适用于联邦组织的思科 Stealthwatch

思科 Stealthwatch™ 技术在民用领域以及国防部和情报体系中得到广泛部署。机构可通过该技术持续监控网络的行为异常和高级威胁。

凭借从网关到主机级别的网络可视性，思科 Stealthwatch 为政府组织提供了切实可行的安全情报，以协助它们更快地做出更明智的决策。在加快事件响应和调查分析的同时，思科 Stealthwatch 可防止代价高昂且有破坏力的数据泄露。

借助于思科 Stealthwatch，您可以：

- 通过经济高效地将您的网络转变为功能强大的安全传感器，将您的现有设备用于检测复杂的攻击
- 快速发现与零日漏洞相关的可疑行为、高级持续性威胁 (APT)、内部威胁和其他复杂的定向攻击
- 在导致灾难性的数据丢失之前阻止攻击，从而保护敏感信息
- 对网络中所有的会话建立并维持一个轻量级且情景丰富的记录，以协助调查分析

思科 Stealthwatch 是国土安全部持续诊断和缓解 (CDM) 计划第 3 阶段的一个基础性事件响应解决方案。Stealthwatch 支持 CDM 的方式：

- 在 Stealthwatch 中提供本地集成功能以实现感知和快速响应，从而通过关注可视性和情景，识别、防止和报告关键网络安全攻击特征 (IOC)。
- 与关键 CDM 技术集成，以实现安全自动化并改进威胁检测和关联，从而实现无处不在的网络可视性和安全性，以加强威胁防御和事件响应。
- 与获批准的系统集成商密切合作，这些集成商在美国联邦总务管理局 (GSA) 一揽子采购协议 (BPA) 下出售 CDM 程序组件和系统。

思科 Stealthwatch 可提供内部可视性

借助思科 Stealthwatch 实现网络即传感器

水平网关

（受信任的互联网连接和计算机网络防御运营商）

实现整个安全栈网关中网络连接的透明性，并提升安全运营中心 (SOC) 的功能。

整个网络

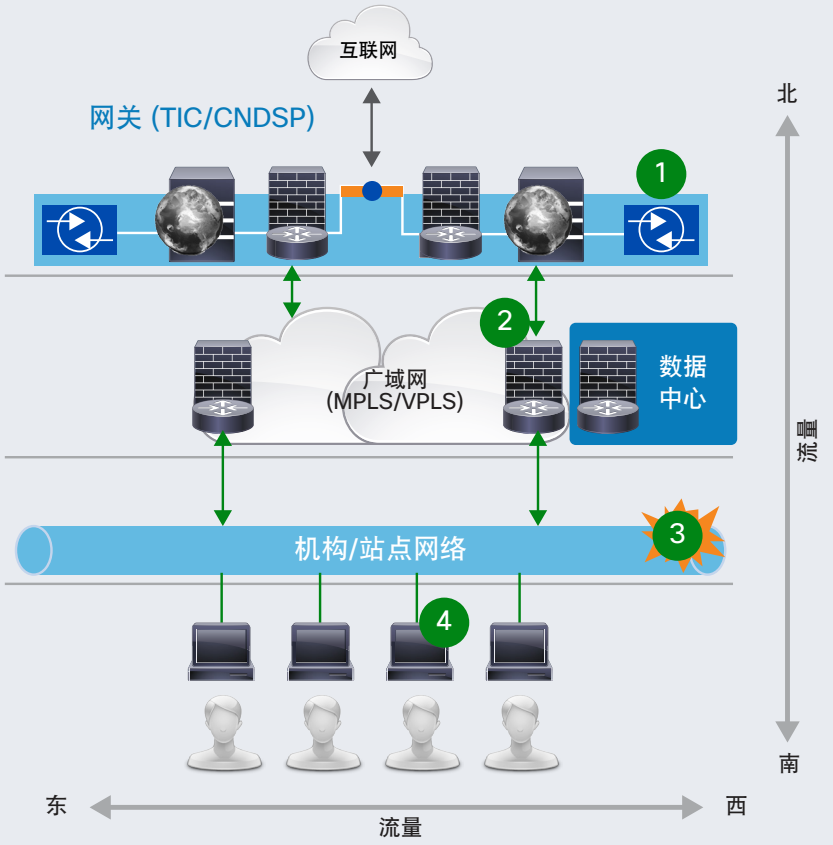
通过流收集确定内部流量的最终源，了解网络行为并提升网络运营中心 (NOC) 的功能。

在网络中横向移动的流量

了解您网络环境下的用户行为以发现可疑活动和检测内部威胁、APT 和 DDoS 攻击。

主机

通过内部终端主机属性和用户身份验证对内部用户进行跟踪，看是否存在策略违规行为和异常活动。



1 TIC 持续监控

观察网关基准活动以分析正常行为和检测异常活动。填补关键的安全监控缺口。监控并验证通过 TIC 和托管受信任互联网协议服务 (MTIPS) 的网络活动的比例。

2 垂直透明性

延长详细流记录的存储时间，以在网络间隙和网关处获得重要的可视性。通过分析大量的拼接、去重处理后的 1:1 流，以充分发挥流数据的作用。

3 事件响应

获取所有网络活动的全面审计追踪，包括到主机和终端级别的设备、身份、位置、应用和时间详细信息。快速分析并访问大量网络和安全数据中的详细信息。

4 横向可视性和行为异常检测

通过您现有网络检测复杂的内部攻击。为正常用户行为确立基准，以便快速地识别和调查异常。检测内部威胁，包括未经授权的访问、数据收集和数据丢失。

C22-737930-00 10/16