



# 事件响应和漏洞发现合作伙伴计划

## 寻找思科合作伙伴事件响应和漏洞发现实践生态系统

每天都有心怀不轨的人攻击各公司的企业网络防护，频繁造成灾难性和产生重大影响的后果。大多数公司都没有配备相关人员、流程或设备来快速全面地识别和修复这些漏洞，致使公司自身暴露于更大的伤害和未来的漏洞之中。提供事件响应和漏洞发现服务的专家公司可以帮助这些公司识别是否遭到攻击（漏洞发现）或者对攻击进行分类、遏制和清除（如果已遭到攻击）。这些专家接受过工具和方法方面的培训，一经通知即可提供这些服务。

思科提供不断发展的专家合作伙伴生态系统，当我们的客户需要这些服务时，他们可以通过该系统与这些专家合作伙伴联系。事件响应合作伙伴计划使思科安全技术合作伙伴计划 (CSTA) 得到增强，为搜索思科安全产品组合的补充产品提供了单独的平台。客户可从更全面和整合的安全解决方案中受益。事件响应和漏洞发现合作伙伴计划提供了资源，我们的客户可以在该资源中查找事件响应和漏洞发现实践。所有这些公司在使用思科安全产品时都雇佣了专家。

## 后续行动

要找到符合条件的思科事件响应和漏洞发现合作伙伴，请访问 <http://www.cisco.com/c/en/us/products/security/partner-ecosystem.html>。

## 优势

- 节省时间 - 提供单一来源供您寻找思科合作伙伴事件响应和漏洞发现实践
- 确保使用思科高级威胁解决方案的合作伙伴提供的专家可帮助对威胁进行识别、分类和遏制
- 利用最新威胁情报确定漏洞的程度
- 修复受影响的系统
- 防止未来出现的漏洞

“超过四分之一的 IR 专业人员 (26%) 对其组织当前的 IR 功能表示不满意，称其为无效功能。”

系统网络安全协会 (SANS Institute)