Problemi noti di Cisco XDR

Sommario

[Introduzione](#)

[Problemi noti:](#)

[Incidenti](#)

[Indagini](#)

[Control Center](#)

[Integrazioni di Cisco](#)

[Integrazioni di terze parti](#)

[Attivo](#)

[XDR Automate](#)

[Appliance/Sensori](#)

[Secure Client](#)

[XDR-A](#)

[Problemi risolti](#)

Introduzione

Questo articolo documenta i problemi tecnici attualmente noti per Cisco XDR.

I problemi tecnici possono essere riconosciuti da Cisco, in fase di revisione, in attesa di risoluzione o ritenuti idonei a funzionare come previsto.

Problemi noti:

Incidenti

Al momento non sono presenti problemi noti per questa funzionalità XDR.

Indagini

Al momento non sono presenti problemi noti per questa funzionalità XDR.

Control Center

1. La tessera MTTR sul Control Center mostra numeri imprecisi per gli incidenti che sono stati risolti utilizzando uno dei nuovi stati, ad esempio "Chiuso: False Positive", "Closed: Minaccia confermata" o altro.

Stato: Problema identificato e risoluzione in sospeso

Dettagli: I nuovi stati incidenti sono stati introdotti il 15 gennaio e la tessera non prende in

considerazione questi stati. I nuovi stati di risoluzione vengono interpretati come semilavorati, quindi anche se l'incidente è stato chiuso utilizzando uno dei nuovi stati, viene considerato come semilavorati.

Soluzione: nessuna

Fasi successive: nessuna

Risoluzione prevista: da definire

Integrazioni di Cisco

1.- Cisco XDR - Il collegamento all'integrazione di Cisco Secure Endpoint non funziona sul portale Cisco XDR

Stato: Problema identificato e risoluzione in sospeso

Dettagli: Nelle schede Admin > Integrations il collegamento "Enable" dell'endpoint sicuro è interrotto. Dopo aver premuto il pulsante di abilitazione, viene eseguito il reindirizzamento alla pagina Threat Response e viene eseguito un ciclo alla pagina di selezione di XDR org anziché alla console di endpoint protetti.

Soluzione temporanea: L'integrazione può essere eseguita dal Cisco Secure Endpoint Portal

Passaggi successivi: Cisco sta lavorando per implementare la correzione per questo problema

Risoluzione prevista: Da definire

2. Cisco XDR - Integrazione completa di Cisco Secure Firewall

Dettagli: per garantire un'integrazione perfetta tra Cisco Defense Orchestrator (CDO), Security Services Exchange (SSX) e Security Analytics and Logging (SAL), è necessario il mapping manuale. Questo processo comporta la connessione a Cisco TAC per eseguire le configurazioni e le mappature necessarie.

Soluzione. Contattare TAC per ottenere assistenza nel collegamento dei relativi account e garantire la corretta integrazione dei sistemi.

Risoluzione prevista: Da definire

Integrazioni di terze parti

1.- I clienti Microsoft con licenze di tipo G non possono utilizzare le integrazioni di XDR Microsoft.

Stato: Progettato

Dettagli: i diritti di tipo G di Microsoft dispongono dell'accesso in ambienti controllati solo per enti governativi.

Passaggi successivi: Cisco sta collaborando con Microsoft per comprendere i requisiti per l'integrazione con l'ambiente Microsoft GCC in cui vengono forniti i diritti di tipo G di Microsoft. Se possibile, Cisco XDR prevede di integrarsi con le licenze Microsoft di tipo G per Microsoft Defender for Endpoint, O365 e EntraID.

Risoluzione prevista: da definire

Attivo

Al momento non sono presenti problemi noti per questa funzionalità XDR.

XDR Automate

1.- Interruzione imprevista dell'esecuzione delle regole di automazione degli incidenti XDR

Stato: problema identificato e risoluzione in sospeso

Dettagli: le regole di automazione degli incidenti alimentate dai workflow e attivano interruzioni impreviste dell'esecuzione. Questo non è indicato nell'interfaccia utente XDR, tranne quando si esaminano le metriche per l'esecuzione dei flussi di lavoro nel tempo. Quando si esegue questa operazione, i clienti vedranno l'esecuzione di flussi di lavoro ridotti o nulli, a seconda di quanto tempo il problema è stato in corso.

