SecFox-SIM 安全信息管理系统

产品白皮书

SecFox
Security Information Management
Product White Paper

V3.0

Revision 2

网御神州
SECWORLD

2008 年 3 月

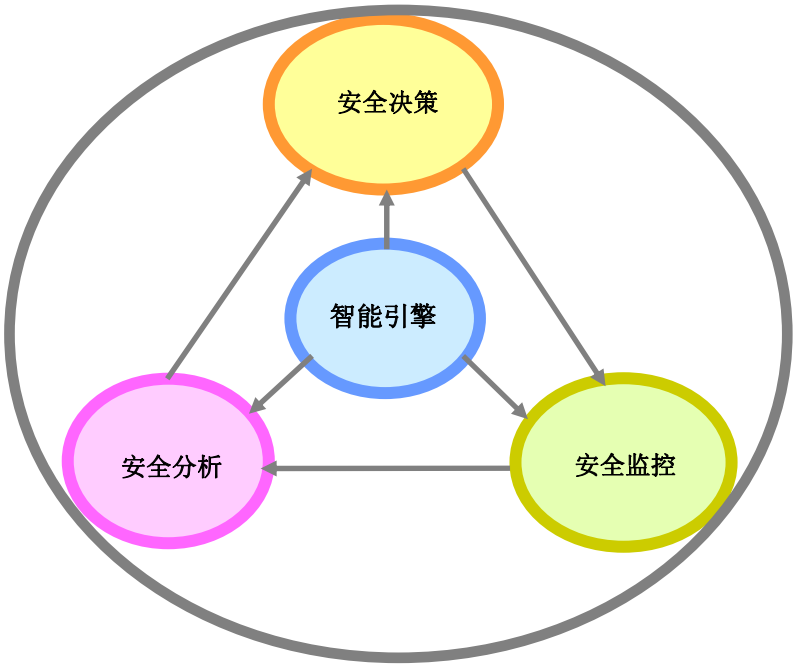
目录

1 SecFox安全管理概述

SecFox 是网御神州科技（北京）有限公司自主研发的新一代安全管理系统。网御神州科技（北京）有限公司具有一支长期在安全管理领域奋斗的高素质研发团队，凭借对安全管理的深刻理解和在安全领域丰富的研发经验，SecFox 厚积薄发，鼎力打造一个高起点、全方位、多层次的安全管理系统。

SecFox 的安全管理理念是：首先，通过对客户计算环境中包括网络设备、安全设备、主机和应用在内的节点进行统一监控，保障计算环境的整体运行安全，及时发现网络和系统主机的故障和性能瓶颈；其次，通过实时获取计算环境中的各类安全信息，进行关联分析，实现计算环境的安全态势感知，发现内部违规和外部入侵；最后，将计算环境的所有资产和威胁信息汇集到一起，通过决策分析获得可测量的安全风险，并通过对计算环境的控制来实施安全策略。整个系统在智能引擎的支持下实现持续的监控、分析、决策循环，构建起面向整体计算环境的全面可管理安全体系。

SecFox 安全管理模型如下图所示。



SecFox 安全集中管理平台由安全监控、安全分析和安全决策三个部分组成。

本产品白皮书主要介绍的产品是隶属于安全分析的 SecFox-SIM 安全信息管理系统。

2 SecFox-SIM安全信息管理系统

当今的企业和组织在 IT 信息安全领域面临比以往更为复杂的局面。这既有来自于企业和组织外部的层出不穷的入侵和攻击，也有来自于企业和组织内部的违规和泄漏。为了不断应对新的安全挑战，企业和组织先后部署了防病毒系统、防火墙、入侵检测系统、漏洞扫描系统、网闸，等等。这些安全系统都仅仅防堵来自某个方面的安全威胁，形成了一个个安全防御孤岛，无法产生协同效应。其次，IT 计算环境及其安全防御设施产生了大量的安全信息，安全管理人员面对如此众多的控制台界面和告警窗口，往往束手无策，工作效率极低，难以发现真正的安全隐患。此外，企业和组织日益迫切的信息系统审计和内控、以及持续增强的业务持续性需求，都对当前安全信息管理提出了严峻的挑战。

此外，随着国家等级保护制度的确定和全面推行，对于集中安全管理的建设的需求也日渐升温，在信息系统等级保护的基本要求中，三级以上已经明确提出要建立“监控管理与安全管理中心”，指出三级以上单位“应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理”。同时，在等级保护基本要求中，也强调了二级以上单位“应记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生”。

综上说述，企业和组织迫切需要一个全面的、面向企业和组织 IT 计算环境的、集中的安全信息管理平台及其系统，这个系统能够收集来自企业和组织计算环境中各种设备和应用的安全信息，并进行存储、监控、分析、报警、响应和报告。

网御神州利用在安全领域的长期积累，结合中国信息安全领域的特殊性，自主研制出了面向中国客户的安全信息管理平台——SecFox-SIM（Security Information Management System），真正满足了客户的安全管理需求。

SecFox-SIM 能够实时不间断地将企业和组织中来自不同厂商的安全设备、网络设备、主机、操作系统、用户业务系统的日志、警报等信息汇集到 SecFox-SIM 服务器，实现海量信息的集中存储和可靠保存。

SecFox-SIM 服务器能够实时地对采集到的不同类型的信息进行归一化和关联分析、最大程度地消除误报和错报、找出漏报，通过统一的 SecFox-SIM 控制台界面进行实时、可视化的呈现，协助安全管理人员迅速准确地识别安全事故，消除了管理员在多个控制台之间来回切换的烦恼，

同时提高工作效率。

对于集中存储起来的海量信息，SecFox-SIM 可以让分析人员借助历史分析工具对信息进行深度挖掘、调查取证、证据保全。

SecFox-SIM 能够自动的或者在管理员人工干预的情况下对识别出来的安全事故进行各种响应。

SecFox-SIM 为客户提供了丰富的报表，使得管理人员能够从各个角度对企业和组织的安全状况进行分析，并自动、定期地产生报表。

SecFox-SIM 基于 Web 浏览器的界面和面向业务的呈现方式使得 SecFox-SIM 不仅适用于安全专家，也适用于业务管理人员。

SecFox-SIM 不仅是一个系统，它更是一个平台。基于这个平台，用户可以不断地扩展信息采集的设备来源和信息的种类；基于这个平台，网御神州为客户配备了专业化的实施和部署团队，并提供从安全信息管理体系建设的咨询、到安全信息管理运维的一系列专业服务。通过网御神州的专业服务，使得客户有计划、分步骤、有针对性的落实企业和组织的安全信息管理，从而真正发挥出 SecFox-SIM 以及计算环境中已有安全设施的价值，并持续为客户带来安全保障。

针对企业和组织的不同规模，以及安全管理的不同发展阶段，SecFox-SIM 提供了很强的伸缩性和扩展性，充分保护和利用客户的已有投资。

伸缩性体现在：对于中小型的企业和组织（SMB），可以采用单一部署的方式，用一个 SecFox-SIM 服务器实现所有 IT 计算环境的安全信息管理。同时，SecFox-SIM 管理控制台可以定义为面向一个专职或者兼职的维护人员使用。对于大型企业和组织（LE），可以采取分布式部署的方式，SecFox-SIM 的管理中心各个组件可以分别运行在不同的服务器上，或者多个 SecFox-SIM 服务器之间级联，实现大规模事件处理和高可用。同时，SecFox-SIM 管理控制台可以定义为面向多种角色和不同专职管理人员操作使用。

扩展性体现在：通过 SecFox-SIM 定义的开放的配置语言，不需要编写代码，就可以轻易地采集各种设备和应用系统的日志和告警信息。此外，还支持将 SecFox-SIM 进行关联分析时用到的各种基础数据通过标准接口进行导入，例如资产信息、弱点信息、待审核用户信息，等等。SecFox-SIM 除了可以将产生的安全事故送入自带的工单系统外，还可以与企业和组织现有的工单系统（例如 HP OpenView）进行集成，实现企业和组织工作流程的一体化。SecFox-SIM 还能够与配置管理和控制系统集成，对安全事故进行控制响应。例如 SecFox-SIM 可以与 SecFox-SNI

安全网络监控管理系统集成，实现对网络设备和主机的控制；与 SecGate Manager 集成，实现对防火墙的策略联动。

3 SecFox-SIM产品特点

SecFox-SIM 安全信息管理平台的主要特点包括：

- 统一安全事件监控：态势感知
- 实时安全事件关联分析
- 高性能事件分析与存储
- 便捷、高效、可视的事件分析手段
- 快速响应与跨设备协同：实现安全管理的闭环
- 符合等级保护要求的安全合规审计
- IT 计算环境整体安全报表报告

