

知

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；

	规则名	触发命中数	风险级别	状态	动作
1	HIS_Rule_02	21	中可疑	可用	记录
2	HIS_Rule_01	0	低可疑	不可用	记录
3	PACS_Rule_01	0	中可疑	可用	记录
4	LIS_表结构变更	0	中可疑	可用	记录
5	药房_表结构变更	0	中可疑	可用	记录
6	心电图_表结构变更	0	中可疑	可用	记录
7	内窥镜_表结构变更	0	中可疑	可用	记录
8	HRP_表结构变更	0	中可疑	可用	记录

之前有命中规则并产生告警，如6月6号

事件ID	风险程度	发生时间	行为	事件描述	触发地点	响应状态	操作
8445989	中可疑	2022-05-05 19:09:15	10.10.45.9	HIS_Rule_02 该事件中 10.10.45.9 进行了 修改 操作。		未响应	事件查看
8425903	中可疑	2022-05-27 10:25:12	10.10.45.2	HIS_Rule_02 该事件中 10.10.45.2 进行了 删除表 操作。		未响应	事件查看
8425907	中可疑	2022-05-27 10:24:47	10.10.45.2	HIS_Rule_02 该事件中 10.10.45.2 进行了 删除 操作。		未响应	事件查看
8425909	中可疑	2022-05-27 10:28:55	10.10.45.2	HIS_Rule_02 该事件中 10.10.45.2 进行了 修改 操作。		未响应	事件查看
8425905	中可疑	2022-05-27 10:28:55	10.10.45.2	HIS_Rule_02 该事件中 10.10.45.2 进行了 修改 操作。		未响应	事件查看
8425904	中可疑	2022-05-27 10:28:55	10.10.45.2	HIS_Rule_02 该事件中 10.10.45.2 进行了 修改 操作。		未响应	事件查看
8425903	中可疑	2022-05-27 10:28:55	10.10.45.2	HIS_Rule_02 该事件中 10.10.45.2 进行了 修改 操作。		未响应	事件查看
8425902	中可疑	2022-05-27 10:28:55	10.10.45.2	HIS_Rule_02 该事件中 10.10.45.2 进行了 修改 操作。		未响应	事件查看

1、确认有产生表结果语句, alter table

SQL	开始时间	耗时	用户	数据库	实例ID	实例名称	主机名	IP地址	端口	连接数	状态	备注
<pre>SELECT * FROM t1 WHERE 1=1</pre>	487853 43	2022-06-09 15:40:39	10.10.45.9	10.2.61.51	51519	11021	01087105					成功
<pre>alter table t modify(name varchar(100))</pre>	497368 99	2022-06-09 15:40:33	10.10.45.9	10.2.61.51	51519	11521	0					无
<pre>select * from v1 where banner like '%Oracle%'</pre>	497374 55	2022-06-09 15:40:20	10.10.45.9	10.2.61.51	51519	11521	14578106					无

2、确认规则配置没问题，可以满足触发条件

修改数据库应用规则

常规设置

规则名：

HIS_Rule_02

规则状态：

可用

 风险级别：

中可疑

 规则动作：

记录

规则描述：

HIS表结构变更

客户端触发条件设置

时间范围：

=

每天

客户端地址：

or

PC

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：

操作表名：

or

请选择：

操作方式：

or

表结构变更

操作内容：

or

请选择：

增加

删除

操作内容（最多加9行）

统计时长：

>

小时

服务端触发条件设置

服务端地址：

or

HIS主数据库

his主数据库2

数据库名：

or

HIS主库实例名

错误代码：

or

请选择：

执行结果：☒成功 ☒失败 ☒N/A

记录返回值：☒记录，记录不超过

4096

 字节

执行时长：

>

秒

影响行数：

>

触发阈值： 次/分钟

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）

。

