白皮书

综合关联：一种三层方法

综合关联：一种三层方法

引言

在确保IT基础设施的安全方面，当今企业面临着很多挑战。利用现有人手来处理越来越复杂的工作就是在可以预见的未来继续存在的挑战。这一复杂性的两个主要来源就在于入侵检测系统（IDS）、防火墙（FW）、操作系统（OS）、应用（APPS）以及防病毒系统（AVS）所检测和报告的数量极大且种类繁多的安全警报。仅一个防火墙每天就能产生超过十亿字节的日志数据，而一个IDS系统每天能产生超过500,000条消息。

更糟糕的是——这些安全系统所产生的很多信息大多是假肯定（即表示有敌对活动，但实际上没有）。多数消息只不过是表示网络资源正常合理使用情况的古老数据。这里的挑战在于如何区分并优先化那几个的确表示真正安全威胁的消息。这一将重要安全事件从IDS、FW、OS、APPS以及AVS等消息的白噪声中区别出来的必要性也是更大规模经济现状的一部分，即要求机构能更有效地利用其现有的安全资源。因此运营中心内部安全运作工作负担和各项任务优先化的自动化是至关重要的。

综合关联：一种三层方法

更有效的安全自动化的关键在于 Cisco 公司率先开发的软件技术——安全信息管理（SIM）。SIM 结合了若干与众不同的特性来实现对安全事件数据的收集、规范化和分析。Cisco SIM 技术的核心在于三种重要的数据关联功能—— 一种是基于安全政策规则的定义，另一种是基于统计威胁评分，而第三种则是基于与资产相关的实际漏洞。

虽然目前存在很多用于事件关联的技术，但Cisco公司的技术处于行业领先地位，因为它集成了可用于衡量两个或多个安全事件之间关系的三种独特的关联功能，来确定事件发生的可能性。当检测出可疑的安全活动时，Cisco SIMS 系统就会提醒操作员注意，进而采取适当对策。

Cisco SIMS基于规则的、统计的和漏洞的关联功能既与众不同又功能强大。虽然每种关联技术都是非常准确的，但实施起来却十分简单和直截了当——其中每种技术都从不同角度来实现事件关联，进而保护企业免遭更广泛的潜在安全事件的威胁。为了实现这一目的，Cisco 公司提供了一种可作为一整套 SIM 功能之有机组成部分的综合管理解决方案。

综合关联——一种三层方法

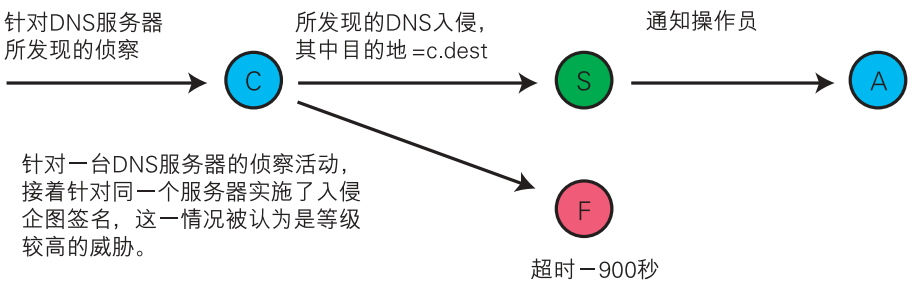
Cisco SIMS 解决方案集成了三种与众不同且功能强大的事件关联方法——第一种是基于规则的关联，它可通过针对从 SIMS 所监控的 IDS、FW、OS、APPS 或 AVS 设备中接收的每个事件来激活“时间警觉型”安全政策规则，将假肯定安全警报与可能十分重要的安全事件区别开来。

