铱迅安全运营中心

管理员手册

南京铱迅信息技术股份有限公司

Nanjing YXLink Information Technology Co. Ltd.

注意

- 未经南京铱迅信息技术股份有限公司（Nanjing Yxlink Information Technology Co.,Ltd.，简称：铱迅信息）的事先书面许可，对本产品附属的相关手册之所有内容，不得以任何方式进行翻版、传播、转录或存储在可检索系统内，或者翻译成其他语言。
- 本手册没有任何形式的担保、立场表达或其他暗示。若有任何因本手册或其所提到之产品信息，所引起直接或间接的数据流失、利益损失或事业终止，铱迅信息不承担任何责任。
- 铱迅信息保留可随时更改手册内所记载之硬件及软件规格的权利，而无须事先通知。
- 本公司已竭尽全力来确保手册内载信息的准确性和完善性。如果您发现任何错误或遗漏，请向铱迅信息反映。对此，我们深表感谢。

商标信息

本手册中所谈及的产品名称仅做识别之用，而这些名称可能属于其他公司的注册商标或是版权，其他提到的商标，均属各该商标注册人所有，恕不逐一列明。

目录

获得帮助

获取网络安全相关资料可以访问铱迅信息网站：http://www.yxlink.com

获取铱迅安全运营中心的最新相关信息可以访问网址：

http://www.yxlink.com/products-waf.html

如需获取更详尽的铱迅信息网络安全专业服务信息、商务信息，您可通过如下方式和我们取得联系：

地址：江苏省南京市雨花台区宁双路 18 号沁恒科技园 D 幢 4 层

邮编：210012

服务热线：400-097-5557

电话：025-83235296，025-83235396，025-58722055

传真：025-83235296，025-83235396 转 601

网站：http://www.yxlink.com

Email：info@yxlink.com

格式与名词约定

设备、产品、系统——除非特指，本手册中均表示铱迅安全运营中心（也称：铱迅 SOC）

1. 概述

1.1. 什么是信息安全管理

1.1.1. 信息安全

信息安全：是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

1.1.2. 信息安全的目标

信息安全管理的目标就是保证被保护对象的：

1. 真实性：对信息的来源进行判断，能对伪造来源的信息予以鉴别
2. 完整性：保证数据的一致性，防止数据被非法用户篡改
3. 保密性：保证机密信息不被窃听，或窃听者不能了解信息的真实含义
4. 可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝
5. 不可抵赖性：建立有效的责任机制，防止用户否认其行为
6. 可控制性 ：对信息的传播及内容具有控制能力
7. 可审查性 ：对出现的网络安全问题提供调查的依据和手段

1.1.3. 信息安全管理体系

信息安全管理体系：是组织在整体或特定范围内建立信息安全方针和目标，以及完成这些目标所用方法的体系。它是直接管理活动的结果，表示成方针、原则、目标、方法、过程、核查表（Checklists）等要素的集合。

1.2. 信息安全管理体系要素

信息安全管理体系至少包含如下要素：

1. 信息安全管理策略制定：信息安全的顶层设计
2. 信息安全标准制定：包括各类与信息安全相关的规定、规范及标准
3. 信息安全合规建设：组织内部信息安全建设的相关符合性情况，包括与国际标准、国内标准、行业标准及企业标准相关策略、规范的符合程度，这是一个循序渐进的过程
4. 信息安全人员的管理和培训：建设信息安全组织机构；人员安全管理，如持证上岗等；培训。

5. 信息安全应急响应处理
6. 信息安全架构建设：涉及到应用安全架构、数据安全架构、系统安全架构、网络安全架构、底层安全策略
7. 信息安全档案管理：一般指资产管理
8. 安全监控

1.2.1. 国内外安全管理体系

国内外有许多关于安全管理体系的标准或规范，下文仅介绍最为常见的三个。

1.2.1.1. ISO27001

信息安全管理实用规则 ISO/IEC27001 的前身为英国的 BS7799 标准，该标准由英国标准协会（BSI）于 1995 年 2 月提出，并于 1995 年 5 月修订而成的。1999 年 BSI 重新修改了该标准。BS7799 分为两个部分：

BS7799-1，信息安全管理实施规则

BS7799-2，信息安全管理体系规范。

第一部分对信息安全管理给出建议，供负责在其组织启动、实施或维护安全的人员使用；第二部分说明了建立、实施和文件化信息安全管理体系（ISMS）的要求，规定了根据独立组织的需要应实施安全控制的要求。

2000 年，国际标准化组织（ISO）在 BS7799-1 的基础上制定通过了 ISO 17799 标准。BS7799-2 在 2002 年也由 BSI 进行了重新的修订。ISO 组织在 2005 年对 ISO 17799 再次修订，BS7799-2 也于 2005 年被采用为 ISO27001:2005。

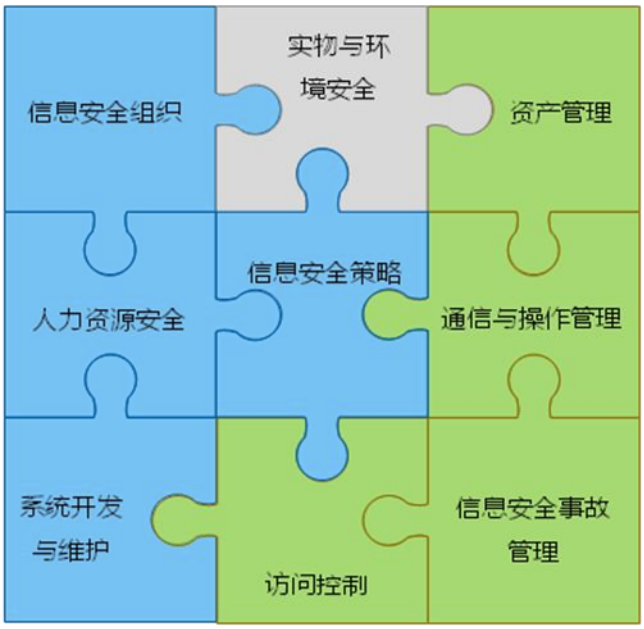
标准的主要内容：

ISO/IEC17799-2000 (BS7799-1) 对信息安全管理给出建议，供组织启动、实施或维护安全的人员使用。该标准为开发组织的安全标准和有效的安全管理做法提供公共基础，并为组织之间的交往提供信任。

标准指出“象其他重要业务资产一样，信息也是一种资产”。它对一个组织具有价值，因此需要加以合适地保护。信息安全防止信息受到的各种威胁，以确保业务连续性，使业务受到损害的风险减至最小，使投资回报和业务机会最大。

信息安全是通过实现一组合适控制获得的。控制可以是策略、惯例、规程、组织结构和软件功能。需要建立这些控制，以确保满足该组织的特定安全目标。

ISO/IEC17799-2000 包含了 127 个安全控制措施来帮助组织识别在运作过程中对信息安全有影响的元素，组织可以根据适用的法律法规和章程加以选择和使用，或者增加其他附加控制。国际标准化组织（ISO）在 2005 年对 ISO 17799 进行了修订，修订后的标准作为 ISO 27000 标准族的第一部分——ISO/IEC 27001，新标准去掉 9 点控制措施，新增 17 点控制措施，并重组部分控制措施而新增一章，重组部分控制措施，关联性逻辑性更好，更适合应用；并修改了部分控制措施措辞。修改后的标准包括 11 个章节，如下图所示：



具体如下：

1. 安全策略：指定信息安全方针，为信息安全提供管理指引和支持，并定期评审。
2. 信息安全的组织：建立信息安全管理组织体系，在内部开展和控制信息安全的实施。
3. 资产管理：核查所有信息资产，做好信息分类，确保信息资产受到适当程度的保护。
4. 人力资源安全：确保所有员工，合同方和第三方了解信息安全威胁和相关事宜以及各自的责任，义务，以减少人为差错，盗窃，欺诈或误用设施的风险。
5. 物理和环境安全：定义安全区域，防止对办公场所和信息的未授权访问，破坏和干扰；保护设备的安全，防止信息资产的丢失，损坏或被盗，以及对企业业务的干扰；同时，还要做好一般控制，防止信息和信息处理设施的损坏和被盗。
6. 通信和操作管理：制定操作规程和职责，确保信息处理设施的正确和安全操作；建立系统规划和验收准则，将系统失效的风险降到最低；防范恶意代码和移动代码，保护软件和信息的完整性；做好信息备份和网络安全管理，确保信息在网络中的安全，确保其支持性基础设施得到保护；建立媒体处置和安全的规程，防止资产损坏和业务活动的中断；防止信息和软件在组织之间交换时丢失，修改或误用。
7. 访问控制：制定访问控制策略，避免信息系统的非授权访问，并让用户了解其职责和义务，包括网络访问控制，操作系统访问控制，应用系统和信息访问控制，监视系统访问和使用，定期检测未授权的活动；当使用移动办公和远程控制时，也要确保信息安全。
8. 系统采集、开发和维护。标示系统的安全要求，确保安全成为信息系统的内置部分，控制应用系统的安全，防止应用系统中用户数据的丢失，被修改或误用；通过加密手段保护信息的保密性，真实性和完整性；控制对系统文件的访问，确保系统文档，源程序代码的安全；严格控制开发和支持过程，维护应用系统软件和信息安全。
9. 信息安全事故管理：报告信息安全事件和弱点，及时采取纠正措施，确保使用持续有效的方法管理信息安全事故，并确保及时修复。

10. 业务连续性管理：目的是为减少业务活动的中断，是关键业务过程免收主要故障或天灾的影响，并确保及时恢复。
11. 符合性：信息系统的设计，操作，使用过程和管理要符合法律法规的要求，符合组织安全方针和标准，还要控制系统审计，使信息审核过程的效力最大化，干扰最小化。

1.2.1.2. ISO13335

ISO13335 是一个信息安全管理指南，这个标准的主要目的就是要给出如何有效地实施 IT 安全管理的建议和指南。该标准目前分为 5 个部分：

1. IT 安全的概念和模型（Concepts and Models for IT Security），该部分包括了对 IT 安全和安全管理的一些基本概念和模型的介绍
2. IT 安全的管理和计划（Managing and Planning IT Security），这个部分建议性地描述了 IT 安全管理和计划的方式、要点
3. IT 安全的技术管理（Techniques for the Management of IT Security），覆盖了风险管理技术、IT 安全计划的开发以及实施和测试，还包括一些后续的制度审查、事件分析、IT 安全教育程序等
4. 防护的选择（Selection of safeguards），它是最新发布的一个部分，主要探讨如何针对一个组织的特定环境和安全需求来选择防护措施，这些措施不仅仅包括技术措施
5. 外部联接的防护（Safeguards for external connections）。

1.2.1.3. 信息安全等级保护

信息安全等级保护是对信息和信息载体按照重要性等级分级别进行保护的一种工作，在中国、美国等很多国家都存在的一种信息安全领域的工作。在中国，信息安全等级保护广义上为涉及到该工作的标准、产品、系统、信息等均依据等级保护思想的安全工作；狭义上一般指信息系统安全等级保护，是指对国家安全、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置的综合性工作。

信息安全等级包括如下五级：

1. 第一级：用户自主保护级

本级的计算机信息系统可信计算基通过隔离用户与数据，使用户具备自主安全保护的能力。它具有多种形式的控制能力，对用户实施访问控制，即为用户提供可行的手段，保护用户和用户组信息，避免其他用户对数据的非法读写与破坏。

2. 第二级：系统审计保护级

与用户自主保护级相比，本级的计算机信息系统可信计算基实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。

数据完整性

计算机信息系统可信计算基通过自主完整性策略，阻止非授权用户修改或破坏敏感信息。

3. 第三级：安全标记保护级

本级的计算机信息系统可信计算基具有系统审计保护级所有功能。此外，还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出 信息的能力；消除通过测试发现的任何错误。

自主访问控制

计算机信息系统可信计算基定义和控制系统中命名用户对命名客体的访问。实施机制（例如：访问控制表）允许命名用户以用户和（或）用户组的身份规定并控制客体的共享；阻止非授权用户读取敏感信息。并控制访问权限扩散。没有存取权的用户只允许由授权用户指定对客体的访问权。阻止非授权用户读取敏感信息。

强制访问控制

计算机信息系统可信计算基对所有主体及其所控制的客体（例如：进程、文件、段、设备）实施强制访问控制。为这些主体及客体指定敏感标记，这些标记是等级分类和非等级类别的组合。计算机信息系统可信计算基控制的所有主体对客体的访问应满足：仅当主体安全级中的等级分类低于或等于客体安全级中的等级分类计算机信息系统可信计算基使用身份和鉴别数据，鉴别用户的身份，并保证用户创建的计算机信息系统可信计算基外部主体的安全级和授权受该用户的安全级和授权的控制。

身份鉴别

计算机信息系统可信计算基维护用户身份识别数据并确定用户访问权及授权数据计算机信息系统可信计算基使用这些数据鉴别用户身份，计算机信息系统可信计算基能够使用用户对自己的行为负责。

数据完整性

计算机信息系统可信计算基通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。在网络环境中，使用完整性敏感标记来确信信息在传送中未受损。

4. 第四级：结构化保护级

本级的计算机信息系统可信计算基建立于一个明确定义的形式化安全策略模型之上，它要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。本级的计算机信息系统可信计算基必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算基的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。加强了鉴别机制；支持系统管理员和操作员的职能；提供可信设施管理；增强了配置管理控制。系统具有相当的抗渗透能力。

强制访问控制

为这些主体及客体指定敏感标记计算机信息系统可信计算基支持两种或两种以上成分组成的安全级。计算机信息系统可信计算基使用身份和鉴别数据，鉴别用户的身份，保护用户创建的计算机信息系统可信计算基外部主体的安全级和授权受该用户的安全级和授权的控制。

隐蔽信道分析

系统开发者应彻底搜索隐蔽存储信道，并根据实际测量或工程估算确定每一个被标识信道的最大带宽。

可信路径

对用户的初始登录和鉴别，计算机信息系统可信计算基在它与用户之间提供可信通信路径。该路径上的通信只能由该用户初始化。

5. 第五级：访问验证保护级

本级的计算机信息系统可信计算基满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算基在其构造时，排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最小程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。

自主访问控制

计算机信息系统可信计算基定义并控制系统中命名用户对命名客体的访问。实施机制（例如：访问控制表）允许命名用户和（或）以用户组的身份规定并控制客体的共享；阻止非授权用户读取敏感信息。并控制访问权限扩散。

自主访问控制机制根据用户指定方式或默认方式，阻止非授权用户访问客体。访问控制的粒度是单个用户。访问控制能够为每个命名客体指定命名用户和用户组，并规定他们对客体的访问模式。没有存取权的用户只允许由授权用户指定对客体的访问权。

强制访问控制

计算机信息系统可信计算基对外部主体能够直接或间接访问的所有资源（例如：主体、存储客体和输入输出资源）实施强制访问控制。为这些主体及客体指定敏感标记，这些标记 是等级分类和非等级类别的组合，它们是实施强制访问控制的依据。计算机信息系统可信计算基支持两种或两种以上成分组成的安全级。计算机信息系统可信计算基外部的所有主体对客体的直接或间接的访问应满足：仅当主体安全级中的等级分类高于或等于客体安全级中的等级分类，且主体安全级中的非等级类别包含了客体安全级中的全部非等级类别，主体才能读客体；仅当主体安全级中的等级分类低于或等于客体安全级中的等级分类，且主体安全级中的非等级类别包含了客体安全级中的非等级类别，主体才能写一个客体。计算机信息系统可信

计算基使用身份和鉴别数据，鉴别用户的身份，保证用户创建的计算机信息系统可信计算基外部主体的安全级和授权受该用户的安全级和授权的控制。

标记

计算机信息系统可信计算基维护与可被外部主体直接或间接访问到计算机信息系统资源（例如：主体、存储客体、只读存储器）相关的敏感标记。这些标记是实施强制访问的基础。为了输入未加安全标记的数据，计算机信息系统可信计算基向授权用户要求并接受这些数据的安全级别，且可由计算机信息系统可信计算基审计。

身份鉴别

计算机信息系统可信计算基初始执行时，首先要求用户标识自己的身份，而且，计算机信息系统可信计算基维护用户身份识别数据并确定用户访问权及授权数据。计算机信息系统可信计算基使用这些数据，鉴别用户身份，并使用保护机制（例如：口令）来鉴别用户的身份；阻止非授权用户访问用户身份鉴别数据。通过为用户提供唯一标识，计算机信息系统可信计算基能够使用户对自己的行为负责。计算机信息系统可信计算基还具备将身份标识与该用户所有可审计行为相关联的能力。

客体重用

在计算机信息系统可信计算基的空闲存储客体空间中，对客体初始指定、分配或再分配 一个主体之前，撤销客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。

审计

计算机信息系统可信计算基能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它访问或破坏。

计算机信息系统可信计算基能记录下述事件：使用身份鉴别机制；将客体引入用户地址空间（例如：打开文件、程序出始化）；删除客体；由操作员、系统管理员或（和）系统安全管理员实施的动作，以及其他与系统安全有关的事件。对于每一事件，其审计记录包括：事件 的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件，审计记录包含请求的来源（例如：终端标识符）；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名及客体的安全级别。

对不能由计算机信息系统可信计算基独立分辨的审计事件，审计机制提供审计记录接口，可由授权主体调用。这些审计记录区别于计算机信息系统可信计算基独立分辨的审计记录。计算机信息系统可信计算基能够审计利用隐蔽存储信道时可能被使用的事件。 计算机信息系统可信计算基包含能够监控可审计安全事件发生与积累的机制，当超过阈值时，能够立即向安全管理员发出报警。并且，如果这些与安全相关的事件继续发生或积累，系统应以最小的代价中止它们。

数据完整性

计算机信息系统可信计算基通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。在网络环境中，使用完整性敏感标记来确信信息在传送中未受损。

隐蔽信道分析

系统开发者应彻底搜索隐蔽信道，并根据实际测量或工程估算确定每一个被标识信道的最大带宽。

可信路径

当连接用户时（如注册、更改主体安全级），计算机信息系统可信计算基提供它与用户之间的可信通信路径。可信路径上的通信只能由该用户或计算机信息系统可信计算机激活，且在逻辑上与其他路径上的通信相隔离，且能正确地加以区分。

可信恢复

计算机信息系统可信计算基提供过程和机制，保证计算机信息系统失效或中断后，可以进行不损害任何安全保护性能的恢复。

1.3. 什么是安全运营中心

安全运营中心（SOC）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。安全运营中心是一种安全管理的形式，他的职能分成管理层面的职能和技术层面的职能，它的存在有效地将企业的策略管理、安全组织管理、安全运作管理和安全技术框架结合在一起，保持一致性。

安全运营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，并触发工单和响应来降低风险，达到管理和控制风险的效果。

服务管理：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，通过企业安全运营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：安全运营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：安全运营中心不会独立于整个企业的 IT 管理系统独立运载，整个维护运作组织也是整个企业维护运作组织的一部分，SOC 充分考虑企业内部 IT 系统融合的需求，提供各类灵活接口。

1.4. 为什么需要安全运营中心

随着各类组织、企业对信息安全的日益重视，于是部署了大量的、不同种类的信息安全产品，如防火墙、防病毒、终端管理、网络准入、网络入侵/防护等，但是这些种类繁多的安全产品带来了巨大的管理问题。

另外，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。铱迅信息密切关注这些问题，开发了安全运营中心产品（简称 SOC）来解决上述这些问题。

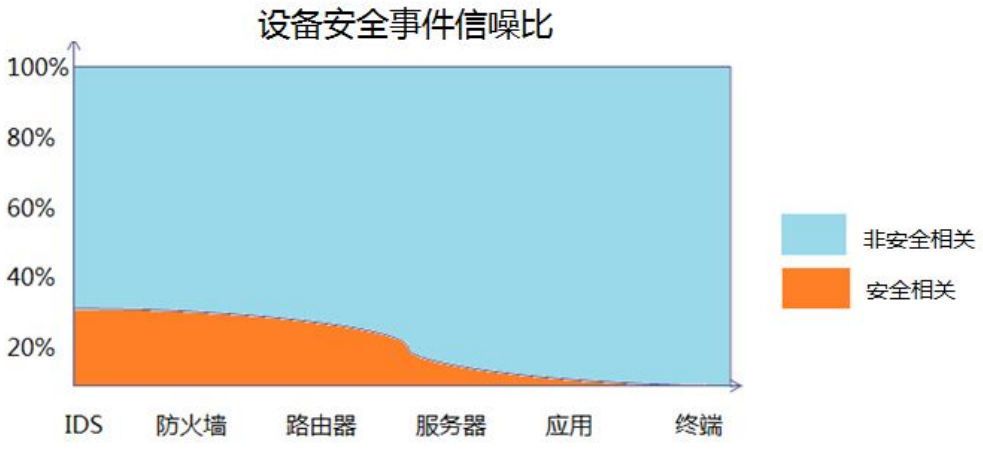
信息安全管理存在的主要问题如下：

1.4.1. 种类繁多的安全产品

安全领域有一个很大的特点，它和现有的所有层面的 IT 技术、产品都有关联：与网络技术、主机操作系统、应用软件、设备硬件、人为管理、内容安全、电话网等所有领域都有关系。信息安全有大量的细分领域：防火墙、入侵检测、扫描器、审计、补丁管理、集中认证、一次性口令、加密存储、链路层加密、防毒、内容安全、PKI/CA、安全服务、策略管理等等，每个领域都存在一个或多个实力很强的厂商，在这样一个环境下，需要面对每个厂商的不同界面，这对大型机构或企业的安全管理人员是一个巨大的挑战。

1.4.2. 海量数据

安全产品部署的过程中，最为严重和突出的现象是会出现大量的安全信息，一个标准的网络入侵检测系统如采用缺省策略，每天可能产生超过数十万数量的事件。因此海量的数据常常让我们的安全产品变得没有任何意义，即使经过调整和优化的策略，也可能充斥着无意义数据和误报。入侵检测等安全产品也正是因为这种原因被人诟病。有些无效数据是由安全产品的机制自身导致的，它本身无法彻底解决该问题，下面的图说明了各种安全产品产生的噪音：



1.4.3. 缺乏统一的风险视图

大部分安全系统纯粹是基于事件的系统，即不能关联到资产，也不能体现资产价值、业务系统价值及资产上存在的脆弱性信息，即这些信息不是按照用户所需要的方式展现出来，用户需要看到的视图是按照资产查看安全信息。

1.4.4. 合规要求

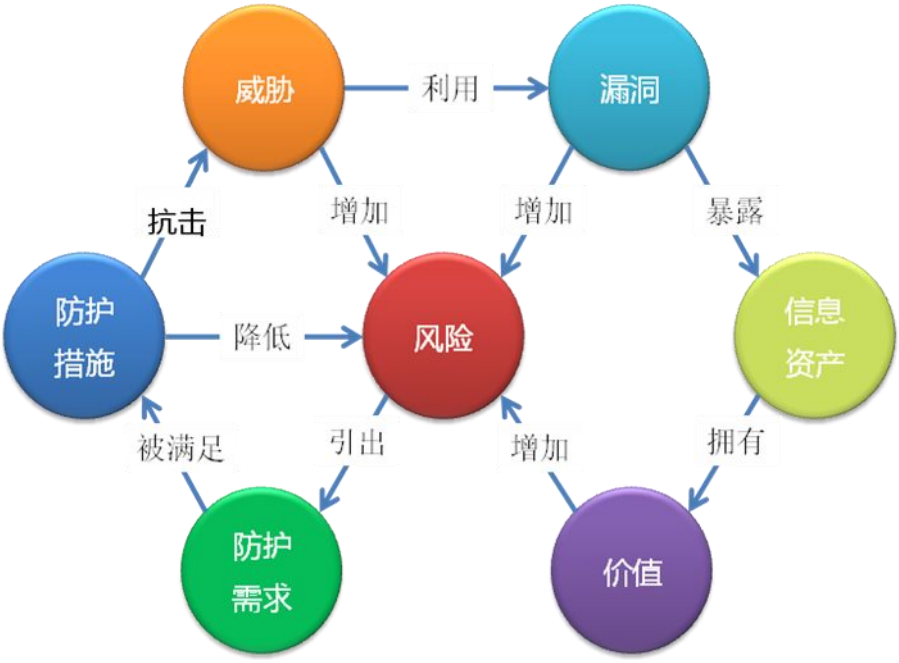
对于大型公司而言，越来越多的政策法规对安全提出了具体明确的要求，例如等级保护、萨班斯法案（SOX）等，均对信息内控提出明确要求，其中安全占据重要地位，特别是对安全日志、帐号口令的流程管理和审计管理，给用户带来大量管理工作，需要自动化系统能够有效对这些控制和管理进行支撑。

1.4.5. 建立基于风险的安全管理体系

信息安全的主要目标是保护信息和信息资产的保密性、完整性和可用性的保持。保密性定义为保障信息仅仅为那些被授权使用的人获取；完整性定义为保护信息及其处理方法的准确性和完整性；可用性定义为保障授权使用人在需要时可以获取信息和使用相关的资产。

如何保证信息资产的保密性、完整性和可用性呢？必须用风险管理的手段来实现，风险管理是企业安全管理的核心，正确的风险管理方法是不断评估和监控企业信息资产中存在的风险，并采取一定的防护措施和响应管理流程，保证对风险的抑制。

在进行风险的控制过程中，参考了 ISO13335 的模型：



可以看出，风险控制是一个动态的模型，在风险控制的过程中最主要需要考量的因素是：资产及其价值、威胁、漏洞和防护措施，据此可以计算出需要关注的风险值：

资产及资产价值：资产是只对某个组织有价值的东西，信息资产分别具有不同的安全属性，机密性、完整性和可用性分别反映了资产在三个不同方面的特性。安全属性的不同通常也意味着安全控制、保护功能需求的不同。通过考察三种不同安全属性，可以得出一个能够基本反映资产价值的数值。

威胁：威胁是对系统和企业网的资产引起不期望事件而造成的损害的潜在可能性。威胁可能源于对企业信息直接或间接的攻击，例如非授权的泄露、篡改、删除等，在机密性、完整性或可用性等方面造成损害。威胁也可能源于偶发的、或蓄意的事件。一般来说，威胁总是要利用企业网络中的系统、应用或服务的弱点（弱点的定义参见弱点一章）才可能成功地对资产造成伤害。

漏洞：弱点和资产紧密相连，它可能被威胁利用、引起资产损失或伤害。值得注意的是，弱点本身不会造成损失，它只是一种条件或环境、可能导致被威胁利用而造成资产损失。

防护措施：防护措施可以是安全产品部署、策略执行、人工加固等，防护措施通过降低威胁发生的可能性，将风险降到可接受的范围之内。

所有的安全产品和安全技术都是通过改变风险的某一属性从而达到降低风险的目标，最终保护了宝贵的信息资产。

2. 安全运营中心系统架构和运行环境

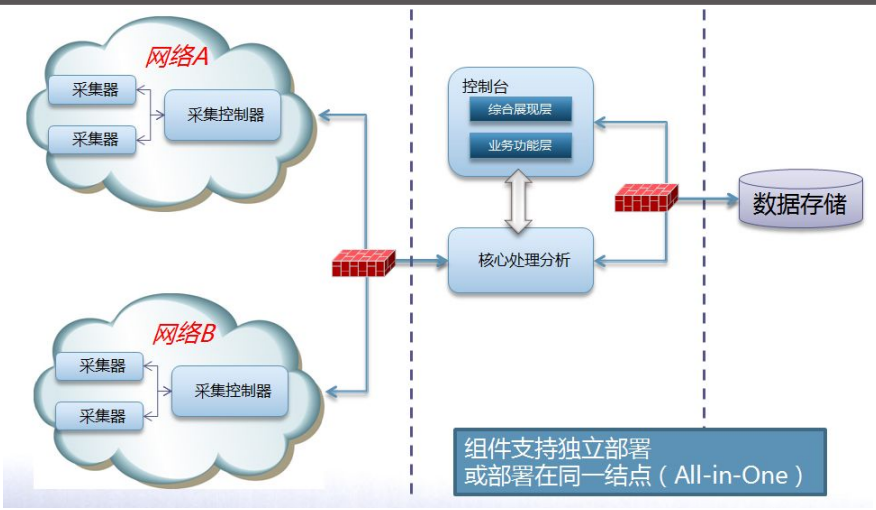
2.1. 总体架构

总体而言，安全运营中心系统包括数据存储、管理控制（控制台）、核心处理分析和采集控制四大组件群。

其中，数据存储部分负责存储系统内所有数据，它不仅包括一般的关系式数据库还包括了一个可分布的原始数据存储器和查询器；管理控制组件主要指一个基于 Web 的控制台；核心处理分析组件群主要包含各类安全数据分析、风险计算、任务调度、响应处理的组件；而采集控制组件群包含了一个到多个可分级部署的数据采集控制器/采集器，它是安全运营中心的主要数据来源。

根据实施规模的大小，上述四个组件群均可分开部署，也可以进行不同的组合。

上述关系如下图所示：



本文主要描述的是管理控制（控制台）的相关主要功能，关于系统的安装部署、核心处理分析及采集控制部分请参看相关安装手册、管理员手册。

2.2. 运行环境

安全运营中心系统的数据存储、管理控制及核心处理分析运行于 CentOS 系统（x86 64 位）上；而采集控制可运行于 CentOS（x86 64 位）及部分运行于 Windows 系统上（采集 Windows 相关信息）。

建议采用 FireFox、谷歌或 IE9（含）以上浏览器查看系统。

3. 安全运营中心系统主要业务及流程

3.1. 资产来源

安全运营中心系统的核心管理对象就是所谓资产。在安全运营中心产品中资产的来源包括如下几种方式：

1. 人工录入
2. 批量导入
3. 自动发现
4. 漏洞扫描
5. 事件接入

其中，前两类是向系统添加正式的资产，而其它则并非是正式的资产（但在进行合适地配置后，也可以进行事件/日志解析、漏洞扫描、安全基线检查，但不能参与风险计算及生成告警；可以将它们转换成正式的资产）。

3.2. 事件管理

事件管理是安全运营中心系统的核心功能之一，下图给出了一个较为详细的事件处理流程示意：

3.3. 漏洞扫描

漏洞扫描也是安全运营中心系统的核心功能之一。与专业的扫描设备不同，安全运营中心的漏洞管理不仅支持分布式的漏洞扫描，也支持对系统内的漏洞进行统一地分析和处理，产生相关告警并指定相关责任人进行处理。

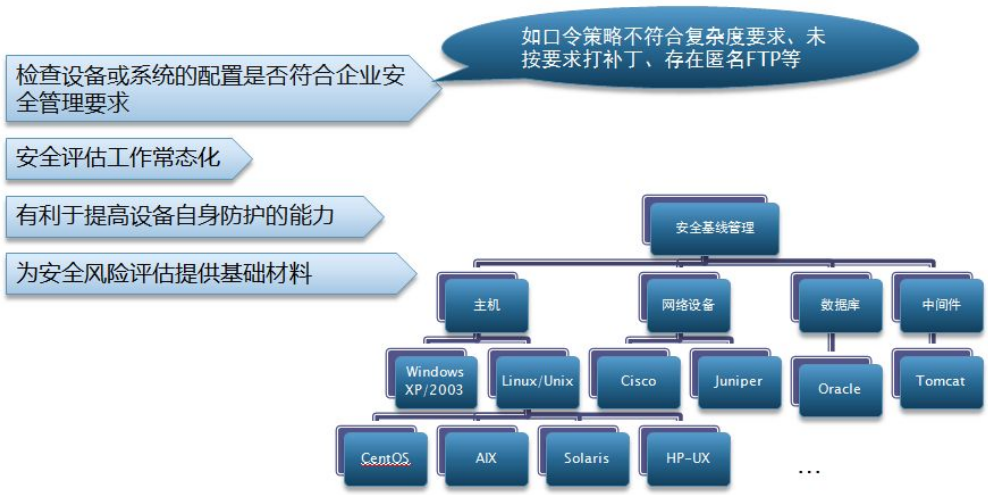
下图说明了普通漏洞扫描和漏洞管理的区别：

3.4. 安全基线检查

安全运营中心引入安全基线检查的初衷在于：

1. 企业内有众多的、不同类型的主机、网络设备、安全设备、数据库、Web 中间件
2. 上述系统或设备都存在配置安全问题
3. 安全配置基线问题，特别是口令强度不够是黑客攻击的主要手段

