聚铭完整性检查（配置变更）管理系统

产品白皮书

南京聚铭网络科技有限公司

2016 年 6 月

版权声明

商标声明

联系信息

地　　址：南京市雨花区软件大道 180 号 07 栋 406 室

邮　　编：210000

电　　话：025-52205520 025-52205570

传　　真：025-52205565

邮　　箱：support@juminfo.com

网　　址：www.juminfo.com

全国服务热线：400-1158-400

目录

1 安全运维面临的问题

随着信息化建设地深入发展、设备种类不断增加，配置安全问题日渐凸出。为了维持 IT 信息系统的安全并方便管理，管理员必须从入网审核、验收、运维等全生命周期各个阶段加强和落实安全要求，同时需要设立满足安全要求的基准点。

针对行业的业务系统建立安全检查点与操作指南的基准安全标准，则成为各个行业安全管理人员最为紧迫的事情。但目前面临如下问题：

1. 误操作或非法修改配置文件导致系统安全性下降，没有相应的手段及时发现
2. 误操作或非法开启的进程、端口、服务等无法及时发现
3. 木马程序无法及时发现

2 传统的手段无法解决

2.1 设备或系统种类繁多

安全运维人员需要面对种类繁多的设备或应用，如何管理这些设备和应用的配置，或者如何定位知道这些设备配置的安全问题，是他们在安全运维过程中遇到的巨大问题和挑战。

而且，由于需管理的设备分布范围广、分属不同的业务系统，如何能快捷、方便的收集和分析这些配置，则成为横亘在安全运维人员面前的一个巨大难题。

一般而言，日常运维人员需要收集和分析各种主机系统、网络设备、数据库系统以及其它中间件的配置；这些配置的收集和分析存在以下问题：

1. 部署位置多种多样
2. 配置的表现形式和存储样式不尽相同，如有的在配置文件中、有的在注册表中；有的配置文件是一般文本，而有的又是 XML 形式
3. 采集过程中可能还需要穿越网关设备或堡垒主机

由于配置在形式上存在千差万别，如何准确地分析则成为困难的事情。

2.2 自动化程度低

以往，对于设备或应用的配置审计，一般都是通过人工方式进行，仅在上线前进行一次评估（安全加固），这样做的缺点是显而易见的：

1. 纯粹依赖手工方式，效率低下

2. 在设备或应用上线后，不能定时地或经常性地进行评估，从而无法反映现网设备或应用的配置情况，这导致系统存在巨大的安全隐患（如未能按口令复杂度设置管理员账号）

结果比较零散，只能依赖于人工汇总。

3 完整性检查的解决方案

完整性检查（配置变更）系统是聚铭网络自主研发的拥有自主知识产权的专业安全配置检查管理产品。它协助用户实现企业内安全配置的集中采集、风险分析、处理的工作，它是企业日常信息安全工作的重要支撑。

图 1 完整性检查管理系统的解决方案

配置问题管理：全面集中检查和分析各类系统存在的本地安全配置问题，减轻用户因对不同设备分散管理而带来的冗余工作。

安全运维管理：建立日常运维工作的服务保障体系；包括各种资产配置库、报表管理、安全知识管理等

它主要解决企业日益繁重的安全配置管理问题。作为统一的安全配置核查和管理系统，能够准确、快速、及时地发现、汇总企业中不同厂商不同种类的网络设备、主机、防火墙、数据库、中间件的安全配置问题，它主要包括如下主要功能：

