



Mark.ma@tophant.com

# 从攻击者视角看待企业安全

马晨



# 提纲

近期安全事件

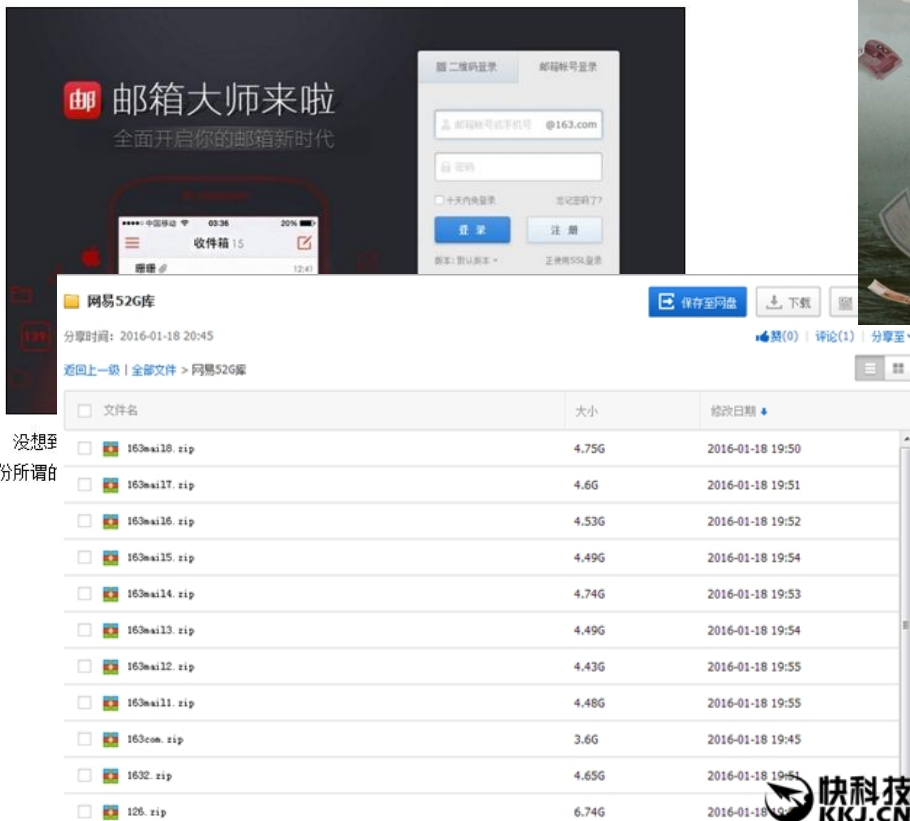
从攻击者视角看待安全

以资产为核心

## 52GB! 网曝网易邮箱数据全公开: 太恐怖了

2016. 03. 30 22: 47: 29 来源: 驱动之家 作者: 驱动之家 ( 2 条评论 )

