某电信运营商 SIM 案例介绍

SOC 事业部

网御神州科技有限公司

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。

2 案例解决方案

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。

3 为客户带来的价值

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：

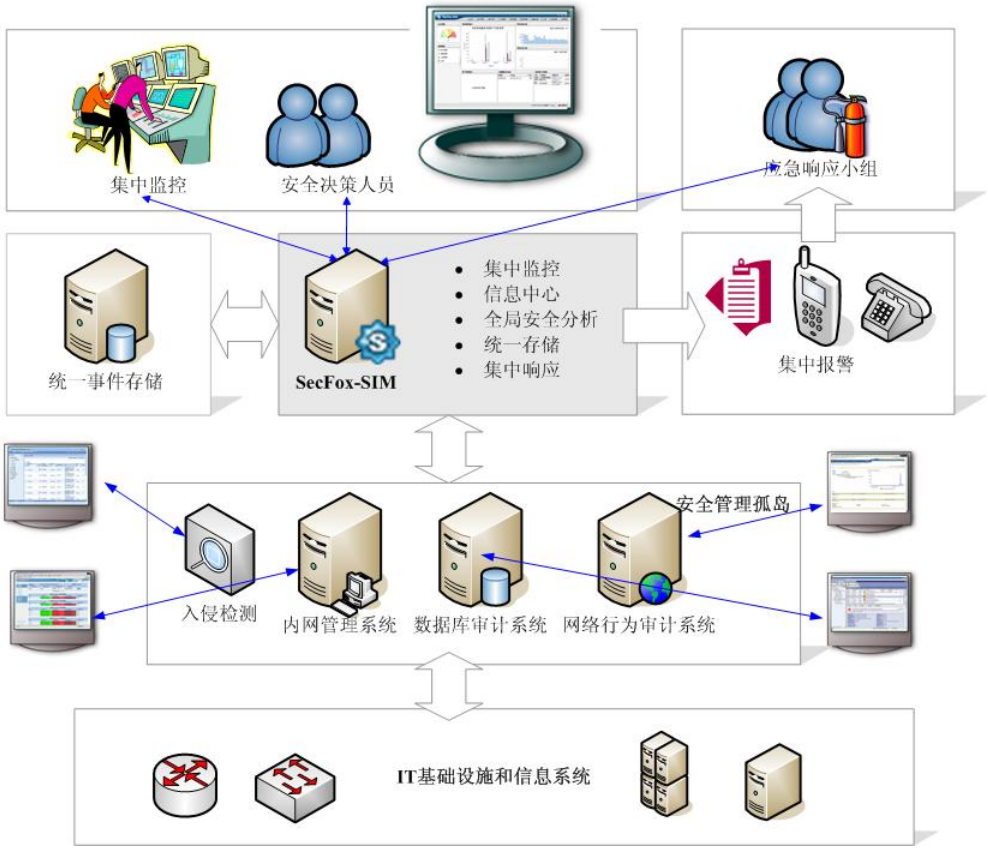
- 随时可以全局掌握企业和组织的安全总体状况，为领导层进行安全建设决策提供依据
- 从整体上提升了企业和组织的安全防护水平
- 通过对 SecFox-SIM 的投资发挥出原有各种安全设施的投资的潜在价值，从而使得企业和组织的成本效益最大化，降低总拥有成本（TCO），提升安全设施的投资回报率（ROI）

4 SecFox-SIM产品优势

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，在多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。

欲获取更多信息，请即联系网御神州科技（北京）有限公司
全国统一热线服务电话：010-87002000（7×24 小时）
E-mail：service@legendsec.com（5×8 小时）
网站地址：www.legendsec.com
网神安全管理博客地址：http://blog.sina.com.cn/legendsec
传真：010-62972896
通信地址：北京市海淀区上地信息产业基地开拓路 7 号先锋大厦 2 段 1 号
邮政编码：100085