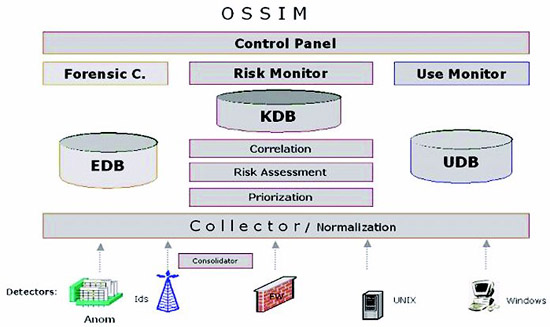
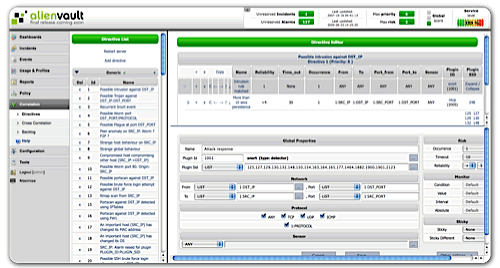
OSSIM企业级开源SOC

OSSIM即开源安全信息管理系统(OPEN SOURCE SECURITY INFORMATION MANAGEMENT)是目前一个非常流行和完整的开源安全架构体系。OSSIM通过将开源产品进行集成,从而提供一种能够实现安全监控功能的基础平台。 它的目的是提供一种集中式、有组织的,能够更好地进行监测和显示的框架式系统。

OSSIM明确定位为一个集成解决方案,其目标并不是要开发一个新的功能,而是利用丰富的、强大的各种程序(包括Snort、Rrd、Nmap、 Nessus以及Ntop等开源系统安全软件)。在一个保留他们原有功能和作用的开放式架构体系环境下,将他们集成起来。而OSSIM项目的核心工作在于 负责集成和关联各种产品提供的信息,同时进行相关功能的整合。由于开源项目的优点,这些工具已经是久经考验,同时也经过全方位测试、可靠的工具。   
  
OSSIM结构体系   
  
实际上,从过程上考虑,安全可以分为评估、防护、检测、响应这四个步骤,现在已经有了不少优秀的开源软件与这四个步骤相对应。但是问题在于这四个步骤属于 一个动态、无缝过程,而所有的开源工具只是针对单一安全问题,如何将现有的安全工具进行综合利用并将他们无缝综合,OSSIM给出了很好的答案,那就是 ——集成。   
OSSIM由数据收集、监视、检测、审计以及控制台这五个模块构成。这5个模块包含了目前安全领域从事件预防到事件处理一个完整的过程,在目前的安全架构 中,OSSIM是最为完备的。这五个功能模块又被划分为三个层次,分别是高层的安全信息显示控制面板、中层的风险和活动监控以及底层的证据控制台和网络监 控,各个层次提供不同功能,共同保证系统的安全运转。   
在OSSIM中,整个过程处理被划分为两个阶段,这两个阶段反映的是一个事件从发生到处理的不同的历史时期,这两个阶段分别为预处理阶段,这一阶段的处理 主要有监视器和探测器来共同完成,它们主要是为系统提供初步的安全控制;另一个事后处理阶段,这一阶段的处理更加集中,更多的是反映在事件发生之后系统安 全策略的调整和整个系统的安全配置的改进。   
在OSSIM的架构体系中,有三个部件比较引人注意,这是OSSIM中的三个策略数据库,是OSSIM事件分析和策略调整的信息来源,分别为以下三种数据库:   
◆EDB(事件数据库):在三个数据库中,EDB无疑是最大的,它存储的是所有底层的探测器和监视器所捕捉到的所有的事件。   
◆KDB(知识数据库):在知识数据库中,将系统的状态进行了参数化的定义,这些参数将为系统的安全管理提供详细的数据说明和定义。   
◆UDB(用户数据库):在用户数据库中,存储的是用户的行为和其他与用户相关的事件。   
  
