La directiva de correlación de FMC Permitir eventos de lista requiere que se habilite la directiva de detección de red

Contenido

Problema

Al configurar las políticas de correlación con las listas de permitidos en Cisco Secure Firewall Management Center (FMC), es importante tener en cuenta que Allow List Events y Allow List Violations no se generan a menos que se configure la política de detección de red para la IP de red de destino. Sin esta configuración, no aparecen eventos en Analysis > Correlation > Allow List Events y Analysis > Correlation > Allow List Violations.

Durante las pruebas de laboratorio, se observaron estas conductas:

- Los eventos de correlación se generan correctamente para la red de destino configurada.
- No se generan Eventos de lista permitidos o Infracciones de lista permitidas cuando el host de red de destino deja de ser conforme.

Entorno

- Cisco Firepower Threat Defence (FTD) gestionado por el centro de gestión de firewall seguro (FMC)
- Política de correlación configurada con direcciones IP específicas de destinatarios de la lista de permitidos
- Permitir lista configurada para permitir una aplicación web, aplicación o protocolo específico

Resolución

Después de extensas pruebas de laboratorio y consultas con el equipo de desarrollo, se confirmó que la política Network Discovery debe habilitarse como requisito previo para que se generen Allow List Events y Allow List Violations.

La resolución implica estos pasos:

Paso 1: Habilitar directiva de descubrimiento de red

Navegue hasta Políticas > Detección de red en la interfaz FMC y cree una regla si no existe ninguna.

Paso 2: Configurar regla de detección de red

Configure la regla de detección de red con la configuración de red de origen adecuada:

- Especifique la red de origen como intervalo de red interna.
- También puede utilizar todas las redes (0.0.0.0/0) si desea supervisar todas las fuentes de tráfico.
- Asegúrese de que la regla cubre las redes desde las que espera generar Allow List Events.

Paso 3: Activar reglas de política de correlación

Verifique que las reglas de la política de correlación estén activas y no en un estado inhabilitado.

Paso 4: Verificar generación de eventos de lista permitidos

Después de habilitar la detección de red y activar las reglas de la política de correlación:

1.- Acceder a los sitios web desde la Red de Destino configurada utilizando un navegador (haciendo que el host no sea conforme).

2.- Monitorear Análisis > Correlación > Permitir Eventos de Lista y Análisis > Correlación > Permitir Violaciones de Lista para la generación de eventos.

3.- Verificar que los eventos se rellenan cuando el host se está convirtiendo en no conforme.

Las pruebas de laboratorio confirmaron que, una vez habilitada la Detección de red, Permitir eventos de lista y Permitir violaciones de lista se generan correctamente para un host no conforme.

Causa

La causa raíz es que Network Discovery Policy es un requisito obligatorio para generar Allow List Events en FMC Correlation Policies. Sin una política de detección de red activa, el sistema no puede evaluar correctamente el cumplimiento del host con respecto a la lista de permitidos configurada, lo que hace que no se genere ningún evento de lista de permitidos cuando el host de la red de destino deja de ser compatible.

Contenido relacionado

- Documentación de las listas de conformidad de Cisco FMC Correlation
- 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).