H3C 安全威胁发现与运营管理平台

知识图谱典型配置举例

目 录

1 简介

本文档介绍知识图谱分析功能的典型配置举例。

安全威胁发现与运营管理平台（以下简称 CSAP）通过对接安全知识大脑平台，实时计算用户网络中发生的安全事件与各类大规模网络安全事件的相似程度，从而识别蠕虫病毒、僵尸网络、APT 攻击等深度威胁，同时提供攻击源、疑似失陷资产、举证日志等关键信息，帮助管理员快速定位内网隐患、阻断攻击源头。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

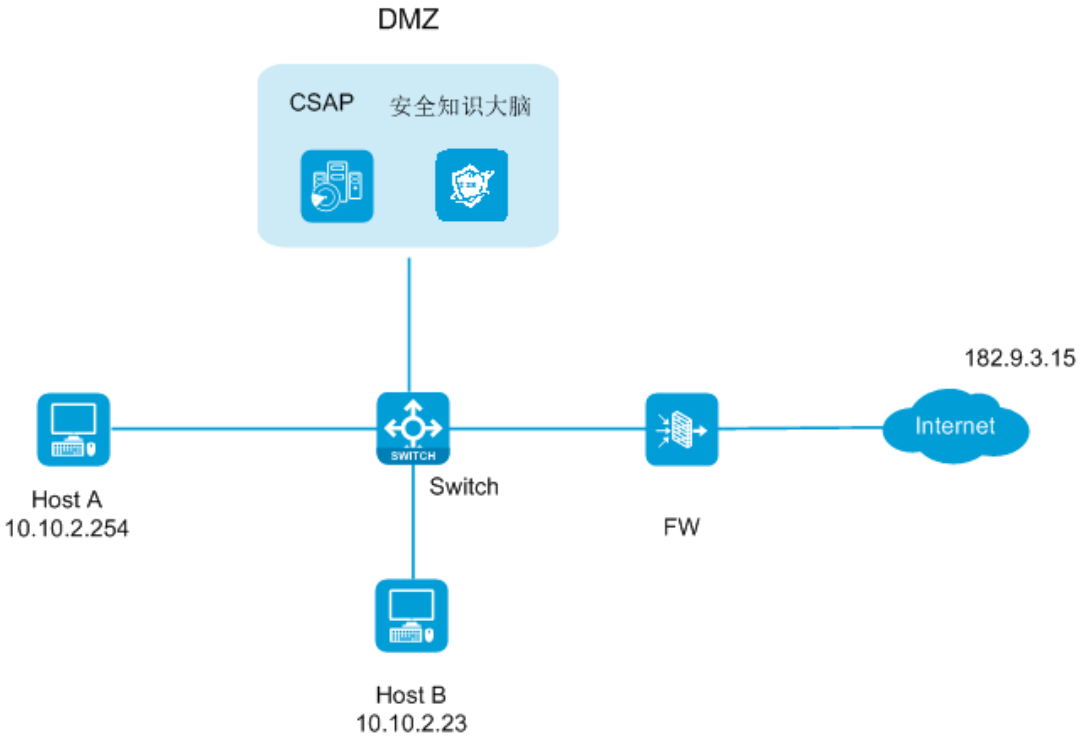
本文档假设您已了解 CSAP 和安全知识大脑平台基本使用。

3 配置举例

3.1 组网需求

如下图所示，日志源（FW）上报的攻击日志，经过安全知识大脑平台及 CSAP 的检测分析，识别出蠕虫病毒、僵尸网络、APT 攻击等深度威胁并展示。

图1 知识图谱分析典型配置组网图



3.2 配置思路

- 安全知识大脑平台注册到 CSAP
- CSAP 接入 FW 的攻击日志

3.3 使用版本

此功能支持 E1142P01 及以上版本。本举例是在 CSAP 的 E1143 版本上进行配置和验证的。

3.4 配置注意事项

安全知识大脑平台与 CSAP 平台网络互通。

3.5 配置步骤

3.5.1 安全知识大脑平台注册

登录安全知识大脑平台，点击态势接入，如下图所示。

图2 安全知识大脑平台注册

- 服务器地址：标准版配置为["186.64.100.111:9092"]，集群版配置为["186.64.9.121:9093", "186.64.9.122:9093", "186.64.9.123:9093"]（cyber1、cyber2、cyber3）
- 归一化日志 topic：security_0
- 安全事件 topic：traffic-dect-result
- 注册 URL：标准版注册 URL 为 https://186.64.100.111/externalInterface/activateMenu，集群版注册 URL 为 https://186.64.9.123/externalInterface/activateMenu（cyber3）

3.5.2 CSAP平台接入FW的攻击日志

配置 CSAP 接入 FW 的攻击日志，具体配置步骤略。

3.6 验证配置

3.6.1 知识图谱分析

登录 CSAP，选择“分析中心>场景化分析 > 知识图谱分析”，可查看到蠕虫病毒攻击事件。如下图所示。

图3 知识图谱分析


统计周期 最近30天
威胁概览 共6个
00014
僵尸网络
影响节点:3
00004
僵尸网络
影响节点:4
00006
僵尸网络
影响节点:3
00051
蠕虫病毒
影响节点:12
00039
僵尸网络
影响节点:3
00008
僵尸网络
影响节点:3


统计周期 最近30天
返回概览
蠕虫病毒
自动布局
手动拖拽
聚集模式
节点IP
图例
请输入IP地址定位节点
缩略图
00008
僵尸网络
00051
蠕虫病毒
00004
僵尸网络
00014
僵尸网络
00039
僵尸网络
00006
僵尸网络
10.10.2.254
10.10.2.23
10.10.2.114
10.10.2.109
182.9.3.15
10.10.2.137
10.10.2.131
10.10.2.144
10.10.2.13
10.10.2.70
10.10.2.84
10.10.2.232
内网用户
内网资产
外网用户
攻击源
疑似C&C，建议验证后加入阻断名单
攻击跳板
疑似失陷资产，建议审计日志、加固防御
攻击目标
疑似暴露敏感端口，建议检查安全基线
疑似攻击源
攻击事件中的攻击源
疑似跳板
攻击事件中的攻击跳板
疑似目标
攻击事件中的攻击目标
编号
发生时间
威胁类型/置信度
影响节点
安全事件总数
攻击链
攻击源
攻击跳板
攻击目标
00051
2020-09-28 06:21:46
蠕虫病毒 / 88.43%
12
9
10
1
1
10