3.1 统一安全事件监控：态势感知

SecFox-SIM 将企业和组织的 IT 计算环境中部署的各类网络或安全设备、安全系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警全部汇集起来，使得用户通过单一的管理控制台对 IT 计算环境的安全信息进行统一的安全事态监控。

统一安全监控给客户带来的直接收益就是态势感知（Situation Awareness）。通过态势感知，客户实现对全网综合安全的总体把控。态势感知的核心客户体验是 SecFox-SIM 特有的智能监控频道（SecMonitor Channel）：每个频道显示某方面的安全信息，可以缩放、可以移动换位、可以更换布局、可以调台，显示管理员想看的内容。SecFox-SIM 提供丰富的频道切换器，在不同的频道间切换。用户也可以自定义频道。

态势感知不是简单的信息堆积和罗列，这些信息是统一收集并归一化之后的信息，是用一种共同语言表达出来的。否则的话，不同的事件用各自的语言表达出来，意思各不相同，用户就会陷入管理的泥沼。

借助 SecFox-SIM 的统一监控，用户不必时常在多个控制台软件之间来回切换、浪费宝贵的时间。与此同时，由于企业和组织的所有安全信息都汇聚到一起，使得用户可以全面掌控 IT 计算环境的安全状况，对安全威胁做出更加准确的判断。

此外，企业和组织部署 SecFox-SIM 后，将有助于优化其安全管理的体系和流程。对于中小规模的企业而言，SecFox-SIM 一体化的安全事件管理界面有助于提高少数专职甚至是兼职安全管理员的工作效率。对于大型企业而言，SecFox-SIM 的角色管理功能可以清晰界定不同管理人员之间的工作职责，使得在监控管理的时候各司其职，提高协同工作的效率。

3.2 实时安全事件关联分析

SecFox-SIM 收集企业和组织中的所有安全日志和告警信息，在归一化后通过智能事件关联分析引擎，帮助安全管理员实时进行事件分析，及时识别安全事故，从而及时做出响应，实现从单点被动防御到全面主动防御的转变。

事件归一化是 SecFox-SIM 区别于传统安全事件审计系统的最大特征。SecFox-SIM 将异构的事件变成系统可识别的统一的安全事件，屏蔽了不同厂商以及不同类型的产品之间的事件差异，使得事件关联分析成为可能；而传统的审计系统直接将日志按照原始格式存储在数据库中，仅仅提供普通的日志查询功能。

实时事件关联分析是 SecFox-SIM 的核心，也是使得 SecFox-SIM 称为安全管理平台的重要因素。正是通过关联分析，将来自不同信息源的事件整合到一起，发掘出事件之间的关系，找到真正的外部入侵和内部违规。

外部入侵和内部违规行为从来都不是单一的行为，都是有时序或者逻辑上的联系的，黑客的攻击一定是分为若干步骤的，每个步骤都会在不同的设备和系统上留下蛛丝马迹，单看某个设备的日志可能无法发现问题，但是将所有这些信息合到一起，就可能发现其中的隐患，而这正是事件关联分析的目的所在。

很重要地，关联分析必须是实时的，SecFox-SIM 在采集和归一化事件后，一方面将事件存入数据库，另一方面同步在内存中（In-Memory）进行事件关联分析。实时性确保了事件被及时处理，同时能够快速发现安全隐患。

实时事件关联分析的核心是 SecFox-SIM 基于安全监测、告警和响应技术（Security Monitor,

Alert and Response Technology，简称 SMART™）的事件关联分析引擎。在关联规则的驱动下，SMART™ 事件关联分析引擎能够进行多种方式的事件关联，包括统计关联、时序关联、单事件关联、多事件关联、递归关联，等等。事件关联分析涉及到的信息包括了资产属性、弱点信息、网络拓扑信息、网络流量信息，以及设备和系统发出的各种安全日志、告警和事件。SecFox-SIM 具有国内绝对领先的事件关联分析核心技术，申请了 2 项专利技术。

3.3 高性能事件分析与存储

事件分析性能与存储能力是衡量一个安全信息管理系统（SIMS）的重要指标。

SecFox-SIM具有海量事件接收、分析和存储的能力。单个SecFox-SIM系统能够以每秒 12000 条的规模接收事件，以每秒 6000 条的规模实时关联分析，并能够在线存储[1]多达 10 亿条日志记录，相当于管理约 800G的数据量。加上系统的数据归档与离线存储功能，SecFox-SIM能够存储的数据量大小仅取决于服务器磁盘存储空间的大小。借助SecFox-SIM分布式部署的方案，日志存储性能还能提升。

SecFox-SIM 在进行数据管理的时候，对数据存储算法进行了充分优化，使得使用小型数据库的情况下就达到了上述性能。此外，用户在使用本系统的时候，无需购买额外的数据库管理系统和许可，也不必花费专门的精力去维护数据库，这些都大大降低了用户的总拥有成本。

SecFox-SIM 提供多种日志存储策略，能够方便地进行日志备份和恢复。

3.4 便捷、高效、可视化的事件分析手段

SecFox-SIM 提供了一套强大的事件分析工具，使得管理员可以便捷、高效地进行各项操作，将主要的精力从发现和查找问题变成解决问题。借助 SecFox-SIM 基于场景的行为分析（Scenario-based Behavior Analysis）技术，用户可以定义不同的实时分析场景，从不同的观察侧面对来自企业和组织各个角落的安全事件进行准实时分析，对安全事件进行下钻、关联、统计、时序分析。

通过 SecFox-SIM，可以协助安全管理人员进行事中的安全分析，在安全威胁造成严重后果之前，及时保护关键资产，阻止安全事态进一步扩散，降低损失。同时，管理员在进行实时分析的时候，可以借助 SecFox-SIM 的案例管理功能为分析过程提供决策支持。

[1] 在线存储是指将数据放置于 SecFox-SIM 在线分析系统中，用户可以随时查询和分析这些数据。相对地，离线存储是指将数据压缩后放置于 SecFox-SIM 的归档系统中。

SecFox-SIM 的事件分析技术包括事件可视化、事件追踪，以及事件趋势对比分析。

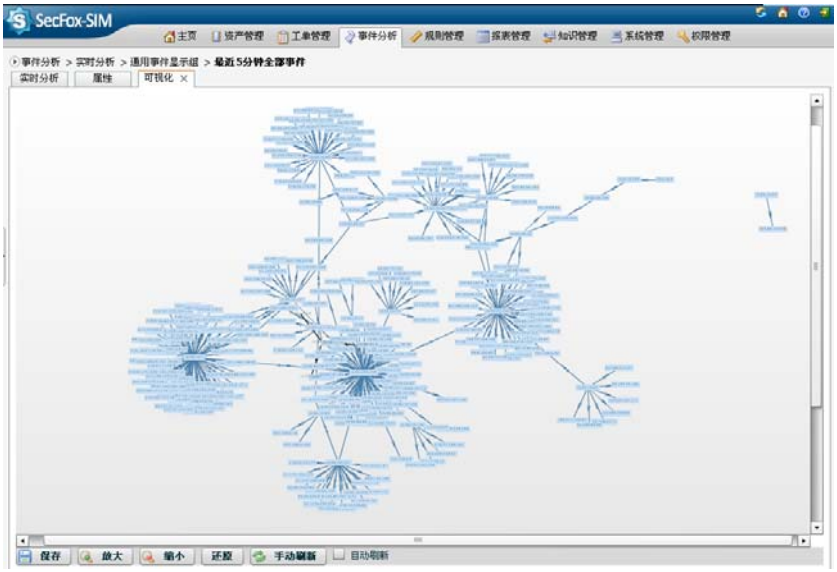
3.4.1 事件可视化

事件可视化（Event Visualization）是指 SecFox-SIM 将归一化和关联分析后的事件、威胁等以图形的形式形象的展示出来的过程。事件可视化是实时的，将安全管理和运维人员从繁重的事件查看工作中解脱出来，及时直观地进行事件调查，发现安全威胁。SecFox-SIM 具备强大的事件可视化能力，变客户日常安全管理的认知为感知。

