# 聚铭安全管理中心产品白皮书



**南京聚铭网络科技有限公司**

2019 年 4 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

全国客服电话：400-1158-400

# 目录

# 1. 信息安全集中管理的必然性

信息安全是 IT 领域的重要分支，它不是单纯的 IT 技术的堆砌，而是集信息学、密码学、管理学、心理学、社会学等多种学科的交叉科学，因此人们对于信息安全的认识也是沿着比较复杂的轨迹发展而来的：

## 1.1. 由简单到复杂

对于一般的组织或企业，和信息安全技术开始有交集总是不可避免地从防毒/杀毒、防火墙、入侵检测（所谓信息安全“老三样”）等基础的系统或设备开始的，故到目前为止，在很多人的概念中，信息安全就是计算机病毒、防火墙、入侵检测。

但随着信息技术持续地发展，各类组织、企业对信息系统的运用也不断深入，为了在复杂条件下应付各类安全情况（如黑客的攻击、内部员工的有意或无意地进行越权或违规操作），企业部署了大量的、不同种类、形态各异的信息安全产品：

- 为了监控黑客的攻击控制，部署了各种入侵检测或入侵防御设备；
- 为了控制内部员工的非法接入部署了网终端管理、网络准入等系统；
- 为了控制数据的非法泄露或重要数据被修改，部署了防泄漏系统、数据库审计系统、日志审计等系统。

## 1.2. 由部分到全面

为了应对日益复杂的信息安全形式，各类组织、企业从最初的、单纯的进行边界安全控制，转而逐渐地向全面地信息安全管控发展，这表现在：

- 不仅注重内外边界安全，也重视内部不同安全区域之间的安全；
- 不仅注重网络的安全，也重视系统（包括应用系统）的安全；
- 不仅注重 IT 技术的安全，更重视数据、内容的安全。

## 1.3. 由被动防御到主动发现

各类组织或企业在实施信息安全伊始，总是处于被动防御状态。如发现网络中存在病毒则实施防病毒系统、在发现网络风暴则被动部署流量异常检测及入侵检测设备、在发现有关键数据被非法读取或下载/修改则实施日志审计系统或数据库审计系统等等，不一而足，总是无法做到事前防御或防范；但随着信息安全工作的逐步深入，组织或企业的决策层开始意识到主动发现的重要性，于是又开始部署漏洞检查、代码检查等系统或工具，试图扭转在信息安全领域总是处于被动挨打的局势。

另外，各个行业领域也逐渐将信息安全与 IT 信息系统的规划、实施、运维同步进行，实现所谓“三同步”，这就要求信息安全工作具备较强的前瞻性和预见性。

综上所述，随着信息安全的发展，集中、综合的安全管理需求越来越突出，这也是业界近年来经常提到的，信息安全其实是“三分技术，七分管理”，这些需求集中表现在：

- IT 技术的不断升级换代，企业部署的安全设备或系统越来约多，这些种类繁多、分散部署的安全产品带来了巨大的管理问题；
- 不同种类的设备或系统产生了海量事件，人们需要有信息安全管理系统来统筹分析、过滤或关联；
- 各类组织或企业对信息安全存在大量的安全合规需求，如等级保护、萨班斯法案等，现有的各种安全产品无法满足这样的需求，故必须有一个管理系统方可进行；
- 各级组织、企业亟需建立统一的、全面的安全管理体系以满足外部或内部的迫切要求。以应对信息安全管理中对于以下内容的需求：
  - 各类安全策略管理和贯彻执行的支撑；
  - 安全组织架构的管理；
  - 安全人员的调度、培训和考核；
  - 各种安全管理流程的流转；
  - 安全事件的监控和应急处理、总结和汇报；
  - 安全系统和对象的全生命周期管理；
  - 各种安全设备的管控。

因此建立一个完整的、统一的安全管理中心就成为各类组织、企业的必然要求。

# 2. 安全管理中心的职能

安全管理中心是协助用户实现安全策略管理、安全组织管理、安全运作管理和安全技术框架的中心枢纽。安全管理中心是一种安全管理的形式，它的职能分成管理层面和技术层面。它的存在能有效地将企业的策略管理、安全组织管理、安全运维管理和安全技术框架结合在一起。


