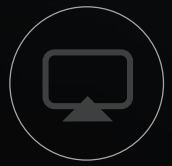
如今的
我们 欲披圣甲

战力天平处于劣势的防守方开始欲披圣甲
思考如何改变攻防的不对等

从毫无办法到千头万绪

也谈威胁情报

《Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression》



翻译版《用结构化威胁信息表达标准化网络威胁情报信息》

被引用在各类威胁情报产品中 全方位的场景契合

1.威胁分析。威胁的判断、分析、调查、保留记录等使用。

2.威胁特征分类。将威胁特征进行分类，以人工方式或自动化工具。

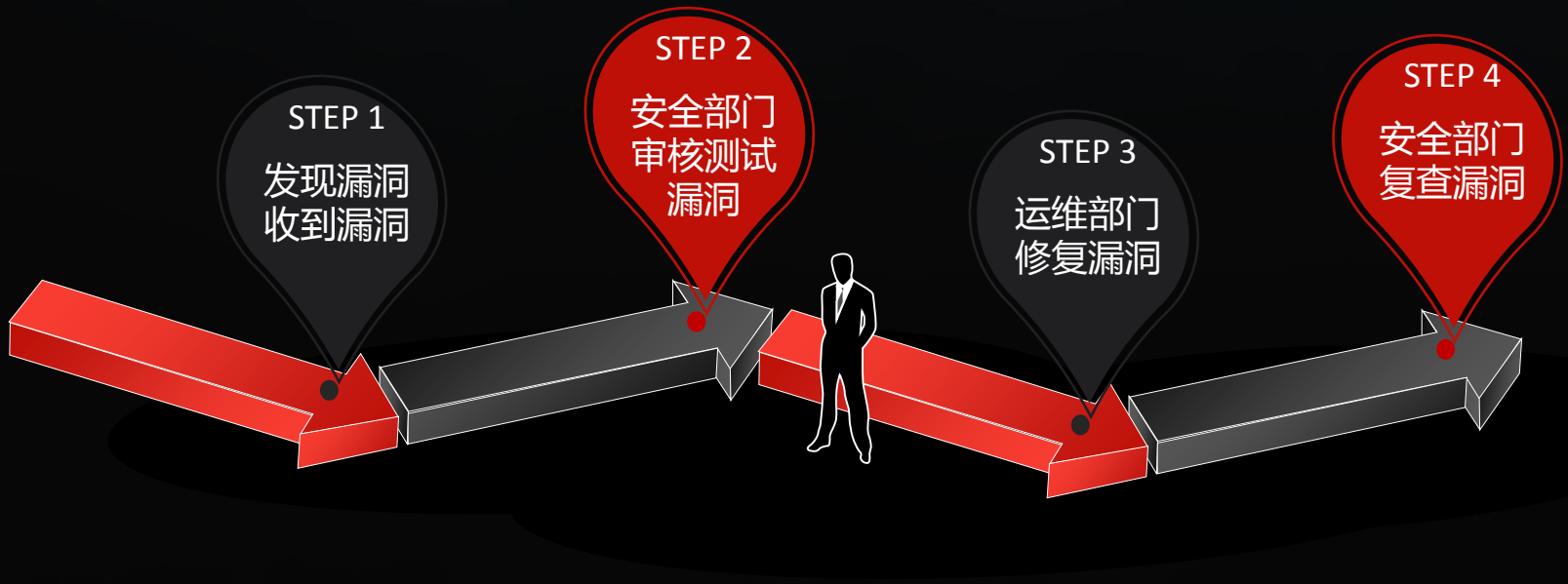
3.威胁及安全事件应急处理：安全事件的防范、侦测、处理、总结等，在安全事件处置过程中可以有很好的借鉴，以前做事件处理没有这么详尽的信息。

