Cisco XDR bekende problemen

Inhoud

Inleiding

Dit artikel documenteert momenteel bekende technische problemen voor Cisco XDR

Technische problemen kunnen worden bevestigd door Cisco, worden beoordeeld, worden behandeld in afwachting van een oplossing of worden geacht te werken zoals verwacht.

Bekende problemen:

Incidenten

1.- Mark Task Not Applicable optie wordt alleen overwogen bij XDR Incident creatie en niet bij Incident update.

> Status: Identificatie van probleem en hangende oplossing
>
> Details: Cisco XDR Guided Response-playbooks selecteer de optie om te verbergen taken die niet van toepassing zijn op het huidige incident. In oktober 2024 heeft Cisco een uitbreiding op Cisco XDR uitgebracht om taken automatisch te verbergen zonder toepasselijke observabels. Deze verbetering werkt wanneer een incident wordt gecreëerd, maar beoordeelt geen toepasselijke taken wanneer deze worden bijgewerkt.
>
> Volgende stappen: Cisco werkt aan de implementatie van de oplossing voor dit probleem
>
> Verwachte resolutie: december 2024

Onderzoeken

Geen bekende problemen voor deze XDR-functie op dit moment.

Cisco-integraties

Geen bekende problemen voor deze XDR-functie op dit moment.

Integraties van derden

1. - Microsoft-klanten met G-type licenties kunnen de XDR Microsoft-integraties niet gebruiken.

    Status: Werken zoals ontworpen

    Details: Microsoft G-type rechten zijn alleen toegankelijk via provisioning in gecontroleerde omgevingen voor overheidsentiteiten.

    Volgende stappen: Cisco werkt samen met Microsoft om de vereisten te begrijpen in integreren met de Microsoft GCC-omgeving waarin Microsoft G-type rechten worden verstrekt. Indien levensvatbaar, Cisco XDR is voornemens te integreren met Microsoft G-type licenties voor Microsoft Defender for Endpoint, O365 en Entra.

Activa

Geen bekende problemen voor deze XDR-functie op dit moment.

XDR automatiseren

1.- De regels van de Automation van het Incident van XDR houden onverwacht op lopend

    Status: Identificatie van probleem en hangende oplossing

    Details: Regels voor incidentautomatisering aangedreven door werkstromen en triggers stop onverwacht met rennen. Dit is niet aangegeven in de XDR-gebruikersinterface, behalve bij het bekijken de maatstaven Werkstromen verlopen over een bepaalde tijd. Als ze dit doen, zullen klanten minder of geen workflows zien draaien, afhankelijk van hoe lang het probleem aan de gang is.

    Volgende stappen: Cisco heeft dit probleem binnen de XDR-backend geïdentificeerd en werkt eraan om het op te lossen. Cisco is ook van plan extra bewakings- en statustracingfuncties te implementeren om te voorkomen dat dit probleem in de toekomst optreedt.

    Tijdelijke oplossing: Schakel de regel uit en weer in om een herstart van het starten en verwerken van de werkstroomregel te starten.

    Verwachte resolutie: januari 2025

XDR-analyse

Geen bekende problemen voor deze XDR-functie op dit moment.

Beveiligde client

1.- Beveiligde client-/endpointimplementaties worden beïnvloed door Microsoft Intune/Microsoft Defender voor endpointupdates, waardoor een juiste installatie wordt voorkomen

Status: Werken zoals ontworpen

Details: Doorlopend: Dit probleem heeft gevolgen voor Cisco XDR-klanten die Cisco Secure Client for Network Visibility Module (NVM) installeren met Cisco XDR. Microsoft Defender for Endpoint settings (geconfigureerd via Intune) zorgen ervoor dat Secure Client niet goed kan worden geïnstalleerd. Wanneer een functie momenteel wordt bekeken in Microsoft Defender for Endpoint Attack Surface Reduction, Vermindering van het aanvalsoppervlak - blokkeer het gebruik van gekopieerde of nagemaakte systeemtools (preview), is uitgeschakeld, kan installatie plaatsvinden.

Volgende stappen: Cisco Secure Client gedraagt zich zoals verwacht wanneer het probeert te installeren. Microsoft Defender for Endpoint / Microsoft Intune veroorzaakt echter onverwachte interferentie met de installatie. Cisco heeft een tijdelijke oplossing geïdentificeerd voor klanten die dit probleem ondervinden.

Tijdelijke oplossing: Het is aan te raden de configuratie voor deze optie te raadplegen bij de applicatieontwikkelaar of deze optie verder te raadplegen via deze kennisbank. Voor onmiddellijke remediëring kunnen we ons beheerde eindpunt in Intune verplaatsen naar een minder restrictief beleid of deze optie tijdelijk expliciet uitschakelen totdat de juiste stappen zijn genomen. Deze instelling onder het Intune-beheerportal werd gebruikt als tijdelijke maatregel om beveiligde endpointconnectiviteit te herstellen.

Kijk hier voor meer informatie over dit probleem voorwerp.

Als u contact moet opnemen met Cisco ondersteuning, volg de instructies die in deze link worden geleverd.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.