OSSIM功能架构   
  
OSSIM的功能一共可以划分为9个层次,各个层次之间是无逢连接的,底层的数据为上层的处理提供信息来源。图1就是OSSIM所提供的功能的层次结构图。



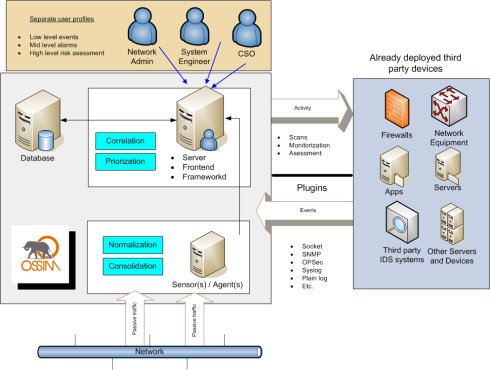


OSSIM可以分成几大部分：一是ossim-agent,二是ossim-framemork,三是ossim-server,四是ossim-web界面。   
老版本的ossim的源代码把所有代码放在一个工程下面，1.0以后的版本基本都分开了，按上面四个部分有四个工程，   
在ossim的CVS服务器上，我们可以看到有五个以下工程：   
1.agent   
2.os-sim   
3.server   
4.web   
5.ossim-gsoc2008   
ossim-gsoc2008是和google的源代码合作项目，google出资金支持一部分高级软件开发者参与开源软件开发，并提供项目的托管等服务，ossim开   
发团队借助Google的开源社区开发者进行一些OSSIM的创新性开发。为避免混乱，刚入门研究OSSIM的代码最好不要去关注ossim-gsoc2008。剩下   
的四个部分就很清楚了，核心的东西是framemork，这是一个处理和整合其他各种插件和数据的框架，代码是用python写的，对应的工程是SVN里   
的os-sim/frameworkd，代码比较多的是界面web，这是用php为主要编成语言实现的，另外server部分是OSSIM和数据库打交道的必经通道，这部分代码主要是用C语言实现的。agent就不用说了，但是真正的源代码是在ossim-gsoc2008下的agent目录下，agent主要也是用python实现的。server,framemork   
和web的代码现在都放在os-sim里了，server主要的代码对应的目录是os-sim/src，web代码对应的目录是os-sim/www。所以只要检出os-sim和agent就可以了。   
ossim源代码CVS库地址：   
host:os-sim.cvs.sourceforge.net   
Repository path:/cvsroot/os-simColinDoug]

