SecFox-SIM安全信息管理系统

当前企业和组织面临的挑战

为了不断应对来自内部和外部的安全挑战，企业和组织先后部署了大量的安全系统，但却造成了安全防御的孤岛，系统之间缺乏协同，各种安全系统产生了大量告警、日志和事件，出现信息过载的现象，造成很多误报和漏报，导致问题不能及时发现和处理。此外，企业和组织正面临不断增大的内控和信息系统审计的压力，要求增强业务持续性的呼声不断提高，这些都促成了面向全网的安全信息集中管理平台的出现。

SecFox-SIM——安全集中管理的基石

统一安全事件监控、态势感知

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、警报等信息汇集到管理中心，实现海量信息的集中分析，进行统一的安全事态监控和态势感知，消除了安全防御的孤岛。

统一安全监控给客户的显性化体验就是态势感知（Situation Awareness）。通过态势感知，实现对全网综合安全的总体把控。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。

实时安全事件关联分析

SecFox-SIM能够实时地对采集到的不同类型的信息进行关联分析、最大程度地消除误报和错报、找出漏报，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。通过事件关联分析，客户可以实现从单点被动防御到全面主动防御的转变。

SecFox-SIM具有国内绝对领先的事件关联分析核心技术，申请了多项专利技术。基于SMART™技术的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。

便捷、高效、可视化的事件分析

SecFox-SIM为了提升管理效率，提供了大量简洁的界面，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。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。

事件可视化是指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。

快速响应与协同防御

系统能够自动地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告警和响应。告警方式包括电话响铃、邮件、短信、电脑语音、SNMP Trap告警的方式通知管理人员。响应方式包括：自动执行预定义脚本，自动将事件属性作为参数传递给特定命令行程序，自动派发工单，自动将事件送入案例库和黑白名单列表。特别的，SecFox-SIM支持与第三方网络和安全设备联动，从而实现安全事件管理的闭环。

符合等级保护要求的安全合规审计

SecFox-SIM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。

IT计算环境整体安全状况报表和报告

SecFox-SIM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，产生报表。报表可以调度，定期运行，自动邮件投递。报表导出为Excel、Word、PDF等格式，可以直接打印，邮件发送。

全面监控IT网络中所有设备和系统的安全事件，用户可以自由切换监控频道

对于IT网络中发现的攻击事件进行实时地图定位

全面监控IT网络中所有设备和系统的安全事件，并支持多种不同的视角

对于IT网络中的大量安全事件进行可视化展示，提高安全威胁定位的准确性和直观性