

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

zhilliao_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：

规则配置	对象组管理	规则优先级	快速加载
ORACLE-003-0004 可疑的账号在非工作时间对数据库的操作 ORACLE-003-0003 可疑的账号访问行为 ORACLE-003-0002 可疑的客户端工具访问行为 ORACLE-003-0001 可疑的IP地址访问行为 ORACLE-002-0028 可疑的系统配置参数变更 ORACLE-002-0027 可疑的library创建、删除 ORACLE-002-0026 可疑的context创建、删除 ORACLE-002-0025 可疑的outline创建、修改、删除 ORACLE-002-0024 可疑的operator创建、修改、删除 ORACLE-002-0023 可疑的java创建、修改、删除 ORACLE-002-0022 可疑的indextype创建、修改、删除 ORACLE-002-0021 可疑的dimension创建、修改、删除 ORACLE-002-0020 可疑的cluster创建、修改、删除 ORACLE-002-0019 可疑的type创建、修改、删除 ORACLE-002-0018 可疑的profile、splitfile、controlfile文件创建、删除 ORACLE-002-0017 可疑的schema创建 ORACLE-002-0016 可疑的profile创建、删除 ORACLE-002-0015 可疑的diskgroup创建、删除 ORACLE-002-0014 可疑的synonym创建、删除 ORACLE-002-0013 可疑的directory变更 ORACLE-002-0012 可疑的物化视图创建、修改、删除 规则名称 bsoft 状态 已启用禁用 规则等级 高 规则类型 普通规则 规则组 ORACLE内置规则组 对象组 系统对象组之所有对象查看 操作类型 Select SQL关键字 条件1: v_sy_fmxx 条件2: zy_fmxx 条件3: yf_fmxx 条件4: yf_fmxx 运算逻辑表达式: 1 2 3 4 每天查告最大个数 1000 业务主机群 没有选择业务主机群 白名单 无 修改 删除			

基本信息 显示更多

规则名称	bsoft
必填项，最大长度255个字节。	
规则等级	☒ 高 ☐ 中 ☐ 低 ☐ 关注行为 ☐ 一般行为 ☐ 不审计
规则类型	☒ 普通规则 ☐ 统计规则
规则组	ORACLE内置规则组

客户端 显示更多

客户端IP	☐ IP ☒ 来访客户网络
等于 如果要配置的选项不存在，可在下拉框中点击“新增”添加，或前往“配置-来访客户网络”页面设置。 例如IP： 可填多值，多个值间以逗号分隔，例：192.168.1.2,192.168.1.3。	
客户端工具	等于全部 如果要配置的选项不存在，可在下拉框中点击“新增”添加，或前往“配置-客户端工具”页面设置。
客户端端口	全部 可配置多个值或区间，多个值间以逗号分隔，例：10-15,20,25,30-40。

服务端 显示更多

服务端IP	等于全部 可填多值，多个值间以逗号分隔，例：192.168.1.2,192.168.1.3。
服务端端口	全部 可配置多个值或区间，多个值间以逗号分隔，例：10-15,20,25,30-40。
数据库账号	等于全部 可填多值，多个值间以逗号分隔，例：xxx,yyy。

行为

显示更多

对象组

系统对象组中的所有对象

新增

查看

操作类型

☒ Select

☐ Insert

☐ Update

☐ Delete

☐ Truncate

☐ Create

☐ Alter

☐ Drop

☐ Rollback

☐ Grant

☐ Revoke

☐ Execute

☐ Call

☐ Login

☐ Logout

SQL模板

全部

请输入SQL模板的ID，可填多值，多个值间以逗号分隔。

SQL关键字

1

☒

v_zy_fymx

2

☒

zy_fymx

3

☒

yf_zyfymx

4

☒

yf_mzfymx

增加条件

条件运算逻辑表达式:

1|2|3|4

请输入条件间的关系，支持“与、或、非、括号”运算(&: 与, |: 或, ~: 非), 条件使用序号表示, 即“1”表示条件1, 例: ~(1&(~3|2))

结果

显示更多

执行时长

大于等于

允许查悉从0到2000000000之间的任意范围。SQL执行时长属于此范围，则触发规则。

影响行数

大于等于

允许查悉从0到2147483647之间的任意范围。SQL操作返回的记录数或受影响的行数属于此范围，则触发规则。

返回结果集

1

☒

增加条件

条件运算逻辑表达式:

请输入条件间的关系，支持“与、或、非、括号”运算(&: 与, |: 或, ~: 非), 条件使用序号表示, 即“1”表示条件1, 例: ~(1&(~3|2))

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



时间范围

最近 12 小时

报文

只查询DB记录

查询

展开

客户端IP	服务端IP	端口	报文	执行结果	时间
55.55.0.51	55.55.0.1	PORTAL...	select * from v_zy_fymx	some records found	2018-10-17 11:53:19
55.55.0.51	55.55.0.1	PORTAL...	select * from v_zy_fymx	some records found	2018-10-17 11:53:09
55.55.0.51	55.55.0.1	PORTAL...	SELECT 'COLUMN' type, owner, table_name object_name, column_name, colu...	some records found	2018-10-17 11:50:38
55.55.0.51	55.55.0.1	PORTAL...	begin SYS.DBMS_UTILITY.NAME_RESOLVE(v_zy_fymx',0,'','',''); end;	PL/SQL Procedure complete	2018-10-17 11:50:38

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

其他

时间

☒ 任意时间 ☐ 天 ☐ 星期 ☐ 月

每天告警最大个数

1000

允许范围0到99999，输入0表示没有限制。

业务主机群

没有选择业务主机群

白名单

无

新增

选择

保存

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。

。

 最新告警



! 2086

! 0

! 0

! 0



16:18:57 2018-10-17	! bsoft 客户端IP: 55.55.64.6, 服务端IP: 55.55.0.1
16:18:46 2018-10-17	! bsoft 客户端IP: 55.55.80.55, 服务端IP: 55.55.0.1
16:18:47 2018-10-17	! bsoft 客户端IP: 55.55.80.18, 服务端IP: 55.55.0.1
16:18:49 2018-10-17	! bsoft