SOPHOS

事件应对专家的四个重要提示

应对危急网络事件时压力巨大，时间紧张。任何办法都无法完全减轻应对攻击的压力，了解事件应对专家的这些重要提示，将为您的团队带来企业防御的优势。

本文重点介绍应对网络安全事件时，所有人应了解的最重要内容，这些内容来自于 Sophos Managed Threat Response 和 Sophos Rapid Response 团队的真实经历，这两个团队共同应对了数千起网络安全事件。

提示 1：尽快应对

企业受到攻击时，分秒必争。

团队长时间无法应对的原因如下：最常见的原因是不了解所处局面的严重性，缺乏意识导致缺乏紧迫感。

攻击者往往在最不方便的时间攻击：节假日、周末、深夜。由于大多数事件应对团队严重人员短缺，形成“明天再说”的态度不是不能理解。但遗憾的是，明天再采取措施减小攻击影响已经为时已晚。

而且张皇失措的团队更可能缓慢应对攻击迹象，因为他们被警示疲劳轰炸，这意味着信号被埋没在噪声中不被发现。即使最初打开案件时，由于缺乏可见性和相关环境内容，可能优先级设置错误。这样浪费时间，而应对事件时，时间并没有站在防御者一方。

即使安全团队意识到受到攻击，需要立刻采取措施，他们也没有经验知道采取哪些措施，这也使得他们应对缓慢。最好的解决方法是事先为事件做好计划。

去年超过一半的企业受到勒索软件攻击 – 攻击者在 73% 的案件中成功加密文件。[1]

提示 2：不要过早宣告“任务完成”

应对事件时，仅仅治标还不够。治本也很重要。

侦测到威胁后，首先解决接下来的攻击。这可能意味着清理勒索软件可执行文件或银行木马或者阻止数据泄漏。但是，团队通常将阻止初始攻击，而没有意识到他们没有真正解决根本原因。

成功移除勒索软件和清理警示并不意味着攻击者已经被驱逐出环境。还可能侦测到的只是攻击者观察防御水平的测试攻击。如果攻击者仍然可以访问，他们很可能将再次发起攻击，但这次更具破坏性。

事件应对团队需要确保他们解决初始事件的根本原因。攻击者是否仍留在环境中?他们是否计划发起第二波攻击?有着丰富攻击应对经验的事件响应操作员知道何时和在哪里更深入调查。他们查找攻击者正在、已经或者可能计划在网络中的任何操作 – 并消除这些威胁。

例如，在一个实例中，Sophos 事件应对专家能够阻止持续 9 天的攻击，发现攻击者用勒索软件攻击企业的三次尝试。

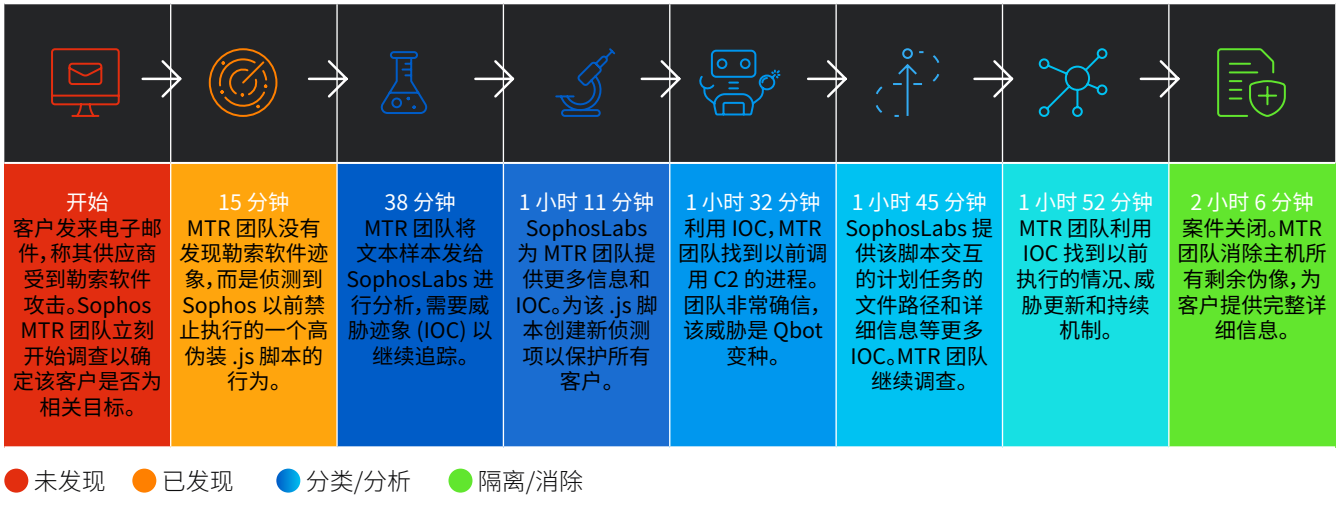
在第一波攻击尝试中（最后由企业的端点防护解决方案阻止），攻击者使用 Maze 勒索软件将 700 台计算机作为目标，勒索 1500 万美元赎金。目标的安全团队在意识到受到攻击后，联系了 Sophos 托管威胁应对 (MTR) 团队的资深事件应对专家。