去年10月份, 网络疯传网易163、126邮箱的多达5亿条用户数据被泄露, 乌云漏洞报告平台也给出了详细的报告, 但是网易官方坚决予以否认, 称绝对没有泄露。



邮箱大师来啦  
全面开启你的邮箱新时代

网易52G库

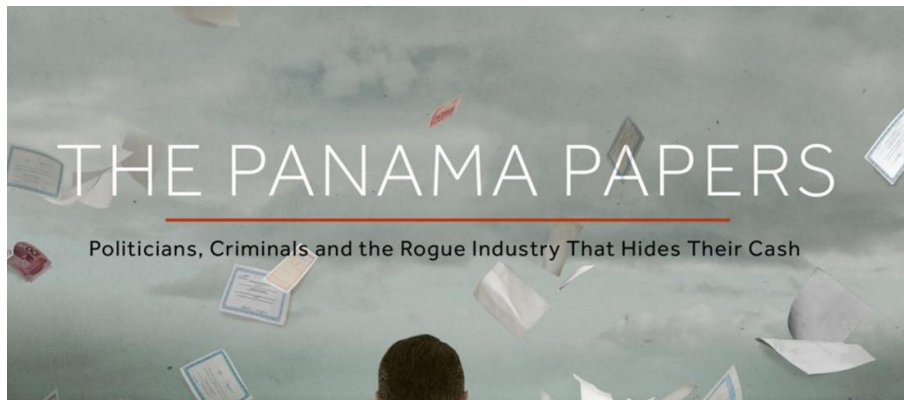
分享时间: 2016-01-18 20:45

返回上一级 | 全部文件 > 网易52G库

文件名	大小	修改日期
163mai18.zip	4.75G	2016-01-18 19:50
163mai17.zip	4.6G	2016-01-18 19:51
163mai16.zip	4.53G	2016-01-18 19:52
163mai15.zip	4.49G	2016-01-18 19:54
163mai14.zip	4.74G	2016-01-18 19:53
163mai13.zip	4.49G	2016-01-18 19:54
163mai12.zip	4.43G	2016-01-18 19:55
163mai11.zip	4.48G	2016-01-18 19:55
163com.zip	3.6G	2016-01-18 19:45
1632.zip	4.65G	2016-01-18 19:51
126.zip	6.74G	2016-01-18 19:51

没想到一份所谓的

快科技 KJKJ.CN



昨天晚上, 据HackerNews网站一则新闻披露, 土耳其国民信息数据库遭到泄露, 涉及 49,611,709位土耳其公民, 泄露出的信息包括每个人的身份证ID、姓名、父母亲姓名、性别、出生日期、出生地、身份证注册地址、居住地详细地址(直到门牌号)。

当我们这个世界正在熟睡之际, 地球的某一端又出事了, 昨天晚上, 土耳其全国国民底裤被扒了, 惨不忍睹。4900万土耳其国民信息泄露, 披露此信息的网站为http://185.100.87.XXX/, 内容很简单, 仅嘲笑了土耳其国民信息加密方法及保护措施的无能, 随后即放出了数据库下载链接给全世界。。。

## Turkish Citizenship Database

Who would have imagined that backwards ideologies, cronyism and rising religious extremism in Turkey would lead to a crumbling and vulnerable technical infrastructure?

This leak contains the following information for **49,611,709** Turkish citizens: (IN CLEARTEXT)

- National Identifier (TC Kimlik No)
- First Name
- Last Name
- Mother's First Name
- Father's First Name
- Gender
- City of Birth
- Date of Birth
- ID Registration City and District
- Full Address

## 最新互联网漏洞

[《互联网漏洞处理流程》](#)

全部

已公开

九斗鱼可获得任意帐号密码，登录任意帐号 **RMB**所属项目：[漏洞盒子挖洞联盟赛](#) 提交者：[ht17\\_in](#) 提交时间：2016-03-11[查看详情](#)网利宝可重置任意用户密码 **RMB**所属项目：[漏洞盒子挖洞联盟赛](#) 提交者：[匿名者](#) 提交时间：2016-03-10[查看详情](#)

## 中南林科大某站点 一处SQL注入 可远程桌面 导致服务器上 数十个站点沦陷并威胁内网安全

所属项目：[互联网漏洞与威胁情报](#) 提交者：[匿名者](#) 提交时间：2016-04-01[查看详情](#)

## 山西师范大学某分站服务器运维不当

所属项目：[互联网漏洞与威胁情报](#) 提交者：[红颜小妖](#) 提交时间：2016-04-01[查看详情](#)民生保险某处未经授权访问涉及千万级用户信息（含姓名、手机号、通讯地址等） **RMB**所属项目：[漏洞盒子挖洞联盟赛](#) 提交者：[匿名者](#) 提交时间：2016-03-27[查看详情](#)

## 民生保险某处存在SQL注入，可泄露大量数据

所属项目：[互联网漏洞与威胁情报](#) 提交者：[匿名者](#) 提交时间：2016-03-29[查看详情](#)