SecFox-SIM 的安全事件可视化包括：

1. iGPS 事件全球定位系统（incident Global Position System）：在世界地图上实时定位源/目的 IP 地址的地理位置

2. AID 主动事件图（Active Incident Diagram）：通过将数千条事件记录变成一副事件图，形象地展现出当前网络安全状态，一目了然。



3. DRD 动态雷达图（Dynamic Radar Diagram）：实时的将当前系统接收到的事件按照严重性和数量动态的展现在雷达窗口中，让管理员及时了解当前阶段的安全态势。

3.4.2 事件追踪

SecFox-SIM 具备强大的事件追踪能力。基于事件关联分析技术和数据挖掘技术，系统使用了启发式事件搜索技术（Heuristic Event Searching Technology），用户可以对任何可疑事件进行追踪，帮助管理员一查到底，方便、快捷、高效。

例如，用户根据统计图标显示的内容可以查看明细，对于明细记录可以进行事件定位，可以查看事件图，也可以对某条事件进行追溯和追踪，找到引起该事件的相关事件。而且，通过事件下钻，追踪可以递归进行下去，直到找到用户关心的事件。

3.4.3 事件趋势分析

SecFox-SIM 允许管理员对比分析两个设备的网络流量或者事件数量的发展趋势，从而判断设备可能存在的隐患，例如异常流量、DDoS 攻击、BT 下载等。

事件趋势分析是事件关联分析的补充，可以在无规则的情况下通过流量建模发现异常的外部攻击和内部违规行为。

3.5 快速响应与协同防御：安全管理的闭环

SecFox-SIM 安全信息管理在识别出安全事故后，能够自动或者用户手工的进行响应，采取安全对策，从而形成安全信息管理的闭环。

SecFox-SIM 由于综合分析来自防火墙、IDS、系统日志、网络、资产价值、脆弱性等等一系列的信息，因而能够更为精确地定位安全威胁，使得实时自动阻止攻击变得更加可行。

在发生告警后，SecFox-SIM 可以通过电子邮件、SNMP Trap 的方式对外发出通告；能够执行预定义命令行程序，并将事件属性作为参数传递给该命令行程序。

SecFox-SIM 可通过与网络设备或安全设备共同协作来关闭威胁通信，以阻止正在进行的攻击。SecFox-SIM 可以与众多第三方网络设备、安全设备进行联动。例如，在发现攻击后，阻断网络交换机的端口，或者更改防火墙和入侵检测系统的安全规则，阻止攻击的扩散和恶化。SecFox-LAS 支持与市场上大部分安全设备和网络设备之间的策略联动。

通过 SecFox-SIM 与其他网御神州 SecFox 安全管理产品的综合使用，可以实现完整的从安全风险监控、分析到决策的安全管理流程的闭环。

SecFox-SIM 还能够在识别出安全事故后派发事故工单，通过信息安全事件响应流程去处理安全事故。工单管理是 SecFox-SIM 的核心流程，它的功能实现遵循 ISO18044 标准和 ISO20000 标准（ITIL）。处理过程中，派单人和责任人可以对现象描述、原因分析、处理意见、处理结果中增加内容，但不能修改以前人输入的内容。系统需记录增加的时间和增加人。在显示工单时，会显示所有的修改记录。

SecFox-SIM 除了内置的工单管理功能，通过工单系统接口，还可以与 HP OpenView Service Desk 集成。

SecFox-SIM 的响应方式包括带内响应和带外响应两种。前面提到的是带内响应，即依靠现有的网络基础设施进行响应。带外响应则可以在网络已经出现运行中断的情况下发出重要的安全事件，及时提醒管理员。使得管理员通过收到的事件线索进行分析和快速响应。典型的带外响应包括电话、短信等。

3.6 符合等级保护要求的安全合规审计

根据国标 GB/T 20271-2006《信息安全技术 信息系统通用安全技术要求》，信息系统由支持软件运行的硬件系统、对系统资源进行管理和为用户使用提供基本支持的系统软件、以及实现信息系统应用功能的应用系统软件组成。信息系统审计要求企业和组织对组成信息系统的上述组成部分从安全的角度进行合规性审计。

SecFox-SIM 为用户提供了一个规则驱动的事件分析引擎。基于这个事件分析引擎，

SecFox-SIM 通过将法律法规和标准映射为一组规则，通过对 SecFox-SIM 采集的大量安全事件进行规则匹配分析，实现审计网络异常流量、审计用户行为，等等。

合规管理包括规则管理、合规检查和分析、报告生成和反馈等功能。

客户可以在网御神州专业合规审计专家的协助下，建立起基于 SecFox-SIM 的合规管理体系，使得企业和组织的信息系统审计符合国标（例如 GB17859 等级化保护）的要求，或者企业和组织内部的规定（例如 NIST SP800-53）。

特别地，网御神州为客户提供了一套基于信息系统等级保护基本要求的合规审计包。该审计包按照等级保护的基本技术要求，针对二级以上的系统建立了一套规则库、合规检查频道和场景、报表模板。

3.7 IT计算环境整体安全报表报告

SecFox-SIM 具有强大的统计分析和报表报告功能，能从多种角度多种维度对数据进行实时分析和历史分析，对比统计的结果，分析事态的发展趋势。

SecFox-SIM 的报表报告生成系统灵活易用。它提供大量预定义的报表模板，用户可使用预定义的报表模板生成报表。

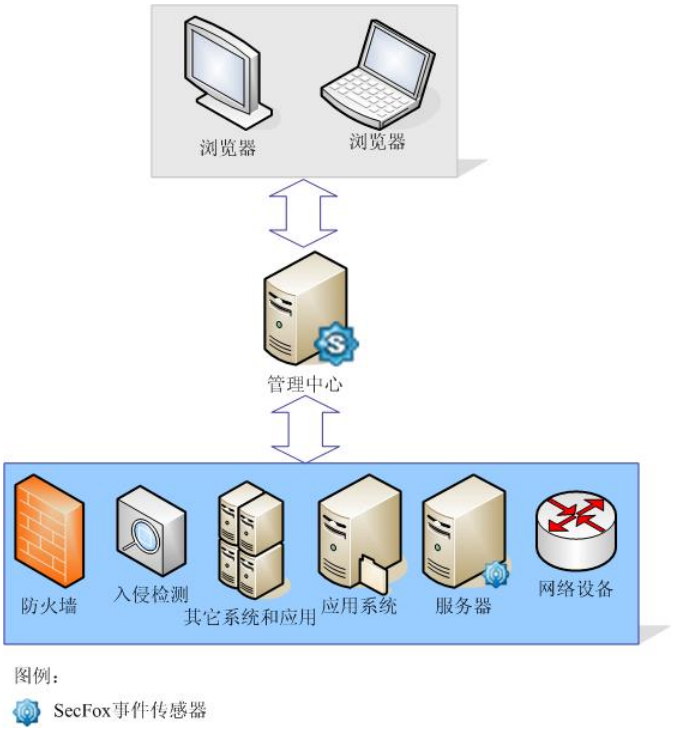
SecFox-SIM 集成了报表编辑器，用户可以根据自己的需求自行创建新的报表。

SecFox-SIM 生成的报表图文并茂，报表可以按组管理，可以对报表生成进行日程规划，并根据计划归档报告，归档之后发送邮件通知。报告可用 PDF、HTML、Excel、CSV 或 RTF 等格式存档。

4 产品简介

4.1 产品组成

SecFox-SIM 产品包括管理中心和可选的事件采集器。用户通过 IE 浏览器登录管理中心进行各种操作。



各部分的软件运行环境如下：

- SecFox 管理中心

平台	支持的操作系统	系统需求
Windows	Windows 2000 Server Windows Server 2003 系列 Windows XP Professional	-最低 Pentium 4 2.93GHz CPU，推荐使用 Intel Pentium Xeon 1.6GHz 以上 CPU -至少 1GB 内存，推荐 2GB -200GB磁盘空间[2]
Linux	Redhat Enterprise Linux AS3 Redhat Enterprise Linux AS4	-最低 Pentium 4 2.93GHz CPU，推荐使用 Intel Pentium Xeon 1.6GHz 以上 CPU -至少 1GB 内存，推荐 2GB 内存 -200GB磁盘空间[3]