因此，安全基线管理就提供了这样的一个集中审计各类系统、设备安全配置情况的功能。下图给出了示意：

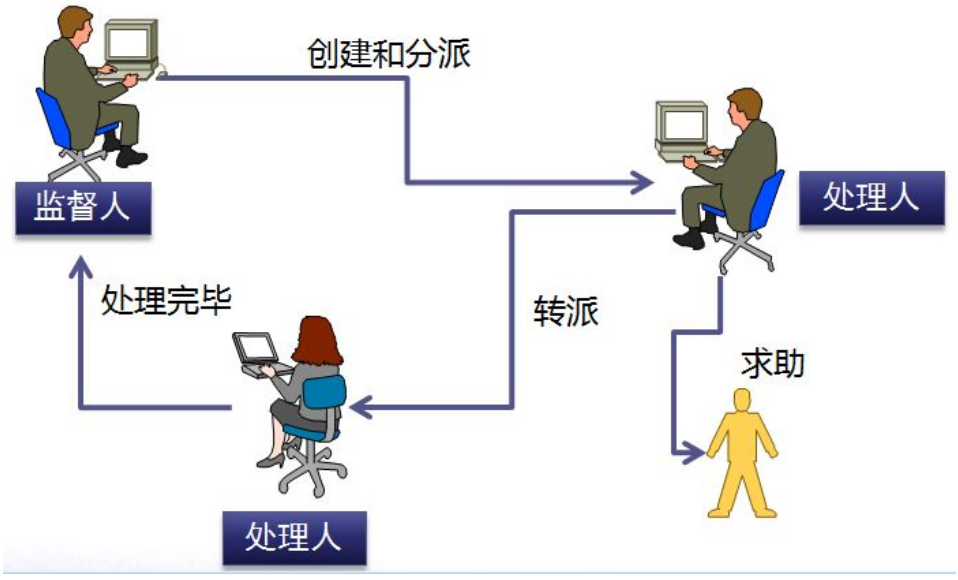


3.5. 告警及响应生成

安全运营中心的告警是指用户特别需要关注的安全问题，它既可以来源于安全事件，也可以来源于漏洞、安全基线违规及其它可能需要处理的问题；告警一般由特定的策略生成，生成告警后，用户可以将这些告警进行派单或产生特殊的响应（如邮件、Syslog 等）。

3.6. 工单处理

工单是处理安全问题的载体，是进行问题分析和处理的重要对象，一个工单的处理流程如下图所示：



3.7. 风险分析

风险是对资产或可能对资产造成损失的度量。安全运营中心参照相关国际和国内标准对系统内的资产及总体风险情况进行评估

鉴于用户可能存在不同的权限，即各用户的风险视图存在不同，但安全运营中心能根据权限精准地计算出不同用户的管辖范围内资产的风险状况。

4. 基础功能

用户在使用安全运营中心前，应通过相关正规渠道获取许可证，在将许可证导入到系统后方可正常使用。

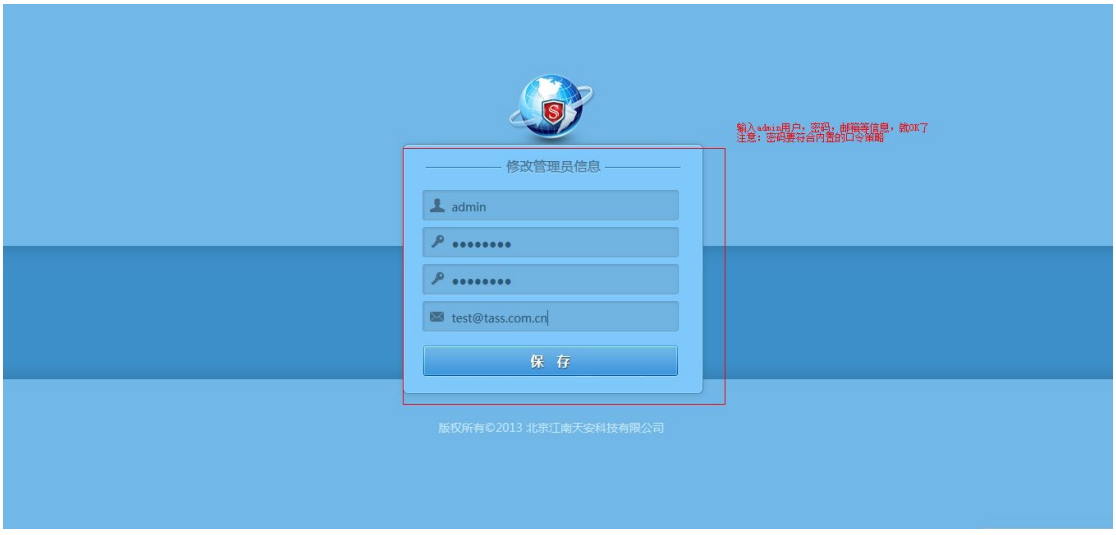
4.1. 功能概述

在铱迅安全运营中心，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、系统管理等子系统组成。

4.2. 初次使用

用户在初次使用安全运营中心时，需要导入许可证信息（License），在获取许可证之前，需要将界面上显示的相关硬件 UUID 告知许可证提供方。

另外，系统会要求用户修改口令并添加管理员邮箱：



4.3. 向导

向导是用户第一次使用安全运营中心时，系统给出的相关使用步骤指引，它主要包括如下几个部分：

1. 设置采集器：由于安全运营中心默认不会建立采集器，故需要用户设置采集器；采集器包括漏洞扫描、配置获取（资产发现、安全基线检查使用此类采集器）和事件三类；一般在一个采集管理器下，只需要建立一个漏洞扫描和一个配置获取类型的采集器，而事件采集器需要根据实际情况配置，一般一种事件类型只能建立一个到三个。上述操作如下图所示：

其中，采集器包含如下几种类别：

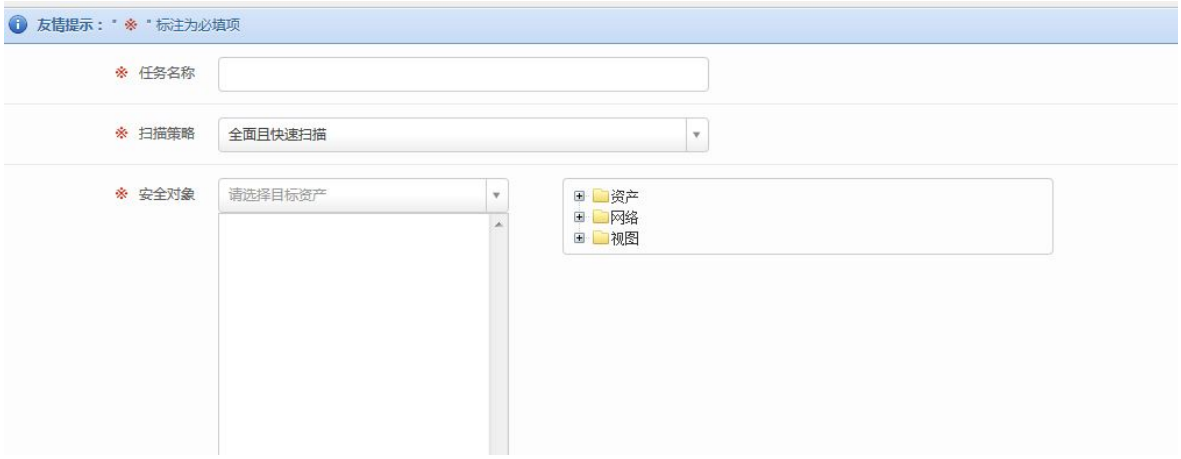
漏洞扫描

安全基线（资产发现、设备状态检查亦使用此类采集器）

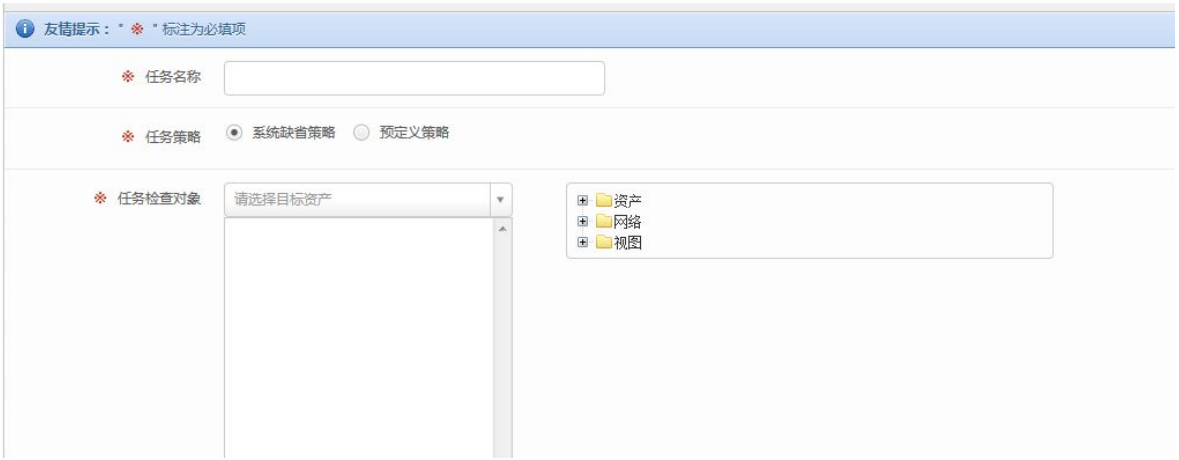
事件

2. 资产发现：自动发现采集管理器所在网络的相关主机、网络设备、安全设备、应用的存活情况，并将发现的相关资产的开放端口、服务类型和服务版本自动保存在系统内；需要注意的一点是发现的资产系统类型不一定非常准确，用户可能还需进行调整；另外，如果要使用安全基线检查，用户需设置资产的登录凭证，即登录方式、端口、用户名及口令。上述操作如下图所示：

3. 漏洞扫描：制定任务对已发现的资产进行扫描并获取报告（也可参见漏洞管理相关功能）。如下图所示：



4. 安全基线检查：制定任务对已发现的资产进行安全基线检查并获取报告（也可参见漏洞管理相关功能）。如下图所示：



一般，用户通过系统的向导指引，就可以完成初始化工作和基本管理操作。

4.4. 资产管理

4.4.1. 什么是安全资产

安全资产是安全运营中心的核心管理对象。与 ISO27001 的关于资产的定义略有不同，铱迅网络安全管理中的资产是特指具有 IP 地址的 IT 类设备及其之上运行的、可管理的服务或应用。

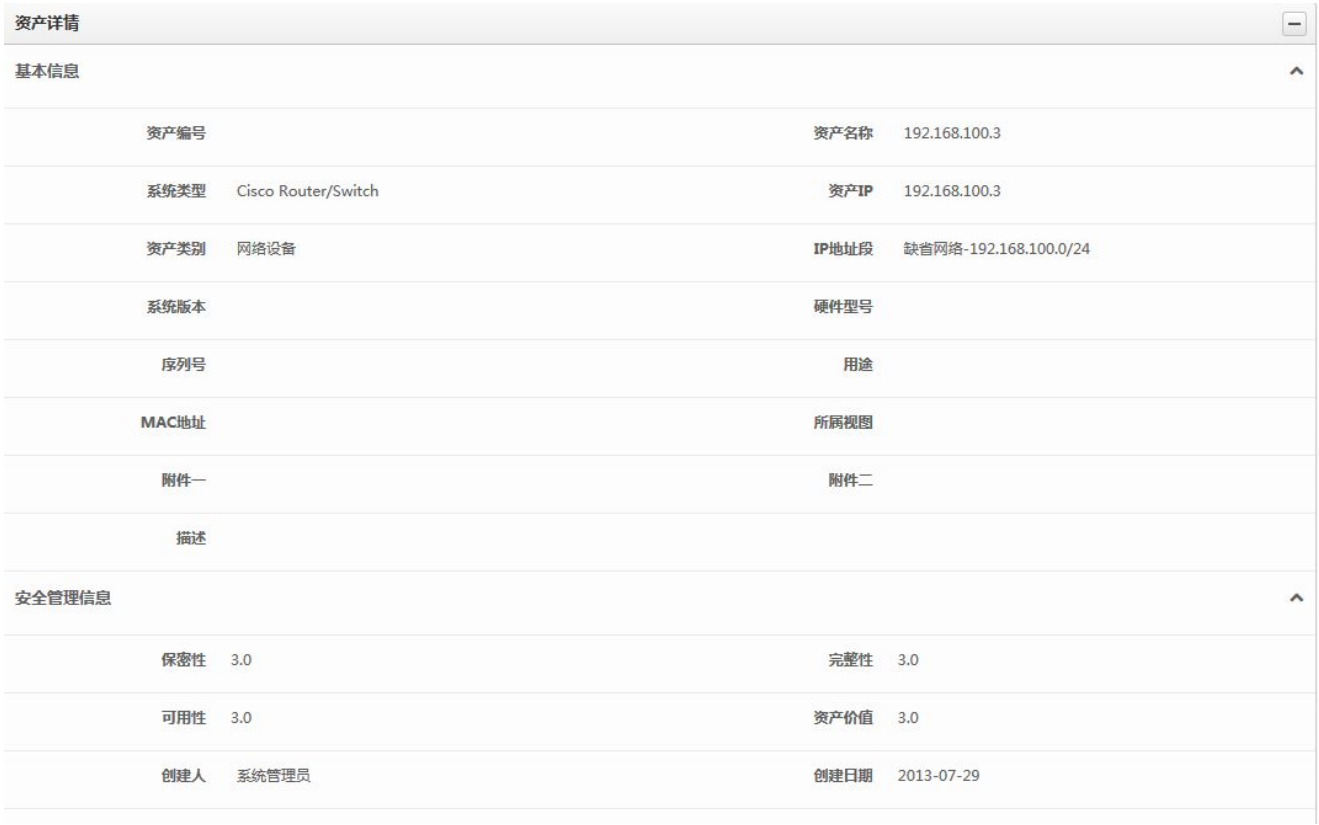
4.4.2. 安全资产的属性

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。

如下图所示：



为了提供一定的扩展性和灵活性，系统支持用户定义多个自定义属性，属性的类型包括数值型、日期型、字符型等。

如前所述，安全运营中心的资产管理支持用户录入、导入或自动发现资产。

4.4.3. 什么是网络

与普通定义的网络不同，安全运营中心的网络是为了处理不同网络（初始安装后系统存在一个所谓的默认网络）的资产同 IP 问题；网络中包括若干网段。

铱迅安全运营中心支持对于网络和 IP 地址段的管理；网段可以通过手工录入或自动发现获得；系统发现的新资产也可在此功能模块中列出，用户可以将它们纳入或归并到已存在的资产中。

4.4.4. 什么是资产视图

为了便于用户集中、灵活地管理所辖范围内的资产，安全运营中心支持用户自定义资产管理视图；所谓资产视图就是用户对于资产的组织形式。

4.4.5. 相关操作

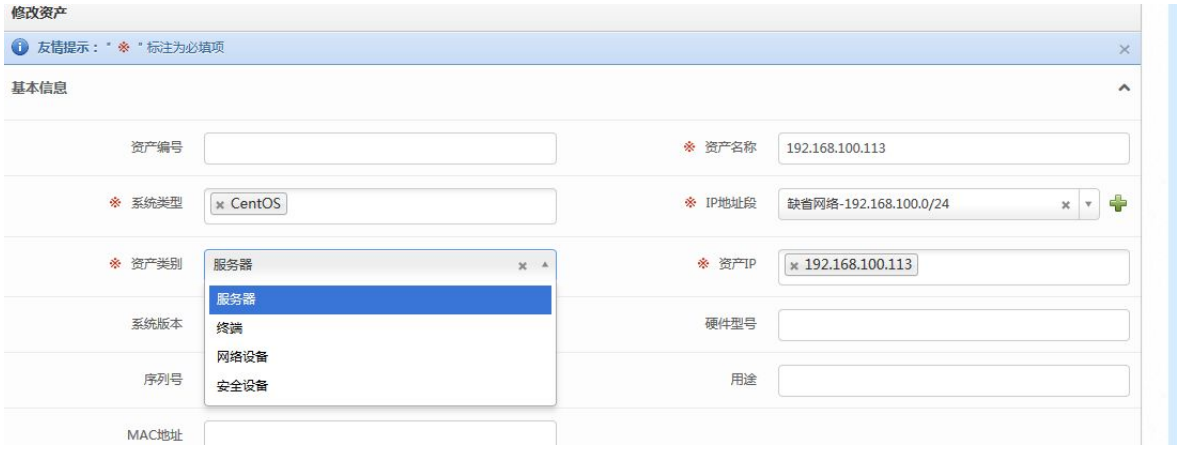
4.4.5.1 资产管理

资产管理功能包括如下内容：

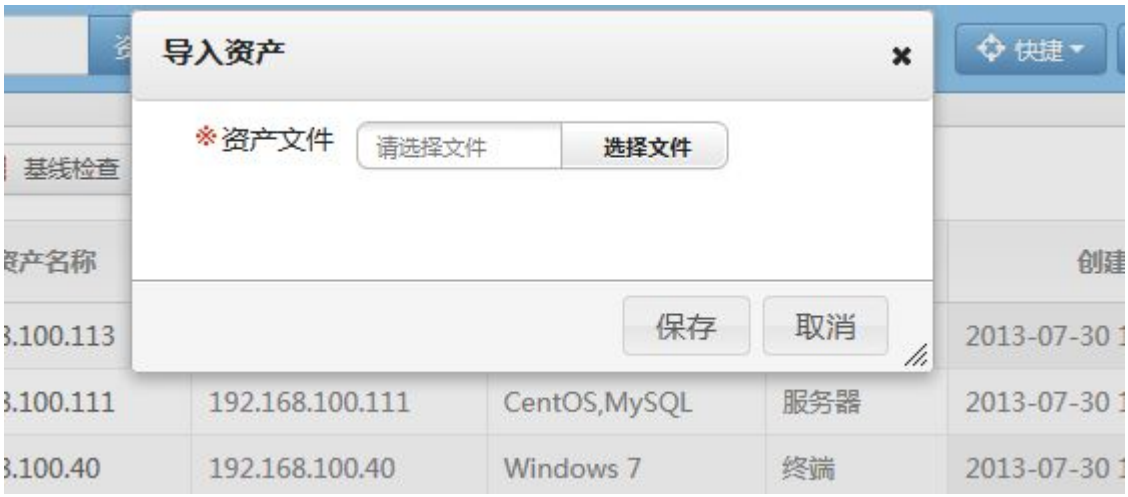
1. 资产查看：用户根据各自权限（含角色中的授权以及资产创建人）查看资产列表，列表查看时可以依据某种选中的视图（和用户个人相关），也可不选择任何视图查看；用户点击某资产链接可查看资产详情，如下图所示：

2. 资产查询：在资产列表中输入相关字段的查询条件（可查询字段参看属性列表），点击查询；查询结果可导出成报告；报告可以另存为 PDF、Word、Excel 和 csv 格式，如下图所示：

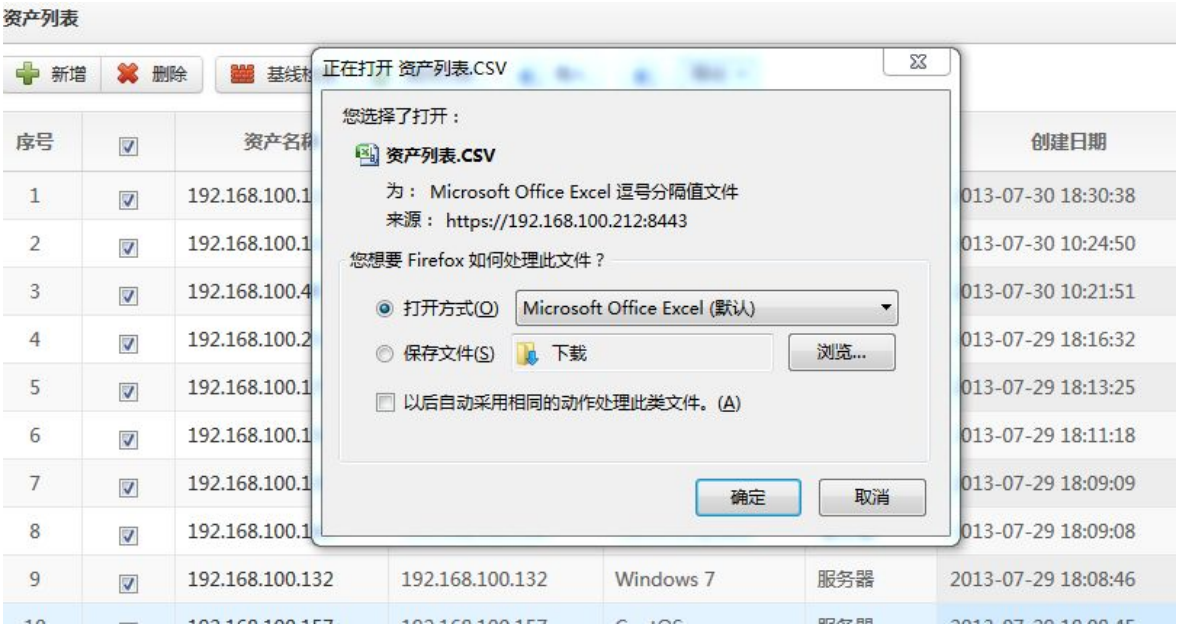
3. 资产维护：资产的增加、修改和删除操作；在新增资产时系统可自动将资产的 IP 地址添加到网络中（导入资产类似），如下图所示：



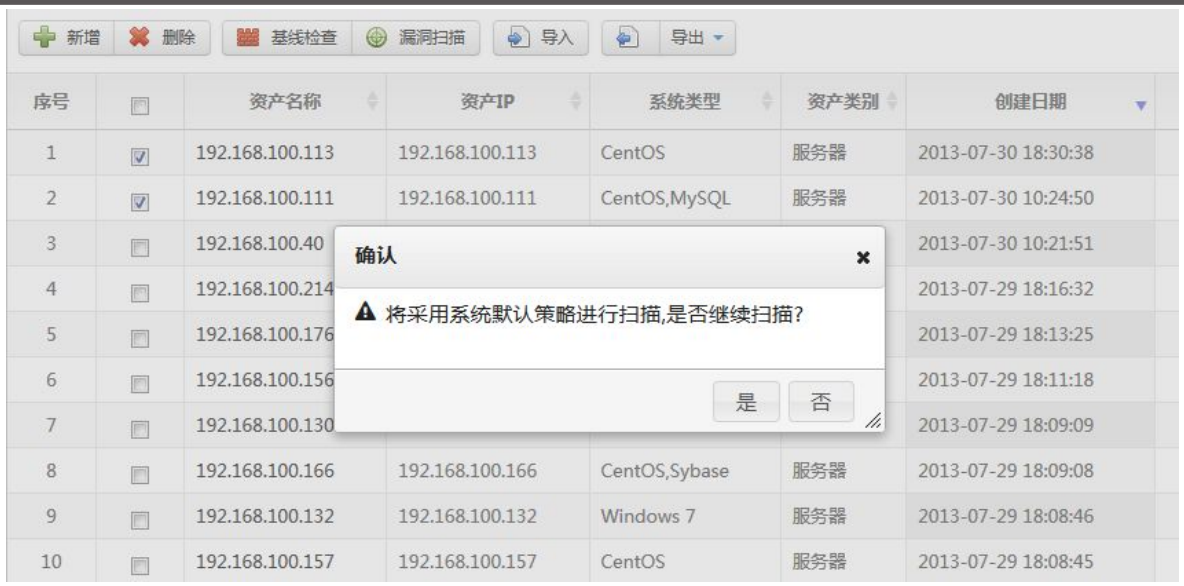
4. 导入资产：根据系统约定格式从外部文件导入资产（模板可从管理界面获得），如下图所示：



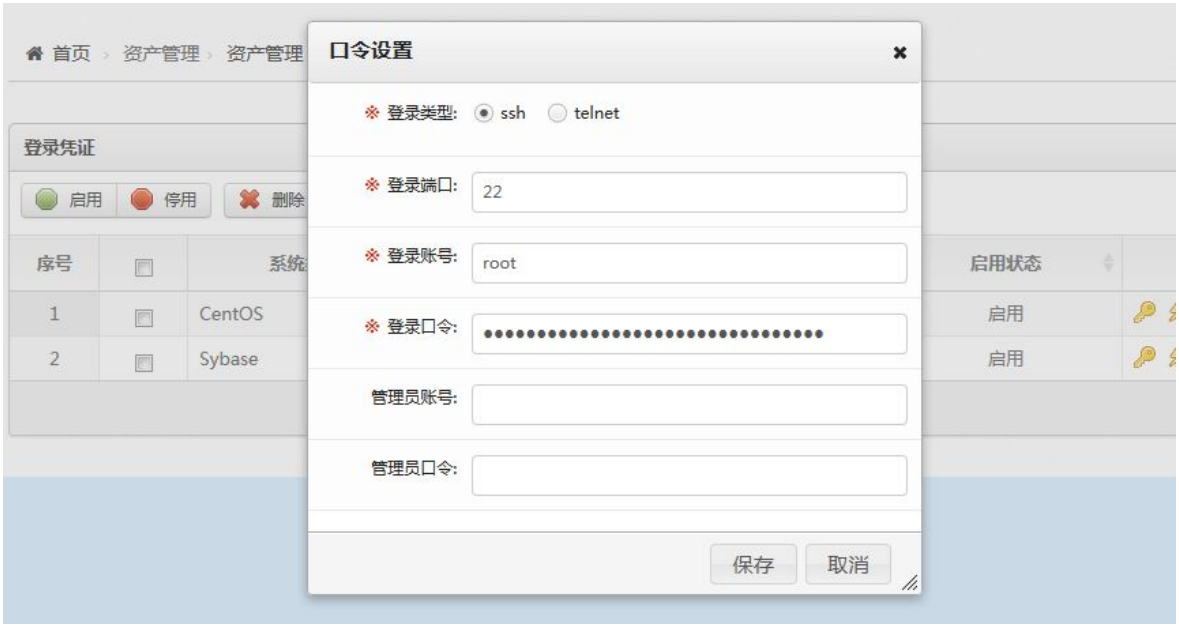
5. 导出资产：根据用户需要，将所选择的或全部资产导出到外部文件，如下图所示：



6. 安全检查：能对一个或多个资产**实时**执行漏洞扫描、安全基线检查等操作（用户也可参见漏洞管理及安全基线管理相关功能），如下图所示：



7. 设置登录凭证：用户可根据资产的系统类型设置相关登录凭证和附加参数（用于安全基线检查），如下图所示：



4.4.5.2 资产自定义属性

资产自定义属性支持：文本、数值（包括整型、浮点型）、日期等类型；可设置字段名称、长度、输入提示（可选）、出错提示。

用户可以定义、修改和删除自定义属性。

界面如下图所示：

4.4.5.3 资产视图管理

资产视图是用户对于所管理资产的组织形式，系统可以使用地理位置、安全域、系统类型等创建资产视图，用户也可以定义其它相关视图并关联资产 。

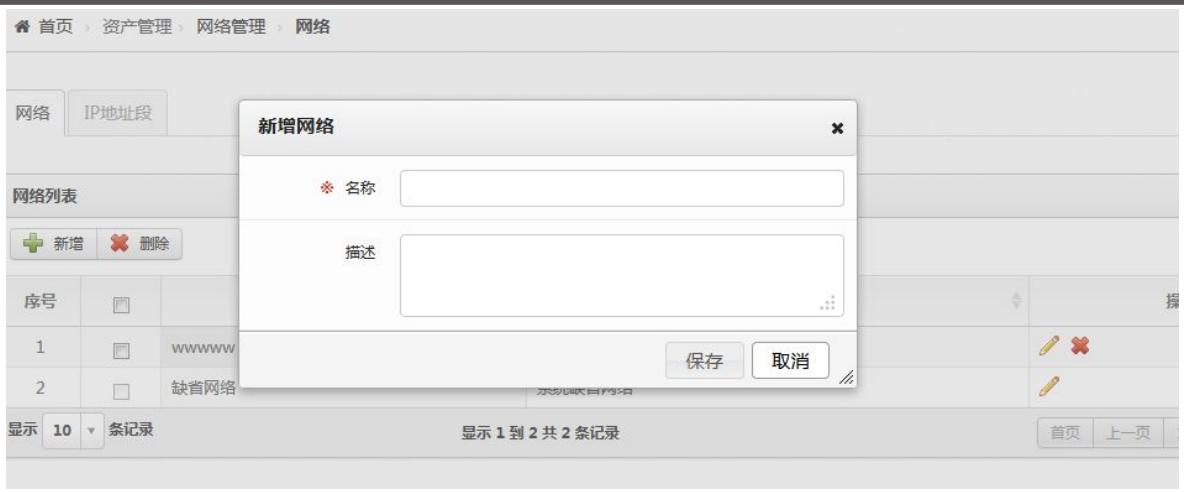
界面如下图所示：

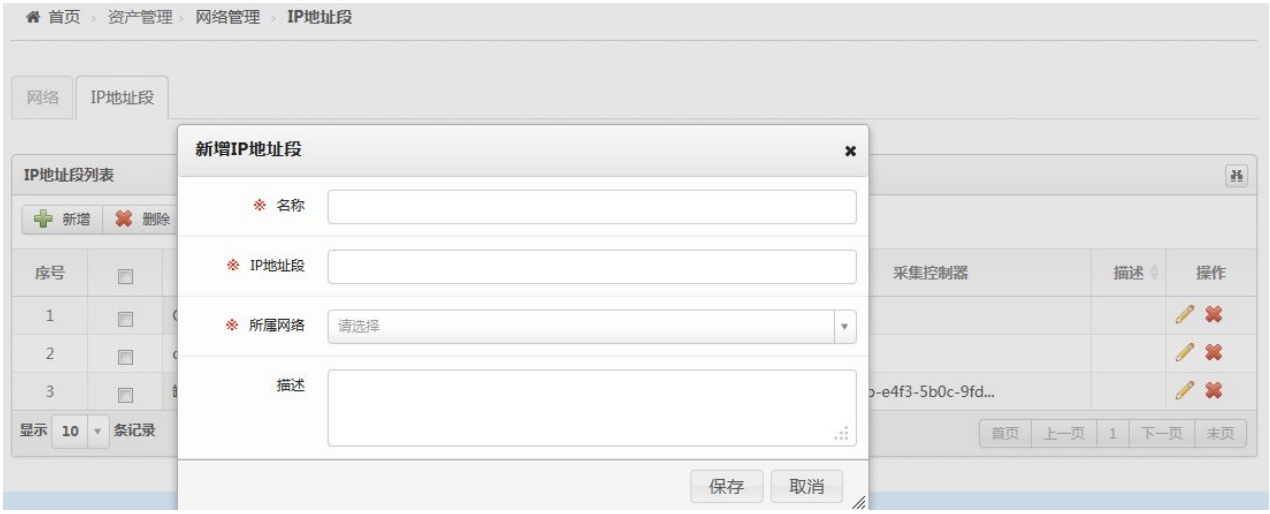
4.4.5.5 网络管理

网络管理：为解决不同局域网中存在相同 IP 地址，以定义不同网络；系统在事件采集、扫描、安全基线检查等会使用此属性；默认可以不增加网络。

网段管理：对网段进行维护，系统仅支持 IP 地址和前缀码形式；系统支持 IPv6 形式的地址段。

界面如下图所示：





4.4.5.6 资产发现管理

资产发现的目的除了发现网络中存活的真实设备，还能尽量地发现其运行操作系统的类型、版本、开放的端口及其端口服务的类型及版本。资产发现的结果不直接添加到资产中（需过滤已经存在资产）。