Sophos 事件应对专家快速找出受威胁的管理员帐户，找出并移除多个恶意文件，拦截攻击者命令和 C2（指挥控制）通信。然后 Sophos MTR 团队能够防御对手的另外两波攻击。如果攻击者成功，受害者不得不支付赎金，这可能是迄今最昂贵的勒索软件赎金之一。

在另一个示例中，Sophos MTR 团队应对潜在勒索软件威胁，但很快意识到没有勒索软件迹象。这时候，有些团队可能结束案件，转向其他工作。但 Sophos MTR 团队继续调查，发现了以前的银行木马。对这个客户来说幸运的是，威胁不再活跃，但这个示例说明了为什么要在初始症状以外查找以确定完整根本原因，这可能是更大型攻击的迹象。

SOPHOS MTR 案件簿：

发现以前的银行木马的勒索软件追踪



提示 3：完整可见性很关键

在防范攻击的过程中，如盲了般捍卫组织是最困难的。必须可以获取合适的高质量数据，能够准确识别潜在攻击迹象，确定根本原因。

有效团队收集合适数据以观察信号，可以分离信号与噪声，知道哪些信号的优先级最重要。

收集信号

环境可见性有限无疑会错过攻击。多年来，许多大数据工具进入市场，试图解决这个具体难题。一些工具依赖以事件为中心的数据，如日志事件，有些则利用以威胁为中心的数据，其他则采用混合方法。无论采用何种方法，目的都一样：收集足够数据产生有意义的情报，调查和应对可能错过的攻击。

从多个来源收集合适的高质量数据确保完全了解攻击者的工具、战术和过程 (TTP)。否则很可能只能看到攻击的一部分。

减少噪声

由于害怕没有掌握攻击全部信息所需的数据，一些企业（以及他们依赖的安全工具）收集所有数据。但是，这并没有减轻大海捞针的难度；反而堆积了更多不必要的信息，增加难度。这不仅增加数据收集和存储成本，而且产生大量噪声，导致警示疲劳，浪费时间追踪误报。

应用相关环境内容

关于威胁侦测和应对专家有这样一个说法：“内容是王，相关环境内容就是后。” 二者都是运行有效事件应对计划所必需的。应用与信号关联的有意义元数据，分析师可以确定此类信号是恶意还是良性。

有效威胁侦测和响应的最关键要件之一，是优先找出最重要的信号。确定最重要威胁的最佳方法是组合安全工具提供的相关环境内容（即端点侦测和应对解决方案）、人工智能、威胁情报和操作员的知识库。

相关环境内容有助于确定信号源头，当前攻击阶段，相关事件，对企业的潜在影响。

提示 4：放心求助

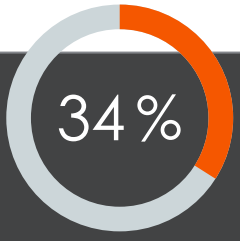
企业都不希望遇到攻击，但是应对事件的体验是无法替代的，这意味着经常面临高压力事件应对工作的 IT 和安全团队被安排到没有相应应对技能的场景；此类场景通常对企业有着巨大影响。

缺乏调查和应对事件的熟练人员是现在网络安全行业面临的最大问题之一。这个问题非常普遍，据 ESG Research 表示[2]，“34% 的企业称最大挑战是缺乏熟练人员调查涉及端点的网络安全事件，确定根本原因和攻击链。”