## 恒大人寿漏洞，服务器敏感信息泄露

所属项目：[互联网漏洞与威胁情报](#) 提交者：[匿名者](#) 提交时间：2016-03-26[查看详情](#)中国人民保险SQL注入之一大量保险订单信息 **RMB**所属项目：[漏洞盒子挖洞联盟赛](#) 提交者：[匿名者](#) 提交时间：2016-03-21[查看详情](#)中国人民保险保单遍历 **RMB**所属项目：[漏洞盒子挖洞联盟赛](#) 提交者：[匿名者](#) 提交时间：2016-03-19[查看详情](#)老百姓大药房某漏洞可导致千万数据泄漏 **RMB**所属项目：[互联网漏洞与威胁情报](#) 提交者：[匿名者](#) 提交时间：2016-04-01[查看详情](#)

做了这么多的合规、基线、补丁稽查，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？

视角不同！

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

# 攻防体系的不对称

---

技术层面：防御通常比攻击慢半拍

---

信息不对称：攻击者 > 安全人员

如：社工库、信息渠道获取&分享、社会工程学

---

攻击面：防护 - 需要考虑到方方面面

攻击 - 目标明确，有各种绕过防护的方法

---

经济角度：攻击 - 收益明确、主动性强

防御 - 工作被动、常抱有侥幸&懒惰心理

---



## 攻击者如何思考？以一个0-Day举例

及时获取最新的漏洞信息

抢占先机，实现漏洞利用

准确&快速

发现哪些IT资产存在漏洞

# Struts2-032, 0-Day集中式爆发一瞥

漏洞标题	风险级别	所属项目	发现日期	漏洞描述	危害	链接
某处struts漏洞	标记: struts2	高危	2016/4/26 12:45	江苏省运动会多struts2漏洞	高危	http://cvs.vulbox.com
存在struts-s2-032漏洞	高危	2016/4/26 14:00	西安米莱国际展览股份有限公司存在命令执行漏洞, 可获得权限, 上传文件	高危	http://cvs.vulbox.com	
struts2直播命令执行	标记: struts2	高危	2016/4/26 15:25	浙富基B2B系统存在漏洞任意命令执行可Getshell	高危	http://cvs.vulbox.com
存在struts远程执行命令	标记: struts2	高危	2016/4/26 15:25	中国人民大学某处命令执行漏洞大量学生信息	高危	http://cvs.vulbox.com
存在struts2S2032命令执行	标记: struts2	高危	2016/4/26 15:26	[Message收发系统存在SQL注入&amp;远程命令执行(无需登录)]	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 15:45	乐风汽车网某处命令执行漏洞=可getshell	高危	http://cvs.vulbox.com
目标存在struts2命令执行	标记: struts2	高危	2016/4/26 15:50	复旦大学某系统命令执行	高危	http://cvs.vulbox.com
存在struts2命令执行漏洞	标记: struts2	高危	2016/4/26 16:40	观众投票某处命令执行导致getshell影响238用户信息	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	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
网站存在struts2命令执行	标记: struts2	高危	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
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 18:05	船舶某系统命令执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 18:30	跨境电商某站存在命令执行	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 19:05	上海长途客运网存在struts2(s2-032) 远程命令执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 19:50	某通用eLearning系统s2032命令执行(命令回显POC和GETSHELL POC)	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 21:20	华为某处命令执行getshell	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 21:25	国研网某处命令执行getshell	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 21:25	国家工商总局某处命令执行	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 21:30	国研网某处命令执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 21:35	北京某处命令执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 21:35	国研网某处命令执行漏洞getshell	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 21:45	广东某处命令执行	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 21:45	船舶网某处命令执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 21:45	国研网某处命令执行漏洞getshell	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 21:45	某处命令执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 21:50	船舶网某处命令执行	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 21:55	恒生电子某处命令执行	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 21:55	渣打银行某处命令执行漏洞导致getshell	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:00	某处命令执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:10	华为网盘某处命令执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:10	国研网某处命令执行漏洞getshell	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:10	某处命令执行漏洞getshell	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:15	中国南方航空某处命令执行	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:15	某处命令执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:25	浙富基B2B系统存在Struts2 s2-032远程代码执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:25	船舶网某处命令执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:25	船舶网某处命令执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:25	成都中院某处命令执行在Struts2 s2-032远程代码执行	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:25	西藏自治区某处命令执行在struts2 s2-032命令执行漏洞, 可getshell	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:25	鞍山高新产业开发区存在Struts2 S2-032漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:25	华南理工大学分校Struts2 s2-032远程代码执行	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:25	青海省民族行政管理局存在Struts2 s2-032 漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	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
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:25	河南某处某处存在Struts2 s2-032 漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:30	福建省某处存在Struts2 s2-032远程代码执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	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
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 22:30	电子科技大学某处存在Struts2 s2-032漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 23:05	某处命令执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 23:15	科大某处命令执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 23:15	某处命令执行漏洞	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 23:15	某处命令执行漏洞导致getshell	高危	http://cvs.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 23:45	中国宝武某处存在Struts2 s2-032漏洞	高危	http://www.vulbox.com
网站存在struts2命令执行	标记: struts2	高危	2016/4/26 23:45	中国移动某平台存在struts2 s2-032命令执行漏洞	高危	http://www.vulbox.com

