基于Webhook的安全事件 ；是 ；不是 ；已接收 at ；内部HTTP连接器 ；用于 SIEM集成

目录

问题

本地HTTP连接器未收到基于Webhook的安全事件以进行SIEM集成。

环境

- 产品：思科安全访问(SSE)
- 技术：解决方案支持 — 安全访问报告和日志记录
- 集成类型：基于Webhook的第三方集成
- 目标连接器：本地HTTP连接器
- 控制面板状态：在“管理”(Admin)>“第三方集成”(Third Party Integrations)中成功加载第三方集成

分辨率

要解决Cisco Secure Access第三方集成的Webhook传输问题，请配置防火墙规则以允许来自这些Cisco SSE源IP范围的入站HTTPS流量。

所需的防火墙配置

允许从以下Cisco SSE源IP范围到本地连接器的入站HTTPS流量：

```
146.112.161.0/24

146.112.163.0/24

146.112.165.0/24

146.112.167.0/24
```

这些IP范围代表欧盟和美国地区的思科SSE用于Webhook传输的共享IP地址。

验证步骤

第1步：在SSE控制面板中验证第三方集成状态。

导航到SSE控制面板中的Admin > Third Party Integrations，确认已为您的组织正确加载集成。

第2步：配置防火墙规则。

更新您的网络防火墙和任何中间防火墙，以允许从提供的SSE IP范围到您的本地连接器服务器的入站HTTPS连接。

第3步：监控webhook事件传输。

实施防火墙更改后，监控您的本地HTTP连接器，以验证是否正在从Cisco SSE接收Webhook事件。

其他故障排除

如果在配置防火墙规则后仍未收到webhook事件：

- 验证本地连接器已正确配置并在预期端口上侦听。
- 检查SSE源IP和连接器端点之间的网络连接。
- 查看SSE控制面板中的Webhook集成配置。
- 考虑安排实时故障排除会话，以实时查看Webhook交付。

原因

当网络防火墙阻止从思科SSE源IP地址到本地HTTP连接器的入站HTTPS连接时，就会发生Webhook传递故障。思科SSE使用来自欧盟和美国地区的共享基础设施的特定IP范围来传送Webhook事件，并且必须明确允许这些内容通过防火墙配置才能成功传送事件。

相关内容

- 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）。