



安全信息管理的领导者

Cisco SIMS **安全信息管理**

Cisco SIMS：安全信息管理

《Cisco SIMS 安全信息管理》一文介绍了 Cisco SIMS v3.1 可如何引导您实现成功的网络防御。

安全信息管理（SIM）

Cisco SIMS 系统使企业能够控制其企业安全性。利用 SIM 系统，管理员能够妥善控制为了解网络攻击所必须分析的极大量数据。通过对实时事件数据进行规范化、汇聚和关联并以易于解释和处理的形式来表示这一数据，管理员就能迅速识别并制止安全威胁。通过利用 SIM 系统来进行深入报告和歷史分析，企业就能更容易地对风险进行评估并作出决策来避免今后可能发生的攻击。SIM 产品使企业能充分利用现有安全设备所产生的信息以及应用数据，而无需聘请更多员工，因此可降低总拥有成本并提高投资回报率。

- 可提供企业安全大环境的实时可视化视图和分析，使企业能轻松了解各种风险并采取明智决策
- 可从极大量不同的安全数据中迅速识别出关键事件，从而使管理员能立刻作出响应并避免攻击对网络产生影响
- 可提供单一的 Java 控制台，使企业能有效地监控和管理其不断扩大的安全系统，而无需配备更多专门人员
- 可提供一个全集成的事事故响应系统，进而可提供集成的知识库和集成的流程来自始至终地管理事故个案



图 1
安全信息管理 (SIM) 可帮助机构识别、分析和快速应对针对关键任务系统和信息的潜在威胁



商业驱动因素

企业经营风险

几乎所有的企业和机构都需要保证其网络基础设施能得到保护，免受内部和外部的威胁并避免可能导致的重大损失。近几个月来，很多企业都经历了 Slammer and Blaster 等一系列各不相同的高风险威胁——给很多环境造成了极大破坏。

企业绩效风险

从本质上说，安全设备会产生大量的详细数据。如果没有行之有效的管理工具，那么我们就几乎不可能识别和筛选这些数据，获得关于各类安全活动的标准化和统一化的视图。这一局限性降低了不同安全要素所能提供的有用性和价值。SIM 系统可提供关于安全基础设施是否正按计划工作以及企业安全投资是否实现了最大成效的文档化和可理解的佐证。

法规要求

目前，美国已经颁布了 40 多项新法规，为很多不同的纵向行业和政府部门提供了安全和保密性指

导方针。强制要求对安全信息的监控和管理采用标准的法规包括萨班斯-奥克斯利法、FISMA法、健康保险转移与责任义务法(HIPAA)以及格拉姆-利奇-布利利法(GLBA)等等——所有这些法律都为加强责任和义务、基准数据收集、各类标准以及(毋庸赘言)市场对有效的端到端安全管理解决方案的更大需求等铺平了道路。

保护声誉、诚信和品牌

客户需要相信企业采取了一切措施来保护他们的个人和财务信息。参与合作伙伴关系和战略联盟的企业则希望确保其专有信息的安全。一个牢固可靠的安全基础设施再配以SIM系统就能建立可为客户提供这一信心的环境。

“在部署SIMS之前，我们只能算是反应性而不是前瞻性的公司。现在，我们总是能提前一步并坚信我们有着最新的安全信息管理。”

——俄亥俄储蓄银行 IT 基础设施与安全副总裁，Matt Speare

认真勤勉与最佳惯例

与IT安全相关的新的标准和政策陆续出台，并定义了什么是“良好商业惯例”和“认真勤勉的安全工作”。SIMS解决方案是十分必要的，因为它可为按照互联网安全环境中的最佳惯例而有效管理安全系统的目的提供整合信息。