- 事件传感器

[2] 实际磁盘空间大小取决于需要存储的数据量或者在线存储的时间。
[3] 实际磁盘空间大小取决于需要存储的数据量或者在线存储的时间。

事件传感器运行在安装了 Windows 系列操作系统的主机和服务器上。

■ Web 控制台

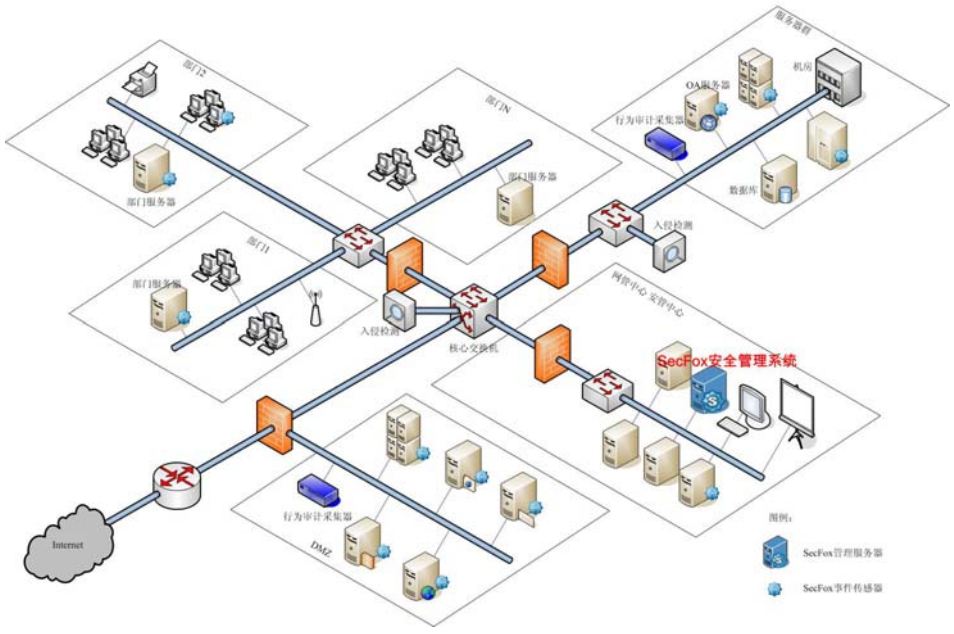
平台	支持的操作系统	系统需求
Windows	Microsoft Windows 2000 系列 Microsoft Windows 2003 系列 Microsoft Windows XP 系列	-最低 Pentium III 1.1GHz CPU -至少 256M 内存 -1G 磁盘空间 -16 位真彩，建议分辨率为 1024×768 以上 -Internet Explorer 6.0 以上

4.2 性能指标

- 推荐配置下达到平均 6000 条/秒 EPS 的事件分析能力
- 事件存储量仅取决于系统所用存储空间大小
- WEB 控制台登录管理中心的用户最大并发连接数：50 个
- 事件采集器对于所在主机和服务器的 CPU 利用率占用：<2%

4.3 运行环境

SecFox-SIM 可应用于大中小各类型企业，其办公地点可能分布在许多地方，他们的业务系统需要跨越不同的局域网段来部署。典型的，SecFox-SIM 管理中心服务器放置在网管中心或者安全中心，管理员通过浏览器可以从任何位置登录管理中心服务器，进行各项操作，如下图所示：



对于大型的、全国性的、分级的网络环境，SecFox-SIM 可以进行级联部署，多个 SecFox-SIM 管理分支可以统一接入到一个主 SecFox-SIM 管理中心。

4.4 支持的产品

SecFox-SIM 具备强大的数据收集能力，支持各种主流产品，通过 SNMP、Syslog、数据库、文件等多种方式完成数据收集功能。下表列举了部分 SecFox-SIM 支持的产品：

设备类型	厂商或产品
交换机	Cisco 交换机系列 华为 QuidWay 交换机系列 H3C 交换机系列
路由器	Cisco 路由器系列 华为 QuidWay 路由器系列
防火墙	网御神州 SecGate 系列 Cisco PIX 系列 Juniper Netscreen 系列 Fortinet 防火墙系列 Symantec 防火墙系列 Checkpoint 系列 天融信系列 联想网御系列 启明星辰天清汉马系列
IDS	网御神州 SecIDS 启明星辰天阗 IDS 东软 NetEye IDS 安氏 LinkTrust IDS 三零盛安鹰眼 IDS 绿盟 IDS
操作系统及服务	IBM AIX HP-UX Microsoft Windows NT/2000/2003/XP Solaris BSM Linux 系列 IIS Server Apache Server EasyMail Server
数据库	Oracle SQL Server
防病毒	瑞星 Symentec AntiVirus TrendMicro

	Macfee
中间件	Weblogic JBoss
VPN	网御神州 SecGate 3600 东软 NetEye VPN 天融信 VPN
物理安防	门禁（需要定制）
业务系统	各种客户自有的业务系统（需要定制）
Syslog 事件源	只要 syslog 事件源，SecFox-SIM 都能够采集
SNMP Trap 事件源	只要 SNMP Trap 事件源，SecFox-SIM 都能够采集

此外，SecFox-SIM还提供设备事件解析工具包，用户可以根据自己的需求很容易地定制开发新的代理，而无需编写程序代码。如果原厂商开放日志并提供相应的日志说明文档，网御神州开发人员可以很快开发出支持新设备的采集器。

5 产品功能

以下简要说明 SecFox-SIM 产品各组成部分的功能。

5.1 智能监控频道

智能监控频道为用户提供了一个从总体上把握企业和组织整体安全情况的界面。通过监控频道，用户可以看到当前企业和组织的整体安全等级。每个监控频道显示某方面的安全信息，可以缩放、可以移动换位、可以更换布局、可以调台，显示管理员想看的内容。SecFox-SIM 提供丰富的频道切换器，在不同的频道间切换。用户也可以自定义频道。

5.2 资产管理

ISO17799-2005 中对资产的定义是：“任何对组织和企业有价值的事务”。

资产是企业和组织的 IT 计算环境的核心，承载了当今绝大部分企业和组织的业务。重要的资产的安全决定了企业和组织的核心竞争力和命脉。企业安全管理很重要的工作就是确保资产安全，评估和分析在遭受安全威胁的情况下资产的受影响程度，从而进行企业和组织的安全风险管理。

SecFox-SIM 按照资产重要程度和管理域的方式组织资产，提供便捷的添加、修改、删除、查询与统计功能，便于安全管理和系统管理人员能方便地查找所需资产的信息，并对资产属性进行维护。

对于每个资产，用户可以设置资产的地理位置，便于将来在世界地图上显示出该资产相关的事件。

基于 SecFox-SIM 的动态资产属性（Dynamic Asset Attribute）技术，用户可以对资产属性进行无限扩展，例如可以根据客户自身的需要为资产增加业务重要性属性、增加资产保护等级属性、增加资产品牌、代号等任何信息。同时，所有这些附加资产属性随时都可以作为查询条件进行检索，也可以作为事件关联分析时的规则的一部分。

5.3 工单管理

SecFox-SIM 工单管理参照 ISO17799、 ISO20000（ITIL 规范），以及 ISO18044，为安全管理人员建立了一套安全事故处理流程。通过工单，实现了安全事故的记录从创建、处理到关闭的生命周期管理。

工单管理是 SecFox-SIM 的核心流程，它的功能实现遵循 ISO18044 标准和 ISO20000 标准（ITIL）。处理过程中，派单人和责任人可以对现象描述、原因分析、处理意见、处理结果中增加内容，但不能修改以前人输入的内容。系统需记录增加的时间和增加人。在显示工单时，会显示所有的修改记录。

管理员在创建工单后，可以由系统自动发送邮件给指定的工单处理人，提醒其及时处理。

5.4 事件分析

事件分析是 SecFox-SIM 的核心，监控管理人员可以通过事件分析对来自企业和组织所有的事件，以及经过 SecFox-SIM 规则关联后产生的事件进行可视化实时分析、历史分析和事件统计，从而快速识别安全事故。SecFox-SIM 采用基于场景的行为分析（Scenario-based Behavior Analysis）技术，将所有的事件分析都以分析场景的方式列举出来，管理人员可以方便的在各种分析场景之间快速切换，就像切换电视频道一样，大大提高分析工作的效率。

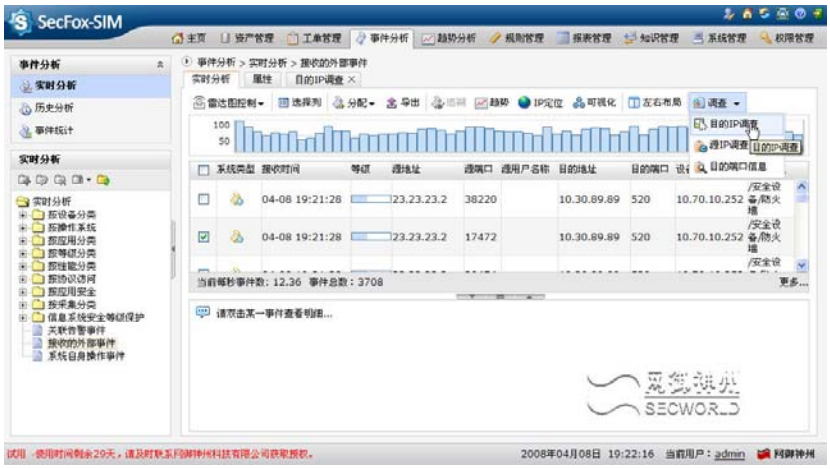
针对每个场景，系统都会实时展示出该场景的事件列表，并且附上一副事件的动态雷达图（Dynamic Radar Diagram）。用户可以实时观察某个事件切片内的事件数量及其不同等级事件的时间分布。点击每个时间切片上的事件方块，可以查看该时切片的事件明细。

