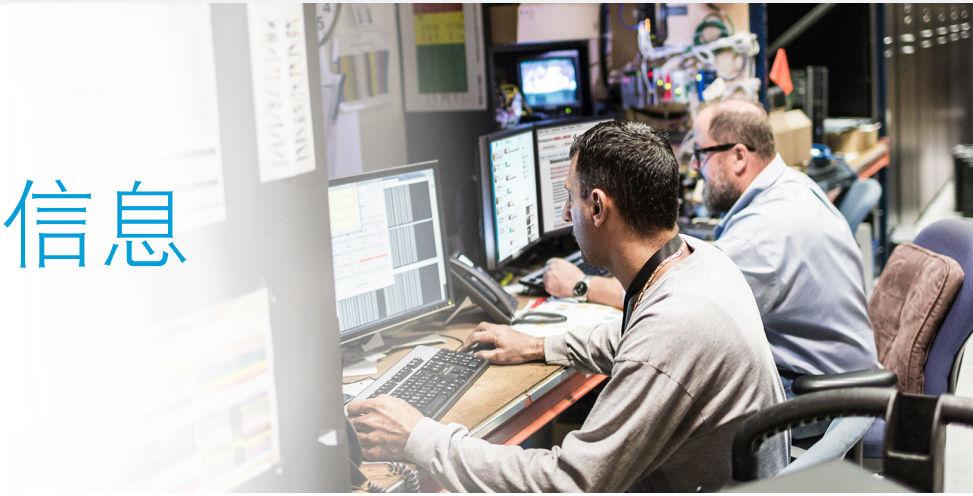
# 思科 Stealthwatch 系统信息事件管理集成服务



## 优势

- 通过显示可疑的 IP 地址活动（例如通过 IP 地址最常访问的目标（对等设备））获得对网络的深度可视性。
- 识别使用的协议，量化传输的数据量，并确定通信时间以帮助检测威胁性异常网络行为。
- 创建顶层摘要报告（例如顶层对等设备（IP 目标）、顶层对话和顶层服务），以便您可快速总结大数据集，并以直观、可用的方式接收数据。
- 简化与系统信息事件管理 (SIEM)（包括 Splunk、QRadar、ArcSight、LogRhythm、AlienVault 等）的集成，以便您能够将实施时间从几周缩短到几天，并节约宝贵的资源。

SIEM 集成通过基于流量的信息增强了传统的 SIEM 数据源，以便您可更深层次地了解网络。其结果是解决事故的成本和复杂度降低，并通过更好的可视性改善整体安全措施。通过将 SIEM 与 Stealthwatch 集成，可支持合规性计划，加强事故调查的网络调查分析，并显著提高网络和应用的可用性和性能。

思科® Stealthwatch 安全事件和事故管理系统集成服务通过将警报通知与流量数据结合，围绕潜在威胁提供额外情景，以便客户可以对威胁进行分类并采取相应的行动。通过将警报通知与思科 Stealthwatch 流量数据汇聚，SIEM 集成服务可对与可疑 IP 地址相关的网络流量实现快速而完整的描述。

该服务还支持接收任何安全系统(入侵防御系统 (IPS)、数据包捕获 (PCAP))的警报通知，SIEM 将通过与标准具象状态传输 (REST) API 集成以自动查询 Stealthwatch。因此，客户可获得用于主机调查的必要数据，并针对可疑主机采取规避措施。该数据可显示在 Stealthwatch 控制台或传输到另一个系统（视安全协议而定）。

## 利用 Stealthwatch 获取整个情景和对 SIEM 设备的可视性

该服务包括：

在 SIEM 控制台内获得对网络中异常 IP 活动的可视性，这是威胁检测功能的一个重要部分。将任何 SIEM 解决方案集成到 Stealthwatch 实例可使您的安全团队通过简单地点击按钮打开 Stealthwatch 窗口来调查来自 IDS、IPS 或安全堆栈中的其他解决方案的警报。点击操作，调查即开始。通过 Stealthwatch 窗口，安全团队可以回看关键信息详情

- 导致警报触发的对象
- 已传输的数据量
- 警报发生时间
- 主动警报涉及的应用

该信息以思科专业服务团队创建的丰富数据元素集提供。可配置获取这些关键报告的逻辑：

- 顶层主机
- 顶层对等设备
- 顶层对话

当您采用此服务时，我们的专业服务团队将为您提供对这一关键数据的独占访问权，缩短对抗高级威胁的平均状态掌握时间 (MTTK)。

## 后续行动

要了解有关思科安全服务的更多信息以及我们的 Stealthwatch 部署服务如何使您的企业受益，请联系您当地的客户代表或经授权的思科分销商。有关思科如何帮助您的组织防护当今不断变化的威胁的更多信息，请访问 www.cisco.com/go/services/security。


C45-736856-00 05/16