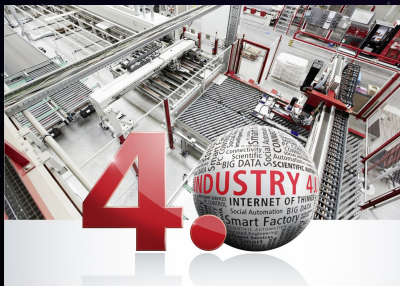
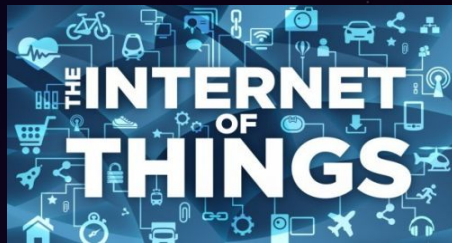


# 企业安全之威胁态势感知

演讲者：谭晓生

360副总裁

# 2015年的IT热点



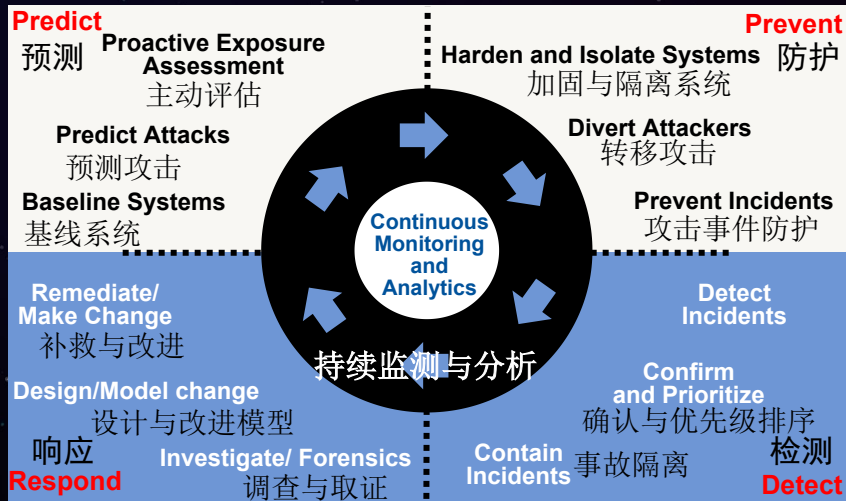
“攻击面”快速扩大，安全人员不够用

“安全生产”中的安全需要得到重新的诠释

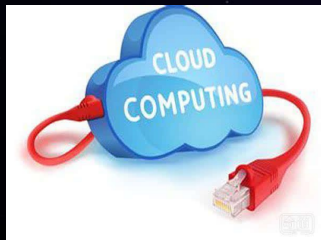
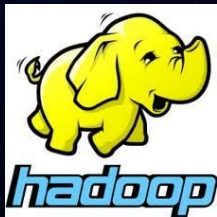
云计算的安全问题