对于发现的攻击和威胁，用户可以借助 SecFox-SIM 的 iGPS 事件全球定位系统在世界地图上可视化地展示出发起和遭受攻击 IP 所在的地理位置。

用户也可以对选中的事件生成可视化的实时主动事件图（Active Incident Diagram），形象地

观测到当前事件的安全态势。用户点击主动事件图上的 IP 节点，可以查看该节点的明细信息，点击节点之间的连线可以查看事件的端口、协议等信息。主动事件图可以放大、缩小、自由拖动。

在事件分析中，SecFox-SIM 还为用户提供了一套进行深入的审计与追踪工具——事件调查工具。借助网御神州独有的启发式事件搜索技术（Heuristic Event Searching Technology），管理员通过事件调查工具可以对某条感兴趣的事件中的源 IP 地址、目的 IP 地址、或者目的端口进行相关性事件检索。例如，管理员通过审计某条事件记录发现某用户违规访问一个敏感的外部 IP 地址，那么管理员可以通过事件调查工具查找最近 5 分钟内访问同一个敏感外部 IP 的其它用户的事件记录，从而追踪违规行为；管理员也可以查找某个事件记录中目的端口的含义，是 MSN 端口？还是 BT 端口？抑或是蠕虫端口？等等，从而快速了解当前用户的行为特征。



5.5 趋势分析

SecFox-SIM 可以对设备的网络连接数、网络流量，以及时间数量等的趋势进行分析，并以图标的形式展示。

趋势分析的时间段可以动态调整，包括最近 24 小时、最近 1 天、最近 1 周，等等，用户亦可自行设置。

5.6 规则管理

规则，即事件关联规则，是对安全事件之间关系的形式化描述。SecFox-SIM 在事件分析引擎的驱动下，根据事件关联规则，针对来自企业和组织的海量事件进行关联分析，抽取出对于安全管理人员真正有用的安全信息，从而协助安全管理人员快速识别安全事故。

规则分为系统预定义规则和用户自定义规则两大类。系统内置大量预定义规则。规则包括两个组成部分，即安全事故的触发条件部分，简称规则条件，以及产生安全事故后的响应动作部分，简称规则动作。

SecFox-SIM 提供可视化、便捷的规则编辑器，用户可以容易地定制规则。系统同时支持直接使用规则描述脚本（XML）创建规则文件。修订规则无需重启系统或者某个模块，规则一旦被应用立刻成为关联引擎的一部分。规则完全与厂商无关，用户即使更换安全设备也无需重写规则。

5.6.1 规则条件

用户在设置规则条件的时候，支持各种运算符，如下表所示：

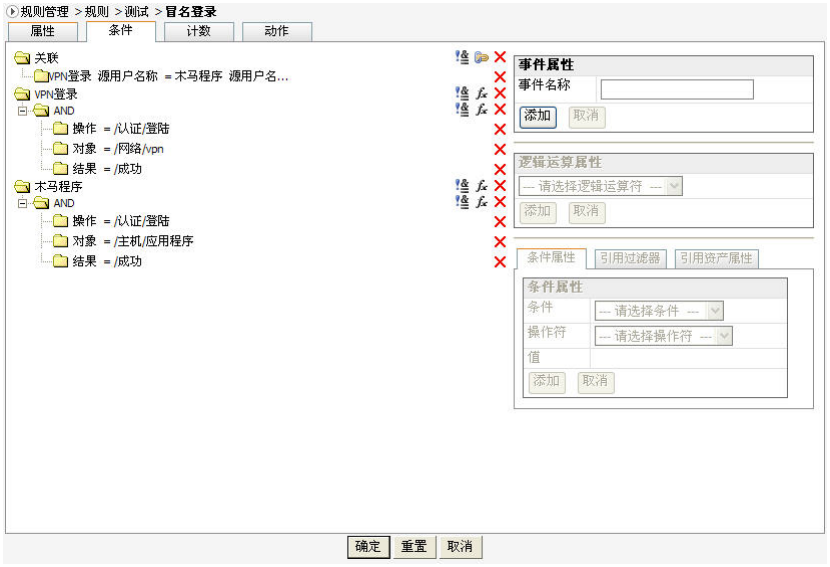
运算符	说明
=	等于
!=	不等于
<	小于
<=	小于等于
>=	大于等于
>	大于
Between	事件发生在指定的日期时间段，或连续数值范围
InNumber	属于一组离散数值范围

In	属于一组字符串
IsNull	是否为空
Contains	包含指定的子串
StartsWith	以指定的子串开始
EndsWith	以指定的子串结束
Matches	扩展正则表达式
MatchesFilter	匹配过滤器
InSubnet	IP 地址在指定子网里
InCategory	资产是否具备某属性

除了支持各种逻辑和条件运算，SecFox-SIM 还允许用户引用各种外部资源，包括过滤器、资产属性、自定义资源、递归规则、过滤器插件、黑白名单，等等。

过滤器是构成规则的基本单位，也是进行事件分析的条件选项。用户定义了过滤器之后，可以进行各种复杂的事件分析场景设置。

通过引用外部资源，使得用户可以方便地、形象化的进行关联规则定义。例如用户可以轻松地定义一条这样的规则“所有‘非工作时间’发起的针对‘核心数据库服务器’发起的登录操作的源 IP 地址在登录操作发生的前后 5 分钟内的告警事件”。该规则中，“非工作时间”和“核心数据库服务器”属于外部过滤器。“非工作时间”定义为“周一至周五 9:00 至 18:00”，……。

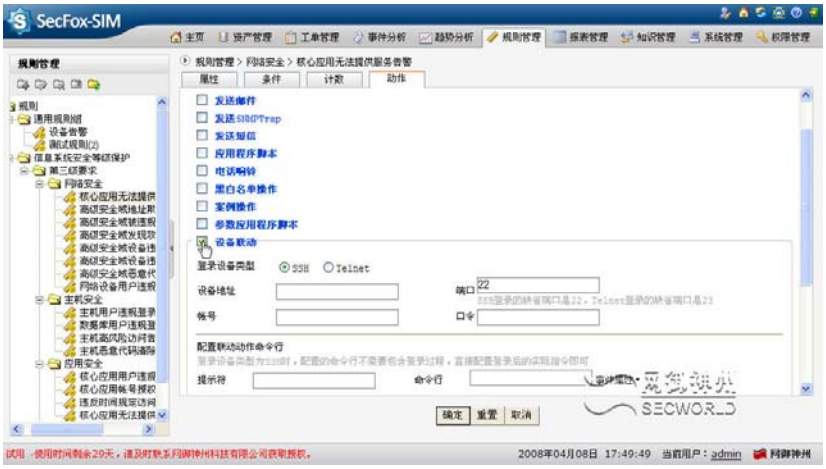


用户可以对规则条件设置计数。通过技术设置实现具有某些相同属性的事件的归并关联，从而发现某些攻击行为，例如水平端口扫描、垂直端口扫描、DoS 攻击，等等。

SecFox-SIM 具备独有的规则条件插件技术（Rule Condition Plug-ins Technology），为用户提供了一个开放的接口，允许将一个外部的条件判断过程导入现行的规则条件中，实现了跨系统的事件关联。例如，可以实现 SecFox-SIM 事件与 AAA 服务器认证结果的跨系统关联，或者与设备控制结果的关联。

5.6.2 规则动作

通过对规则动作的设定，确保 SecFox-SIM 在识别出安全事故后，系统能够及时进行响应处理，包括发送邮件、短信、SNMP Trap、执行程序脚本、电话响铃、策略联动，以及将安全事故分配到工单、黑白名单和案例。



