Sophos Compromise Assessment

在业务受影响前发现受骇的证据

去年，企业平均用时 37 天和 240 万美元查找安全漏洞并从中恢复。Sophos Compromise Assessment 受骇威胁评估由事件响应专家组成的专家团队提供，是发现环境中的进行中或过往攻击者活动的最快最有效手段，帮助您的企业快速采取决定性措施。

找出活跃或最近的攻击者活动

Sophos Compromise Assessment 受骇评估由威胁猎手和事件响应专家组成的专家团队提供，快速确定攻击是否攻破您的防御，量化对您企业的风险等级，提供消除威胁所需要采取的措施的详细指导。

Sophos Incident Response (IR) Services 事件响应 (IR) 服务团队拥有响应现在最先进威胁的丰富经验，通过针对性调查潜在受威胁资产，确定入侵指标 (IoC)，得到快速彻底的评估，帮助您的企业控制风险和合规性，同时保持运营效率。

Sophos 受骇评估方法

Sophos IR 服务团队在威胁评估的每个阶段保持与您企业的直接沟通，说明威胁、风险暴露以及解决事件和根本原因需要采取的措施。

1. **初始协调通话** – 评估开始时，高效交换潜在威胁信息，确定关键联系点，确认部署范围和要跟进的调查流程。
2. **部署调查工具** – 引导安装获奖的云交付 Sophos 平台，确保立刻捕获指定设备的数据，支持 Sophos IR 服务团队彻底评估设备运行状况。
3. **威胁调查与风险评估** – 如果确认活跃威胁，Sophos IR 服务团队将与您的关键联系点立刻开始活跃威胁通话，讨论广泛安全事件的风险和要采取的紧急措施。
4. **总结通话和书面报告** –取得技术文档和非技术执行总结，详细说明攻击者活动证据、风险暴露以及消除威胁和解决根本原因的指引。

Sophos Compromise Assessment 的所有四个阶段通常在初始协调通话 后7 天内完成。

亮点

- 快速识别攻击者是否在您的环境中执行操作而未被发现
- 量化广泛安全事件的潜在风险
- 在调查的每个阶段直接与威胁猎手和事件响应专家团队沟通
- 接收攻击者活动、风险暴露以及消除威胁和解决根本原因指引的综合分析
- 支持风险管理和合规性计划，以及与兼并活动相关的尽职调查工作

SOPHOS

快速彻底调查

Sophos 威胁评估调查并确定完整攻击者活动，包括：

- 可疑网络活动
- 横向移动
- 异常或恶意文件
- 自动恶意软件执行
- 未经授权访问
- 权限提升
- 避开防御
- 凭据盗窃
- 数据泄露
- 未经验证的脚本

评估后

如果 Sophos IR 服务团队确认攻击者已经攻破您的防御，威胁您的数据和企业，可以选择优先采用 Sophos 快速响应。这一全规模事件响应服务将解决、隔离和消除整个 IT 环境内的活跃威胁。24/7 全天候远程事件响应专家团队将快速行动，将对手赶出您的环境，并建议实时预防性措施以解决根本原因。

如果没有发现入侵迹象，Sophos Managed Detection and Response (MDR) 托管式侦测与响应 可以为您的企业提供持续 24/7 全天候侦测与响应服务。我们的全天候威胁猎手和响应专家主动追捕和验证潜在威胁与事件。团队持续采取措施，中断、隔离和消除不断演变的威胁，提供可行建议以解决事件根本原因，改善您的安全状况。

正遭到攻击？

Sophos Rapid Response 快速响应 通过 24/7 全天候远程事件响应、威胁分析和威胁追捕专家，帮助您快速脱离危险。数小时内就位，大多数客户在 48 小时内得到分流安排。如果您遇到活跃威胁，请随时拨打下面的地区电话，联系事件顾问。

如果您遇到活跃威胁，请给快速响应团队发电子邮件 rapidresponse@sophos.com 或拨打下面的地区号码：

美国 +1 4087461064

澳大利亚 +61 272084454

加拿大 +1 7785897255

法国 +33 186539880

德国 +49 61171186766

英国 +44 1235635329

正遭到攻击？

获取 Sophos Rapid Response 的快速支持

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

© 版权所有 2022。Sophos 有限责任公司 保留所有权利。
英格兰和威尔士注册编号 2096520，The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos 是 Sophos 公司的注册商标。所有其他产品和公司名称均是其各自所有者的商标或注册商标。

2022-06-13 DS-ZHCN (DD)

SOPHOS