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

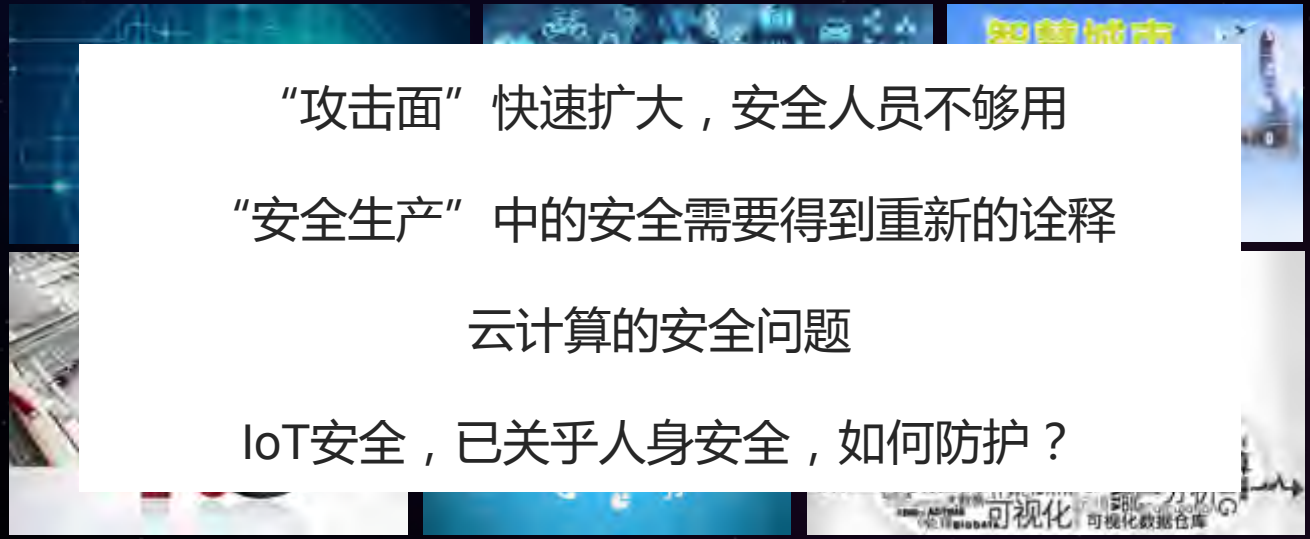

互联网+


THE INTERNET OF THINGS


智慧城市


BIG
DATA
大数据
实时性计算
分析
可视化
可视化数据仓库

热点背后的安全挑战



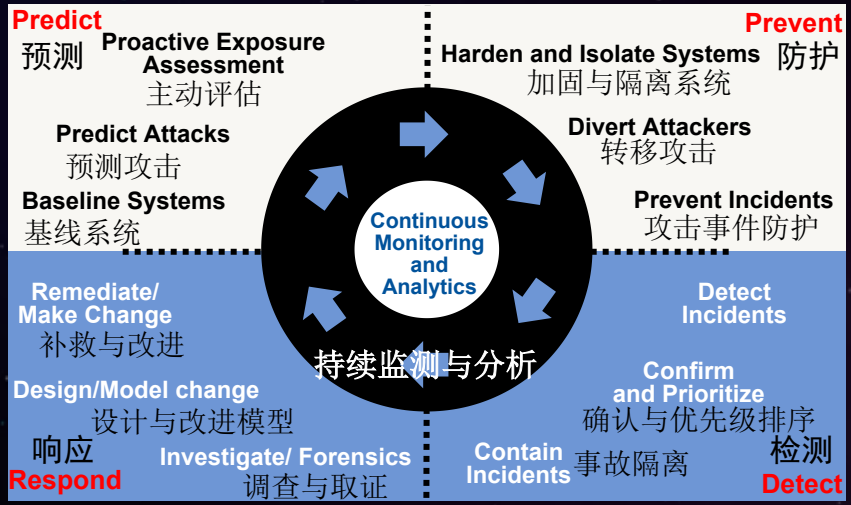
“攻击面”快速扩大，安全人员不够用

“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

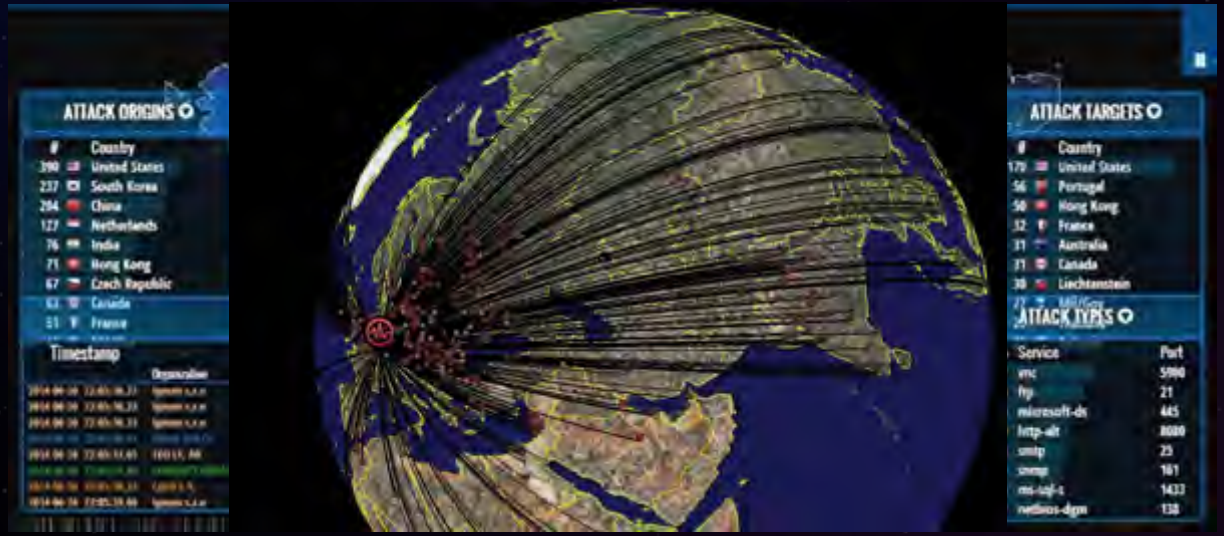

Predict
预测
Proactive Exposure Assessment
主动评估
Predict Attacks
预测攻击
Baseline Systems
基线系统
Prevent
防护
Harden and Isolate Systems
加固与隔离系统
Divert Attackers
转移攻击
Prevent Incidents
攻击事件防护
Continuous Monitoring and Analytics
持续监测与分析
Remediate/ Make Change
补救与改进
Design/Model change
设计与改进模型
响应
Respond
Investigate/ Forensics
调查与取证
Detect Incidents
Confirm and Prioritize
确认与优先级排序
Contain Incidents
事故隔离
检测
Detect

我们的“马克沁机枪”

完成“攻击拼图”

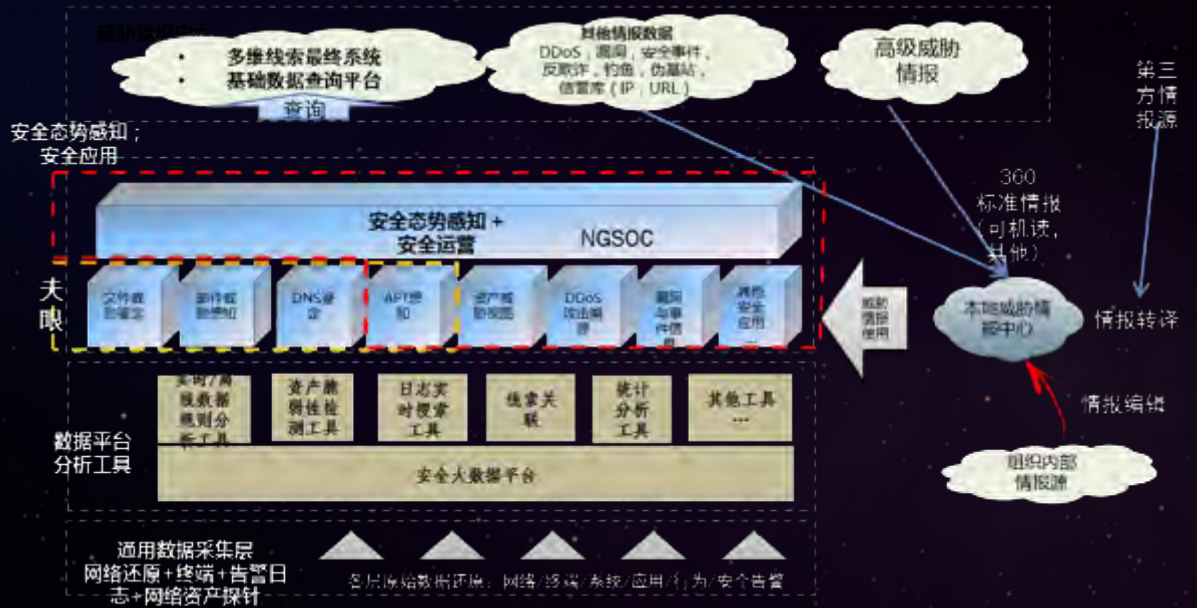

攻击动机：他们为什么要干
