检测并抵御内部威胁

前美国国家安全局合同员工爱德华·斯诺登将机密信息泄露给主流媒体的事件，引发了公众对内部威胁危害性的重视。这不无理由。

内部威胁是最难检测的威胁之一，而且可能会导致大量敏感数据泄露。据 Forrester Research 公司的一项报告显示，36% 的数据泄露事件是由于员工偶然的数据使用不当所导致的，25% 的数据泄露事件是由于恶意内部人员滥用数据所导致的，因此数据泄露的首要原因在于内部人员。

对于经常接触机密信息的政府机构来说，其危害尤为明显。由于丢失机密数据会导致严重后果，因此许多组织都按照联邦法规的要求监控、缓解并记录所有内部威胁活动。

无论是针对粗心大意的员工或恶意内部人员，还是针对破坏合法凭证的外部人员，许多组织都尚未建立能够有效解决内部攻击的安全计划。对抗内部威胁的最佳方法是在早期将它们检测出来。为此，安全人员需要无处不在的网络可视性和深入的行为分析。

利用可视性和行为分析将网络转变为传感器

由于内部人员享有一定的特权，因此他们往往能够避开众多安全措施。而外部攻击者则必须首先考虑如何获得受保护网络的访问权限。内部人员访问敏感数据的权限是组织主动给予的。随着自带设备 (BYOD) 办公的兴起，人们越来越多地使用个人设备进行工作，员工甚至可以从家中使用智能手机访问数据。要对抗这些威胁，防御者需要采用不同的安全措施。

[1] Forrester Research 报告，《了解数据安全和隐私状态：2013 年至 2014 年》（2013 年 10 月）

检测并抵御内部威胁

要检测内部威胁，您需要依托于全面的内部网络可视性和安全分析。其中一种方法是使用思科® Stealthwatch 大量收集和分析 NetFlow 及其他类型的安全数据。借助 Stealthwatch，您可以充分利用您现有的网络基础设施来识别可能代表内部威胁的行为。

例如，如果某个用户收集超大量的数据或尝试访问受限网段，则意味着该用户可能准备窃取敏感信息。同样，如果某个用户突然向本地打印机发送大量流量，则意味着该用户可能正在将机密文件复印到纸上以避开边界安全保护措施。如果有内部威胁或外部攻击在网络中扩散，Stealthwatch 可以检测到与其相关联的横向运动。

若缺乏内部网络可视性，则很难在出现数据泄露后发现这些活动，更不要说进行调查。但仅有可视性还不够。如果无法存储、整理数据，并将其转化为切实可行的情报，就不可能发挥可视性的真正优势。

Stealthwatch 强大的分析功能可以快速地处理网络流量数据，识别可疑和异常的行为。主要途径是收集既有设备中的 NetFlow 和其他网络元数据。这样便可有效地将网络转变为功能强大的安全传感器。您无需花费巨额成本部署监控设备，便可获得端到端可视性。

完成数据收集后，Stealthwatch 会将这些数据修整为简化的数据对象，然后使用专有算法确定正在发生的活动。它会突出显示所有可能构成威胁的事件（见表 1），这样安全人员便可在出现重大损失之前避免这些事件的发生。

遵从联邦政府关于内部威胁方面的规定

联邦机构对于防止内部威胁有强烈的紧迫感。他们必须保护机密信息的安全性，同时满足合规要求。Stealthwatch 具有高级异常检测功能以及对 NetFlow 活动的可视性，能够帮助政府机构遵从与内部威胁相关的政策。通过使用 Stealthwatch 监控网络流量，并持续执行可提供丰富信息的审计追踪，可满足“第 13587 号行政命令”和“情报体系标准 500-27”等法规的合规要求。

作为一项强制要求，美国国防部 (DOD) 和其他一些美国政府机构必须制定专门的计划来防范内部威胁。不仅如此，根据《国家工业安全计划操作手册》的要求，数以千计的政府承包商也必须建立内部威胁防范计划。然而，情报和国家安全联盟 (INSA) 网络委员会的内部威胁工作组表示，许多此类组织都未建立内部威胁程序，并且大部分组织都存在严重的缺陷。

过去十年里，由恶意内部人员造成的国家安全机密信息泄漏事件超过 120 起。[2]

[2] CMU，http://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_427430.pdf，2014 年 4 月

检测并抵御内部威胁

通过情景感知加快威胁检测速度

即使拥有了内部网络可视性，也可能无法看到内部威胁。攻击者可以分散地在多台设备上、多个时间范围内进行操作，从而隐藏其活动。识别可疑行为并不能起到很大作用，除非您可以将其与某特定用户联系起来。事实上，Ponemon Institute 的研究表明，在确定内部人员是否构成威胁时遇到的最大障碍在于缺乏安全工具提供情景信息。[3]