在定义资产发现任务时，用户可以给出需发现的 IP 地址段或系统可以采集器安装的情况进行自动发现；资产发现功能不支持 IPv6 设备的发现。

用户可以将系统发现的 IP 设备加入为资产或者删除。

界面如下图所示：

注意：如果系统内部署多个采集控制器，则既可以全部进行发现，也可以选择其中几个进行。

4.5.漏洞管理

在铱迅信息的安全运营中心系统中，漏洞管理中的任务管理和策略管理以及结果的展示，分别被划分在不同的功能菜单中。其中漏洞任务管理在“任务管理”中，漏洞扫描策略管理则在“安全策略”模块中，而在安全仪表板、资产管理和风险管理中均可查看到扫描结果，只不过维度存在一定的差异；但为了能使用户对漏洞管理有一个整体的认识，故在本手册中将它们合并进行介绍。

4.5.1. 什么是漏洞

漏洞就是软件编码时的疏忽或错误；如 Windows 操作系统的漏洞，我们经常要打补丁，打补丁实际就是修复这些漏洞；黑客就是利用漏洞入侵的 。

漏洞分为：

1. 技术漏洞如缓存区溢出漏洞、SQL 注入漏洞
2. 管理漏洞如职责不分、过度授权等

安全运营中心采集的漏洞仅指利用扫描器发现的漏洞，主要指技术上的漏洞。

4.5.2. 为什么需要漏洞管理

上文已对为什么需要漏洞管理进行了一定的解释，与普通的漏洞扫描器相比，需要进一步说明的是：

1. 普通扫描器的主要作用是发现漏洞，管理能力较弱
2. 普通扫描器不能看到漏洞的变化情况，新增哪些漏洞，修复了哪些漏洞等
3. 普通扫描器中漏洞无法关联到资产，从而无法进一步分析风险
4. 可能存在不同的扫描器产品，扫描结果不统一

4.5.3. 什么是漏洞扫描插件

漏洞扫描插件是针对某种或某些计算机服务、程序漏洞而开发的探测或检测工具，它会根据漏洞的一些特征对扫描目标进行测试。

漏洞扫描插件一般是以脚本方式书写的，但在一些特殊场合下也不排除使用二进制代码实现。铱迅安全运营中心的漏洞扫描插件一般也是由 NASL 脚本语言开发的。

4.5.4. 什么是漏洞扫描策略

漏洞扫描策略是漏洞为了完成某些特定目的而制定的，它一般包含一个到多个漏洞扫描插件。我们一般不建议用户自定义漏洞扫描策略，因为一般默认的系统策略在大多数情况下已经足够用户使用了；除非

用户只希望扫描某些特定类型的软件或系统漏洞，如 FTP、SMTP，或某类系统，如 Windows、Cisco IOS 等。

4.5.5. 相关操作

4.5.5.1. 漏洞管理

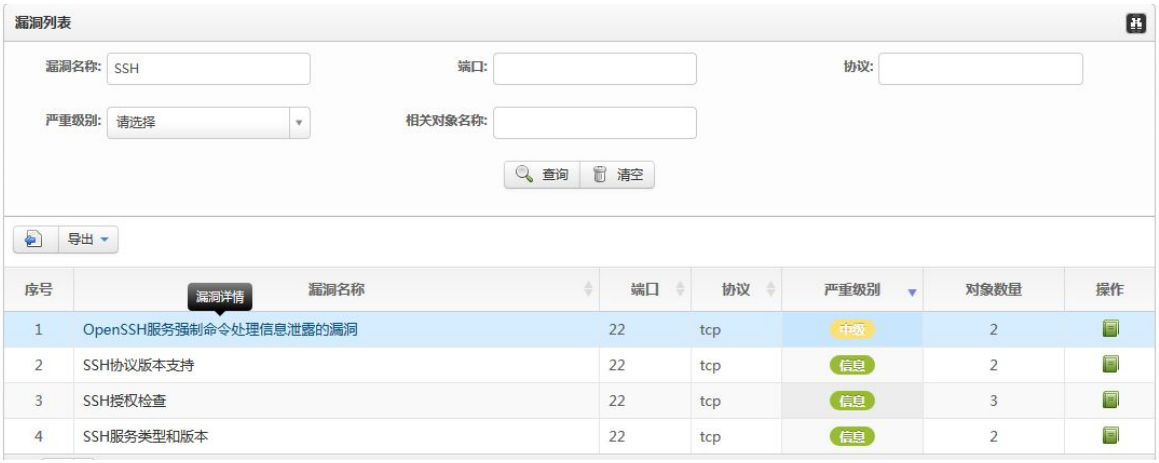
漏洞管理包括如下主要操作：

1. 漏洞查看：列表查看登录用户权限范围存在的漏洞，列表中除应显示漏洞的列表属性，还应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）； 如下图所示：

用户将鼠标移动到某个具体漏洞名称，系统显示相关漏洞的全部详细情况，如下图所示：

2. 漏洞查询：用户可以根据漏洞的相关属性对系统存在的当前漏洞进行查询；查询结果可以导出成报告报告可以另存为 PDF、Word 等格式。

如下图所示：



4.5.5.2. 漏洞扫描任务管理

漏洞的扫描任务管理在“任务管理”中。

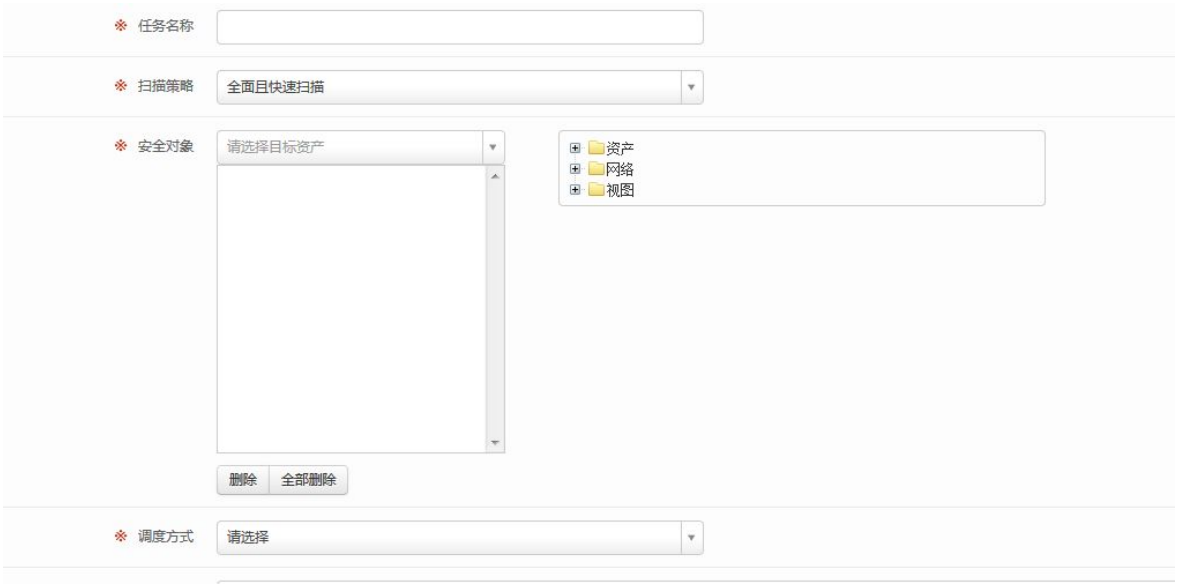
漏洞任务管理应包括三个部分：任务列表（可定义任务、正在执行的任务、和已完成的任务（即漏洞扫描报告）。相关漏洞任务的操作包括：

1. 任务查看：多于所有类型的任务，列表查看任务相关属性，列表默认按任务修改时间倒序排列。系统会将正在执行的任务单独列表显示出来并且显示其执行进度。如下图所示：

定义任务

2. 任务新建：用户输入任务相关属性；如扫描对象选择为 IP 地址段则可支持 IPv4 地址段、一个或多个独立的 IPv4 地址或 IPv6 地址；任务执行的参数包括调度方式（一次还是周期）、周期类型（天、周、月）。

如下图所示：

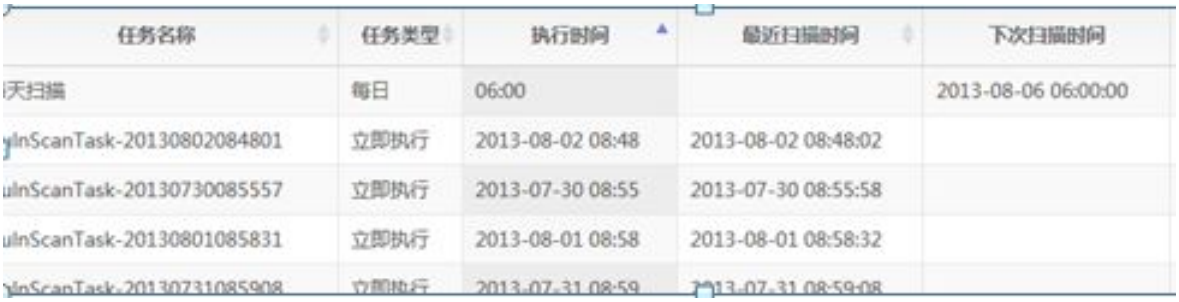


3. 任务删除：用户可以在任务列表中删除一个或多个任务（正在执行的任务也可以删除）。

4. 停止调度：对于周期型任务可以停止调度，这里停止调度的含义是今后不再进行调度，但如果用户需要继续其任务的调度，则可以使用“启用”功能（即恢复调度）。如下图所示：

序号		任务名称	任务类型	执行时间	最近扫描时间	下次扫描时间
1		每天扫描	每日	06:00		2013-08-06 06:00:00
2		VulnScanTask-20130802084801	立即执行	2013-08-02 08:48	2013-08-02 08:48:02	
3		VulnScanTask-20130730085557	立即执行	2013-07-30 08:55	2013-07-30 08:55:58	
4		VulnScanTask-20130801085831	立即执行	2013-08-01 08:58	2013-08-01 08:58:32	
5		VulnScanTask-20130731085908	立即执行	2013-07-31 08:59	2013-07-31 08:59:08	

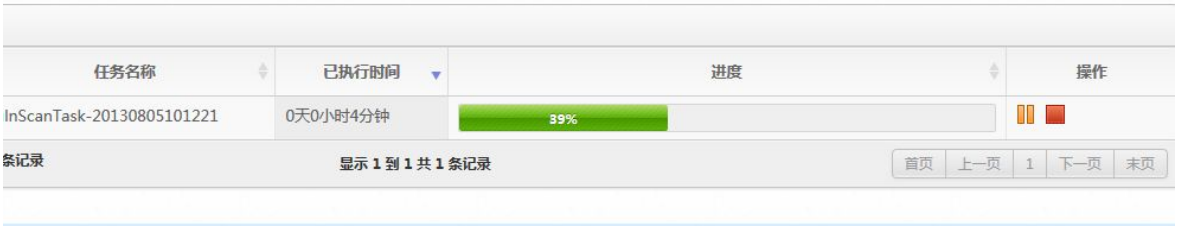
5. 启用（恢复调度）：对于已经被停止调度的任务，用户可以选择恢复调度。如下图所示：



任务名称	任务类型	执行时间	最近扫描时间	下次扫描时间
天扫描	每日	06:00		2013-08-06 06:00:00
lnScanTask-20130802084801	立即执行	2013-08-02 08:48	2013-08-02 08:48:02	
lnScanTask-20130730085557	立即执行	2013-07-30 08:55	2013-07-30 08:55:58	
lnScanTask-20130801085831	立即执行	2013-08-01 08:58	2013-08-01 08:58:32	
lnScanTask-20130731085908	立即执行	2013-07-31 08:59	13-07-31 08:59:08	

正在执行的任务

6. 任务停止：用户可以停止正在运行的一个任务；任务停止后将在正在执行任务列表中消失。如下图所示：



7. 任务暂停：用户可以暂停正在运行的一个任务；任务暂停后将继续出现在执行任务列表中，但状态为暂停（ ）。

8. 任务继续：用户可以继续运行已被暂停的一个任务。如下图所示：

任务执行结果

9. 报告查看：在任务报告列表中选择一个报告，点击查看详细；报告可以另存为 PDF、Word、Excel、HTML 等格式。如下图所示：

扫描主机[192.168.100.130]

序号	漏洞信息	漏洞描述
1	漏洞名称: 检查rlogin服务运行 CVE编号: CVE-1999-0651 端口/协议: 513/tcp 严重级别: 高级	远程主机正在运行rlogin服务，一个远程登录进程，它允许人们登录到这台主机，并获得一个交互式的shell。从某种意义上来说这项服务没有密码保护，也就是说，任何人都可以监听到在远程登录客户端和远程登录服务器端之间传送的数据，这些数据包括登录名和密码，还有远程主机执行的命令。您应当禁用这项服务，并且使用openssh 来代替它(www.openssh.com)
2	漏洞名称: snmpXdmid 溢出 CVE编号: CVE-2001-0236 端口/协议: 32782/tcp 严重级别: 高级	远程RPC服务100249 (snmpXdmid)中存在一个缓存溢出的漏洞，这个漏洞允许任何用户获得这台主机的一个root命令解释程序。 如果您不使用这项服务，就禁用它(/etc/init.d/init.dmi stop)，或者联系Sun公司获取补丁程序。
3	漏洞名称: TCP序列号相似重置拒绝服务漏洞 CVE编号: CVE-2004-0230	远程主机可能存在TCP序号相近漏洞，这个漏洞可能允许攻击者向远程主机发送欺骗的RSP数据包，导致远程主机关闭TCP连接。这可能导致一些专门的服务(BGP,VPN等...)TCP连接中断。在BGP里面，会造成Internet中断。

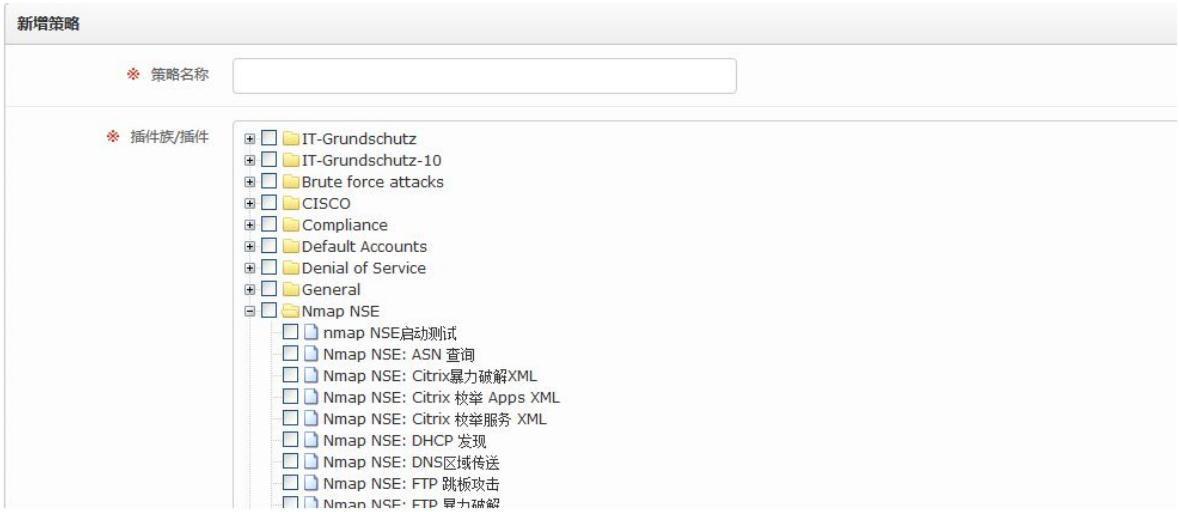
10. 报告删除：用户可以删除系统一个或多个任务执行报告。

11. 报告对比：用户可以选择一个任务的两次报告进行比对，比对的内容有：任务名称、对象范围、任务类型、两次报告的生成时间对比、两次报告的漏洞数量对比（按照总数、严重级别）、两次任务中发现相同和不同的漏洞；比对结果可以导出为 PDF、Word 等格式。

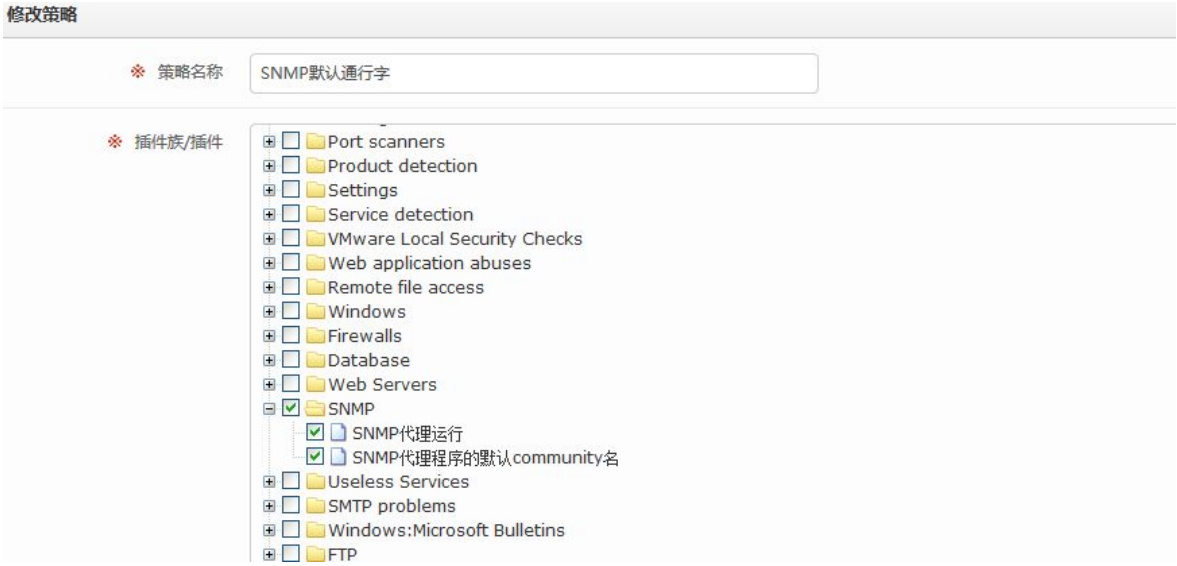
4.5.5.3. 漏洞扫描策略管理

漏洞的扫描策略管理在“安全策略”模块中。漏洞扫描策略包括如下操作：

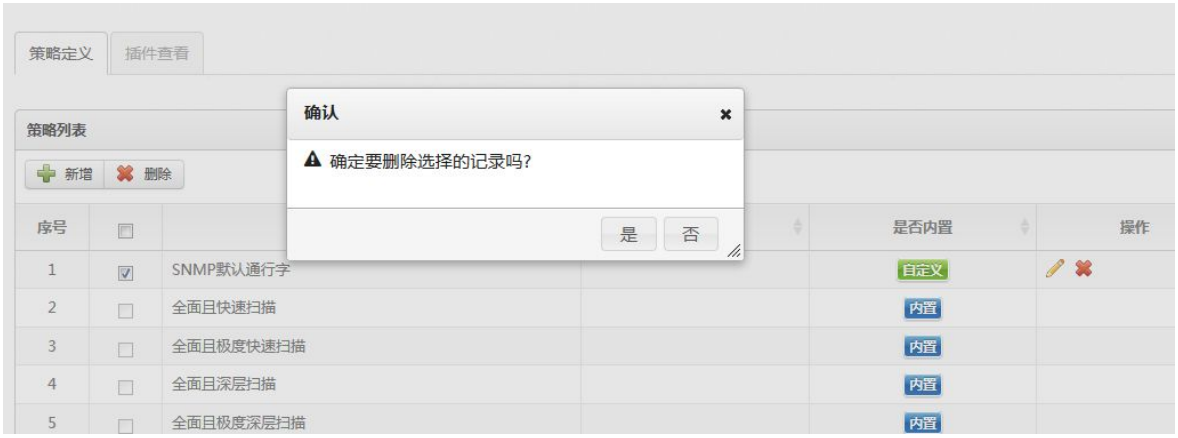
1. 漏洞策略新增：输入相关漏洞策略属性，包括名称描述等，选择系统已有插件（插件按插件族（Family）进行组织和呈现；另外，用户也可以查看漏洞插件的相关属性）进行添加。如下图所示：



2. 漏洞策略修改：在策略中选择一个需要修改的策略（策略即使被任务引用也应该能够修改）；重新在系统已有插件中选择若干插件。如下图所示：



3. 漏洞策略删除：在策略中选择一个或多个需要删除的策略，提交删除请求。如下图所示：



4.6. 安全基线管理

与漏洞管理类似，在铱迅信息的安全运营中心系统中，安全基线管理中的任务管理和策略管理以及结果的展示，分别被划分在不同的功能菜单中。其中安全基线检查任务管理在“任务管理”中，安全基线策略管理则在“安全策略”模块中，而在安全仪表板、资产管理和风险管理中均可查看到安全基线检查结果，只不过维度存在一定的差异；但为了能使用于对于安全基线管理有一个整体的认识，故在本手册中也将它们合并进行介绍。

与扫描漏洞类似，安全基线的违规也是系统脆弱性的重要来源之一。

4.6.1. 什么是安全基线

严格来说，安全运营中心中的安全基线应称作“安全配置基线”，它们是各类系统、数据库、安全设备、中间件的安全配置基准，如果违反则称作“安全基线违规”；例如，操作系统的口令长度过短、口令更改时间过长、未配置记录日志功能等等。

4.6.2. 为什么需要安全基线检查

这是因为如下几点原因：

1. 企业内有众多的、不同类型的主机、网络设备、安全设备、数据库、中间件
2. 这些系统都存在配置安全问题
3. 安全配置问题，特别是口令强度不够是黑客攻击的主要手段

而以往我们都是人工对这些配置的安全情况进行检查，这存在如下不足：

1. 工作量很大
2. 不同的系统类型使用的检查方法存在较大差异
3. 一般只在系统加固前进行评估，无法适应系统的变化情况
4. 无法方便地对检查结果进行统一的分析和比较

4.6.3. 什么是安全基线检查策略

由于在安全运营中心中，每种系统的安全基线被拆分为不同的插件，故在进行安全基线检查时需要将其组合起来进行，所以安全基线检查策略也就是这些插件的集合。与漏洞扫描策略管理类似，我们一般也不建议用户自定义安全基线检查策略，因系统内已经内置了这些策略（每种系统均有一个默认策略）。

4.6.4. 安全基线检查的先决条件

由于一般安全基线检查是通过远程方式进行，故用户需要配置资产的登录凭证而且目标资产必须能被安全运营中心的某个采集管理器所管理（必须配置“配置获取”型的采集器）。

4.6.5. 相关操作

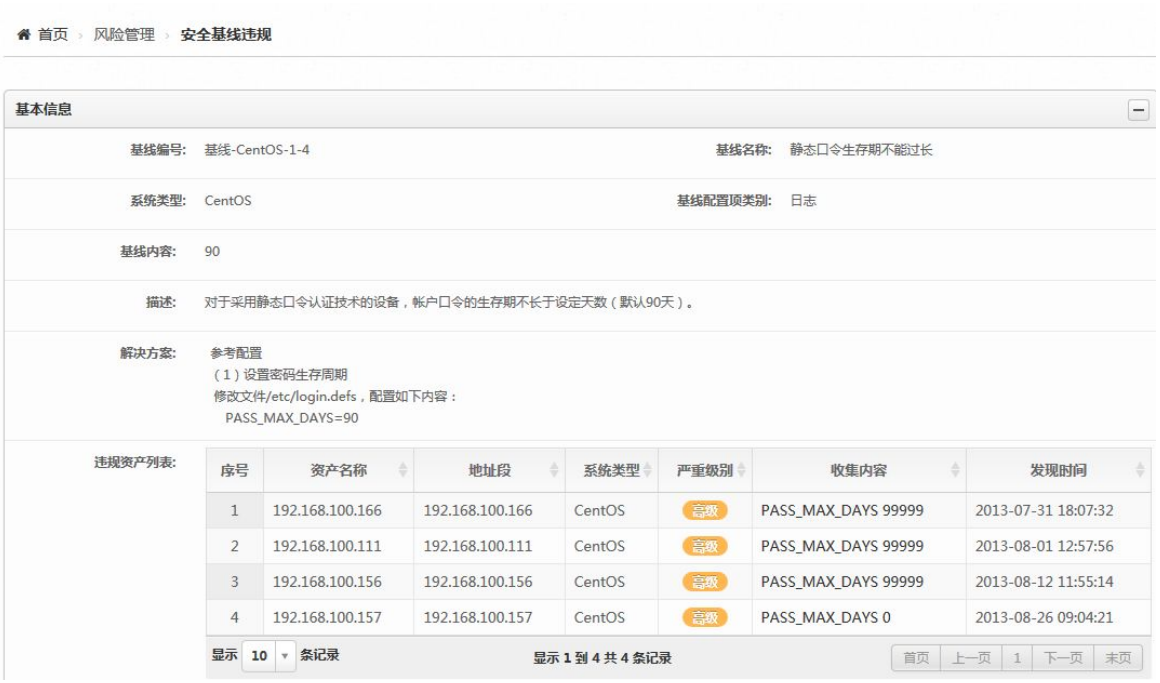
4.6.5.1 安全基线违规管理

安全基线违规管理的相关操作包括：

1. 违规列表：需显示系统内所有的违规信息情况，以列表方式呈现，列表查看时可以依据某种选中的视图（和用户个人相关），也可不选择任何视图查看；列表内容包括：违规基线名称、违规基线描述、违规对象数。如下图所示：

序号	违规基线编号	违规基线名称	违规基线描述	系统类型	违规对象数	操作
1	基线-CentOS-1-4	静态口令生存期不能过长	对于采用静态口令认证技术的设备，帐户口令的生存期不...	CentOS	3	
2	基线-CentOS-1-5	静态口令不能连续重复使用	对于采用静态口令认证技术的设备，应配置设备，使用户...	CentOS	2	
3	基线-CentOS-1-6	连续登录失败账号锁定	对于采用静态口令认证技术的设备，应配置当用户连续认...	CentOS	2	
4	基线-CentOS-1-8	检查是否存在除root之外UID为0的用户	帐号与口令-检查是否存在除root之外UID为0的...	CentOS	1	
5	基线-CentOS-2-11	检查异常隐含文件	文件系统-检查异常隐含文件	CentOS	1	
6	基线-CentOS-3-3	远程日志功能配置检查	设备配置远程日志功能，将需要重点关注的日志内容传输...	CentOS	2	
7	基线-CentOS-3-4	日志功能配置检查	设备应配置日志功能，对用户登录进行记录，记录内容包...	CentOS	3	
8	基线-CentOS-3-6	安全事件日志功能检查	设备应配置日志功能，记录对与设备相关的安全事件。	CentOS	1	
9	基线-CentOS-3-7	启用记录cron行为日志功能	启用记录cron行为日志功能	CentOS	2	

2. 违规详细查看：在安全基线违规列表中，选择某个违规信息，可进一步查看该违规的详细信息。包括：基线编号、基线名称、基线配置项类别、基线内容、系统类型、描述、解决方案等。如下图所示：

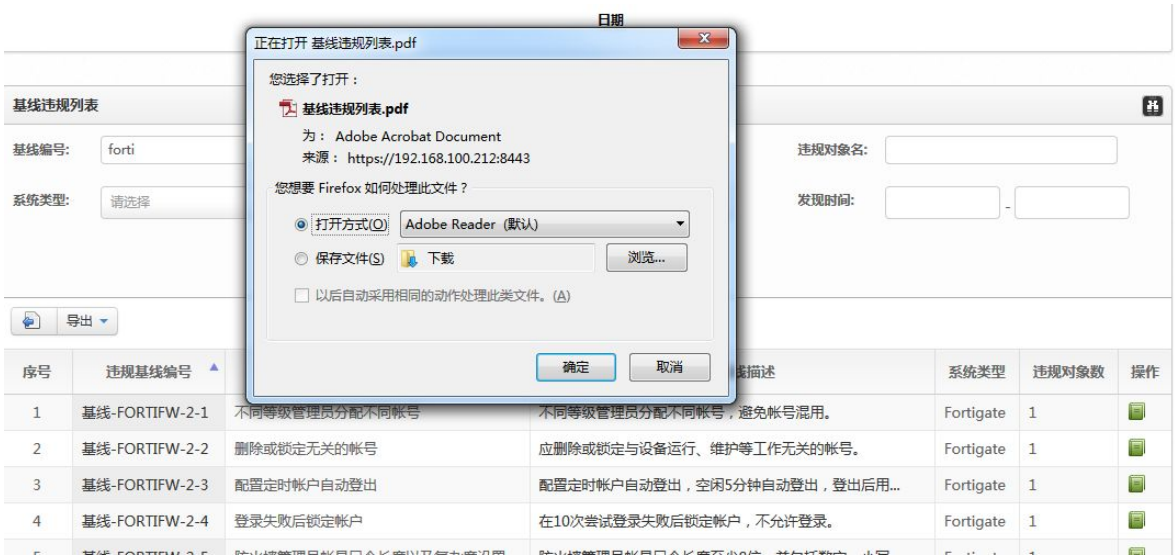


序号	资产名称	地址段	系统类型	严重级别	收集内容	发现时间
1	192.168.100.166	192.168.100.166	CentOS	高级	PASS_MAX_DAYS 99999	2013-07-31 18:07:32
2	192.168.100.111	192.168.100.111	CentOS	高级	PASS_MAX_DAYS 99999	2013-08-01 12:57:56
3	192.168.100.156	192.168.100.156	CentOS	高级	PASS_MAX_DAYS 99999	2013-08-12 11:55:14
4	192.168.100.157	192.168.100.157	CentOS	高级	PASS_MAX_DAYS 0	2013-08-26 09:04:21

显示 10 条记录　显示 1 到 4 共 4 条记录　首页 上一页 1 下一页 末页

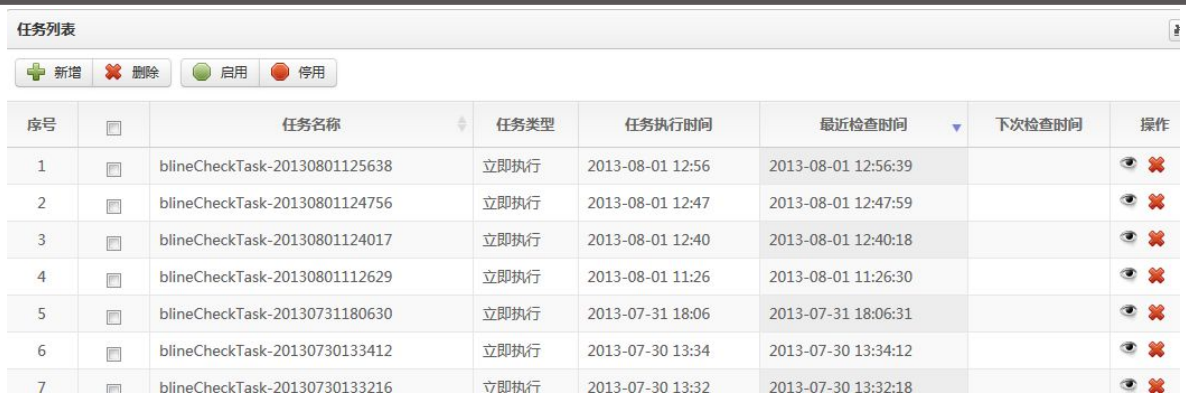
3. 查询：在违规列表中提供查询功能，输入相关查询字段进行查询。可查询字段参看上文“安全基线违规”属性表。如下图所示：