作为企业，如何快速有效的解决问题？

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

然而，道理都懂，说起来容易，做起来难。HOW?  
有安全预警渠道、哪些资产上存在漏洞、检测工具、修复方案？

以资产为核心

# 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

## 端口扫描/指纹识别

NMAP

ZMAP

MASSCAN

全网资产搜索引擎 (ZoomEye、SHODAN、Censys)

## 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

## 子域发现

## 关联IP

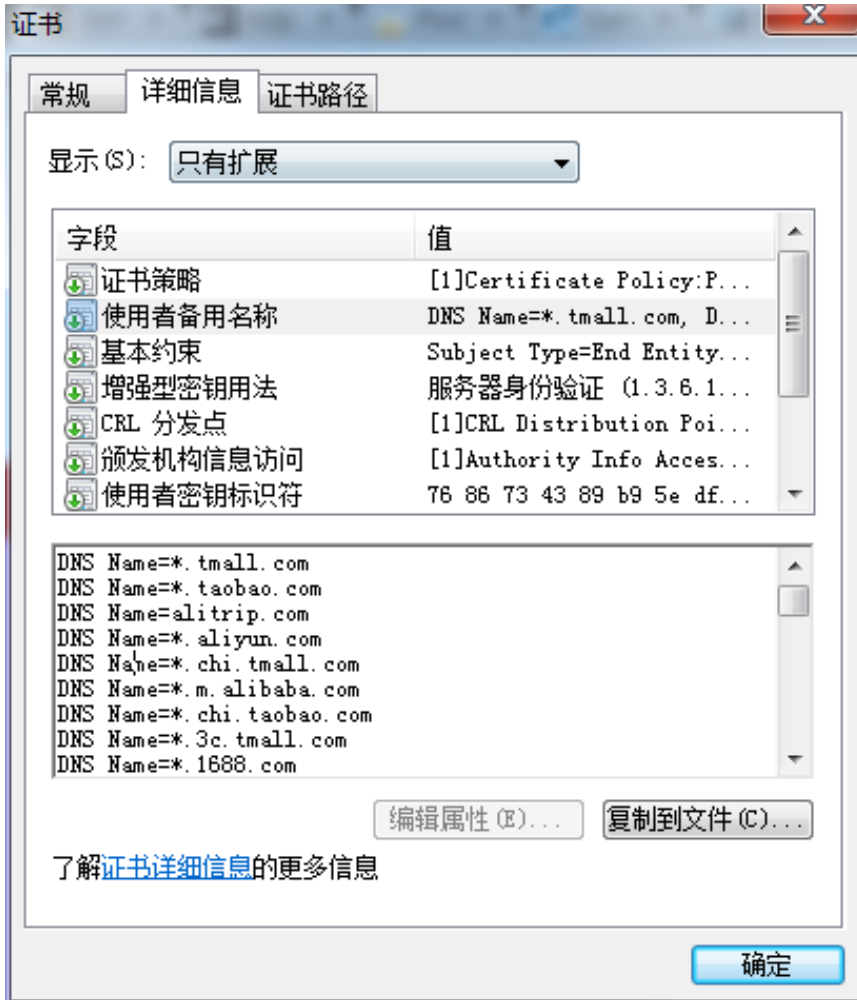
子域C段扩展

全网资产搜索引擎 (ZoomEye、SHODAN、Censys)

