Solución de problemas de Cisco XDR y análisis de malware seguro Integración con la nube

Contenido

Introducción

Este documento describe cómo resolver problemas del módulo Secure Malware Analytics Cloud con Cisco XDR.

Colaboración de Javi Martínez, ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Nube de análisis de malware seguro
- Cisco XDR

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Consola de Secure Malware Analytics Cloud (cuenta de usuario con derechos de administrador)
- Consola Cisco XDR (cuenta de usuario con derechos de administrador)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco Secure Malware Analytics Cloud es una plataforma avanzada y automatizada de análisis de malware e inteligencia de amenazas de malware en la que se pueden detonar archivos sospechosos o destinos web sin que ello repercuta en el entorno del usuario.

En la integración con Cisco XDR, Secure Malware Analytics es un módulo de referencia que permite acceder al portal Secure Malware Analytics para recopilar inteligencia adicional sobre los hashes de archivos, las IP, los dominios y las URL en el almacén de conocimientos Secure Malware Analytics Cloud (SMA Cloud).

Consulte la última Guía de integración en la nube de Secure Malware Analytics,

- Nube NAM.
- Nube de la UE.

Troubleshoot

Licencia

- Verifique que tiene una licencia SMA adecuada para obtener acceso a la consola Secure Malware Analytics Cloud

Azulejos de módulo

- Verifique que selecciona los ***mosaicos*** adecuados para Secure Malware Analytics Cloud Module
  Vaya al portal Cisco XDR > Panel > Botón Personalizar > Seleccione el módulo SMA Cloud > Agregar los mosaicos adecuados

Función de administrador

- Compruebe que dispone de una cuenta de Secure Malware Analytics con la función de administrador en el portal de Secure Malware Analytics
  Vaya al portal de Cisco XDR > Administración > Su cuenta

- Compruebe que dispone de una cuenta SecureX con derechos de administrador en el portal SecureX
  Vaya al portal de análisis de malware > Mi cuenta de análisis de malware

Nota: si no tiene un rol de administrador en la consola de Secure Malware Analytics y en la consola de Cisco XDR, su administrador podrá cambiar el rol de cuenta directamente desde el portal en cuestión

Plazo

- Verifique que Timestamp esté configurado correctamente en el portal Cisco XDR.
  Navegue hasta Portal Cisco XDR > Panel > Opción de plazos > Seleccione el plazo adecuado en función de la actividad del SMA

Volver a crear módulo

- Elimine el módulo SMA antiguo y cree un nuevo módulo SMA.
  Vaya a Secure Malware Analytics Cloud console > My Malware Analytics account > API Key > Copy the API key
  Vaya al portal de Cisco XDR > Módulos de integración > Seleccione el módulo SMA Cloud > Agregar la clave de API y URL (Seleccione la nube SMA) > Crear el panel

Nota: solo los usuarios con el rol de administrador de organización o usuarios pueden obtener la clave de la API que habilita el módulo de integración Análisis de malware seguro en Cisco XDR.

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).