SANS

WHAT WORKS™

借助思科 Stealthwatch 增强关键安全控制措施的成效，推动安全性提升

主办方

CISCO™

WhatWorks 是一项用户互助计划。通过该计划，拥有高效互联网安全技术实施经验的安全管理员可以讲述他们部署该技术的原因、该技术的工作方式、该技术如何提高安全性、他们所面临的问题，以及他们的经验总结。您是否也有真实案例想要分享？或者您有什么想要了解的产品？请告诉我们。

www.sans.org/whatworks

关于 Erie Insurance 公司

九十多年来，Erie Insurance 公司一直恪守对客户的承诺，本着诚实、正直、服务至上和价格适度的原则，提供车险、房屋保险、商业保险和人寿保险服务。他们的产品为客户提供了可靠的保护。他们凭借庞大的独立保险代理人网络，为美国 12 个州和首都华盛顿的 400 多万保险客户提供服务。在这些代理人的努力下，Erie Insurance 公司矢志不渝地践行创立时的宗旨：“以最低的成本为我们的投保人提供近乎完美的保障和尽可能完善的服务”。

关于用户

Jamison Budacki 是一名高级信息安全架构师，于 2011 年加入 Erie Insurance 公司。Jamison 在 Erie Insurance 公司主要负责开发可用的安全架构，以及可在整个企业网络中使用的监控和检测解决方案。在业务合作伙伴的协助下，他每天致力于从人员、流程和技术的角度开发符合要求的安全解决方案。加入 Erie Insurance 公司之前，Jamison在某财富 100 强公司的事件响应团队中担任安全工程师。他于 2005 年在印第安纳大学信息与计算机学院获得信息学学士学位，于 2007 年取得 CISSP 认证并持续至今。他目前与妻子和两个儿子居住在宾夕法尼亚州的伊利市。

关于采访者

John Pescatore 是 SANS 的新兴安全趋势总监。

Pescatore 先生于 2013 年 1 月加入 SANS，在计算机、网络和信息安全领域拥有 35 年经验。他曾在 Gartner 担任了 13 年首席安全分析师，与全球 5000 家公司及主要技术和服务提供商有过合作。在于 1999 年加入 Gartner 之前，他是 Entrust Technologies 公司和 Trusted Information Systems 公司的高级顾问，负责组建、发展和管理专注于防火墙、网络安全、加密和公钥基础设施的安全咨询团队。更早之前，他曾在 GTE 公司工作了 11 年，从事于安全计算和电信系统的开发工作。Pescatore 先生的职业生涯始于美国国家安全局（从事安全语音系统的设计）和美国特勤局（从事安全通信和监视系统的开发）。他拥有康涅狄格大学电气工程学士学位，是一名 NSA 认证的密码学工程师。他还是一名业余无线电爱好者，呼号是 K3TN。

摘要

通过一系列审核、渗透测试和自我评估，Erie Insurance 公司的高级信息安全架构师确信，公司要想加快检测、应对和解决网络威胁的速度，必须提高情景感知能力。为此，该公司开始集中精力寻找可在安全团队与网络运营团队之间共享的工具，以求加强协作和工作协调。在评估了若干产品后，Erie Insurance 公司最终选择了思科 Stealthwatch，继而在多项安全指标上得到改善（包括提高了覆盖效率，实施了 CIS 关键安全控制措施等）。

问 首先，请您介绍一下个人背景和您在 Erie Insurance 公司的职务。

答 我叫 Jamison Budacki，是 Erie Insurance 公司的高级信息安全架构师。我来这家公司已经快有五年了。我负责为公司制定信息安全方针，确保企业在注重安全性的同时实现未来的发展目标。在此之前，我在一家财富 100 强公司的事件响应团队作为信息安全工程师工作了五年。

问 作为一名 InfoSec 架构师，您是否直属于首席信息安全官?

答 我目前在企业架构团队工作。每天都要与信息安全部门打交道。企业架构部门和信息安全部门都直属于首席信息安全官。

问 是什么问题或什么原因促使您寻找像 Stealthwatch 这样的解决方案?

