Identificare il motore di rilevamento in Secure Endpoint Console

Sommario

Introduzione

In questo documento viene descritto come identificare il motore responsabile di un rilevamento specifico nella console dell'endpoint sicuro.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Endpoint console

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Secure Endpoint Console v5.4.2025030619

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

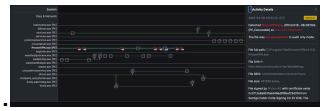
Problema

Identificare il motore corretto responsabile di un rilevamento specifico è uno dei passi iniziali per comprendere la natura dell'evento e verificarlo in modo efficace.

Soluzione

1. Passare alla pagina Eventi della console AMP per individuare l'evento che si desidera analizzare ulteriormente.
2. Fate clic sull'icona evidenziata per aprire Traiettoria periferica (Device Trajectory). 

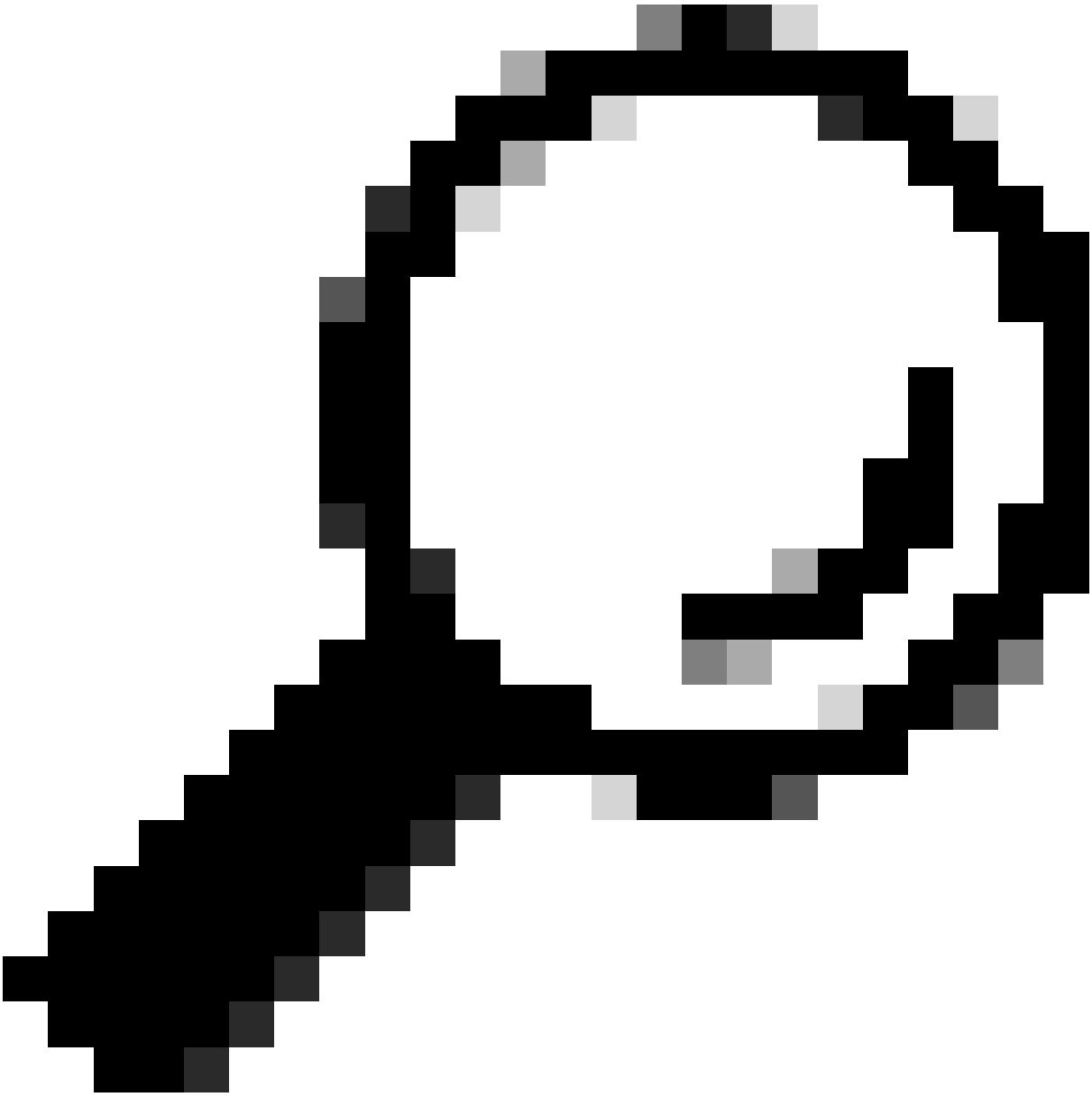
   Icona della traiettoria del dispositivo

3. È possibile visualizzare i dettagli dell'evento a destra in Dettagli attività. 

   Dettagli evento nella traiettoria del dispositivo

4. Scorrere verso il basso per individuare la sezione Rilevato da. 

   Rilevato da sezione



Suggerimento: La comprensione di queste informazioni è essenziale per valutare la natura della minaccia e determinare rapidamente l'esclusione appropriata da configurare. Inoltre, fornire questi dettagli quando si sottopone un caso a TAC per indagini sui falsi positivi può contribuire a velocizzare il processo.

Se non è possibile visualizzare la sezione Detected By (Rilevato da) o per ulteriore assistenza, contattare TAC.

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).