*图 1 安全管理中心的作用*

安全管理中心的主要职能包括：

**风险管理：**全面收集信息资产的漏洞和相关事件，通过关联分析去除各种误报，发现有用信息，给出级别度量。系统能够自动完成以往需专家完成的风险计算工作，并自动触发任务单和响应来降低风险，达到管理和控制风险的效果。

**运维管理：**该中心提供日常运维工作的服务保障体系；包括各种资产配置库、安全知识管理、流程管理实现等；例如工单管理用于追踪风险和事故的处理情况；例如预警管理可以实现主动的预警，通过企业安全管理中心和各个安全服务供应商共同合作，形成一条完整的预警处理链，可以保证在漏洞出现还未被利用前就送达各个管理员并保证被采取了应对的措施；还有通过对日常工作的评价来促使我们找到如何提高安全水平的方法。

**专业安全系统：**安全管理中心还提供各种专项的安全集中管理功能来保证用户对某些专门安全问题的管理，例如安全事件管理、安全基线管理、漏洞管理等。

**接口：**安全管理中心不会独立于整个企业的 IT 管理系统独立运行，整个维护运作组织也是整个企业维护运作组织的一部分，安全管理中心充分考虑企业内部 IT 系统融合的需求，提供各类灵活接口。

# 3. 安全管理中心功能概述

## 3.1 概述

安全管理中心是由综合展现层、业务功能层、综合分析层、专项管理层、采集层以及接口等部分组成，如下图所示：

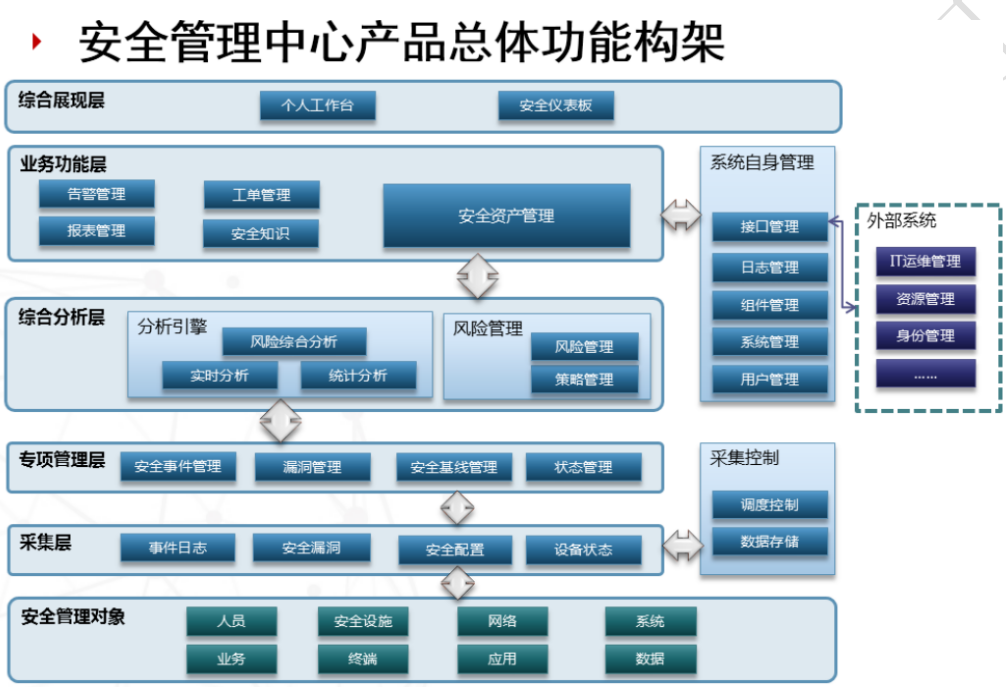



*图 2 安全管理中心产品功能架构*

在安全管理中心中，Web 主要由安全仪表板、个人工作台、资产管理、风险管理、告警管理、安全事件管理、漏洞管理、安全基线管理、报表管理、知识库管理、工单管理、系统管理组成。下面的章节会较为详尽地介绍每个部分。