答 我们需要提高整个网络的情景感知能力，尤其是对远程分支机构位置的洞察力。我们以前使用的工具集存在很多问题，下面是其中的一部分：

存在的问题	期望的目标
同时使用多种工具	减少查找信息所需的时间
信息过多	提高效率，有效利用时间
需要手动执行关联	缩短补救时间
主动警报和报警功能较差	优化平均获知时间 (MTTK)
数据保留能力有限	延长历史数据保留时间
不能兼容其他技术	利用兼容性提高价值
不支持用户属性	获得用户和设备的信息

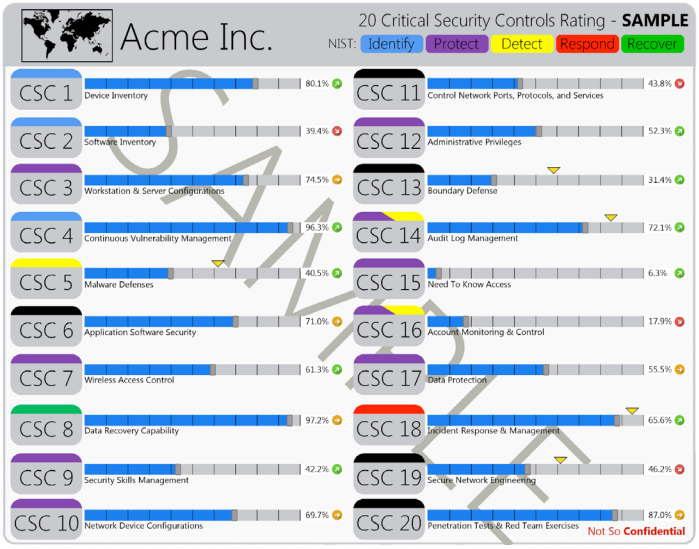
问 通常安全部门可能会购买和使用自己的一些工具，网络运营部门也会使用自己的一些工具。安全部门能否在一个整合的视图中查看整个网络的运行情况？还是说两个部门各自为政？实际情况是怎样的?

答 以前，两个部门是完全独立的。但在最近几年，我们开始与网络团队密切合作。通过相互协作，我们逐渐对一些事情有了深入的了解。这归功于结合使用 NetFlow 和 Stealthwatch，以及部署思科 ISE 并将其集成到现有流程和技术中。最近的协作确实使两个团队都受益良多，我们可以分享技术和想法，从而共同提高。

问 您在寻找解决方案时应该意识到，您最终不得不支出一笔费用。您如何获得这笔预算，或者说您如何说服管理层？您要开展的是一项专门的计划，还是只是架构改进计划的一部分？您如何证明这笔预算的合理性?

答 我们事先进行了大量渗透测试，这些测试围绕着相似的主题，而且有力地证明我们需要在网络分段以及监控和检测功能等方面做出改进。为了解决这些问题，我们采用了 CIS 关键安全控制措施（版本 5.1）。我们针对 20 项控制措施进行了自我评估，以便了解我们在各项控制措施上的实际得分。在购买新的信息安全技术或执行信息安全计划时，我们会详细了解相关技术，并根据 CIS 关键安全控制措施对其进行评估。我们会询问自己：“这样做是否有助于提高我们的自我评估分数？”Stealthwatch 提供的分析和功能对我们的自我评估分数有极大的影响。

为了方便大家了解我们的方法，我们用下面的记分卡来展示一家虚构公司在实施 Stealthwatch 前后，自我评估分数的变化情况。蓝色条和每项控制措施右侧的百分比表示虚构公司 Acme, Inc. 实施 Stealthwatch 前的分数。黄色三角表示实施后的自我评估分数。



- CSC 5：恶意软件防御能力提高 21%。
- CSC 13：边界防御能力提高 27%。
- CSC 14：审计日志的维护、监控和分析能力提高 13%。
- CSC 18：事件响应和管理能力提高 7%。
- CSC 19：安全网络工程能力提高 15%。

几年后，我们又对NIST 网络安全框架执行了相同的过程。与前面的 CSC 记分卡一样，我们设计了下面的记分卡来反映我们的 NIST 网络安全框架自我评估结果。同样，蓝色条表示实施 Stealthwatch 前的成熟级别，黄色三角表示实施后的成熟级别。Stealthwatch 对检测功能有显著的影响，对响应功能有中等程度的影响，对识别和保护功能也有一定程度的影响。最后，我们向记分卡中添加了两部分内容：“主要里程碑”和“针对性目标”。“主要里程碑”部分着重展示自我评估期内表现出色的方面；“针对性目标”部分列出下一个评估期内需要完成的工作。重要的是，这两部分内容要用商业术语来写，因为记分卡可能会提交董事会，用于回答诸如“我的信息安全团队工作得怎么样？”这样的问题。

