SOPHOS

Sophos EDR 和 XDR 使用案例

随 Intercept X Advanced with XDR、Intercept X Advanced with EDR、Intercept X Advanced for Server with XDR 和 Intercept X Advanced for Server with EDR 提供

Sophos XDR

解答业务关键 IT 运行和威胁捕猎问题，然后在需要时采取措施。IT 管理员和网络安全分析师可以利用强大的功能。

执行 IT 安全操作和威胁捕猎工作

- 选择完全可自定义的预先编写的 SQL 查询
- 获得需要的信息后快速采取操作
- 覆盖端点、服务器、防火墙、电子邮件、云主机等

IT 操作用例

IT 运行使用案例保持 IT 运行健康处于最佳状态。下面是一些示例使用案例：

设备运行状况检查

找出存在性能问题的设备，然后远程访问并采取所需操作。

- 找出磁盘空间低、内存/CPU 使用率高或等待重新启动的设备
- 远程访问设备以释放磁盘空间，调查高使用率原因，根据需要重新启动

弱点

侦测存在可能被恶意软件或攻击者利用的问题或漏洞的设备。

- 找出存在软件漏洞、运行未知服务或未经授权浏览器扩展的设备，侦测共享或失窃的帐户凭据
- 远程访问设备以安装补丁程序，调查和终止未知服务，卸载浏览器扩展程序，更新云帐户凭据

不需要的软件

跟踪可能导致合规性或生产力问题的软件。

- 找到不想要程序，如 Spotify、Steam 和 Bittorrent
- 远程访问设备，卸载软件

配置管理

查找存在配置问题可造成安全风险的设备和云载荷

- 识别启用 RDP 和 SSH 的服务器，网络端口保持打开的云安全组，监视和库存公共云主机，容器等
- 远程访问服务器，禁用 RDP/SSH，检查在打开端口侦听的服务器

合规性

识别并处理本地和云端合规性问题。

- 为 AWS、Azure 和 GCP 环境查找敏感文件、评估配置
- 远程访问设备以删除敏感文件，确保针对 CIS 基准的安全云配置

项目推出

检查是否已经在所有设备部署 IT 项目。

- 了解软件是否已经部署在设备上，衡量推出进度
- 远程访问设备，确保成功部署，如果需要，重启以进行任何必要改动

办公室网络问题（需要 XDR）

发现并纠正办公地点的网络问题。

- 了解为什么办公室存在减慢速度的网络问题
- 发现导致问题的应用

设备管理（需要 XDR）

找出并理解企业 IT 环境的设备。

- 发现未管理和未受保护的设备，如笔记本电脑、手机和物联网设备
- 获取传统或未管理设备的额外信息，如专用医疗器械

防范意外事件（需要 XDR）

有了 30 天云存储，不用担心被意外事件困扰。

- 查看丢失设备上过去 30 天的异常活动
- 即使被擦除或销毁，也能了解设备发生的情况

威胁追踪用例

跟踪隐蔽的威胁，快速清理。下面是一些示例使用案例：

网络攻击

识别进行异常网络访问尝试的进程。

- 侦测尝试连接非标准端口或来自云载荷异常出站流量的进程
- 分析云安全组以找出暴露在公共互联网下的资源
- 远程访问设备/工作负荷，终止进程，检查横向移动

修改的文件

找出被意外修改的项。

- 找出最近修改过文件或注册表项的进程
- 远程访问设备，检查改动，采取措施

伪装脚本

基于内存的免文件攻击是一种常见攻击载体。

- 挖掘不预期的 PowerShell 执行的详细信息
- 远程访问设备，运行额外鉴证工具，终止可疑进程

伪装进程

一些恶意进程伪装自己以避免侦测。

- 侦测伪装自己的进程
- 远程访问设备，终止可疑进程，运行鉴证工具

MITRE ATT&CK 框架

MITRE ATT&CK 框架是用于识别攻击技术的常用模板。

- 使用您自己的或 Sophos 查询，识别对手采用的攻击战术和技巧
- 根据识别的技术开展调查，找出潜在后续攻击或需要反复检查的区域

事件范围

了解事件的影响，受到影响的设备和用户。

- 找出单击过网络钓鱼电子邮件链接的设备
- 发现从网络钓鱼站点下载文件的设备，访问并执行清理

延长调查期限（需要 XDR）

除了设备数据存储 90 天，还使用 30 天云数据。

- 研究 30 天数据，无需恢复设备在线
- 了解遭遇攻击瘫痪设备发生的情况

使用丰富的网络数据（需要 XDR）

将网络数据加入威胁追踪和调查。

- 与其他 IoC 交叉参考阻止的恶意通信，从宏观层面了解攻击
- 从防火墙使用 ATP 和 IPS 侦测，调查可疑主机和设备

使用丰富的电子邮件数据（需要 XDR）

集成电子邮件信息，获取环境的更多信息。

- 与其他 IoC 比较电子邮件页标题信息，更好地了解事件
- 识别可疑文件，快速从设备和 O365 邮箱删除

要更多了解 Sophos XDR、EDR 以及 Intercept X 的强大防护功能，请访问 www.sophos.com。

21-03-26 UC-ZHCN (MP)

SOPHOS