一汽集团安全管理平台案例介绍

SOC 事业部

网御神州科技有限公司

1. 项目背景和用户需求

作为我国汽车行业的龙头企业，中国第一汽车集团公司（以下简称“一汽”）投入巨资进行企业信息化建设，完成了企业网络基础设施的构建，上线了多个重要业务应用系统，这些都极大地提高了一汽集团的生产效率和企业竞争力。但另一方面，企业业务对信息化的依赖程度越来越高，网络和应用系统的不正常造成的损失会越来越大，而一汽集团是一个下辖众多分支机构，分布全国多个地域的超大型企业，网络和业务系统都非常复杂，为此，一汽集团成立的专门的信息系统公司来维护企业信息化系统的正常运转。为了保证企业业务的连续性，一汽集团对网络进行合理改造，对重要系统配置冗余设备和冗余系统，建立灾备中心，以保证系统有较高的可用性，并且部署了防火墙、身份认证、IDS、VPN、防病毒系统等多种安全设备来保障网络的安全。

然而，由于一汽集团的企业网络规模很大，结构较复杂，网络中的设备和系统众多，管理员对网络的管理和监控工作量极大，对管理员的技术水平要求较高，而且实时性难以得到保证。为能全面地监控网络中各重要设备和应用系统的运行状态，一汽集团部署了 HP OpenView 的网管平台，大大提高了对网络可用性地监控能力。但对于安全事件的监控和对各种操作日志的分析和审计，由于缺乏统一的平台，依然需要管理员分别登录不同的设备和系统，查看相关的安全日志，人工进行分析和审计。由于原始事件量极大，管理员要么被淹没在海量的事件当中，无法顾及其它工作，要么干脆忽略对事件的分析，直到出现问题后再回过头来查找原因，安全预警水平不高，即使在事后进行审计时，由于缺乏完整的审计数据、统一的审计策略，没有易用的审计工具，很难获得令人满意的审计结果。因此，一汽集团迫切地希望能够建立一套统一的安全监控和审计平台。经过广泛调研和深入的技术交流后，一汽集团最终选择了网御神州为其构建统一安全监控和审计平台。

2. 网御神州解决方案

针对一汽集团提出的目标，网御神州首先派出咨询顾问，对用户的网络和应

用的情况进行调研，对用户各层级各角色进行访谈，充分了解用户的网络应用现状和需求。通过对一汽集团网络拓扑和网络实际应用的分析，以及通过与管理员共同对重要业务系统的分析，提出一套适合用户当前需求的统一管理解决方案，并帮助一汽集团制定了一份详尽的实施方案，包括监控点范围的选择、监控数据的确定，等等。

根据实施方案，网御神州在一汽集团数据中心部署安全监控和审计服务器，在数据中心各网段及各下属机构中部署事件采集器，实时采集网络中重要的网络设备、安全设备、服务器主机、重要应用系统等的事件数据，事件分析引擎利用预定义的分析规则对采集的事件进行实时关联分析，发现重要安全事件及时向管理员告警，极大地过滤了无效事件，压缩了事件规模。同时，根据集团对数据的保存期限的要求，将所采集的数据保存在本地磁盘和网络存储中，按用户要求定制的报表和报告任务可以定期执行，利用这些数据生成所需的安全统计报表和分析报告，并能根据用户对内控的要求，针对特定的操作或帐号，生成审计报告。最后，所有的监控与审计信息都汇总到监控中心，由一汽集团的信息系统网络运维管理人员进行集中的监视与应急响应。

3. 应用效果

网御神州在为用户部署了上述平台后，用户可以实时地获取整个网络运行的安全视图，能够根据用户角色的不同，将其关注的内容友好地展示给用户，使其实时掌握网络的安全态势。当出现安全事件时系统可以及时产生告警，并能以事件图、地理位置图的方式帮助管理员迅速定位事件源，极大地提高了网络安全预警和事件响应能力。另一方面，利用统一采集和存储的事件数据，可为用户提供指定时间段内网络运行的安全报告，帮助用户掌握网络安全趋势和风险状况，根据统一的审计策略可对网络的访问行为进行各种合规检查和审计，极大地加强了一汽集团网络安全内容和审计能力。用户认为在部署上述平台后，对网络的整体安全监控能力和对事件的响应水平，对企业 IT 内控和安全审计水平都上了一个大的台阶。

4. 关于网御神州

网御神州安全管理团队根据长期以来在安全管理领域的深入研究，结合来自客户的需求与市场的现状，提出了具有完全自主知识产权的网神 SecFox 安全管理产品理念，尤其强调网络管理、安全管理与运维管理的一体化，为政府、军队、公安、税务、电力、保险、电信、金融、交通等各个领域的客户提供全面的安全运营保障平台。网御神州建立了专门的安全管理研发和实施队伍——SOC 事业部，在国内市场突飞猛进，取得了令人瞩目的市场成就，在 CCID《2007-2008 中国信息安全产品市场研究年度报告》中网御神州位居安全管理（SOC）市场第一名，成为了中国安全风险管理与运维的市场领导厂商之一。

欲获取更多信息，请即联系网御神州科技（北京）有限公司

全国统一热线服务电话：010-87002000（7×24 小时）

E-mail：service@legendsec.com（5×8 小时）

网站地址：www.legendsec.com

网神安全管理博客地址：http://blog.sina.com.cn/legendsec

传真：010-62972896

通信地址：北京市海淀区上地信息产业基地开拓路 7 号先锋大厦 2 段 1 号

邮政编码：100085