除了显著提高我们的自我评估分数外，Stealthwatch 还缩短了我们的平均获知时间 (MTTK) 和平均响应时间 (MTTR)。不仅如此，Stealthwatch 还能与其他调查工具集成，在操作层面提供更出色的事件洞察力，并帮助我们全面了解网络所有区域的情况。

问 看来你们有一个不错的开端。能否介绍一下你们在评估和寻找理想解决方案时使用的流程？

答 最基本地，我们制定了一系列对我们至关重要的标准。然后，我们调查了相关领域的多家供应商，并参加供应商网络研讨会来了解每家供应商的能力。在缩小范围后，我们与挑选出的少数几家供应商进行了更深入的讨论。最后，我们在实验室环境中进行了概念验证。在这个过程中，我在以前的公司积累的 NetFlow 技术相关经验起到很大作用。

问 在进入概念验证阶段之前，你们比较了几家公司？

答 最初，我们使用了思科和 Plixer 两家公司的商业产品，以及一些开源程序。有些产品因为不能满足我们的部分要求，所以很快就被我们淘汰了。当时，我们有一些想要实现的用例，于是就对思科 Stealthwatch 解决方案进行了全面的实验室测试。其中一个用例是利用 Gigamon 创建数据流。这是 Gigamon 的一项新功能，我们希望确保我们能获得预期的效果。第二个用例是测试新的防火墙代码，以便实现我们所需的 NAT 拼接功能。

问 你们最重要的前两项或前三项标准是什么？

答 我们最重要的标准一是可扩展性，二是与其他工具的兼容性。前面我曾提到，我们有很多想要集成的工具，例如 SIEM、Gigamon、IP 地址管理、思科 ISE 和思科 ASA 防火墙。此外，我们还使用了二级防火墙和无线入侵检测传感器。

我们迫切希望实现的用例就是 NAT 拼接，以及从我们已有的防火墙日志中提取某些用户属性的能力。在兼容性方面，我们希望实现的主要用例是沿用我们现有的 Gigamon 基础设施。我们需要使用 Gigamon 的 SPAN 会话、重复数据删除和 NetFlow 记录创建功能。所以对我们来说，Gigamon 基础设施几乎是我们所有 NetFlow 的起点，只有少数几个防火墙除外。

问 我们来总结一下您的情况：你们使用 Gigamon 向 Stealthwatch 馈送 NetFlow 数据，在很大程度上依赖 SIEM/报告功能，而且你们拥有 IP 地址管理数据。那么你们用什么处理用户属性这样的信息？又是用什么将这些信息联系在一起呢？

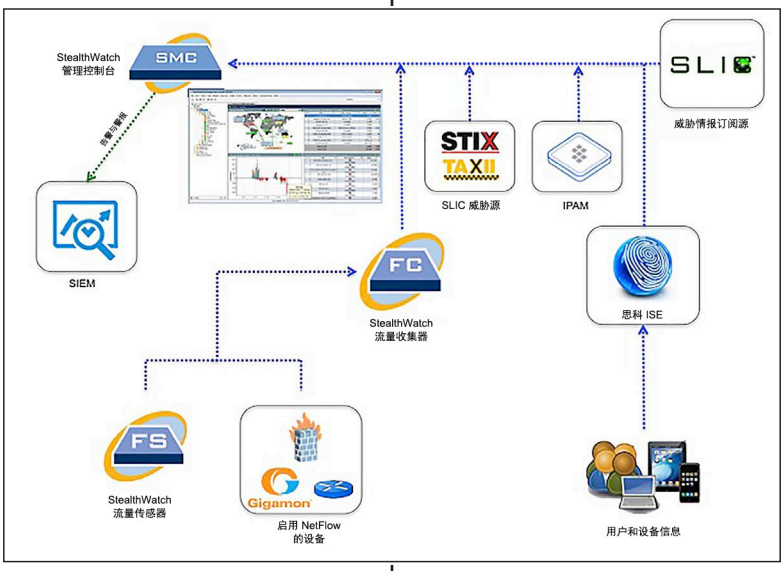
答 确实，用户属性也是我们的要求之一。为此，我们正在着手部署思科 ISE。这有助于为我们已经做出的决定提供有力支持，因为思科 ISE 能够与 Stealthwatch 解决方案集成，提供我们所需的用户属性。通过这种集成，我们可以轻而易举地在 Stealthwatch 中搜索用户。今后，我们将尝试在某些情况下根据 Stealthwatch 规则自动实施补救措施。例如，如果某个客户端正在尝试访问已知的不良站点或渗漏大量数据，我们可以将该客户端发送到补救 VLAN，以限制它的网络访问活动并做出补救，等问题解决后再将它送回生产环境。

