Problemas conocidos de Cisco XDR

Contenido

Introducción

En este artículo se documentan los problemas técnicos conocidos de Cisco XDR.

Cisco puede reconocer los problemas técnicos, revisarlos, resolverlos o considerar que funcionan según lo previsto.

Problemas conocidos:

Incidentes

No hay problemas conocidos para esta funcionalidad XDR en este momento.

Investigaciones

No hay problemas conocidos para esta funcionalidad XDR en este momento.

Centro de control

No hay problemas conocidos para esta funcionalidad XDR en este momento.

Integraciones de Cisco

1. Cisco XDR: integración completa con Cisco Secure Firewall

Detalles: para garantizar una integración perfecta entre Cisco Defense Orchestrator (CDO), Security Services Exchange (SSX) y Security Analytics and Logging (SAL), se requiere asignación manual. Este proceso implica ponerse en contacto con el TAC de Cisco para realizar las configuraciones y asignaciones necesarias.

Solución: Póngase en contacto con el TAC para ayudar a vincular las cuentas pertinentes y garantizar la integración adecuada de los sistemas.

Resolución esperada: TBD

Integraciones de terceros

1.- Los clientes de Microsoft con licencias tipo G no pueden utilizar las integraciones XDR de Microsoft.

Estado: Trabajo según diseño

Detalles: los derechos de tipo G de Microsoft solo se proporcionan acceso en entornos controlados para entidades gubernamentales.

Siguientes pasos: Cisco está trabajando con Microsoft para comprender los requisitos para integrarse con el entorno de Microsoft GCC en el que se proporcionan los derechos de tipo G de Microsoft. Si es viable, Cisco XDR pretende integrarse con las licencias Microsoft G-type para Microsoft Defender for Endpoint, O365 y EntraID.

Resolución esperada: resuelta, integración disponible aquí.

Recursos

No hay problemas conocidos para esta funcionalidad XDR en este momento.

Automatización de XDR

No hay problemas conocidos para esta funcionalidad XDR en este momento.

Dispositivos/sensores

No hay problemas conocidos para esta funcionalidad XDR en este momento.

Cliente seguro

Para consultar los problemas de Secure Client, siga el artículo.

XDR-Analytics

1. - Varias direcciones IP y/o varios nombres de host pueden asociarse a un único nombre de dispositivo en XDR-A