4. 导出报表：在违规列表中，点击导出按钮，选择导出的格式类型，支持格式包括 WORD、PDF、HTML 等。如下图所示：



4.6.5.2 安全基线检查任务管理

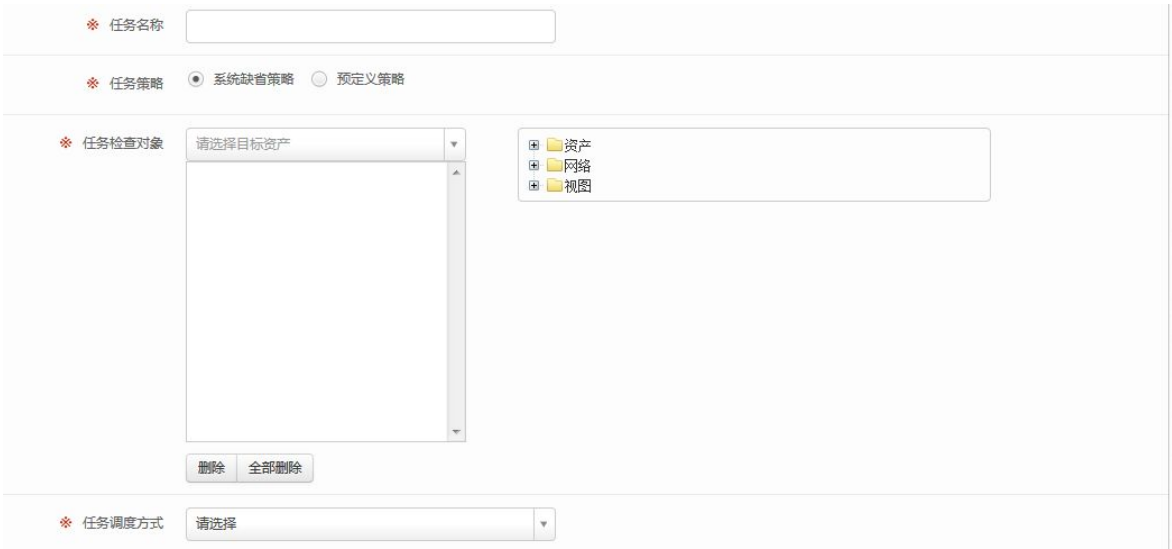
1. 任务列表：安全基线任务列表包括：任务列表（可定义任务）、正在执行任务、已完成任务三部分；如下图所示：



2. 任务查询：系统提供任务查询功能，在列表上方提供查询区域，输入查询条件，包括任务名称、任务类型、执行时间等。如下图所示：

定义任务

3. 任务新增：用户输入任务名称、收集对象（以 IP 为对象，可以是单个 IP 或是个 IP 地址段）、检查策略、任务调度方式（定时、立即执行、一次运行）、描述等。如下图所示：



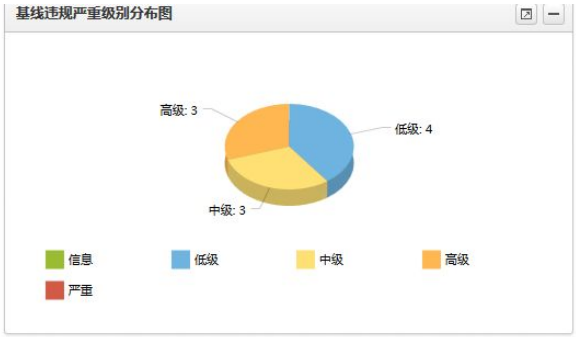
4. 任务删除：在列表中选择需要进行删除的一个或多个任务；点击删除功能进行删除，删除前提示用户是否删除该任务，另如任务正在执行也可以删除；删除成功，在列表界面中看不到该任务相关信息，该任务之前完成的安全基线检查将参与统计，系统不提供查看删除后查看任务对应产生的报告功能。

5. 停止调度：对于周期型任务可以停止调度。如下图所示：

6. 恢复调度：对于已经被停止调度的任务，用户可以选择恢复调度。

任务执行结果

7. 报告查看：选择某一任务，可查看该任务详细报告情况，详细内容包括：任务基本信息（包括任务名称、开始时间、结束时间、任务类型、检查策略）、基线违规严重级别分布图、主机列表（包括主机 IP 地址、任务执行状态、符合、不符合、基线类型）、产生违规主机的详细信息（包括基线名称、基线编号、严重级别、发现时间、描述、解决方案等）。如下图所示：

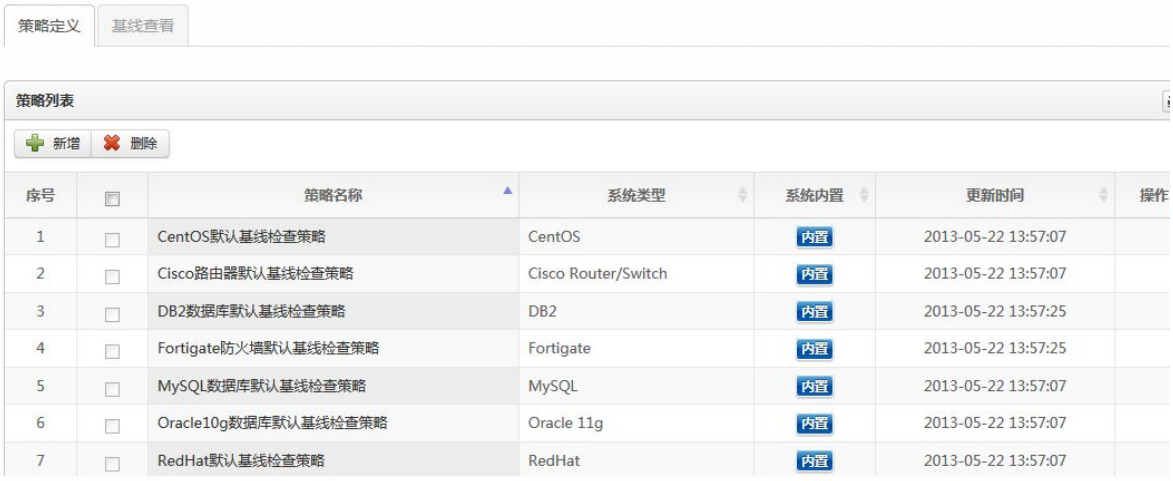


8. 报告导出：在任务列表中进入详细报告功能，在详细报告页面中可导出报告，支持 Word、PDF 等格式。
9. 报告对比：点击一个任务，在报告列表中选择 2 个报告；报告内容包括任务名称、任务类型、两次报告的生成时间对比、两次报告的基线数量对比（按照总数、严重级别）、两次报告的基线合规率对比、两次任务中发现相同的和不同的基线。

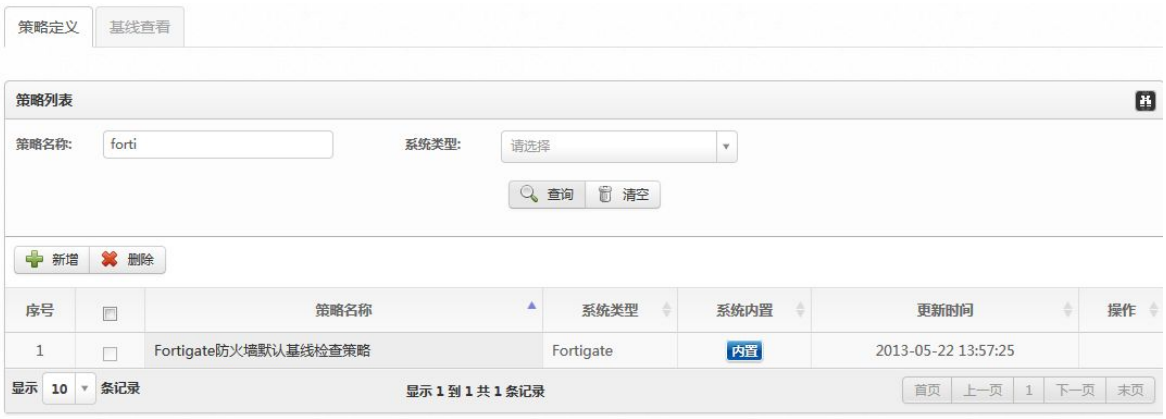
4.6.5.3 安全基线策略管理

安全策略的操作包括如下内容：

1. 策略列表：以列表方式呈现安全基线策略信息，列表内容包括策略名称、系统类型、更新时间等，如下图所示：

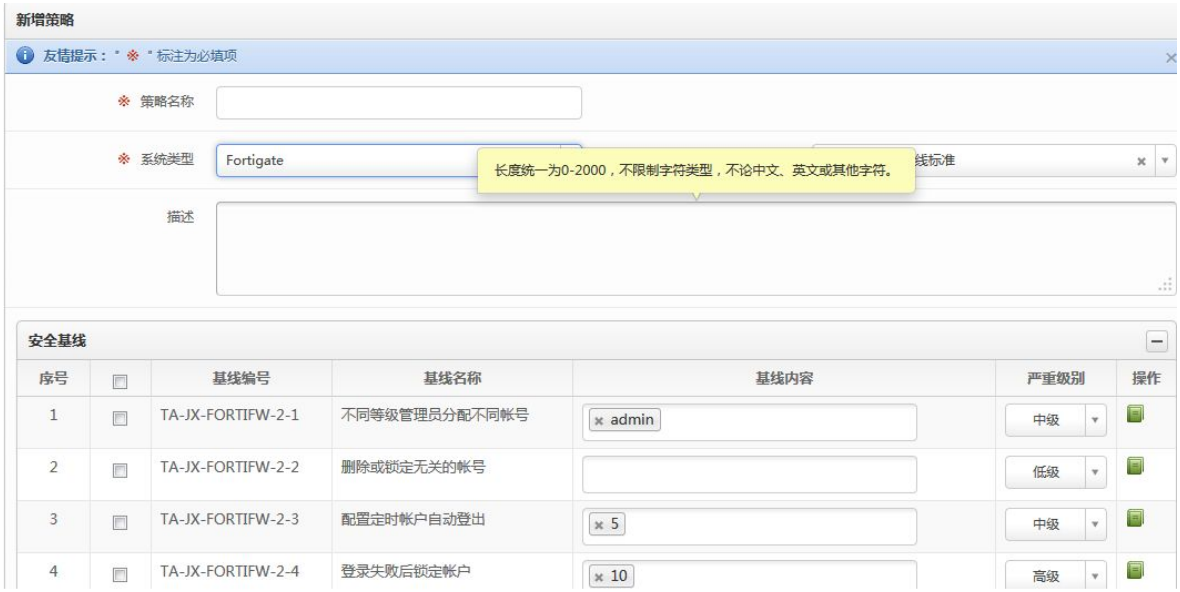


2. 策略查询：系统提供安全基线策略查询功能，支持的查询条件包括：策略名称、系统类型等，如下图所示：



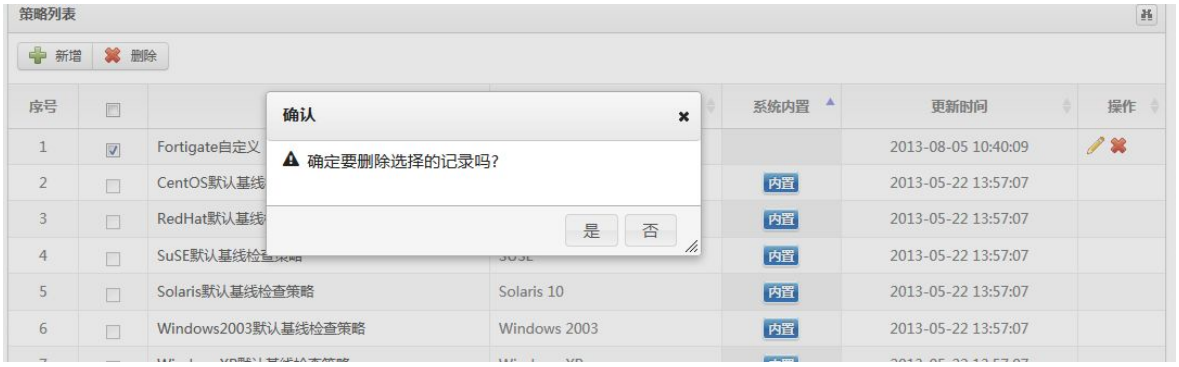
3. 查看策略：在策略列表中，选择某个策略，查看所选策略信息，策略内容包括策略基本信息（包括策略名称、系统类型、策略描述等），策略所有安全基线信息（包括基线名称、基线编号等）。

4. 新建策略：系统除了内置安全策略，也提供新建策略功能，在新增功能页面，选择系统类型、基线标准、输入策略名称、描述、选择需进行安全检查的基线项并定义基线项严重级别等。如下图所示：



5. 修改策略：系统新建的策略可进行修改，在修改功能页面，可修改策略描述、修改选择的需进行安全检查的基线项并重定义严重级别；系统内置策略不可以修改。

6. 删除策略：用户可以删除一个到多个自定义策略，但不能删除系统内置策略。如下图所示：



7. 基线列表：以列表方式呈现安全基线信息，列表内容包括基线编号、基线描述等。如下图所示：

序号	基线编号	基线名称	系统类型	基线配置项类别	操作
1	基线-FORTIFW-2-1	不同等级管理员分配不同帐号	Fortigate	访问控制	
2	基线-FORTIFW-2-2	删除或锁定无关的帐号	Fortigate	访问控制	
3	基线-FORTIFW-2-3	配置定时帐户自动登出	Fortigate	访问控制	
4	基线-FORTIFW-2-4	登录失败后锁定帐户	Fortigate	访问控制	
5	基线-FORTIFW-2-5	防火墙管理员帐号口令长度以及复杂度设置	Fortigate	访问控制	
6	基线-FORTIFW-2-6	登录失败后锁定帐户设置解锁时间	Fortigate	访问控制	
7	基线-FORTIFW-3-1	日志记录设置	Fortigate	日志	
8	基线-FORTIFW-3-2	远程日志记录设置	Fortigate	日志	

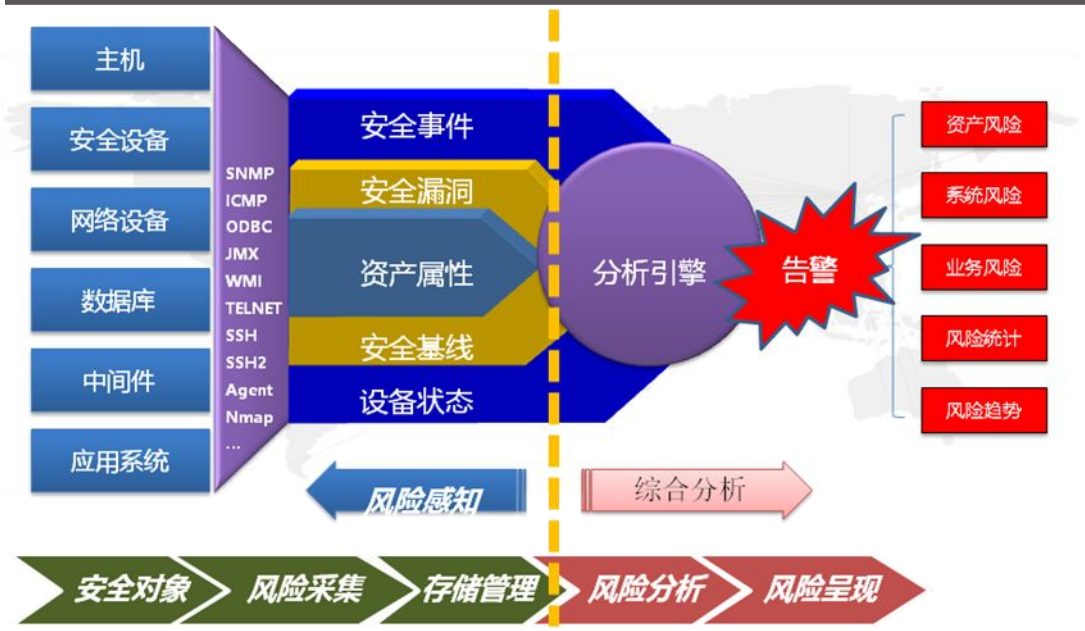
8. 查看基线详细：在列表中选择需要进行查看详细的安全基线；显示该安全基线详细信息，包括基线编号、基线名称、基线配置项类、基线配置项内容、基线描述、解决方案等。如下图所示：

4.7. 安全事件管理

与漏洞管理和安全基线管理类似，安全事件管理中的接入管理、策略管理分别在系统管理（组件管理）和安全策略管理中，而安全事件的查看、查询、导出等则在风险管理中，故没有单独的模块称作“安全事件管理”。

如用户对如何编写标准化策略、如何接入常用系统或设备的日志有更进一步了解的需求，请参见专门的事件管理用户手册。

下图说明了安全运营中心系统是如何处理事件的：



4.7.1. 什么是日志

从各类设备或系统中产生、能代表其运行状态、配置状态及报警等数据，如用户登入/登出、系统启动/停止等。

一般日志均有不同的等级，例如 Syslog 就包含有 8 个等级，分别从 0 到 7，级别越高数值越小，另外，Syslog 中还包含有可以表示其日志产生模块或类型的 facility 属性，这在分析日志时也经常会被用到；而对于 Windows 的 EventLog 则是另外一种形式，其级别包括错误、警告、信息、成功审核或失败审核，其日志的类别包括系统、安全和应用类型。

4.7.2. 日志是如何采集的

铱迅安全运营中心对各类日志的采集一般是通过如下几种方式：

1. Syslog：这是一种最为常见的形式，一般 Linux/Unix 主机、各类网络设备、安全设备等均支持将自身日志通过 Syslog 形式发送出来
2. SNMP Trap：这也是一种较为常见的形式，一般网络设备和部分安全类设备可以发送此类日志
3. 数据库：不是特别常见，有些防毒类产品、VPN 设备仅支持这种类型，它需要设置若干参数方可获取，如数据库的类型、IP 地址、服务监听端口、实例名称、日志表名、序列字段等；安全运营中心是主动获取此类日志的
4. Socket：直接连接到相关的设备服务，设备通过双方约定的格式传递日志信息；OPSEC 也是一类特殊的 Socket 日志接入方式，目前仅针对 CheckPoint 防火墙
5. 文件：从外部的文件中逐行（有时候也支持将多行合并为一行）获取日志，它一般用于无法直接或实时获取设备、系统日志的场合（用户需将日志单独导出成文件，传送到安全运营中心指定的目录或自行设置的目录下）

6. SMB：这是一类基于文件共享（SAMBA）的日志接入方式
7. WMI：Windows 系统日志的主要接入方式

4.7.3. 什么是安全事件

能表达或反映某种安全问题的日志或数据，包括攻击类、恶意代码类、异常行为、敏感行为类等。

4.7.4. 标准化

鉴于各类设备或系统产生的日志、安全事件格式五花八门、形式不一而足，故在安全运营中心进行分析之前需要进行标准化，如下列不同设备的日志：

SUN Solaris

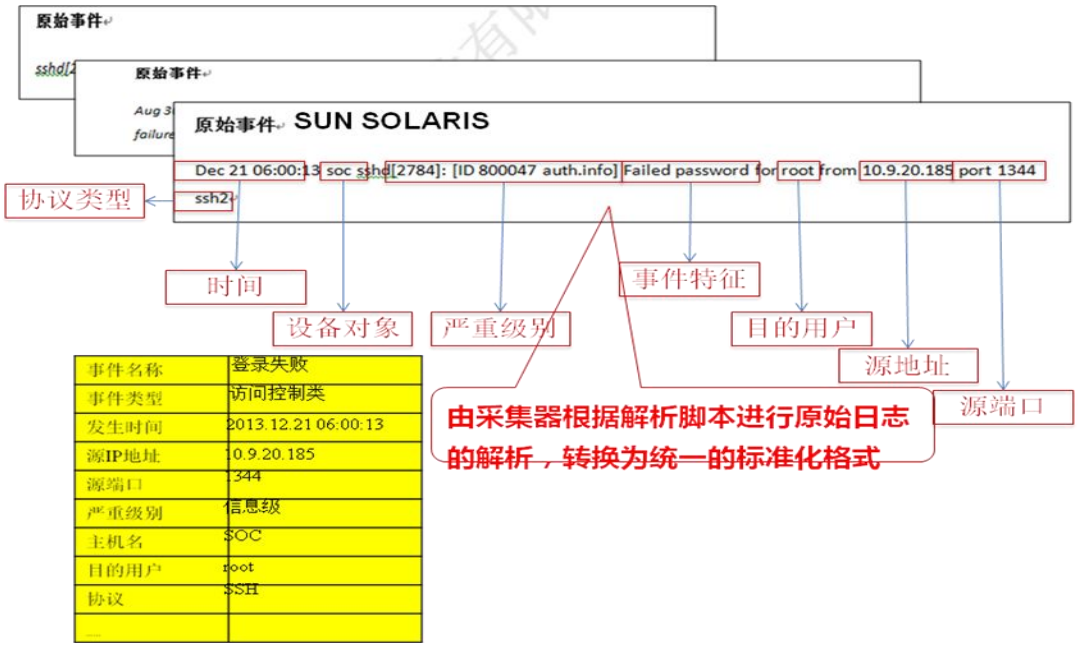
Aug 27 13:04:09 sshd[3228]: [ID 70112 auth.info] Failed password for root from 79.16.133.71 port 4489 ssh2

Cisco 路由器

4066: Aug 17 20:04:31.388: %SEC-6-IPACCESSLOGP: list ZJ_MPLSLINK_IN permitted tcp 129.9.11.247(9801) -> 10.34.14.200(1067), 203 packets

标准化的目的实际上就是将类似上述不同的日志进行规格化,然后存储为内部格式。例如，我们会将第一条日志的名称转换为“root 用户登录失败”，将源地址转换为“79.16.133.71”；而第二条的名称则会转换为“连接”,源地址、源端口、目的地址和目的端口分别转换为“129.9.11.247”、“9801”、“10.34.14.200”和“1067”。

下图为一个日志标准化的示例：



至于，如何编写标准化脚本，则会在相关文档再进行详细介绍，本文不再涉及。

4.7.5. 什么是过滤和归并

有时，为了使用户集中关查看他所需要关注的相关日志或事件，或者有时我们并不需要保存所有的原始日志或事件，那么我们可以设置一个或多个过滤或归并策略。

其中，过滤与归并策略的不同点在于，归并策略既可以丢弃被归并的原始日志或事件，也可以保留这些原始日志或事件，而如命中过滤策略则直接丢弃，当然归并策略中也包含需要归并的一个到多个字段。

在后面的操作中可以看出，过滤或归并策略是应用在采集器上的，而且一个采集器可以包含多个过滤策略和归并策略。

4.7.6. 安全事件的关联

为了挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系，系统提供了关联功能，该功能的具体使用方法见下。

关联的类型包括基于规则的和基于统计的。

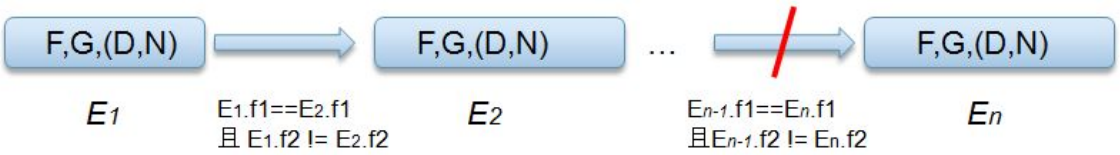
基于规则

基于规则的关联条件是一个状态机，它包括若干个状态及关联运算符，且每两个状态之间均有一个关联运算符（即它是一个二元算子）；但与一般的关系运算不同的是，它有两种属性：

1. 时序：后续发生或后续不发生

2. 关联过滤条件：可选；前后状态之间的关联关系定义

其形式类似下图：



其中，F,G,(D,N)为一状态，F 表示过滤器，G 表示分组字段（支持多个），而 D 表示持续时间（以秒为单位，必须设置），而 N 为重复次数（可不设）。

需要注意如下几点约束：

1. 关联过滤条件不是必须的，但如果设置，则其左操作数和右操作数分别为相邻事件集的事件属性（属性类型必须相容），不能为常量且必须加入到各自状态的分组条件中（系统应提示并自动添加），例如：

E1[事件名称==”登录失败”,”源地址”,(60,3)] 后续发生[E1.源地址==E2.源地址] E2[事件名称==”登录成功”,”源地址”,(60,1)] 为合法，而

*E1[事件名称==”登录失败”,”源地址”,(60,3)] 后续发生[E1.源地址==E2.源地址 且 E1.目标地址==E2.目标地址] E2[事件名称==”登录成功”,”源地址”,(60,1)]*为非法，因为它没有将目标地址加入到分组条件中

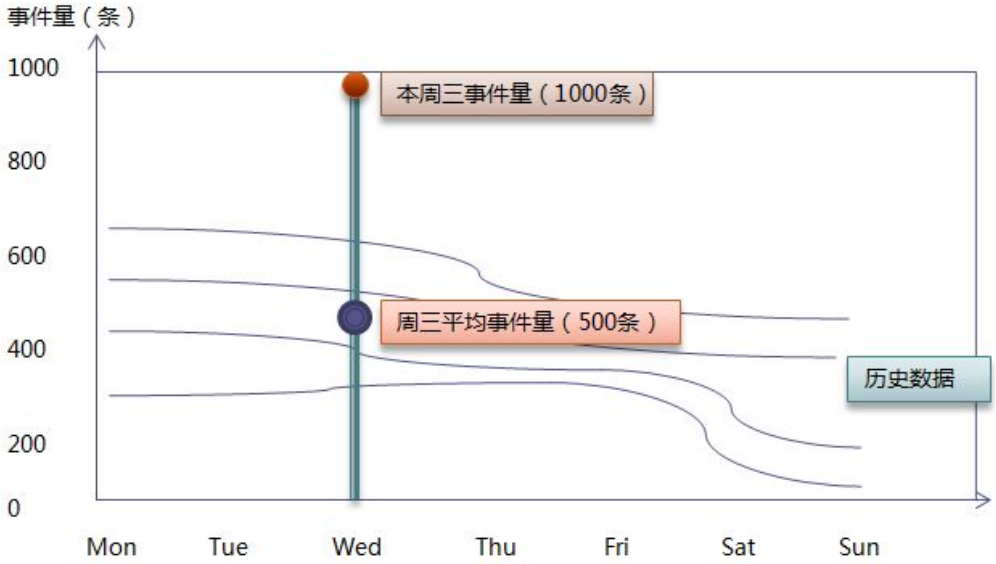
2. 对于关联条件中的过滤条件，其关系运算仅支持等于和不等于

3. 如果关联条件中的时序类型为后续不发生，则它必须是整个状态序列的最后一个（如上图所示），否则错误

基于统计

基于统计的关联需要有基线数据（这里的基线和安全基线管理中的基线不同）；基线类型包括日基线和周基线；其中日基线包含最近若干天，每个时段（以小时为单位）的基于指定聚合字段的统计数据，而周基线包括最近若干周每周几的基于指定聚合字段的统计数据。

下图周基线为例（假定学习了最近 4 周的数据），而过去一天为周三，则：



从上图可以看出，过去最近四周，周三的平均事件量为 500 条，而刚过去的一日为 1000 条，与基线相比，超出了 100%，如触发条件设定为 100，则触发响应。

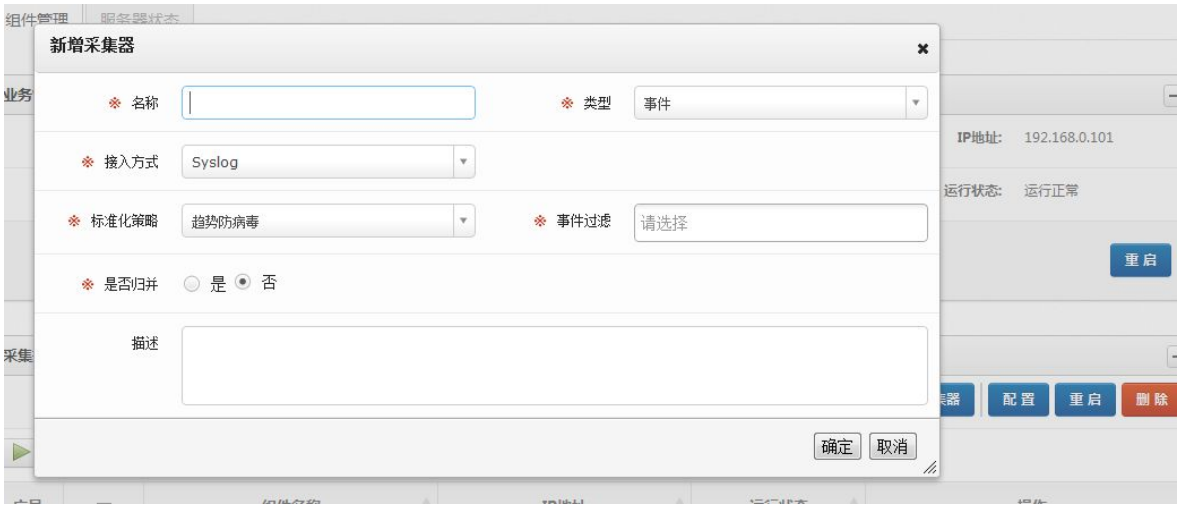
响应的类型包括如产生告警、邮件、Syslog 等。

4.7.7. 相关操作

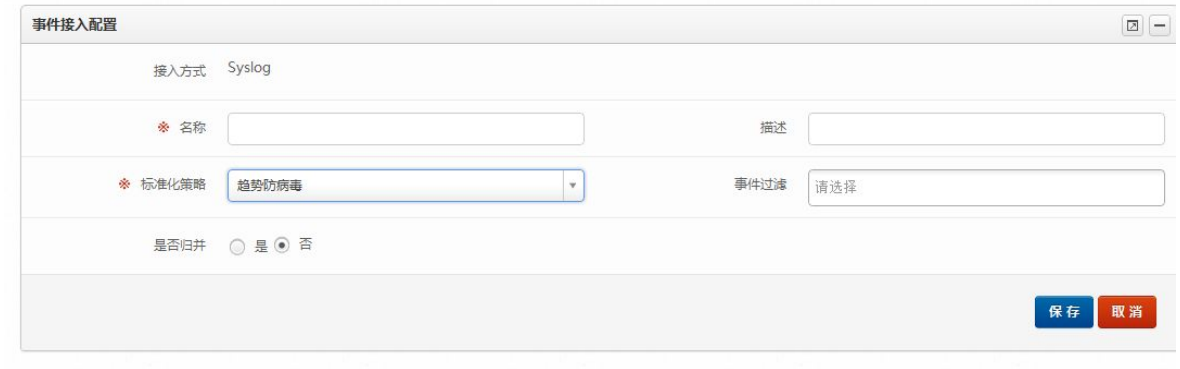
4.7.7.1 接入管理

事件接入管理是为了在采集控制器上设置需要接收、标准化哪些设备/系统的安全事件/日志；它是安全事件管理的核心内容，也是系统安全事件/日志的唯一来源。

1. 新建事件采集器：选择相应的采集控制器，配置事件采集器的名称、采集类型（Syslog、SNMP Trap、数据库等）、应用的标准化脚本（可以多选，但不能重复选择）、采集参数等字段；提交后系统会将相关配置传送到相应的采集控制器上。如下图所示：



