D2020-G(二代) 有数据库语句记录但未触发告警的案例分析

数据库审计 李熙 2022-06-24 发表

组网及说明

不涉及

告警信息

不涉及

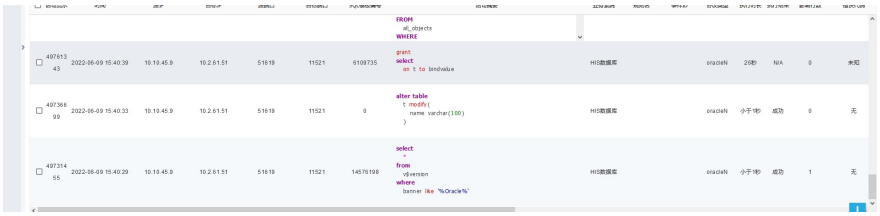
问题描述

对Oracle数据库进行审计，当前查询到有表结构变更的语句，但未命中设置的规则，规则HIS_Rule_02触发命中数为21，是之前触发结果，未清空；

之前有命中规则并产生告警，如6月6号

过程分析

1、确认有产生表结果语句，alter table



2、确认规则配置没问题，可以满足触发条件

3、经确认，6月9号截图中的表结构变更SQL语句(alter table t modify（name varchar（100））)模板为0，系统没有SQL模板与之匹配，所以只能审计到这条语句，但是命中不了规则；之前的SQL语句模板不为0，和截图反馈的不一样

解决方法

非故障，未正常现象；sql模板为0的语句不触发告警（cache，mongo，redis这三个数据库类型除外）。