技术 探索 创新

ITshare 分享会 | IT趣学社 让技术更有趣 | IT大咖说 知识分享平台

首席技术官应该考虑的网络安全问题

谭晓生—360 首席安全官

2017.9.15

没有攻不破的网络

范围扩大

- 互联网20年应用不断深入，从少数人上网->全民上网->智慧城市 / 智慧国家

漏洞万出

- 2016年，360补天漏洞平台就发现超过8万个漏洞

防不胜防

- 美国前网军司令基思·亚历山大，在2015年第三届ISC大会上发表观点：“世界上只有两类组织：一类是被黑了，另一类是不知道自己被黑了”

CSO与CISO

首席安全官（CSO）：负责整个机构的安全运行状态，既包括物理安全又包括数字信息安全。CSO负责监控、协调公司内部的安全工作，包括信息技术、人力资源、通信、合规性、设备管理以及其他组织，CSO还要负责制订安全措施和安全标准。CSO需要经常举办或参加相关领域的活动，如参与跟业务连续性、损失预防、诈骗预防和保护隐私等相关议题的活动。

首席信息安全官：即CISO，负责整个机构的安全策略。首席信息安全官需要经常要向CIO（首席信息官）汇报，有时甚至直接向CEO（首席执行官）进行汇报。

CSO与CISO即将成为标配

- 倪光南院士表示：“因为安全在很多情况下可以成为首要条件，根据安全需求，‘一票否决’或‘一票通过’都是很正常的。中国企业等单位还基本上没有设立CSO。我认为，有条件的单位不妨学习发达国家的经验，设立CSO，以便使网络安全、信息安全得到更好的保障。”
- 启明星辰创始人，CEO严望佳在另一个关于网络安全的提案中建议“在关键基础设施、敏感部门、政府机构中推行首席信息安全官制度。”