走在安全管理前沿

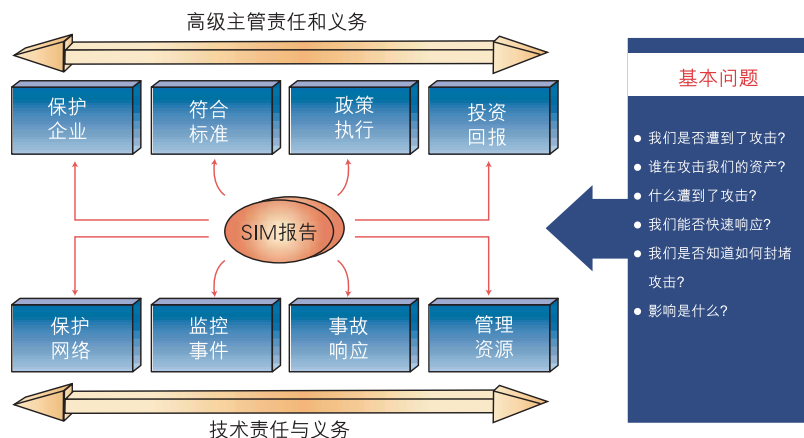
开发Cisco SIMS系统的目的是要填补IT安全体系结构中的一个空白。利用Cisco SIMS系统，安全操作员能够通过分析工具来定量分析企业风险并面向未来快速实施安全政策，从而消除安全漏洞。Cisco SIMS公司的SIM平台可实现设备间关系的分析，进而提供关于所有安全事件的广泛和统一的视图。Cisco SIMS的强大功能可实现对安全告警的实时(或历史)分析并可通过一整套负责执行必要汇聚工作、进一步过滤和语法分析技术的综合性软件方法对告警进行关联。

Cisco SIMS 的关键特性

Cisco SIMS 软件解决方案提供了安全分析员以前所无法获得的强大的安全智能功能，包括：

- 统一的任何时间/任何地点管理控制台
- 广泛的设备和应用程序支持
- 实时关联
- 用户协作区
- 全集成事故响应管理系统
- 直观的更新和系统健康管理
- 高性能分布式体系结构
- 签名管理功能
- 资产——风险漏洞评分

图 2

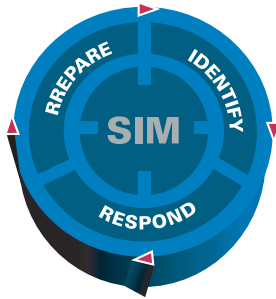


Cisco SIMS v3.1 概述

Cisco SIMS v3.1 是一个安全信息管理 (SIM) 应用程序，它可实现与多种不同安全产品之间的异构机互操作性，因此可使网络管理人员集中监控、管理和监督企业网络的安全性。

Cisco SIMS 公司让其合作伙伴也参与到了确保合格而稳定的异构机互操作性的工作中，它所秉承的以客户为中心的宗旨甚至超出了客户支持的范围。Cisco SIMS 公司是唯一可实现与 Cisco、Check Point、Nokia、Netscreen、Sourcefire、Foundstone、Tipping Point 和 Network Associates 等主要安全供应商的异构机互操作性的 SIM 厂家。

Cisco SIMS v3.1 通过已经建立的准备、识别和响应等安全流程可实现有效的安全信息管理。Cisco SIMS 可在较高水平上通过规范化和汇聚来收集信息并处理信息。



准备

- **规范化**—— Cisco SIMS 代理可利用来自不同设备的本机协议来收集安全事件数据，将这些事件关联为警报 ID 然后使用安全的 TCP 在网络上传输这些信息。多个代理可对工作量进行平衡，从而实现最高性能并支持分布式企业网络。
- **汇聚**—— Cisco SIMS 引擎可对这些数据进行进一步处理，进而确定事故类型和发生的风险。重复性报告会被删除，所产生的事故会得到评分，威胁水平随之得到确定。

完成数据准备后，Cisco SIMS 随之可根据这一数据形成智能，应用实时多维关联，用关键企业资产数据和相关漏洞信息进行确证，最终推出事故响应程序。

识别

实时关联——系统会测量各类事件并进行相互对比，以确定事故可能性。作为其资产风险评估计算的一部分，Cisco SIMS 别出心裁地将基于规则的关联与统计关联的功能相结合，因此可按照具体模式、漏洞和异常情况等各类威胁进行分析，从而提供更快速和更有效的响应信息。