2. 设置事件采集器：用户选择修改某个事件采集器的设置，提交后需将相关配置传送到相应的采集控制器上。如下图所示：

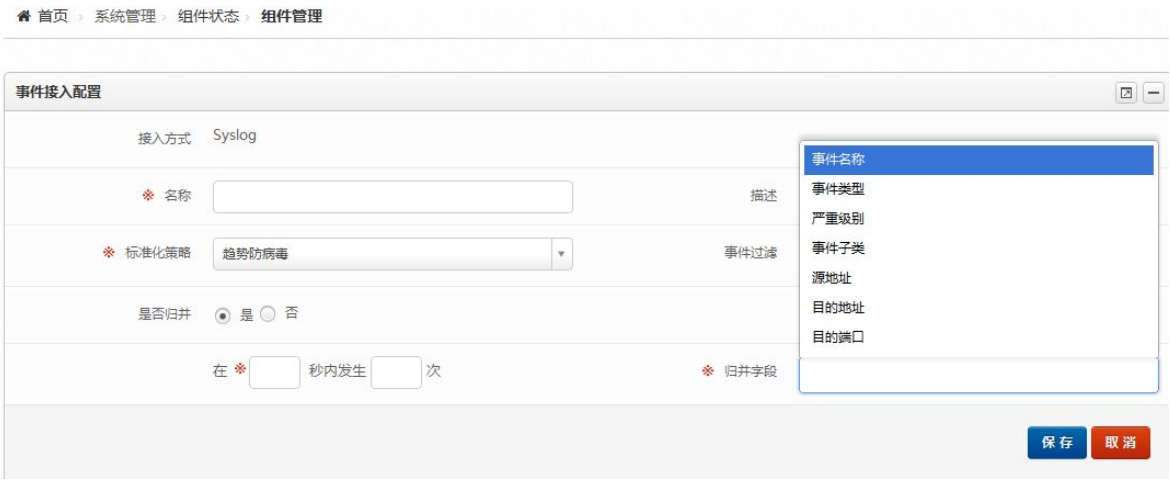


3. 删除事件采集器：用户可以选择删除一个或多个事件采集器，提交后相应的采集控制器应在自己的容器中进行删除。

4. 启用事件采集器：对于一个或多个已经停用的事件采集器，用户可以进行停用，如下图所示：

5. 停用事件采集器：对于一个或多个已经启用的事件采集器，用户可以进行启用。

6. 设置过滤策略或归并策略：用户可以为一个事件采集器选择需要应用的过滤策略、归并策略；用户也可以取消相关的设置；多个过滤器策略、归并字段可以调整其优先级。



4.7.7.2 安全事件管理

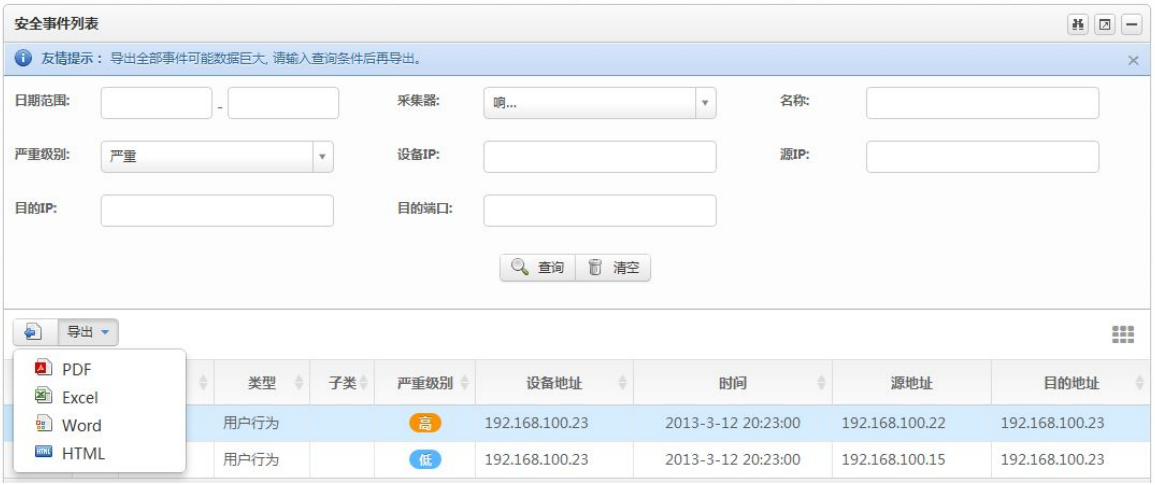
1. 事件查看：系统可按事件分类、子类查看事件，也可以按设备类型、产品名称两个视图对事件进行查看；事件列表字段不能排序，需按事件时间倒序排列，即最近发生的排列在列表最前。用户点击某个具体事件名称，系统显示相关事件的全部详细情况并可关联知识库查看其现象、分析和解决方案。如下图所示：

2. 事件查询：

- 在事件列表中输入相关字段的查询条件（必须包含事件时间属性；可查询字段参看安全事件属性）；如下图所示：

- 点击查询（如查询字段中含有事件时间则查询最小粒度为小时，而不是分钟或秒）；默认为查询当日事件，用户可以选择查询某个时间段的事件，若用户选择的时间段跨周，系统将按自然周以页签形式显示。

3. 事件导出：针对上述查询出的事件，用户可以选择将其导出，导出的格式为 csv，如遇有事件中含有逗号，则将其转义。如下图所示：

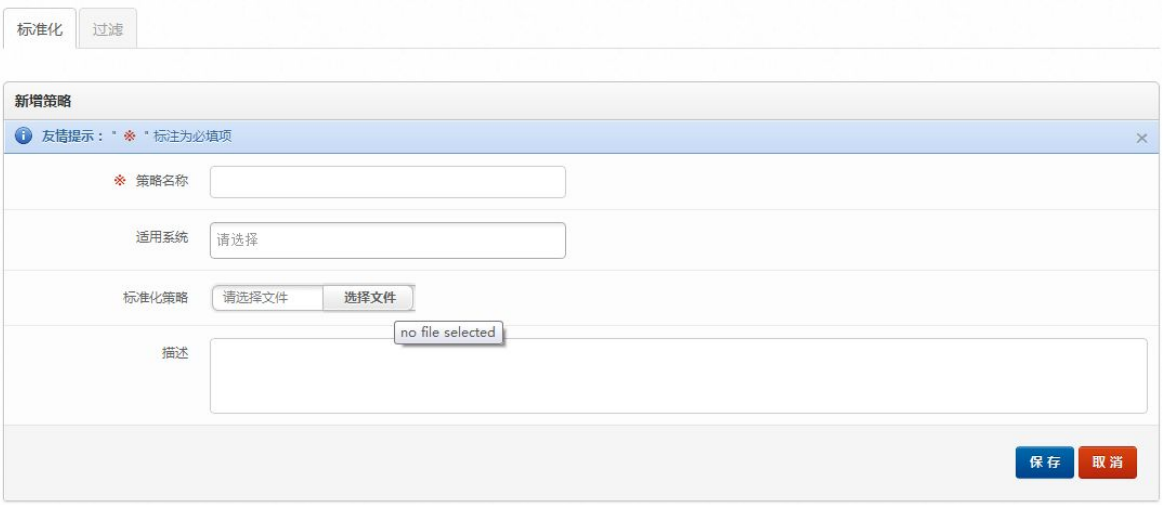


4.7.7.3 安全事件策略管理

- 标准化策略

需要说明的一点是系统内置的标准化策略是不能删除、修改的，而且它们是加密的。

1. 新建标准化策略：用户可以直接输入或从外部文件中导入标准化策略及其附加文件。如下图所示：



注意：在安全运营中心系统中，录入的标准化策略应是 UTF-8 编码格式，而不要使用 GB 系列编码，否则标准化后相关中文会变成乱码。

2. 修改标准化策略：在列表中选择需要修改的一个事件标准化策略，点击修改按钮 ；按事件标准化策略相关属性设置（如果此策略为系统内置则用户只能增加自定义部分，否则可以全部修改）；用户不能修改系统内置事件标准化策略。如下图所示：

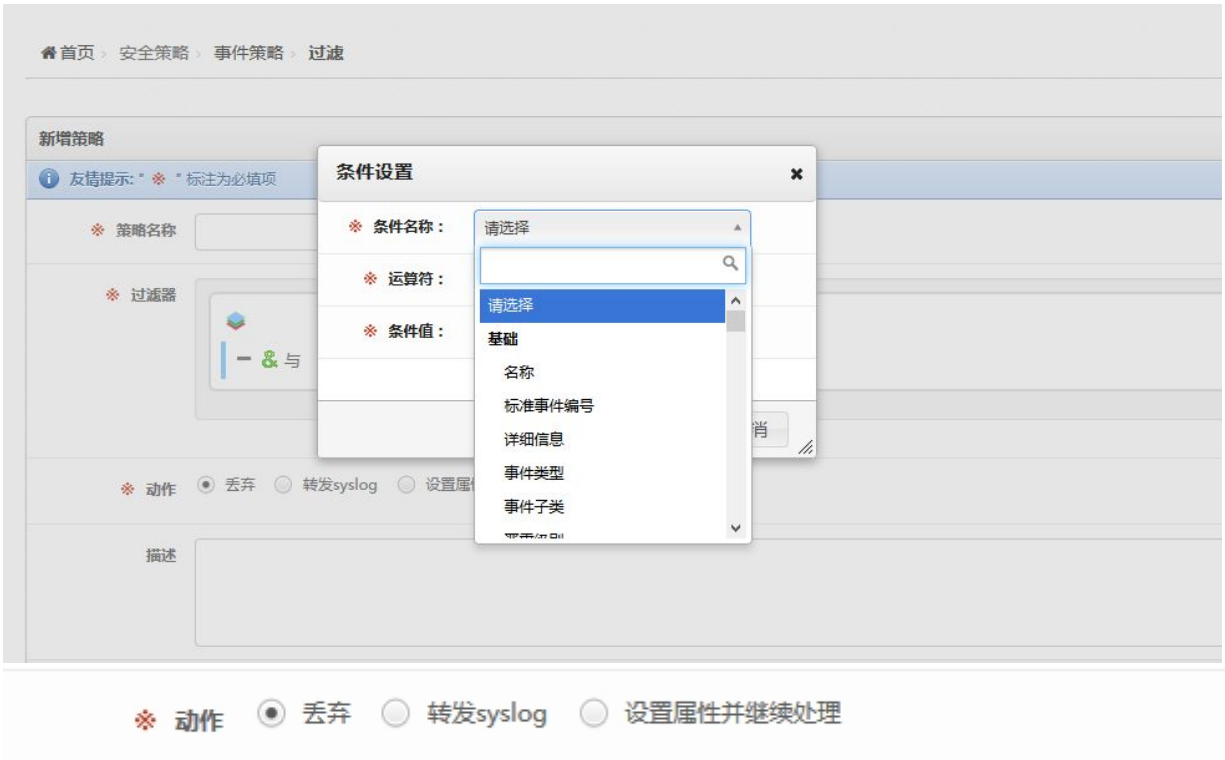
3. 删除标准化策略：在列表中选择需要删除的一个或多个事件标准化策略；如果该策略已经被应用则提示用户删除或修改相关事件采集器再删除策略；系统内置策略不能被删除。

4. 导出标准化策略：选择需要到出的一个或多个策略，选择存储的路径、输入需保存的文件名称，确定导出（仅针对自定义）。如下图所示：

过滤策略

1. 新建事件过滤策略：用户可以直接创建事件过滤策略，或从事件过滤器中选择一个作为事件过滤策略的组成部分；另外，一个事件过滤策略中可以包括如下动作：

- 丢弃
- 修改事件属性：修改命中过滤器事件的属性
- 转发：可以将命中事件通过 Syslog 方式（系统管理中定义的 Syslog 服务器或者直接指定 1 到 2 个 Syslog 服务器地址）转发到外部系统
- 执行外部命令：方式参见告警管理中的响应方式；参数为过滤器命中的事件；如下图所示：



2. 修改事件过滤策略：在列表中选择需要修改的一个事件过滤器，修改相关过滤器设置或动作设置；用户提交修改后，提示是否立即应用到采集器上。

3. 删除事件过滤策略：在列表中选择需要删除的一个事件过滤策略，提交删除请求。

4. 启用事件过滤器策略：在列表中选择需要启用的一个到多个事件过滤策略（状态为停用），提交启用请求。

5. 停用事件过滤器：在列表中选择需要停用的一个到多个事件过滤策略（状态为停用），提交停用请求。

- 告警策略

参见安全策略管理中数据来源为“事件”且“基于规则”的相关操作部分。

4.8. 设备状态管理

4.8.1. 什么是设备状态

设备状态是指各类设备或系统运行的状态，其状态主要包括：

1. 设备的运行时长（其实是 SNMP 服务的运行时长）

2. 通/断情况

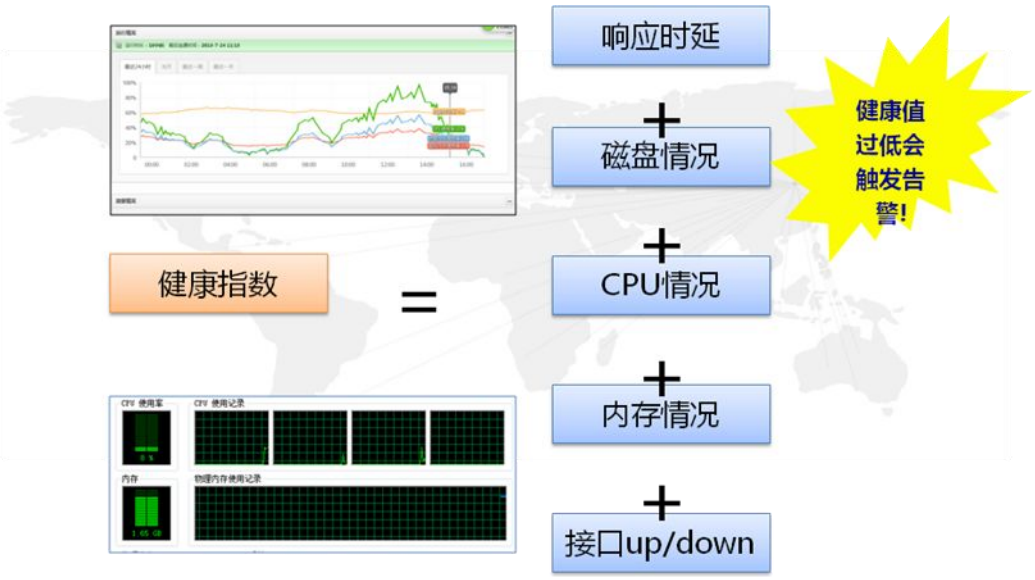
3. CPU 使用情况

4. 内存的使用情况：一般指物理和虚拟内存的使用情况，而对于 Linux/Unix 主机主要是物理交换内存的使用情况

5. 接口可用情况：一般会过滤掉本地回环接口，如 loopback、lo 等；用户也可以指定需过滤的接口，以免计算结果无法反映真实情况

6. 接口流量：会统计单个接口以及全部接口的网络流入和流出流量

通过获取各个系统或设备的运行情况，安全运营系统可以计算它的健康指数，如下图所示：



用户需注意，如果某设备或系统上的 SNMP 服务未启动，系统也会认为该系统或设备的状态无法获取，从而导致健康指数为 0。

4.8.2. 什么是 OID

OID 是简单网络管理协议中所使用的对象标识（Object IDentification）。每个 OID 均代表一组或一个对象的定义；一般，在 RFC 中规定了一些标准的 OID（如系统描述、接口名称、速率等），而某些系统或设备也制定了自有的 OID（如思科网络设置中的 CPU 使用率等）。

所以，安全运营中心系统既内置了一些已知的 OID，也提供了相关的扩展功能，使用户能灵活定义自有的 OID。

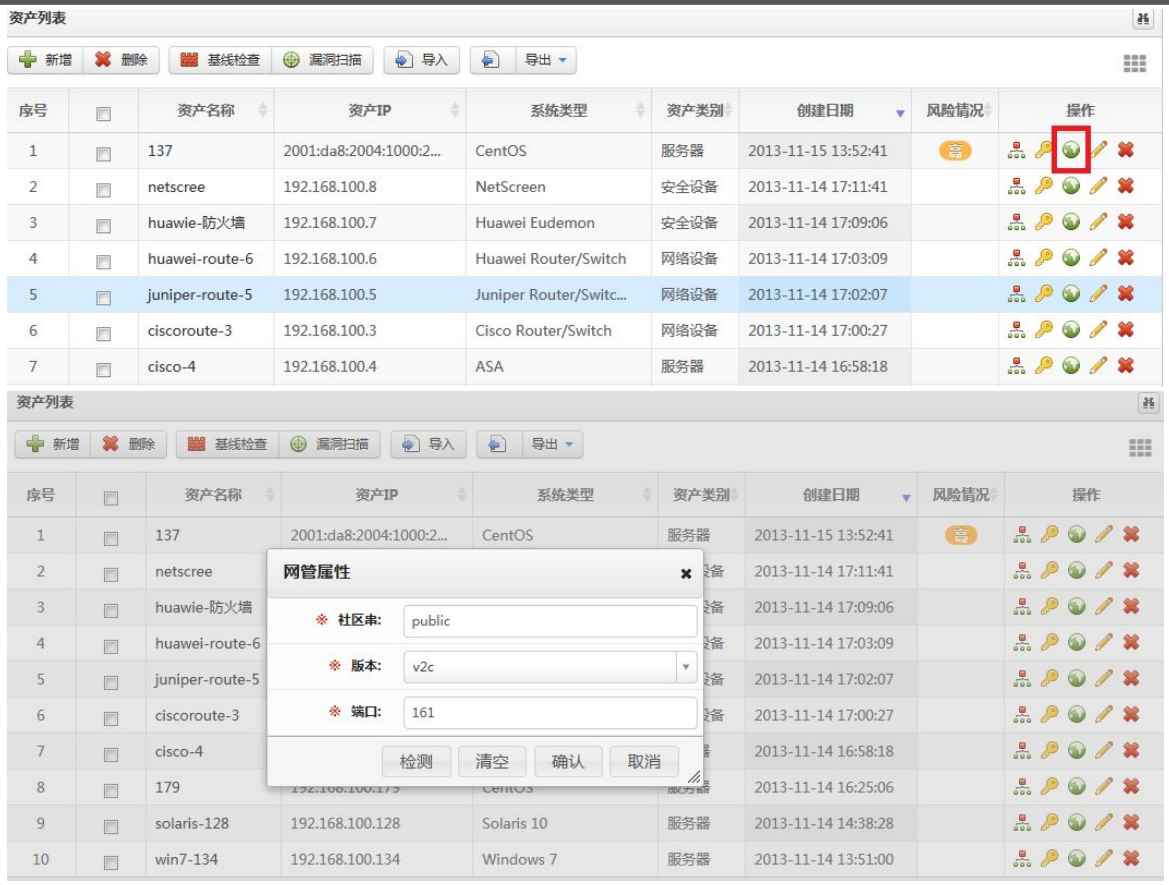
4.8.3. 设备状态是如何采集的

安全运营中心系统是通过简单网络管理协议（Simple Network Management Protocol）获取目标对象的运行状态的，目前支持 V1、V2C 和 V3 三个协议版本，V3 支持 AuthPriv、AuthNoPriv 和 noAuthNoPriv 三个安全等级；故用户如需要使用此功能应先在**资产管理中配置相关参数**并且在目标上**开启 SNMP 代理**并**授予相关权限（如哪些主机可以进行查询以及可以查看哪些对象标识，即 OID）**。

4.8.4. 相关操作

4.8.4.1 资产参数设置

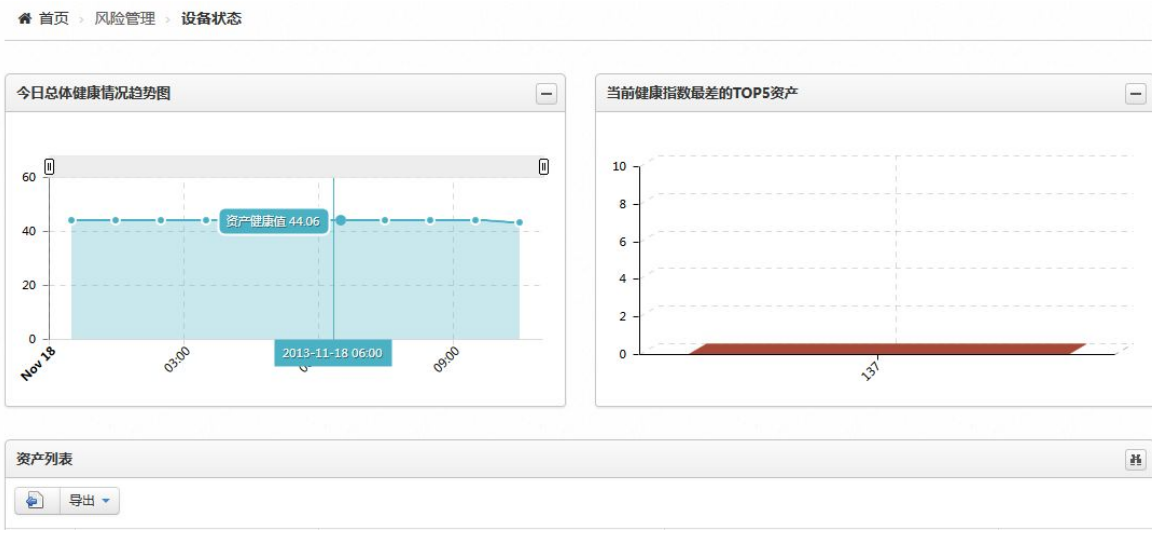
如前所述，在获取某个资产的运行状态之前，用户应在资产管理中设置其参数，包括社区串、端口和协议版本，如下：



4.8.4.2 状态查看

当获取相关资产状态后，用户可以在风险管理或资产管理中查看到相应的数据。

在风险管理“设备状态”栏中可以看到：



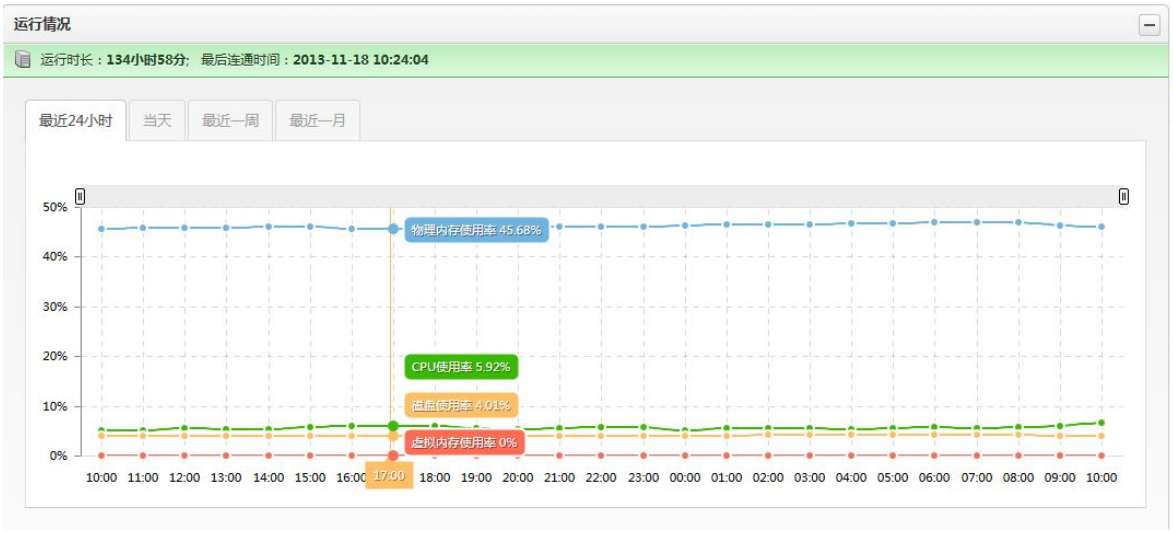
各个资产的健康情况也可以从列表中看到：

资产列表

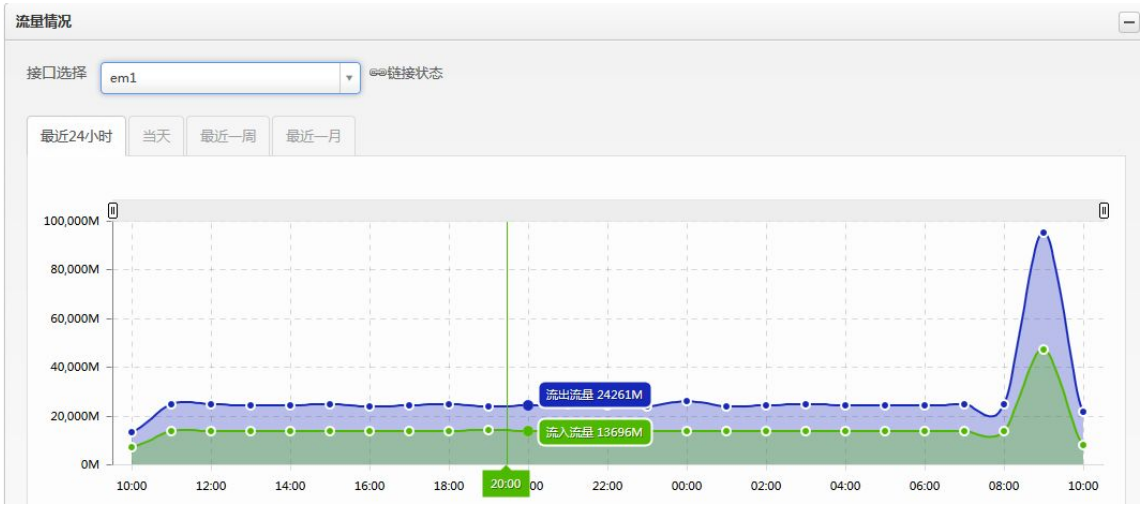
导出

序号	资产名称	资产IP	系统类型	健康指数
1	156	192.168.100.156	CentOS	危
2	231	192.168.100.231	CentOS	危
3	136	192.168.100.136	CentOS	危
4	150	192.168.100.150	CentOS	危
5	179	192.168.100.179	CentOS	危
6	cisco-4	192.168.100.4	ASA	危
7	juniper-route-5	192.168.100.5	Juniper Router/Switc...	危
8	huawei-route-6	192.168.100.6	Huawei Router/Switch	危
9	137	2001:da8:2004:1000:2...	CentOS	危
10	solaris-128	192.168.100.128	Solaris 10	差

如果进入资产，还可以看到如下详情：



也可以查看到该资产各接口的流量情况：

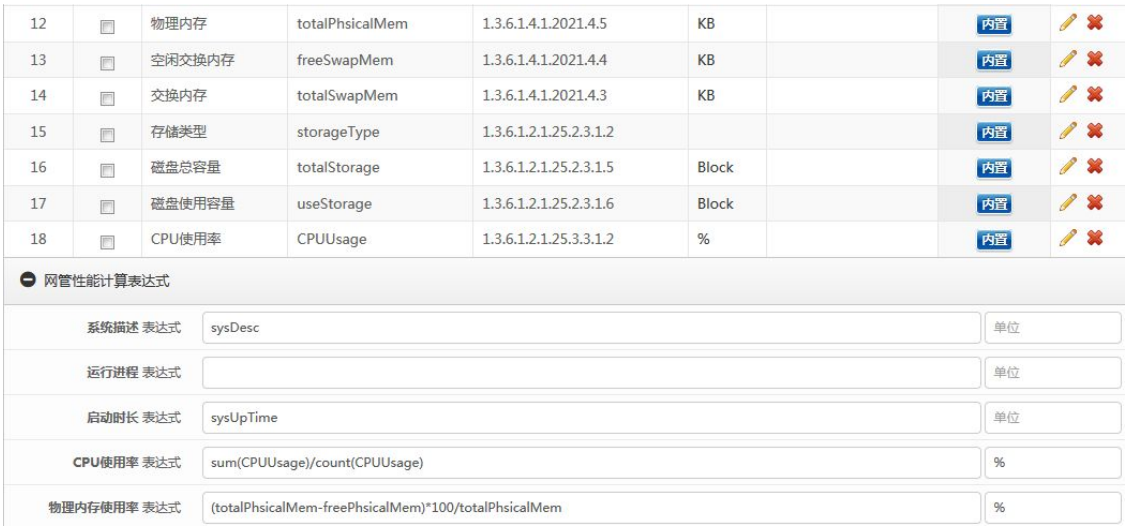


4.8.4.3 告警制定

如果用户需要对某个资产的运行状态制定告警策略，则可以进入策略管理->告警策略中定义数据来源为“资产健康状况”的策略，如下：

4.8.4.4 网管参数设置

如果用户需要修改内置的网管参数或者新增网管参数，可以进入系统管理->内置对象->系统类型进行设置，如下：



4.9. 安全策略管理

铱迅信息的安全策略管理集中包括了所有系统内可能需要使用到的各类安全策略，如漏洞扫描策略、安全基线策略、安全事件的标准化策略、安全事件的过滤策略、告警策略等等。其中，漏洞扫描策略、安全基线策略和安全事件相关策略均分别在漏洞管理、安全基线管理、安全事件管理中进行了介绍，本章仅介绍告警策略。

4.9.1. 告警策略的组成

安全运营中心的告警策略包含两个大类：其一为基于规则的，其二为基于统计的。不同类型的告警策略包含有不同的属性，分别描述如下：

4.9.1.1 公共属性

无论是基于规则的还是基于统计的告警策略均含有如下相同属性：

1. 策略名称：告警策略的名称
2. 策略描述：告警策略的描述信息
3. 知识库信息：和策略相关的知识库信息，包括告警的描述、症状、处理方法和参考等
4. 策略分类信息：策略的细分类型（可能是树状，基于管理需要）
5. 数据来源：目前包括安全事件/日志、漏洞和安全基线违规
6. 筛选器：一组过滤条件，其字段和数据来源具有紧密的关系；只有满足筛选器中规定的条件，系统方可进行后续处理
7. 响应方式：满足告警策略后所产生的动作，具体见下节

4.9.1.2 响应方式

响应方式包含如下：

1. 产生告警：系统产生告警，用户需输入产生告警的名称、严重级别、告警的分类信息（类别和子类）、告警处理人、告警生成的详细信息（告警信息和原始信息，可约束长度）；用户可以选择是否追加告警，追加告警的依据相同的对象（资产）上存在的相同名称的告警
2. 保存到活动列表：对于数据来源为事件/日志类型时，用户可以设置此响应方式；用户可以从系统中存在的活动列表中选择一个或直接创建一个新的活动列表；活动列表包括如下属性：
   - 活动列表名称
   - 活动列表描述

- 存活时间：列表中数据存活的时间，支持按分钟/小时/天来设置；最长不超过 30 天

- 字段定义：从事件字段中选取一个子集（详见相关需求文档的事件可归并字段）

需注意的一点是：同一个活动列表不能既出现在策略的筛选器部分又被其响应方式所引用。

3. 邮件通知：可设置邮件通知人（包括规则制定人的邮箱、相关资产响应人的邮箱、其它用户邮箱、自定义邮箱，其中自定义邮箱可以输入多个，中间用逗号分隔；可多选）

4. 转发外部系统：

- Syslog 方式：使用系统定义 Syslog 服务器或指定两个 Syslog 服务器

- SNMP Trap 方式：同上

默认转发外部系统内容均只含部分原始数据；系统应提供选项以便于用户转发所有原始信息（原始信息的转发字段应可以配置）；对于 Syslog 和 SNMP Trap 而言，由于其长度有限，系统应使用分片发送。