## 3.2 安全仪表板

安全仪表板是聚铭安全管理中心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。

默认出厂，安全管理中心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. 安全事件概况；

5. 脆弱性概况；

6. 任务概况；

7. 工单概况。

## 3.3 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（漏洞扫描、基线检查、资产发现）；

2. 个人待办事宜：工单、告警；

3. 通知功能：任务完成情况、工单情况；

4. 系统状态:每秒事件量（EPS）。

## 3.4 资产管理

安全资产是安全管理中心的核心管理对象。与 ISO27001 的关于资产的定义略有不同，安全管理中心的资产是特指具有 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、安全基线检查等使用）、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、安全事件、漏洞、安全基线违规问题等。

安全管理中心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，安全管理中心还支持对于网络和 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，安全管理中心支持用户自定义资产管理视图。

## 3.5 拓扑管理

拓扑管理中提供了丰富的图元和工具，让用户可以编辑出多种多样的拓扑图。

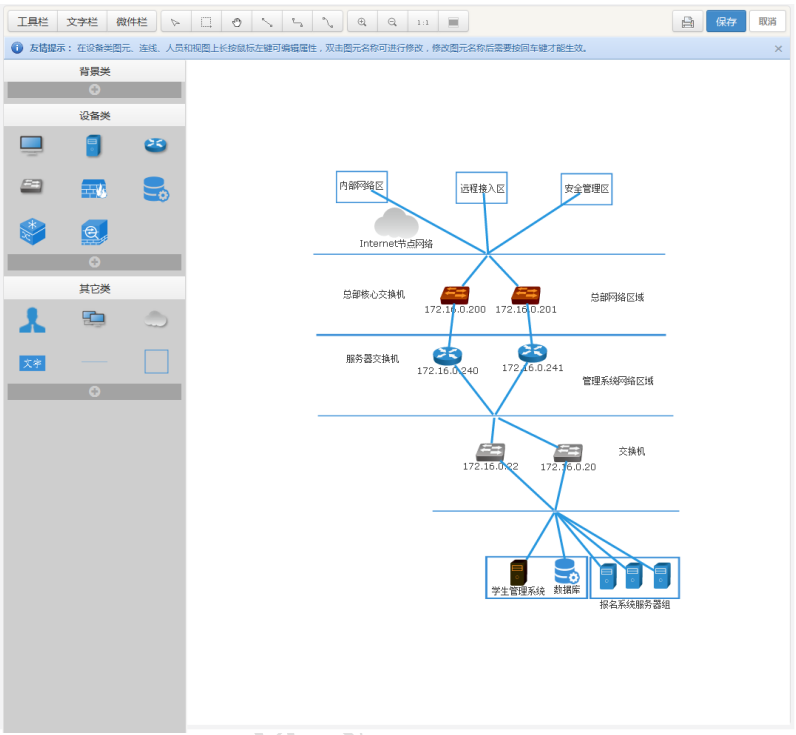
➢ 工具包括：点选模式、框选模式、浏览模式、普通连线、折线、曲线、

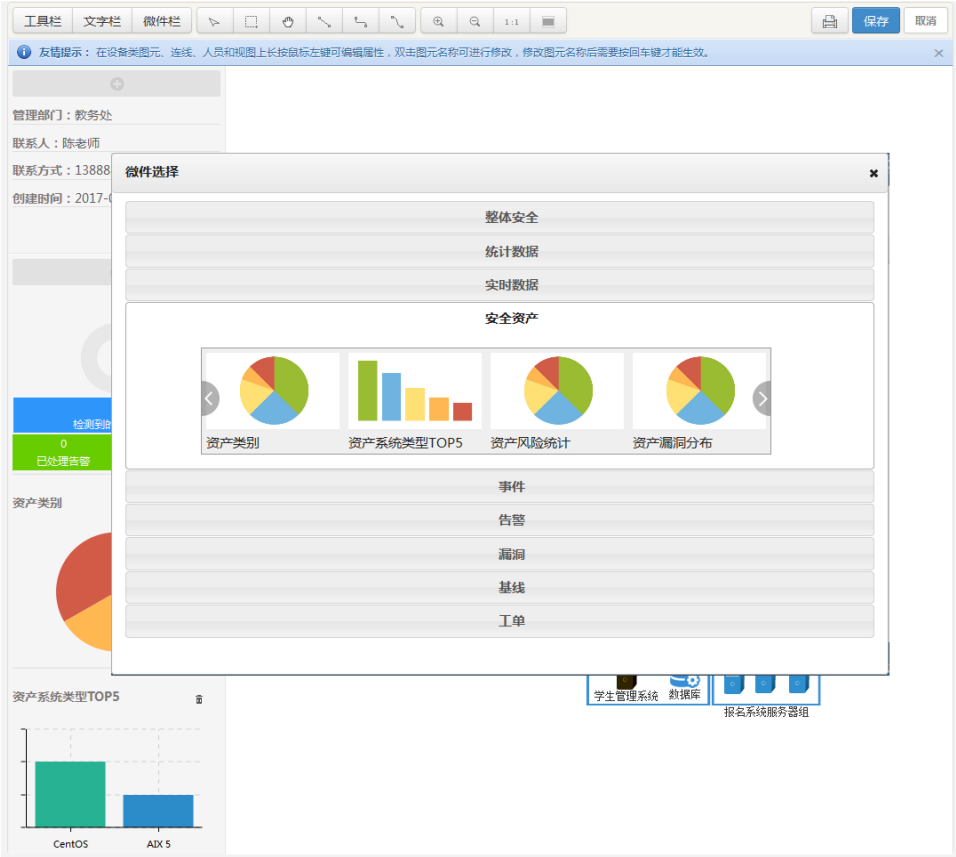
放大、缩小、1 比 1 展示、纵览展示、导出图片和打印预览。

➢图元分为：背景类、设备类和其它类三大类，系统自带部分图元，同时支持用户自己上传。设备类图元可绑定资产，其它类中的人员可绑定系统中的用户信息，其它类中的视图图元可绑定系统中的视图信息。

