天津烟草 IT 综合安全运维管理平台

背景概述

长期以来，烟草行业作为一个计划性很强的行业，一直以计划经济的模式在运行和操作。但是随着市场经济的迅速发展，各行业市场化程度都在不断提高，烟草行业也不可能始终置身于市场化大潮之外。在全国烟草信息化工作会议上，国家局提出了当前行业信息化建设的基本思路，即紧紧围绕行业改革和发展的主题，以建平台、抓应用、成体系为主要内容，抓紧重点工程建设，大力加快行业信息化建设。具体体现在：一是建平台，尽快形成统一平台，统一数据库、统一网络；二是抓应用，逐步实现系统集成、资源整合和信息共享；三是形成体系、树立起打造“ 数字烟草 ”的目标；四是抓紧重点工程建设，把解决实际问题作为工作的突破口。

天津烟草积极针对自身条件，对其自身进行信息化改造，决定对全区烟草行业从行业的整体供销链 、管理链出发，以电子商务为技术依托，做出天津烟草信息化建设的总体规划，通过信息化的建设实现烟草销售的电子化 、管理的电子化，使天津烟草的整体实力更上一个台阶，做强、做大！

知己知彼 因需而变

天津市烟草系统下设有 18 个区县烟草专卖局（分公司），由市局（公司）统一领导，实行二级管理（直接管理）。建设前市局还没有一个以市局为中心的，覆盖全市各区县局（公司） 、网点的全面的计算机信息化管理系统，这显然不能满足天津烟草对集团化运作的需要。卷烟零售商户近十万户，基本采用电话访销、访送分离的模式进行卷烟的销售。烟草系统中的物流、配送等都受到了很大的制约，结算系统、数据传输、视频会议也不能实现。

选择好的安全服务比选择产品更重要

网络安全是无法做到百分之百的安全保障的，因为网络安全是一个动态发展的过程。在应用系统建设完成后，天津烟草曾经经历了一次大规模的网络蠕虫病毒事件，大量的病毒攻击流量汇总到了核心网络区域造成严重堵塞，严重影响了天津烟草的核心电话访销业务的运转。东软作为天津烟草的网络安全系统集成商，第一时间赶赴现场进行处理，最终定位的事件原因是新型恶性蠕虫病毒大规模泛滥所致，天津烟草虽然已经在全网部署了防病毒软件，但是真正当新型或恶性蠕虫病毒爆发时，天津烟草同样遇到了所有企业面临的问题，就是杀毒软件的查杀效果并不是很理想。在这种安全威胁日益恶劣的环境下，东软与天津烟草用户签订了长期的安全保障服务合作协议，同时也开始为用户设计实现了一套真正切合烟草行业用户网络与应用特点的 IT 综合运维管理平台。

安全运维 因御而安

天津烟草针对几年来在安全方面总结的经验，为了提升安全管理和防御效果，提出需要进一步加强网络状况及网络流量的监控管理，加强终端主机的安全管理，以及加强网络安全体系的综合监控管理，并建立起合理有效的网络安全运维处理流程和机制。这正符合了 IT 综合运维管理平台建设项目所要实现的目标。

根据天津烟草的实际需求，并借鉴和吸收其它省烟草公司的建设经验，通过构建一套先进、完善的综合 IT 安全运维管理平台，集中采集信息系统的日志信息、配置信息、性能信息、流量信息、安全信息等，实时监控主机系统、网络系统、业务系统、数据库系统、安全系统的运行状况，并进行智能化的关联分析，找出 IT 威胁事件的根本原因，同时还可自动触发 IT 工单系统，督促相关责任人进行快速处理。

IT 综合运维管理平台以东软 NetEye 安全运维管理平台为基础进行建设。该平台以信息资产为核心，以风险管理为主要途径，通过技术手段提升网络安全管理成熟度，建立主动安全防御体系，有效降低安全风险。

此平台是一个以资产为核心的管理体系，首先需要完成包括主机设备、网络设备、业务系统、数据库系统在内的资产调查，建立资产数据库，进行资产管理，通过对信息资产进行风险评估，利用直观的动态拓扑结构清楚的展示出组织当前的安全状况和安全风险。

此平台主动收集网络、系统、主机与应用系统的各种性能运行状态数值，定期轮询关键配置参数，实现了详尽的系统性能监控与故障监控。同时更创新的将安全事件威胁分析与性能值进行关联考虑，即通过系统性能值在面对攻击事件后的变化波动范围来智能判断攻击事件的成功可能性，使得全面的风险计算得以实现。

此平台是为网管人员提供检测和管理组织网络安全的技术手段，其通过风险管理展示了组织当前的网络安全风险状况，同时给出降低安全风险的方法，驱动 IT 维护人员进行降低安全风险、解决安全问题的工作，使得管理员能够将降低安全风险在安全事件发生之前，在日常工作中有效的完成，并且可以降低组织的管理成本。

