解决方案手册

SOPHOS

Sophos Emergency Incident Response

从调查到恢复的全方位服务协助

立即响应攻击中的威胁

当企业遭遇攻击时，分秒必取。发生安全事件时，您需要的是快速响应、高效行动以及跨领域的安全技能与专业知识。同时还需洞悉并了解不断演变的全球威胁态势，掌握威胁行为者的最新战术与技术。

Sophos Emergency Incident Response (紧急事件响应) 可在网络安全紧急事件爆发时即刻驰援，迅速开展评估、遏制、分析和修复工作。我们的跨职能专家团队凭借多年实战经验，快速分类、遏制并消除活跃威胁，驱逐攻击者以避免损失扩大。Sophos 凭借数千次应急响应中积累了丰富的实战经验，提供改善指导和预防措施，这不仅找出事件根本原因，更能协助增强您组织防范未来攻击的韧性。

主动强化防御与安全态势

Sophos Emergency Incident Response 采用协作互动模式，与您的团队快速评估现状，按需遏制和清除威胁，并提供可操作的恢复指导。我们团队提供数字取证、恶意软件分析、威胁狩猎等专业技术，结合 Sophos X-Ops 及 Counter Threat Unit 研究团队的情报，务求找出并清除威胁。通过渗透测试人员我们运用跨领域专业人才 (比如渗透测试人员、威胁研究员)，来确保全面开展风险缓解与恢复工作。

侦测和调查

初步接洽与调查

为实现最快速响应，Sophos 会优先聚焦于部署代理程序至可发现的资产。这远程事件响应协助，可即时撷取取证数据，用于支持初步分析、制定适当的遏制措施，并判断是否需要追加技术手段以在整个处理过程中快速扩大对环境的可视度。

深度调查

数据捕获：受影响的资产、服务、业务影响及其他攻击媒介。

迭代取证与威胁分析：研究员、威胁猎手、渗透测试员与分析员协作，全面掌握威胁全貌。

修复规划：与调查同步启动修复计划。

攻击面缩减：Sophos 可提供互动式的对威胁行为者动向的见解，以验证管控措施，并识别其他二次入侵点，从而全面降低风险。

赎金谈判：经验丰富的谈判专家基于对勒索软件威胁行为者的深度认知，可令谈判更为轻易并提供谈判指导，协助以安全、具成本效益的方式从勒索软件行为者手中恢复数据。

客户收益

- 借助跨职能的数字取证与事件响应能力与专业知识，扩编您的团队。
- 全面了解威胁，降低事件影响及未来复发的风险。
- 快速提升可见性，掌握关键事实，迅速找出解答并制定正确应对措施。

修补

安全防护与验证

针对性安全强化：IR 事件响应团队指导并支持战术性安全控制措施加固工作，防止威胁行为者再次入侵。

隔离：切断威胁行为者与命令控制中心的连接。

攻击者驱逐：要彻底驱逐已被遏制网络中的攻击者，需协调消除其作案手法，并重设被入侵的域。

恢复

系统与数据恢复：为协助重建系统、清理数据并让业务恢复正常运营，Sophos IR 团队与可信任的合作伙伴协作，提供无缝且安全的复原服务。

主机验证：采用我们行业领先的代理技术，确保恢复后的主机可重新投入运营。

后续跟进

持续改进

Sophos 利用其在数千次事件响应中积累的经验，为客户提供响应流程优化建议及战略性建议，来协助您制定安全转型路线图。在项目结束时，我们可提供正式的事件调查报告，详细列出所采取的行动、发现内容及防止未来发生类似事件的长效建议。

为何选择 Sophos 的事件响应服务?

Sophos 以丰富的经验为每一次网络安全应急响应提供专业的全方位服务支持。我们为各种类型，不同行业的组织及不同的事故类型提供全方位事件响应协助 - 无论是单一系统遭入侵的小型事件，还是造成业务重大中断或妨害的企业级危机事件，皆能妥善处理。

Sophos 的资深事件响应团队成员背景涵盖国家级、军事、组织级的计算机安全事件响应团队（CSIRT）、执法机关及情报机构，他们结合了对关键网络安全实务的实战理解、前线事件响应经验、来自我们 X-Ops 与 Counter Threat Unit 研究团队的威胁情报、安全测试与评估工作的发现，以及安全分析能力，可加速事件调查并协助您有信心地完成复原。

客户的效益

- 快速识别并清除正在进行的威胁。
- 迅速部署相关技术。
- 撷取并分析数字取证数据，以识别入侵指标并追踪攻击敌手行为。
- 开展威胁狩猎，识别相关威胁行为者活动。
- 提供远程和现场的技术支持、事件指挥与咨询能力。
- 资深和获认证的全球事件响应团队，具备处理常见与非常规网络威胁的丰富经验。
- 针对特定事件的威胁情报，洞察当前攻击敌手的作案手法。
- 专业赎金谈判
- 提供事件后报告，详细记录所采取的措施、发现结果与改进建议。

正遭到攻击?

请随时拨打下面的地区电话，联系事件顾问 (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

如果所有事件顾问均繁忙没空，请留言，将有专人尽快回复您。

电子邮件：EmergencyIR@sophos.com

要了解更多信息，请访问：
sophos.com/emergency-response

中国（大陆地区）销售咨询
电子邮件 : salescn@sophos.com

© Copyright 2025.Sophos Ltd. 保留所有权利。
英格兰和威尔士注册号：2096520，地址：The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos 是 Sophos Ltd. 的注册商标。本文提到的所有其他产品和公司名称是其各自所有者的商标或注册商标。

2025-06-04 BRZHCN (MP)

SOPHOS