——————2015年全国两会报道，中国经济网

未来的世界，万物互联的世界

智慧城市

智能电网

智能家居

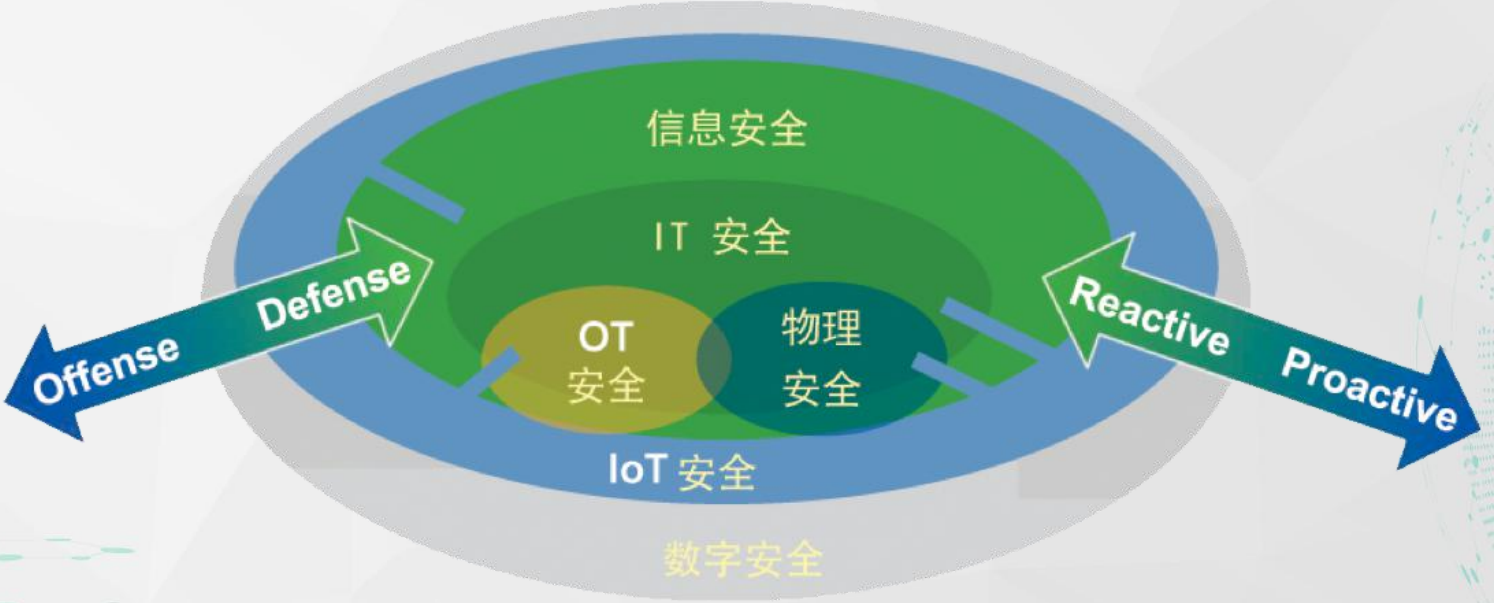
万物互联

车联网

智能工厂&制造

联网的可穿戴设备

数字安全的全景图



Gartner

敲诈者病毒处于“全修性流行病”级别

研究公司Osterman

2015年近**50%的美国公司**都经历过敲诈者病毒的攻击

趋势科技

CryptoWall系列的1个老版本就攫取到约**3.25亿美元**

美国国会众议院

好莱坞长老教会

旧金山公交售票系统

香港海事处

Facebook

印度三家银行

2016年被敲诈者病毒敲诈过的知名机构

IBM Security

2016年带有勒索软件的**垃圾邮件**数量同比增长了**6000%**，近**40%的垃圾信息**中都带有勒索软件

70%的商业用户受害者向黑客支付了赎金。其中，**50%**的支付额超过了**1万美元**，**20%**超过**4万美元**

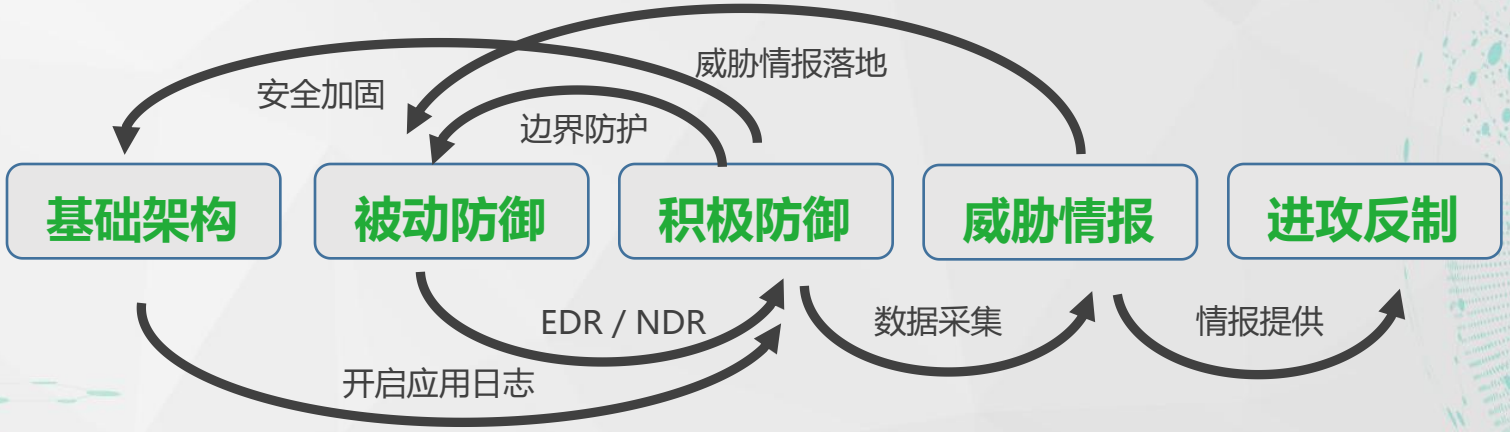
勒索软件业务规模有望达到**10亿美元**

近**40%**的个人消费者原意支付**100美元**以上来恢复数据，大部分勒索软件能从每位受害者手中勒索**300美元**以上赎金

超过**50%的父母**原意支付赎金来恢复个人照片

例：“永恒之蓝”病毒传播态势（中国）

不同阶段的关系：叠加演进，安全协同



注：EDR（Endpoint Detection & Response）：具备采集全量数据能力的终端安全软件，并以此开展安全检测与响应
注：NDR（Network Detection & Response）：具备采集全量数据能力的边界安全设备，并以此开展安全检测与响应

