# 医疗机构

## 主动威胁分析 – 高级版

思科主动威胁分析凭借卓越的威胁检测性能帮助这家顶尖的美国大学医疗机构保护患者数据，并让担心数据安全的高管高枕无忧。

### 客户概况

- 顶尖的美国大学医疗机构
- 异构联网设备
- 初步成型的安全运营计划

### 解决方案

- 思科主动威胁分析高级版
- 利用一种久经考验的事件响应方法来应对该大学异构环境中的安全挑战
- 资深安全专家

### 要点

- 冗余安全事件和警报平均数量减少 99%
- 每月为客户分析师和调查员节省的时间平均超过 93 个小时
- 整合 FBI 威胁情报，在假期保护大学的安全

## 安全挑战

鉴于网络攻击日趋复杂且不断扩散，一家顶尖美国医疗机构（一所知名大学附属）的高管对其网络安全感到焦虑不安。这些高管希望限制出现数据泄露的可能性。如果网络犯罪分子成功窃取宝贵的数据，不仅会给患者带来严重风险，还会有损人们对该医疗机构品牌的信任。此外，严格的医疗法规也给这些高管增加了压力，促使其确保该医疗机构具备可靠的安全架构。

为了防止遭受潜在的网络攻击，该医疗机构决定构建并改进其自身的安全运营。但是，事实证明，由于一些原因，构建安全运营非常困难。

该医疗机构采用了大量不同的安全技术，但很难将设备有效组合在一起来确保网络安全。另外，该医疗机构缺乏足够的安全专业人员。由于安全资源不足，致使管理该医疗机构的网络及其收到的海量日常安全事件占用过多时间。

## 思科解决方案

由于在获得高级安全的同时遵守预算限制是该医疗机构高管首先要考虑的问题，因此主动威胁分析高级版成为最佳解决方案。主动威胁分析高级版是三个版本中最全面的版本，可在降低成本的同时提供全面的安全可视性。

主动威胁分析高级版可以在该医疗机构以前难以有效利用其安全技术的领域提供成熟的事件响应方法和工具集。此服务将思科技术与该医疗机构的第三方软件和设备相集成，并将所有安全相关网络活动收集到 OpenSOC 这个大数据分析平台中，完成数据的汇聚和精密分析。这样一来，主动威胁分析专家就可以提供高级检测和有针对性的补救建议。

借助主动威胁分析高级版提供的集中事件检测以及经过培训的安全专家的支持，该医疗机构得以高效地利用其现有人员和资源来执行有效的安全计划。这种专业知识与主动威胁分析高级版服务的高级分析和既定方法相结合，可以帮助实现该医疗机构高管寻求的卓越威胁检测水平。

## 业务成果

该医疗机构无需拼凑复杂的安全技术，也无需构建内部安全运营中心，因此节省了资源，并且限制了遭受网络威胁的可能性。

主动威胁分析的威胁检测非常准确，每月可针对该医疗机构网络中的约 5000 个唯一且经过调整的事件发出警报。在这数千个事件中，平均只有 32 个事件被确认需要进行补救。这种准确的过滤可以将冗余客户调查和误报安全警报减少 99%。

思科调查员和分析师重点关注该医疗机构的高保真事件，在他们的支持下，该医疗机构节省的时间平均超过 270 个小时。如果没有主动威胁分析高级版，该医疗机构的安全人员将不得不在人数有限而任务繁重的情况分析这些事件。该医疗机构的安全团队可以利用节省的时间和资源集中处理关键业务计划，而不必一直费力地进行威胁监控。

## 关于主动威胁分析

思科主动威胁分析 (ATA) 将深厚的专业知识与前沿技术、领先的智能功能和高级分析相集成，从而以超快的速度、超高的准确性和超强的针对性来检测和调查威胁。作为一个全面的安全解决方案，我们的专家调查员会运用我们一流的全球安全运营中心网络全天候监控客户网络，提供不间断的警戒和深入分析。

www.cisco.com/go/securityservices