

CiscoWorks 安全信息管理解决方案

问：什么是 CiscoWorks 安全信息管理解决方案？

答：CiscoWorks 安全信息管理解决方案（CiscoWorks SIMS）是一个可以从整个企业搜集和分析安全事件信息的解决方案，它让您可以及时地检测到安全事件，并采取相应的措施。利用 CiscoWorks SIMS，您可以在不增加您现有的安全人员的人数的情况下，管理您的不断扩充的安全设备基础设施。

CiscoWorks SIMS 可以提供：

- 对 SAFE 和多厂商环境的全面事件管理
- 能发现已知和未知威胁的实时事件关联
- 用于快速、直观的安全监控的高级虚拟化功能
- 有助于了解企业中任何特定资产的总体危险性的集成化风险评估功能
- 针对所有级别的安全运营和管理的全面报告和预测功能

CiscoWorks SIMS 可以利用曾获大奖的 netForensics v3.1 软件提供这些功能。netForensics v3.1 可以自动执行今天的很多安全分析和报告任务。利用实时的深入分析功能、先进的搜索功能、虚拟化和报告功能，netForensics v.3.1 让您可以从任何一个 Web 浏览器访问关键的安全信息。netForensics v.3.1 的高度可扩展的分布式架构使得 CiscoWorks SIMS 成为了一个高性能的安全解决方案，适用于各种规模的企业。

问：什么是安全信息管理？

答：安全信息管理（SIM）技术可以通过四个不同的阶段，搜集、分析和关联来自于整个企业的安全事件信息：规范化、汇总、关联和虚拟化。在规范化和汇总阶段，CiscoWorks SIMS 会从几乎所有的入侵检测系统（IDS）、防火墙、操作系统、应用和防病毒系统搜集安全事件，并将其转换成通用的、便于理解的可扩展标记语言（XML）格式。经过格式化的记录将通过两个功能强大的关联引擎进行关联。这些关键引擎采用了基于统计和可选规则的关联技术。最后，netForensics v3.1 将利用一个图形化、功能强大、直观友好、基于 Java 的界面，在一个集中的实时控制台上显示关联结果。

问：思科和 netForensics 之间是什么关系？

答：长期以来，思科和 netForensics 之间一直保持着密切的合作关系，其中包括思科对 netForensics 的投资，以及联合进行工程设计、技术支持、销售、市场开发和培训。

问：CiscoWorks SIMS 是如何销售的？

答：客户可以选择下列方式，订购 CiscoWorks SIMS（包括 netForensics v3.1）：

1. 基于 Solaris 的起步工具包（包括对于监控 30 个设备的使用许可，1 个主引擎，1 个分布式引擎，1 个 Oracle 数据库，以及代理软件）
2. 基于 Linux 的起步工具包（包括对于监控 30 个设备的使用许可，1 个主引擎，1 个分布式引擎，1 个 Oracle 数据库，以及代理软件）
3. 对于监控 20 个附加设备的使用许可
4. 对于监控 1 个附加引擎的使用许可
5. 对于监控 1 个附加的、基于 Solaris 的 Oracle 数据库的使用许可
6. 对于监控 1 个附加的、基于 Linux 的 Oracle 数据库的使用许可

它们的产品编号都列在 CiscoWorks SIMS 产品简介中。思科将来还将提供一个预装在使用 Linux 的硬件服务器上的 CiscoWorks SIMS 装置。请保持对 Cisco.com 上的 CiscoWorks SIMS 产品简介的关注，以便在这种订购方式将来推出时及时获知。

CiscoWorks 安全信息管理解决方案

问：什么是规范化、汇总、关联和虚拟化？

答：规范化：今天的周边安全设备可以生成超过 20,000 种不同类型的事件。通过 netForensics v3.1 代理技术，这些事件类型可以被对应到 100 种基于 XML 的 netForensics 警报 ID——从而大幅度减轻安全数据分析的负担。

汇总：事件汇总是一个消除重复事件的过程，它可以将大量的事件数据减少到可以管理的范围之内。这对于 ping sweep 或者端口扫描等事件尤为有用，因为防火墙设备会重复报告类似的事件。事件汇总还可用于消除来自于多个 IDS 设备的重复警报。

关联：经过格式化的记录将利用两种不同、但是互相补充的事件关联方式进行关联——第一个是一种统计关联机制，它依靠事件类别和威胁等级来确定异常情况的潜在威胁。第二个是一种基于可选规则的关联功能。它可以通过为接收到的每个事件调用“时间感知型”安全策略规则，将“误报”安全警报和潜在的重要安全事件区分开。