OSSIM确实功能比较强大，因为其定位与SIM，所以完全具备了PDRR，也包含了PDCA。内部集成了NM领域（Nagios，ntop），Security领域的HIDS（osiris，snare，ossec），NIDS（snort，acid），漏洞扫描（nessus），以及诸多ossim的插件（plugsin）。能与部分AV厂家日志融合（趋势、symantec），支持网络设备（cisco）；提供了简单的关联分析；提供了dashboard（简报面板）。可以这么说，目前世面上稍微稳定点的概念产品功能都集成了。  
不过，它没有集成Hyperic HQ产品，所以数据库监控效率不高；集成的产品比较多，展示风格不太统一；为集成mrtg（未找到），所以无法调出交换机等的背板流量曲线（家里条件不具备）。  
我个人认为，只要完成如下工作，就可以将其修改为一个非常友好的SOC。  
1、增加C/S的网络安全拓扑图。不是我喜欢回到C/S时代，C/S在展示拓扑图上，确实有其优势，可以将图像生成放在客户端上，减轻服务端的负担，从而可以生成优美的拓扑界面，改变当前呆板的式样。Nagvis虽然可以生成美观的图像，但在IE里展示图像，目前还是无法与C/S媲美。  
2、增加快速响应功能。目前ossim上的响应都是先配置一个action，然后再利用此action。这个是个优雅方法。但是，现场发生情况时，不能这么优雅。看到设备上新起了可疑进程、激活了可以用户时，最快速的方法不是在收到告警后去制定一个action，然后再下发该指令，让sensor去执行。这样太慢了。而应该是快速结束进程、中断用户session。最后才能为这类新事件添加一个action，等下次再发生时就能自动执行了（我一直怀疑自动执行，因为在某些时候，可能会非常滞后了）。  
3、增加审计。ossim的审计功能我个人认为比较不尽人意，其报表只能满足简单要求（开源能做到这步已经非常好了）。如果要做成产品，必须增加典型场景自动审计（与用户业务环境耦合）；此外，需要增加手工审计功能。手工审计我希望能做成象google一样的搜索引擎，用户可以对中心日志文件（或日志库）进行任意检索，并作出自己的决定。  
4、承3，需要增加一个日志中心服务，保留所有的日志，并完成搜索引擎功能。此外，还需要提供搜索结果转IDMEF格式xml的功能，互联是网络产品的出路，不能拒绝与别的产品互通。而IDMEF是标准化的攻击消息交换格式，可以直接给其他安全产品用（直接提供syslog格式也可以，不过太不专业了）。  
5、增强关联分析。是的，ossim已经提供了简单关联分析（我认为还是有点简单），我们还需要增强。增加关联的力度，深度挖掘（用户在利用搜索引擎时积累下的经验，可以变换成关联规则，并被自动执行）。  
6、增强资产管理。ossim的资产管理还是不好用。最大的缺陷是：你只能配置资产、或采集局部资产。而SOC应该以资产为基础核心，事件为其通信核心。所以SOC在配置了资产下去后，应该时刻关注设备上的所有资产。配置资产与采集资产不一致时，就是违规了。这点ossim没有实现（我认为是这样的，如果你找到了，请告诉我）。  
7、增加文档管理。ossim集成了snare，可以有效管理文件的创建与访问，但是，文档也是企业的资产核心（另外一个是数据库）。需要增加文档拷贝、部分复制、外发等安全管理。真正做到文件生命周期管理：文件申请、授权、拷贝、销毁。  
8、增加数据库管理。我未看到ossim的数据库管理亮点，所以才强调本点。数据库管理除了性能外，还包括数据库连接、访问、访问特定表的前后顺序管理。最好是在特定数据表访问前，将请求包都保存起来，用于自动审计、场景审计和手工审计。  
9、增加主机/终端接口管理。ossim利用snare可以监控usb呢，真是棒极了。70％的信息泄漏是内部员工引起的，监控住了USB，就可以将这70％中的80％管住吧（80－20原理）。此外，蓝牙、CDRW、WiFi都可以泄漏、打印机也会泄漏。将通过这些接口外发的文件都监视起来，可以安全不少吧？  
10、增加外发邮件管理。邮件管理可以集成邮件管理专用软件或插件来完成。  
11、增加内容过滤、url过滤管理。我非常奇怪，ossim为何不增加这样的插件，至少给个提示也好呵，可它根本未涉及。难道它只关注os基本，不关注应用？SOC需要关注企业应用呢。  
12、增加认证功能（CA最好）。包括节点认证、用户认证。ossec的客户端需要一个author码，nagios不要。要将ossim包装成一个可接受的产品，必须增加此功能。  
13、集成ossim的客户端集合功能。ossim的客户端繁多，不修改直接来用，肯定会引起用户反感。需要对其进行整合，一键启动、一键停止。  
14、增强用户终端管理功能。ossim的客户端都是瘦客户端，管理功能比较弱（因为其功能单一）。用户终端至少应该有环境检测、网络诊断、脚本执行功能吧？我希望增加防火墙功能、本地合归性检查功能（是否安装了非法软件、是否未升级补丁、到期的文档是否已经删除等）、简单防rootkit功能。同时，自身必须利用rootkit技术进行必要的数据隐藏，防止用户断线后进行的违规活动记录被清理，防止用户随意卸载。  
15、增加与企业业务耦合的插件，为客户业务服务是SOC的宗旨。只有安全成为了一个关键业务因素时，用户才愿意为安全付费。在其未充分重视此点之前，SOC只能为业务服务。  
16、增加知识库。ossim没有知识库概念。出于isms或soc的普通合规性，我们也要提供知识库，以便与用户共同进步。  
市场开拓  
1、为ossim是开源，所以适应将新增的功能做成plugsin，这样即使不公布源代码也未违法GPL。  
2、整个产品做成一个box，收取硬件费用、施工费用、插件开发费用、培训费用、维护费用，ossim免费。  
3、定制报表。为用户提供定制报表，定制报表收费。  
4、OEM，如果哪个企业有开发或进入安全关联领域，可以联系我们

