SOPHOS

Managed Threat Response (MTR)

专家领导的威胁响应

Sophos Managed Threat Response (托管式威胁回应，MTR) 提供由专家团队以全托管服务形式带来的 24/7 全天候威胁搜捕、检测和响应功能。

产品亮点

- 以全托管服务形式，提供先进的威胁搜捕、检测和响应功能
- 与 24/7 全天候响应团队协作，后者负责远程隔离和清除威胁
- 您负责决定和控制 MTR 团队所采取的操作以及管理事件的方式
- 将顶尖机器学习技术与训练有素的专家团队结合在一起
- 两级服务体系 (Standard 和 Advanced) 为处于各个成熟度的企业提供丰富的功能组合

威胁通知并非解决方案 – 只是起点

很少有组织内部拥有能全天候管理安全计划，同时主动防御新兴威胁的适当工具、人员和程序。Sophos MTR 团队不仅仅能将攻击或可疑行为告知您，更代表您采取针对性操作，清除最复杂成熟的威胁。

有了 Sophos MTR，您的企业将获得一支 24/7 全天候威胁搜捕和响应专家团队，负责：

- 主动搜捕和验证潜在威胁与事件
- 利用所有可用信息确定威胁范围和严重程度
- 对有效威胁布置合适的业务环境
- 采取操作远程中断、隔离和清除威胁
- 提供解决反复出现事件根本原因的可行建议

机器加速的人工响应

Sophos MTR 以我们的 Intercept X Advanced with EDR 技术为基础，融合机器学习技术和专家分析，改进威胁搜捕与检测，更加深入调查警报，采取针对性操作快速精确地清除威胁。Sophos 顶级端点防护与和智能 EDR 与世界级安全专家团队的融合，造就了我们所说的“机器加速的人工响应”。

完全透明与控制

利用 Sophos MTR，您可以决定和控制上报潜在事件的方式和时间，希望我们采取的响应操作 (如果有)，以及沟通的对象。Sophos MTR 提供三种响应模式，您可以选择事件期间最适合 MTR 团队的工作方式：

通知：我们通知您检测结果，提供详细信息帮助您确定优先级和响应。

协作：我们与您的内部团队或外部联络点一起响应检测结果。

授权：我们负责隔离和清除操作，将通知您采取的操作。

Sophos MTR 服务层级

Sophos MTR 提供两级服务体系（标准和高级），为所有规模和成熟度的企业提供丰富的功能组合。无论选择哪一级服务，企业都可以利用三种响应模式（通知、协作或授权）中的任一种满足自己的独特需求。

Sophos MTR: 标准

24/7 全天候负责人推动威胁搜捕

自动阻止或终止确认的恶意事件或活动（强信号），解放威胁搜捕人员，开展负责人推动的威胁搜捕。此类威胁搜捕聚集并调查日常和相邻事件（弱信号），发现以前可能未检测到的新攻击迹象 (IoA) 和威胁迹象 (IoC)。

安全运行状况检查

保持 Sophos Central 产品--从 Intercept X Advanced with EDR 开始--以最佳性能运行，主动检查运行状况，提出配置改进建议。

活动报告

案例活动汇总支持优先级排序和通信功能，这样，您的团队了解每个报告期内检测到的威胁，以及采取的响应操作。

对手检测

大多数成功攻击依赖执行对监测工具来说合法的进程。我们的团队利用独有调查技术，确定合法行为与攻击者运用的战术、技术和过程 (TTP) 之间的差异。

Sophos MTR: 高级 包含所有标准功能，以及：

24/7 全天候无负责人威胁搜捕

运用数据学、威胁情报和资深威胁搜捕人员的直觉，将公司档案、高价值资产和高风险用户结合在一起，预测攻击者行为和识别新攻击迹象 (IoA)。

增强遥测

为威胁调查补充其他 Sophos Central 产品的遥测功能，超越端点范围，提供对手活动的全面信息。

主动状态改进

主动改进安全状态，用规范性指导加固防御，解决影响整体安全功能的配置和架构弱点。

威胁响应负责人

确认事件后，提供威胁响应负责人，直接与您的现场资源（内部团队或外部合作伙伴）协作，直到清除活跃威胁。

直接电话支持

您的团队可以直接致电我们的安全作战中心 (SOC)。我们的 MTR 操作团队随时在线，遍布全球 26 个地点的支持团队作为其坚强后盾。

资产发现

我们根据资产信息（包括操作系统版本、应用程序、漏洞）确定托管和非托管资产，在影响评估时提供宝贵信息，进行威胁搜捕，并提出主动状态改进建议。

中国（大陆地区）销售咨询
电话: 400 650 6598
电子邮件：salescn@sophos.com

2019-09-17 DS (GH)

SOPHOS