

Eventos de seguridad basados en Webhook are not Received at the On-prem HTTP Connector for Integración con SIEM

Contenido

Problema

Los eventos de seguridad basados en Webhook no se reciben en el conector HTTP local para la integración con SIEM.

Entorno

- Producto: Cisco Secure Access (SSE)
- Tecnología: Asistencia para soluciones: informes y registros de acceso seguro
- Tipo de integración: integración de terceros basada en Webhook
- Conector de destino: conector HTTP local
- Estado del panel: las integraciones de terceros se cargan correctamente en Administración > Integraciones de terceros

Resolución

Para resolver problemas de entrega de webhook con integraciones de terceros de Cisco Secure Access, configure reglas de firewall para permitir el tráfico HTTPS entrante desde estos intervalos de IP de origen de Cisco SSE.

Configuración de firewall necesaria

Permitir el tráfico HTTPS entrante desde estos intervalos de IP de origen de Cisco SSE al conector local:

146.112.161.0/24

146.112.163.0/24

146.112.165.0/24

146.112.167.0/24

Estos intervalos de IP representan las direcciones IP compartidas que utiliza Cisco SSE de regiones de la UE y EE. UU. para la entrega de webhook.

Pasos de verificación

Paso 1: Verifique el estado de integración de terceros en el panel de SSE.

Vaya a Admin > Third Party Integrations en su panel de SSE y confirme que las integraciones se cargan correctamente para su organización.

Paso 2: Configurar las reglas del firewall.

Actualice el firewall de red y cualquier firewall que intervenga para permitir conexiones HTTPS entrantes desde los intervalos IP SSE proporcionados al servidor del conector local.

Paso 3: supervise la entrega de eventos de webhook.

Después de implementar los cambios del firewall, supervise su conector HTTP local para verificar que los eventos de webhook se reciben desde Cisco SSE.

Resolución de otros problemas

Si los eventos de webhook siguen sin recibirse después de configurar las reglas del firewall:

- Verifique que el conector local esté configurado correctamente y que escuche en el puerto esperado.
- Compruebe la conectividad de red entre las IP de origen de SSE y el terminal del conector.
- Revise la configuración de integración de webhook en el panel de SSE.
- Considere la posibilidad de programar una sesión de resolución de problemas en directo para revisar la entrega de webhook en tiempo real.

Causa

El fallo en la entrega de webhook se produce cuando los firewalls de red bloquean las conexiones HTTPS entrantes de las direcciones IP de origen de Cisco SSE al conector HTTP en las instalaciones. Cisco SSE utiliza rangos de IP específicos de la infraestructura compartida en las regiones de la UE y EE. UU. para ofrecer eventos de webhook, que deben permitirse explícitamente a través de configuraciones de firewall para que la entrega de eventos se realice correctamente.

Contenido relacionado

- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).