

思科 Stealthwatch 主机组 自动化服务



优势

- 处理不断更改 IP 地址的动态服务器行为。对于动态配置思科 Stealthwatch 以将策略应用于这些自动化动态主机组，主机组自动化必不可少。
- 主动管理与第三方威胁源的集成。需实时更新不断变化的 IP 地址，以便在与恶意主机通信时，减少错误警报。
- 当您的系统与配有动态 IP 地址的第三方应用服务器交互时，您需要主机组自动化服务来确保其正确配置。
- 优化思科® Stealthwatch 性能并减少操作开销，以在减少错误、多余警报和多余作业通知的同时，降低运营成本。
- 自动化主机组更新，使 Stealthwatch 以最佳效率运行，从而实现最佳保护以免受各种威胁。

自动化主机组创建以获得精细可视性

Stealthwatch 主机组自动化服务使客户以逻辑方式对网络资产进行归类以提高可视性和控制力。此服务用于：

- 优化 Stealthwatch 系统性能和自动管理特定地址 IP 池。
- 通过降低 Stealthwatch 的整体运行成本和减少假阳性警报来减少团队资源的过度消耗。当发出警报时，在确定要进行调查方面，安全团队具有很高的可信度。
- 自动化主机组同步。当可以保持准确的分组时，我们可确保用户已按公司政策正确分配。

可以按照逻辑工作组、地理位置、组织、工作职能和许多其他方式对网络和用户进行分段，这使富有远见的组织可严密监控流向每个组的网络流量。例如，对重要公司资产分组可使 Stealthwatch 监控出入这些资产的流量，并对所有异常活动发出警报。自动化主机组提供了常规和可重复方法用于返回主机组环境中出现的任何异常报告。

自动化主机组用于精确的 Stealthwatch 定制

思科 Stealthwatch 主机组自动化服务采用来自可信赖的 IP 地址管理系统的数据对 Stealthwatch 主机组进行定期更新。该服务将以一组可定制的工具和脚本交付，我们的专业服务工程师将根据您的独特环境对这些工具和脚本进行定制。将 Stealthwatch 主机组与您的网络基础设施保持同步可减少开销，并有利于优化 Stealthwatch 的运行。

自动化主机组是使 Stealthwatch 保持最佳运行状态，且使您的网络安全人员接收到及时、无错误数据的理想方法。所有这些都将是缩减运营开销，并避免浪费安全团队时间的假阳性警报，自动化主机组使安全人员可接收更准确的警报，因此，在判断警报为有意义的事件的方面具有较高的可信度。

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。