4. 威胁情报分享。用标准化的框架进行描述与分享。

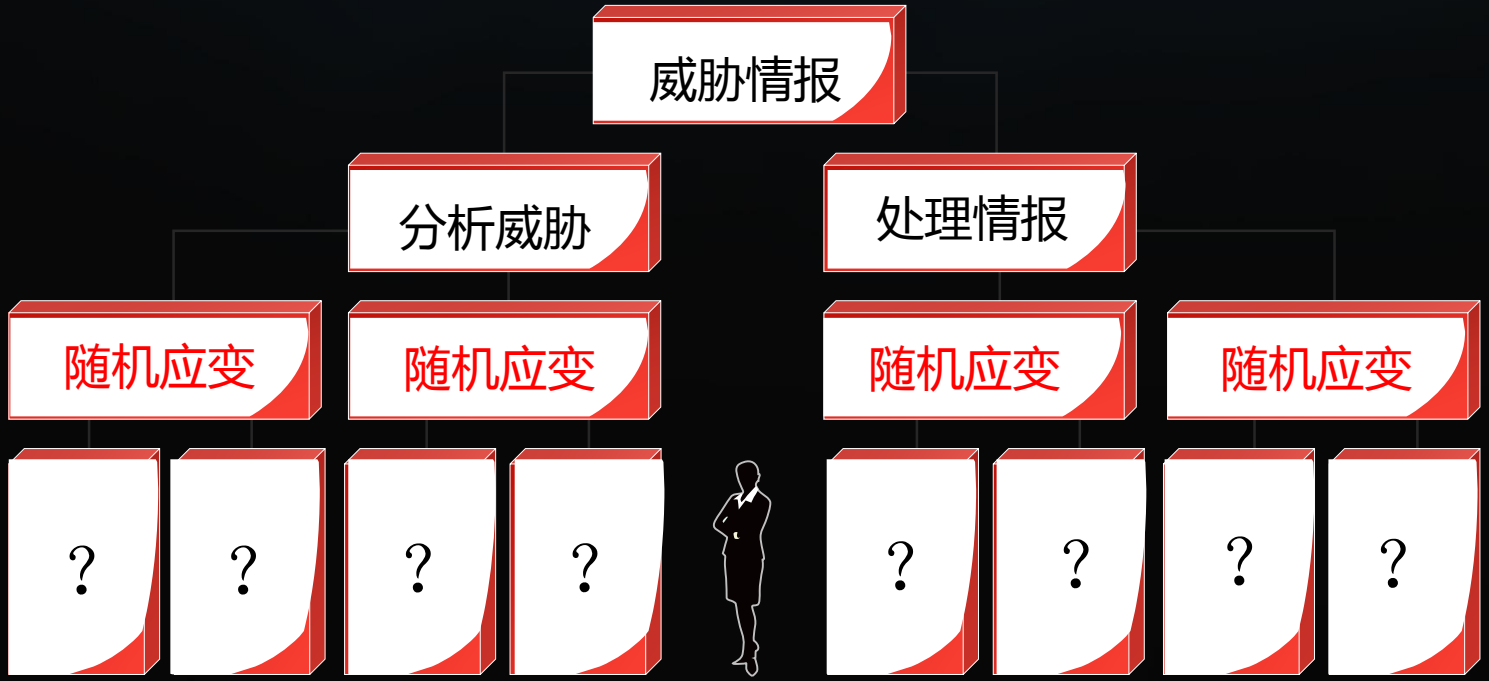
T.I

先看看企业针对漏洞

针对企业出现的相关安全漏洞，不停更迭出的“简单流程”