在安全领域，也存在众多的开源架构，OSSIM就是其中的代表之一，通过将各种安全工具集成形成一整套的开源安全架构体系，带来了高级别的安全性。

图1 OSSIM结构图

[](http://photo.blog.sina.com.cn/showpic.html#blogid=60c3194c0100dpcy&url=http://static8.photo.sina.com.cn/orignal/60c3194cg6cfb880919d7&690)

大多数主流安全产品针对的是计算机单一安全缺陷，他们更多的是提供某一单独的安全保护功能。目前安全领域内还没有一套相对完整系统安全解决方案，而且由于主流商业安全软件的闭源特性，让我们对其自身的安全特性也不能够完全信服。

随着软件开源趋势的不断推进，现在出现了很多甚至可以说性能毫不逊色于任何商业软件的安全工具（如Nessus、Netfilter、Snort等），那么有没有一种可能将这些工具进行整合并形成一整套系统安全的解决方案或者架构呢？答案是肯定的，这就是OSSIM。

OSSIM即开源安全信息管理系统（OPEN SOURCE SECURITY INFORMATION MANAGEMENT）是目前一个非常流行和完整的开源安全架构体系。OSSIM通过将开源产品进行集成，从而提供一种能够实现安全监控功能的基础平台。它的目的是提供一种集中式、有组织的，能够更好地进行监测和显示的框架式系统。

OSSIM明确定位为一个集成解决方案，其目标并不是要开发一个新的功能，而是利用丰富的、强大的各种程序(包括Snort、Rrd、Nmap、Nessus以及Ntop等开源系统安全软件)。在一个保留他们原有功能和作用的开放式架构体系环境下，将他们集成起来。而OSSIM项目的核心工作在于负责集成和关联各种产品提供的信息，同时进行相关功能的整合。由于开源项目的优点，这些工具已经是久经考验，同时也经过全方位测试、可靠的工具。

OSSIM结构体系

实际上，从过程上考虑，安全可以分为评估、防护、检测、响应这四个步骤，现在已经有了不少优秀的开源软件与这四个步骤相对应。但是问题在于这四个步骤属于一个动态、无缝过程，而所有的开源工具只是针对单一安全问题，如何将现有的安全工具进行综合利用并将他们无缝综合，OSSIM给出了很好的答案，那就是——集成。

OSSIM由数据收集、监视、检测、审计以及控制台这五个模块构成。这5个模块包含了目前安全领域从事件预防到事件处理一个完整的过程，在目前的安全架构中，OSSIM是最为完备的。这五个功能模块又被划分为三个层次，分别是高层的安全信息显示控制面板、中层的风险和活动监控以及底层的证据控制台和网络监控，各个层次提供不同功能，共同保证系统的安全运转。

在OSSIM中，整个过程处理被划分为两个阶段，这两个阶段反映的是一个事件从发生到处理的不同的历史时期，这两个阶段分别为预处理阶段，这一阶段的处理主要有监视器和探测器来共同完成，它们主要是为系统提供初步的安全控制;另一个事后处理阶段，这一阶段的处理更加集中，更多的是反映在事件发生之后系统安全策略的调整和整个系统的安全配置的改进。

在OSSIM的架构体系中，有三个部件比较引人注意，这是OSSIM中的三个策略数据库，是OSSIM事件分析和策略调整的信息来源，分别为以下三种数据库:

