思科安全咨询服务

主动威胁搜索

当今瞬息万变的威胁形势

如今，网络攻击空前活跃，而安全人才却日益短缺，这让许多组织难以抵御网络威胁。思科 2017 年度安全报告显示，仅有 53% 的公司认为“他们有良好的系统用于验证安全事件是否实际发生”。

现在，世界各地的组织已经意识到，如果只是坐以待毙等待风险通告，或者更糟糕的，等来的是执法机构或其他外部实体，告诉他们其环境中的事件已经将他们置于危险境地。类似于渗透测试，必须进行演练才能发现网络中的薄弱之处。主动执行搜索，发现现有网络中的隐患，可以做到未雨绸缪，也是评判网络健康状态的真正的衡量标准。

只有 43% 的首席信息安全官真正认为“能够轻松确定感染的范围，加以遏制并进行修复”

优势

- 通过主动寻找和解决未知问题加强安全状态。
- 对您的网络中真实发生的状况（包括对您的运营工作和基础设施上有更好的可视性以及更深入了解）更有信心。
- 联系富有经验的事件响应专家（他们长年从事于解决各类事件）。
- 在解决事件的过程中，可以使用思科各种工具套件增强威胁的可视性，从而更加快速、全面地了解网络中的所有威胁。

案例研究：财富 500 强零售企业

挑战

- 客户对其电子商务网站在零售假日季来临之前以及当中的情况感到忧心忡忡。
- 虽然客户自己有一支团队，但他们不想从日常运行中分散注意力，于是采用 CSIRS 来主动寻找其电子商务环境中存在的危害情况。

解决方案

- 在为期六周的合约里，思科与客户紧密合作，部署了必需的技术、搜索危害情况、确定持久机制并阻断发现的危害。
- 思科的工作还包括在剩余假日期间监控环境，直到确定网站中没有目标明确的攻击者。

成果

- 安装并部署了思科的行业技术，提供更好地可视性，让您在保护运行环境时更感可靠。
- 在基础设施内找到客户传统 AV 解决方案无法捕获的各类商业恶意软件。

并非所有组织的情况都相同

并非所有组织的情况都相同。利用最新情报、多年的经验、世界级思科技术和最佳做法，思科安全事件响应服务 (CSIRS) 团队将与您携手合作，设计出为您量身定做的搜索计划，该计划将定义约定范围、确定可视性的覆盖情况以及存在的隐患、部署获得全面可视性所需的专有思科技术、利用最新情况评估环境、分析调查结果并提供包含调查结果和优先处理建议的最终报告。在危害评估过程中，CSIRS 在对各种调查结果做出响应的过程中还可以扮演主导或辅助角色。

让我们的专家与您合作，确定您的组织目前是否受到攻击。

主动搜索

确定范围和搜索设计：我们将与您的团队一同确定搜索重点，其属性是广泛、有限范围还是目标明确。根据搜索重点，规划覆盖这些范围所要采用的合适工具和方法。

部署技术：根据需要，我们将在环境中部署所需的技术，并对其进行配置和调整。

搜索：制定好计划并做好环境准备后，我们将使用多种方法来寻找环境中存在的危害。

最终报告：服务结束时，我们会提供一份报告（内容包括事件摘要、回顾、调查结果和建议）。

后续行动

请访问 www.cisco.com/go/securityservices，立即联系我们的顾问，为您的企业提供保护。