基于规则的关联被紧密映射到SIM 模型中，一般是从事件数据的收集和规范化开始的——也就是将安全事件数据规范化成同一种格式。当采用基于规则的关联时，首先是按厂家、咨询顾问或最终用户来预定义若干种可疑活动。一种情况中包括一系列用来定义某种可能的恶意安全事件或攻击的事件。以域名服务器（DNS）攻击情况为例，其中攻击者先实施 DNS 服务器侦察活动（如针对一台 DNS 服务器进行端口扫描），然后再针对IDS 所检测到的同一个 DNS 服务器进行一系列入侵尝试——我们可以利用简单的“如果”（“if”）、“则”（“then”）和“另”（“else”）等语句创建一些逻辑来捕捉这种情况。用中文表示，我们的 DNS 攻击规则可写为：如果我们从一个防火墙接收到一个针对该 DNS 服务器的侦察企图（DNS 版本检查或其他连接请求），则如果我们从一个 IDS 接收到一个或多个针对同一个 DNS 服务器的入侵企图，则向操作员发出一个通知。[用英语表示，我们的 DNS 攻击规则可写为：if we receive a reconnaissance attempt from a firewall against the DNS server（DNS version checking or other connection requests），then if we receive one or more exploit attempts from an IDS against the same DNS server, then send a notification to the operator]

当收到安全事件并将其与规则进行比较时规则就会触发。随着时间的推移，系统就会创建出事件“状态”来跟踪那些成功执行的关联规则。在我们的 DNS 攻击例子中，一次端口扫描事件会激活我们新定义的规则，进而导致“创建”或“开始”状态的建立。如果此后在预定义的时间范围内再次接收到一个 DNS 入侵事件，那么就会触发一个“成功”状态。当然，这以后接着就会是一个活动状态，该状态可导致向操作员发出通知。否则，经过一段时间后，就会触发一个“失败”状态，在该状态中规则也许会复位到“空”或“零”状态。用图形表示，针对我们的 DNS 攻击例子的 SIMS 基于规则的状态模型可以如下方式描绘：

基于规则的关联举例

图 1
基于规则的关联举例



虽然说这个例子对于当今异常复杂的攻击情况环境而言似乎显得过为简单化，在这里用到这个例子主要是为了说明如何实施一般的基于规则的关联。读者可以直观地看到基于规则的关联在发现已知攻击情况方面的强大威力，尽管更为精确的识别属于 SIMS 关联技术的功能。

我们来考虑登录一台服务器这种较为普通的操作。每次登录成功后，一个或多个安全设备都会产生而SIMS也都会处理至少一个消息。这些消息的绝大多数可以归类为正常用户活动。之所以要设计基于规则的关联就是要识别“万一会发生”的非法访问。

基于规则的关联是通过激活时间敏感型关联规则来发现这些万一会发生的情况的。在我们的登录例子中——在收到一个端口扫描事件后，我们可以将规则设定为连续 15 分钟寻找非法登录企图。在这一 15 分钟期间内，所有非法登录企图都会导致向操作员发送消息。显然，错误设定一个时间参数可导致极大量的假肯定。所以，虽然说这种关联方法能有效地检测出具体安全事件，但当它单独使用时代价却是假肯定信息比例增大以及运算处理要求提高。

单独使用的基于规则的关联的另一局限性在于，它只能检测出有限的一组安全情况——也就是那些在系统中定义的情况。为此，Cisco 公司认为必须采用一种多层方法——也就是在采用基于规则的关联的同时配合使用统计和漏洞关联。

统计关联是内置在SIMS体系结构中的第二种关联方法。利用统计关联，我们可按资产或资产组将规范化安全事件归类为不同安全事件类型——事件类型的范围包括侦察攻击、病毒攻击、拒绝服务攻击——等等。对于每种资产，系统可连续计算出一个威胁分数，也就是通过将事件严重程度

综合关联：一种三层方法

与资产价值相加来确定对安全事件的总体衡量。这种关联方法的优点在于，它基本上是不知道攻击情况的，也就是说，统计关联是针对系统中潜在的异常情况的，而与它们所最初产生的流程无关。

统计关联还有其他一些关键优点，其中一个优点在于，它是一种实施前不要求定义规则或重要“基线”（可确定统计正常状态）的“即插即用”技术。另一个主要优点在于，它能找出基于规则的关联机制可能未检测到的那些异常情况。另一方面，统计关联也有其内在局限性，这主要在于其统计本质。事件威胁评分模型是用来寻找安全异常情况和事件可能性的——而不是寻找具体威胁情况的。它是依靠归类和统计评分机制来实现这一目的的。

