

解决方案概要

Sophos MDR

专家主导的威胁调查

Sophos Managed Detection and Response (MDR) 是一项全天候提供的全面托管式服务, 由专门侦测和应对瞄准您的计算机、服务器、网络、云工作负载、电子邮件帐户等的网络攻击的专家所提供。使用 Sophos MDR, 我们的专家团队能够阻止先进的人工主导的攻击, 并在攻击中断业务运营或入侵您的敏感数据前采取即时行动来加以消除。

实用案例

1 | 全天候威胁监控

期望结果: 通过拥有能够代表您应对威胁的专家, 扩展您的 IT 和安全团队。

解决方案: 我们拥有熟练技术的专家全天候监控、调查和响应威胁, 执行即时的、人为主导的响应行动, 以阻止已确认的威胁。Sophos 雇有 500 多名威胁侦测和响应专家, 由七个全球安全运营中心 (SOC) 提供支持。

2 | 加速威胁响应

期望结果: 改善对已确认威胁的平均响应时间 (MTTR)。

解决方案: Sophos MDR 分析师可以代表您执行威胁响应行动, 以阻断、遏制和消除攻击者, 平均威胁响应时间为 38 分钟, 比行业基准快 96%。

3 | 拦截安全工具未能识别的威胁

期望结果: 侦测的网络威胁数量超过安全工具本身的识别能力。

解决方案: 65% 的勒索软件攻击始于攻击者利用合法用户凭证或未知漏洞, 而 29% 则始于泄露的凭证。Sophos MDR 分析师执行主动威胁搜索, 以识别只有人类才能侦测到的攻击者行为, 并迅速消除仅靠工具无法阻止的威胁。

4 | 提高投资回报

期望结果: 整合来自您整个环境的安全技术, 从您的技术投资中获得更多的投资回报。

解决方案: Sophos MDR 可以提供您所需的技术, 或者充分利用您已有的第三方网络安全技术投资来侦测和响应威胁。通过采用一种互联的技术方法, 收集和关联来自最常用的安全产品的安全数据, Sophos MDR 能够过滤掉杂讯和多余的安全警报, 并以快速、准确和高透明度消除已确认的威胁。



评级最高、评论最多的 MDR 服务, 以及获评 Gartner “客户之选” 托管式侦测和响应服务



由 G2 上的客户评价和评论所评定的整体最高评级的托管式侦测和响应服务



在 MITRE ATT&CK 托管式安全服务评估中表现顶级的厂商

了解更多, 获取一个定制服务建议

Sophos MDR:
www.sophos.com/MDR

© 版权所有 2023。Sophos Ltd. 保留所有权利。注册于英格兰和威尔士, 注册编号 2096520, 地址: The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, 英国。Sophos 是 Sophos Ltd. 的注册商标。所有其他提及的产品和公司名称均为其各自所有者的商标或注册商标。

Gartner Peer Insights 标志是 Gartner, Inc. 和/或其附属公司的商标和服务标志, 在此获得许可后使用。保留所有权利。Gartner Peer Insights 的内容由个人最终用户根据自己与平台上所列厂商的合作经验发表的意见组成, 不应被视为事实陈述, 也不代表 Gartner 或其附属机构的观点。Gartner 不认可本内容中描述的任何厂商、产品或服务, 也不对本内容的准确性或完整性做出任何明示或暗示的保证, 包括对适用性或特定用途的适用性做出任何保证。

2023-12-19 SB-ZHCN (NP)

SOPHOS