解决方案概要

Sophos NDR

深入您网络内部的关键可见性

Sophos Network Detection and Respons 网络侦测与响应适用于 Sophos MDR 和 Sophos XDR，用于侦测网络内部深处，连端点和防火墙无法察觉的的恶意网络活动。Sophos NDR 持续分析流量，寻找可疑模式，包括源自未知或未受托管设备的异常活动、恶意资产、新的零日 C2 服务器以及未预期的的数据传输。

实用案例

1 | 关键可见性

期望结果：获得对其他产品无法看到的网络活动的关键可见性

解决方案： Sophos NDR 与您的托管中的端点和防火墙一起工作，监测网络活动中的可疑和恶意模式，这是您的端点和防火墙都无法看到的。它侦测非托管的系统和 IoT 设备、恶意资产、内部人为威胁、以前未见过的零日攻击以及网络深处异常行为的异常流量。

2 | 提早侦测

期望结果：五个独立的侦测引擎实时工作，以更早地识别威胁

解决方案： Sophos NDR 包括五个实时协同工作的独立侦测引擎，能采用深度学习、深度数据包检查、加密有效负载分析、域名分析和强大的分析等技术来快速侦测可疑或恶意流量。我们独特的分析提供仅高价值的警报，确保您不会被过多噪声所干扰。

3 | 自动响应

期望结果：自动当场立即停止主动攻击敌手和威胁

解决方案： Sophos NDR、Sophos XDR、Sophos MDR 和 Sophos Firewall 之间的跨产品自动化提供即时响应，来当场立即阻止主动威胁。当 Sophos NDR 识别出威胁指标、主动威胁或攻击敌手时，分析人员会立即收到警报，并可以立即将威胁信息传递给 Sophos Firewall，触发自动响应以隔离受影响的主机。

4 | 通过单一控制台管理

期望结果：花费更少的时间管理您的网络安全

解决方案： 通过 Sophos Central，您可以获得一个单一的云管理平台，用于管理所有 Sophos 产品，包括 NDR、XDR、端点、防火墙等。您将获得丰富而强大的工具，利用我们的深度数据湖进行跨产品的威胁捕猎、管理早期响应以及报告和审计。这最终意味着您将花费更少的时间来管理您的网络安全。

识别未受保护和恶意资产

揭示异常数据移动和内部威胁

探测前所未见的零日攻击

了解更多并尝试
Sophos NDR
sophos.com/ndr

2023-11-06 DS-ZHCN (MP)

SOPHOS