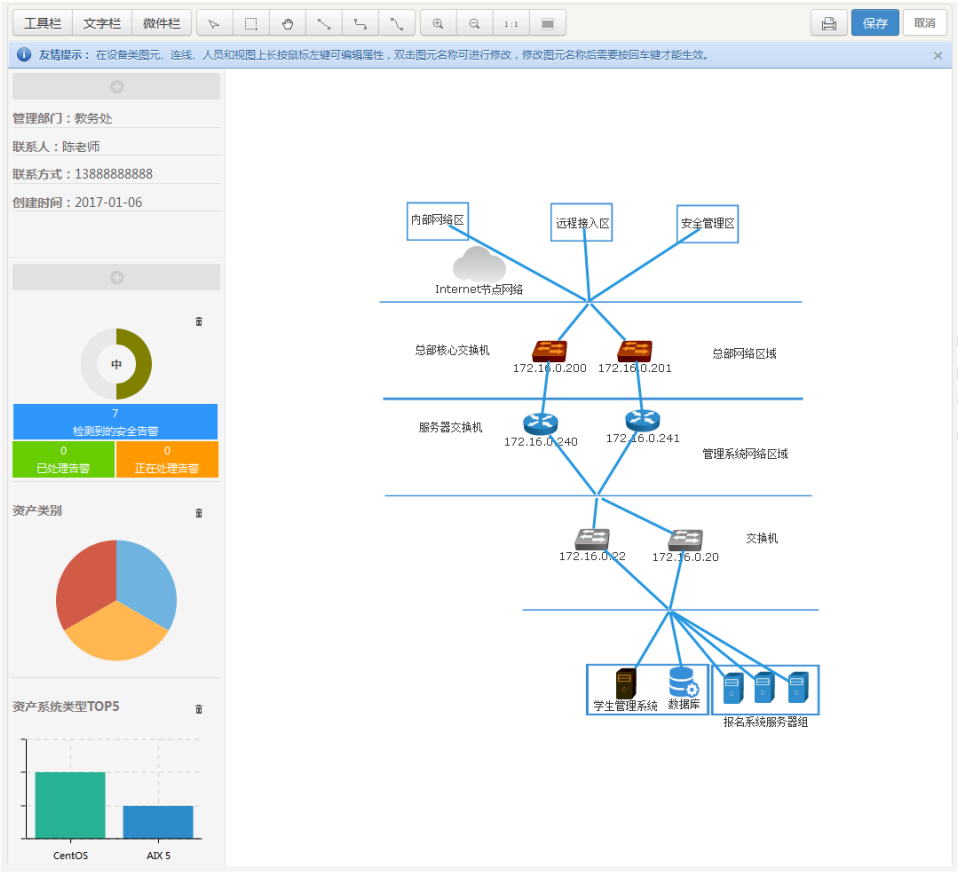
➢端口信息配置：拓扑图中的连线中可配置连线两端的设备的端口信息。

➢子拓扑图配置：除设备类和背景类图元外，其它图元都可以创建下一级拓扑图。






拓扑管理中，用户可根据需要在左侧添加文字信息和微件信息，添加后效果如下图所示：




## 3.6 预警管理

所谓预警是指根据权威机构发布的相关信息安全警告，对系统内可能存在警告中出现的问题进行通知。

聚铭安全管理中心支持以手工和自动方式创建预警，其中自动预警可根据各类安全问题产生的覆盖范围生成。

## 3.7 风险管理

风险管理以资产为视角进行管理，根据风险的来源不同，风险主要有：资产风险、安全事件风险、漏洞风险、安全基线风险、设备状态风险。

在聚铭安全管理中心，风险的主要来源为各类安全问题所产生的告警（告警由相关的策略生成）；另外，风险的高低还依赖于相关资产的重要程度，即资产价值。

安全管理中心内的资产价值来源于如下三个属性的综合计算：

1. 机密性（Confidentiality）

根据资产机密性属性的不同，将它分为 5 个不同的等级，分别对应资产在机密性方面的价值或者在机密性方面受到损失时对资产价值的影响，分别是很高（VH）、高（H）、中等（M）、低（L）、可忽略（N），并且从高到低

分别赋值 1-5。

2. 完整性（Integrity）

根据资产完整性属性的不同，将它分为 5 个不同的等级，分别对应资产在完整性方面的价值或者在完整性方面受到损失时对资产价值的影响，分别是很高（VH）、高（H）、中等（M）、低（L）、可忽略（N），并且从高到低分别赋值 1-5。

3. 可用性（Availability）

根据资产可用性属性的不同，将它分为 5 个不同的等级，分别对应资产在可用性方面的价值或者在可用性方面受到损失时对资产价值的影响。分别很高（VH）、高（H）、中等（M）、低（L）、可忽略（N），并且从高到低分别赋值 1-5。

### 3.7.1. 资产风险

以资产及其相关视图为视角，将资产关联的风险问题用列表的方式呈现。

资产风险情况的列表显示风险统计视图——包括近期风险趋势图和当前资产风险级别分布图；按列表方式显示资产风险情况，默认按风险级别从高到低排序。