IoT安全，已关乎人身安全，如何防护？

# 由“防护”到“检测”的转变



# 我们的“马克沁机枪”

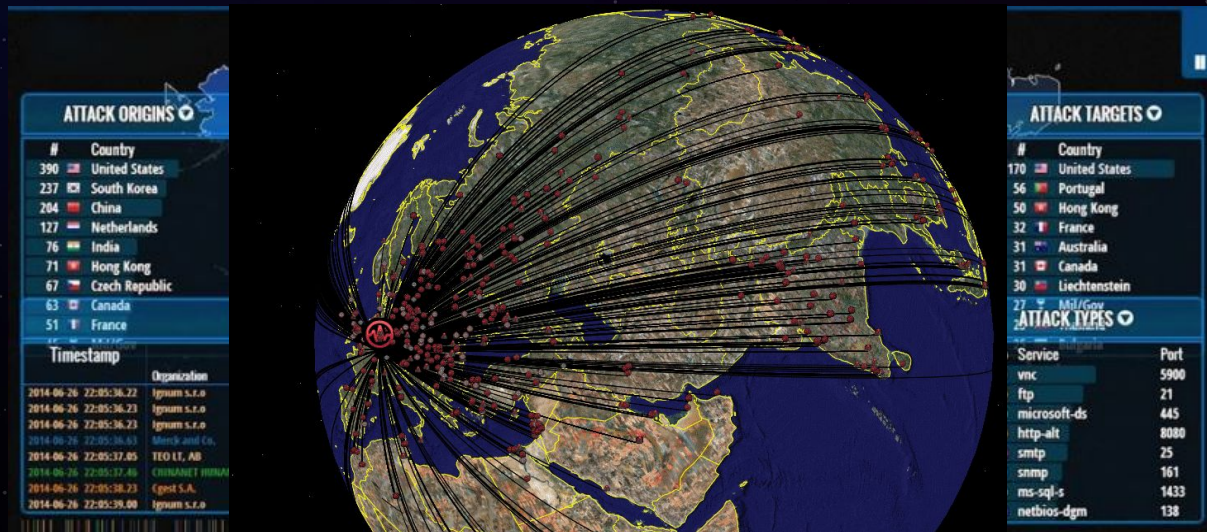


# 完成“攻击拼图”





# 安全态势感知的几个误区

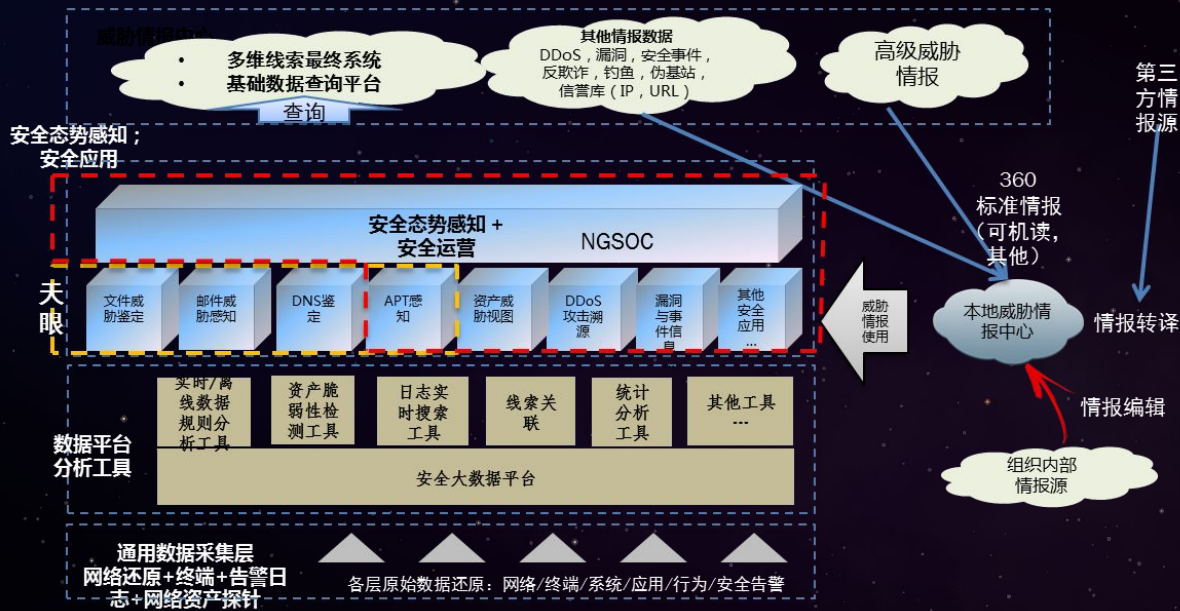


# 安全态势感知的几个误区





# 360安全态势感知



# 360安全态势感知

## 天眼未知威胁感知系统

- App1: 未知威胁感知;
- App2: 日志检索;
- App3: 文件威胁(沙箱)鉴定器;
- App4: 威胁-资产视图
- App5: 邮件威胁
- App6: DNS鉴定

### 产品形态:

硬件: 天眼分析平台 + 天眼采集器 + 沙箱鉴定器;

## 威胁情报中心

- App1: 多维线索追踪系统;
- App2: 基础数据查询平台;
- App3: 威胁态势(DDoS, 木马病毒, 反欺诈...)
- ...

### 产品形态:

1. 云端查询服务;
2. 本地威胁情报中心;

## NGSOC

- 安全态势感知Dashboard;
- 未知威胁感知+日志检索;
- DDoS攻击态势;
- 漏洞信息与安全播报
- ...

### 产品形态:

硬件: SOC 态势感知分析平台 + SOC日志采集器+ 流量采集器

# 安全态势感知能力背后

海量情报数据

存储计算能力

数据挖掘技术

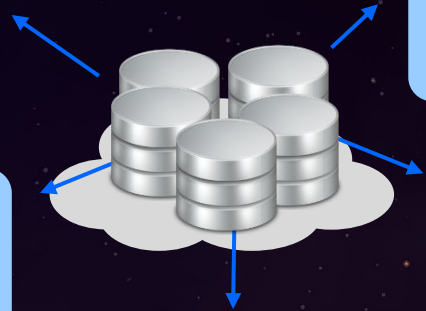
可视化分析技术

全球独有的样本库

- 总样本 > 100亿
- 每天新增 100万+
- 服务器 4万+ 台

最大的中文漏洞库

- 总漏洞数超过 4万
- 每天新增达 100个



全球唯一的主防库

- 覆盖 5亿 客户端
- 总日志数 6000亿
- 每天新增 10亿

互联网域名信息库

- 40亿 递归解析
- 每天新增 2000万
- 13年+ whois 信息

最大的存活网址库

- 每天处理 350亿 条
- 覆盖国内 96% 客户端

# 安全态势感知能力背后

海量情报数据

存储计算能力

数据挖掘技术

可视化分析技术

- 互联网大数据技术路线
  - 利用最廉价PC服务器+开源/自主开发软件构建而成
  - 数据的可靠性，扩展性全部自主可控，成本不到IOE方案的1/100
- 存储计算能力的关键在于规模
  - 大数据服务器规模超过40000台
  - 总存储数据量大于1EB，每天新增超过1PB
  - 每天各种数据计算任务10万个，每天处理数据量10PB
  - 具备一分钟内调动几十万颗CPU核参与计算能力
  - 具备一秒钟处理1TB数据的能力

# 安全态势感知能力背后

海量情报数据

存储计算能力

数据挖掘技术

可视化分析技术

- 以未知恶意软件发现引擎为例
  - 基于海量**数据挖掘**、引入**机器学习**算法，能够有效准确识别未知恶意软件，是人工智能技术在恶意程序自动分析领域中的首次商业应用
- 深度学习的应用
  - 搭建了高性能**GPU并行计算平台**，专门用于**深度学习**，如未知协议识别、同源性域名发现等

# 安全态势感知能力背后

海量情报数据

存储计算能力

数据挖掘技术

可视化分析技术

- 基于多维数据的关联，通过多种图形展现方式，构造能够帮助安全专家对未知威胁进行分析、发现、回溯、跟踪及预警的能力





# 安全态势感知能力背后





技术引领变革  
数据驱动安全