ISE 与 Stealthwatch 的集成对利用用户属性以及更深入地了解网络设备很有帮助。现在，我们能在所查看的数据流中提取用户名信息。我们还能获得 MAC 地址、设备操作系统和设备制造商等信息，从而提高了对设备的可视性。这些附加的用户名和设备信息均直接来自 ISE 集成。

问 您曾提到，可扩展性是你们最重要的标准之一。那么，你们预期的部署规模和部署范围是多大？或者说，所要部署的网络节点、用户或位置的数量是多少？

答 Erie Insurance 公司大约有 5000 名员工，以及近 18000 名独立代理人和支持人员。代理人不在我们的网络中，但他们会与我们的系统进行交互。我们的目标是让我们的网络尽可能多地覆盖到这些人员。我们目前每秒处理大约 20000 个数据流，这些数据流包括网络上的所有流量：工作站到 DMZ/数据中心的流量、DMZ/数据中心到工作站的流量、工作站到外部的流量，以及 DMZ/数据中心到外部的流量。现在，我们正在评估工作站之间的流量。

问 是不是无论你们在哪里使用了 Gigamon 功能，都能将 Gigamon 数据转发到 Stealthwatch？还是说，虽然你们使用了 Stealthwatch，但是也必须添加其他 SPAN 端口，或者添加原来没有的其他监控功能？



答 我们基本上使用 Gigamon 来创建 SPAN 会话，删除重复的流量数据，并创建 NetFlow。这些 NetFlow 记录会被转发到 Stealthwatch 收集器。我们还从防火墙（内部和外部）中获取 NetFlow 数据。这不仅为我们提供了更多用户属性，而且为我们提供了两种防火墙所具备的某些 NAT 拼接功能。NAT 拼接减少了我们看到的流数量。拼接会将公共互联网 IP 地址和我们的内部 IP 地址合并到单个流记录。这使我们能够看到具体是哪个主机存在问题，而不仅仅是 NAT 地址。

问 能否介绍一下从决定使用 Stealthwatch 到目前为止，你们经历的整个过程？你们是如何进行部署的？部署过程用了多久？

答 和通常情况一样，最长的阶段是签订各种合同和协议。完成这一步后，部署很快就能完成。我们使用现有的技术和 Stealthwatch 解决方案进行了大量前期测试。我们使用 Stealthwatch 分析来自 Gigamon 的数据流，以确保我们能够将所需的数据提取到思科和我们的实验室环境。由于当时我们是第一批从 Gigamon 创建 NetFlow 的公司之一，所以有很多专家参与了实验室测试，验证是否一切正常。在我们仔细完成所有测试工作后，解决方案在短短一周内就部署完毕。整个过程十分简单：将数据流发送到收集器，设置所有硬件和部分虚拟映像。

问 据我们所知，Stealthwatch 由三个组件构成：管理控制台、流传感器和流收集器。那么，收集器是否为物理设备，你们能否将控制台作为虚拟软件来运行？具体运作方式如何？

答 实际上，我们是以虚拟机的形式运行 Stealthwatch 管理控制台，以物理硬件的形式运行流收集器和流传感器。我们目前的监控对象包括数据中心、各个 DMZ、园区，以及全部 25 个分支机构位置。借助 Stealthwatch，我们能够深入了解过去无法监控的网络区域。

问 什么人负责查看控制台并执行所需操作？是身为架构师的您，还是运营人员，还是很多人一起？

答 是很多人一起。网络团队用 Stealthwatch 取代了已被淘汰的传统工具。他们还使用 Stealthwatch 进行容量规划、制定 QoS 策略，并在出现拥塞时确定最大流量生成者。

不过，Stealthwatch 主要还是由 InfoSec 团队使用，是执行各种调查（DDoS、感染、数据泄露、策略违规）的主要工具之一。为了确保 InfoSec 工作取得成功，我们学会了在处理新的流程或技术时询问自己四个主要问题：

