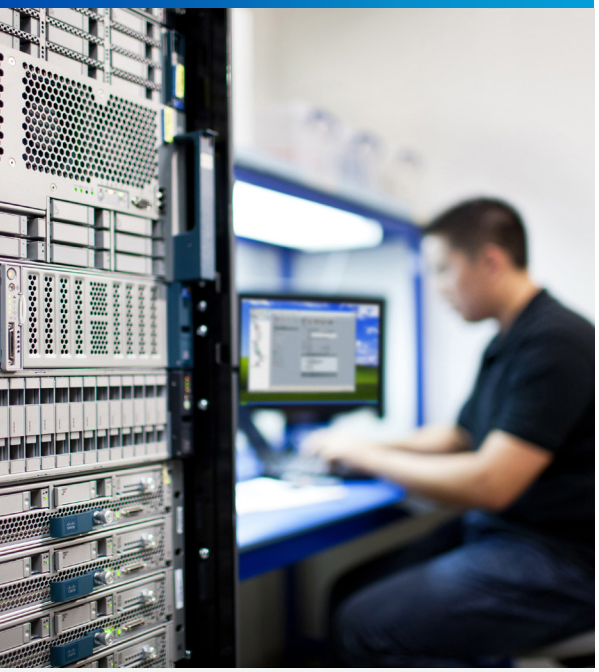
威胁
管理能力



优势

- 通过全面的方法做到时刻准备和及时响应，从而改善安全状态
- 通过经过验证的方法、独特的情报和经验丰富的团队提供持续的保护，从而增强信心
- 通过使用创新技术和专家广泛持续的分析提高可视性，并加深对运营和基础设施的了解

思科安全咨询服务
事件响应

组织随时面临攻击风险。根据 IDC 调查，2014 年安全漏洞导致的损失接近 5000 亿美元。同时，《思科 2015 年年度安全报告》中指出，全球安全专业人才严重短缺，预计有 100 万个缺口。

当今瞬息万变的威胁形势

人才的短缺加上安全事件的增加，导致大多数组织的安全状态普遍堪忧。成功的攻击会造成巨大的经济损失、知识产权受损、客户信息和信心受影响并降低企业估值。

思科® 安全事件响应服务可显著增强网络和信息安全防御。利用最新情报和最佳做法，它引入了一个涉及所有防御层的流程，并提供能够帮助组织快速有效地进行事件准备、管理、响应和恢复的各种功能。

只有 50% 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，防止事态进一步扩大”

– 思科 2015 年年度安全报告

通过准备与响应增强安全状态

思科® 安全事件响应服务是思科咨询安全服务中的一个解决方案，利用该方案提供的专业知识可以评估和设计促进业务增长、降低成本、缓解风险的安全方法。通过综合最佳实践和利用有效的行业安全框架，思科事件响应团队可以提供全面的功能来帮助组织。我们的事件响应团队由信息安全专家组成，并且这些专家具有执法、企业安全和技术安全等领域的独特背景。我们的团队直接与综合安全情报 (CSI) 小组合作，识别已知和未知威胁，量化风险和划分优先级，并降低未来的风险。

让我们的专家与您一起制定新计划、重新评估现有计划，或在攻击中提供快速帮助。

准备：主动式服务

- **基础设施漏洞准备情况评估：**通过评估网络设计、安全控制、操作系统、人员安全配置、自动化补丁系统、防火墙、日志记录和其他相关系统，思科对客户环境有了深入的了解，并能够预测潜在攻击和推荐必要的安全控制措施。
- **安全运营准备情况评估：**通过根据之前的事件以及当前的角色和职责对安全团队的准备情况进行评估，思科可就您的组织是否拥有进行各种调查所需的资源、知识和工具提供相应建议。
- **运营准备情况评估：**通过评估运营模式和活动，提供有助于未来活动的建议。
- **漏洞通信评估：**思科可帮助建立起具有适当合规结构的通信框架，在董事会级别、组织的供应链之间以及外部与客户的合作之间提供一致的认识和响应。
- **安全运营和事件响应培训：**提供在领导、协调和支持事件方面的最新技能培训。此外，思科还可向安全运营人员提供恶意软件分析和各种安全工具方面的技术培训。

响应：被动服务

- **评估和调查：**通过对受感染的系统进行技术检查，确定攻击方法，汇总出恶意代码的详细信息，包括其轨迹、目标和最终目的。
- **应对措施的制定：**制定应对措施，以帮助检测、隔离、跟踪和停止攻击者的进一步行动。进一步行动可能造成危害表现、信息泄漏和漏洞被利用的情况。
- **应对措施的部署：**部署所制定的所有应对措施，帮助检测和停止事件，并且所有这些应对措施均符合信息安全和供应商最佳做法。
- **应对措施的验证：**验证新部署的应对措施的有效性，并就设计中任何需要改进之处编制绩效评估。输出包括针对董事会、监管机构和执法机关的文档，详细说明事件摘要、缓解措施和损失情况（如果适用）。

案例研究

案例研究：零售公司

挑战

客户遭遇入侵，他们缺乏安全专家来响应高级威胁，并且基础设施无法阻止恶意软件。

解决方案

在为期七天的合作中，思科通过网络取证调查、恶意软件样本分析、恶意软件应对措施的制定、网络异常检测和全面的情报审查，提供定制的恶意软件检测功能。

结果

- 针对终端恶意软件、传输中的数据以及基础设施内的整体通信功能，提供相关数据，形成稳定的安全状态。
- 在基础设施内找到客户的传统 AV 解决方案无法捕获的各类商业恶意软件。
- 利用揭露安全缺陷、错误配置、应用缺陷（与安全相关）的解决方案，提高对网络的可视性。

思科的事件响应可能包括以下任一或所有隔离和补救攻击的措施：

- 日志来源评估
- 分析和数据挖掘
- 取证调查图像分析
- 受感染系统动态监测
- 恶意软件逆向工程
- 漏洞利用分析和重新实施

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。