云计算数据中心的可视化安全管理

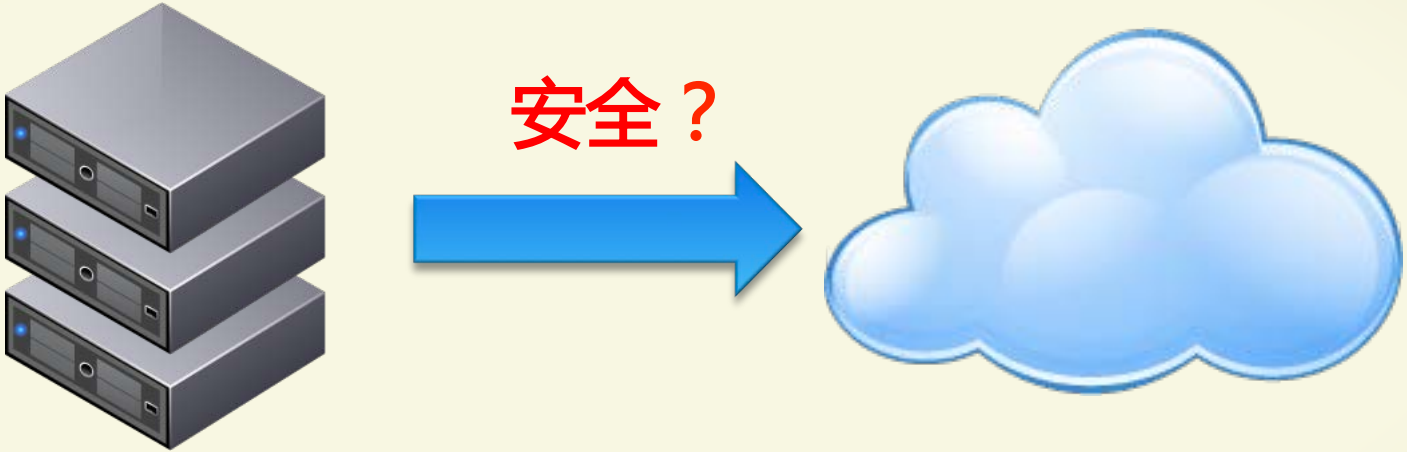
安贤科技
NUBOSH

朱民航

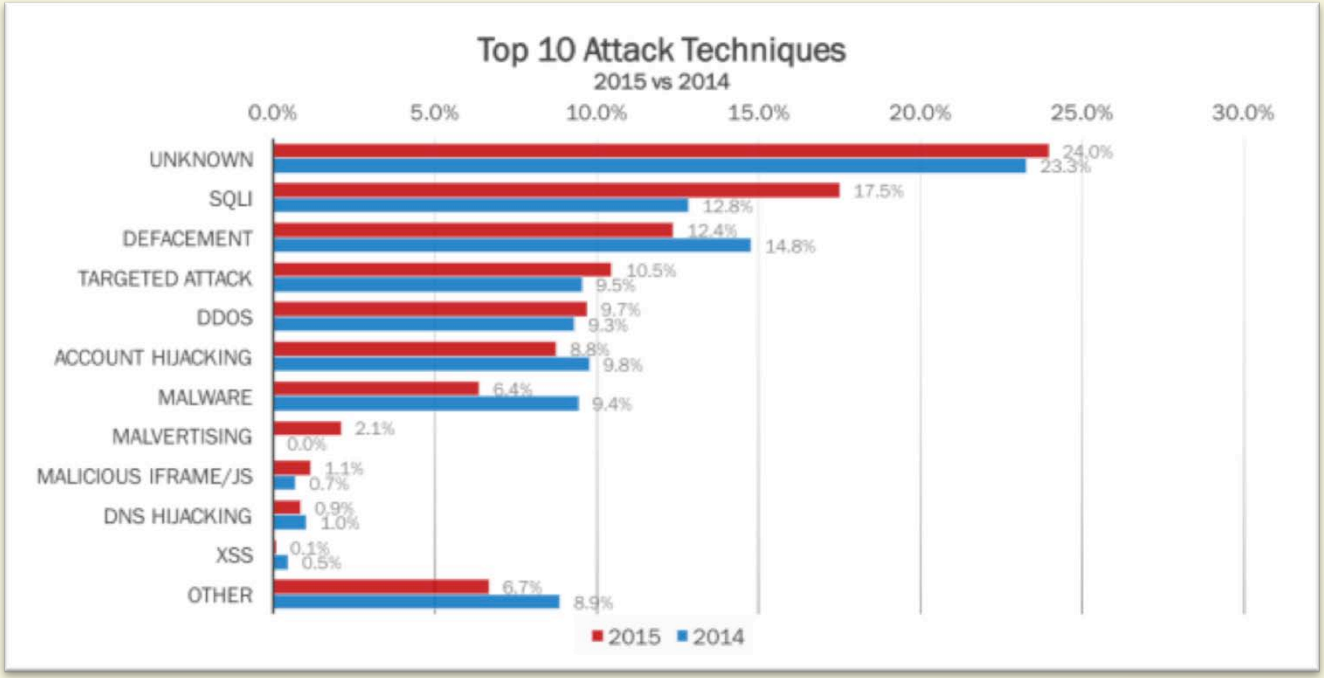
- 南京安贤信息科技有限公司创始人
- 15年以上的网络、安全产品研发经验
- 主要研究方向：云计算、网络安全防护