SecFox-SIM 提供了策略联动的机制，实现了安全事件管理的闭环。SecFox-SIM 使用开放技术，支持各种第三方的网络设备和安全设备。

下表列举了 SecFox-SIM 的响应机制：

响应方式	说明
设置告警属性	设置通过规则引擎生成的关联事件的告警属性
运行参数应用程序脚本	运行用户指定的某个程序的 CLI 脚本，并能够将告警属性作为参数传递给 CLI 程序
设备联动	自动执行一组针对第三方网络设备或者安全设备的联动指令
发送电子邮件	发送一封电子邮件给指定人
发送 SNMP Trap	发送 snmp trap 信息到指定 IP
发送一个事件到网管系统	例如发送给 HP OpenView NNM
发送一个事件到服务台系统	例如发送给 HP Service Desk，或者 BMC
将攻击者或受害人添加到黑白名单中	将产生该关联事件的重要原始属性添加到黑白名单中，供管理员重点观察。对于加入黑白名单的资产，管理员可以设定观察周期
创建或附加一个案例	根据关联事件生成一个案例，供以后遇到类似情形时提供辅助决策
带外响应	指通过网络之外的方式进行告警响应，避免由于网络故障导致告警不可达。包括发送手机短消息、电话响铃

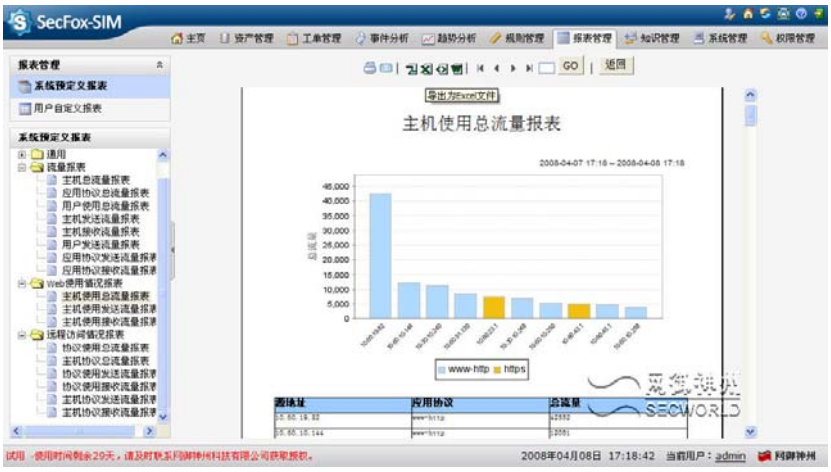
5.7 报表管理

安全管理人员可以将事件分析的结果生成报表，作为工作内容汇报的一部分提交给相关部门。

SecFox-SIM 将报表分为系统预定义报表和用户自定义报表两大类。

SecFox-SIM 内置大量预定义报表，例如：

- 当天，当月，该季度，该年度的出现率最多的十种安全事件统计分析报表，既能够图文并茂地显示十种安全事件的统计值，也能够选择察看具体的安全事件明细表；
- 当天，当月，该季度，该年度的出现率最多的十个源 IP 地址统计分析报表，既能够图文并茂地显示十个源 IP 地址的统计值，也能够选择察看出现该 IP 地址的具体的事件内容；
- 每月，每周事件告警严重程度级别趋势表，分类统计每个月所有的安全事件的严重程度级别，察看其发展趋势；
- 每天的安全事件统计表，统计每一天的所有安全事件发生的总数；
- 可以指定源 IP，目的 IP，源端口，目的端口一项或者几项内容制作出对应安全事件的详细报表。
- 每天，每周，每月出现最多的十种病毒统计分析报表；
- 每天，每周，每月的事故统计报表；
- 每天，每周，每月的各种安全状况的总览表，在一张报表上图文并茂地展示这一天，这一周，或者这个月的，全网的安全状况的多种指标统计和趋势图表。



SecFox-SIM 具备强大的自定义报表功能。用户可以通过报表编辑器，只需 4 步，即可方便地自己定义各种复杂的报表，包括报表的内容、布局，以及运行调度设置，满足企业和组织自身不断业务发展的需要。

5.8 知识管理

SecFox-SIM 知识管理为用户提供了一套面向业务的管理工具，方便用户进行安全事件的识别和应急响应处理。SecFox-SIM 知识管理包括黑白名单管理和案例管理。

- **黑白名单管理**

黑白名单，是指需要格外关注的事件属性，比如某黑白名单定义为某些符合规则条件的事件的某个属性的列表。

黑白名单是一个非常灵活的信息收集工具，它可以基于事件属性的任意组合或自定义字段组监控活动，而不仅仅是 IP 地址。在记录可疑的或恶意的 IP 地址以及有可能已被攻击成功的目标方面，黑白名单非常有用。

用户可以手动增加黑白名单的内容，也可以通过规则响应动态地增加或删除黑白名单中的记录。例如，我们在发现一个恶意攻击之后，可以将攻击源添加到恶意列表中，并在以后严密监控该 IP 的各种行为。

SecFox-SIM 包含了大量预定义的黑白名单列表，比如恶意列表、可疑列表、受信任的列表、不受信任的列表、受威胁列表等等，用户可以把它们作为模板使用。

- **案例管理**

案例是由一组相关事件组成的有意义的、值得借鉴的情景，用于安全信息管理经验和知识的积累。

通过将安全信息管理运维过程中遇到的具有典型性的事件放入案例库中，并记录下当时事故的影响情况、采取的安全处理措施，为将来遇到类似事故提供辅助策略的依据。

5.9 系统管理

5.9.1 系统配置

SecFox-SIM 的系统管理员可以通过系统管理中的系统配置对 SecFox-SIM 系统自身进行各种参数配置，包括数据的备份与恢复、系统自身运行状态的监控，等等；通过系统管理中的事件传感器管理连接到 SecFox-SIM 平台的事件传感器；在系统管理中还有过滤器和资源定义模块。

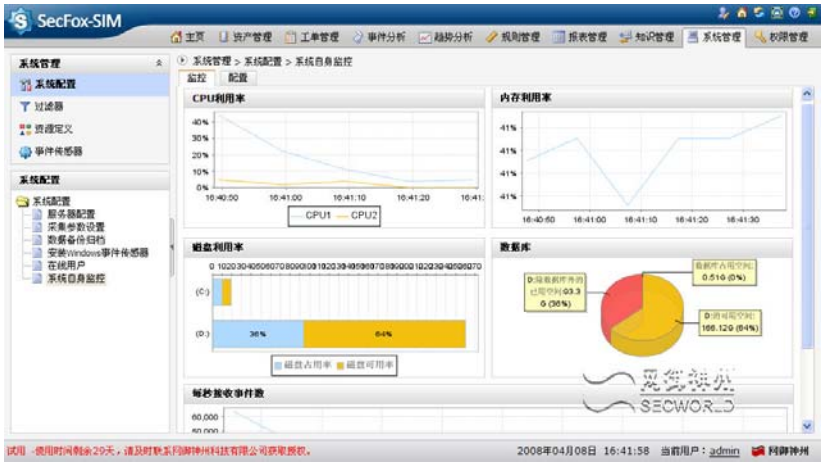
事件传感器是 SecFox-SIM 提供的、用于安装在企业和组织网络中的目标主机上的应用程序。通过事件传感器，SecFox-SIM 可以主动地采集目标主机上的事件，在管理服务器上进行事件分析。

过滤器是构成规则的基本单位，也是进行日志审计的条件选项。用户定义了过滤器之后，可以进行各种复杂的日志实时分析场景设置。

通过资源定义，用户可以建立安全领域的知识库，并建立业务相关的集合。例如可以定义办公 IP 地址组、定义上班时间、定义 BT 常用端口集合或者常见的蠕虫端口集合，等等。在定义好资源后，用户可以在过滤器和告警规则中任意引用，使得管理员的各种设置操作真正基于业务和领域知识，而不是基础的端口、IP、时间等原始信息。

5.9.2 系统自身健康监控

SecFox-SIM 具有完善的系统自身健康监控功能（System Self Healthiness），能够对系统自身运行状态进行监控，包括系统 CPU 和内存利用率，存储可用容量，等等，遇到问题自动报警，确保安全管理平台自身的可靠性。