再看企业针对威胁情报



一个案例

这是一个非常有趣的例子，让我和我的团队思考了很久！

拿到某地下XSS平台的数据
发现数据中大量针对A企业的XSS攻击数据，且攻击成功，已知攻击者的攻击点，攻击手法，受害人列表。

向A企业提供威胁情报与相关证据

您提交的情报中：
1.出现问题的XSS漏洞已经一个月前修复了。
2.没有修复的一些攻击点，我们暂时还没有复现成功。
3.我们对您表示感谢。

其中的问题

情报能够复现？

为什么把重点放在了漏洞复现上？

XSS漏洞的特殊性

漏洞是修复了，可是用户cookie任然在被利用着，依然在刷新保持新鲜度。

受害范围与止损

那些受害者谁来管？怎么挽回损失？

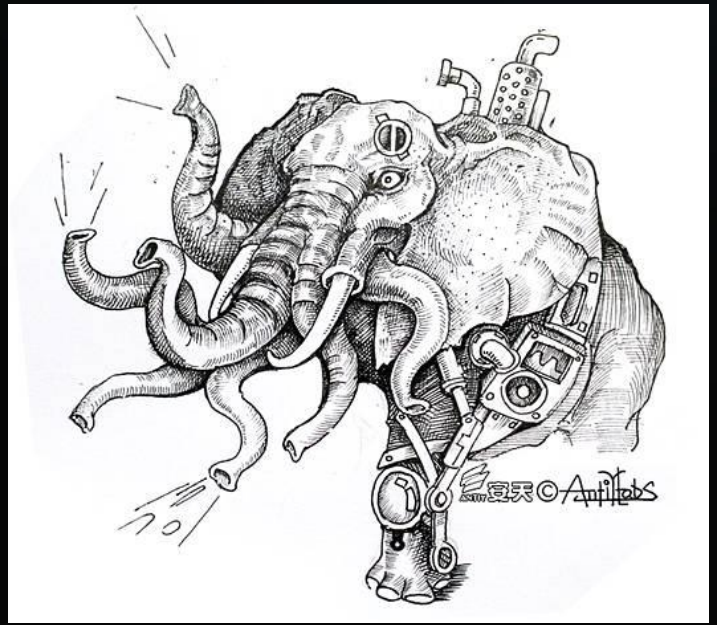
情报 OR 漏洞？

也许情报提供者与A企业都没搞清楚