任务制定：提供灵活的功能用于制定不同类型或周期的配置检查任务，任务中可以方便地设置检查对象和检查策略。

采集分析：全面集中检查和分析各类系统存在的本地安全配置问题，减轻用户因对不同设备分散管理而带来的冗余工作。

检查报告：提供全面、详尽、清晰的扫描报告管理功能，并能对不同的检查结果进行比对。

4 系统功能概述

4.1 功能概述

完整性检查（配置变更）管理系统是由综合展现层、业务功能层、分析处理层、采集层等部分组成，如下图所示：

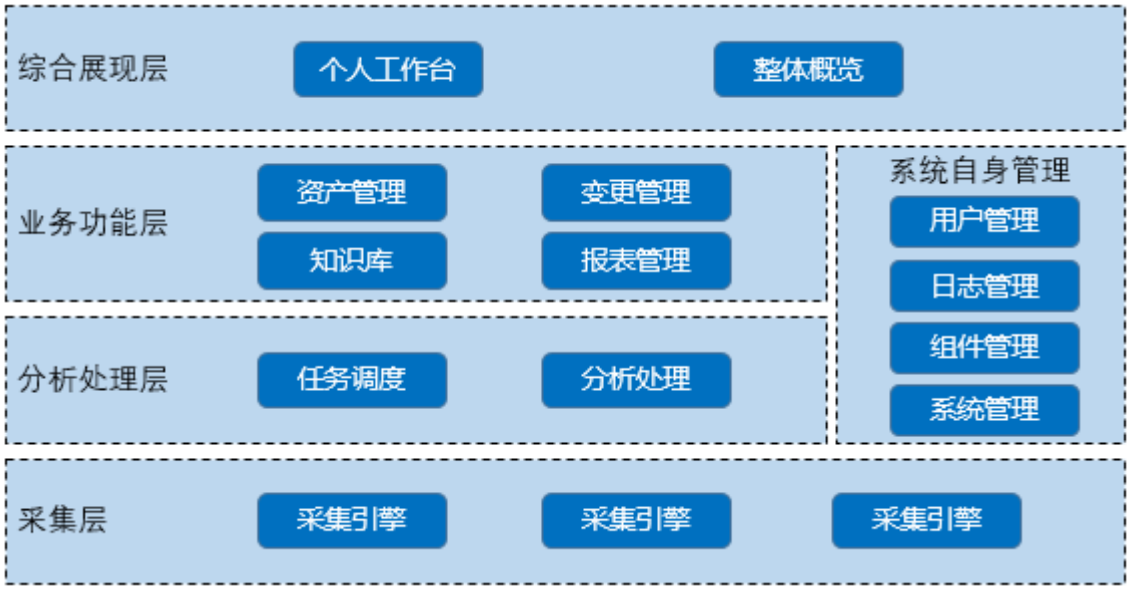

图 1 完整性检查（配置变更）管理系统功能架构

在完整性检查管理系统中，Web 主要由安全配置变更管理、整体概览、个人工作台、资产管理、告警管理、报表管理、知识库管理、系统管理组成；下面的章节会较为详尽地介绍每个部分。

4.2 变更检查管理

变更管理检查计算机系统的文件、端口、进程等的变化信息，以监控系统的变更状况发现其中的异常，以便及时采取相应措施保护系统安全。

目前，支持的系统或设备主要包括：

1. 主流操作系统（Linux/Unix、Windows）
2. 主流路由器/交换机
3. 主流防火墙

变更管理主要分以下模块：

1. 配置变更项问题查看：列表查看登录用户权限范围存在的配置项变更问题，显示资产上存在哪些配置项变更的情况；

2. 任务管理：任务管理包括三个部分：任务列表、正在执行的任务以及已完成的任务，检查报告可以导出为 Word、PDF、HTML 等格式；

3. 策略管理：用户可以自定义检查策略。可设定用户自定义配置检查项，例如文件、目录、端口、进程等。

4.3 安全仪表板

安全仪表板是系统风险的集中展示区域，也是系统展现给用户的第一个视觉界面；它支持以 TAB 页及微件（Widget）形式展现，用户也可对仪表的布局和内容进行定义和调整。

系统支持如下类型的仪表板：

1. 整体安全概况
2. 安全资产概况
3. 告警概况
4. 脆弱性概况
5. 任务概况

4.4 个人工作台

个人工作台是登录用户用于便捷操作的窗口。它固定的放置于页面的一个位置（通常是顶部），起到管理入口的作用。它主要包含了与登录用户相关的一些信息，但需对用户的权限进行过滤，其功能主要包括：