响应

事故响应管理——与 Cisco SIMS 紧密集成的是一套事故响应子系统，它可在安全——知识型环境中统一进行与事件相关的个案管理活动。

特性

强大的安全信息体系结构

图 3
强大的安全信息
体系结构



Cisco SIMS v3.1 采用了一个可分布性和可扩展性较高的体系结构，其中采用了不同组件用于事件捕捉、过滤、汇聚、数据存储、实时的基于规则的和统计的关联以及直观的进行表示。其安装、快速部署以及远程代理配置等只需最少的资源即可完成。这就是说，无论您的机构的网络扩展到多大的规模，Cisco SIMS 系统的功能都能满足您的需要。

Cisco SIMS v3.1 采用了行业主流关系数据库管理系统 Oracle 9i，用于其数据信息库并将该系统与本产品捆绑起来。其中还包括了数据库自我管理工具，可杜绝大多数数据库管理和配置问题。Cisco SIMS 还提供了一些自动化脚本来管理几乎所有的安装以及备份、恢复和索引管理等数据库管理工作——所有这些都可以通过中央管理控制台来访问。系统可安排数据库存档/清理任务的时间，能针对任何设备类型在一天、一周或一月的任何时间自动执行或在任何规定时间内对设备自动执行。

Cisco SIMS 数据库安装针对 OLTP 和 DSS 等处理方法进行了优化，因为多个 Cisco SIMS 引擎可以极高速度插入数据，而法律和分析工具可在整个数据库上同时执行复杂的数据挖掘查询。

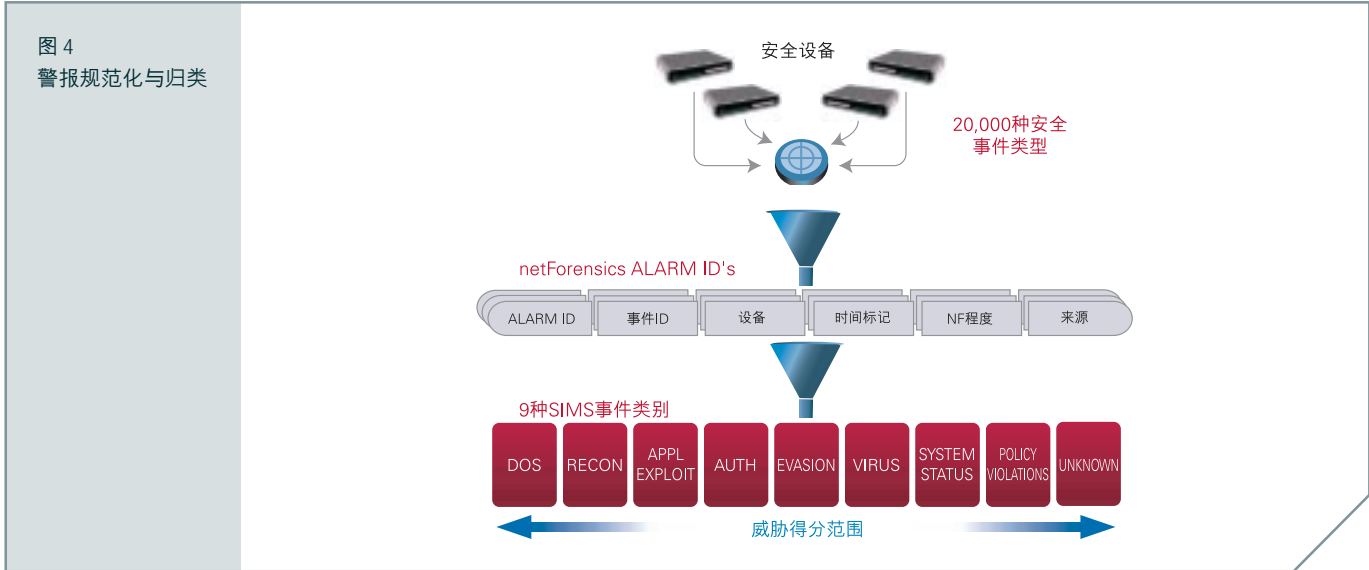
Cisco SIMS 数据库可被设置为配备 Oracle Real Application Cluster 的群集模式，因此规模扩展后可超过单一服务器配置。