内置在SIMS产品中的另一种关联方法就是漏洞关联。它可以根据系统漏洞来进行系统的评分。这一漏洞是由来自漏洞扫描器的数据输入来确定的。漏洞评分越高，系统对攻击的敏感性就越大。当然，只有当攻击能充分利用系统所具有的具体漏洞时，攻击才能成功。此类关联是十分重要的，因为它可使管理员关注于那些容易遭到这些事件攻击的系统。

这种关联方法还可实现更好的时间管理和更好的人员利用。它能确保根据所观察的事件和相关的漏洞而发现针对系统的真正威胁。其他优点还包括可将漏洞数据实时关联到资产价值和威胁，进而使操作员能看到具体事件的实际影响。漏洞关联可根据 ——依据输入到系统中的漏洞数据而产生的——当前漏洞简况而实现自动化漏洞和暴露程度评分。

三层关联方法的真正威力在于，一方面，它能搜索具体威胁情况，而另一方面，又能用统计方法来测量其他可能的威胁异常情况，并可利用这两方面的数据来分析资产实际上是否会遭到该事件的攻击。Cisco 公司坚信，企业只有采用这种三层方法才能实现我们所说的“综合关联”。

SIMS 基于规则的关联——概述

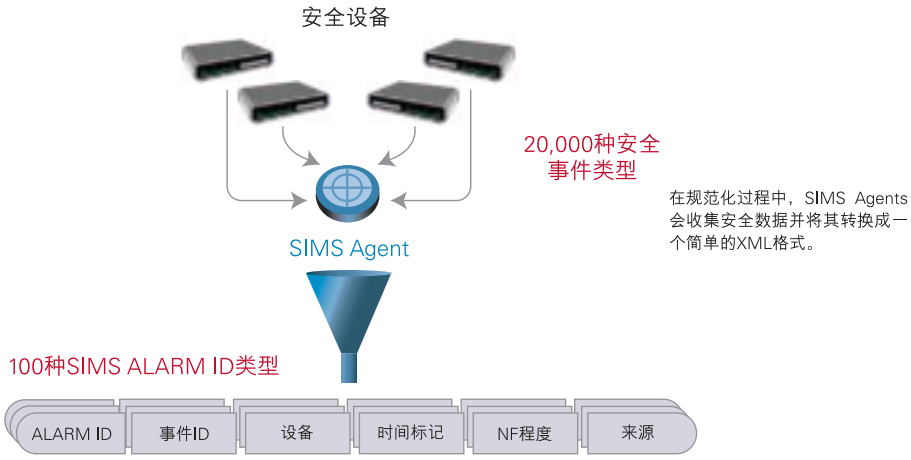
在 SIMS 系统中，基于规则的关联深深地根植在 SIM 流程之中，而且是从规范化阶段开始的。它要求进行数据规范化，因为目前在各安全设备制造商之间存在的标准并不多。每个设备制造商都有它自己产生具体设备日志信息的格式。这就是说，Cisco PIX 防火墙日志信息看起来会与 Check Point 防火墙日志信息非常不同。实际上，最近一项研究得出的结论表明，目前各种安全设备可产生 20,000 多种不同类型的安全设备事件。这一规范化要求不仅适用于基于规则的关联，而且也适用于统计关联。

SIMS 规范化过程有两个步骤。首先，SIMS Agent 技术将目前所产生的这 20,000 种事件类型映射到约 100 个不同的 SIMS Alarm ID。SIMS Agent 然后进行规范化阶段中的第二个重要步骤，将日志记录重新格式化为同一个共同的 XML 格式——这是 SIMS 系统独一无二的专有流程。在这一称作语法分析的过程中，事件 ID、来源、源端口 ID、目标以及目标端口 ID 等关键信息被转换成同一个共同 XML 记录，该记录与新分配的 Alarm ID 相连后就被称为一个 Alarm ID 记录。

语法分析结束后，XML Alarm ID 记录随后可通过 TCP/IP 安全地传递到一个或多个 SIMS Engine（引擎）——也就是 SIMS 的重型机器。SIMS Engine 的任务就是进行汇聚（在此期间会进一步减少数据以消除重复的事件信息）和关联等工作——既包括基于规则的关联也包括统计关联。