1. 对象快捷创建菜单，菜单中包含：资产、用户、任务
2. 个人待办事宜：告警
3. 通知功能：任务完成情况

4.5 资产管理

安全资产是完整性检查管理系统管理对象。与 ISO27001 的关于资产的定义略有不同，完整性检查管理系统中的资产是特指具有 IP 地址的 IT 类设备及其之上运行的、可管理的服务、应用。

一般而言，安全管理中的资产具备如下两类属性：

1. 基本属性：名称、编号、系统类型（产品类型、操作系统类型、版本等）、IP 地址（支持 IPv4 核 IPv6 格式）、响应人（出现安全问题应由何人处理）、登录凭证（获取配置、安全配置检查等使用）、上架信息等；
2. 安全属性：完整性、可用性、保密性、风险信息、开放端口、安全配置变更问题等。

系统的资产管理支持用户录入、导入或自动发现资产。

为了处理不同网络的资产同 IP 问题，系统还支持对于网络和 IP 地址段的管理。

为了用户便于集中、灵活地管理所辖范围内的资产，系统支持用户自定义资产管理视图。

4.6 告警管理

所谓告警是指用户特别需要关注的安全问题。

告警管理中包括了如下功能：

1. 告警监控：监控系统内存在的各种告警；用户可以通过定义过滤器以监控需要特别关注的告警信息；用户也可以根据个人需求，设置告警的提示音、界面显示方式等；
2. 告警处理：处理监控列表中相关告警；针对告警，用户可以清除、确认（不能确定是否需要处理）或转工单；
3. 策略定义：用户可以定义各类告警产生的策略（系统内置了部分策略）；在告警策略中可以设定对于安全数据的筛选条件、归并字段、时长和次数以及命中后产生何种响应；响应包括包含发送邮件、发送 Syslog 或 SNMP Trap、执行外部程序或脚本等。

4.7 报表管理

报表管理的作用为展示系统安全工作的结果。报表内容包含各种信息的统计情况，包括：告警报表、资产报表、配置变更报表等。

用户可以定义相关条件以生成报表，它们均可以导出为 PDF、Word、HTML 等格式：

4.8 知识库管理

知识库管理为系统运行和维护提供了知识来源以及安全问题的处理依据、方法或参考，目前支持如下几类：

1. 安全基线类：各种操作系统、网络设备、防火墙、Web 中间件及数据库等可被威胁所利用而导致安全性问题的标准描述及解决方案；
2. 漏洞类：通过扫描器发现的在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷的描述及解决方案；

3. 安全经验类：基于系统安全事件、漏洞、配置问题等信息综合生成的安全警示信息的描述、告警触发建议及解决方案等。

用户可以通过全文检索功能对系统提供的安全知识进行查询。

4.9 系统管理

系统管理的主要功用在于管理支撑平台正常运行的各种基础功能和参数配置。主要功能有：用户管理、系统参数管理、内置对象管理、升级管理、许可证管理、日志管理、口令策略管理等、常用工具。

5 优势概述

提供了业界领先的安全配置检查管理方案，其主要优势体现在于：

5.1 配置变更的自动分析

支持定期的配置收集和审计，实现了人工评估的自动化和常态化。

5.2 简便易用的界面风格

系统通过提供入门向导、个人工作台、任务通知、快捷菜单等方式，为用户提供了简单易用的界面，即使是初次使用系统，也完全能在较短的时间内掌握。

5.3 灵活通用的系统设计

从产品设计角度而言，系统具有极大的灵活性，主要体现在如下几个方面：

1. 可扩展的安全配置检查项
2. 可配置的安全仪表板
3. 可配置的系统功能菜单
4. 支持用户自定义的检查策略和告警策略
5. 支持灵活的部署方式

5.4 极度快速的处理性能

快速检查，而且网络占用带宽小。