通过点击资产可以查看资产风险信息，包括资产当日安全事件的分布情况（按级别、类型）、漏洞严重级别分布情况和安全基线违规严重级别分布情况。查看的方式，就是用资产为查询条件，搜索当前资产上存在的安全问题，给出详细的描述。

可查看的安全问题包括：

1. 与资产相关的告警；
2. 相关日志或事件；
3. 与资产相关的漏洞；
4. 与资产相关的安全配置；
5. 与资产相关的设备状态；
6. 与资产相关的端口/服务情况。

### 3.7.2. 安全事件风险

可进行安全事件的事件查看、查询，并呈现风险的统计情况。主要包括事件

的严重级别分布、事件类型的统计等。

可根据条件，对安全事件进行浏览和查询，可看到的安全事件属性有：事件名称、类型、子类、严重级别、源地址、目的地址、发生时间，以及其关联的资产地址等；查询的结果可以导出。

系统支持基础、高级和专家模式的查询，用户可将查询的条件进行保存，待今后使用。

### 3.7.3. 安全漏洞风险

可进行安全漏洞的查看和查询，呈现风险的统计情况。主要包括漏洞的严重级别分布、漏洞类型的统计、漏洞的端口统计和趋势统计等。

可根据条件，对安全漏洞进行浏览和查询，可看到的安全漏洞属性有：漏洞名称、端口、端口类型、严重级别、以及其关联的资产对象。

对于漏洞可以进行知识库的查询。

### 3.7.4. 安全基线违规风险

可进行安全基线违规的查看和查询，呈现风险的统计情况。主要包括违规项的严重级别分布、类型的统计和趋势统计等。

可根据条件，对违规基线进行浏览和查询，可看到的安全基线属性有：基线名称、基线编号、基线的系统类型、以及其关联的资产对象数量。

对于违规基线可以进行知识库的查询。

### 3.7.5. 设备状态风险

可进行设备状态的查看和查询。主要包括设备运行情况、健康情况等。提供了针对设备状态的统计信息，健康状态的分布情况等。

设备状态主要属性有：连通性、连续运行时间、CPU、内存、硬盘、流量等。

## 3.8. 告警管理

所谓告警是指用户特别需要关注的安全问题，这些问题来源于安全事件、安全基线违规、高危漏洞、高危端口开放等。

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、暂存数据（用户可以将数据保存在临时表中作为其它策略的输入）等。

