csap-s/csap-c 资产自动发现原理

日志采集器 安全监测中心 **杨雅伦** 2022-05-19 发表

问题描述

流量发现资产：开启流量发现功能后，系统基于网络流量自动识别区域中可管理的资产，将其添加到资产列表。通过该方式添加的资产，其添加方式为“流量发现”。

具体的原理机制是什么

解决方法

基于设备上报的日志，主要是流量日志，根据流量日志里的源目的IP，如果在区域里（且不在用户网段），就会发现为资产。