综合关联：一种三层方法

图 2
SIMS 如何进行
规范化的过程



SIMS 基于规则的关联方法是专门用来通过实现以下功能而解决常见安全事件分析问题的:

- 减少假肯定安全警报总数
- 识别具体安全事件
- 确定工作优先级并首先解决风险最大的问题
- 重复性任务和 / 或关键时间响应的自动化

基于规则的关联可通过激活从 SIMS 所监控的 IDS、FW、操作系统、应用或 AVS 设备中收到的每个消息的“时间警觉型”商业政策规则而将假肯定安全警报将重要的安全事件区别开来。

SIMS Engine 负责执行基于规则的关联任务。每个 Engine 可作为其他 SIMS Engine 的分布式对端而运行，所以，就象其他 SIMS 组件一样，安全信息也是实时处理的。SIMS Engine 负责执行用来将非法活动从合法活动中分离来的安全规则和分析功能。

通过应用此类规则（如在我们举出的 DNS 攻击例子中），系统可以对每一个成功的登录事件进行检查而识别出此前发生过端口扫描等可疑活动的极少数登录事件。请注意：这些 Engine 可针对实时安全消息流和 / 或针对在规定时间内发生的消息的合法数据库而运行或操作。

Cisco 公司可提供一整套各种各样的预定义规则，因此可立刻实现即时价值。此外，其中所包括的一种规则创作编辑工具还可支持新规则的定义和/或预定义规则的定制。除了能通过规则创作编辑而扩展功能之外，还可通过简单地在 SIMS 基础设施中添加更多 Engines 来逐步扩展 SIMS Engine 的工作负载能力。

综合关联：一种三层方法

基于规则的关联还可通过提供以业内公认的最佳惯例以及SANS研究所和CERT等机构所制定的标准为基础的成熟可靠的、时间敏感的、实时定量的威胁信息而确定工作的优先级，进而专注于风险最高的环节。

当检测出原始消息或相关联安全事件时，系统就会触发重复性任务和/或关键时间操作的自动执行。这些行动包括:

- 执行一个用户定义的功能
- 将事件记录在日志中
- 发出一个电子邮件通知
- 向寻呼机发送一个通知
- 生成一个 AHD (自动化帮助台) 故障单
- 在实时控制台上显示该事件
- 向一个或多个目的地签发一个 SNMP 陷阱
- 将源 IP 地址添加到入侵者监视列表中
- 将目的地 IP 地址添加到资产监视列表中

此外，还可连同分支机构、条件、循环和同时处理流等的逻辑而一起规定上述任务的任意组合。

凭借其针对网络安全事件实时分析的内置可扩展性和易用性，SIMS基于规则的关联提供了突破性的技术，可极大提高您现有安全团队的工作成效。

SIMS 基于规则的关联之特性和优点

特性	优点
预配置的安全规则，可立刻开始识别安全威胁	基础产品安装后可立刻实现投资回报
基于规则的关联可减少假肯定安全警报次数	可减轻安全运行和分析人员的工作负担
易于使用的规则编辑器	技术专家可利用简单的“所见即所得”（WYSIWYG）“无代码”开发环境而修改和扩展预配置安全分析
能识别混合型攻击的成熟可靠的多变量事件检测逻辑	可轻松识别复杂威胁，可使运营和法律人员关注于威胁和风险最大的环节
预定义规则遵循智能化模型来测量与关键资产相关的威胁	运行过程可确定工作的优先级从而首先解决最重要的安全事件，而无需定义额外规则
可将根据多个原子事件而配伍的混合事件相互联系起来作为相关警报	可进行法律和实时分析，从而确定与某个混合事件相关的原子事件模式
可发现行动与被检测事件之间的关系	可实现自动化响应机制，进而可实现针对潜在安全攻击的快速封锁和解决
检测和响应逻辑可结合定时、布尔条件和定序技术规范	可检测出复杂混合型攻击，可触发多步工作流过程
关联规则是根据 SIMS 规范化和已归类警报而定义的	用于安全分析的逻辑与厂家或防火墙、入侵检测系统以及防病毒系统等安全设备所产生的具体消息格式均无关
支持可由用户扩展的一组相关联事件类型，并可联回与标准相关的 nfAlarm	可将多个事件或事件序列整合为数量少得多的混合或相关事件
开放式和可扩展的关联体系结构	可通过 SIMS 合作伙伴技术轻松扩展 SIMS Engine 功能