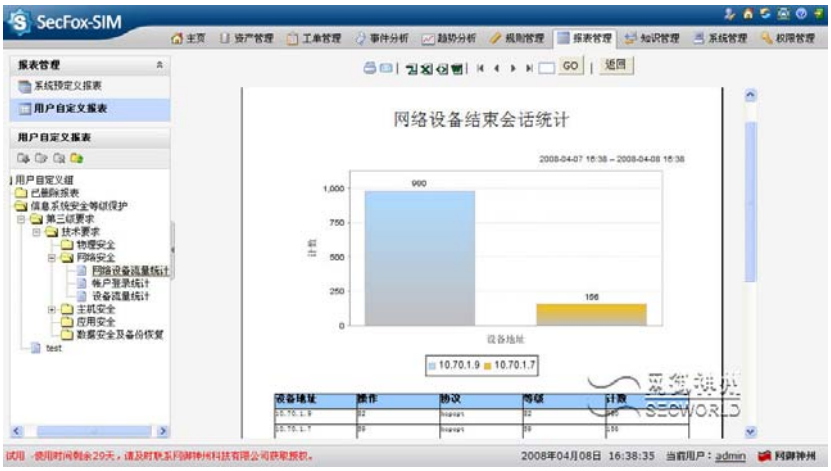
5.10 权限管理

SecFox-SIM 是一个多用户系统，不同的用户可以具备不同的权限。这意味着不同权限的用户可以使用 SecFox-SIM 的全部或者部分功能。

SecFox-SIM 采用基于角色的权限管理机制。通过权限管理，管理员可以为不同的用户分配角色，指定该用户能够使用的功能。

5.11 等级保护模块

SecFox-SIM 能够对审计系统中管理的所有信息资产进行统一的等级化保护管理，按照等级化保护 2 级到 4 级的基本要求提供实时审计的分析场景知识库，以及针对等级化保护要求的报表模板。



5.12 与外部系统集成

SecFox-SIM 提供了丰富的 API 接口，能够与广大第三方管理平台（包括 IBM Tivoli，HP OpenView Operations，BMC 等）和服务控制台（Service Desk）集成，包括事件和告警信息的集成，以及策略联动的集成。

6 SecFox-SIM不仅仅是一款安全产品

作为一款集成企业和组织 IT 计算环境各种安全设施的集中管理系统，SecFox-SIM 不仅提升了原有的安全管理方式，而且也有助于提升企业和组织的安全管理策略。因而，如果没有好的规划、部署、实施和运维的流程、管理经验和最佳实践，企业和组织建立一个行之有效的安全信息管理体系并非轻而易举。

例如，在部署安全信息管理系统之前，需要确定针对哪些安全设施采集日志和事件？采集哪些日志和事件？如何配置这些安全设施使得事件能够发送到管理中心？企业和组织的网络中哪些位置还需要部署额外的安全设施？在实施安全信息管理系统的时候，需要清楚企业和组织最关注的安全问题是什么？这些关注的安全问题如何映射到安全信息管理系统之中？是否需要和企业或组织的其它信息系统（例如工单系统、OA 系统、安全门户）集成？在运行安全信息管理系统的过程中，何时进行有效的事件审计？收到安全告警应该如何进行应急响应和处理？

上述问题不是购买了一个安全信息管理系统就能够解决的，关键在于部署之后的安全运维，在于系统的日常使用，也就是使用安全信息管理系统的方法和流程。

网御神州通过大量的安全信息管理系统的部署、实施和运维，积累了大量的实践经验，归纳和总结出了一套行之有效的安全运行管理的标准操作流程（SOP），下表显示了部分摘要：

阶段	标准操作流程	说明
规划阶段	网络拓扑分析、安全现状分析和部署建议书	分析网络和计算环境安全现状，提出需要如何部署 SecFox-SIM，例如采集哪些安全设施的信息，如何采集，等等
	职责和流程建议书	结合企业和组织的现状，给出 SecFox-SIM 安全运维的职责和流程建议
部署和实施阶段	日志和事件源采集	配置事件源，定义数据归一化映射关系，必要的情况下进行定制开发和测试
	定义场景、关联规则和报表	根据企业和组织的安全目标来定义
	和其它系统集成	如有必要，将 SecFox-SIM 和其他系统集成，例如企业和组织的工单系统、OA 系统、安全管理门户网站、网管中心系统，等等
	培训	各类管理、维护和使用的培训，及其文档
运行和维护阶段	安全事件分析流程	如何分析安全事件，发现安全威胁
	安全告警应急响应处理流程	遇到安全突发事件，如何进行响应和处理 参照 ISO18044-2004
	安全信息审计流程	如何进行安全审计、内控和合规性检查

	SecFox-SIM 配置维护流程	如何修改现有安全设施事件源的配置以适应企业和组织的安全目标变化？何时以及如何采集新的安全设施的日志和事件？

本质上，SecFox-SIM 产品是一个管理平台，是一套集成了业界最佳实践的工具集。结合网御神州安全运维的标准操作流程和相关知识积累，以及专业化的实施、运维的服务支持，有助于用户使 SecFox-SIM 迅速发挥功效，真正实现预期的安全目标。

7 SecFox-SIM价值

SecFox-SIM 从不同层面为企业和组织的用户带来价值回报。

对于安全管理员、安全分析员、安全运维人员：

- 明确工作职责，各类安全管理人员各司其职，协同合作
- 提高工作效率，更加快速准确的识别安全告警，发现违规行为，进行应急响应
- 发生安全问题，事后调查有据可循

对于安全负责人，负责安全的高管：

- 有助于建立一套可行的安全策略的执行方针，并通过 SecFox-SIM 真正落实
- 通过持续有效的安全事件分析识别安全事故、策略冲突、欺诈行为和操作行为
- 通过安全事件分析有助于进行审计和取证分析、支持内部调查、建立基线，以及进行安全运行趋势预测，确保企业和组织的业务的持续性和可靠性
- 通过设备和系统的日志以及安全事件的统一存储，符合企业和组织的需要，符合国家和行业的法律法规
- 自动产生各种分析报表和报告，随时掌控整个企业和组织的安全状况

对企业和组织，领导层：

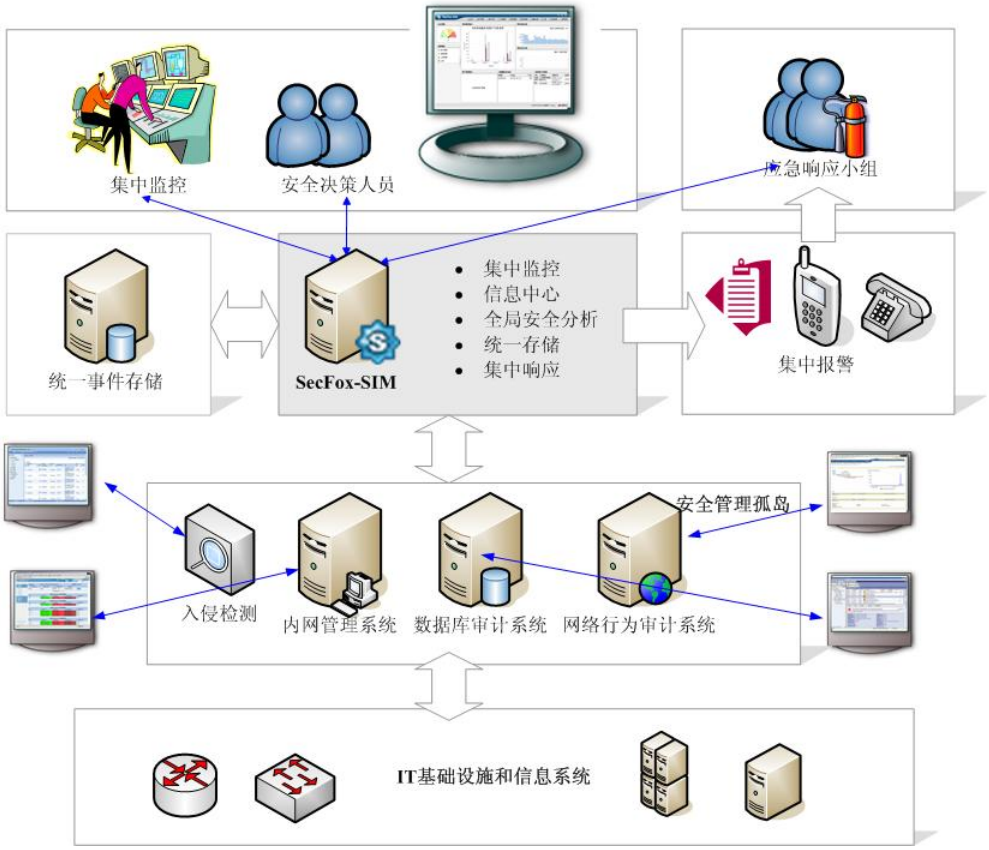
- 随时可以全局掌握企业和组织的安全总体状况，为领导层进行安全建设决策提供依据
- 从整体上提升了企业和组织的安全防护水平
- 通过对 SecFox-SIM 的投资发挥出原有各种安全设施的投资的潜在价值，从而使得企业和组织的成本效益最大化，降低总拥有成本（TCO），提升安全设施的投资回报率（ROI）

