安全威胁发现与运营管理平台CSAP-S 联动漏扫设备是SecPath SysScan-AE 处于离线状态

漏洞扫描 **陈启敏** 2021-09-30 发表

组网及说明

安全威胁发现与运营管理平台CSAP-S
漏扫设备SecPath SysScan-AE
二者路由可达

问题描述

现场在csap-s平台上添加漏扫设备scan-ae后，设备一直处于离线状态

过程分析

安全威胁发现与运营管理平台CSAP-S 联动漏扫设备是SecPath H3C安全威胁发现与运营管理平台漏扫联动配置举例 见下面链接

https://www.h3c.com/cn/d_202109/1472326_30005_0.htm

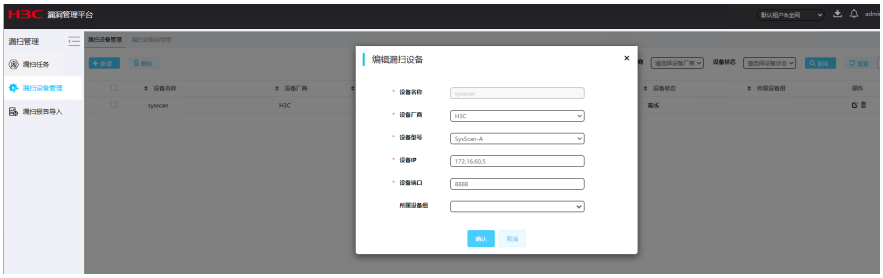
联动的配置前提是：

- CSAP平台、H3C漏扫设备、扫描目标之间网络互通
- 扫描目标为内网资产
- 添加H3C漏扫设备且状态在线

现场添加设备后能ping通，但是一直处于离线状态

信息如下：

一、态势感知平台内添加漏扫设备配置



二、设备状态为离线：

三、漏扫上ping平台正常：

四、态势感知版本及漏洞扫描版本信息

关于CSAP-S联动漏扫SCAN-AE，现有的软件版本是不支持的，需要提需求做适配

但是实验室还原了现场的设备做了测试，测试结果如下：

漏扫设备版本升级到6202P03版本，态势感知平台E1143P05，配置漏扫设备选择SysScan-AK，端口号的参数不配置，可以联动成功。

联动成功后出现下面问题：

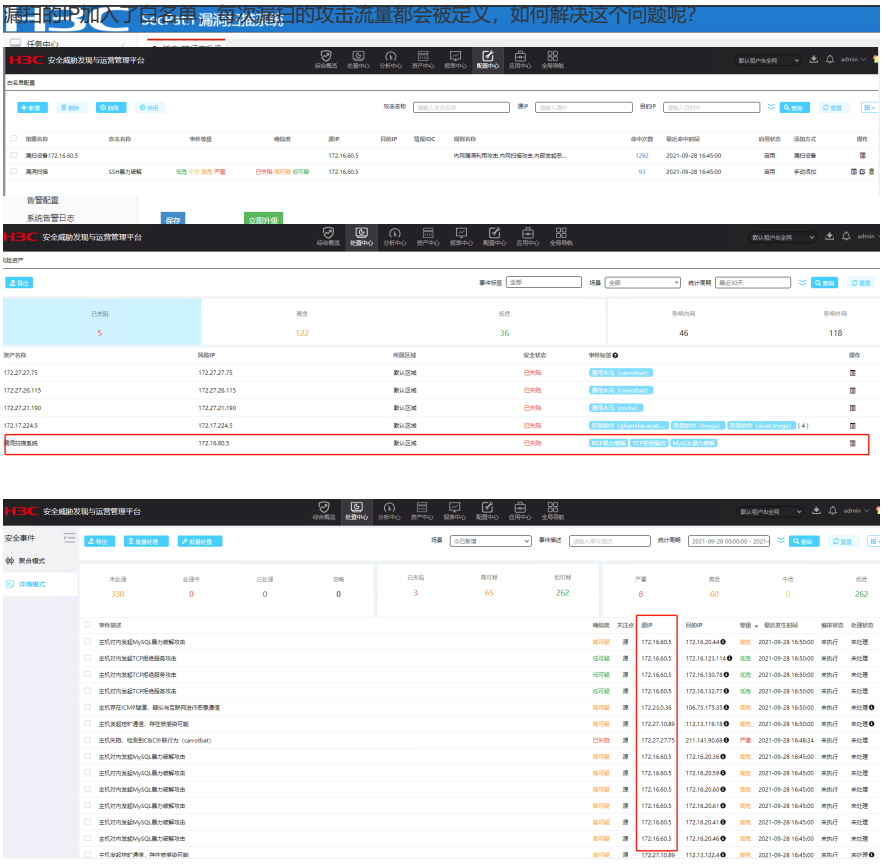
1)现场以SysScan-AK的方式可以添加，但是又出现问题：扫描目标不能超过64个

解决：确认了一下，是受设备型号限制，AE型号限制，与授权无关。目前只能现场那边多建几个扫描任务，一次不要超过64

2）新增了一个web扫描，任务开始后一直没反应。登录之漏洞扫描设备上后查看任务详情，发现任务一直排队等待中。直接在漏扫上面是可以正常扫描的，态势感知目前只加了一个web。

解决：远程确认现场的漏扫设备没有web扫描引擎，需要加入漏扫的web授权，这样漏扫的web扫描才会正常执行。web扫描属于扩展的增量授权，基础授权仅含系统扫描和数据库扫描。

3）现在漏扫对内网发起扫描后，态势感知便将漏扫扫描的流量记录下来了，并定义为风险资产，即使漏扫IP加入了白名单，每次漏扫的攻击流量都会被定义，如何解决这个问题呢？



解决：删除白名单配置里的攻击名称之后，可以正常过滤。配置攻击名称则只会过滤与名称一致的攻击流量。