◆EDB（事件数据库）:在三个数据库中，EDB无疑是最大的，它存储的是所有底层的探测器和监视器所捕捉到的所有的事件。

◆KDB（知识数据库）:在知识数据库中，将系统的状态进行了参数化的定义，这些参数将为系统的安全管理提供详细的数据说明和定义。

◆UDB（用户数据库）:在用户数据库中，存储的是用户的行为和其他与用户相关的事件。

OSSIM功能架构

OSSIM的功能一共可以划分为9个层次，各个层次之间是无逢连接的，底层的数据为上层的处理提供信息来源。图1就是OSSIM所提供的功能的层次结构图。

模式匹配

大部分传统的探测器都使用模式探测，一个比较常见的例子就是IDS（入侵检测系统）。模式探测就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，来发现违背安全策略的入侵行为。该过程可以很简单，也可以很复杂。

一种进攻模式可以利用一个过程或一个输出表示。这种检测方法只需收集相关的数据集合就能进行判断，能减少系统占用，并且技术已相当成熟，检测准确率和效率也相当高。但是，该技术需要不断进行升级以对付不断出现的攻击手法，并且不能检测未知攻击手段。

异常监测

异常检测首先给系统创建一个统计描述，包括统计正常使用时的测量属性，如访问次数、操作失败次数和延时等。测量属性的平均值被用来与网络、系统的行为进行比较，当观察值在正常值范围之外时，IDS就会判断有入侵发生。

异常检测一个突出的优点就是它的自学习能力，用户不用告诉系统哪些是正常行为哪些是非正常行为，异常检测根据已经定义好的行为描述，当检测到的行为违背了这个正常行为的描述时，会自动发出警报。

异常检测的优点是可以检测到未知入侵和复杂的入侵，缺点是误报、漏报率高。误报是可以容受的，但是漏报就是应该避免的。但是由于网络入侵行为的多样性和复杂性，现在还不能给出一个相对精确的正常行为和非正常性行为的确切描述。

集中化和规范化

集中化和规范化的目标是通过某些协议将安全事件的处理进行统一管理。目前几乎所有的安全产品都倾向于采用标准的协议进行集中化的管理，这种管理在某种程度上将会更加有利于全局控制并且清晰，但是由于各种开源安全产品之间存在各种差异，如何在他们的基础上提供一种有效的集中化和正规化的管理方式，是OSSIM必须要解决的问题。

规范化需要一种翻译机制，这种机制能够将来自于不同监测器所捕捉的事件信息或者报警信息进行统一类型规范处理，处理之后形成一种能够被系统接纳的信息。OSSIM中采用事件数据库同时利用控制台进行相关事件的处理和显示。

优先级

一个系统的优先级取决于系统的拓扑结构及系统的运行状态，总而言之，一个事件的安全级完全根据系统的实际情况和安全策略来决定。

优先级制定是在系统收到报警信息之后一个非常重要的步骤，这个步骤完成的是对这些信息的过滤，同时也把收到的报警信息进行排队，优先处理对于系统威胁较大的事件。

危险评估

系统中一个事件重要与否主要取决于三个因素，分别为与事件相关的安全评估值;事件对系统所能造成的危险程度;事件能够发生的可能性。危险评估通过综合上述三个事件要素给出每个系统安全事件的危险评估值并让相应组件完成处理。

交互

在OSSIM中，交互指的是对于输入数据和输出数据的操作。由于网络事件的复杂性，多数情况下一个探测器收到的信息并非一个事件的完整输入，只是其中的一个组成部分，如何将这些部分的信息进行组合形成完整的系统需要的信息来源就是交互所要完成的事情。

监视器

监视器有一系列的探测工具组合而成，完成五个方面的功能,分别为危险监视、使用Profile监视、路径监视、硬连接分析和软连接分析。

控制台

控制台提供用户一个系统收集到的所有事件信息的访问接口。控制台也是一个基于事件数据库的搜索引擎，能够让管理人员从一种更加集中的方式针对整个系统的安全状态分析每一个安全事件。同时，控制台的存在也给我们提供了关于一个安全事件最为详细的相关信息，这为事件的处理提供依据和来源。