微信号： tonyzhu9601

安贤科技
NUBOSH

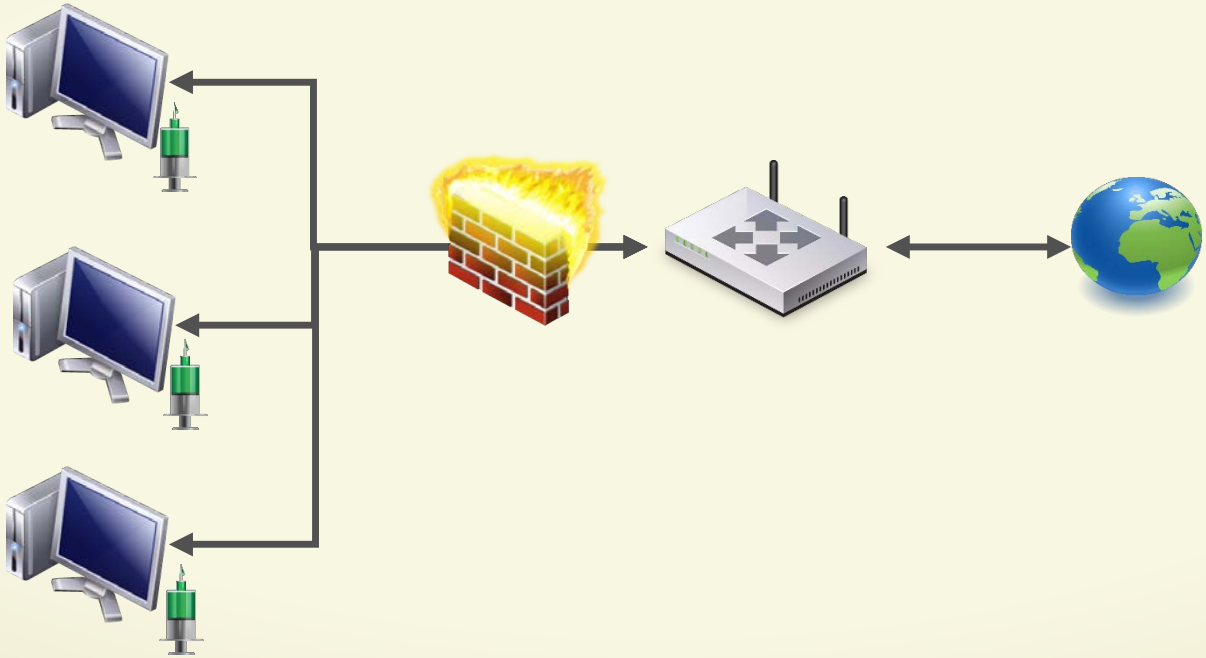


安全攻击以窃取数据为主



安贤科技
NUBOSH

传统的安全部署



安贤科技
NUBOSH

迁移到云，数据安全吗？

网络边界消失，无法部署传统安全方案

+

云平台常见的防DDos、SQL注入等安全服务

≠

数据安全

因为“东西向”内网攻击、隔离性不足、平台的漏洞、**未知威胁**...