google hack

github hack





资产信任边界划分

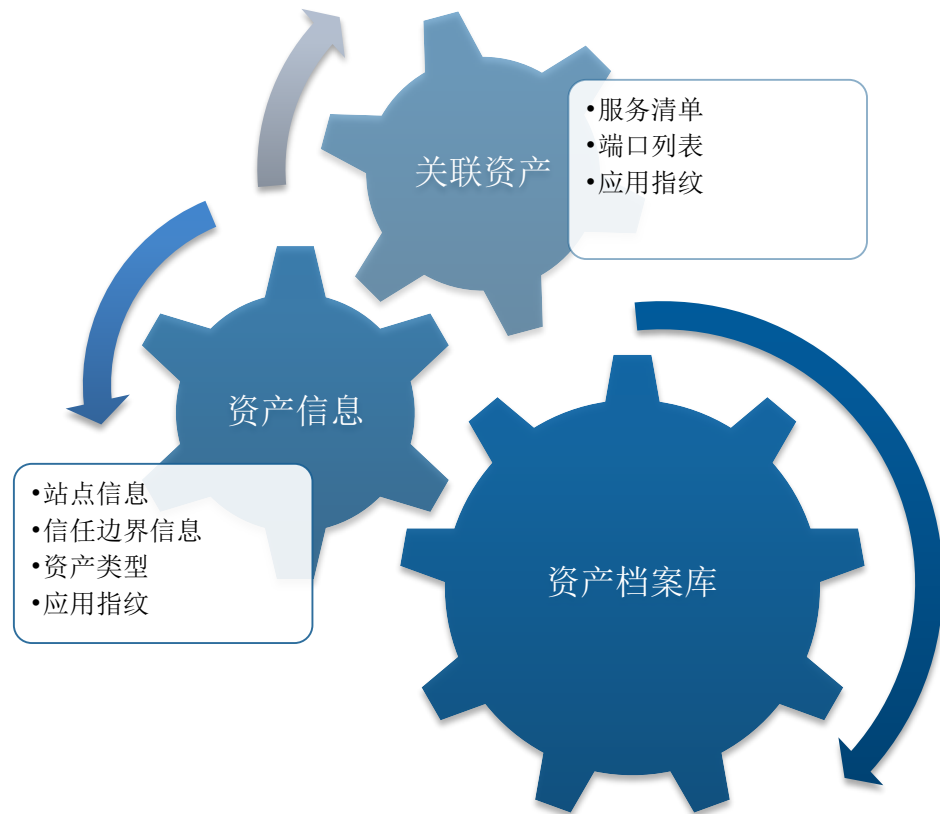


## 建立企业资产档案库/模型

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



## 回到主题，如何从攻击者视角降低0-Day带来的风险？

### 威胁情报功能

针对0-Day，第一时间提供最新安全漏洞预警

