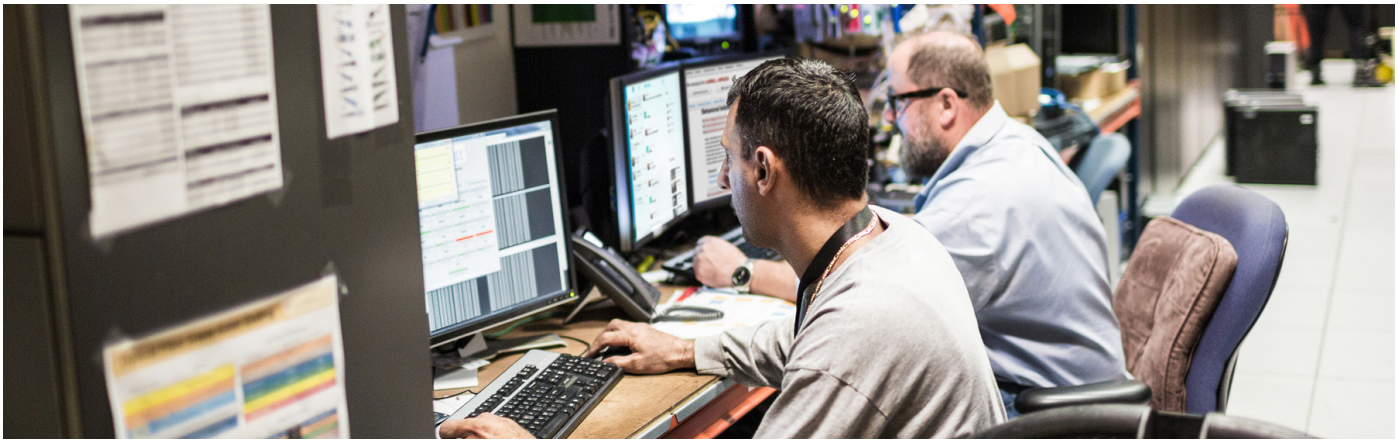
案例研究

利用思科 Stealthwatch 提升可视性和安全性



执行摘要

客户名称： Erie Insurance

公司所在地： 美国宾夕法尼亚州伊利市

员工数量： 5000 以上（另有 12000 名独立代理人）

“借助 Stealthwatch，我们能够深入了解过去无法监控的网络区域。

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。”

Jamison Budacki
Erie Insurance
高级信息安全架构师

存在的问题 – 缺乏网络可视性

Erie Insurance 是一家总部位于美国宾夕法尼亚州伊利市的上市公司，提供车险、房屋保险、商业保险和人寿保险服务。该公司成立于 1925 年，秉承客户服务高于一切的宗旨。如今，Erie Insurance 业已成为一家美国财富 500 强公司，拥有 5000 多名员工、12000 名独立代理人和 500 万份保险合同，其客户遍布美国 12 个州和哥伦比亚特区。

该公司的 IT 团队通过一系列审核、渗透测试和自我评估后意识到：公司需要通过提升网络可视性来加快威胁检测和事件响应速度。

Erie Insurance 高级信息安全架构师 Jamison Budacki 表示：“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。”

他解释说，他的团队以前使用的工具集存在很多问题，其中包括：

- 由于工具种类过多、信息量太大且需要手动执行大量关联才能找到正确的数据，导致威胁检测和响应速度变慢
- 数据保留能力有限
- 不能兼容其他技术

扩展网络洞察力，提升响应速度

Erie Insurance 求助于思科 Stealthwatch™ 解决方案来解决这些问题。通过收集和分析 Erie Insurance 现有网络基础设施中的 NetFlow 数据，Stealthwatch 可提供端到端可视性和安全情报。

现在，Stealthwatch 不仅用于监控公司的园区、数据中心、各个隔离区 (DMZ) 和全部 25 个分支机构位置，同时也是公司安全分析师的每日必用工具。

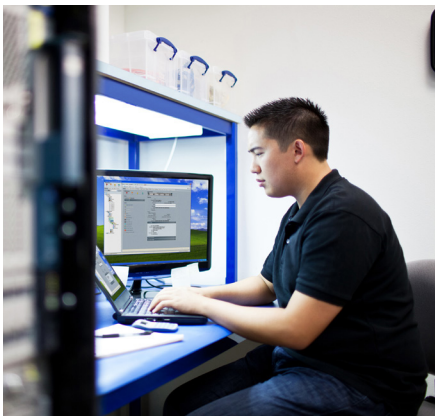
Stealthwatch 是 Erie Insurance 安全团队在执行任何类型的调查期间使用的主要工具之一 – 无论是用于 DDoS 攻击、恶意软件感染、数据泄露、策略违规还是其他方面。

CIS 关键安全控制措施和 NIST 网络安全框架都是该公司安全策略的组成部分。Stealthwatch 提高了该公司针对每个相应框架的自我评估分数。

Budacki 表示：“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。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。”

他补充说道：“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。”

通过产品集成实现全方位的安全性



Erie 已将 Stealthwatch 与其他工具（SIEM、Gigamon 基础设施和多个思科® ASA 防火墙等）进行了集成以提供更加无缝的安全性。该公司还将 Stealthwatch 与思科身份服务引擎 (ISE) 进行集成，从而获得网络活动的用户属性。

Budacki 表示:“通过这种集成，我们可以轻而易举地在 Stealthwatch 中搜索用户。ISE 和 Stealthwatch 的集成在用户属性，以及获得对网络设备更深层次的洞察力方面发挥了极其重要的作用。”

未来，Erie 计划通过修复决策的自动化来扩展 StealthWatch 与 ISE 的集成。例如，如果 Stealthwatch 检测到异常用户行为，便可将命令发送到 ISE，从而隔离该用户。

Stealthwatch 的新增优势

对于 Erie，Stealthwatch 部署可提供以下新增优势：

提升安全团队和网络团队之间的协作

Budacki 表示：“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，我们可以相互利用对方的技术，让工作更加顺畅。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。”

长期保留数据以优化调查分析

过去，Erie 的目标是保留至少 120 天以前的流数据，现在借助 Stealthwatch，他们能保留 1 年以上的流数据。

产品

安全

- 思科 Stealthwatch
- 思科身份服务引擎 (ISE)
- 思科 ASA 5525-X 和 5545-X 自适应安全设备

利用 NAT 拼接提升可视性

Budacki 表示：“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，而不仅仅是一个 NAT 地址。”

有效的客户支持和培训

Budacki 指出，Stealthwatch 支持团队非常乐于尽一切努力帮助 Erie 找到答案或解决问题。他还表示为 Stealthwatch 客户提供的培训使 Erie 的新员工入职变得更加容易。

借助思科安全，Erie Insurance 能够更好地继续为数百万客户提供堪称典范的服务。Budacki 表示：“借助Stealthwatch，我们能够深入了解过去无法监控的网络区域。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。”

相关详细信息

本案例研究基于系统网络安全协会 (SANS Institute) 开展的一项长篇问答。打开如下链接访问完整访谈：http://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/cisco-erie.pdf。

如需了解更多有关思科 StealthWatch 和 ISE 的信息，请访问 http://www.cisco.com/go/stealthwatch 和 http://www.cisco.com/go/ise。

美洲总部
思科系统公司
San Jose, CA

亚太总部
Cisco Systems (USA) Pte. Ltd.
新加坡

欧洲总部
思科 Systems International BV 阿姆斯特丹
荷兰

思科在全球设有 200 多个办事处。思科网站 **www.cisco.com/go/offices** 中列有各办事处的地址、电话和传真。

C36-738691-00 03/17