5. 执行程序：执行一个保存于核心分析组件的可执行程序或脚本，它应能在 CentOS 系统下被执行；参数之一为匹配的告警策略信息和原始信息。

4.9.2. 基于规则的告警策略

如告警策略为基于规则的且其数据来源为安全事件，除了上述公共属性外，它还应包括关联条件属性。

关联条件是一个状态机（这在安全事件管理部分已经介绍过），它包括若干个状态及关联运算符，且每两个状态之间均有一个关联运算符（即它是一个二元算子）；但与一般的关系运算不同的是，它有两种属性：

1. 时序：后续发生或后续不发生
2. 关联过滤条件：可选；前后状态之间的关联关系定义

4.9.3. 基于统计的告警策略

基于统计的告警策略只针对数据来源为事件/日志，它包括如下属性：

1. 统计类型：移动平均线、移动方差

2. 归并字段：根据不同数据来源，对原始数据进行分组统计

3. 统计字段：可选；目前仅支持安全事件的流出和流入字节数；如果不填则计算相关原始数据的数量

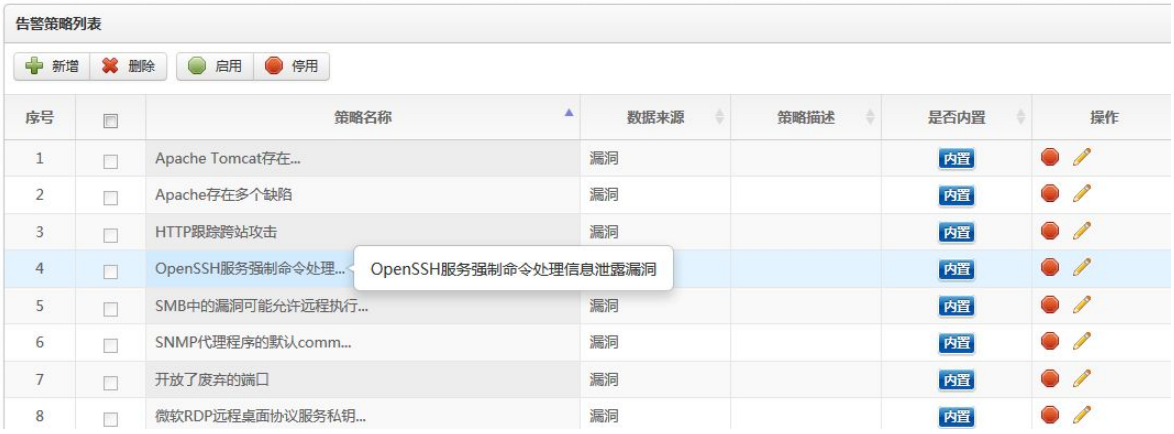
4. 基线类型：可多选；包括日基线和周基线（但必须有足够多的数据支撑）

5. 学习时长：基线的学习时间长度；如果用户选择基线类型为日基线则至少需要学习最近 4 天的统计数据，而基线类型为周基线则至少应学习最近 4 周的统计数据

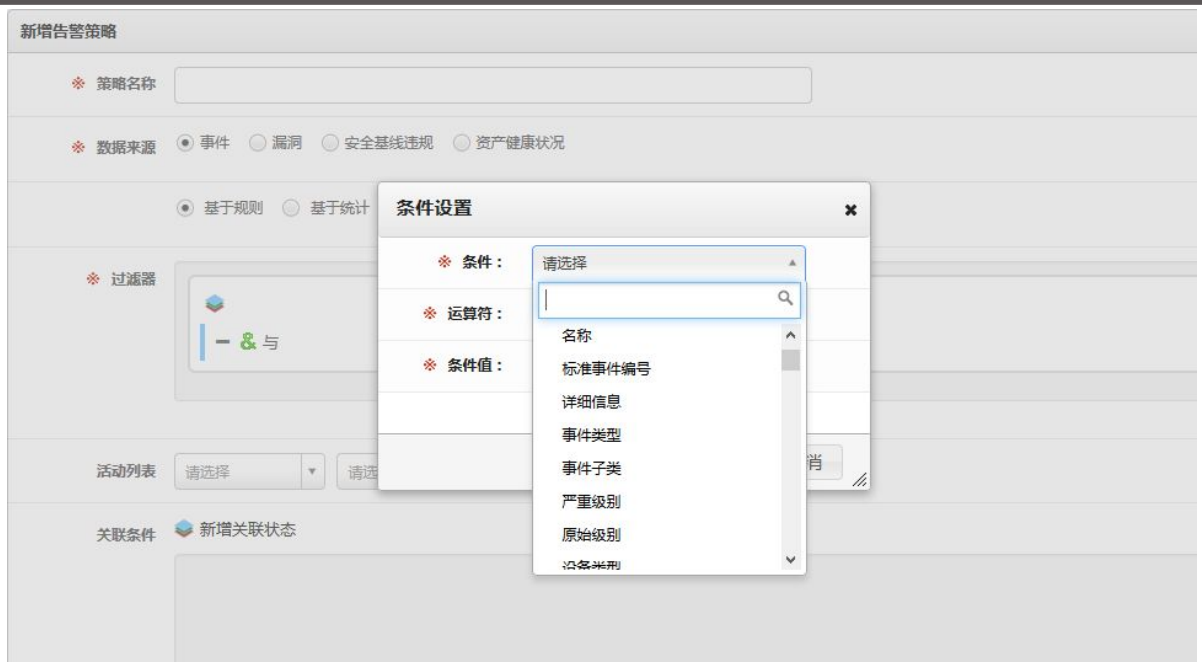
6. 响应触发条件：超出基线的百分比，即：（过去时段的统计数据-同时段的基线统计数据）/同时段的基线统计数据；如达到这个触发条件则执行响应；例如，如基线类型为日基线，则过去 15：00-15:59 的事件/日志量为 1000 条，而基线中的同时段统计数据为 100 条，而触发条件中设定的为 100（即超过 100%），那么应触发响应

4.9.4. 相关操作

1. 列表查看告警策略：以列表的形式呈现告警策略，点击告警策略名称可以显示告警策略的详细策略内容信息。如下图所示：



2. 新建告警策略：新增一条告警策略并将消息发送至后台核心分析。如下图所示：



3. 删除告警策略：在告警策略列表中选择一个或多个策略进行删除；当告警策略中有未处理完的告警引用被删除时，但应该要给出提示，但不影响删除该告警策略；另外系统会通知后台核心分析被删除的告警策略，以避免策略仍被应用。

4. 修改告警策略：选择列表中需要修改的一条告警策略，修改相关属性；提交修改后系统通知后台核心分析重新应用新的告警策略。如下图所示：

5. 停用告警策略：可以停用一条至多条告警策略（原状态为启用）；停用后会通知后台核心分析停止进行策略的关联解析。

6. 启用告警策略：可以启用用一条至多条告警策略（原状态为停用；启用后会通知后台核心分析重新进行关联分析。

4.10. 告警管理

4.10.1. 什么是告警

与普通的安全事件不同，告警是特别需要关注的安全问题，这些问题可能来源于安全事件、安全基线违规、高危漏洞、高危端口开放等方面，也可能是若干不同安全问题的综合体；总之，在安全运营中心中用户需要关注的主要问题就是告警。

4.10.2. 告警的级别

告警被分为如下级别：

级别	级别名称
1	一般
2	警告
3	严重
4	极度严重

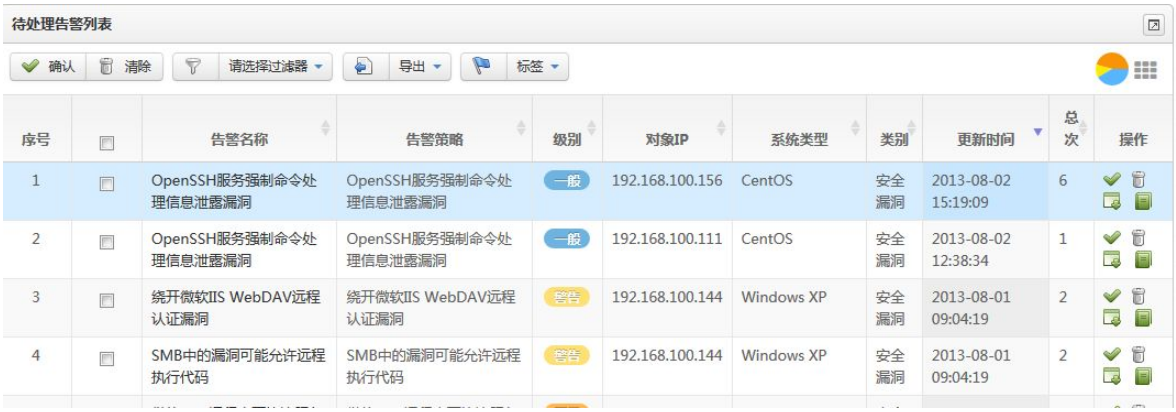
4.10.3. 告警的处理

对于告警的处理主要包括清除（认为不是问题）、确认（认为可能是问题，如果今后确认是问题则也可以转工单，否则清除之）和转工单（需要处理）。

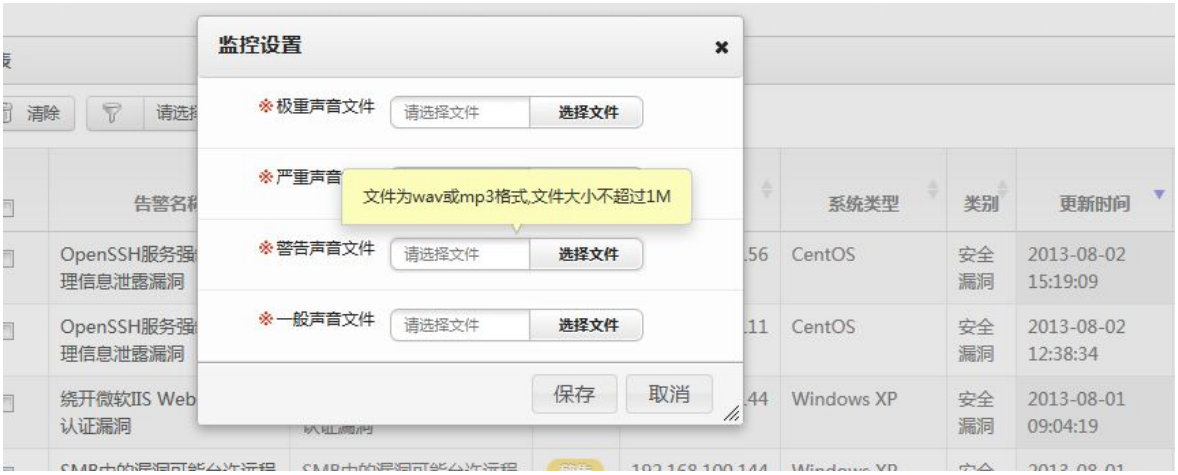
4.10.4. 相关操作

4.10.4.1 告警监控

1. 列表查看告警：以列表的方式展示告警；并能在点击告警名称，进入该告警详细展现页面。如下图所示：

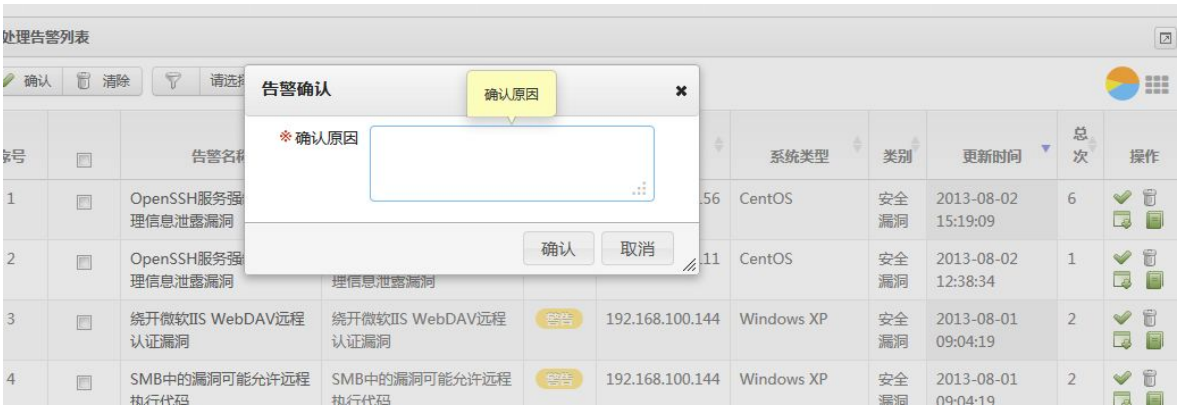


2. 告警声音提示设置：可以设置不同级别告警的提示声音。如下图所示：

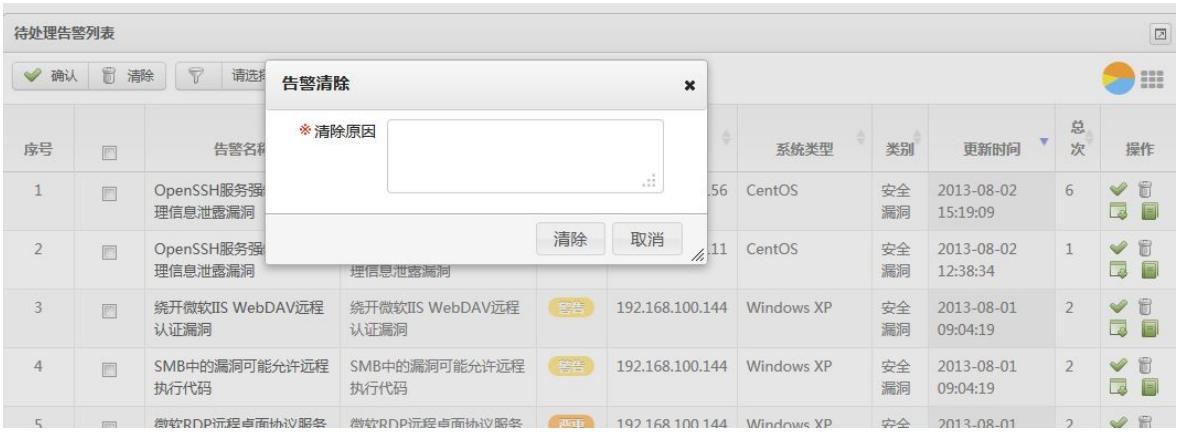


3. 告警监控过滤器设置：该功能是根据不同的过滤器条件来筛选告警，包含操作：新建、查询、删除和修改；过滤器中应包括和告警相关的属性：告警名称、级别、对象类型、对象名称、对象 IP、对象系统类型、告警创建时间及最后修改时间等。如下图所示：

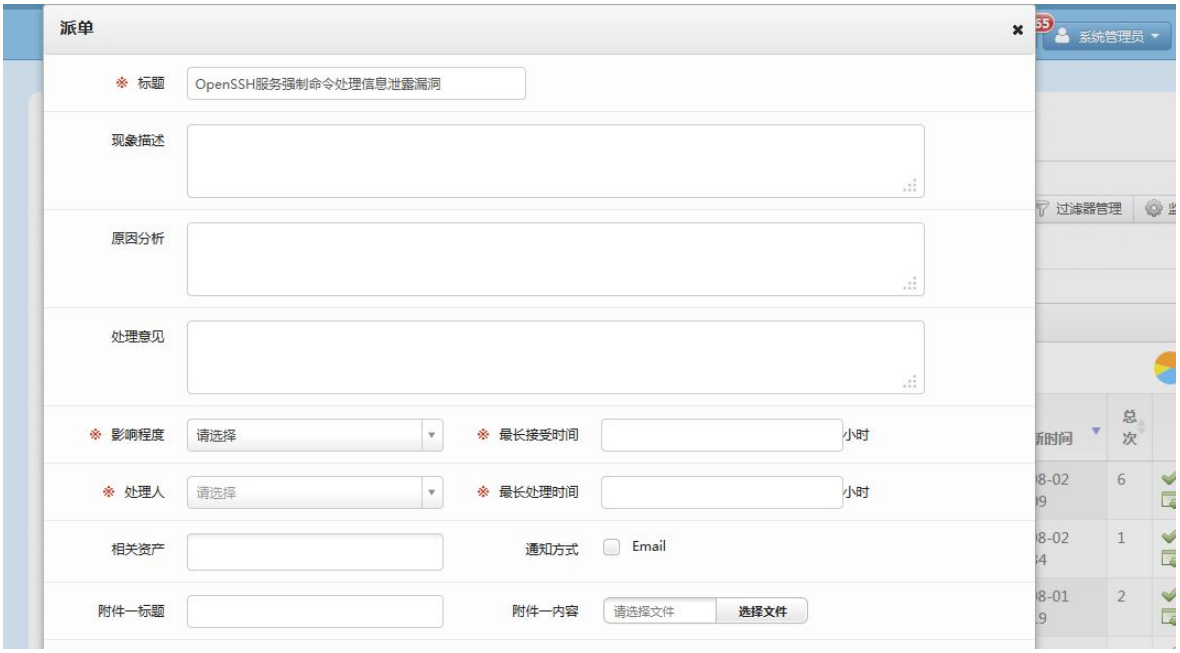
4. 确认告警：选择要确认的告警，填写确认原因并点击确认；确认执行前需给出确认提示；确认操作支持单条、多条、全选和反选；系统应通知后台核心分析被确认的告警。如下图所示：



5. 清除告警：选择要清除的告警，填写清除原因并点击确认；确认执行前需给出提示；清除操作应支持单条、多条、全选和反选；系统应通知后台核心分析被清除的告警。如下图所示：



6. 告警派单：选择要派单的告警，填写相关工单症状（自动填写）并点击确认；派单执行前需给出提示；派单操作仅支持选择单个对象上的多条告警；系统应通知后台核心分析被派单的告警。如下图所示：



4.11. 风险管理

4.11.1. 什么是风险

在安全运营中心中，所谓风险实际上信息资产遭受损失可能的度量。系统将风险分为五级：

级别	级别名称	颜色指示
0	无风险	绿
1	低风险	蓝
2	中风险	黄
3	高风险	橙
4	极度风险	红

4.11.2. 风险的来源

在铱迅安全运营中心内，风险的来源主要就是没有处理的告警，如果用户将这些告警处理掉则系统风险就会归零。

而且，风险的取值范围就是 0~100 之间，风险值越高则表明风险越高，风险值和风险级别之间也有一定的映射关系。

4.11.3. 风险的计算方法

在安全运营中心内，风险的计算主要是依赖于计算各个资产的风险，而且为了避免个别重要资产的有风险，其它绝大多数资产无风险时，这些重要资产的风险被湮没从而不能准确定位风险，系统采用对于不同资产级别分开计算，再利用不同权重将它们进行加权综合计算。

安全运营中心也可以根据不同用户的权限、不同的资产视图分别计算风险，从而达到风险真正的所见即所得，故从这个角度出发，用户在对于资产定级时应慎重为之，而不要随心所欲地赋值。

4.11.4. 相关操作

4.11.4.1 风险概览

这是一个综合展现资产风险情况的列表，显示风险统计视图——包括 30 天风险趋势图和当前资产风险级别分布图（**是按用户资产权限筛选资产，实时计算**）；如下图所示：

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；如下图所示：

导出

序号	资产名称	资产IP	开放端口数	存在漏洞	违规基线	风险级别
1	192.168.100.157	192.168.100.157	1	29	11	高
2	192.168.100.176	192.168.100.176	1	31		高
3	192.168.100.30	192.168.100.30	1	18		高
4	192.168.100.132	192.168.100.132	1	27		高
5	192.168.100.214	192.168.100.214	1	29		高
6	192.168.100.144	192.168.100.144	1	28		高
7	192.168.100.3	192.168.100.3	1	17	13	高
8	192.168.100.155	192.168.100.155	1	24		高
9	192.168.100.88	192.168.100.88	1	26		低
10	192.168.100.166	192.168.100.166	1	19	8	低

显示 10 条记录　显示 1 到 10 共 16 条记录　首页 上一页 1 2 下一页 末页

4.11.4.2 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。具体如下：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。如下图所示：

可查看的安全问题包括：

1. 安全事件

   参考事件管理中的事件查看和查询。默认查看当日的安全事件，不允许跨天查看。

2. 漏洞

   参考漏洞管理中的漏洞查看和查询。

3. 安全基线

   参考安全基线管理中的基线查看和查询。

4.12. 工单管理

4.12.1. 什么是工单

工单在有的系统中又称为任务单，它是分派任务、处理任务的载体；在铱迅安全运营中心中集成了工单管理，同时如果用户有自有的工单管理系统，则可以经过少量地修改，将安全运营中心中的工单派发到外部的工单系统中。

在安全运营中心中，用户既可以在工单管理中直接建立工单，也可以从告警监控中生成工单。

4.12.2. 工单有哪些状态

工单的状态包括待接受、处理中、完成、求助、退回（工单接收者认为可能是和自己无关的任务，退回到工单创建者处）、驳回（工单创建者认为处理结果不合格）、已关闭和作废等。

4.12.3. 相关操作

4.12.3.1 监督工单

用户可以查看当前自己监督的工单列表，超时的工单以红色对是否超时字段进行突出显示。 操作栏可进行分配、驳回、关闭、作废操作；用户还可以查询知识库。

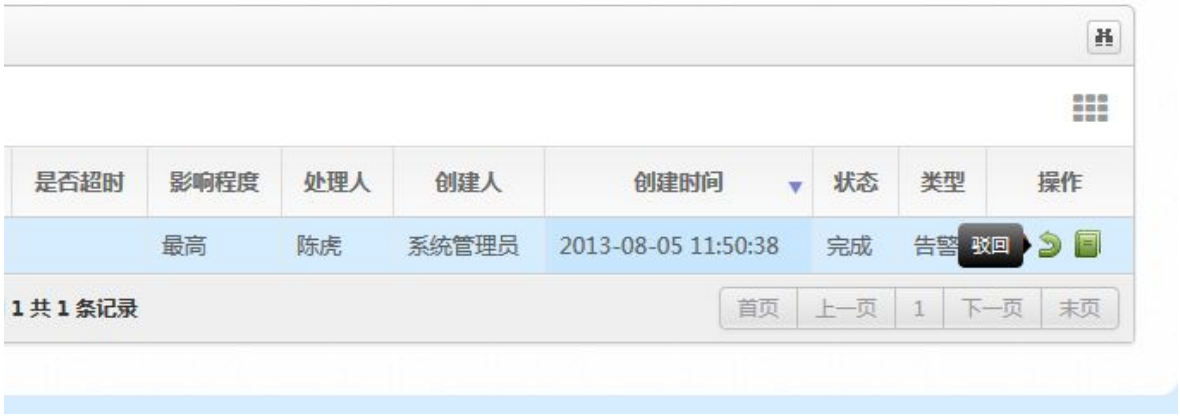
1. 查看工单详情：用户点击列表中工单标题链接，进行工单详情查看，详情页面显示工单标题、工单类型、创建时间、创建人、影响程度、最长接受时间、最长处理时间、相关资产、状态、分配时间、接受时间、完成时间、退回原因、驳回原因、作废原因、现象描述、原因分析、处理意见、处理结果；如下图所示：

2. 工单查询：在监督工单列表中输入相关字段的查询条件，进行监督工单查询,状态字段只针对监督工单列表可以进行查询。如下图所示：

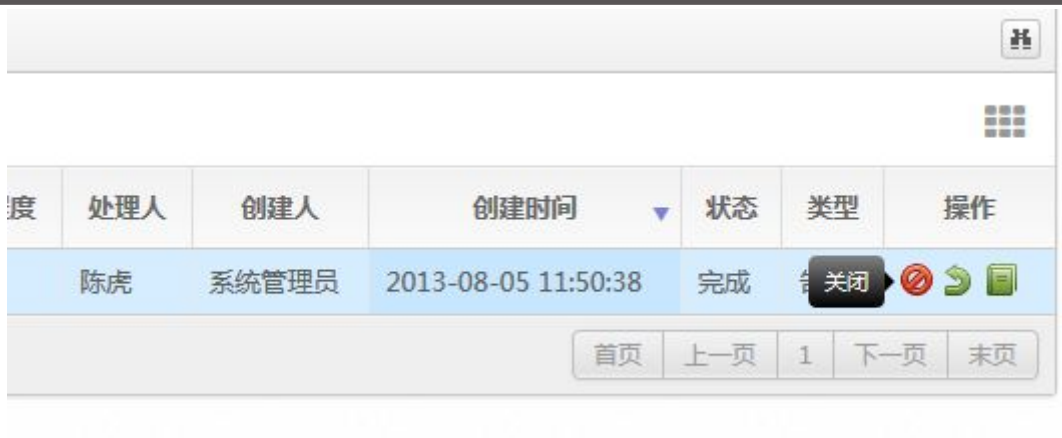
3. 新增工单：手工创建工单，填写工单相关属性。如下图所示：

4. 分配工单：对于退回的工单，用户点击工单列表操作栏中的分配链接；选择处理人，填写相关备注信息并提交。

5. 驳回工单：对于已经结束但未关闭的工单，用户点击工单列表操作栏中的驳回链接，填写驳回原因并提交。如下图所示：



6. 关闭工单：对于已经结束但未关闭的工单，用户点击工单列表操作栏中的关闭链接并提交确认。如下图所示：

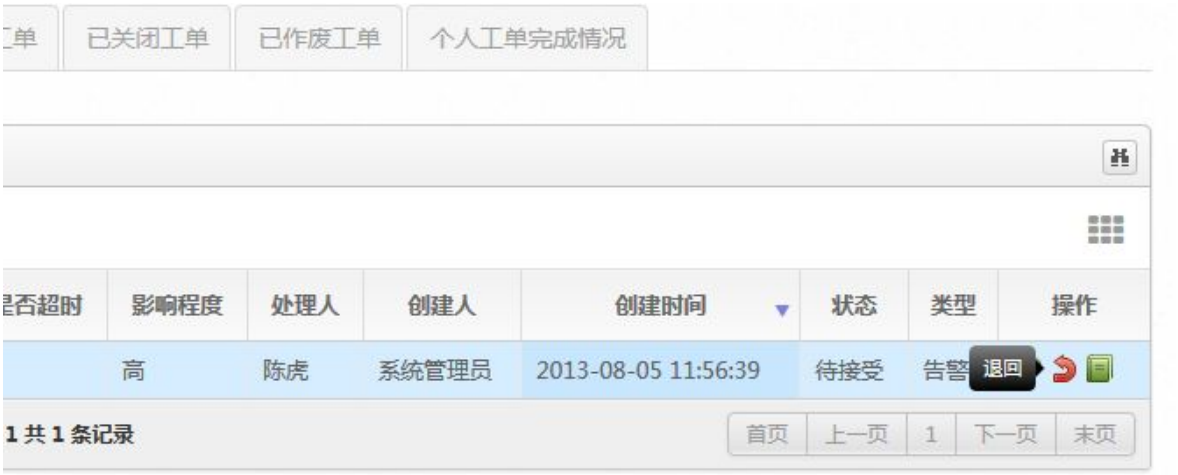


7. 作废工单：对于新增未分配或退回的工单，用户点击工单列表操作栏中的作废链接并提交。

4.12.3.2 待接受工单

1. 接受工单：用户选择要接受的工单（可多选）。如下图所示：

2. 退回工单：如果用户认为工单并不属于自己处理则可以退回给工单创建者（监督人）。如下图所示：

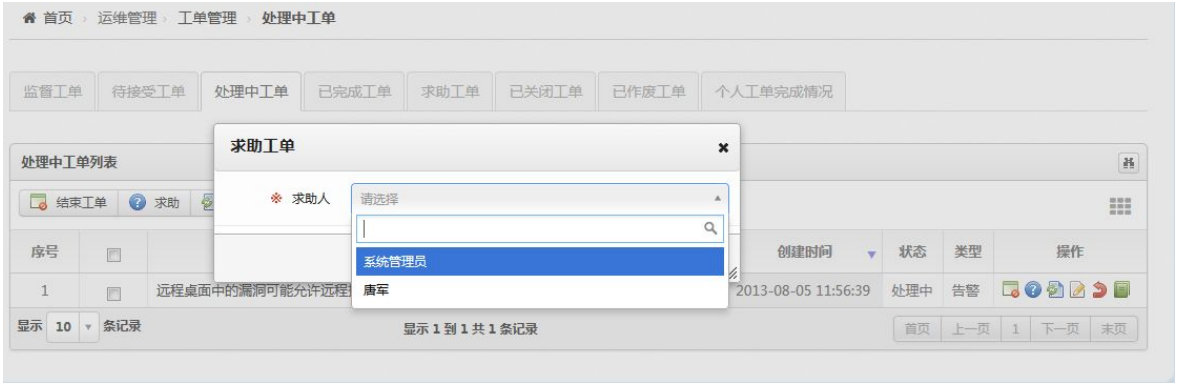


4.12.3.3 处理中工单

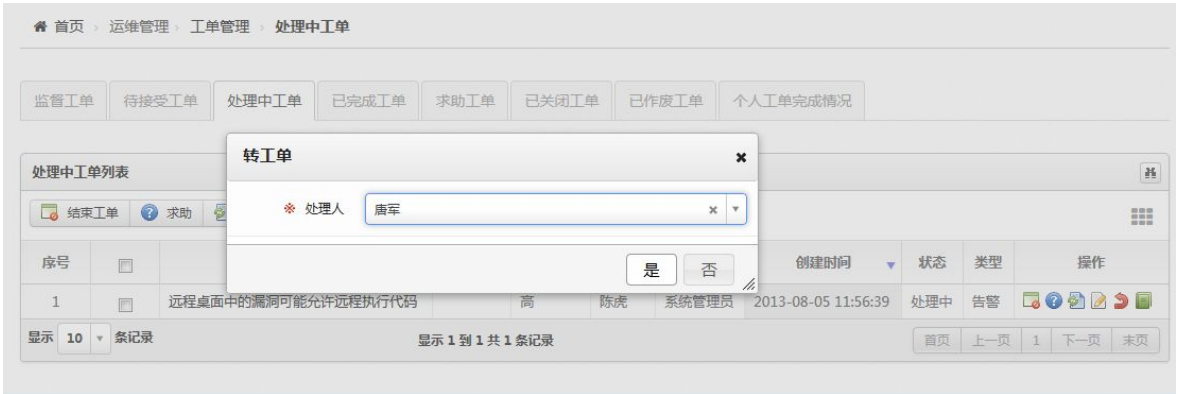
1. 填写工单处理结果：对于用户认为已经处理有阶段性成果的工单，可填写工单的原因分析、处理结果、处理意见等信息；用户可以直接提交，也可以针对工单的信息在知识库中进行查询。如下图所示：