综合关联：一种三层方法

SIMS 基于统计的关联——概述

在统计关联过程中，SIMS 流程可对事件数据进行规范化处理，确定安全事件类型及其发生的风险。这是通过一个两步次序来进行的。首先，将 SIMS Alarm ID 归类为 9 个不同事件类型之一。这些事件类型代表了常见类型的安全攻击情况并包括：拒绝服务（DoS）、侦察、应用利用、授权、躲避、病毒、系统状态以及政策违反等。通过使用这些常见的事件类型，操作员和分析员就能查看到归类事件数据并轻松确定正在进行中的攻击。

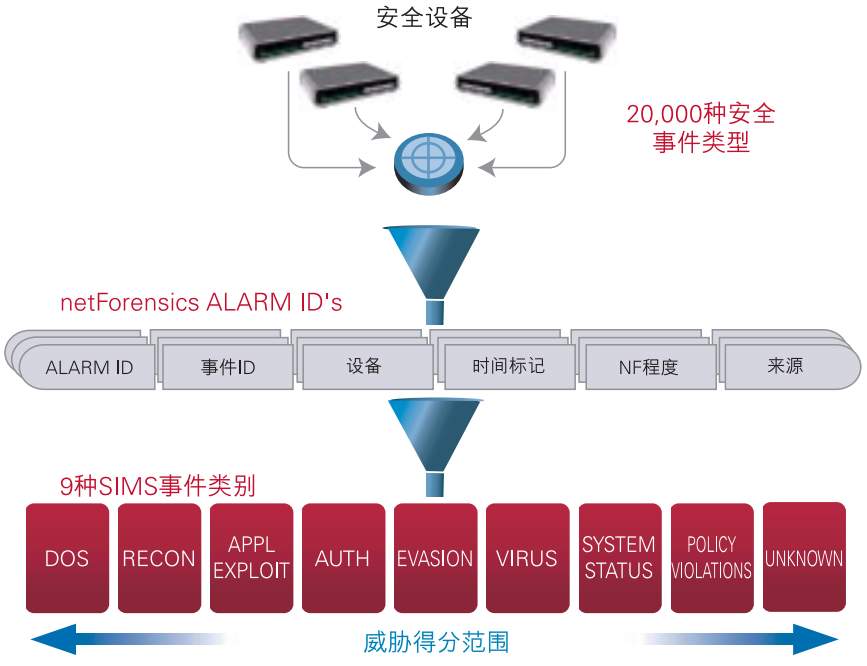
在瞄准潜在威胁的最后一步中，SIMS 可对所产生的事件类型进行“评分”来确定威胁程度。威胁评分是针对警报严重程度（Alarm Severity）再结合资产价值的时间加权衡量。警报严重程度（Alarm Severity）或资产价值越高，威胁分数就越大。

评分方法适用于入侵者和资产。

- **资产威胁得分**：这是一个时间敏感型和严重程度加权数值，当资产遭受攻击威胁时，该分数可用于实时识别安全调查并确定其优先级
- **入侵者攻击得分**：这是一个时间敏感型和严重程度加权数值，当入侵者实时发动攻击时，该分数可用于识别针对入侵者的安全调查并确定其优先级

当需要确定一种或多种资产是否正遭到攻击时，相关联威胁分数是非常准确的测量指标。分数越高，就表示针对所考虑的设备或资产的威胁可能性越大。

图 3
SIMS 统计关联



综合关联：一种三层方法

SIMS 统计关联的特性和优点

特性	优点
“即插即用”统计安全模型可实现即时和高效的事件检测	可立刻产生结果，不要求或只需很少的基线操作
安装时不要求预配置	实施快速而轻松
统计模型能找出基于规则的关联方法所漏掉的安全事件	统计关联可以很好地补充有限的基于规则的关联功能
可根据用于定义的门限水平来定制成熟可靠的评分和归类机制	可减少假肯定次数并可使操作和法律人员仅关注于那些威胁可能性最大的事件
评分算法可检测出多类原子事件所产生的简单和混合事件	对于特定事件类型而言，评分和归类算法可通过提供相关威胁可能性水平而识别出相应威胁类型，因此操作员可关注于真正的威胁
关联算法是根据 SIMS 的规范化和已归类警报而定义的	用于安全分析的逻辑与厂家或防火墙、入侵检测系统以及防病毒系统等安全设备所产生的具体消息格式均无关
开放式和可扩展的关联体系结构	可通过 SIMS 合作伙伴技术轻松扩展 SIMS Engine 功能