1) 我们面临的威胁是什么？

2) 我们需要监控什么？

3) 这对 Erie Insurance 公司有何帮助？

4) InfoSec 如何进行事件响应？

我们面临的威胁是什么？

我们通过多种方法来了解我们面临的威胁，其中包括执行风险评估和利用威胁情报。我们利用的威胁情报多种多样，例如，我们订阅了 Stealthwatch 实验室情报中心 (SLIC) 威胁数据源，并加入了各种信息共享组织，我们还会根据以前的事件自己创建威胁情报，同时积极利用开源情报 (OSINT)。

我们需要监控什么？

我们根据企业重视的问题来制定监控决策，所采用的依据是内部业务影响分析报告。此外，我们还监控现有策略、存在风险的资产、任何与互联网相关的信息，以及合规性/法规遵从性。

这对 Erie Insurance 公司有何帮助？

这个问题涉及自我衡量。为了解答这个问题，我们会依据 CIS 关键安全控制措施和 NIST 网络安全框架进行自我评估。

InfoSec 如何进行事件响应？

我们有响应流程手册，其中列出了处理事件的具体步骤。此外，我们还有指导在发现已知警报时如何行动的手册，以及指导如何在网络中寻找恶意迹象的预防性手册。这些手册会不断改进，以便帮助我们衡量各种事件，并将今后发生的事件与过去出现的事件关联起来。这些手册也有助于我们将科学方法引入基于想象的事件响应措施中。

问 我们再来谈谈警报和针对警报的响应措施。你们是否有人使用 Stealthwatch 控制台来查看各种警报，并进行调查？还是说这些警报会被转发到 SIEM，由您来处理？

答 两种情况兼而有之。我们会通过邮件收到一些警报，然后我们会直接在 Stealthwatch 上进行调查。所有已触发的警报都会被发送到 SIEM，以便我们将其添加到关联性搜索库中，以备将来使用。我们可以结合终端漏洞或终端警报等其他数据来审视这些警报。对于不是直接从 Stealthwatch 进行的其他调查，这些警报也很有帮助。

问 根据你们当前的成就和过去的经历，在您看来有没有什么让您不满意的地方，或者您有没有什么经验要分享给那些想要借鉴你们经验的人？

答 要说经验，不得不提的是大家一定要寻找一种可供企业重复使用的解决方案。如果解决方案能被多个团队接受并采用，那么让管理层接受它将不再是难事。所以应该寻找一种能够巩固和补充现有流程与技术的解决方案。与网络团队合作很重要。我最初加入 Erie Insurance 公司时，两个团队之间的协作并不多，这是我最想立即改变的事情。我们也确实做到了这一点。现在，有了良好的关系做保障，我们可以互相利用对方的技术，让工作更加顺畅。另一个经验是，大家可以使用自我评估及安全框架来验证计划的有效性，并展示计划的进展情况。例如，我们使用的是 CIS 关键安全控制措施和 NIST 网络安全框架。最后一点是，大家应询问供应商他们如何根据您选择的框架提供完整的解决方案。让他们证明您是不是有理由购买他们的解决方案。

问 现在有个口号是“了解您的网络”。在这方面，你们尝试以用户属性为突破口。但是很多时候，人们在尝试识别特定计算机及特定用户时，往往会遇到“我们的计算机命名方式或目录结构化方式存在问题”等难题。你们是不是也必须解决这样的问题？

答 在一定程度上是这样。我们的用户名并不便于手动识别。例如，分析师在查看用户名时，并不能很容易地认出：“哦，这是 Jamison。”不过，我们只需要把警报和用户名发送到 SIEM，警报中便会自动填充实际的人员姓名。这是通过对所需的用户存储库进行 LDAP 查询来实现的。像这样的操作都是在后台执行。同样，识别计算机名称也不是难事。思科 ISE 会自动提取计算机名称、MAC 地址和设备制造商，并将这些信息添加到 NetFlow 记录。

问 你们目前已将 Stealthwatch 和 ISE 结合到一起，你们能否主动进行网络访问控制和隔离？比如，分析师会收到并查看警报，然后作出决策？

答 现在，我们有一名分析师负责查看警报并作出决策。此外，我们也在使用网络设备的 802.1x 功能作为处理自带设备访问的方式。我们还使用了安全状况评估和设备分析功能。我们希望能根据 Stealthwatch 检测到的特定警报或活动实现自动响应。实际上，我们利用手册来指导流程。