防御体系与防御思想的演化

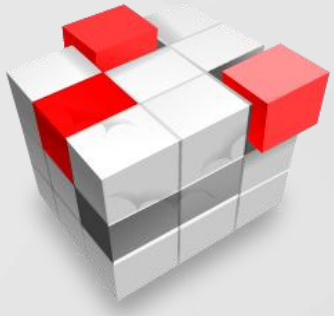
早期的P2DR安全模型

本质：安全就是响应+防护的安全运维体系

后来的安全木桶理论

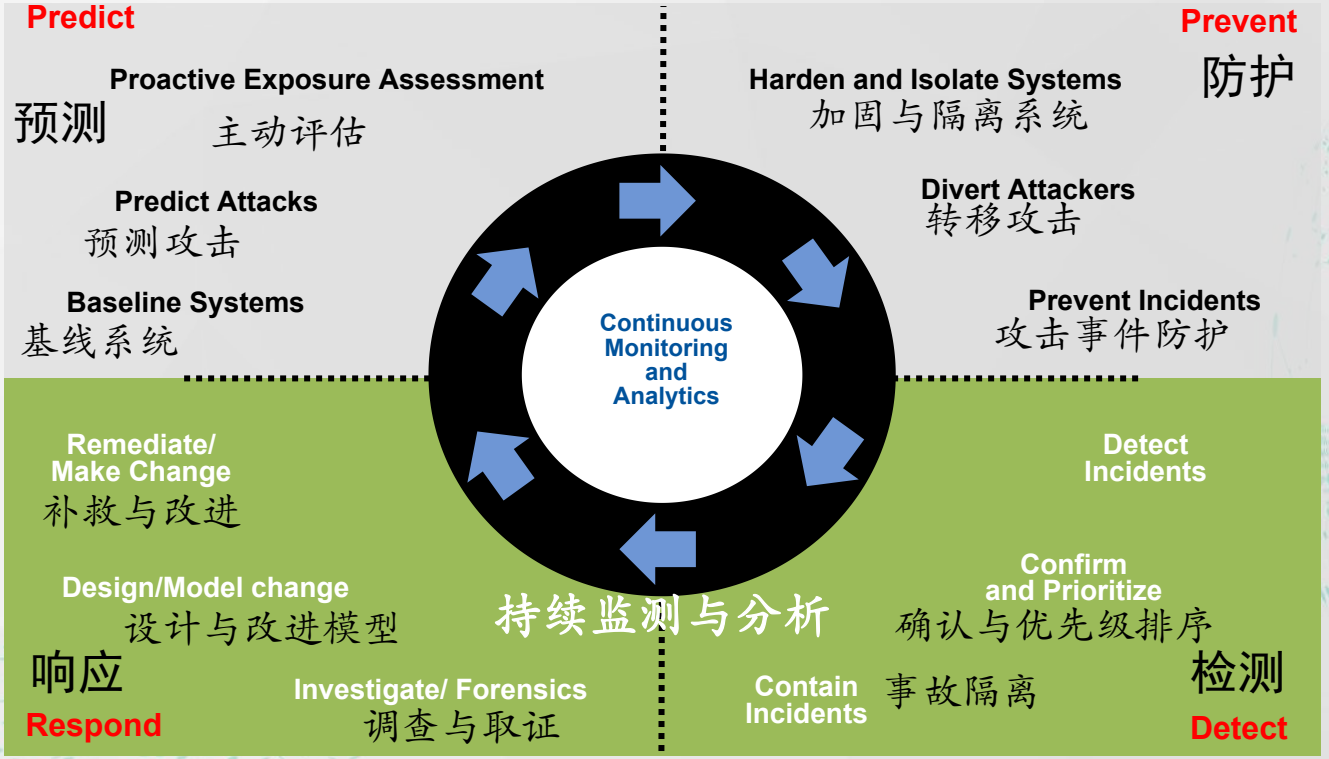
本质：安全就是用安全产品堆砌出来的线式防御体系