威胁指标：真的受到了攻击
表象行为：观察的表象行为
威胁源头：究竟谁干了这些
攻击手段：威胁的技术手段
突发事件：究竟发生了什么
威胁目标：他们想攻击什么目
响应方案：我们做什么补救
Campaign
TTP
Observable
ThreatActor
Incident

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


多维线索最终系统
基础数据查询平台
查询
其他情报数据
DDoS，漏洞，安全事件，
反欺诈，钓鱼，伪基站，
信誉库（IP，URL）
高级威胁
情报
第三
方情
报源
安全态势感知，
安全应用
安全态势感知 +
安全运营
NGSOC
大
脑
文件威
胁感知
邮件威
胁感知
DNS安
全
API感
知
资产威
胁视图
DDoS
攻击响
应
漏洞
与事
件信
息
消息
安全
应用
威胁
情报
使用
360
标准情报
（可机读，
其他）
本地威胁情
报中心
情报转译
情报编辑
组织内部
情报源
数据平台
分析工具
实时/离
线数据
规则分
析工具
资产脆
弱性检
测工具
日志实
时搜索
工具
线索关
联
统计
分析
工具
其他工具
...
安全大数据平台
通用数据采集层
网络还原+终端+告警日
志+网络资产探针
多层次原始数据还原：网络/终端/系统/应用/行为/安全告警

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

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

最大的中文漏洞库
- 总漏洞数超过4万
- 每天新增达100个

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景

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