iMC-EBM usb文件复制操作审计不到

DAM 钟俊 2023-02-27 发表

问题描述

现场想要实现审计USB存储设备和终端之间传输文件的过程，包括文件名，传输的时间。测试发现，在usb存储设备上复制文件，usb存储设备复制文件到本地，本地复制文件到usb存储设备上，文件操作日志内都没有记录。

过程分析

配置如下图：


用户 > 终端行为管理 > 文件操作策略 > 文件操作策略详情
帮助
文件操作策略详情
基本信息
策略名称
USB外设监控
描述
文件操作参数
文件备份参数
创建 重命名 复制 读取 修改
备份文件阈值（MB）
100
监视磁盘类型
所有类型 指定类型 不监视
磁盘类型
本地磁盘 可移动磁盘 网络盘（网上邻居） 光盘（光驱）
监视指定文件目录
文件目录
描述
监视/排除
未找到符合条件的记录。
监视指定文件名
不监视指定文件名 只监视指定文件名


监视操作文件的进程
进程名称
描述
wps.exe
WPS Office的主进程
notepad.exe
是Windows自带的记事本程序
winword.exe
微软Microsoft Word的主程序
监视指定后缀的文件
不监视指定后缀文件 只监视指定后缀文件
文件后缀
描述
.txt
txt是Windows操作系统上附带的一种文本格式，是最常见的一种文件格式，主要存文本信息，即为文字信息
.docx
是Word2007之后版本的文本文档
返回


返回
终端IP地址
操作时间
创建时间
修改时间
操作文件进程
操作类型
文件名称
文件大小
源文件路径
2023-02-27 10:57 2023-02-27 10:55 2023-02-27 10:57 NOTEPAD.EXE 修改 H3C测试01.txt 1 E:\H3C测试01.txt
2023-02-27 10:57 2023-02-27 10:55 2023-02-27 10:55 NOTEPAD.EXE 创建 H3C测试01.txt 1 E:\H3C测试01.txt
2023-02-27 10:57 2023-02-27 10:55 2023-02-27 10:55 NOTEPAD.EXE 创建 H3C测试01.txt 1 E:\H3C测试01.txt
2023-02-27 10:57 2023-02-27 10:55 2023-02-27 10:55 NOTEPAD.EXE 创建 H3C测试01.txt 1 E:\H3C测试01.txt
2023-02-27 10:57 2023-02-27 10:55 2023-02-27 10:55 NOTEPAD.EXE 创建 H3C测试01.txt 1 E:\H3C测试01.txt
2023-02-27 10:57 2023-02-27 10:55 2023-02-27 10:57 NOTEPAD.EXE 读取 H3C测试01.txt 0 E:\H3C测试01.txt

解决方法

如果日志内没有信息，检查策略请求周期参数。

现场目前创建，读取，重命名，修改都可以在文件操作日志中看到，只有复制看不到。后续在进程列表中加上explorer.exe，可以正常识别到复制操作。

explorer.exe为复制粘贴的进程，和资源管理器有关的全是explorer.exe。