流行的立体防御体系

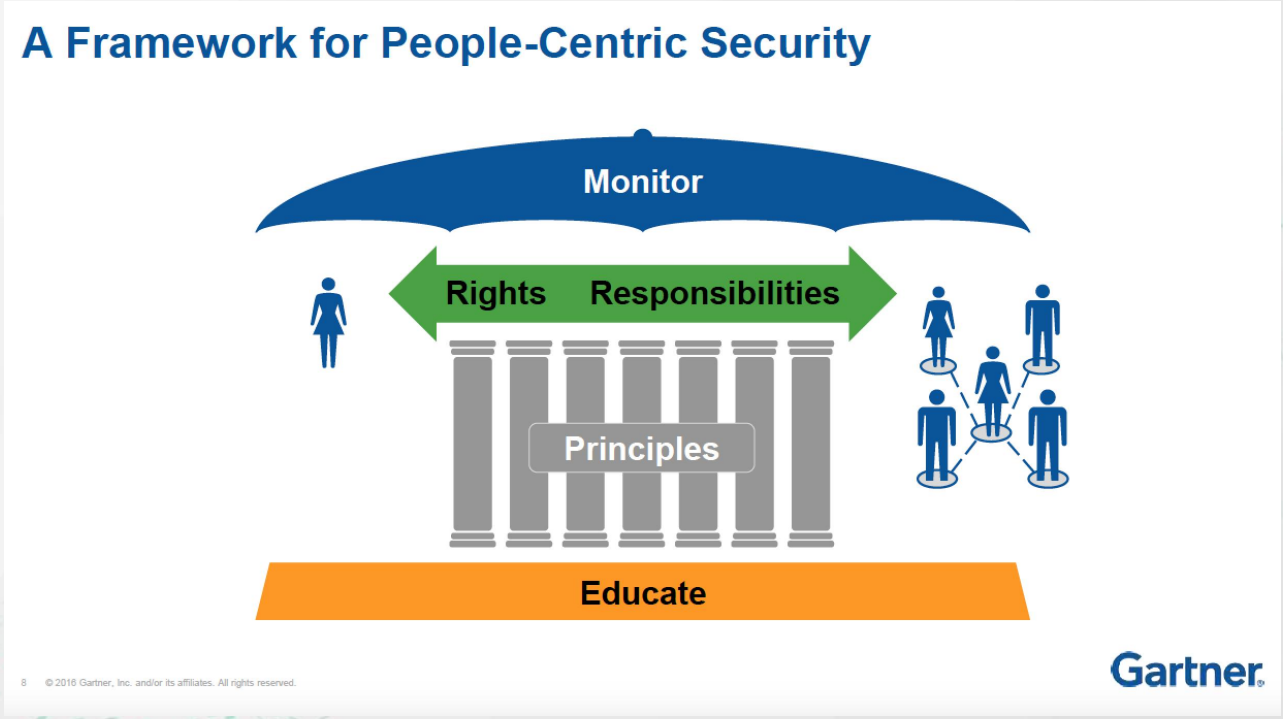


本质：安全就是分层的、分级的多层次防护体系

ADAPTIVE SECURITY模型



GARTNER 以人为中心的安全框架



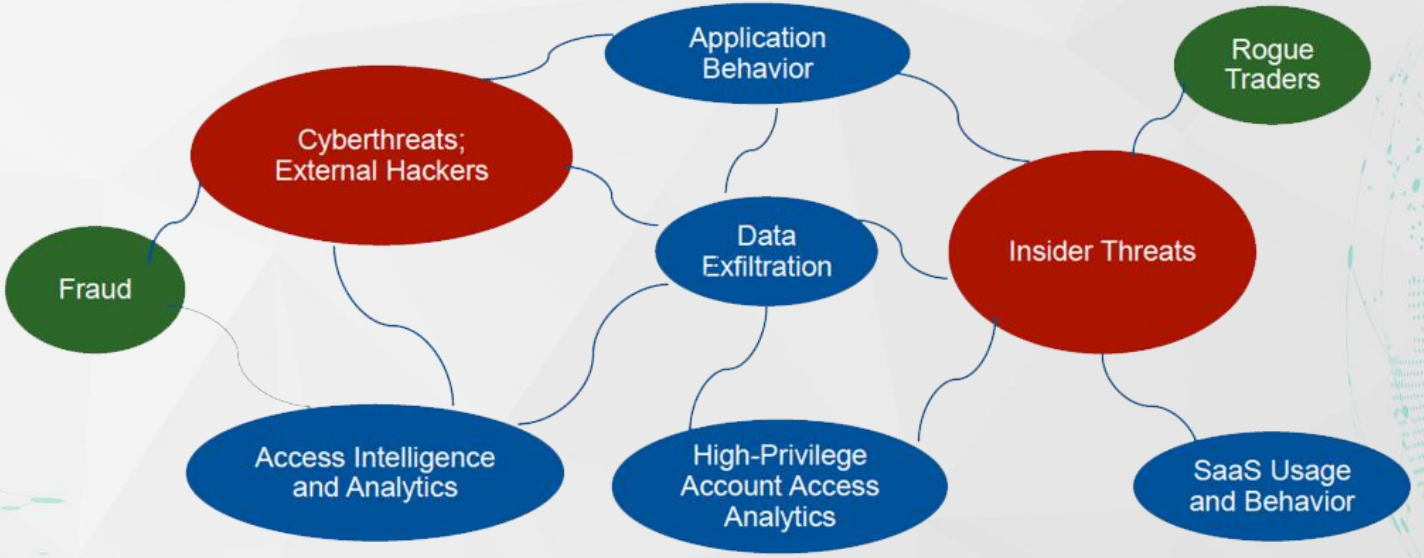
“安全产品”向“产品安全”的转变