利用统计关联，异常的安全事件将被按照资产或者资产群组归入不同的类别。对于每个资产，CiscoWorks SIMS 将通过把事件的严重程度和资产的价值结合到一起，不停地计算威胁指数，以确定安全事件的总体潜在威胁。CiscoWorks SIMS 的主要优点在于能够发现那些被一个基于规则的关联系统所忽视的异常情况。

这两种关联技术都非常准确，而且部署方法非常简单明了。每种技术从一个不同的角度处理事件关联，因而可以更加全面地防止企业受到多种潜在的安全事件的影响。netForensics v3.1 提供了一个全面的关联解决方案，它是整个 SIM 功能套件的一个不可或缺的组成部分。

虚拟化：利用 netForensics v3.1，安全人员可以利用一个实时的、基于 Java 的控制台集中检测整个企业的安全事件，并及时地采取对策——在安全威胁造成损失之前消除它们。

问：netForensics v3.1 架构具体包括哪些组件？

答：netForensics v3.1 为全面的 SIM 提供了一种创新的架构。该架构的组件包括：

- netForensics v3.1 代理——从不同的、由多个厂商提供的安全技术和应用搜集数据；将厂商特有的格式转换为标准的 XML 数据，进而将这些信息转发到 netForensics v3.1 引擎。
- netForensics v3.1 引擎——搜集、过滤、分析和分类由代理提供的标准化数据；利用多种并行引擎功能，netForensics v3.1 可以为任何规模的网络或者增长要求确保无限的可扩展运营，并通过这种分布式架构添加本身可以支持增长的运营方式。
- Forensics 数据仓库——经过整合的、规范化的历史数据将自动地在 netForensics v3.1 数据仓库中进行维护；除了缺省的 netForensics v3.1 报告和分析功能以外，客户还可以利用现有的、业界标准的报告、查询和业务智能工具，分析和报告这些保存在一个 Oracle 数据库中的数据。这些搜集来的数据对于研究过去发生的问题，发现和跟踪趋势，以及通过探索性运营不断改进安全效率具有非常重要的意义。

问：netForensics v3.1 是否可以取代我们目前采用的安全技术？

答：不。netForensics v3.1 需要与您现有的安全基础设施合作，搜集、分析和关联由今天的安全设备生成的大量安全事件信息。在出现安全漏洞时，netForensics 可以帮助运营商和分析师迅速地确定几乎所有安全威胁的来源。

更加重要的是，netForensics 让企业可以通过提高他们现有安全团队的能力和效率，加强对企业安全管理的控制。在 netForensics 的帮助下，您可以在不增加您的安全人员的人数的情况下，管理您的不断扩充的安全设备基础设施。

问：一些现有的安全技术不是已经能够实时地检测和解决安全问题了吗？

答：今天的很多安全攻击都是针对整个企业的（例如拒绝服务攻击）。客户需要利用其他一些技术来搜集在企业终端发生的安全事件的信息，并对它们进行关联，以确定是否在整个网络基础设施中发生了攻击。netForensics 可以检测那些没有被隔离到某个 IDS 或者防火墙、而是分散到基础设施中的多个系统上的事件。

问：你们真的能够实时地检测和防范所有安全事件吗？

答：因为攻击技术多种多样，潜在的攻击者不计其数，而且安全威胁技术的发展日新月异，所以没有任何一种技术可以检测和防范所有的安全问题。但是，netForensics v3.1 可以为您提供检测为数众多的安全事件所需要的技术优势——远远超过一些独立设备所能检测到的事件。

netForensics 让安全团队可以立即检测到可疑的活动，并进行深入的调查。在大多数情况下，netForensics 将会及时地检测到特定的攻击，从而让操作人员可以采取适当的措施消除威胁，或者最大限度地减少损失。

问：请介绍一下 netForensics v3.1 的界面。

答：利用 netForensics v3.1，一个实时的、基于 Web 的控制台将帮助您集中地检测和响应您的整个企业中发生的安全事件——从而让您可以在安全威胁造成损失之前消除威胁。您的安全团队无需添加人手，就可以更加有效地发现和响应更多的威胁。实时控制台从主引擎接收信息。主引擎可以为多引擎安装提供高级汇总和关联功能，并将实时数据流发送到实时控制台（RTC）。

RTC 完全是用 Java 语言编写的，因而可以在客户端提供非常强大的功能。然而，尽管 RTC 的功能非常丰富，但是它必须与一个专用的 Web 服务器进行互操作，才能执行很多任务。这让 RTC 可以兼具强大性和轻便性。