虽然目前OSSIM更多地停留在研究和探索阶段，但是其本身的优势确是显而易见的，OSSIM的开源特性和透明性，以及它所能提供的整体的安全解决方案是目前其他商业安全软件所无法比拟的。

目前OSSIM还是存在着不足和缺陷，主要体现在本身架构的不成熟和相关组件存在安全缺陷，但随着研究的不断深入和更多优秀开源安全工具的加入，OSSIM的应用将得到更大的普及。

## [OSSIM的Agent架构](http://liu-hliang.javaeye.com/blog/827398)

**Agent**

    OSSIM Agent的主要职责是收集网络上存在的各种设备发送的所有数据，然后按照一种标准方式（standardized way）有序的发送给OSSIM Server，Agent收集到数据后在发送给Server之前要对这些数据进行标准化处理，这样Server就可以依一种统一的方式来处理这些信息，并且也简化了Server的处理过程。

注释代码 [复制代码](http://liu-hliang.javaeye.com/blog/827398)

1. <SPAN style="COLOR: #ff00ff">这一点和Hyperic HQ 的Agent有很大的区别：HQ Agent只负责数据的采集，将采集到的数据通过HTTP协议发送给HQServer，然后HQServer将数据存入数据库。</SPAN>

这一点和Hyperic HQ 的Agent有很大的区别：HQ Agent只负责数据的采集，将采集到的数据通过HTTP协议发送给HQServer，然后HQServer将数据存入数据库。

    OSSIM Server接收到的每一个事件都是被某个Agent事先处理过的，即便是当一个Server只有**另外一个Server**（被设计用来只负责转发数据的server）和他链接时（即该server不和Agent直接链接，而是和别的Server链接），那个处在这个链接链的最后的那个Server的数据肯定也是某个Agent处理后发送过来的。

注释代码 [复制代码](http://liu-hliang.javaeye.com/blog/827398)

1. <SPAN style="COLOR: #ff00ff">老外的上面这段话有点绕，概括一下就是：Server中的数据信息归根到底肯定是由某个Agent事先处理后发送过来的，即便该Server不和任何其他Agent直接相连接！
2. 通过这段话我们也可以得出结论：OSSIM网络中，Server和Server是可以互联的，也就是说Server既可以作为Server也可以作为Agent？</SPAN>

老外的上面这段话有点绕，概括一下就是：Server中的数据信息归根到底肯定是由某个Agent事先处理后发送过来的，即便该Server不和任何其他Agent直接相连接！

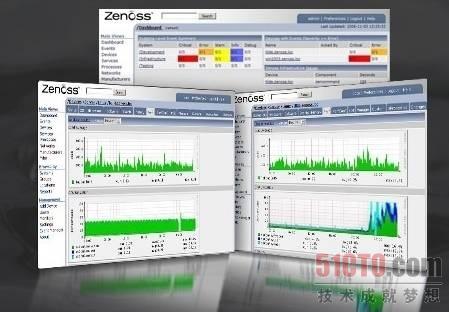
通过这段话我们也可以得出结论：OSSIM网络中，Server和Server是可以互联的，也就是说Server既可以作为Server也可以作为Agent？

    OSSIM Agent发送给Server的数据，绝大多数情况下是通过读取网络设备终端中的日志文件得来的。OSSIM有计划将来会实现从其他类型的数据来源（如DB或Socket）中读取数据信息。

    Agent和Server的连接断掉后，Agent便不能将事件发送给Server了，但是Agent会将这些事件入栈(stacks)，当连接重新建立后Agent会自动将这些事件按照到达的顺序发送给Server端。