## 3.9. 安全事件管理

安全事件管理主要完成对事件的集中收集、管理和分析。主要的功能包括事件收集、事件集中处理。

### 3.9.1. 事件收集

事件收集主要是对事件采集和格式化的过程。

安全管理中心能够支持以下事件源：

1. 防病毒、防火墙、入侵检测/防御系统等安全设备或系统；
2. 操作系统记录的重要安全相关的日志和事件告警，支持 Windows 2000/2003/NT/XP/Vista/7/2008/8，各种版本的 Linux/Unix 系统；
3. 各种类型的数据库日志，例如 Oracle、MySQL 等；
4. 防病毒系统、访问控制系统、用户集中管理和认证系统；
5. 各种应用系统的日志，如 Apache、Tomcat、IIS 等。

安全管理中心能够通过多种方式收集、分析各事件源发送的安全事件：

1. Syslog 方式：以 Syslog 方式接收安全事件；
2. SNMP trap：接收来自设备的 SNMP Trap 的事件；

3. 数据库方式：可以通过 JDBC 数据库接口获取事件源存放在各种数据库中的安全相关信息；支持的数据库类型包括 Oracle、Microsoft SQLServer、DB2、MySQL 和 Sysbase；
4. 网络 Socket 接口方式：可以通过 TCP/IP 网络，以 Socket 通信的方式获得安全事件；
5. 本地文件方式：可以通过读取事件源的日志文件，来获取其中与安全有关的信息；
6. 第三方代理或者应用程序：第三方的应用程序或者代理可以通过以上方式或者标准输出直接将安全事件转发给安全事件采集。

### 3.9.2. 事件处理

事件处理主要负责对事件进行标准化、集中存储、合并和统计；另外，安全管理中心提供了丰富的事件脚本定义语言，能定义任何符合用户需求的策略。

## 3.10. 漏洞管理

所谓漏洞是脆弱性的一个子集，专指可通过扫描器发现的脆弱性，其中部分具有国际上标准的 CVE 编号；而如企业没有安全管理负责人之类的脆弱性则不被认为是漏洞。

安全管理中心内置扫描器，支持分布式的漏洞扫描模式以及集中的漏洞分析和处理。

在漏洞管理中，能够集中查看、统计系统存在的系统漏洞，以及目标网页所存在的 Web 漏洞。还可以制定扫描策略及任务，对系统内安全资产进行一次或周期性的扫描。

系统支持设置 IPv4 地址段或选择资产的方式扫描对象；也可以支持对单个 IPv6 地址对象扫描。

漏洞管理主要分以下模块：

1. 漏洞查看：列表查看登录用户权限范围存在的漏洞，显示某漏洞在哪些资产上存在（列表中显示相关资产数量，点击可查看具体哪些资产存在此漏洞）；可显示相关漏洞的全部详细情况；
2. 扫描任务管理：漏洞任务管理包括三个部分：正在执行的任务、已定义的任务和任务执行的结果，即漏洞扫描报告，报告可以导出为 Word、

PDF 等格式；对于正在执行的任务用户可以停止、暂停或继续任务的执行；

3. 扫描策略管理：用户可以自定义漏洞扫描策略（通过选择系统内存在的插件）。

安全管理中心还提供扫描插件的升级。

## 3.11. 安全基线管理

在安全管理中心中，安全基线是指各类系统、设备的安全配置标准；而安全基线的违规问题是指实际的系统或设备的配置违反了基线的要求。例如是否存在不允许的用户账号、账号的口令策略存在一定问题（不满足复杂度、长度、更改时间的要求）等等。

安全基线管理的作用主要体现在如下几个方面：

1. 安全评估工作常态化；
2. 有利于提高设备自身防护的能力；
3. 为安全风险评估提供基础材料。

安全基线可被划分为账号类、口令类、授权类、日志配置类、路由配置类等等，例如：应删除或锁定与设备运行、维护等工作无关的账号等。

目前，安全管理中心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；
4. 主流数据库；
5. 主流 Web 中间件。

