

SecFox-LAS

日志审计系统

SecFox-LAS (Log Audit and Analysis System) 日志审计系统是一个全面的、面向业务的、集中的安全审计平台，能够收集来自IT资源环境中各种设备和应用的安全日志，并进行存储、监控、分析、报警、响应和报告。

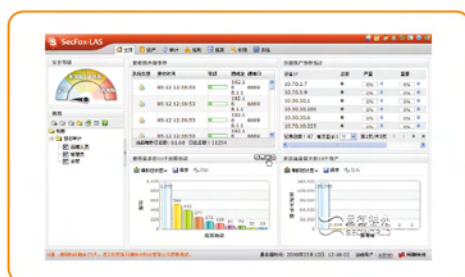
► 需求分析

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。一方面，网络中的各种网络设备、安全设备、主机、应用和业务系统在工作中都产生了大量的安全事件和日志，却没有统一的进行管理，使得各个系统之间缺乏协同，整体安全无法得到保障。另一方面，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，也对当前日志审计提出了严峻的挑战。

► 安全日志审计——企业全网综合安全审计解决之道

■ 统一日志监控

SecFox-LAS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（日志）进行统一监控。



统一日志监控门户



■ 日志归一化与实时关联分析

SecFox-LAS收集并归一化企业和组织中的所有安全日志和告警信息，然后通过智能事件关联分析引擎，帮助安全管理员实时进行日志分析，迅速识别安全事故，从而及时做出响应。

日志归一化和实时关联分析是SecFox-LAS的核心，也是该系统区别于传统安全日志审计系统的最关键特征。SecFox-LAS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，拥有完全自主知识产权。

■ 集中日志存储

SecFox-LAS可以将采集来的所有日志、事件和告警信息统一存储起来，建立一个企业和组织的集中日志存储系统，实现了国家标准和法律法规中对于日志存储的强制性要求，降低了日志分散存储的管理成本，提高了日志管理的可靠性，消除了本地日志存储情况下可能被抹掉的危险，也为日后出现安全事故的时候增加了一个追查取证的信息来源和依据。

■ 灵活的部署方式

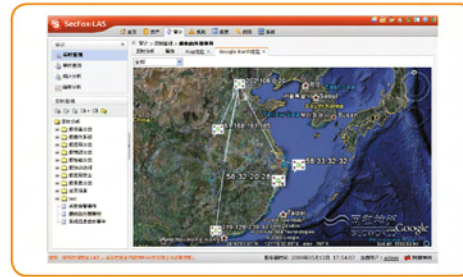
SecFox-LAS的部署方式十分灵活，对网络环境的适应性极强，既能够支持单一的中小型网络，也支持跨区域、分级分层、物理/逻辑隔离的大规模网络。产品分为软件形态和硬件形态两种，用户可以根据自身需要选择。系统部署对现有网络结构无影响，支持多端口日志采集，支持通过硬件探针采集日志，支持级联部署。

SecFox-LAS支持通过Syslog、SNMP、NetFlow、ODBC/JDBC、OPSEC LEA、内部私有TCP/UDP等网络协议，以直接或者借助软件日志采集器和硬件网络探针的方式收集日志信息。

■ 可视化日志分析

SecFox-LAS具备强大的事件可视化能力，使数据信息更加直观和形象化。事件可视化不是简单的柱图、饼图、曲线图等统计趋势图表的展示，必须反映出大量事件之间的相互作用关系。SecFox-LAS的可视化功能包括：

- 1) 事件全球定位系统
- 2) 主动事件图
- 3) 事件行为分析
- 4) 动态雷达图



地图定位



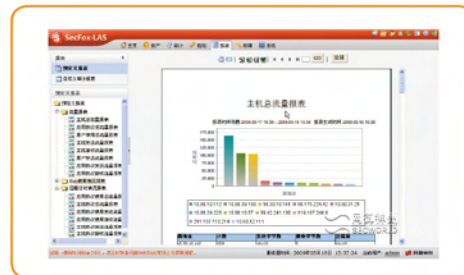
行为分析图



事件攻击图

■ 报表报告

SecFox-LAS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，提供打印、导出以及邮件送达等服务，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。用户可以自定义报表。



报表

► 功能列表

功能点	说明	
产品形态	分为软件型和硬件型	
管理范围	能够对企业 and 组织的IT资源中构成业务信息系统的各种网络设备、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、告警等安全信息进行全面的审计	
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，用户可以快速导航到系统的各个功能界面，可以看到当前企业和组织的整体安全等级	
资产管理	按照设备资产重要程度和管理域的方式组织设备资产，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设备资产的信息，并对资产关键度赋值	
事件采集和归一化	通过 SNMP、Syslog、数据库、文件、NetFlow、OPSEC LEA、软件日志采集器、硬件探针等多种方式完成数据收集功能。收集后进行字段和安全等级的归一化处理，并保留原始日志	
事件监视、分析和响应	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进行实时监视、查询、分析以及历史分析和事件统计，从而快速识别安全事故。所有的事件分析都以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，提高分析工作的效率。在识别出安全事故后，自动告警，监控管理人员能够及时进行响应处理，响应方式包括发送邮件、SNMP Trap、执行程序脚本，等等	
趋势分析	通过采集NetFlow数据流或者防火网的网络流量日志，对最近一段时间的网络流量或者网络连接数进行统计，并描绘趋势曲线。通过某个IP地址的流量趋势分析获悉该IP地址的访问流量模型，并发现异常流量和行为	
事件追踪和可视化	用户可以对关联事件进行追溯；可以通过事件调查工具对某条感兴趣的日志中的源IP地址、目的IP地址、或者目的端口进行相关性日志检索；可以对历史事件进行行为分析；可以对重要事件分配黑白名单。系统具备多种可视化功能将事件展示出来	
规则管理	在事件关联分析引擎的驱动下，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	
报表管理	提供丰富的报表管理功能。根据时间、数据类型等生成报表，提供打印、导出以及邮件送达等服务；直观地为管理员提供决策和分析的数据基础，帮助管理员掌握网络及业务系统的状况。报表可以保存为html、excel、文本、pdf等多种格式	
权限管理	采用基于角色的权限管理机制，通过角色定义支持多用户访问。角色能够从设备和功能两个维度进行定义，从而达到对每一台设备、每一项功能进行操作的控制粒度	
系统配置	系统自身的健康状况监控，以及对系统的各项配置工作	
性能指标	事件采集性能	30000EPS (事件数每秒)
	事件关联分析性能	6000EPS (事件数每秒)
	事件存储性能	事件存储量仅取决于系统所用存储空间大小
	浏览器并发连接数	50个 (即同一时刻可以有50个用户使用本系统)
其他	用户使用模式	无需安装客户端，使用IE浏览器访问管理中心
	部署方式	可以独立部署，也可以级联部署