1.行业背景

近年来，医院信息化在快速发展的同时，也逐渐暴露出了安全建设的不足。另外，随着移动医疗和远程医疗的日趋广泛的应用，如何保障移动医疗和远程医疗的应用安全也是一个极其严峻的挑战。

2.痛点及需求

当内部出现高级威胁攻击，医疗行业需要安全产品能判断出是否存在恶意攻击行为，能分析恶意攻击行为的记录、恶意攻击行为的来源、恶意攻击行为的操作步骤、实现方式，以及分析恶意攻击行为是否成功等。企业的主要关注点在于希望做到事前预防，事中防御，事后及时响应。

3.解决方案

根据医院行业目前的现状，网思科平首先通过安全服务的定期审核对现有安全架构进行摸底，完成**整体安全解决方案**的设计工作。利用相关的技术手段，深化到医院的对外服务及内网生产终端系统，通过围绕新一代的威胁分析理念，解决医院的应用层安全、终端的未知威胁、攻击监测和溯源等安全问题。

主要从以下几点体现：

1. 威胁情报输出 2. 漏洞风险评估 3. 信息安全应急响应 4. 渗透测试 5. 安全宣传培训

4.客户认可的价值

- 检测、发现敏感信息、利用防护弱点攻击，尽可能地突破现有安全防护体系，可对目标资产做越权操作。帮助安全人员直观地了解到目前业务系统的安全现状，为后续的安全工作提供有力支撑。
- 通过渗透测试过程的演练，提高了医院人员的应急响应处置能力。
- 提高医院办公人员和事件响应者的生产力和有效性。

- 强化医院运维人员对高级威胁的识别能力。
- 通些专业的人员培训，有效强化了医院各部门人员对于安全问题的认识，通过各种宣传方式和手段加强员工安全意识。