FMC关联策略允许列表事件需要启用网络发现策略

目录

问题

在思科安全防火墙管理中心(FMC)上使用允许列表配置关联策略时，请务必注意，除非为目标网络IP配置了网络发现策略，否则不会生成允许列表事件和允许列表违规。如果没有此配置，则Analysis > Correlation > Allow List Events和Analysis > Correlation > Allow List Violations下不会显示任何事件。

在实验室检测过程中，观察到以下行为：

- 为已配置的目标网络正确生成关联事件。
- 当目标网络主机变为不合规时，不会生成允许列表事件或允许列表违规。

环境

- 由安全防火墙管理中心(FMC)管理的Cisco Firepower威胁防御(FTD)
- 使用允许列表针对特定IP地址配置的关联策略
- 允许配置为允许特定Web应用、应用或协议的列表

分辨率

经过广泛的实验室测试并与开发团队协商，确认必须启用网络发现策略，才能生成允许列表事件和允许列表违规。

解决方案涉及以下步骤：

步骤 1：启用网络发现策略

在FMC界面中导航到Policies > Network Discovery，并创建规则（如果不存在）。

步骤 2：配置网络发现规则

使用适当的源网络设置配置网络发现规则：

- 将源网络指定为内部网络范围。
- 或者，如果监控所有流量源，请使用所有网络(0.0.0.0/0)。
- 确保规则涵盖预期从中生成Allow List Events的网络。

步骤 3：激活关联策略规则

验证关联策略规则处于活动状态且未处于禁用状态。

步骤 4：验证允许列表事件生成

启用网络发现并激活关联策略规则后：

1. — 使用浏览器从已配置的目标网络访问网站（使主机成为不合规）。

2. — 监控分析>关联>允许列表事件和分析>关联>允许列表违规生成事件。

3. — 验证主机不符合要求时是否填充了事件。

实验室测试确认，一旦启用Network Discovery，将为不合规主机成功生成Allow List Events和Allow

List Violations。

原因

根本原因是，网络发现策略是在FMC关联策略中生成允许列表事件的必备条件。如果没有活动的网络发现策略，系统无法根据配置的允许列表正确评估主机合规性，导致目标网络主机变为不合规时，不会生成允许列表事件。

相关内容

- Cisco FMC关联合规性列表文档
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。