SecCenter CSAP-S 安全威胁发现与运营管理平台异常流量分析没有数据

日志采集器 **孔凡安** 2022-06-11 发表

问题描述

SecCenter CSAP-S 安全威胁发现与运营管理平台异常流量分析没有数据

解决方法

异常流量主要是基于流量日志匹配UEBA规则产，需要查看设备有没有接入流量日志，有没有命中对应规则。

此外，脆弱性中漏洞top10主要是基于漏扫联动或者漏扫报告导入，产生的资产漏洞信息，恶意文件主要是沙箱APT检测的恶意文件。