安全基线管理主要分以下模块：

1. 安全基线违规问题查看：列表查看登录用户权限范围存在的安全基线违规问题，显示某违规问题在哪些资产上存在；

2. 安全基线检查任务管理：任务管理包括三个部分：正在执行的任务、已定义的任务和任务执行的结果，即检查报告，报告可以导出为 Word、PDF、HTML 等格式；

3. 策略管理：用户可以自定义基线检查策略。可通过选择系统内的基线项进行组合。另外可设定用户自定义基准值，例如口令长度要求等。

## 3.12. 工单管理

工单是安全管理中心用于安全问题处理的一种形式，是安全运维支撑的流程体现。

当系统产生告警后，用户可以创建工单并分配给专人去处理。工单的状态包括待接受、处理中、已完成、求助、已关闭和作废等；而个人工单完成情况是供用户查看工单各种状态的分类信息。

下图说明了一个工单的基本处理流程：

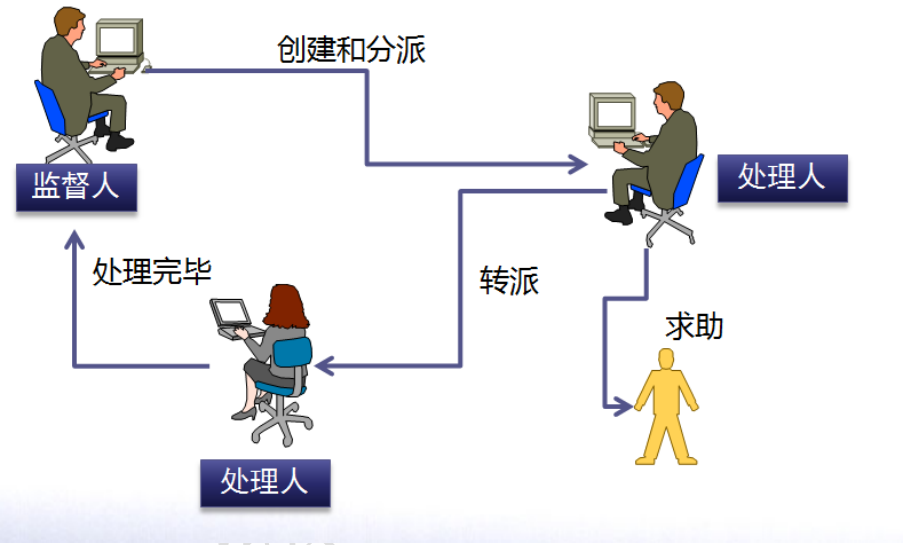



*图 3 安全管理中心的工单管理流程*

## 3.13. 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、安全事件报表、漏洞报表、安全基线报表、工单报表等。

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，如下图所示：

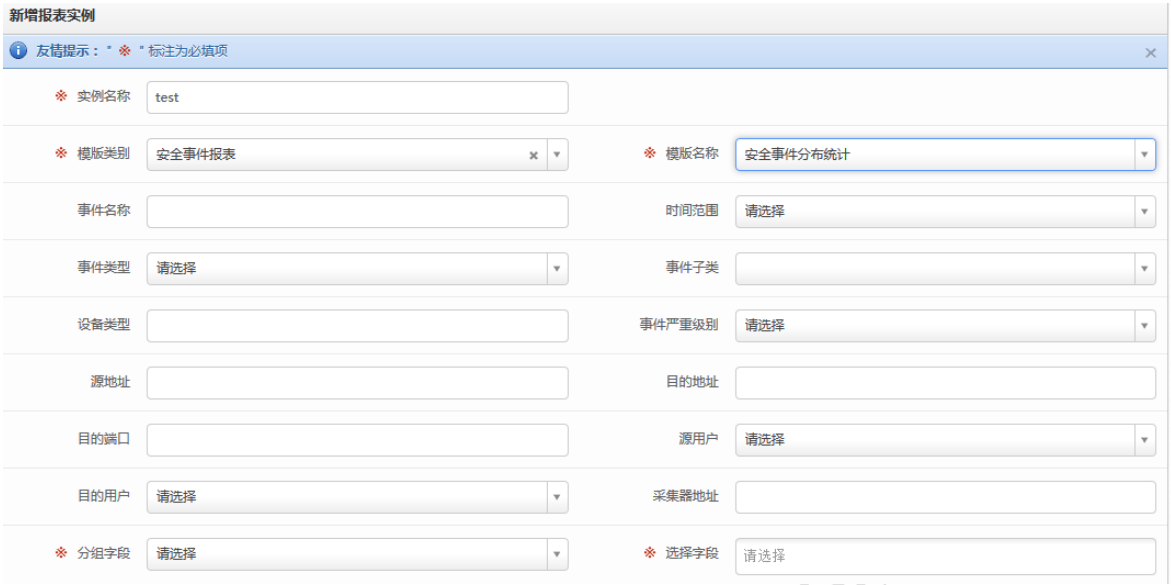



*图 4 安全管理中心的报表管理*

## 3.14. 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. 配置类：各种操作系统、网络设备、应用系统及数据库等接入安全管理平台日志的配置收集方法；

2. 安全事件/日志类：各种安全系统的报警以及操作系统、网络设备、服务器及数据库的日志信息；

3. 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；

4. 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；

5. 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。

## 3.15. 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。

# 4. 产品优势

聚铭网络提供了业界领先的安全管理中心方案，其主要优势体现在于：

## 4.1. 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，即使是初次使用安全管理中心，也完全能在较短的时间内掌握。

## 4.2. 灵活通用的系统设计

从产品设计角度而言，安全管理中心具有极大的灵活性，主要体现在如下几个方面：

