某局点SecPath D2020 设备自定义规则不生效问题处理经验案例

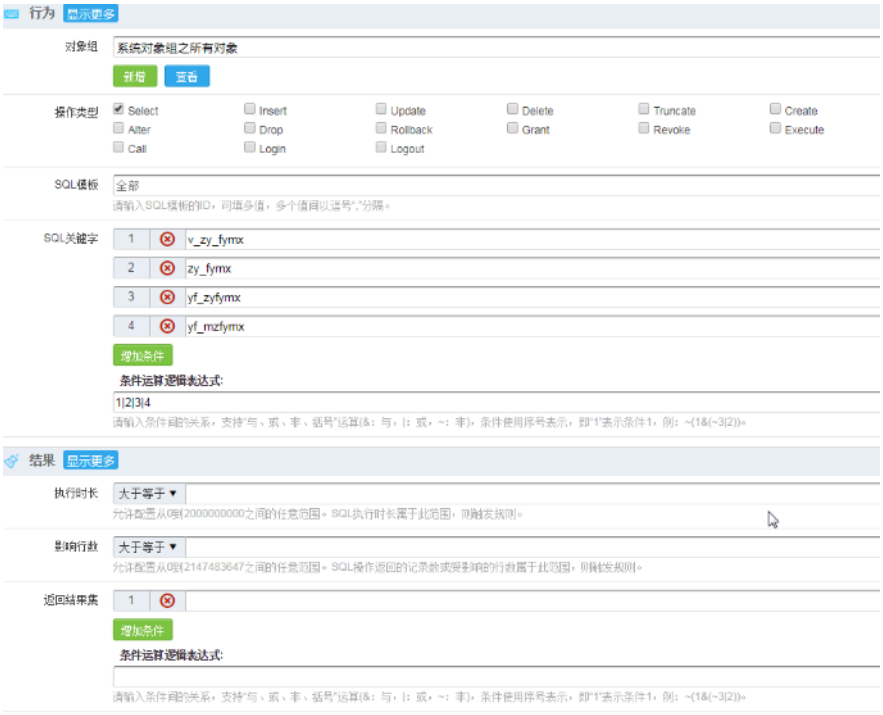
数据库审计 其他 zhiliao_7xnC7 2018-10-22 发表

组网及说明

不涉及

问题描述

目前是在规则配置中配置了一条Oracle的规则组，里面加了一条bsoft的规则，该规则定义如下：



现场模拟规则中的动作，发现系统已经审计到了，但并未触发告警

过程分析

通过对比官网配置，没有大的出入，其中针对业务主机群有特别的说明，在自定义规则的时候可以先不选，规则可以顺利创建，但是该规则在启用之后不会生效。

业务主机群	添加时可先不选，但如果想要此规则生效，必须要选择规则对应生效的业务主机群

跟现场核实发现未选择业务主机群

解决方法

让现场将对应的业务主机群填上后，再一次匹配模拟规则中的动作时，发现可以查看到告警日志信息。