现在，我们有一套非常好的关于警报的基础手册，专门用于说明如何处理各种警报。我们计划在下次更新手册时进一步完善指导如何主动寻找问题的手册。我们要求分析师每天一上班就坐下来浏览这些手册。他们需要仔细阅读手册，并尝试寻找可能的恶意迹象来帮助主动发现问题。为此，我们鼓励分析师执行新的关联搜索、发现新的策略违规情况，并生成新的控制面板报告。

问 在运维方面，Stealthwatch 是否需要由全职员工管理？Stealthwatch 人员的职务可不可以由分析师或其他安全人员分担？

答 我们的环境是一个中等规模环境，需要一名全职员工把自己一半的管理时间放到 Stealthwatch 上。也就是说，可能需要有半个全职员工来负责管理、更新和增强该工具，并根据需要添加更多信息源，确保它始终保持最新状态，从而保证解决方案运行良好。分析师每天都会使用它。在进行调查时，我首先要做的工作之一就是从 Stealthwatch 中提取相关资产的流信息。

问 我们再来谈谈 Stealthwatch 的支持。你们在部署时是否使用了支持服务？从运行 Stealthwatch 以来，你们是否使用了相关的支持服务？

答 就我的体验而言，支持服务是有求必应。可以确定的是，他们在过去几年里一直在努力加强客户支持，而且也确实拥有这样的能力。他们非常乐于尽一切努力帮助我们找到答案或解决问题。有时，他们甚至会在节假日、下班后或周末与我们联系，以确保一切正常。过去几年里，Stealthwatch 团队不仅在改善客户支持方面取得了成效，而且通过客户社区门户扩大了支持服务的范围。他们提供的传授知识的文章以及各种讨论对研究很有帮助，与 Stealthwatch 相关的培训让新员工入职变得更加容易。这些培训专门面向

Stealthwatch 客户，可按需提供。最后需要提到的是，我们还参与了测试计划。这项计划使我们可以在不属于我们的生产实例的环境中测试我们今后可能希望使用的新代码或新功能。

问 你们最初购买该解决方案是在什么时候？

答 大约两年以前。

问 这么说，你们在思科收购 Lancope 之前就购买了该解决方案。那么在收购期间，该解决方案是否收到任何影响？在收购完成后，思科是如何提供支持和响应服务的？

答 没有任何影响。虽然发生了收购，但是他们在业务上没有任何变化。从客户服务的角度来看，我没有感觉有任何影响。

问 你们有没有在功能方面对思科 Stealthwatch 团队提出过任何请求或要求，比如“如果产品能加上某种功能就更好了”？

答 他们非常擅于紧追最新的技术和集成趋势。我最希望他们做到的是，他们能一直使产品不限定于某个供应商，能不断与其他多家供应商合作和多种产品互相兼容。

问 你们是否需要进行任何类型的网络调查分析式的分析活动？你们是存储流数据，还是存储警报并置之不理？你们是否会为了进行某种类型的调查分析而存储网络流或数据包捕获信息？

答 数据保留是我们的要求之一。不过有了数据包捕获能力，这方面的要求不在话下。我们曾希望保留至少 120 天以前的流数据，但实际上我们能保留 1 年以上的流数据。当我们查找和挖掘过去的数据时，这种能力确实很有帮助。比如说，“如果我们在六个月之前就受到感染，我们能知道吗？”是的，我们有能力追溯并查看数据，这对我们非常有益。

问 你们是通过 Stealthwatch 还是通过集成其他产品来做到这一点的？

答 是通过 Stealthwatch。我们能保留一年左右的流数据，这也是我们选择 Stealthwatch 的主要原因之一，因为它能满足我们在数据保留方面的需求。这样，我们就不用忧心忡忡地使用开源工具，因为它们在可扩展性和数据保留方面常会出现问题。Stealthwatch 用于存储流信息的数据库和压缩技术真的非常出色。我们选择 Stealthwatch 的另一个原因是，在出现硬件故障时，我们完全不必构建新系统、在上面设置软件以及进行各种配置。他们会寄来一个新硬件，我们只需恢复备份即可应用所有当前配置。

问 你们未来有什么计划？

答 进一步加强与 SIEM 的集成和自动化操作；丰富情报源；完善 ISE 部署，以便充分利用与 Stealthwatch 的交互功能，例如网络访问隔离。