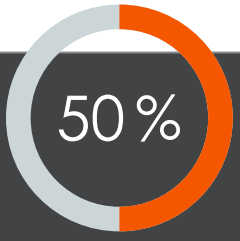
这一困境带来了新的替代方式：托管安全服务。具体来说，托管侦测与应对 (MDR) 服务。MDR 服务是专家团队提供的外包安全操作，是客户安全团队的延伸。这些服务将人主导的调查、威胁追踪、实时监测和事件应对与各种技术相结合，收集并分析情报。据 Gartner 表示，“到 2025 年，50% 的企业将使用 MDR 服务”[3]，这意味着企业正意识到他们需要帮助来运行完整安全操作和事件应对计划。

对于还没有采用 MDR 服务但正在应对活跃攻击的企业来说，事件应对专家服务是一个很好的选择。安全团队焦头烂额，需要外部专家分类攻击并确保解决对手时，引入事件应对专家。

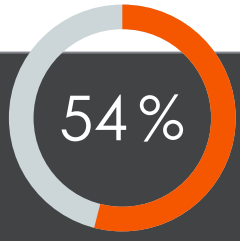
即使企业拥有熟练安全分析师团队，与事件应对服务协作也有好处，可以弥补覆盖（即晚上、周末、节假日）和应对事件需要的专业角色的不足。



据分析公司 ESG 表示，34% 的企业称最大挑战是缺乏熟练人员调查涉及端点的网络安全事件，确定根本原因和攻击链。”[2]



到 2025 年，50% 的企业将使用 MDR 服务（2019 年不到 5%）。[3]



在 2019 年一项对 3,100 名 IT 和安全专业人员的调查中，54% 的受访者表示由于缺乏经验丰富的人才，“无法充分发挥 EDR 解决方案的优势”。[4]

Sophos 可以帮助做什么

Sophos Managed Threat Response (MTR) 服务

担心您的企业应对潜在严重事件的能力？如果是，可以考虑 Sophos Managed Threat Response (MTR) 服务。

Sophos MTR 提供由专家团队以全托管服务形式带来的 24/7 全天候威胁追踪、侦测和响应功能。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。如果发生事件，MTR 团队将启动措施，远程中断、隔离和消除威胁。安全操作专家团队还提供解决反复发生事件的根本原因的可行建议。

了解更多 www.sophos.com/mtr

Sophos Rapid Response 服务

如果您的企业正在遭受攻击，需要立刻提供事件应对协助，Sophos 可以帮助。

由事件应对专家团队提供的 Sophos Rapid Response，为企业提供识别并消除作动中威胁的快速协助。数小时内就位，大多数客户在 48 小时内得到分配。服务为现有 Sophos 客户和非 Sophos 客户提供。

Sophos Rapid Response 远程事件应对团队快速采取措施分类、隔离并消除活跃威胁。将对手挡在企业之外，避免进一步破坏您的资产。

了解更多 www.sophos.com/rapidresponse

Sophos Intercept X Advanced with EDR

希望提高侦测、调查和应对内部事件能力的企业应考虑增加 Sophos 端点侦测和应对 (EDR) 功能。

Sophos Intercept X Advanced with EDR 支持您的团队开展威胁追踪，帮助在整个企业范围内平滑开展 IT 操作保健。Sophos EDR 让您的团队可以提出详细问题，找出高级威胁、活跃威胁和潜在 IT 漏洞，然后快速采取相应措施阻止。

了解更多和免费试用 www.sophos.com/edr

[1] 2020 年对 5,000 名 IT 经理的调查 https://secure2.sophos.com/zh-cn/medialibrary/Gated-Assets/white-papers/sophos-cybersecurity-the-human-challenge-wp.pdf

[2] https://www.esg-global.com/blog/soapa-discussion-on-edr-and-xdr-with-jon-oltsik-and-dave-gruber-video-part-1

[3] Gartner，托管侦测和应对服务市场指南，2020 年 8 月 26 日，分析师：Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneider

[4] 2019 年对 3,100 名 IT 经理的调查 https://secure2.sophos.com/zh-cn/security-news-trends/whitepapers/gated-wp/uncomfortable-truths-of-endpoint-security.aspx

中国（大陆地区）销售咨询
电子邮件: salescn@sophos.com

20-10-30 WPZHCN (PS)

SOPHOS