[Esterno] - Utilizzo di Advanced Malware Protection (AMP) - Rilevamenti falsi, epidemie e risposta a incidenti

Sommario

Introduzione

Dell si impegna sempre a migliorare ed espandere la funzionalità di intelligence delle minacce per la tecnologia Advanced Malware Protection (AMP). Tuttavia, se la soluzione AMP non ha attivato un avviso o ne ha attivato uno erroneamente, è possibile adottare alcune misure per evitare ulteriori ripercussioni sull'ambiente. Il presente documento fornisce linee guida per tali azioni.

Descrizione

Azioni immediate

Se si ritiene che la soluzione AMP in uso non protegga la rete da eventuali minacce, procedere immediatamente come segue:

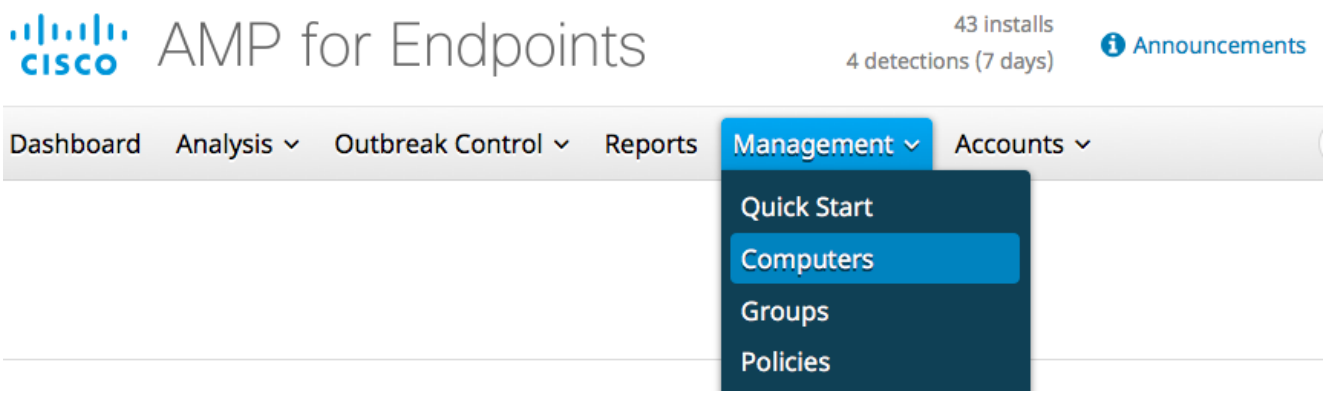
1. Isolare le macchine sospette dal resto della rete. Ciò può includere lo spegnimento della macchina o la sua disconnessione fisica dalla rete.
2. Annotare le informazioni importanti sull'infezione, come l'ora in cui la macchina potrebbe essere infettata, le attività degli utenti sui computer sospetti, ecc.

Avviso: non pulire o ricalcare la macchina. Elimina la possibilità di trovare il software o i file offensivi durante le indagini forensi o le procedure di risoluzione dei problemi.

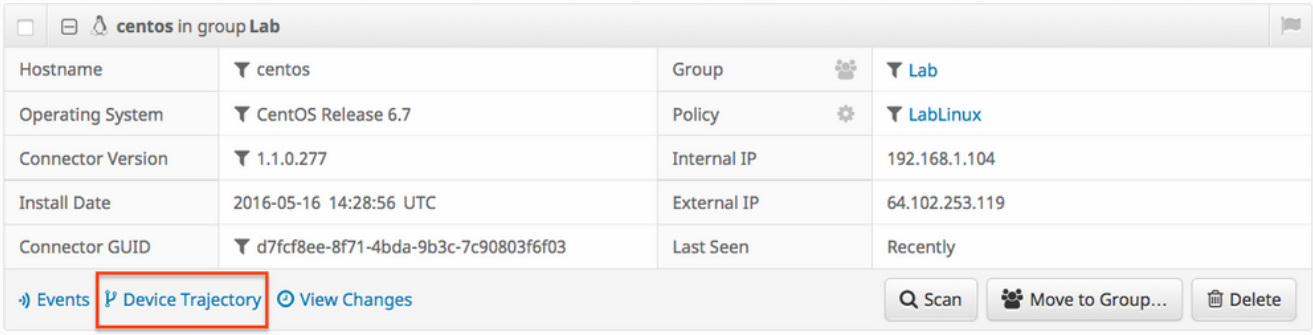
Analisi

1. Utilizzate la funzione **Traiettoria periferica (Device Trajectory)** per avviare un'analisi personalizzata. La traiettoria periferica è in grado di memorizzare circa i 9 milioni di eventi di file più recenti. La traiettoria del dispositivo AMP for Endpoints è molto utile per individuare i file o i processi che hanno causato un'infezione.

   Nel dashboard, passare a **Gestione > Computer**.



Individuare il computer sospetto ed espandere il record per tale computer. Fare clic sull'opzione **Traiettoria periferica**.



2. Se si individuano file o hash sospetti, aggiungerli agli elenchi di rilevamento personalizzati. AMP for Endpoints può utilizzare un elenco di rilevamento personalizzato per trattare un file o un hash come dannoso. Questo è un ottimo modo per fornire una copertura stop-gap per prevenire un ulteriore impatto.

Analisi di Cisco

1. Sottomettere eventuali campioni sospetti per l'analisi dinamica. È possibile sottometterli manualmente da **Analisi > Analisi file** nel dashboard. AMP for Endpoints include funzionalità di analisi dinamica che generano un report del comportamento del file da Threat Grid. Questo ha il vantaggio di fornire il file a Cisco nel caso in cui sia necessaria un'analisi aggiuntiva da parte del nostro team di ricerca.

2. Se si sospetta la presenza di rilevamenti *falsi positivi* o *falsi negativi* nella rete, è consigliabile utilizzare le funzionalità personalizzate della lista nera o della lista bianca per i prodotti AMP. Quando si contatta il Cisco Technical Assistance Center (TAC), fornire le seguenti informazioni per l'analisi:Hash SHA256 del file.Se possibile, una copia del file.Informazioni sul file, ad esempio l'origine e il motivo per cui deve trovarsi nell'ambiente.Spiegate perché ritenete che si tratti di un falso positivo o un falso negativo.
3. Per ottenere assistenza nel mitigare una minaccia o eseguire la valutazione dell'ambiente, è necessario rivolgersi al team Cisco Talos Incident Response (CTIR), specializzato nella creazione di piani d'azione, nella ricerca di macchine infette e nell'utilizzo di strumenti o funzionalità avanzati per mitigare un'epidemia attiva.
Nota: Il Cisco Technical Assistance Center (TAC) non fornisce assistenza per questo tipo di progetti.È possibile contattare qui CTIR. Si tratta di un servizio a pagamento con costo iniziale di 60.000 dollari, a meno che l'organizzazione non disponga di un'utilità di

conservazione per i servizi di risposta a richieste di assistenza Cisco. Una volta coinvolti, forniranno ulteriori informazioni sui loro servizi e apriranno una richiesta di assistenza per il tuo incidente. Ti consigliamo anche di contattare il tuo Cisco Account Manager per avere ulteriori informazioni sul processo.

Articoli correlati

- Raccolta di dati diagnostici da un connettore FireAMP in esecuzione su Windows
- Tipi di file analizzati dal connettore FireAMP