- IOT产品安全
- 工业自动化系统安全
- SDL的价值
- 安全参照设计的价值
- 安全顾问咨询服务的价值

“数据防泄漏”的思路转变

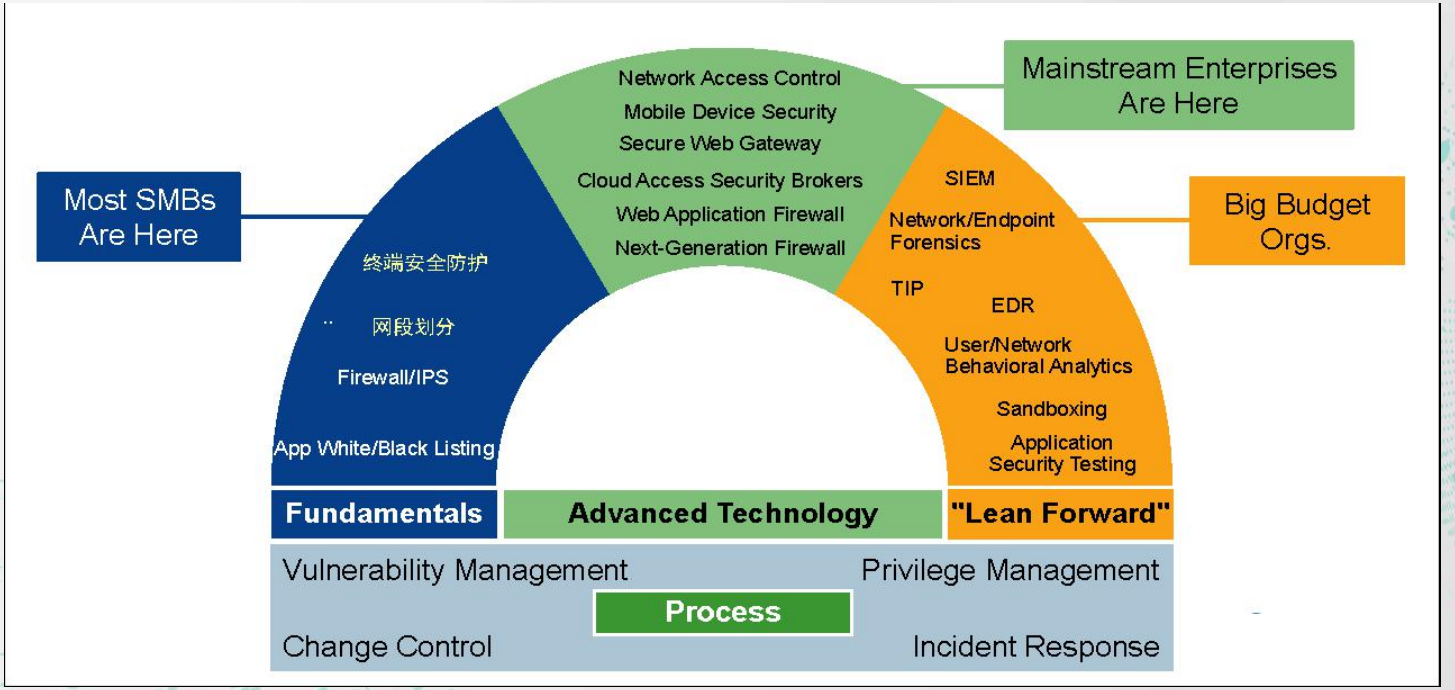
- 数据防泄漏是一项任务而不是一个系统 / 产品
- 数据加密 & 内容检测 & 数据流向监测