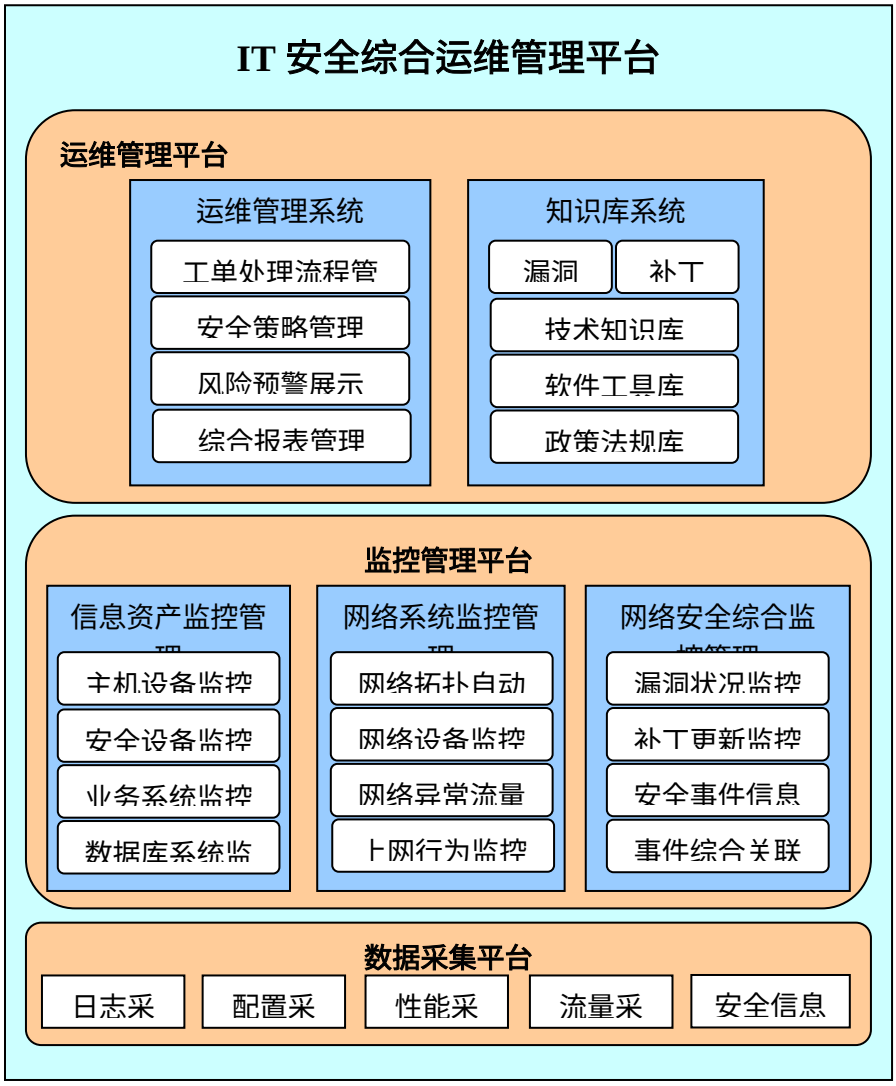
此平台为组织提供了完善的工单流程，能够高效的协调 IT 人员。平台通过验证和审核安全维护的行为（包括 IT 维护人员、信息资产的相关责任人的行为），防止人员在安全方面的疏忽，强调每个人都要遵守的安全规则，确保组织的安全策略得到落实。

此平台特有的异常流量检测功能，支持多种方式从多种骨干网络设备采取骨干链路的流量，实时展示和监控全网网络流量状况，同时考虑到网络大部分时间工作在无人值守的状态下，系统还可以任意回溯网络中的历史流量，通过先进的设计架构最多可以保存长达数年的细粒度访问流量。流量监测功能还可以通过 BPS 和 PPS 两个关键参数的实时监控及时对 DDoS 攻击、大规模蠕虫爆发、潜在的僵尸网络、P2P 应用等严重消耗网络带宽资源的非法流量进行追踪识别和报警。

东软 NetEye IT 安全综合运维管理平台的整体架构

为了充分满足天津烟草的实际需求，IT 综合运维管理平台从体系架构上可分为数据采集平台、监控管理平台、运维管理平台三个层面，各个层面包括了多个功能模块或子系统，从而共同组成 IT 综合运维管理平台。

IT 安全综合运维管理平台的整体架构示意图如下：



数据采集平台：根据系统指定的策略负责从网络设备、安全设备、主机系统等数据来源采集各种安全告警、日志信息。

监控管理平台：将采集到的原始安全信息根据策略进行整理、归类和统一标准格式化，并结合信息资产的安全保护等级进行智能化的综合关联分析，科学合理的定义 IT 事件的性质和处理级别。

运维管理平台：实现东软 NetEye IT 运维管理平台的统一界面展示和运维管理。通过统一的图形化管理界面，东软 NetEye IT 运维管理平台实现了安全监控、维护、管理、展示的全部功能。

实施效果

该 IT 安全综合运维管理平台正式上线以后，配合东软专业的网络安全服务，天津烟草的网络系统稳定运营，尤其是 2008 北京奥运期间，借助于 IT 安全综合运维管理平台的自动化安全监控和事件处理机制，天津烟草的网络系统一直保持着稳定高效的运转。