利用 netForensics v3.1 的虚拟化功能，操作人员、分析师和管理人员可以搜集必要的信息，确定总体安全状况，并在各种攻击对您的企业造成破坏性影响之前消除隐患。netForensics v3.1 提供了一系列直观的实时界面和深入的报告、历史分析功能，有助于了解威胁情况和响应安全攻击，其中包括：

- 面板视图可以提供一个实时的企业级安全趋势视图
- netForensics v3.1 RTC 可以利用实时的关联和深入分析功能，迅速地隔离安全攻击
- SIM 报告可以提供全面的风险和威胁趋势分析

问：思科依靠什么成为这个市场的领导者？

答：尽管在今天的市场中有很多信息安全厂商，但是 CiscoWorks SIMS 是建立在曾获大奖的技术的基础上的。《Network Computing》杂志在去年的 NetWorld + Interop 展会上，向 netForensics 授予了编辑选择奖和完美连接奖。

问：netForensics v3.1 怎样与企业管理解决方案（例如 HP Openview 和 Micromuse）共用？

答：netForensics v3.1 可以将关于安全事件的信息发送到企业管理控制台，其中包括 MicroMuse Netcool 和 HP Openview。netForensics v3.1 可以在设置企业管理安全支持时提供多种选项，并可以自动地在基于管理员定义的规则的帮助台系统中建立故障记录。

netForensics v3.1 完全关注于全面的 SIM。netForensics v3.1 的优势在于它能够理解它所获得的安全信息的意义，并能够提供关于所有安全事件的信息。这些功能让 netForensics v3.1 成为了企业管理解决方案的一个出色的补充产品。通过将 netForensics v3.1 与 MicroMuse Netcool 或 HP OpenView 集成到一起，企业管理人员可以集中精力解决安全问题。

问：netForensics v3.1 支持哪些安全设备？

答：netForensics v3.1 采用了一种完全可扩展的三层架构，可以通过有限的设备支持部署于单个地点，或者全面地部署于某个不断扩展的分布式环境。

它可以提供两种设备支持：

1. 固有集成——固有代理正在被统一地添加到 netForensics v3.1 架构中，其中包括思科设备、Check Point 设备、ISS IDS、Entercept HIDS、思科访问控制列表（ACL）和虚拟专用网（VPN）、Windows NT 和 UNIX 日志，以及 Snort 和 Dragon 传感器。
2. 通用代理集成——netForensics v3.1 的一个关键功能是能够将越来越复杂和多样化的设备、应用和定制数据集集成到它的实时智能引擎和仓库中。netForensics v3.1 可以提供一组业界标准的 XML 工具，整合通用代理，以及在它的架构中集成几乎无限的安全信息。

CiscoWorks 安全信息管理解决方案

netForensics v3.1 的底层架构是安全、可靠、基于 TCP 的 XML。它还附带了一组自助管理工具，从而进一步降低了对于额外的系统和数据库管理的需要。

问：什么是风险评估？

答：风险评估是威胁、危险性和价值的结合体。因为危险性是指让威胁得以发生的安全漏洞，一个资产的危险性可以通过评估它的公开性和曝光性估计得出。资产的公开性可以衡量它成为攻击目标的可能性（对于一个 Web 服务器的访问个数），而它的曝光性可以衡量它的功能（监听网络服务的开放端口个数和特性）。尽管资产的价值是一个主观的概念，但是企业管理人员仍然可以对他们所管理的所有资产的价值进行一个相对的估计。在 netForensics v3.1 中，资产的价值、公开性和曝光性都由管理员明确定义，可以用于量化的安全评估。

问：什么是风险管理？

答：风险管理是评估整个企业面临的威胁和确保这些威胁所带来的挑战处于可以接受的范围内的连续流程。根据 SANS 机构的说法，风险由威胁、价值和危险性构成。威胁是指一些代表了对网络资产的潜在危险的活动。网络资产和它们所包含的信息的价值是一个主观的概念，可能会随时间发生变化。价值通常是由系统在企业中扮演的角色和系统所存储、处理的数据决定。危险性是指让威胁可以造成损失的系统和软件漏洞。

netForensics v3.1 可利用专用的公式为企业提供威胁和风险管理功能。这种公式可以根据事件的 netForensics 严重性系数、资产价值、公开性、曝光性，以及入侵者威胁的系数和频率，计算威胁和风险指数。



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/或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。