### 资产建模功能

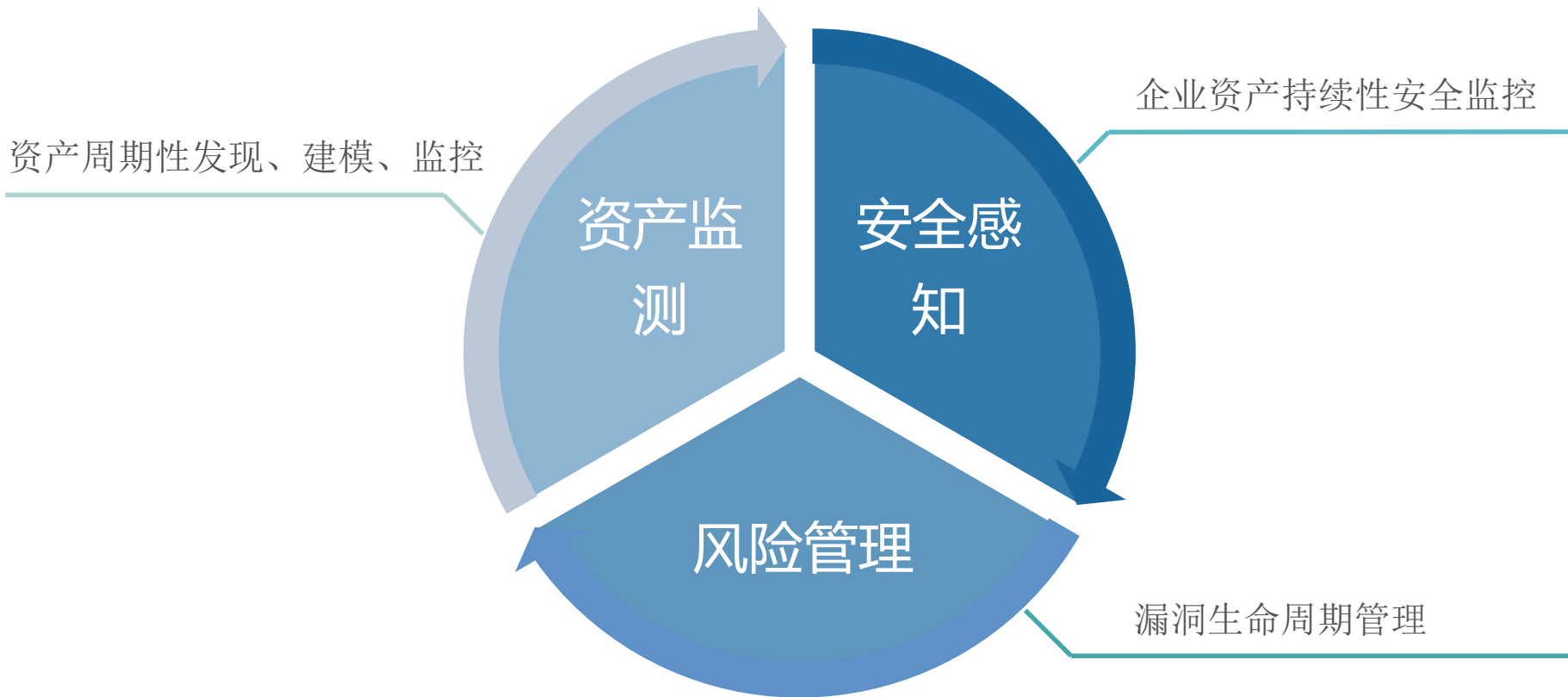
精确定位，哪些资产特征符合0-Day指纹信息

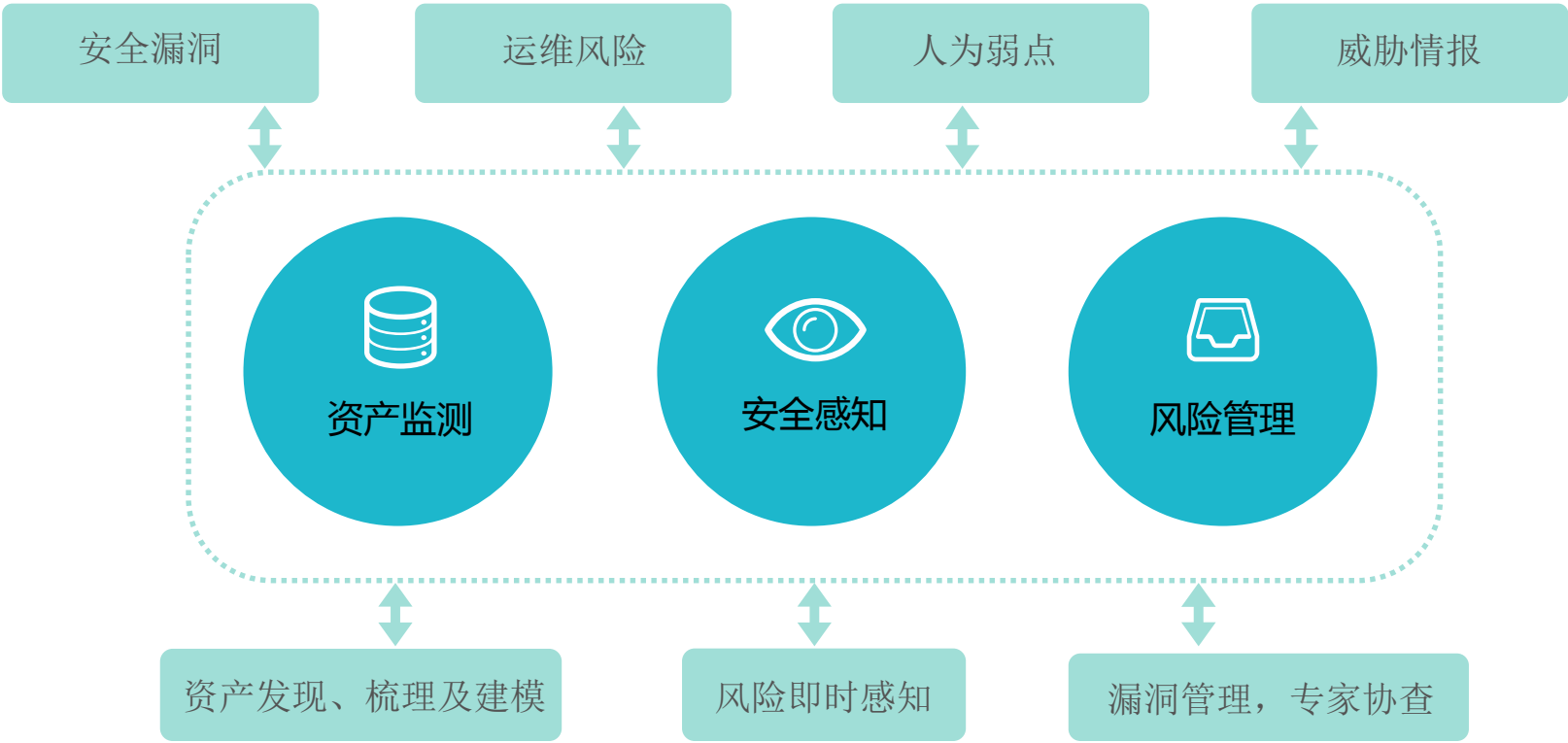
### 自动化检测 + 解决方案

快速自动化检测并提供完整的修复方案、专家协查



安全 = 监测 + 感知 + 管理







通过网藤SaaS引擎，对企业关联资产进行安全风险感知



## 安全风险

### 漏洞检测

全面的漏洞规则库：OWASP-TOP10、CVE、CNVD  
支持最新漏洞检测：漏洞盒子最新漏洞及0-Day高效转换

SQL注入、命令注入  
跨站脚本攻击-XSS  
失效的认证和会话管理  
不安全的直接对象引用  
跨站伪造请求-CSRF  
安全配置错误  
尚未验证的重定向和转发