安贤科技 NUBOSH

单纯的防御，不能解决问题

- 集中的数据，攻击的高回报
- 大量的未知威胁
- 复杂的攻击过程

- ✓ 智能安全系统，及时预警
- ✓ 直观的展现安全威胁，找到问题根源
- ✓ 快速修复，避免损失

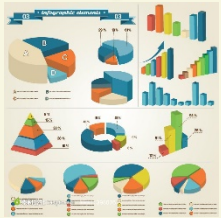
安贤科技 NUBOSH

可视化安全管理

探针

大数据分析

裁决执行



可视化管理中心

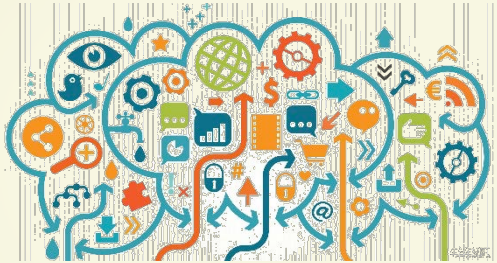
安贤科技
NUBOSH

探针，数据收集

- 部署在数据中心的任何关键节点
- 采集数据包括文件、系统、网络、业务……
- 海量数据

安贤科技
NUBOSH

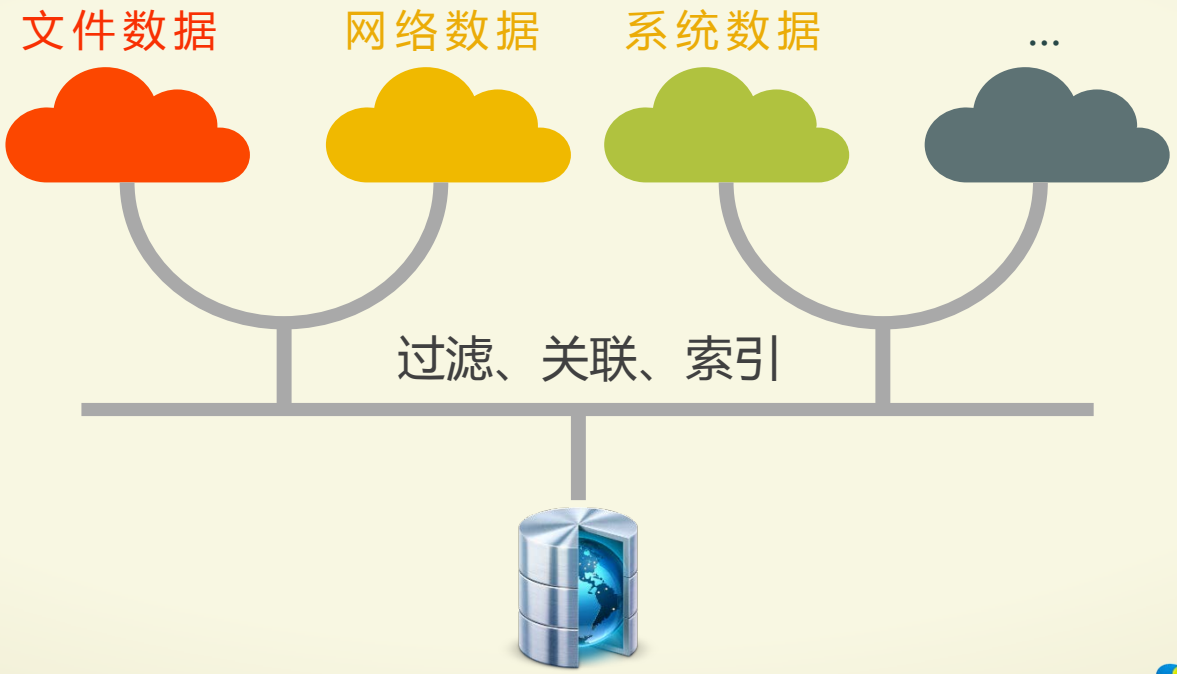
大数据分析，可视化的基础



- 数据存储
- 建立安全数据模型
- 智能学习

安贤科技
NUBOSH

数据存储



安贤科技
NUBOSH

建立安全数据模型

不仅基于安全特征码

更多的基于时间、行为、地点、人员等数据域

数据模型包含：

- 数据域
- 数据域的过滤条件
- 统计的维度、方法
- 异常报警的条件

