



D2000-G数据库审计规则命中数为0问题

数据库审计

王树岭

2022-06-07 发表

组网及说明

不涉及

告警信息

不涉及

问题描述

增加数据库应用规则

常规设置

规则名称:

规则状态: 启用 风险级别: 安全 规则动作: 记录

规则描述:

客户端触发条件设置

时间范围: = 请选择: +

客户端地址: or 请选择: +

计算机名: or 请选择: +

数据库用户名: or 请选择: +

应用程序名: or 请选择: +

操作名称: or 请选择: +

操作方式: or 请选择: +

操作内容: or 请选择: +

操作内容 (最多加9行)

统计时长: > 小时 ?

自定义规则，风险等级为安全

事件中查看该规则命中数一直为0

同时用sec账号登录设备，查看报表统计能看到该规则的命中信息

过程分析

对于风险等级为安全的规则，设备不会将命中升级为事件，因此，在事件中对于该规则不统计命中数

而报表中的数据来源是实时审计（实时查询），这部分会统计到规则中涉及到操作的命中

解决方法

机制问题