### 运维风险

配置问题  
权限过大  
控制宽松  
内部端口对外  
弱口令  
敏感数据外泄  
开发后门

### 人为弱点

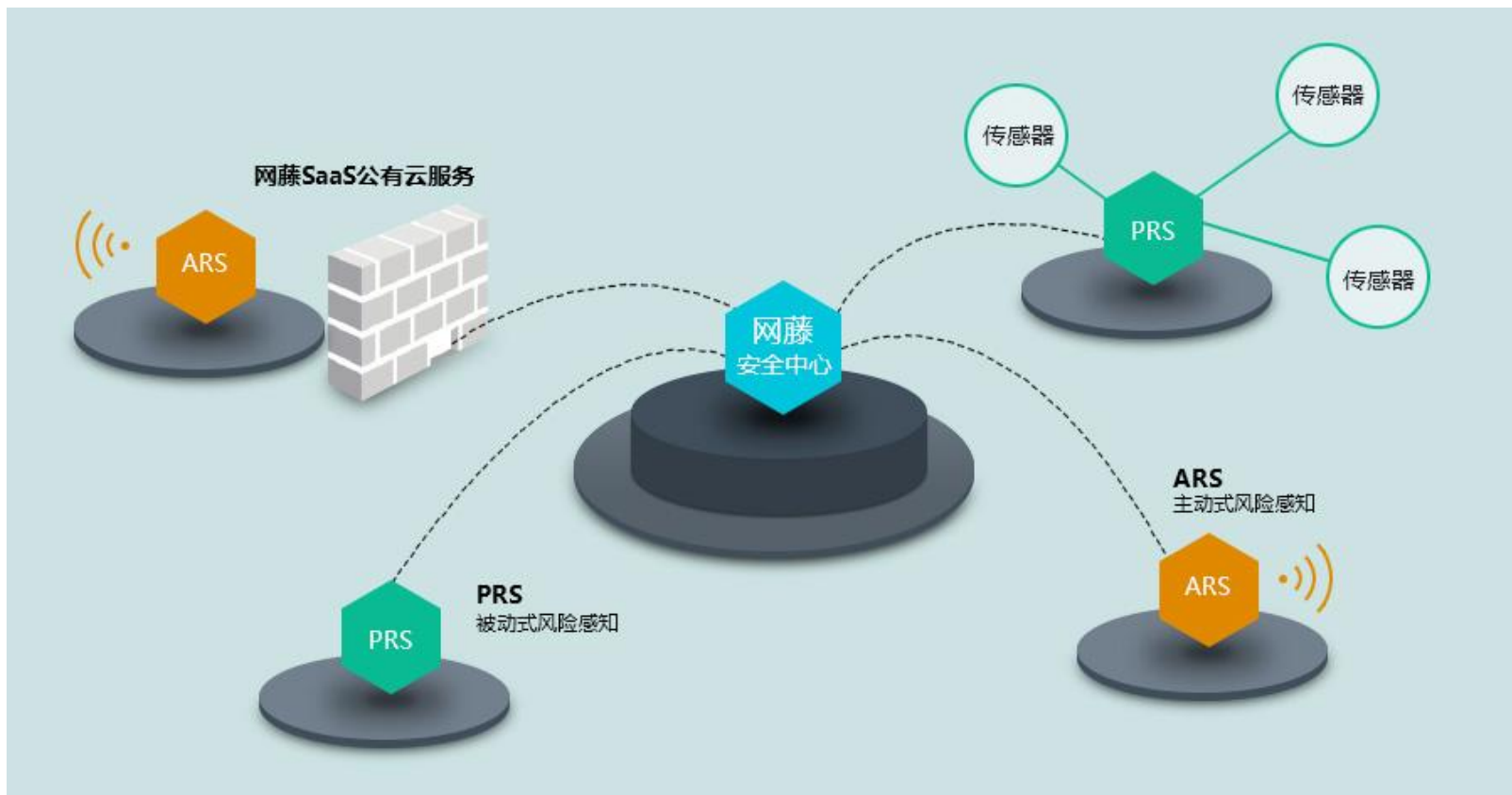
### 威胁情报

互联网漏洞平台  
全网数据侦查  
最新安全动态





# 网藤全方位解决方案



感谢聆听