SIMS 事故响应管理

当今的安全管理挑战

安全行业的多数人都已经熟知我们每一天所面对的传统挑战，安全数据太多而无法筛选、假报警太多而无法应对，缺乏足够预算或资源来处理越来越多的安全事件。还有一个经常被人们所忽视的挑战在于安全管理流程本身。在事件响应计划（IRP）中所定义的明确规定的、记录在文件中的、可重复的安全管理流程，是确保企业快速而准确地处理安全事件的必要条件，而当今很多IT企业却基本上忽视了这一点。

对于任何机构而言，及时和有效的事件响应直接关系到能否最大限度降低事件所导致的损失。它也许还有助于避免代价高昂而往往很难恢复，往往会随安全事故而导致声誉损失。有鉴于此，通过制定一份系统化事故响应预案而做好准备，不失为机构可以采取的成本效益最好的安全措施之一。

IRP 可以帮助企业回答在安全事故发生之中乃至之后所引发的关键问题。这些问题可能包括:

- 我们现在该怎么办?
- 我们该如何使网络恢复原来的正常状态?
- 谁该负责处理此次事故？事故是否得到了有效处理?
- 我们该如何避免此类事故今后再次发生?
- 我们如何把准备工作做得更好以避免其他事故的发生?

建立IRP的过程比我们想象的要更容易，SANS研究所最近就刚刚公布了一套最初是为美国能源部开发的，而后被美国政府其他部门采纳的六步事故响应方法。这套方法包括处理安全事故的六个关键步骤:

1. 准备
2. 识别
3. 封堵
4. 根除
5. 恢复
6. 后续

SIMS 事故响应管理

当在整个企业中部署IRP时，企业一般是依靠事故响应管理系统来实现尽可能多的程序的自动化。然而，经常发生的问题在于，今天的多数企业所依赖的都是Remedy或Computer Associates帮助台系统等一般化、非安全的智能化“事件跟踪”系统。

这就要求企业建立一个针对安全管理而定制的全面的事故响应管理系统——这个系统应该完美地集成到总体安全信息管理（SIM）解决方案之中。

SIMS解决方案再配合以新推出的事故响应管理模块就构成了对任何IRP系统的完美补充，因为它包含了全部或至少大部分解决哪怕是最复杂的安全事故所需要的数据和程序信息。更具体地说，SIMS 事故响应管理（Incident Resolution Management）专注于收集安全事件数据并将其组织成逻辑形式，然后执行适当的安全响应工作流，从而实现对安全事故的快速和有效响应。此外，通

过利用SIMS的事故响应管理知识库，用户就能获得进一步的决策支持来帮助自己解决几乎任何安全事件。

SIMS实现了安全信息管理系统与事故响应管理模块的紧密集成，因此可为所有的安全操作员和分析员提供很多重要优势。通过建立一个同时针对事件管理和事故响应管理的控制点，操作员和分析员就都有了一个强大的解决方案，可轻松监控各类事件进而对已发生事件进行响应和跟踪。

SIMS 事故响应管理高级特性

很少有别的SIM解决方案能提供内置的事故响应管理（IH）模块——相反它们往往依赖的是Remedy 公司或 Computer Associates 公司等厂家所提供的外部系统。Cisco SIMS 集成了目前市场上最先进的安全事故响应管理解决方案之一，提供了一整套特性来处理哪怕是最复杂的安全事件管理需求。而且，Cisco SIMSIH 实现了与基础 SIM 产品的全面集成，并可实现事件检测 / 响应与事故响应管理 / 跟踪之间的无缝转换。在本节中，我们将着重探讨 Cisco SIMS IH 的几个重要特性。

直观易用的图形用户界面

SIMS IH 采用了一个强大而易用的图形用户界面（GUI）。利用这个 SIMS IH GUI，操作员和分析员可轻松打开、编辑和关闭安全事件。利用这个直观的界面，用户可以根据向导完成创建并解决几乎任何安全事件所需要的步骤。SIMS IH 可使分析员根据所观察到的实时事件、法律报告所揭示的历史事件或客户企业中所采用的任何其他事件指标来打开个案。

内置的工作流

SIMS IH 集成了 SANS 研究所的六步事件响应流程。利用这个灵活、全面和可定制的工作流，用户可利用一个专门针对安全事件而设计的严格的、定义的、记录在文件中的且完整的流程来处理每个安全事件。此外，Cisco SIMS 还提供了预配置的事件模板以及可对站点定制的事故响应管理程序，进而简化事故响应管理流程。利用 IH 的定制特性，用户可对 Cisco SIMS 进行定制设计，使之符合几乎所有的客户需求和流程。

图 1

内置的知识库

SIMS IH 集成了一个灵活的知识库，能提供对具体厂家设备信息的全面补充，还提供了存有来自 CERT 和 CVE 等来源的安全最佳惯例的完整数据库。手头有了这一存有安全信息的仓库，操作员和分析员就能获得强大的决策支持能力，反过来又能使事件响应成为更容易和更顺畅的过程。

图 2

佐证保存与安全

SIMS IH 可将任何文件、图像或其他数据附加在每一个事件个案上。例如，SIMS 事件和报告可轻松附加在事件个案上。被扫描图像、音频采访录音及数据流捕捉等其他文件也可添加到个案上，且插入时可对其进行密码类校验和检查以确保佐证的完整性。被授权的不同用户也可在个案上添加说明和备注来提醒其他人注意并覆盖调查工作的其他方面。

基于角色的访问、事件协作与事件安全

SIMS IH 个案可被分配给不同的系统用户。也可被一组用户所共享。个案更改通知既灵活又可配置。个案数据和 IH 系统功能采用了颗粒化访问控制，所以若干个分析员可以在同一个个案上进行协作，同时还能保持“需要知道的”重要授权结构完好到位。这个关键特性为存储个案佐证以及对个案数据采用严密颗粒化访问控制等提供了一种安全的方法，同时仍允许调查员通过协作来调查个案。此外，系统用户对个案所采取的所有行动均被记录在审计日志中。

最后，在调查结束时，个案处理者可以选择将个案输出给 Cisco 公司以外的人员使用。所产生的报告包括了所有个案数据且可以打印或通过电子邮件发送。

报告

SIMS IH 可提供可靠的报告功能，其特性包括事件级和行政级报告。被授权操作员和分析员可从事件个案数据库中轻松检索事件个案。系统可对逐个个案或多组个案生成个案报告。系统可为管理人员和行政主管人员轻松生成个案监控和汇总报告。此外，用户还可对 SIMS IH 进行配置，使之能自动生成事件报告供公司管理层或第三方分享。

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

2004 年 11 月印刷