Passaggi successivi: Cisco ha identificato questo problema come appartenente al back-end XDR e sta lavorando per risolverlo. Cisco prevede anche di implementare ulteriori funzionalità di monitoraggio e monitoraggio dello stato per evitare che il problema si verifichi in futuro.

Soluzione: disabilitare e riabilitare la regola per avviare un riavvio dell'attivazione e dell'elaborazione della regola del flusso di lavoro.

Risoluzione prevista: marzo 2025

Appliance/Sensori

1.- Cisco XDR-Analytics - Errore di installazione dell'ONA negli ambienti virtuali con un errore che indica "verifica checksum non riuscita"

Stato: problema identificato e risoluzione in sospeso

Dettagli: Quando si installa un sensore ONA in un ambiente virtuale, l'ISO non completa il processo di installazione e genera errori.

Soluzione temporanea: Installare Ubuntu Server 24.04 in modo indipendente con Ubuntu ISO e seguire i passaggi di [installazione avanzati](#) per eseguire ONA come servizio. Utilizzare la compatibilità 7.0 U2

Passaggi successivi: Cisco sta lavorando per implementare la correzione per questo problema

Risoluzione: Versione successiva del sensore XDR

2.- Cisco XDR-Analytics - Grafico del traffico nei dettagli del sensore ONA non popolato quando è configurata solo la sonda ETA

Stato: problema identificato e risoluzione in sospeso

Dettagli: Il grafico del traffico non mostra alcun traffico quando gli ONA sono configurati solo con la sonda ETA.

Soluzione: nessuna

Passaggi successivi: Cisco sta lavorando per implementare la correzione per questo problema

3.- Cisco XDR-Analytics - La telemetria ETA proveniente da Cisco Telemetry Broker (CTB) non viene utilizzata per popolare il dashboard ETA

Stato: problema identificato e risoluzione in sospeso

Dettagli: La telemetria ETA generata da CTB o caricata tramite CTB e generata da altri dispositivi non viene utilizzata per popolare il dashboard ETA

Soluzione temporanea: Usa ONA con sonda ETA

Passaggi successivi: Nessuna

Risoluzione: Versione successiva del sensore XDR

Secure Client

Per consultare i problemi relativi a Secure Client, seguire l'[articolo](#).

XDR-A

1. - È possibile associare più indirizzi IP e/o nomi host a un singolo nome di dispositivo in XDR-A

Stato: Non Risolto/Posticipato

Dettagli: Vari indirizzi IP attivi possono essere associati a un singolo dispositivo all'interno del portale SNA/XDR-A. tra cui dispositivi NVM e non NVM. Alcuni dispositivi dispongono anche di più nomi host. In base all'implementazione corrente, la registrazione dei dispositivi potrebbe determinare la presenza di più indirizzi IP (località) in un dispositivo. Alcuni di questi indirizzi IP potrebbero provenire dalla rete domestica dell'utente e potrebbero entrare in conflitto con gli indirizzi IP della rete dell'organizzazione.

Soluzione. Al momento non è disponibile alcuna soluzione per questo problema, che è ancora presente nell'architettura corrente. Ci sono buone speranze che questo problema possa essere affrontato meglio in futuro, una volta implementata una nuova architettura che permetterà di normalizzare e riunire le attività di rete da entrambe le fonti ONA e NVM a OCSF.

Passaggi successivi: N/D

Risoluzione: Futuro/Da definire

Problemi risolti

1.- L'opzione Contrassegna task come non applicabile viene considerata solo alla creazione di un incidente XDR e non all'aggiornamento di un incidente.

Stato: risolto

Dettagli: i playbook con risposta guidata Cisco XDR consentono di nascondere le attività non applicabili all'incidente corrente. Nell'ottobre 2024, Cisco ha rilasciato un miglioramento a Cisco XDR per nascondere automaticamente le attività senza alcun osservabile applicabile. Questo miglioramento funziona quando viene creato un incidente ma non valuta le attività applicabili quando vengono aggiornate.

Passaggi successivi: correzione implementata

Se è necessario contattare il supporto Cisco, seguire le istruzioni fornite in questo [collegamento](#).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).