2. 结束工单：对于用户认为已经处理完毕的工单，可以选择结束。

3. 求助：如无法独立处理的工单，用户可以将工单发送给求助人。如下图所示：



4. 转工单：如果用户认为不是自己应该处理的工单，则可将其转移给其他处理人。如下图所示：



4.12.3.4 完成工单

完成工单中主要是帮助用户查看和查询已经处理完毕的工单（用户完成的工单），并无其它特殊的要求。如下图所示：

4.12.3.5 求助工单

求助工单中主要可以查看、查询其它用户发送的求助工单的信息，用户可以对其进行批注，以帮助求助者完成工单的处理流程。如下图所示：

4.12.3.6 关闭工单

用户可以查看和查询已经被关闭的工单信息。如下图所示：

4.12.3.7 作废工单

用户可以查看和查询已经被作废的工单信息。

4.13. 预警管理

4.13.1. 什么是预警

所谓预警是对系统内可能发生的安全问题作出警示，如攻击扩散、病毒的扩散、高危补丁未修补等。

4.13.2. 预警有哪些类型

在安全运营中心系统中，预警可由系统自动生成，或者人工创建。类型包括：网络攻击、恶意代码、安全漏洞等。

4.13.3. 预警有哪些状态

预警包括如下状态：

1. 待发布：系统自动创建或人工创建但未发布
2. 发布：正式发布且在有效期内
3. 作废：无用的待发布预警
4. 归档：过期的已发布预警

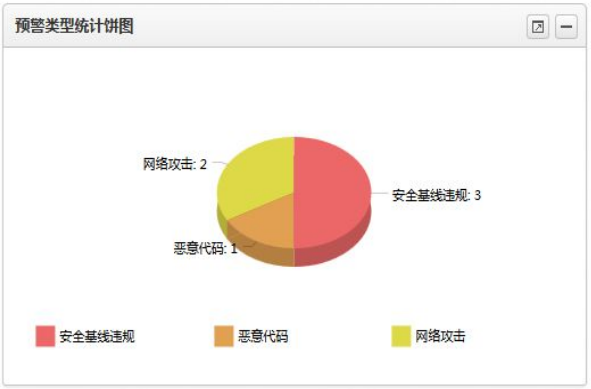
4.13.4. 相关操作

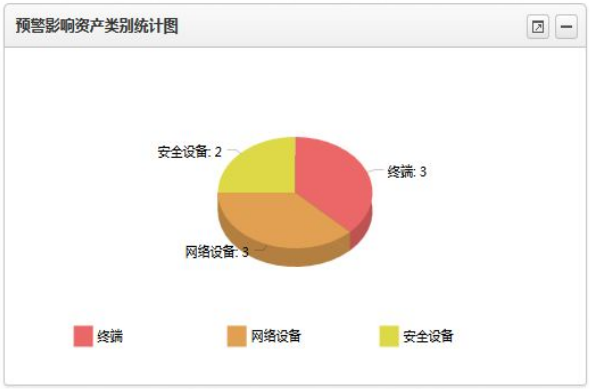
4.13.4.1 发布预警查看

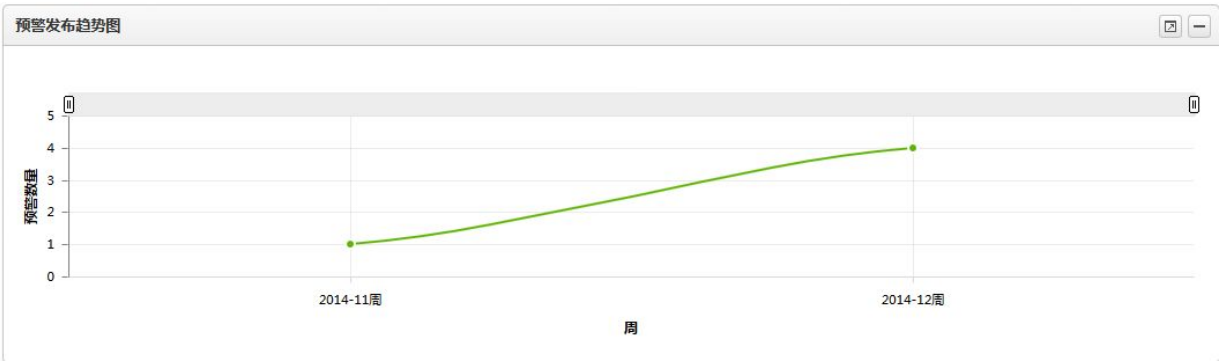
用户登录系统后，如存在已发布的预警，则可以在屏幕下方看到，如下图所示：

4.13.4.2 预警概览

进入预警管理模块，可以看到预警相关统计，包括类型、影响资产、发布趋势等，如下：

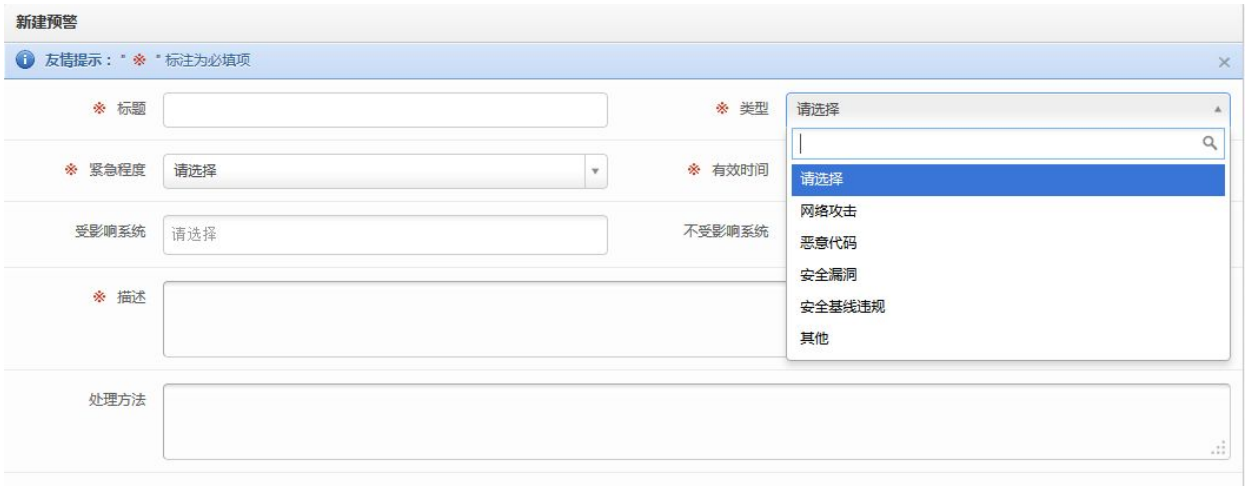






4.13.4.3 待发布预警

用户可在待发布预警中查看、新增预警，如下图：

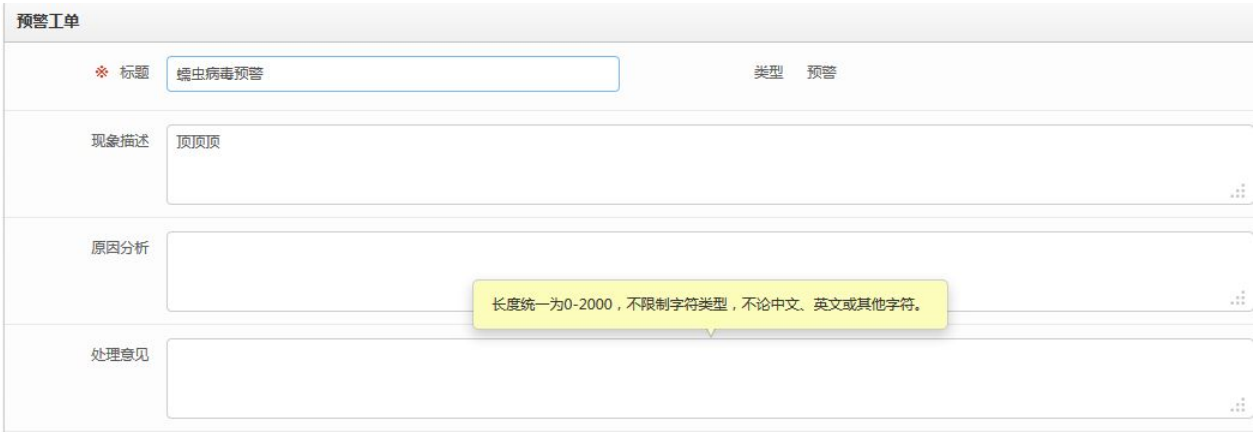


也可以在此对相关待发布预警进行发布，如下图所示：

发布时可以关联相关需要预警的资产。

4.13.4.4 已发布预警

在此模块可以查看已经发布的预警，对于预警的创建人，也可以直接将预警进行派送工单处理，如下图：



4.13.4.5 预警工单

在此模块可以查看已经发布的并且转工单的预警情况，如下图：

序号	标题	相关资产	处理人	处理时限	状态
1	不受影响AIX5111		shasuqin	1	处理中
2	不受影响AIX51		shasuqin	1	完成
3	不受影响AIX5		shasuqin	1	完成

4.13.4.6 已作废预警

在此模块可以查看已经作废的预警信息，如下图所示：

6	作废4	其他	低	2014-03-17 14:56:31	2014-03-17 14:56:51	系统管理员
7	作废1	恶意代码	低	2014-03-17 14:48:33	2014-03-17 14:50:32	系统管理员
8	作废2	恶意代码	很低	2014-03-17 14:48:47	2014-03-17 14:50:32	系统管理员
9	作废3	其他	一般	2014-03-17 14:50:08	2014-03-17 14:50:32	系统管理员
10	受影响系统测试2	网络攻击	很低	2014-03-17 13:53:04	2014-03-17 13:54:14	系统管理员

4.13.4.7 已归档预警

在此模块可以查看已经归档的预警信息（超过发布时限的预警），如下图所示：

序号	标题	类型	紧急程度	相关资产	发布人	发布时间
1	不受影响AIX5	安全漏洞	低	192.168.100.216...	系统管理员	2014-03-18 11:30:38
2	test5	其他	很高	192.168.100.216	系统管理员	2014-03-18 11:25:50
3	新建预警新建预警新建预警新建预...	其他	高	192.168.100.216...	系统管理员	2014-03-18 11:25:41
4	直接发布看工单类型	网络攻击	很低	192.168.100.163	系统管理员	2014-03-18 11:20:36
5	派单后发布验证	恶意代码	低	192.168.100.216...	系统管理员	2014-03-18 10:47:25

4.14. 知识库管理

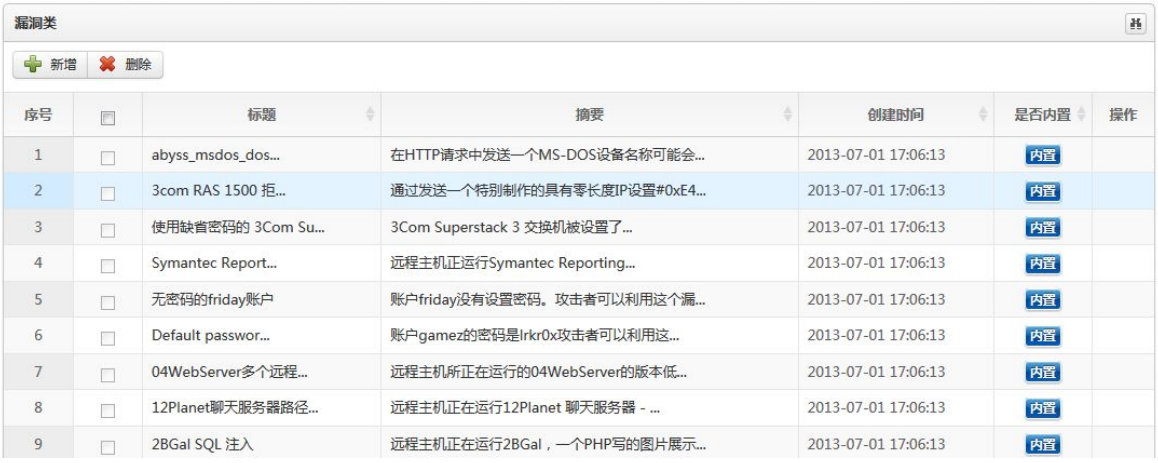
4.14.1. 知识库有哪些分类

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，包括如下几类：

1. 日志配置类（各种操作系统、网络设备、应用系统及数据库等接入安全运营中心日志的配置收集方法）
2. 日志类（各种操作系统、网络设备、服务器及数据库的日志信息）、安全事件类（反映系统运行/状态、安全问题、用户行为等的计算机记录或日志）
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、应用系统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）

4.14.2. 相关操作

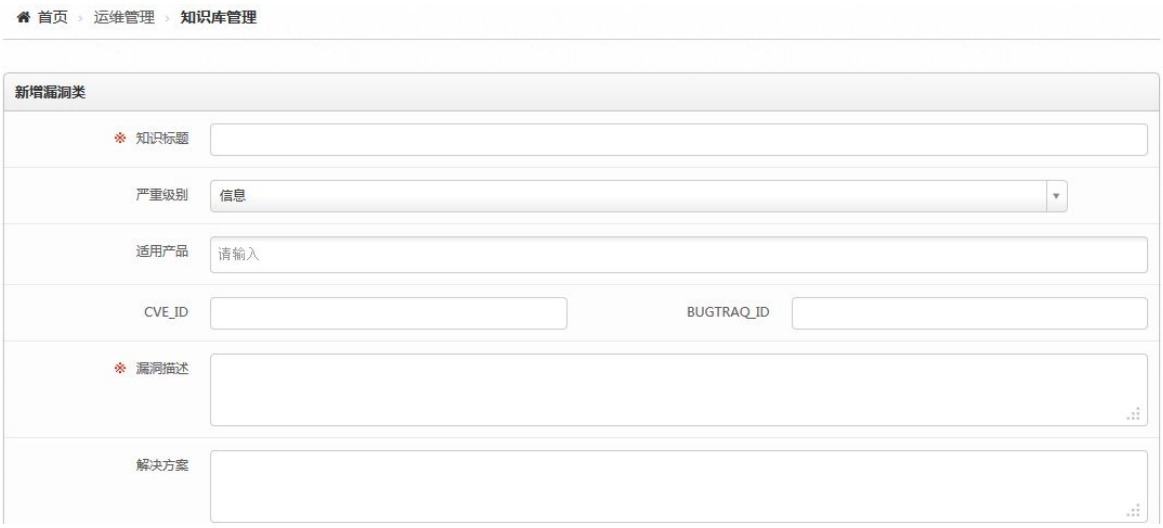
1. 查看知识库列表：用户可以通过显示的类别查看各分类的知识库信息，可过滤显示自己要看的类别的知识库信息。如下图所示：



2. 查看知识库详情：查看支持库的详细内容。如下图所示：

3. 知识库列表：知识库列表显示知识库信息，显示：标题、摘要、日期、操作等。注意：系统内置的知识库不可以修改和删除。

4. 知识库维护：用户可以增加、修改（不能修改系统内置知识）、删除知识库（不能删除系统内置知识）。如下图所示：



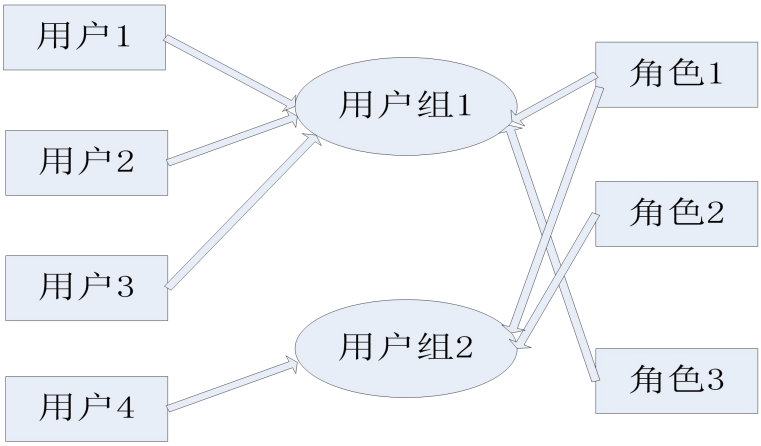
4.15. 系统管理

安全运营中心的系统管理包括了各类系统自身管理的模块，包括组件状态、用户管理、日志管理、升级管理、口令策略（管理）、内置对象（管理）、许可证（管理）等。

4.15.1. 相关操作

4.15.1.1 用户管理

用户管理中包含用户管理、用户组管理、角色管理。一个用户只能属于一个用户组，一个用户组可以拥有多个角色。用户组与角色之间是多对多的关系。另，系统内置三种角色：安全管理员、安全审计员、系统管理员。安全管理员对除了日志管理、系统管理以外的所有菜单进行了功能授权，且可以对所有安全对象有访问权限。安全审计员只对日志管理菜单予以授权，且对安全对象无访问权限。系统管理员仅对系统管理菜单予以授权，且对安全对象无访问权限。下图是一个权限的示意图：



4.15.1.2 角色管理

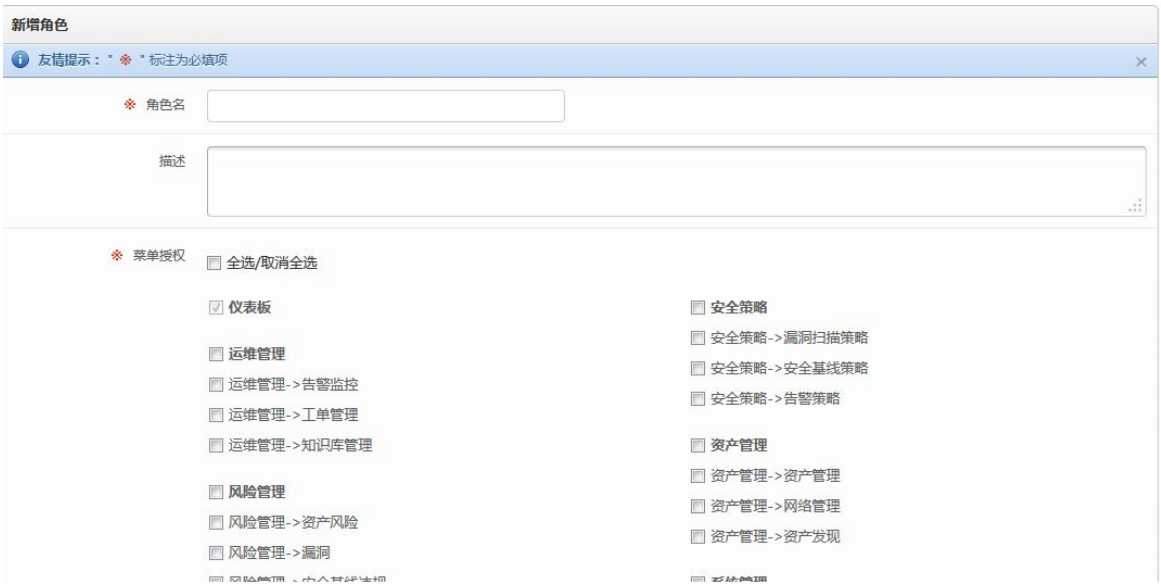
1. 列表查看：系统内置三个角色：安全管理员、安全审计员、系统管理员。

安全管理员对除了日志管理、系统管理以外的所有菜单进行了功能授权，且可以对所有安全对象有访问权限。

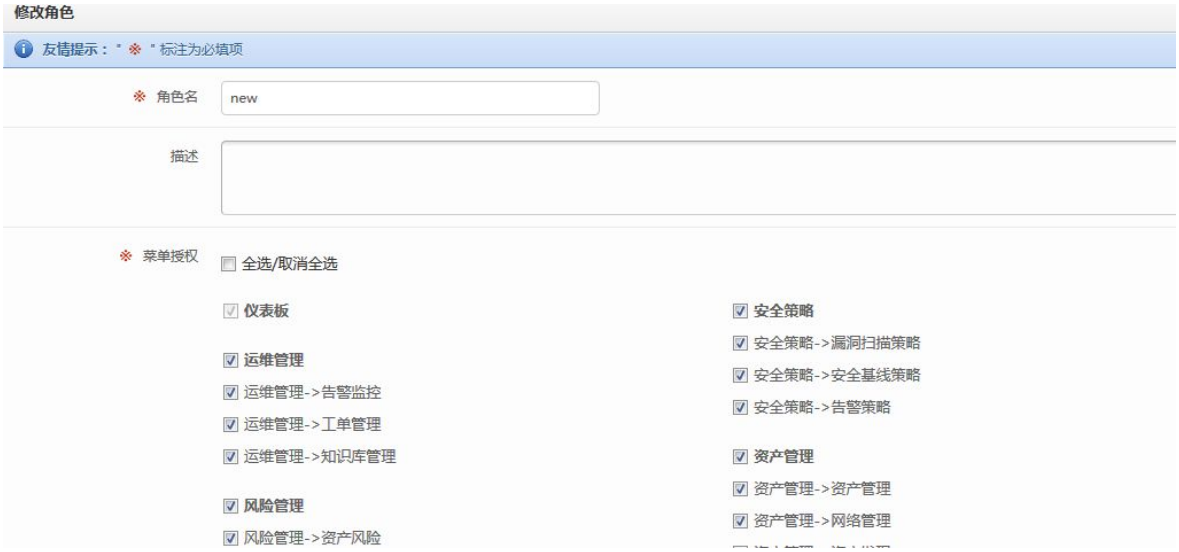
安全审计员只对日志管理菜单予以授权，且对安全对象无访问权限。

系统管理员仅对系统管理、组件管理菜单予以授权，且对安全对象无访问权限。如下图所示：

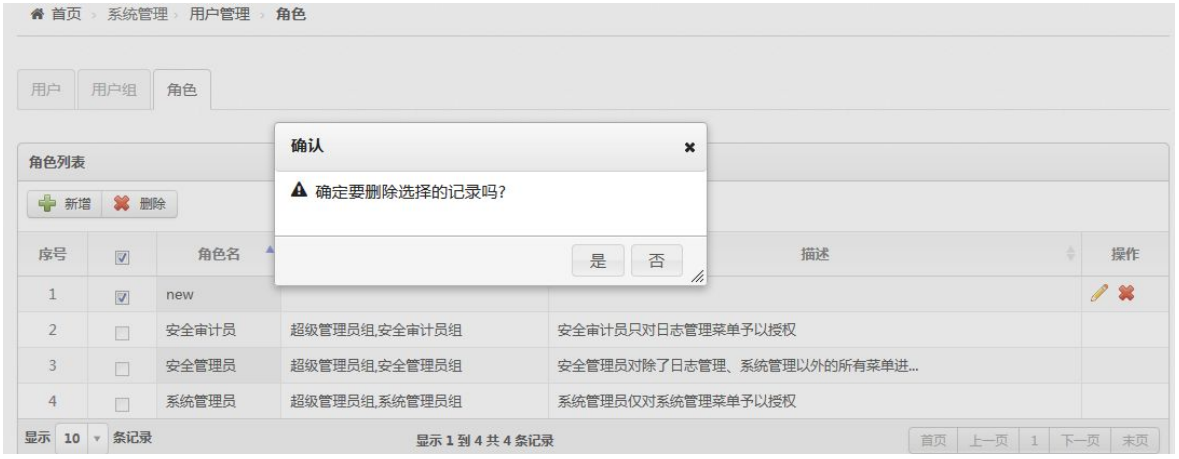
2. 新建角色：在新建角色页面中，输入角色名称，在菜单授权与安全资产授权中勾选授权的项目，填写描述（可选）。菜单授权：以树状结构列出各个菜单及其下一级菜单。如下图所示：



3. 修改角色：用户可以修改角色的相关属性及授权定义。如下图所示：



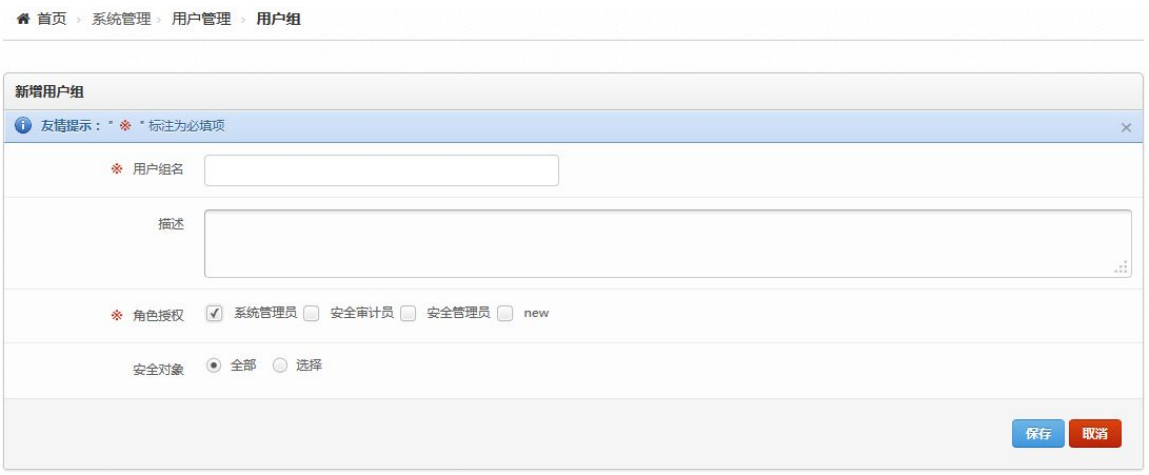
4. 删除角色：用户可以选择删除一个或多个角色（系统正在使用的角色及系统内置的角色也可以被删除）。如下图所示：



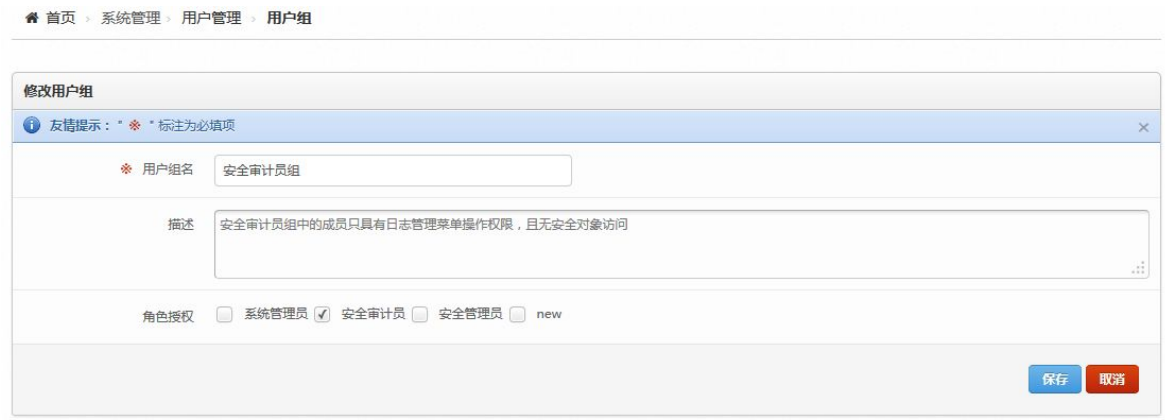
4.15.1.3 用户组管理

1. 用户组列表查看：系统内置四个用户组：超级管理员组（包含角色：安全管理员、安全审计员、系统管理员）、安全管理员组、安全审计员组（包含角色：安全审计员）、系统管理员组（包含角色：系统管理员）。如下图所示：

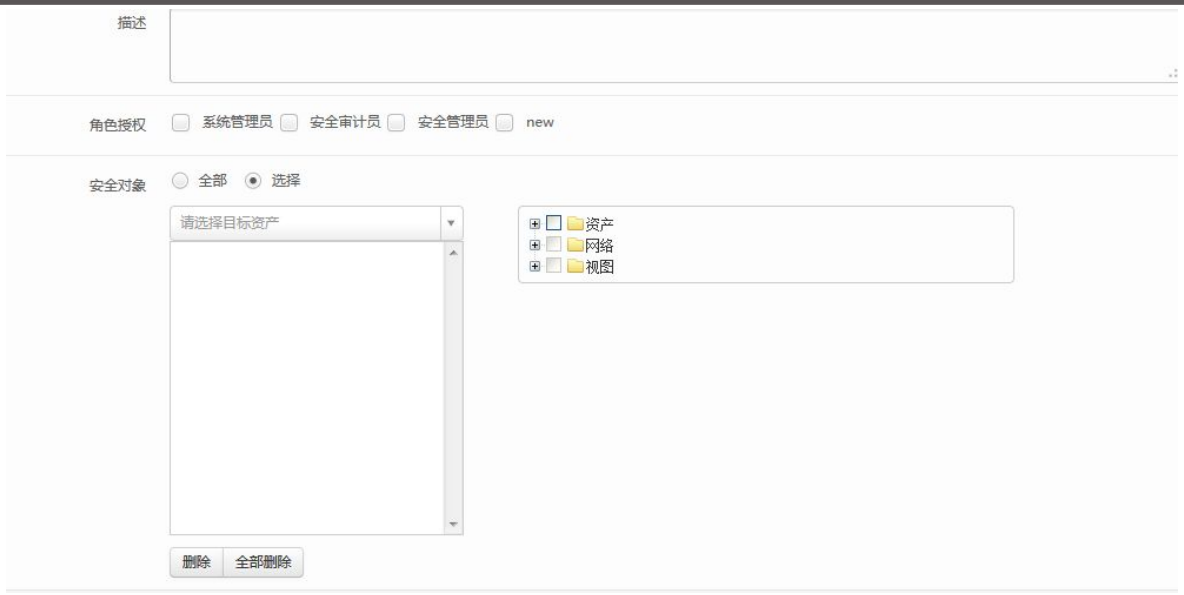
2. 新建用户组：输入用户组名称、描述（可填）、选择本系统角色授权（至少选一个，可以多选）；点击提交。如下图所示：



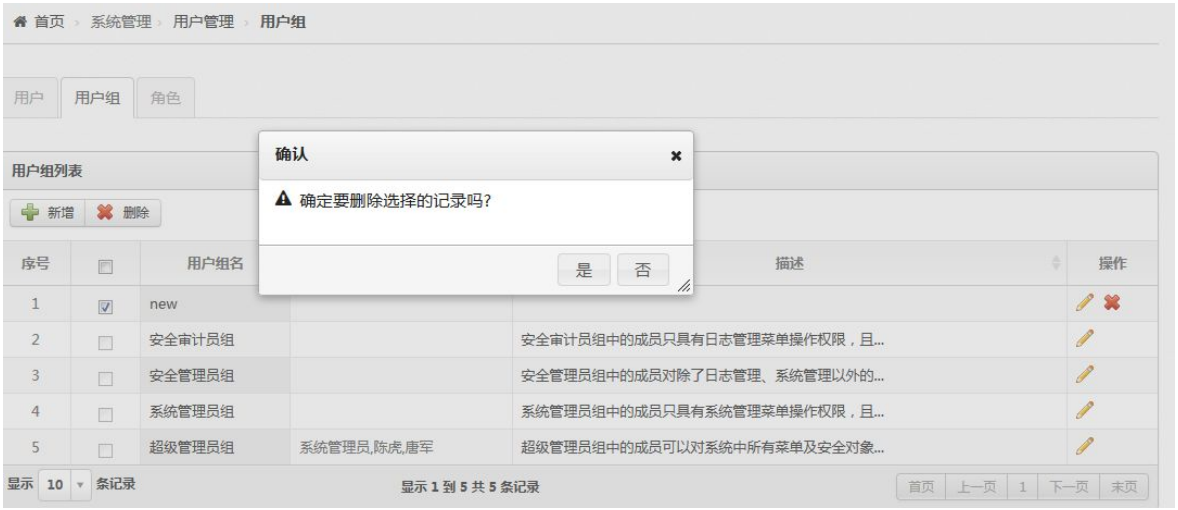
3. 修改用户组：修改用户组相关属性。如下图所示：



4. 安全对象授权：选择资产（根据视图选资产），可以具体到某一个具体的资产。如下图所示：



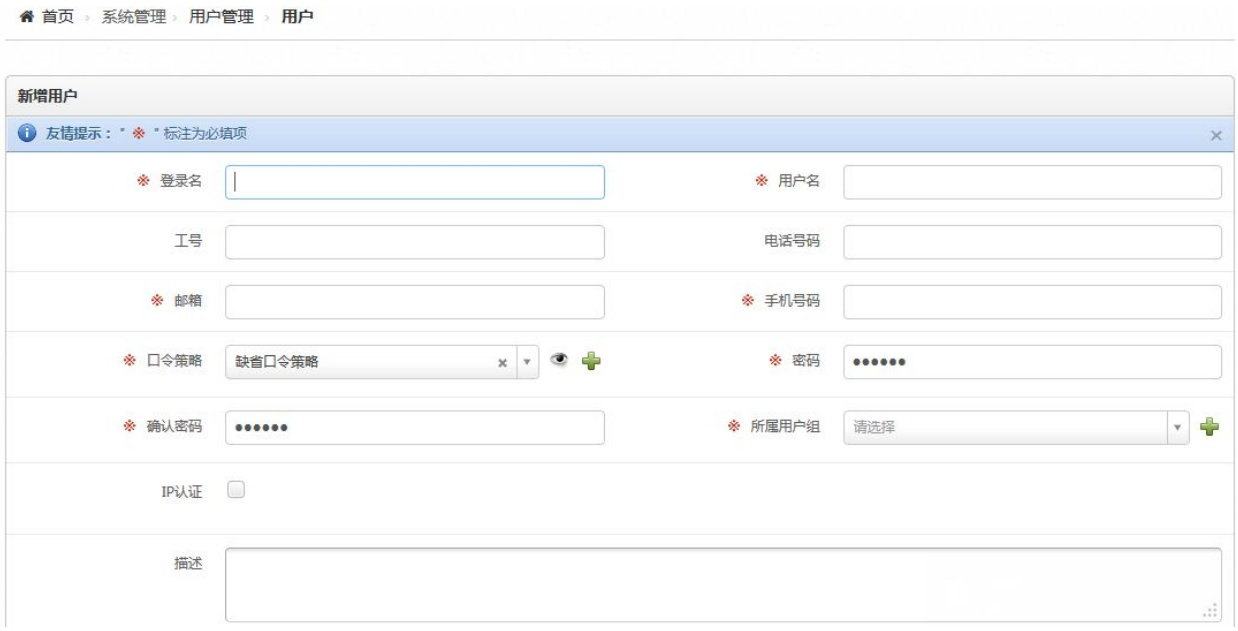
5. 删除用户组：删除用户选定的一个或多个用户组；如用户组中包含了用户则应提示用户先删除。如下图所示：



