Problemas conhecidos do Cisco XDR

Contents

Introdução

Este artigo documenta problemas técnicos conhecidos atualmente para o Cisco XDR.

Problemas técnicos podem ser reconhecidos pela Cisco, estão sob revisão, pendentes de resolução ou podem ser considerados como funcionando conforme esperado.

Problemas conhecidos:

Incidentes

Não há problemas conhecidos para esta funcionalidade XDR no momento.

Exames complementares de diagnóstico

Não há problemas conhecidos para esta funcionalidade XDR no momento.

Centro de controle

O bloco 1.-MTTR no Centro de controle mostra números imprecisos de incidentes que foram resolvidos usando um dos novos estados, como "Fechado: Falso Positivo", "Fechado: Confirmed Threat" (Ameaça confirmada) ou outra.

Status: Problema identificado e resolução pendente

Detalhes: Novos estados incidentes foram introduzidos em 15 de janeiro e o bloco não leva

esses estados em consideração. Os novos estados de resolução são interpretados como trabalhos em andamento, portanto, mesmo que o incidente tenha sido encerrado usando um dos novos estados, ele é contabilizado como trabalho em andamento.

Solução alternativa: nenhuma

Próximas etapas: Nenhum

Resolução esperada: a ser definida

Integrações da Cisco

1.- Cisco XDR - O link de integração do Cisco Secure Endpoint não está funcionando no Cisco XDR Portal

Status: Problema identificado e resolução pendente

Detalhes: Nas guias Admin > Integrações, o link "Habilitar" do ponto de extremidade seguro está quebrado. Quando pressionamos o botão enable, ele é redirecionado para a página Threat Response (Resposta a ameaças) e faz o loop para a página do seletor XDR org em vez de ir para o Secure Endpoint Console.

Solução: A integração pode ser realizada no Cisco Secure Endpoint Portal

Próximas etapas: A Cisco está trabalhando para implementar a correção para esse problema

Resolução esperada: TBD

2. Cisco XDR - Integração total do Cisco Secure Firewall

Detalhes: Para garantir a integração perfeita entre o Cisco Defense Orchestrator (CDO), o Security Services Exchange (SSX) e o Security Analytics and Logging (SAL), é necessário o mapeamento manual. Esse processo envolve entrar em contato com o Cisco TAC para executar as configurações e os mapeamentos necessários.

Solução alternativa: entre em contato com o TAC para ajudar a vincular as contas relevantes e garantir a integração adequada dos sistemas.

Resolução esperada: TBD

Integrações com terceiros

1.- Os clientes da Microsoft com licenças do tipo G não podem utilizar as integrações XDR da Microsoft.

Status: Trabalhando como projetado

Detalhes: os direitos do tipo G da Microsoft têm acesso fornecido em ambientes controlados somente para entidades governamentais.

Próximas etapas: a Cisco está trabalhando com a Microsoft para entender os requisitos para integrar com o ambiente Microsoft GCC no qual os direitos do tipo G da Microsoft são fornecidos. Se viável, o Cisco XDR pretende se integrar com licenças do tipo G da Microsoft para Microsoft Defender for Endpoint, O365 e EntraID.

Resolução esperada: a ser definida

Ativos

Não há problemas conhecidos para esta funcionalidade XDR no momento.

XDR automatizado

1.- As regras de automação de incidentes do XDR param inesperadamente de funcionar

Status: Problema identificado e resolução pendente

Detalhes: Regras de automação de incidentes ativadas por fluxos de trabalho e acionadores param inesperadamente de funcionar. Isso não é indicado na interface de usuário do XDR, exceto ao revisar as métricas de Workflows Run Over Time (Fluxos de trabalho executados ao longo do tempo). Ao fazer isso, os clientes verão fluxos de trabalho reduzidos ou zero serem executados, dependendo de quanto tempo o problema está ocorrendo.

Próximas etapas: a Cisco identificou isso como um problema dentro do backend XDR e está trabalhando para resolvê-lo. A Cisco também planeja implementar recursos adicionais de monitoramento e rastreamento de estado para evitar que esse problema ocorra no futuro.

Solução alternativa: desative e reative a regra para iniciar uma reinicialização do disparo e processamento da regra de fluxo de trabalho.

Resolução esperada: março de 2025

Dispositivos/Sensores

1.- Cisco XDR-Analytics - Falha na instalação do ONA em ambientes virtuais com um erro indicando "falha na verificação do checksum"

Status: Problema identificado e resolução pendente

Detalhes: Ao implantar um sensor ONA em um ambiente virtual, o ISO falha ao concluir o processo de instalação e elimina erros.

Solução: Instale o Ubuntu Server 24.04 independentemente com o ISO do Ubuntu e siga as etapas de instalação avançada para executar o ONA como serviço. Use a compatibilidade 7.0 U2

Próximas etapas: A Cisco está trabalhando para implementar a correção para esse problema

Resolução: Próxima versão do sensor XDR

2.- Cisco XDR-Analytics - O gráfico de tráfego nos detalhes do sensor da ONA não é preenchido quando apenas a sonda ETA é configurada

Status: Problema identificado e resolução pendente

Detalhes: O gráfico de tráfego não mostra nenhum tráfego quando os ONAs são configurados somente com sonda ETA.

Solução alternativa: nenhuma

Próximas etapas: A Cisco está trabalhando para implementar a correção para esse problema

3.- Cisco XDR-Analytics - A telemetria ETA proveniente do Cisco Telemetry Broker (CTB) não é usada para preencher o painel ETA

Status: Problema identificado e resolução pendente

Detalhes: A telemetria ETA gerada pelo CTB ou carregada pelo CTB e gerada por outros dispositivos não é usada para preencher o painel ETA

Solução: Usar ONA com sonda ETA

Próximas etapas: Nenhum

Resolução: Próxima versão do sensor XDR

Cliente seguro

Para consultar os problemas do Secure Client, siga o artigo.

XDR-A

1. - Vários endereços IP e/ou vários nomes de host podem ser associados a um único nome de dispositivo no XDR-A

Status: Não Resolvido/Adiado

Detalhes: Vários endereços IP ativos podem ser associados a um único dispositivo dentro do portal SNA/XDR-A. Isso pode incluir dispositivos NVM e não NVM. Alguns dispositivos também têm vários nomes de host. Com base na implementação atual, o registro de dispositivos pode fazer com que um dispositivo tenha mais de um endereço IP (local). Alguns desses endereços IP podem ser da rede doméstica do usuário e podem colidir com os endereços IP na rede da organização.

Solução alternativa: não há solução alternativa para esse problema no momento e o problema ainda existe na arquitetura atual. Há esperanças de que este problema possa ser melhor tratado no futuro, uma vez que a nova arquitetura é implementada, o que permitirá que as atividades de rede de ambas as fontes ONA e NVM sejam normalizadas para OCSF e reunidas.

Próximas etapas: N/A

Resolução: Futuro / a ser definido

Problemas Resolvidos

1.- A opção Marcar tarefa como não aplicável é considerada somente na criação do incidente XDR e não na atualização do incidente.

Status: Resolvido

Detalhes: Os manuais de atividades de respostas guiadas do Cisco XDR oferecem a opção de ocultar tarefas que não se aplicam ao incidente atual. Em outubro de 2024, a Cisco lançou um aprimoramento para o Cisco XDR para ocultar automaticamente as tarefas sem nenhum Observable aplicável. Essa melhoria funciona quando um incidente é criado, mas não avalia as tarefas aplicáveis quando atualizadas.

Próximas etapas: correção implementada

Se precisar entrar em contato com o Suporte da Cisco, siga as instruções fornecidas neste link.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.