附录:10款免费的企业级安全监控工具

**1. Zenoss**



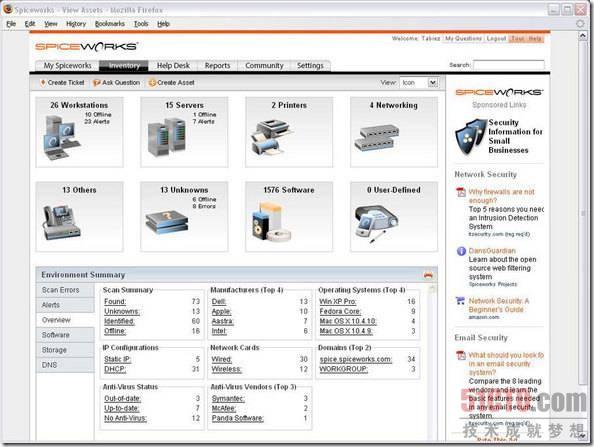
Zenoss是一款企业级开源服务器和网络监控工具，它最引人注目的是虚拟化和云计算监测能力，其它年老的监测工具很难看到具备有这个功能。

**2、OSSIM**



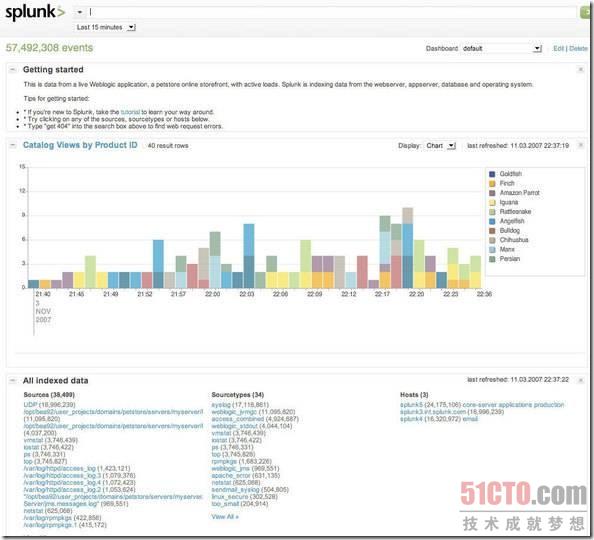
OSSIM是Open Source Security Information Management（开源安全信息管理）的缩写，它具有完整的SIEM功能，提供了一个开源检测工具程序包和一个关联引擎，旨在减少分析部门繁重的任务。

**3、Spiceworks**



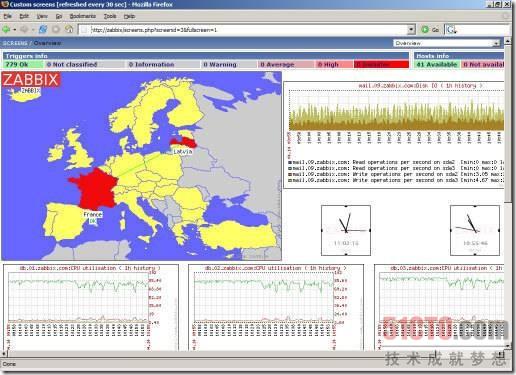
Spiceworks是一个坚实的IT网络和系统管理引擎，附带了安全监控功能，让中小型企业可以独立监控应用程序和系统，在问题扩大之前提供警告。

**4、Splunk**



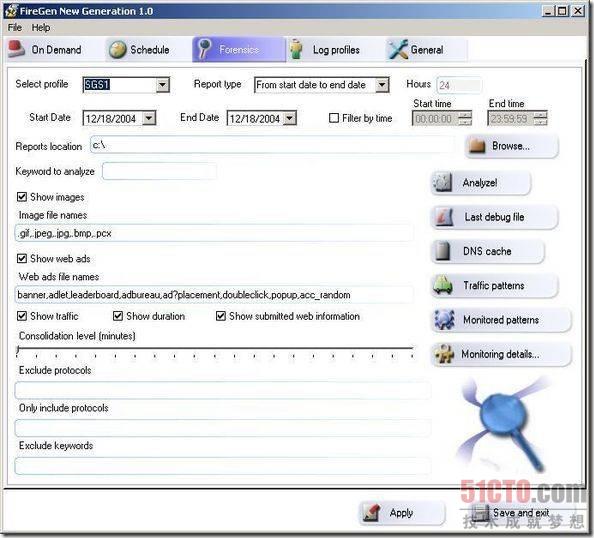
Splunk是一款日志收集和分析工具，让管理员可以浓缩应用程序、网络设备和服务器等的监控数据，以便需要时提交可作为证据的报告，但免费版本每天只能收集500MB日志。