8 SecFox-SIM优势

SecFox-SIM 作为网御神州完全自主研发的一款针对中国市场的面向整个企业和组织的整体安全信息集中管理解决方案，具有无可比拟的优势。主要体现在以下几个方面：

1、 和其它类型的安全产品相比，SecFox-SIM 着眼于企业和组织的整体安全管理

SecFox-SIM 不是 IDS，也不是单纯的审计系统，而是一款超越现有安全产品的集成性管理平台，实现了安全信息的集中管理，包括集中的数据采集和分析、统一的存储、集中的应急响应和控制，有助于落实安全策略、实现企业和组织的安全目标。



SecFox-SIM 有助于企业和组织消除安全防御的孤岛，同时不会造成新的孤岛。SecFox-SIM 可以充分发挥现有安全设备和系统的功效。

SecFox-SIM 符合国家信息系统安全等级保护制度中对于安全管理中心的建设要求，可以作为企业和组织的安全总控中心（SOC/SMC）的基础技术平台。配合网御神州 SecFox 系列其它安全管理类产品，可以构成一个真正意义上的安全运行中心（SOC）。

2、 和同类型产品相比，SecFox-SIM 具有明显的技术领先性

SecFox-SIM 建立在完全自研的微内核中间件架构的基础上，整个架构轻量级、并且具有很强的实时性，规避了传统中间件平台的复杂性。系统采用面向服务架构（SOA）的组件方式进行设计，具有极强的开放性和可扩展性，能够方便地将各类安全设施纳入管理范围，同时能够顺畅和其它系统进行互联互通，例如与网管平台接口、与运维/工单/服务台系统对接、与企业信息门户集成，等等。

SecFox-SIM 性能和伸缩性俱佳，单个系统能够支持每秒采集 12000 条事件、关联分析 6000 条事件，在线存储超过 800G 的数据。通过分布式部署和级联，可以满足大型企业的需求。

SecFox-SIM 具有业界最佳的关联分析引擎，独有的关联分析算法支持多种分析方式，配合基于异常的检测机制，全面感知网络整体安全态势。

SecFox-SIM 的关联分析引擎具有很强的实时处理能力，所有操作都在内存中进行，使用已经申请通过的“内存快速符号表检索”专利技术，避免了传统基于状态机的规则引擎的处理效率低的问题。

SecFox-SIM 具有极强的信息可视化展现能力，变用户认知为感知，提升安全运营的效率。

3、 SecFox-SIM 完全自主研发，针对国内市场，真正把握用户需求

SecFox-SIM 是网御神州安全管理团队历时数年完全自主研发的一款针对中国市场需求的安全信息管理产品。

在产品设计上，SecFox-SIM 充分考虑了中国用户的安全管理体制和运行使用的模式，着重于安全整体态势的监测，安全隐患的识别、审计和响应，简化安全问题处理的流程和繁复的安全预配置。系统安装简单，而且无需手工安装和配置数据库管理系统。系统内置大量预定义的规则、模板，安装完毕，即可使用。此外，SecFox-SIM 在设计之时，遵循我国的安全标准和规范，尤其是信息系统安全保护等级基本要求和实施指南，以及国家部委和各行业的安全指引。

在系统的操作和使用上，SecFox-SIM 采用业界最先进的 WEB2.0 技术，所有操作和交互都符合中国用户的使用行为，界面上的名词和术语都符合中国用户的理解方式。

4、 SecFox-SIM 不仅是一款产品，而且包含网御神州丰富的安全管理、实施和运维经验

SecFox-SIM 不仅是一款安全信息管理产品。结合网御神州安全运维的标准操作流程和相关知识积累，以及专业化的实施、运维的服务支持，有助于用户使 SecFox-SIM 迅速发挥功效，真正实现预期的安全目标。

网御神州建立了专门的安全管理项目实施队伍，在 2 年的工作中成功实施了大量安全管理项目，并承担了多个安全管理平台的运行和维护工作，积累了丰富的实施和运维经验。

9 网御神州运营安全保障平台

SecFox-SIM 与网御神州的其他 SecFox 安全管理类产品和组件基于相同的安全管理平台架构，可以很容易地形成一个完整的 SecFox 安全管理解决方案。将 SecFox-SIM 与 SecFox-SNI（Security Network Inspector）安全网络监控系统，以及 SecFox-OMS（Security Operation Management System）安全运维管理系统集成到一起，可以形成一个集 IT 资源管理、安全信息管理和运维管理于一体的全面运营安全保障平台（Platform for Operation Security Assurance，简称 POSA）。

网御神州 POSA 平台以客户 IT 计算环境为保护对象，不仅提供了一套以安全监控、安全分析和安全决策循环为流程的安全管理支撑系统，同时紧扣人、技术和流程三个安全管理的核心要素。并且，基于网御神州对等级保护制度、ISO27000 等标准的深刻理解，使得 POSA 同时成为一个全面基于安全标准的安全合规管理平台。最后，在安全服务的支持下，真正将以 SecFox 安全管理为核心的 POSA 平台运转起来。

10 典型应用场景

10.1 某电信运营服务商

10.1.1面临问题

案例用户是国家授权进行国际互联网业务的十大互联单位之一，拥有独立的广域骨干网络，建设规模庞大。

由于运营系统直接对外提供互联网接入功能，因此时刻都要面对互联网上可能出现的各种安全问题。安全事件种类复杂多变，仅靠简单的日志查看来分析安全状况基本上得不到令人满意的结果。

此外，运营商的设备大多是高端设备，不仅拥有互为备份的高性能骨干路由器，千兆及防火墙，核心交换机等基础设施，还拥有提供诸如 VoIP 等各种服务的专用接入设备在同时运营。因此每时每刻各种不同类型的设备都可能有大量事件产生。如何从海量事件中提取出主要的运行状况趋势和发掘潜在影响，成为运营商必须关注的问题。

10.1.2解决方案

采用 SecFox-SIM 安全信息管理系统为运营商搭建了集中监控，实时分析各种来源事件的基础平台，使运营商能够实时掌控各种基础设施和应用的安全状况。

SecFox-SIM 作为集中安全事件分析的管控中心，为大型运营商提供了灵活而坚固的管控系统。运营商可以为不同的网络区域部署单独的 SecFox-SIM 管控系统，各个单独运行的管控系统之间可以方便地设置级联关系，从而形成具有良好层次结构的一体化集中管控体系。

SecFox-SIM 可以分析种类众多的原始安全事件，涉及的范围涵盖主要的网络设备、安全设备、主机服务器系统以及各种应用。SecFox-SIM 可以迅速地将安全事件流划分为各种重要的场景，让管理员同时关注网络中出现的各种状况。对于运营商来说，可以设定几种不同的场景，通过统一的视图，实时监控比如被火墙阻断的事件场景和非法授权登陆访问的事件场景，并根据他们的趋势变化做出判断。

SecFox-SIM 具有很强的事件处理能力，可以轻松分析每秒数千条的安全事件，通过采用级联和分布式采集的方式，能够满足大型运营商对安全事件分析处理的需求。

SecFox-SIM 同时为运营商提供了完备的事件备份存储机制，并采用了最先进的技术手段以确保这些安全事件可以作为审计数据的依据，并为运营商提供解决法律法规依从性要求的技术手段。

10.2 中小企业安全事件管理

10.2.1面临问题

中小企业的高端设备虽然不是非常多，但各种系统与基础设备往往关系紧密，业务系统对设备的复用度比较高。因此准确定位安全事件的根源需要花费比较大的精力。

中小企业的计算机管理人员负责的事情很多，很少专门针对安全管理制定单独的监控措施。有很多需要安全专家专职的岗位往往都由计算机的维护管理人员兼任。这对中小企业的安全管理而言是一个极大的挑战。

10.2.2解决方案

SecFox-SIM 安全管理信息系统提供了统一的事件采集机制和集中的安全事件监控界面，让管理员花费很少的精力就能洞察整个企业中各种设备和应用的安全运行状况。

SecFox-SIM 内置了大量的安全规则相关的领域知识，让管理员迅速达到安全专家的分析水平。通过使用内置的安全规则，就可以发现并解决相关的安全问题。

SecFox-SIM 采用了一站式的安装方式，并且操作使用的学习曲线很低，使得管理人员能够非常容易的展开工作。