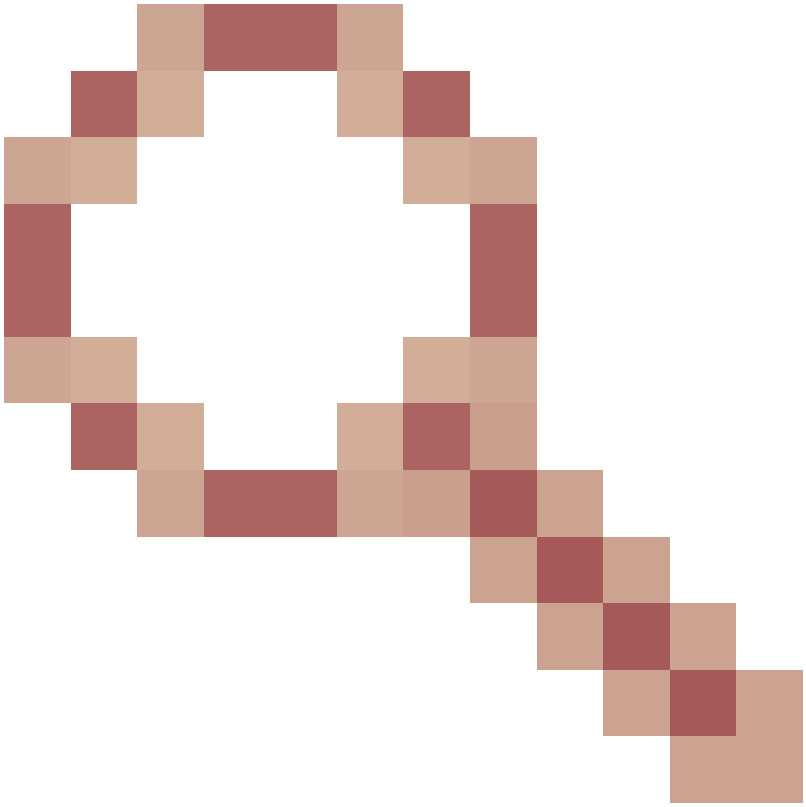
Estado: No resuelto/Pospuesto

Detalles: Varias direcciones IP activas pueden asociarse a un único dispositivo dentro del portal SNA/XDR-A. Esto puede incluir dispositivos NVM y no NVM. Algunos dispositivos también tienen varios nombres de host. Según la implementación actual, el registro de dispositivos podría dar lugar a que un dispositivo tuviera más de una dirección IP (ubicación). Algunas de estas direcciones IP pueden proceder de la red doméstica del usuario y pueden colisionar con direcciones IP de la red de la organización.

Solución: no hay ninguna solución alternativa para este problema en este momento, y el problema sigue existiendo en la arquitectura actual. Se espera que este problema se aborde mejor en el futuro, una vez que se implemente una nueva arquitectura que permita normalizar las actividades de red de ambas fuentes, ONA y NVM, a OCSF y agruparlas.

Pasos siguientes: N/A

Resolución: Futuro/por determinar



CDET de seguimiento: CSCwo67299

Problemas resueltos

1.- Cisco XDR: el enlace de integración de Cisco Secure Endpoint no funciona en el portal Cisco XDR

Estado: Problema identificado y pendiente de resolución

Detalles: En las pestañas Admin > Integrations el link "Enable" de Secure Endpoint está roto. Una vez que pulsamos el botón de activación, se redirige a la página Threat Response (Respuesta ante amenazas) y se redirige a la página del selector de organización XDR en

lugar de ir a Secure Endpoint Console.

Solución alternativa: La integración se puede realizar desde Cisco Secure Endpoint Portal

Pasos siguientes: Cisco está trabajando para implementar la solución para este problema

Resolución esperada: se ha resuelto este problema.

2.- XDR Automatizar Incidentes Reglas de Automatización inesperadamente deja de funcionar

Estado: problema identificado y pendiente de resolución

Detalles: las reglas de automatización de incidentes basadas en flujos de trabajo y desencadenadores dejan de ejecutarse inesperadamente. Esto no se indica en la interfaz de usuario de XDR, excepto cuando se revisan las métricas de Workflows Run Over Time. Al hacerlo, los clientes verán flujos de trabajo reducidos o nulos ejecutados, dependiendo del tiempo que el problema haya estado en curso.

Siguientes pasos: Cisco ha identificado este problema como un problema en el back-end XDR y está trabajando para resolverlo. Cisco también tiene previsto implementar funciones adicionales de supervisión y seguimiento de estado para evitar que este problema se produzca en el futuro.

Solución: deshabilite y vuelva a habilitar la regla para iniciar un reinicio de la activación y el procesamiento de la regla de flujo de trabajo.

Resolución esperada: resuelta.

3. - Cisco XDR-Analytics: error en la instalación de ONA en entornos virtuales con un error que indica "error en la verificación de la suma de comprobación"

Estado: problema identificado y pendiente de resolución

Detalles: Al implementar un sensor ONA en un entorno virtual, la ISO no puede completar el proceso de instalación y se produce un error.

Solución alternativa: Instale el servidor Ubuntu 24.04 de forma independiente con la ISO de Ubuntu y siga los pasos de instalación avanzada para ejecutar ONA como servicio. Utilice la compatibilidad 7.0 U2

Pasos siguientes: N/A

Resolución: Este problema se ha resuelto en la última versión del sensor ONA

4.-El cuadro MTTR del Centro de control muestra números inexactos de incidentes que se han resuelto mediante uno de los nuevos estados, como "Cerrado: "Falso positivo", "Cerrado: "Amenaza confirmada" u otra.

Estado: Problema identificado y pendiente de resolución

Detalles: El 15 de enero se introdujeron nuevos estados de incidente y el mosaico no toma en

consideración esos estados. Los nuevos estados de resolución se interpretan como trabajos en curso, por lo que incluso si el incidente se ha cerrado con uno de los nuevos estados, se contabiliza como trabajo en curso.

Solución alternativa: Ninguna

Siguientes pasos: Ninguno

Resolución esperada: resuelta

Si necesita ponerse en contacto con el Soporte de Cisco, siga las instrucciones que se proporcionan en este enlace.

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).