**5、Zabbix**



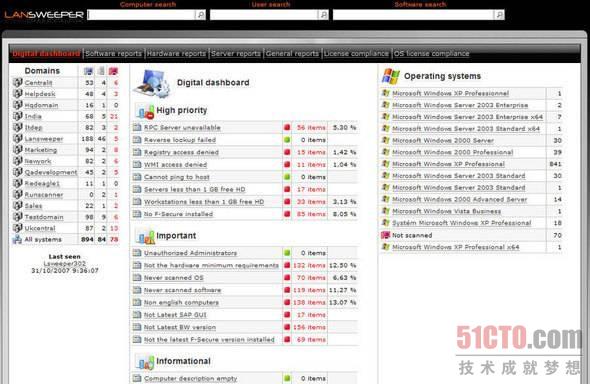
你可以使用Zabbix跟踪网络设备、服务、服务器和应用程序进行传统的安全日志记录和分析，还可以进行性能管理和容量规划。

**6、FireGen**



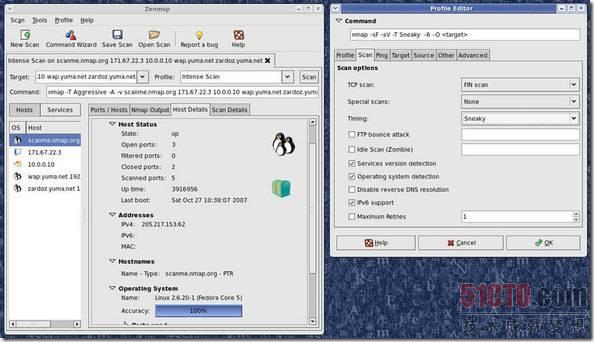
分析主流防火墙厂商的防火墙日志，如思科，瞻博，SonicWall，Fortigate和赛门特克，它可以识别和解释记录的事件，为枯燥的数据注入了更多有意义的信息。

**7、LANSweeper**



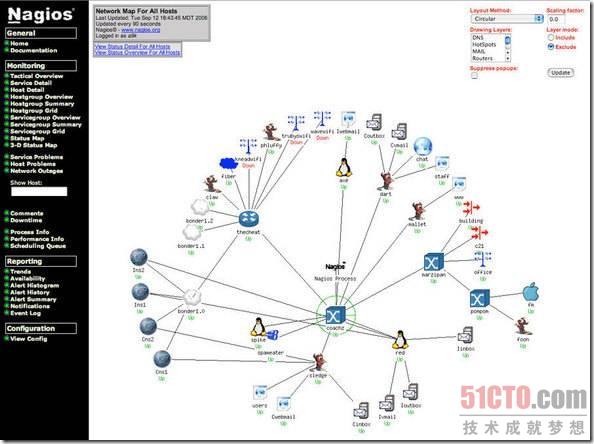
你不能监测你不知道的资产，使用LANSweeper可以更好地看到你网络中的硬件和软件资产，LANSweeper是一个开源的，无代理的扫描仪，可以帮助你更好地监测打下坚实的基础.

**8、Nmap**



Nmap虽然上了年纪了，但一样充满活力，它允许管理员跟踪异构网络中的设备清单，管理服务升级计划，监控主机和服务正常运行时间.

**9、Nagios**



Nagios是一款功能齐全的开源网络管理和监控工具，它提供了网络服务，主机资源监控和网络探测能力，支持远程运行脚本监控和通过加密隧道实现远程监控。

**10、OSSEC HIDS**



和所有操作系统保持兼容，OSSEC HIDS属于基于主机的入侵检测系统，提供日志分析，完整性检查，Windows注册表监控和rootkit检测，提供了基于时间的报警和积极响应。