UEBA：用户与实体行为分析



Gartner

不同阶段的企业所采用的安全产品



那些最基础，但最起作用的工作

- 漏洞管理
- 网络隔离 / 网段划分
- 集中日志管理和分析
- 应用程序白名单
- 应用安全
- 身份与访问管理
- DNS过滤与监控
- 数据备份
- 系统加固
- 到位的系统管理

安全理念：一、二、三、四

安全理念：一个中心

办公网
十多个lan办公网络

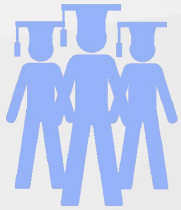
数据中心
八十多个数据中心

VPN 网络
随时接入

整体防护怎么做

安全理念：两个原则

攻防平衡原则

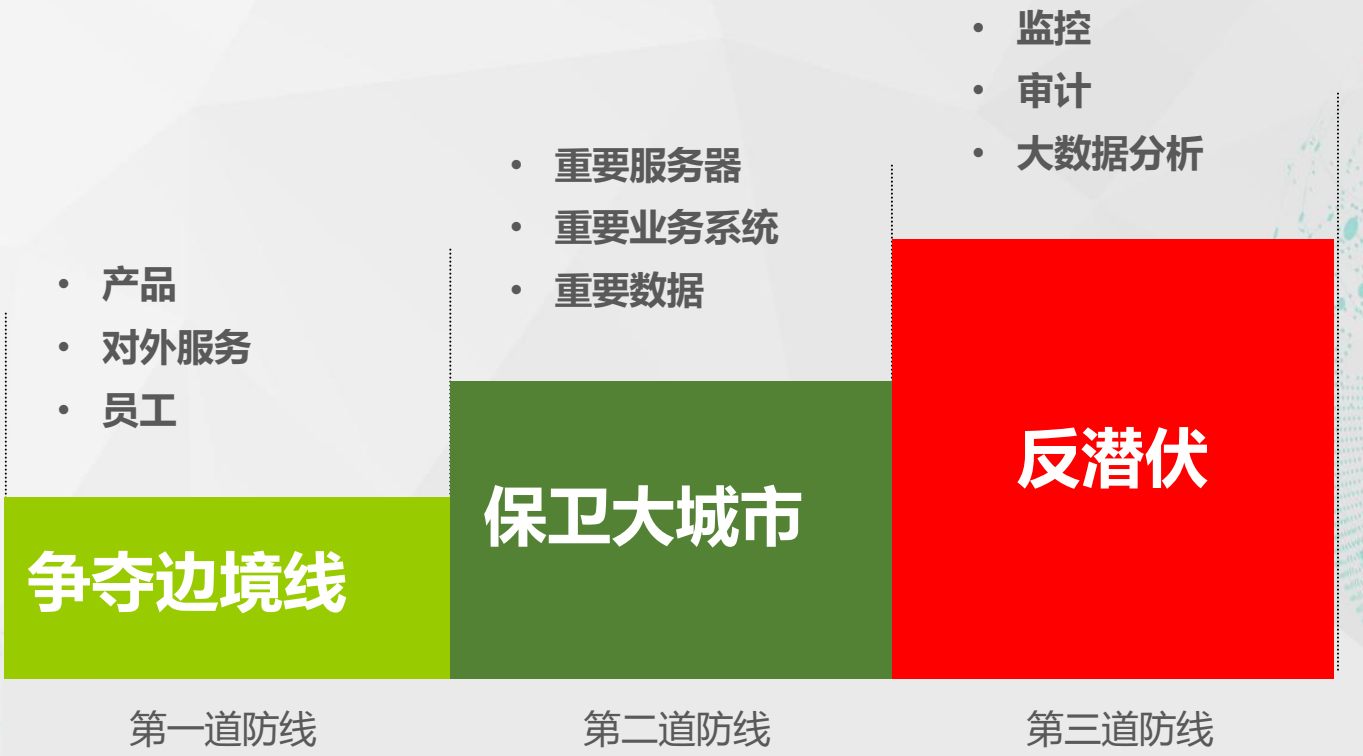


自主可控原则

- 现实社会中，攻防本质是成本的对抗；
- 防守就是在***受保护的目标价值***、***安全投入***、***性价比***三者之间做 **tradeoff**；
- 攻防之间是***动态的平衡***，攻击在不断变化，决定防守需要持续升级，否则将失去平衡。

