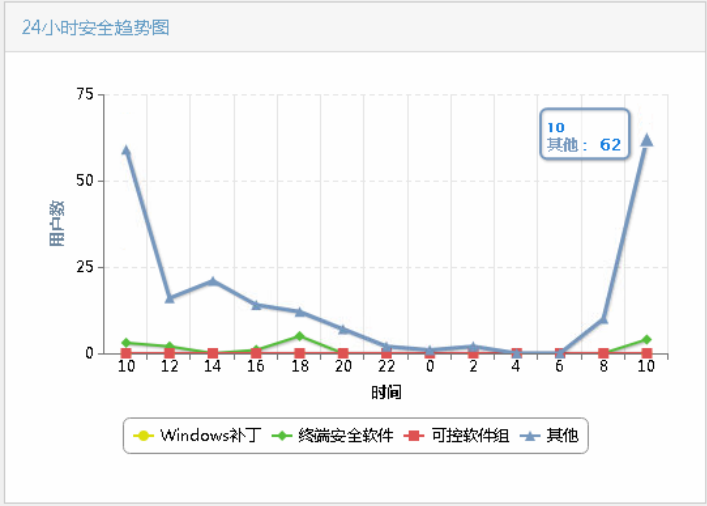
安全趋势图中“其他”项用户数量过多

汤祺　2018-01-04 发表

用户首页的“24小时安全趋势图”中“其他”项用户数量远远大于其他三项，但安全策略中只开启了一项杀毒软件检查项，应该被记录在“终端安全软件”检查项中。



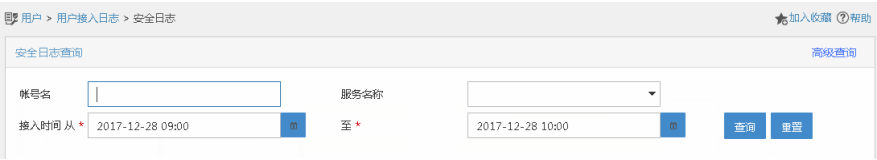
无任何报错，只是“其他”项远大于“终端安全软件”项的用户数。

1、 查看引用的安全策略

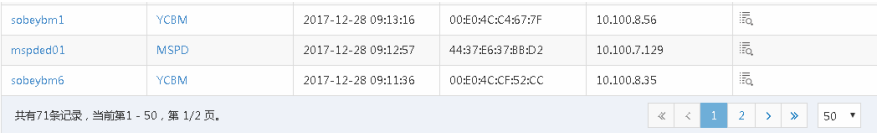
确认进行安全检查的用户采用的接入服务中引用的安全策略除了进行杀毒软件一项检查外，没有进行其他安全项检查。

2、 查看安全日志

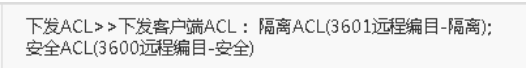
将安全日志的查看时间段设定为9:00-10:00段内，查看该时间段内进行安全检查的用户数量，及安全检查完成后用户状态信息。



在该时间段内进行安全检查的用户记录有71条，然而安全趋势图中，多达62个用户数量被记录在“其他”项中。



3、 查看用户的详细信息，查看用户安全检查后的安全状态



该用户在进行杀毒软件该安全项检查通过后，直接下发了安全ACL，下发安全ACL后，也会被记录在“其他”项中。

安全日志中记录的9:00-10:00进行安全检查的用户数量有71位，安全趋势图中记录的10:00时“其他项”的用户数量有62位，且通过安全日志查看所有的用户信息，安全检查通过后都下发了安全ACL，所以都被记录在了“其他项”中，故为一正常现象。

1、安全趋势图中所列出的三项：windows补丁、终端安全软件、可控软件组，这三项以外的检查项都会被统计在“其他”项中。

2、且安全趋势图中默认记录安全检查不通过的用户数量，若想要将检查通过的用户数量也统计其中，可进入安全策略管理中的系统参数配置中，将“安全检查通过记录日志”选项勾选上即可。

3、检查安全趋势图中明确列出三项时，即使检查合格后下发了安全ACL，此时也会被记录在“其他”项中。

4、安全趋势图中明确列出的三项同时进行检查时，任何一项检查不通过都会分别在安全趋势图的相应的检查项中记录一次。

5、安全趋势图和在线用户趋势图中，同一时间点记录的用户数量没有对应关系，在线用户趋势图则根据在线用户数量进行统计的，为一累加项。安全趋势图则是根据安全日志中的用户安全检查项的不合格状态进行统计的，统计某一时间点某几项安全检查不通过用户数量。