安贤科技 NUBOSH

数据模型管理

例子:“撞库”攻击的模型

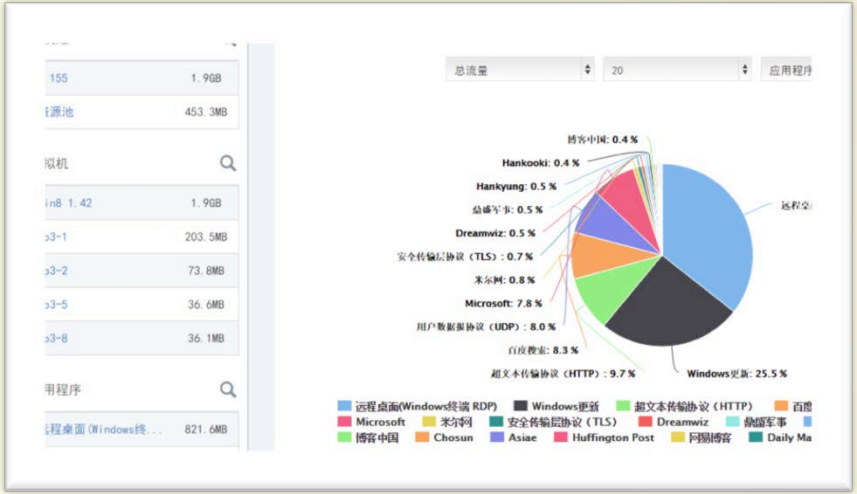
1. 数据域包含：客户端地址、账号、时间、登录结果
2. 统计的维度：客户端地址、时间、账号、登录结果的组合
3. 统计方法：次数累加
4. 异常报警的条件
   a) 地址相同
   b) 短时间内连续登录，账号不同，登录结果以错误居多
   c) 每次错误，不重试密码，换账号登录

安贤科技 NUBOSH

可视化数据展示

基于数据模型：

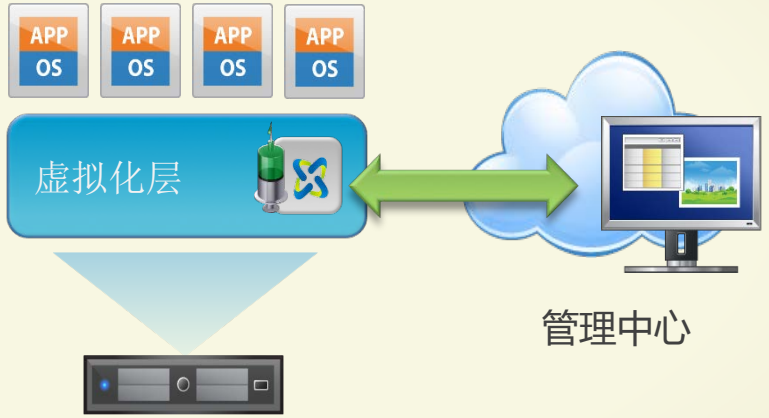
- ✓ 显示实时统计数据
- ✓ 异常报警
- ✓ 数据挖掘



安贤科技
NUBOSH

裁决执行

- 部署在数据中心的关键节点
- 根据预定义的规则，执行数据分析结果的裁决



安贤科技
NUBOSH

优势

1. 将文件、网络、系统、业务等数据相关联，通过可视化的图形工具，让用户了解安全事件发生的整个过程。

2. 按需定制用户的整个安全防御系统

3. 基于数据模型的分析，智能学习，防御未知威胁

安贤科技 NUBOSH

安贤科技
NUBOSH

感谢聆听！