欲披却还没披上的是黄金圣甲还是皇帝的新衣？

未来的他们 路在何方

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

企业安全角色

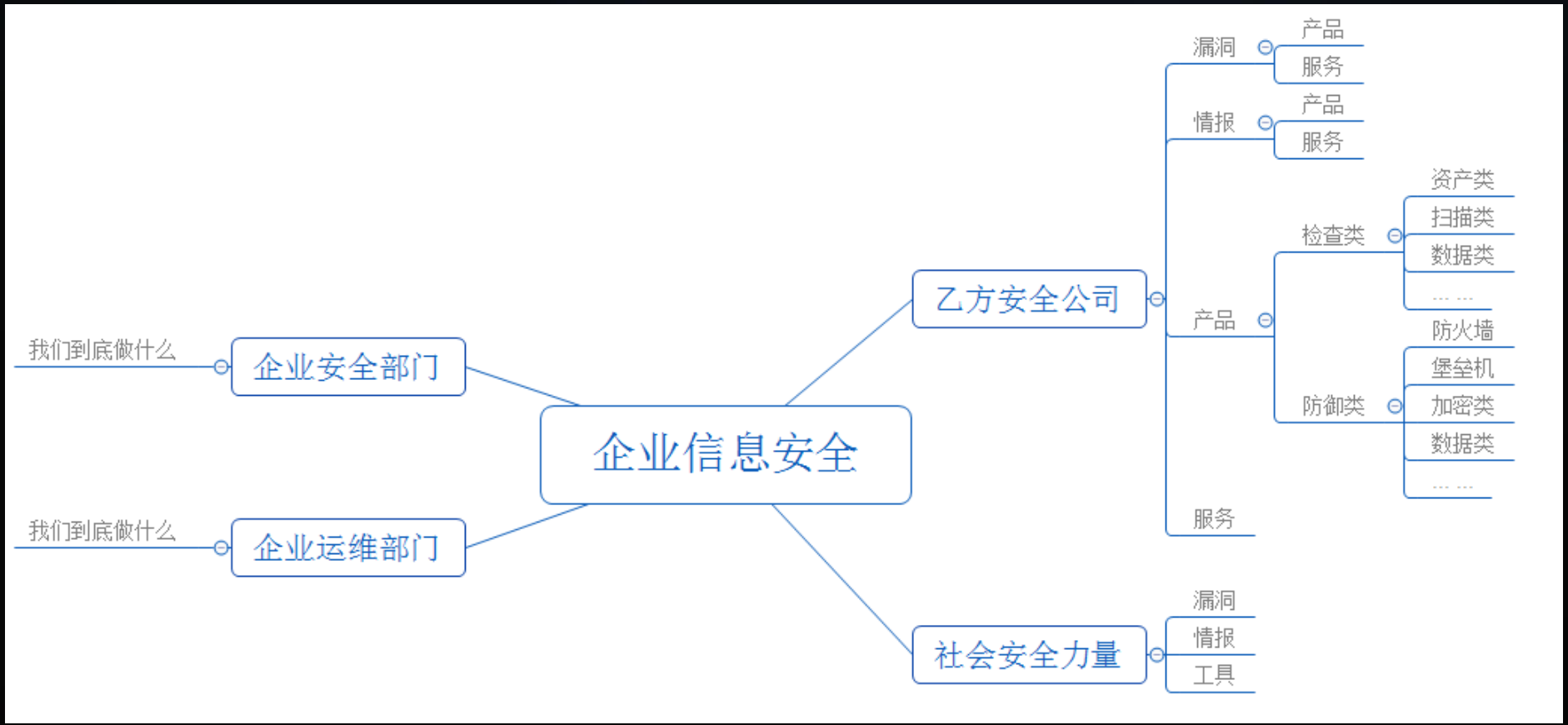
企业安全相关负责人

企业安全部门人员

企业运维人员

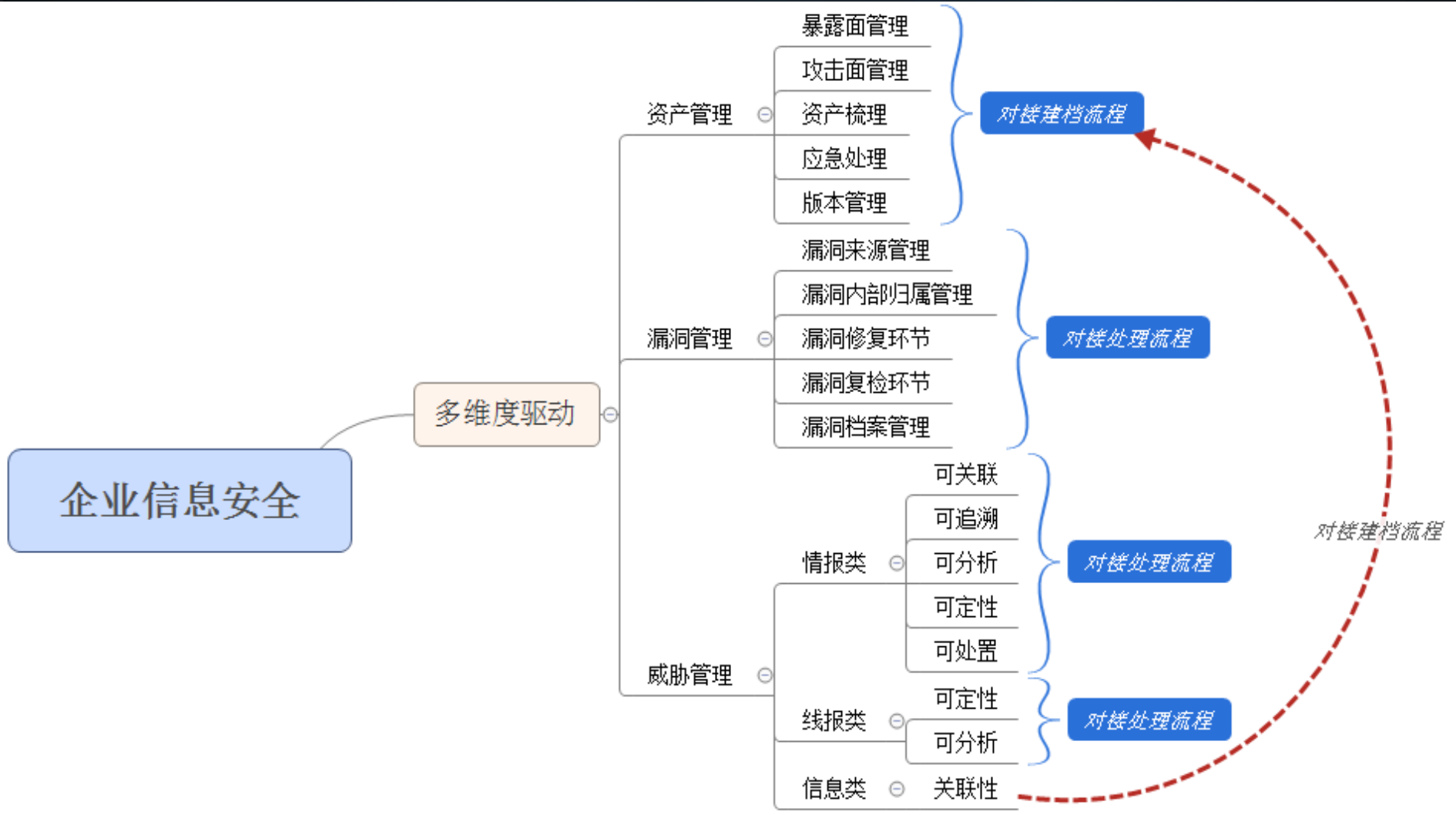
企业研发人员

现在我们做什么

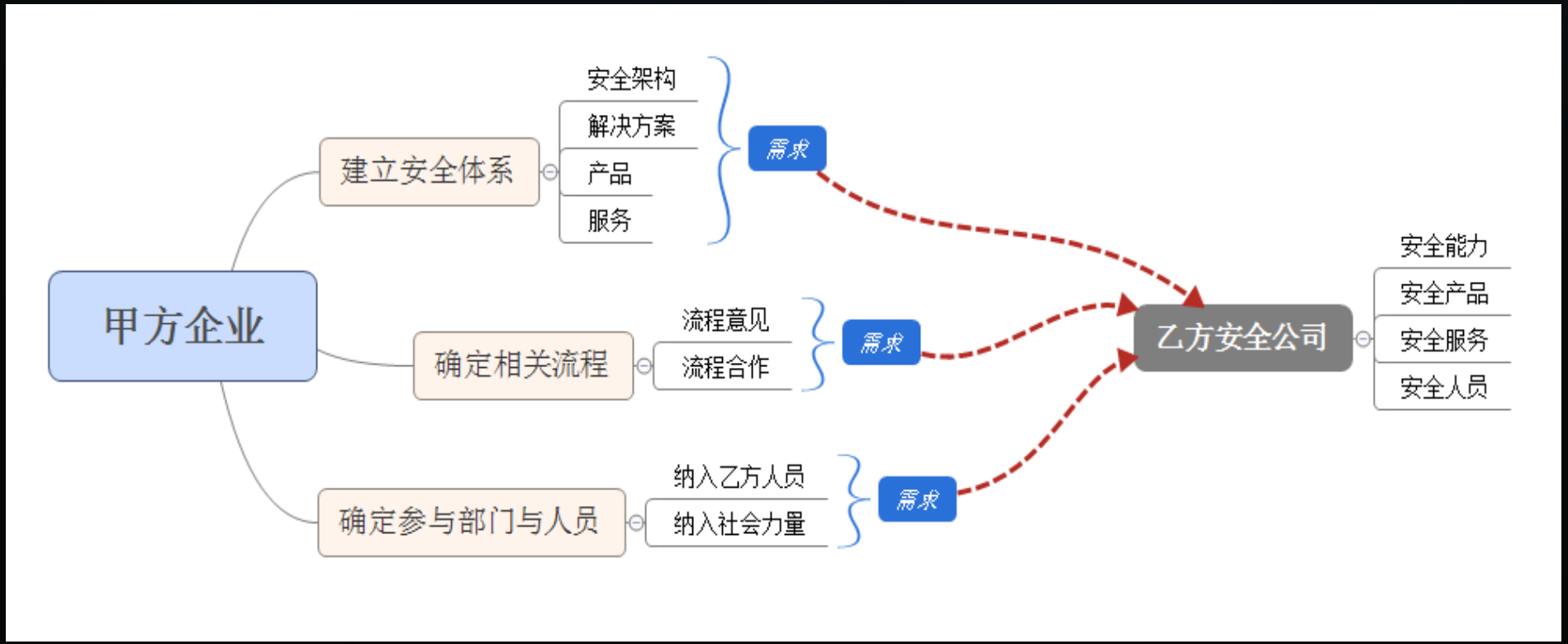

企业信息安全
企业安全部门
我们到底做什么
企业运维部门
我们到底做什么
乙方安全公司
漏洞
产品
服务
情报
产品
服务
产品
检查类
资产类
扫描类
数据类
... ...
防御类
防火墙
堡垒机
加密类
数据类
... ...
服务
社会安全力量
漏洞
情报
工具

多军种联动

抛开体系与产品，我们先聊聊流程与联动：


企业信息安全
多维度驱动
资产管理
暴露面管理
攻击面管理
资产梳理
应急处理
版本管理
对接建档流程
漏洞管理
漏洞来源管理
漏洞内部归属管理
漏洞修复环节
漏洞复检环节
漏洞档案管理
对接处理流程
威胁管理
情报类
可关联
可追溯
可分析
可定性
可处置
对接处理流程
线报类
可定性
可分析
对接处理流程
信息类
关联性
对接建档流程

看似简单的过程


甲方企业
建立安全体系
安全架构
解决方案
产品
服务
需求
确定相关流程
流程意见
流程合作
需求
确定参与部门与人员
纳入乙方人员
纳入社会力量
需求
乙方安全公司
安全能力
安全产品
安全服务
安全人员

打赢企业信息安全这场仗
其实很多
我们还没准备好

感谢你的参战

by:姚威(p0tt1)