所有 Cisco SIMS 组件都包括内置的诊断功能。诊断工具分为两大类：主动工具和被动工具。主动工具能直接访问 Cisco SIMS 组件，而被动工具则可关联 Cisco SIMS 调试消息。诊断工具可使管理员从单一计算机对任何 Cisco SIMS 组件进行远程调试。

Cisco SIMS 系统健康监控器可监控数据库的健康情况并可在数据库或某些表格超出预定义门限时提供实时的告警（含页面）。

提供商可为所有注册 Cisco SIMS 组件提供主数据服务。这些服务包括报告、监督、配置、补丁软件管理以及主数据更改通知等服务。提供商还负责为所有组件的补丁软件、热修复和 XML 配置等提供适当的下载和更新。提供商驻留在与 Cisco SIMS 数据库相同的服务器上，它是采用简单对象访问协议(SOAP)标准而实施的一个客户机——服务器系统。

警报规范化与归类



Cisco SIMS 安全管理

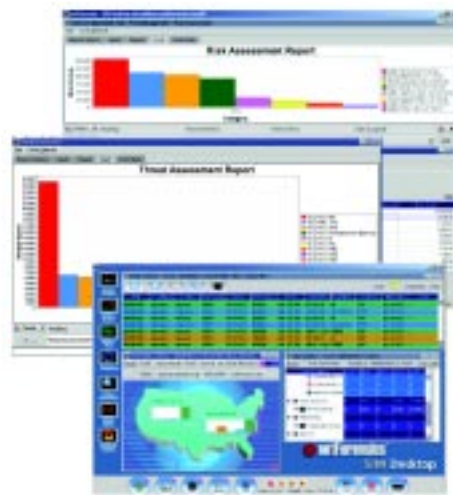
Cisco SIMS 警报规范化可提高性能并简化呈现给用户的信息。Cisco SIMS 代理可根据最初的设备警报对具体设备警报进行规范化并将其整合为更高级的类别。Cisco SIMS 代理可将 20,000 多种不同的设备警报缩减到不超过 100 种规范化的 Cisco SIMS 警报。

这些设备警报随后被进一步规范化并缩减到以下 9 种 Cisco SIMS 安全事故类别，从而更快速地识别当前威胁的性质（按字母顺序排列）：

- 访问 / 身份验证 / 授权
- 应用程序盗用
- 配置 / 系统状态
- 拒绝服务
- 躲避
- 违反政策
- 侦察企图
- 未知 / 可疑
- 病毒 / 特洛伊木马

实时关联

图 5
实时关联



风险管理是一个评价对整个企业的威胁并确保这些威胁所构成的风险在可接受程度内的连续过程——甚至也包括那些尚属未知的威胁。SANS 研究所指出，风险是由威胁、价值和漏洞组成的。威胁是那些对网络资产可能构成危险的活动。网络资产的价值以及驻留在网络中的信息的价值本质上都是主观的因此会随时间而改变。它通常是由系统在公司中所发挥的作用以及该系统所存储或处理的数据来限定的。漏洞系指可导致威胁造成破坏的系统和软件薄弱环节。

Cisco SIMS 采用能计算威胁和风险分数并将这些统计数据关联到针对该环境而定制的基于规则的计算结果中的专用公式为企业提供了威胁和风险评估。Cisco SIMS 系统的评分功能可连续处理低水平攻击，以识别出表示高风险威胁的模式。其独特的评分算法可通过采用高级关联技术而检测出不同类型的威胁和攻击，可使企业识别出杂音、减少假肯定次数并迅速识别出真正的威胁，从而加快响应速度。

