SOPHOS

销售与技术 FAQ – Sophos Emergency Incident Response

外部 FAQ

综述

什么是 Emergency Incident Response（紧急事件响应）？

当您遭遇网络安全紧急事件时，Sophos Emergency Incident Response 会迅速为您提供支持，评估事件、遏制威胁、分析原因并提出修复建议。我们的跨职能专家团队凭借多年实战经验，快速分流、隔离并消除活跃威胁，驱逐攻击者以避免损失扩大。

此外，该服务还能帮助您判断贵组织是否受到事件的影响，并厘清其影响范围。服务内容包括各种调查活动，以识别该事件发生的根本原因、进行入侵评估以判断观察到的行为是否恶意、开展威胁狩猎与威胁情报提供，并在需要时协助进行赎金谈判。

Emergency Incident Response 服务适用于哪些客户？

适用于所有正在经历安全事件、近期遭受攻击且需要进一步调查，或遇到可疑活动、需要确认是否存在威胁的组织。

我必须是 Sophos 的客户才能购买该服务吗？

不。Emergency Incident Response 为现有和非 Sophos 客户提供。

我正在遭遇入侵事件，该怎么办？

请随时拨打下面的地区电话，联系我们的事件顾问 (Incident Advisors)。

- 澳大利亚：+61 272084454
- 奥地利：+43 73265575520
- 加拿大：+1 7785897255
- 法国：+33 186539880
- 德国：+49 61171186766
- 意大利：+39 02 94752 897
- 瑞士：+41 445152286
- 英国：+44 1235635329
- 美国：+1 4087461064

请发送邮件至 EmergencyIR@sophos.com 联系我们。

Emergency Incident Response 是远程还是现场服务？

我们同时提供远程和现场两种服务选项。

Emergency Incident Response 服务有多快？

大多数客户可在 2 小时内入驻，并在 48 小时内分流。由于服务完全远程进行，因此在您首次联系 Sophos 后，即可在数小时内开始响应。

多快可以开始入驻流程?
Emergency Incident Response 团队在收到客户批准后即可开始入驻流程并启动调查。

Emergency Incident Response 服务采用什么方法论?
在您接受服务协议后，我们将召开项目启动会议。如您要求，也可通过电子邮件进行。我们在了解您此项目的目标后，会立即开始调查。

Emergency Incident Response 包含多个工作类别，我们都可向客户提供。我们会在最初的范围界定电话会议中，与您共同确定所需的服务类别和预估的工作时长。

涵盖的工作类别包括：项目管理、事件响应、数字取证、入侵评估、威胁狩猎、威胁情报与研究、赎金谈判、项目报告、现场支持（如适用）、商务邮件受骇（BEC）调查、软件部署等。

Emergency Incident Response 服务支持哪些语言?
目前该服务的支持语言为英语和日语。您必须具备良好的英语或日语技术沟通能力。

Sophos 会与其他数字取证与事件响应服务（DFIR）公司协作处理问题，还是取而代之?
Emergency Incident Response 本身就是一项 DFIR 服务。无需额外聘请第三方安全公司进行 DFIR，因为通过 Emergency Incident Response 提供的该服务范围，可涵盖数字取证。

我是否必须在端点上安装 Sophos 技术?
不需要。我们的团队可以通过 Sophos XDR 提供 Emergency Incident Response，或者可以将 Sophos XDR 传感器与您现有解决方案并行部署。无论是哪种情况，我们都能快速启动事件调查。

Emergency Incident Response 团队不需要等待部署完成，就可以开始采取补救措施，隔离和消除威胁。团队将利用任何现有数据，借助适合辅助响应的工具。

如何报价?
Sophos 会根据范围界定问题，预估响应此次事件所需的工时。您只需为实际使用的工时付费。

有任何额外费用吗?
如果您要求提供现场服务，则将向您收取差旅费用。

我们可否在环境的一部分上部署 Emergency Incident Response，还是整个环境必须纳入服务范围的一部分?
在某些特定情况下，Emergency Incident Response 可以仅应用于您的部分环境。Emergency Incident Response 专家可在界定范围时说明详情。

Sophos 可以与代表我方的中间人（如律师事务所）合作签署合同吗?
可以，我们支持与中间人合作。

Sophos 能确定哪些文件在攻击中被外泄或窃取吗?
Emergency Incident Response 服务会尽最大努力确定哪些文件已在攻击中被外泄，但并不保证这一点，因为这取决于调查中取得的数据。

Sophos 会代表我解密勒索软件吗?
不，这不是 Emergency Incident Response 服务的内容。

Sophos 会协助我谈判或支付赎金吗?
Emergency Incident Response 服务包括与威胁行为者进行专业的赎金谈判。但 Sophos 不会协助支付赎金。如有需要，我们可以推荐第三方并与之合作处理相关事务。

2025-06-03 (WP-NP)

SOPHOS