安全信息管理

2003 年《计算机世界》荣誉案例研究

安全信息管理可通过管理和应对安全应用程序所产生的极大量告警而自动执行削弱和消除网络威胁的过程。这样企业既能最大限度地降低潜在攻击的风险又能在攻击发生时快速作出响应。

应用

Cisco SIMS是一种安全信息管理产品，设计该产品的目的是要实现与针对企业信息资产的威胁相关的活动的自动化收集、关联和响应。

仅一个防火墙每一天就能产生超过十亿字节的日志数据，而一个 IDS 检测器每天也能产生 500,000 多条消息。鉴于如此之多的信息大部分都是所谓“假肯定”(也就是表示存在敌意活动但实际上却没有)的无关数据，因此必须采用自动化技术来识别极少数表示真正安全威胁的消息并确定其优先级。

更有效的安全自动化的关键就在于 Cisco 公司率先开发的一种软件技术 —— 安全信息管理(SIM)。SIM结合了独特而强大的特性来收集和分析,认真谨慎的企业所必须面对和处理极大量的安全事件数据。Cisco SIMS 可通过自动进行数据整合和分析以及提高其现有安全团队的能力和成效使这些企业能掌控企业安全管理。Cisco SIMS 解决方案已被 150 多个全球 1000 强及政府企业所广泛采纳，可帮助企业实现安全性和快速投资回报(ROI)，并籍此赢得了多项媒体表彰和奖励。

Cisco 公司已申请专利的 SIM 技术可通过四个不同的阶段来收集、分析和关联整合企业中所产生的安全设备信息：这四个阶段分别是规范化、汇聚、关联和可视化。在规范化和汇聚阶段，系统可从几乎所有入侵检测系统、防火墙、操作系统、应用程序以及防病毒系统中收集安全事件并将其转换为简单文本记录。然后可利用两个功能强大的关联引擎，对这些格式化记录进行关联，并可立刻在统一、直观和实时控制台上以图形方式标记出各类威胁和攻击。

优点

在确保企业IT基础设施的安全性方面，今天的企业面临着很多挑战。这些挑战包括如何掌控数量多且复杂性高的安全警报、如何处理太多的假肯定事件、如何最大限度降低潜在攻击的风险以及如何在攻击发生时加快响应速度。

利用现有人力来处理这些问题使得这些挑战变得更加严峻。企业今后将购买的安全技术应该是那些肯定能实现商业效益并能解决与安全运营和有关低效环节等相关的问题的技术。也就是说这些技术的特点应该是投资回报速度快、实施成本低、可轻松分阶段部署以及货真价实。

为保护自己的企业外围，今天的大多数企业都投巨资购置了防火墙、防病毒软件以及IDS。每过一年，这些设备的数量都会大幅增加，并导致安全团队面对他们所必须监控和关联的极大量数据而无所适从。例如华盛顿特区某大型MSSP提供商，他们有一个12人的安全运行团队，负责照管整个企业中的450多台安全设备——也就是每人负责监控超过35台设备。来年，这个MSSP的设备数量会增加到550台以上——也就是每人将负责监控超过45台设备！为适应不断扩大的安全设备基础设施，该MSSP打算在其现有团队中再增加5名安全人员——也就是每年额外人员开支将超过$550K美元/年。

此外，Cisco SIMS解决方案注重于风险管理并把它看作是这样一个持续的过程，即不断评估整个企业中的各类威胁并不断确保这些威胁所造成的风险维持在可接受的限度内。根据SANS研究所的标准，风险是由威胁、价值和漏洞构成的。威胁指的是那些对网络资产构成可能危险的活动。网络资产的价值以及驻留在网络中的信息本质上都是主观的并可随时间而改变。它一般是根据系统在公司中所发挥的作用以及系统所存储或处理的数据来定义的。漏洞指的是那些容许威胁造成破坏或损失的系统和软件薄弱环节。根据这一定义，Cisco SIMS解决方案针对威胁和风险采用了系统化的专有分析技术，专注于分析据信对企业是至关重要的各类公司数据。例如，虽然说二者都重要，但在医疗保健企业中，病例数据也许应获得比电子邮件服务器更高的优先级而得到保护，也应获得更高的风险评分乃至更高的响应优先级。