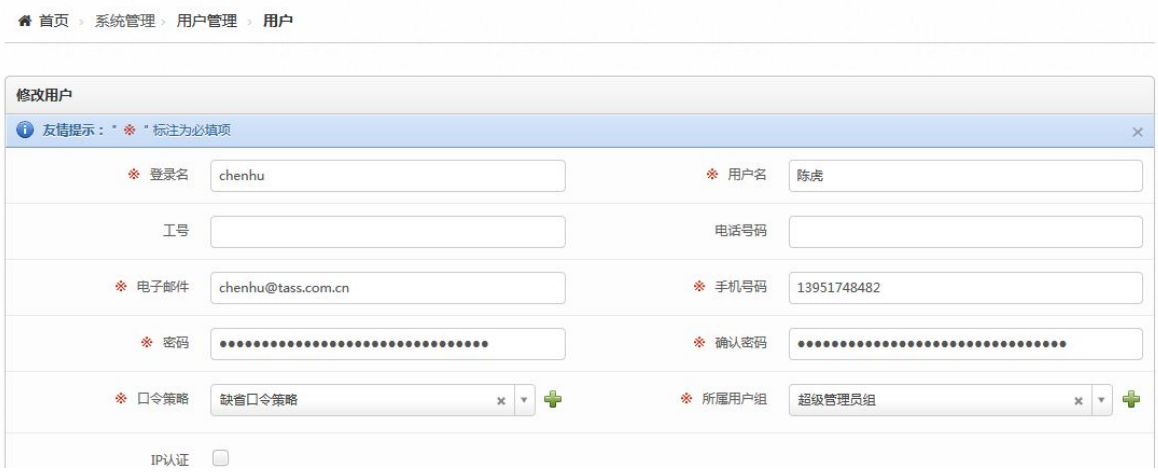
4.15.1.4 用户管理

1. 用户列表：点击用户管理系统默认显示用户列表页面，用户列表下显示系统内置用户（该用户属于超级管理员组）。用户列表上方显示新建、删除、修改、用户解锁、查询操作按钮。另外，也显示了按照用户组查看的收缩功能按钮。如下图所示：

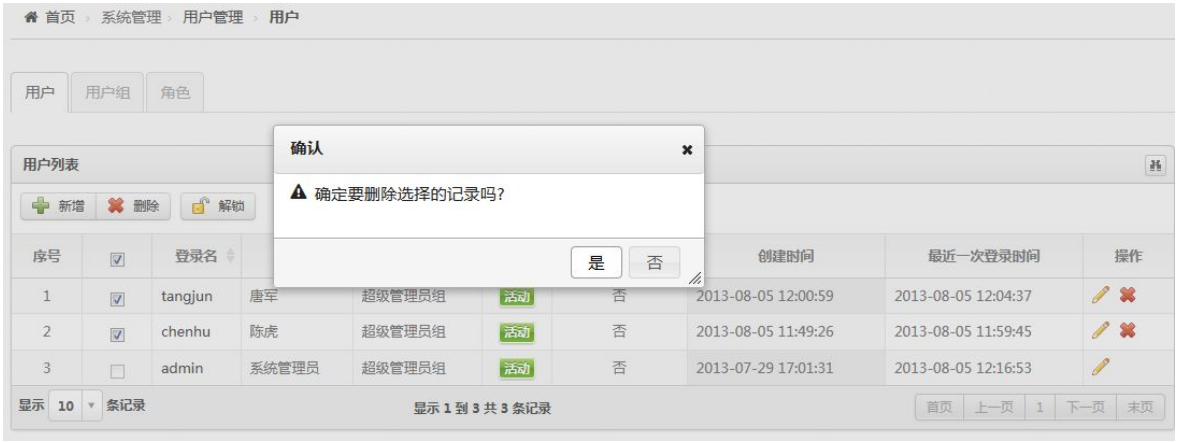
2. 新增用户：在新增用户页面，输入登录名、用户名、工号、电子邮箱、电话号码（可填可不填）、手机号码、IP 范围（可填可不填）、密码、确认密码（**如果系统设置为用户密码通过邮件发送则不显示上述两个输入**）、描述（可填可不填），选择口令策略、所属用户组（只能选一个）；用户只能属于一个用户组。用户密码的设置方式可以在系统管理中进行设置，设置方式有两种。一种是在新建用户页面设置，另一种是系统自动生成密码发送给用户（发送至用户新建时设置的邮箱地址）。如下图所示：



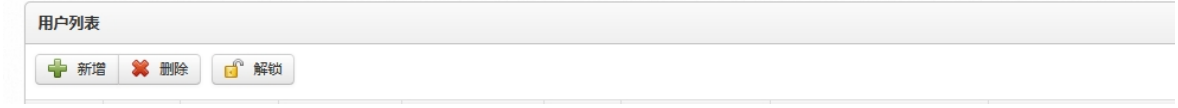
3. 修改用户：在修改用户页面，修改用户的相关属性。登录名、用户名、工号、电子邮箱、电话号码、手机号码、IP 范围、密码、确认密码、描述、口令策略、所属用户组。如下图所示：



4. 删除用户：删除用户选定的一个或多个用户。系统内置的用户可以删除（admin）。但当删除系统内置的用户时，系统中一定要存在已经创建的其他超级管理员，即保证系统至少存在一个超级管理员。如下图所示：



5. 用户解锁：在用户列表中，勾选需要解锁（锁定的原因是用户多次输错密码）的一条或多条用户信息点击“解锁”（支持多条用户解锁）；要解锁用户的用户状态必须是锁定。如下图所示：



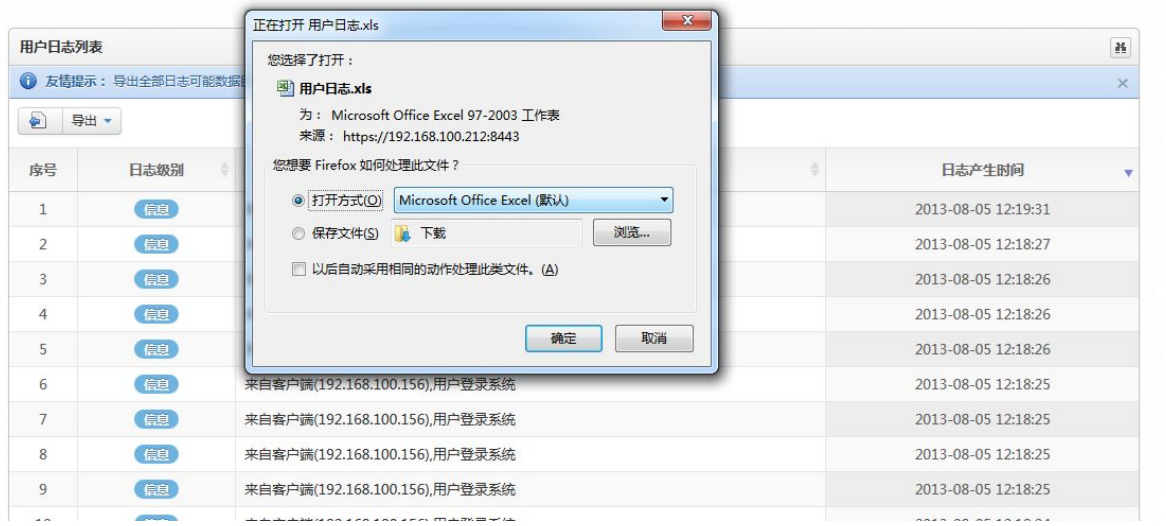
4.15.1.5 日志管理

安全运营中心中的日志管理是提供给用户查看、导出系统自身运行和操作日志的模块。

用户日志管理

1. 用户日志查看和查询：查看和查询用户指定的日志，查询的条件包括时间段、IP 地址、严重级别等。如下图所示：

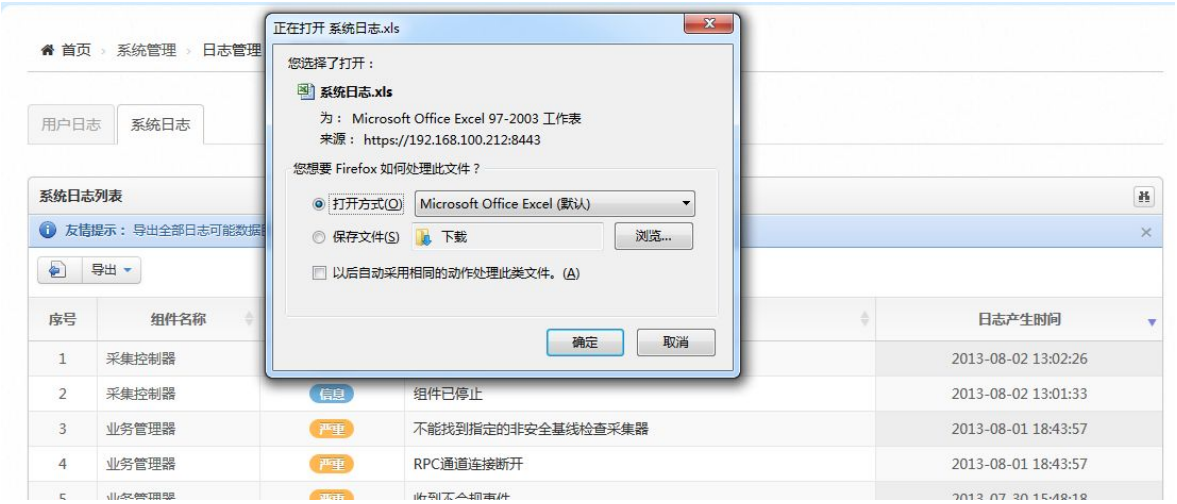
2. 用户日志导出：用户可以将查询出的日志导出成 xls 文件，内容包括时间、用户名、IP 地址、操作模块、详细信息、严重级别等。如下图所示：



系统日志管理

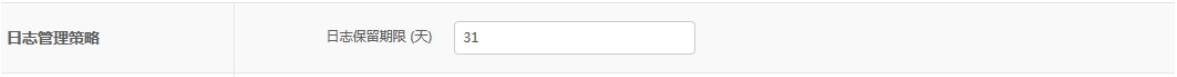
1. 系统日志查看和查询：查看和查询用户指定的系统日志，查询的条件包括时间段、IP 地址、严重级别等。如下图所示：

2. 用户日志导出：用户可以将查询出的日志导出成 xls 文件，内容包括时间、组件名、组件 IP 地址、详细信息、严重级别等。如下图所示：



日志清理参数设置

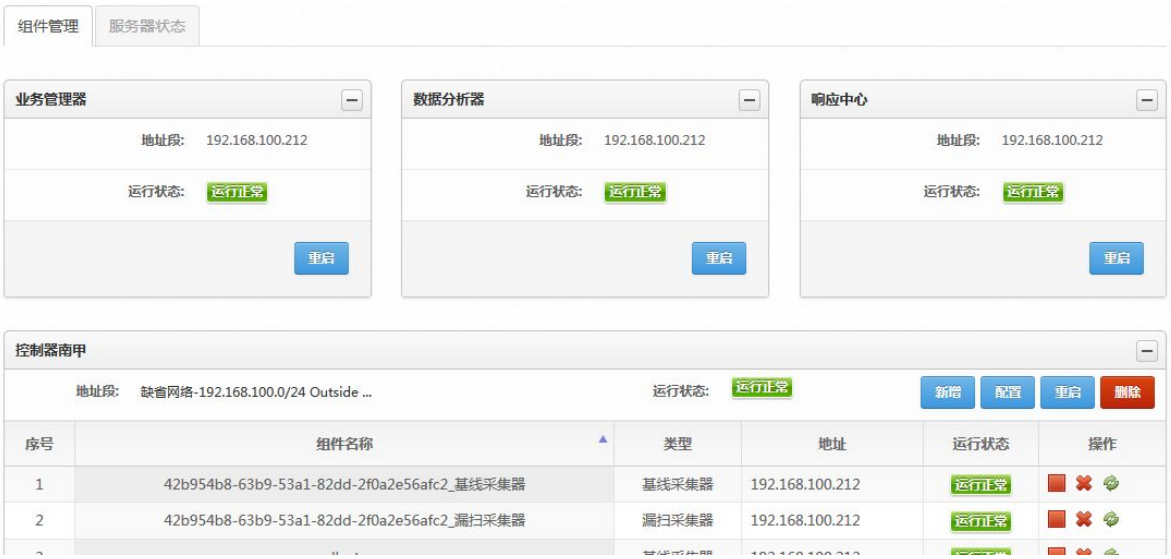
设置用户日志和系统日志保留天数（在系统参数管理中），默认为 30 天，即系统仅保留最近 30 天的日志，而会将 30 天之前的日志清除。如下图所示：



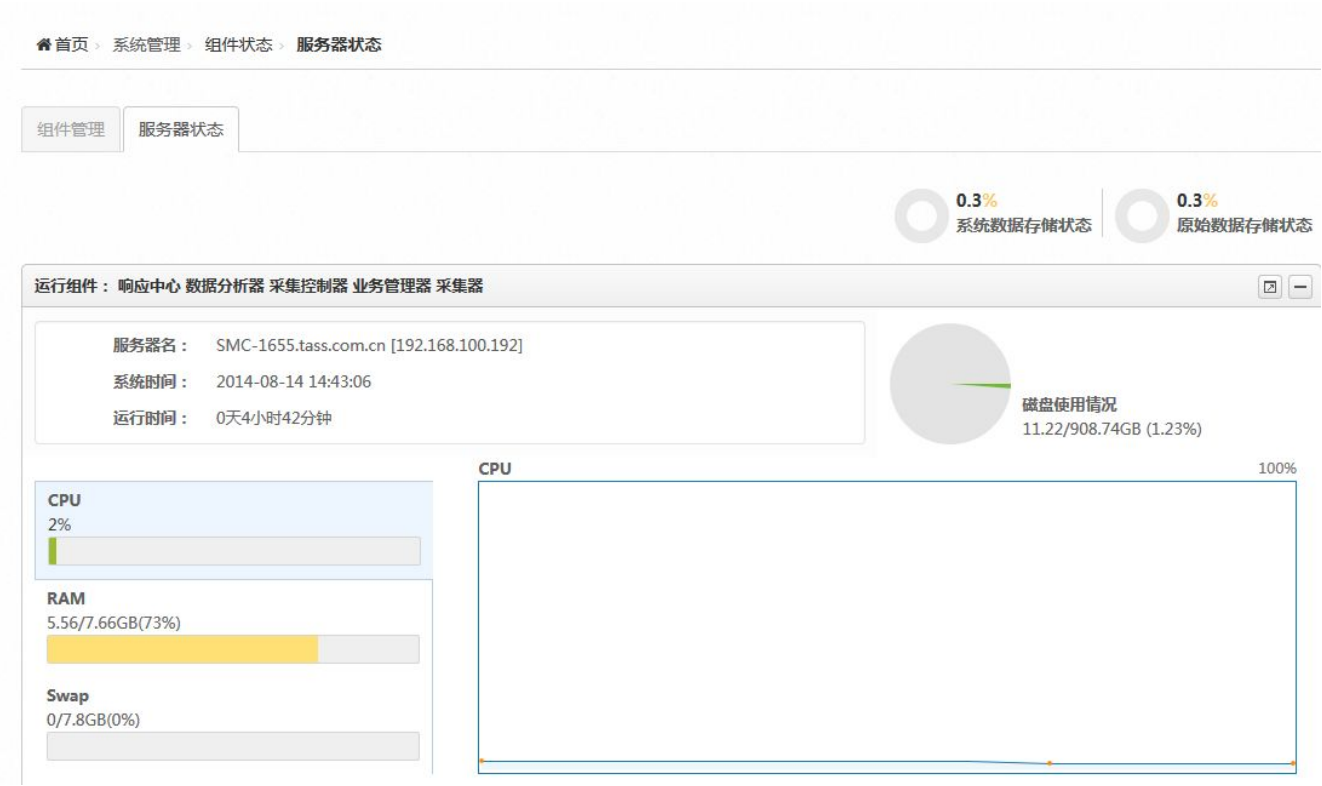
4.15.1.6 组件管理

组件管理中会列出安全运营中心的所有组件状态，包括核心分析（业务管理器、数据分析器、响应中心）、采集管理器及采集器、数据服务的状态、所在服务器的状态等，具体如下：

1. 列表查看：列表查看系统内所有组件的状态和资源使用状态；采集控制器下包含多个采集器，用户可以增加采集器并配置采集器相关参数（特别是事件类采集器，这在安全事件管理中业已阐述，这里不再重复），如下图所示：



2. 服务器状态：列表显示各个已经安装了安全运营中心组件的服务器状态，如 CPU、内存、交换空间、磁盘空间等，如下图所示：



3. 数据储存状态：数据存储包含了数据库和文件存储（存放原始事件）；数据库储存状况主要显示数据空间使用状况，包括：使用的空间，剩余的空间；文件存储显示当前文件分区使用的百分比状态。当上述存储超过 80%时应明确提示用户并发送邮件采取相关措施以防数据丢失。

4.15.1.7 系统参数管理

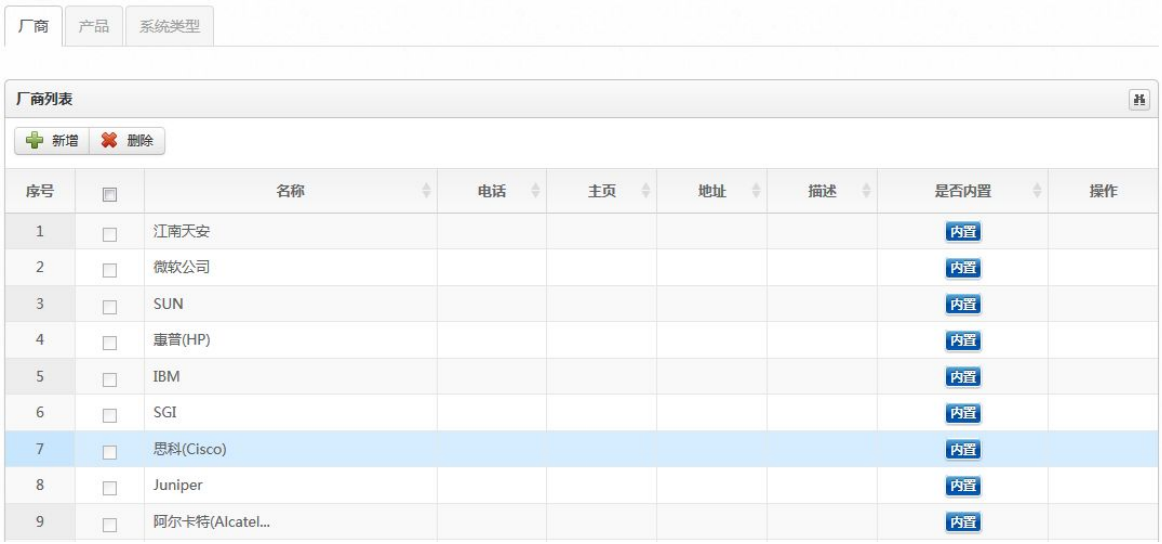
系统参数管理中包含了安全运营中心在运行中需要设置的一些参数。

系统参数中可以设定邮件服务器参数（IP 地址、端口等）、SNMP Trap 参数、Syslog 服务器（服务器地址、端口，支持 4 个）、NTP 服务器（地址、端口等）、登录密码允许错误次数（如 3 ~ 5 次）、锁定时间（如 5、15、30 分钟，即重鉴别功能）、是否允许同名用户在线（**即如一个用户已在线，那么同名的用户则不允许登录，直到前面的用户注销**）、用户密码获取方式（邮件还是界面设置）等，如下图所示：

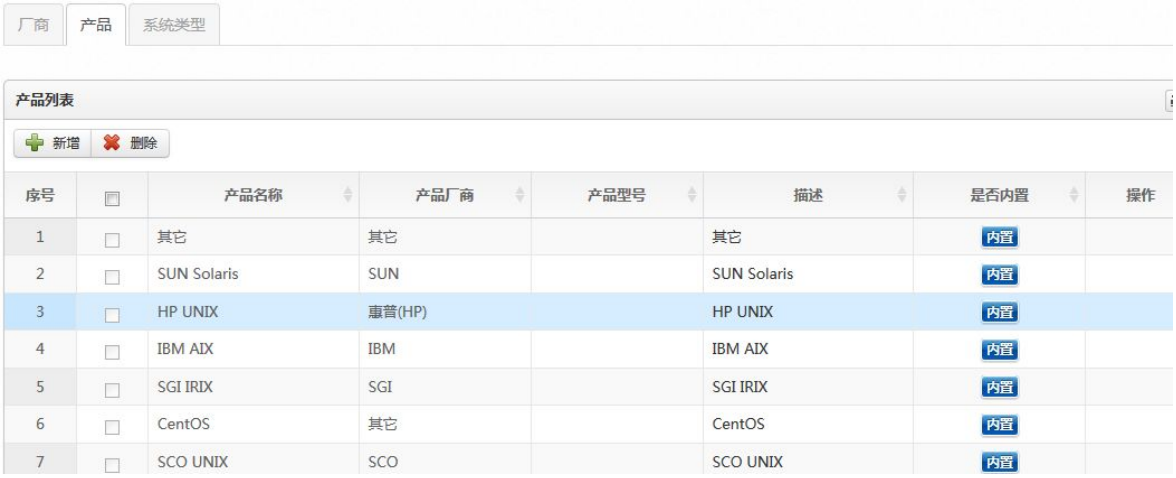
4.15.1.8 内置对象管理

内置对象管理包括：

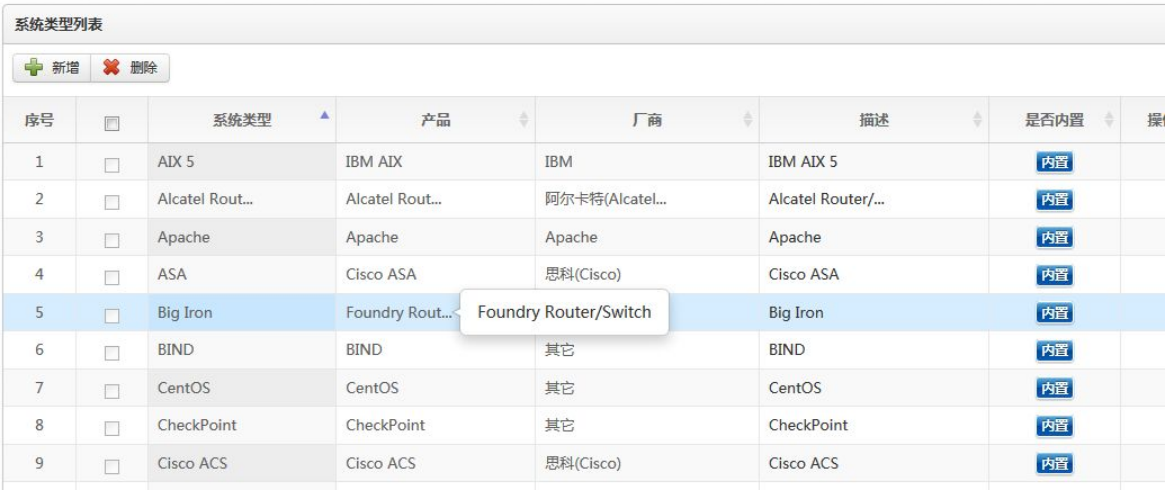
1. 厂商管理：维护厂商信息，如 Oracle、微软等，如下图所示：



2. 产品管理：维护产品信息，它和厂商之间有关联关系；产品如 Windows（厂商是微软）、AIX（厂商是 IBM）等，如下图所示：



3. 系统类型管理：维护某种产品的不同系统版本，如 Windows7、AIX 5.2，如下图所示：



4.15.1.9 升级管理

用户可以从正规渠道获得系统升级包，然后在安全运营中心的系统管理->升级管理中导入升级包，系统会记录升级的记录。升级管理如下图所示：

4.15.1.10 许可证管理

用户可以查看和升级系统许可证；许可证包括客户名称、主机标识码、有效期、设备数（包括资产和非资产）、采集控制器数量、功能模块限制（包括漏洞管理、安全事件管理、安全基线管理及其它后续开发功能），如下图所示：

4.16. 其它

4.16.1. 安全仪表板

安全仪表板是安全运营中心系统风险的集中展示区域，也是安全运营中心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调整。

Tab 页面，主要指一级菜单下的 web 分类页面，不需要刷新整个页面而分别显示不同内容。

微件（Widget），主要指 Tab 页面中，用来显示的各种仪表、图表等。

安全仪表板应能支持用户自定义布局和展现内容。仪表板应根据权限和许可证情况进行展示；仪表板提供 TAB 管理功能，管理的内容主要有：

1. TAB 的添加、删除、排序、全屏显示。排序是调整 TAB 的先后顺序

2. TAB 中微件的添加、删除、隐藏

如下图所示：

4.16.2. 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，但会对用户的权限进行过滤，其功能主要包括：

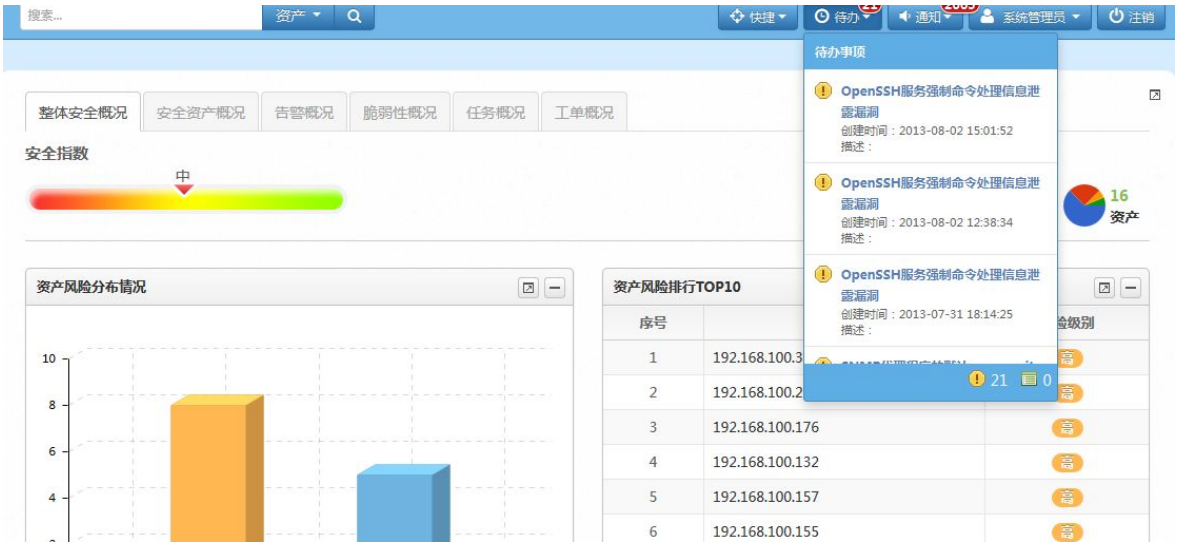
1. 对象快捷创建菜单，菜单中包含：资产、用户、任务（漏洞扫描、基线检查等）

2. 个人待办事宜：需处理的工单、告警

3. 通知功能：任务完成情况、工单变化情况

4. 系统状态:EPS（每秒事件量）

如下图所示：



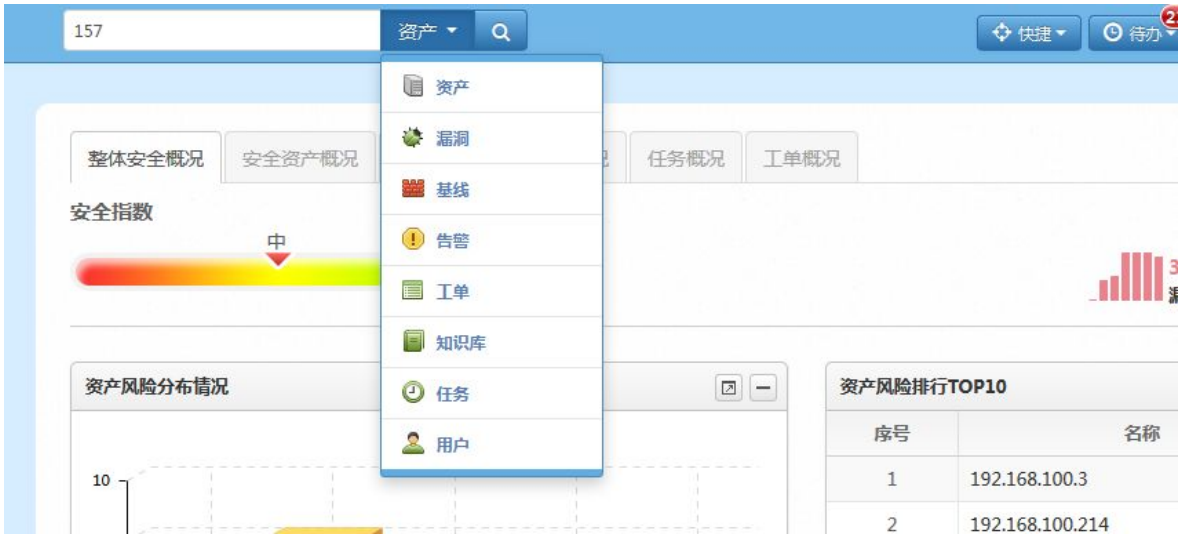
4.16.3. 全文检索

由于安全运营中心涉及到的安全数据或安全问题较多，为了便于操作，系统提供了一个全文检索功能。能对系统内的对象提供全文检索功能，对于海量数据的检索可限定检索时间段（主要针对安全事件）。全文检索提供一个输入栏，需要置顶，在任何页面都能够看到。

一个搜索输入框，可以选择搜索时间段。检索的范围主要有：

1）.资产 2）.漏洞 3）.安全基线 4）.告警 5）.工单 6）.知识库 7）.任务 8）.用户

安全事件如下图所示：



铱迅信息

Yxlink

南京铱迅信息技术股份有限公司

江苏省南京市雨花台区宁双路 18 号沁恒科技园 D 幢 4 层

Nanjing Yxlink Information

Technology Co., Ltd.

4th floor, Building D of Qinheng Science Park, No. 18

Ningshuang Rd., Yuhua District, Nanjing, Jiangsu,P.R.China

NJYXHWAFAM010-11(02)