表 1. 可能构成威胁的异常行为

活动	说明
未经授权的访问	用户尝试访问网络中禁止访问的资源。
策略违规	员工使用的服务违反组织策略且可能绕开组织监控。
内部侦测	用户对网络进行扫描。(内部人员在提取数据之前必须先对其进行盘查。)
可疑的数据收集活动	用户开始收集超大量的数据。
针对性数据收集活动	用户从某特定主机上提取大量数据。
可疑的数据丢失情况	若有特权用户向网络外部发送超大量数据，表明可能存在数据泄露行为。

案例研究：Stealthwatch 增强联邦网络的安全性

鉴于网络攻击日益复杂且越来越受到广泛关注，联邦机构清楚地意识到仅按照最低要求遵从联邦法规的规定并不足以保护其重要资产。

Stealthwatch 的自动监控、设立基准和报警功能使该机构从中受益。Stealthwatch 不依赖于签名更新，即可发现复杂的零日攻击并检测内部威胁，包括策略违规、网络滥用、设备配置错误和数据泄露等。

Stealthwatch 的高级安全功能可简化故障排除过程，显著提升保护能力。这些功能也有助于增强合规性，对事故调查的网络调查分析起到辅助作用。这些创新功能包括：

- **对整个网络的全面持续监控**可提升可视性
- **行为异常检测功能**可加快内外部威胁的故障排除过程，而无需通过更新签名来检测攻击
- **关注指数**可对组织面临的首要安全问题进行自动优先级排序
- **自动缓解功能**使得 IT 管理员可快速控制安全问题
- **蠕虫病毒跟踪器**可直观地显示恶意软件在整个网络中的传播状况，以便立即掌握传播范围和影响
- **主机组锁定功能**可限制与敏感系统的通信
- **身份感知功能**可准确找出问题负责（或受影响）人员
- **网络调查分析功能**可对调查起到促进作用

最重要的是，Stealthwatch 为该组织增添其所需的“耳目”，促使流程不断改进，从而保护其机密资产的安全。该系统使现有的安全部署得到增强，从而更快速地检测事件，更及时、敏捷地响应事件。

请于此处阅读完整案例研究：www.lancope.com/csusfed

[3] Ponemon Institute 研究报告《特权用户的滥用行为和内部威胁》（2014 年 5 月）

检测并抵御内部威胁

Stealthwatch 可提供多层安全情景。管理员可明确掌握用户的活动，并做出明智的决策。此情景包括以下内容：

- **用户身份：**将网络活动与负责的用户联系起来对于内部威胁识别至关重要。
- **设备感知：**设备信息有助于识别未授权或不安全的设备，以及快速识别可能被入侵的设备。
- **应用级别可视性：**通过查看哪些应用正在使用中有助于准确地对攻击和恶意程序进行定位。
- **威胁源数据：**此数据有助于识别与已知恶意主机交互的用户或设备。

一些高级攻击可能需要一年或更长时间才能发现。在此期间，它们潜伏在网络中，造成严重破坏。额外的安全情景层可显著减少各种威胁的检测时间 (TTD)。

通过调查分析发现攻击范围

识别到安全威胁后，必须对网络被入侵的过程进行调查，更重要的是必须调查有哪些数据已被获取。除非您存有网络事务记录，否则很难进行。NetFlow 本身就可能产生大量的数据，要想有效地存储这些数据可能比较困难。但 Stealthwatch 可以简化数据流，大大降低对数据的要求，而不会丢失重要信息。因此，Stealthwatch 用户可以存储数月甚至数年的流量数据以实现更全面的调查分析。

Stealthwatch 具有高度可扩展性，即使对于最大规模的企业，也可满足其需求。Stealthwatch 每个收集器的分析速度高达 24 万个数据流/秒 (fps)，总体速度达到 6 百万个数据流/秒。Stealthwatch 管理控制台提供直观的用户界面。可以轻易地利用一系列参数查询数据流记录，并查看与调查相关的元素。

当今众多企业都面临一系列威胁，但很少有企业已准备好处理内部攻击。Stealthwatch 在利用深入的网络可视性和情景感知安全分析来检测内部威胁方面具有极其出色的性能。您可以对各种威胁进行监控、检测、分析和响应，从而避免造成无法挽回的损失。

相关详细信息

有关思科 StealthWatch 的更多信息，请访问：

http://www.cisco.com/c/en/us/products/security/stealthwatch/。

(08/23/16-r02)