全集成事故响应系统

图 6
全集成事故响应系统



建立极其高效的事故响应流程是至关重要的，因为这可以限制安全事故所造成的破坏并提高安全团队和基础设施投资的效率。有了 Cisco SIMS 安全信息管理 (SIM) 解决方案及其事故响应 (IR) 模块，企业就能实现一箭双雕的目的——既可实现强大的安全事件管理又可实现牢固可靠的事故响应流程。

与基础 SIM 产品完全集成的 Cisco SIMS 事故响应系统对任何事故响应计划都构成了完美补充。其中包括了解决哪怕是最复杂的安全事故所必须的数据和程序信息。有了一个能同时实现事件管理和事故处理的控制点，操作员和分析员就能在问题发生时轻松监控各类事件并跟踪各类事故。Cisco SIMS IR 的主要目的是将这一安全事件数据收集并组织成某种逻辑形式，执行适当的安全响应 workflow，从而实现快速和有效的事故响应。

借助 IR 知识库，用户就能获得进一步的决策支持来帮助他们解决多种不同的安全事故。此外，该系统还有助于响应团队不同成员之间的实时协作，使之能尽快交换意见并作出决策。

强大而灵活的用户工作空间——SIM 桌面

SIM 桌面是一个安全分析员 Java 应用程序，它可提供对 Cisco SIMS 系统中现有的和可用的所有实时和历史监控、工具和特性的访问。SIM 桌面是一个“任何时间/任何地方”图形化用户环境，可实现对网络中发生的安全事件的实时监控和分析。

安全的通信

Cisco SIMS 采用了 TCP 上的 XML 来实现多个不同组件之间的通信。XML 允许使用简单“标记”文本在 Cisco SIMS 基础设施中进行通信。系统采用高度优化的 XML 将安全事件转换成 XML 格式并对数据进行规范化。Cisco SIMS 通信架构提供了一种检查机制，可杜绝消息遗漏并确保可靠的数据传输。

Cisco SIMS v3.1 包括以下新增的安全和通信特性：

- 在所有组件之间进行可选的由 SSL/TLS —— 确保安全的通信
- Cisco SIMS 引擎可利用数字证书对所有用户类 Cisco SIMS 代理进行身份验证
- 增强的用户和管理界面可采用基于 SSL 的身份验证
- 补丁软件的自动管理 —— Cisco SIMS 组件可从中央服务器中自动下载补丁软件
- 可在所有 Cisco SIMS 组件之间实现统一的 XML 配置





思科系统（中国）网络技术有限公司

北京

北京市东城区东长安街1号东方广场
东方经贸城东一办公楼19~21层
邮编: 100738
电话: (8610)65267777
传真: (8610)85181881

上海

上海市淮海中路222号
力宝广场32~33层
邮编: 200021
电话: (8621)33104777
传真: (8621)53966750

广州

广州市天河北路233号
中信广场43楼
邮编: 510620
电话: (8620)87007000
传真: (8620)38770077

成都

成都市顺城大街308号
冠城广场23层
邮编: 610017
电话: (8628)86758000
传真: (8628)86528999

如需了解思科公司的更多信息, 请浏览<http://www.cisco.com/cn>

思科系统（中国）网络技术有限公司版权所有。

2004 ©思科系统公司版权所有。该版权和其它所有权利均由思科系统公司拥有并保留。Cisco, Cisco IOS, Cisco IOS标识, Cisco Systems, Cisco Systems标识, Cisco Systems Cisco Press标识等均为思科系统公司或其在美国和其他国家的附属机构的注册商标。这份文档中所提到的所有其它品牌, 名称或商标均为其各自所有人的财产。合作伙伴一词的使用并不意味着在思科和任何其他公司之间存在合伙经营的关系。