momenta

终端事件

admin 2025-02-21 15:01:52

ID：233

事件属性

通道：应用程序(文件访问)

动作：放行

事件状态：新

安全级别： 高

最大匹配：1

匹配总数：2

文件名称：cve-2017-12149_cmd.py 大小：9.93 KB

流量大小：9.93 KB

详细信息：C:\Users\yijuan.liu.ext\Downloads\cve-2017-12149_cmd.py;

检测时间：2025-02-21 14:50:45

事件时间：2025-02-21 14:51:14

检测引擎：Endpoint(PC-PF33KB5E.momenta.ai)

分析引擎：Content Analysis Engine (PC-PF33KB5E.momenta.ai)

工作模式：仅监控

来源Risk Level：

来源属性

全名：yijuan.liu.ext

登录名：yijuan.liu.ext

用户名：yijuan.liu.ext

部门：N/A

主管：steven.wang

IP地址：10.6.1.59,fe80::1d88:9b35:850d:7943%30

域名：momenta.ai

MAC：38-87-d5-d8-78-54

应用程序：百度网盘(Windows)

目标属性

全名：百度网盘(windows)

部门：N/A

方向：出向

命中策略及详情

策略名称1：01代码审计

规则名称：测试代码指纹

文件指纹［1次匹配： cve-2017-12149_cmd.py；］

策略名称2：01文件类型

规则名称：文件类型

文件名称［1次匹配： cve-2017-12149_cmd.py；］