采用传统的安全分析方法，安全操作员可监控整个企业中的系统活动数据来揭示网络攻击或漏洞。他们必须以手工方式来处理每台安全设备中所包含的极大量信息，创建关于正在发生什么事件的全面视图。以这种传统和无效的方法为基础建立法律分析系统的过程既耗费大量时间又代价非常高昂，而且还会占用本可用于其他更有价值的运营和/或安全活动的专家资源。此外，传统的安全数据分析方法需要若干天或若干周来执行。到那时，网络也许已经遭到了若干次攻击，并可因数据盗窃、客户和合作伙伴失去服务或机构生产效率降低等而导致重大损失。

鉴于这一现实，以技术为基础的实时安全数据监控和关联系统也就应运而生，并能检测出所发生(甚至发生前)的网络攻击或漏洞。被业内一般称为安全信息管理(SIM)解决方案的这些技术系统正作为负责确保企业系统安全性的首席安全官(CSO)、首席信息官(CIO)以及其他IT专业人员的成本效益更好的强大资产而纷纷涌现出来。

重要性

Cisco SIMS软件是根据Cisco公司团队、华尔街的领先企业以及软件行业的第一手实践经验而开发出来的，目的是适应不断强化的驱动因素增长。这些驱动因素包括:

1. IDS和防火墙等安全产品组合不能满足安全性期望
2. 要求必须报告安全事故的立法和法规压力
3. 安全产品的资源和管理给安全人员增添了出乎意外的和不可管理的负担
4. 不但要从外围而且要在整个机构中(包括各个应用程序)监控和关联事件的越来越大的压力

目睹企业安全领域中日趋严重的数据泛滥问题，他们利用Oracle、XML、Java和SilentRunner等尖端组件重新开发和建立了成熟可靠的技术。Cisco SIMS技术只依赖于这样一个事实，即数据是由一些需要被审查来看是否存在安全问题的设备或应用程序所产生的。该技术与厂家无关，这就使它能成为更好的“捕鼠器”并能分析各类告警和处理产生红色标记的异常情况。

独创性

“如果在攻击发生后三十天得到全部回答，那么您很容易就能成为安全专家。但到那时机构就已经损失了宝贵的时间和金钱。”

—— 某《财富》500 强制药企业首席安全官

Cisco SIMS系统是作为主要擅长企业和网络管理产品的专业服务机构 NetCom Systems 公司的一个内部工程项目而开发的。凭借其在 CA Unicenter TNG 和 HP Openview 部署中的深厚背景，工程师们十分了解这些产品的极高数据要求和有限数据管理功能。所以该团队具备与众不同的资格和能力来开发一种可提高这些投资的价值并加强人员的能力的企业软件产品。将这一宗旨延伸到安全领域，他们认识到，在企业实施了防火墙、入侵检测系统(IDS)以及其他基于基础设施的安全措施后，他们还会遭遇类似问题；因此，他们就构思出Cisco SIMS并创办了公司。

作为 Cisco 公司开发的第一个安全信息管理(SIM)系统，Cisco SIM 技术已被有效部署在 150 多个大型企业和政府部门之中。其针对资产漏洞或风险独特的实时测量和告警功能堪称无与伦比。

实施了安全信息管理解决方案的企业可以通过将来自多种不同数据来源的智能汇聚成一个系统而采取企业全盘方法来监控安全网络，因为这可使企业系统安全操作员和分析员能逐一地观察和分析威胁可能性。

成功

作为安全信息管理的领导者，Cisco SIMS是一个可全面运行的SIM 系统。

美国最大的城市医疗保健提供商纽约市健康与医院公司(NYCHHC)三年前就开始了满足 HIPAA 要求的努力。该公司拥有 11 所急性病诊疗医院、四所长期护理疗养院、六个诊疗中心、超过 65 个社区型诊所以及 35,000 多名员工 ——这些资源全都通过广域网(WAN)相连——因此该项目的艰巨性是可想而知的。

在纽约市工作的NYCHHC公司信息服务助理副总裁Arnold McCormick指出：“我们有一个广泛分布的数据通信网络，而我们也在通过这些医疗保健网络传输着极大量的病人诊疗信息。为此，我们需要一个牢固可靠的网络和可靠的安全措施来保护这个网络。”

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19一21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32一33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

欢迎下载电子文档，http://www.cisco.com/cn/power/security/

2004年11月印刷