SIMS 漏洞关联 —— 概述

漏洞关联的目的在于要识别出假肯定警报，同时为那些尚未确定是否为假肯定或假警报的事件分配一个置信等级（通过 nF Severity）。这种方法的主要优点在于，它能极大提高威胁运算的有效性并可提供适用于自动响应和 / 或告警的事件。

SIMS Vulnerability Correlation（漏洞关联）引擎使安全人员能确定不同事件的优先级从而及时地对这些事件作出响应。SIMS 可从多个来源收集漏洞数据。然后将这一数据关联到从代理处收集的资产威胁数据并为每个系统分配一个风险分数。

当观察到事件时，安全管理员可实时和自动地将正在发生的该事件与系统的漏洞分数进行比较和评价并确定是否应该采取措施。如果系统不容易遭到该事件的攻击，则无需采取任何行动。

通过将若干加权暴露参数相加，即可分配一个绝对的漏洞分数。在多个系统上进行规范化可提供适用于风险运算的系数。

这种体系结构的一个例子是，如果管理员看到一次 Microsoft SQL 服务器缓冲区溢出攻击，但根据最新输入的漏洞数据可判定被攻击的系统不容易遭受缓冲区溢出攻击的威胁，那么就不需要采取任何措施来保护该系统。然而，如果还是观察到这种攻击，而被攻击的系统容易遭受缓冲区溢出攻击的威胁，那么管理员就知道必须马上采取行动。

漏洞关联

- 将 IDS 数据与漏洞相关联来分配置信等级
- 从噪声中分离出真肯定
- 用于关联的免维护规则逻辑
- 可利用漏洞索引来自动繁殖资产数据库
- 全面包括 CVE 和厂家漏洞信息

综合关联：一种三层方法

图 4
漏洞关联

漏洞关联的组件

- 符合 CVE 的 IDS
- 漏洞评估扫描器 / 服务
- 从扫描器中采集的 OS 指纹
- CVE/ICAT 数据库
- 实时 SIMS 事件供给

结果

- 基于规则和基于威胁（统计）的关联并提供主机简况
- 可接获事件和条件
- 可利用上下文来丰富 NIDS 的数据，从而帮助 NIDS 更好地工作
- 可简化事件响应
- 可实现自动化响应操作

综合关联：一种三层方法

特性	优点
IDS 告警验证	可帮助管理员识别出与 IDS 相关的全部假肯定
可根据当前漏洞简况而自动进行漏洞和暴露评分	可降低风险并用更多时间去调查和消除真正的威胁
被关联到资产价值和威胁的漏洞数据可显示具体事件的影响	可缩短对真正威胁的响应时间
可利用行业标准风险公式来进行真正的风险计算	可提供针对企业的威胁的真实视图
知识库中的漏洞信息	这一信息可帮助管理员通过学习必要知识而做好应对威胁的准备，同时节省搜索互联网来寻找相应信息的时间
符合标准类型的先进漏洞报告和弥补进度跟踪功能	可生成供管理层审查并显示真正 ROI 的报告。还有助于化解和政策符合性战略

SIMS 关联——综合性方法

安全事件关联是一项复杂任务，其中涉及到对在特定时间内发生的两个或多个事件进行分析以确定相关威胁可能性。Cisco 公司的 SIM 技术结合了三种关联功能，即基于规则的关联、统计关联和漏洞关联。这些关联功能中的每一种都有它们自己与众不同的优点。这些技术结合起来使用能提供一套强大而独特的分析功能并为企业提供一种既能检测和弥补安全事件同时又能最大限度减小安全事件检测的局限性并提高其有效性的综合性关联解决方案。

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