- 真正的安全来自于可控的安全团队加上可控的安全工具；
- 一手抓安全防护；
- 一手抓安全工具的自主开发。

安全理念：三个阵地



安全理念：四个假设

A

- 如何发现漏洞利用行为
- 如何检测攻击行为

系统一定有未发现的漏洞

C

- 如何发现系统已经被渗透
- 如何处理已经被渗透的漏洞
- 如果重现攻击过程
- 如何溯源

系统已经被渗透

B

- 及时发现漏洞
- 强制修补漏洞

一定有已发现但仍未修补的漏洞

D

- 如何发现员工的异常行为
- 如何检测并阻断来自内部的攻击

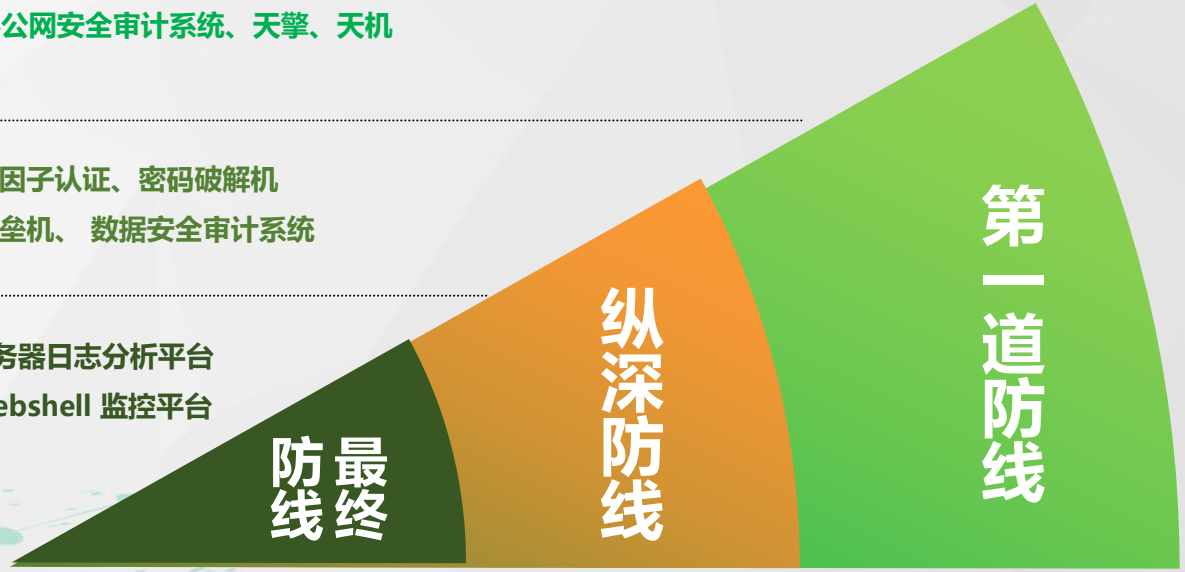
员工并不可靠

安全防护技术体系

- 网络访问控制统一管理平台
- 天眼威胁感知系统、无线入侵检测与防护系统
- Web安全扫描系统 、Webshell白盒扫描系统、 Andriod漏洞半自动化扫描系统
- 安全扫描系统、第三方安全漏洞监测系统
- 办公网安全审计系统、天擎、天机

- 双因子认证、密码破解机
- 堡垒机、 数据安全审计系统

- 服务器日志分析平台
- Webshell 监控平台



360信息安全部

日常工作	攻防类：安全测试、方案评估、产品研发、应急处理 产品类：设计、开发、运营、应急处理

ITshare 分享会　IT趣学社 让技术更有趣　IT大咖说 知识分享平台

CTDC
首席技术官领袖峰会

后会有期

2018.9.8

+ 乌镇再聚 +

更高规格、更优质的服务，只为更好的遇见你！