某民航信息中心安全运行中心（SOC）项目

客户问题

该信息中心负责管理其管辖范围内民航的出票与旅客离港信息。信息中心网络环境复杂，网络设备众多，划分了三个逻辑网络，并采取了较严格的隔离措施。信息中心已有较完善的网络运行中心（NOC），而且防火墙、UTM、VPN、IDS、防病毒系统、漏洞扫描器、AAA等安全设备均已部署，并且都是国内外知名品牌，但是缺乏对这些安全设备所产生事件的综合分析管理的手段。这些设备每天产生的大量事件信息管理员根本无法顾及，发生较大安全事件后审计时也缺乏有效的审计手段，不能满足用户对企业信息安全的要求。

项目实施

根据客户需求，网御神州为客户部署了一套SOC系统。该系统针对信息中心的安全基础设施、OA网络系统和民航出票离港业务系统进行集中安全监控与管理。与此同时，网御神州还为客户设计并建立了安全管理的相关制度、策略，以及运维管理的流程。系统将设备上收集的事件进行归一化处理，生成统一的内部格式的事件，传给管理中心，通过多种展现方式展现（包括列表、统计图、统计表、事件图、地图信息图等）。借助过滤器，管理中心根据预先定义好的规则对接收到的事件进行聚合和关联分析，最终向用户展现高度聚合、更有价值的事件，有效地解决了海量数据难以处理、事件误报、漏报的问题。同时，规则还可触发预定义的动作，实现多种方式的告警（控制台、邮件、短信）和联动，并将关联分析之后的事件保存到数据库中，用于对过去的安全事件进行研究或进行审计。系统还提供了丰富的报表模版，可以根据用户的要求非常直观地定制各种统计报表，用于生成各个管理级别的统计报告。

客户价值

该系统投入使用后已成功地发现了用户网络中的蠕虫、内部用户的违规操作、外部用户窃取企业数据的企图、疑似DDoS攻击的非正常流量等安全事件，真正帮助安全管理人员及时解决了实际问题，得到客户的信赖。在此基础上，该信息中心与网御神州建立了日常支持保障与应急响应安全伙伴关系，以保障08年奥运会的正常运行。