1. 可配置的系统功能菜单；
2. 支持用户自定义的检查策略和关联策略；
3. 灵活的安全事件标准化脚本；
4. 可扩展的安全基线和漏洞扫描功能；
5. 方便的第三方接口。

## 4.3. 全面强大的分析能力

支持基于规则和基于统计的关联分析，支持多种数据来源和响应方式，能够基于资产进行综合风险分析和计算。

## 4.4. 多级分布的部署方式

支持多级数据交互或者同步。同时安全管理中心建立了灵活的授权体系，不同群体之间互不影响，感觉就像在使用一套独立的系统。

## 4.5. 极度快速的处理性能

支持极高的事件处理速度，支持分布式采集、集中处理和存储。

## 4.6. 扫描引擎的一体化方案

通过内置扫描器，将传统的扫描工具上升到基于资产的漏洞管理的高度，通过安全管理中心解决方案的强大功能获得了企业级的漏洞管理、维护和关联功能。

## 4.7. 配置基线的自动分析

支持定期的配置收集和审计，实现了人工评估的自动化。

# 5. 南京聚铭网络科技有限公司简介

南京聚铭网络科技有限公司(Nanjing Juming Network technology Co.,Ltd)，是国内领先的安全产品提供商和安全运营商、“**双软企业**”、“**高新技术企业**”、“**江苏省民营科技企业**”、“**创业南京” 高层次创业人才企业**，服务于“能源、电信、教育、金融、政府、军工、医疗、公安”等多个行业。公司通过了 **ISO9001、ISO20000、ISO27001** 等众多的标准体系认证，“**聚铭综合日志分析系统**”**荣获江苏省软件产品金慧奖、南京市新兴产业重点推广应用的新产品，**公司始终秉承“真诚合作、互利共赢、优势共享，服务客户”的经营理念、先进的技术、优秀的产品和专业的配套服务，引领国内安全的发展方向。

为掌握核心科技，公司投入了大量的科研经费，先后成立了“**聚铭安全攻防实验室**”和“**智库评价和数据科学联合实验室**”两大科学研究和应用研究实验室。其中：“数据科学联合实验室”为本公司与南京大学中国智库研究和评价中心联合成立，专业从事于数据科学相关的理论研究和应用研究方向。“聚铭安全攻防实验室”专业从事于信息安全攻防应用研究方向。

公司现有团队超过一半以上的人员具有十年以上的安全产品研究、开发以及安全数据分析、运营、服务的经验；公司坚持技术自主创新，以产品服务为中心，以满足客户业务需求为目标，凭借多年的客户服务经验，构建了安全产品、安全运营、大数据分析平台及服务等系列产品和服务，以满足不同用户的需要。

未来，公司将继续致力于引领大数据、信息安全产业的发展，应对大数据和信息安全领域更趋日新月异的挑战。