Risoluzione dei problemi relativi all'analisi dei file falsi positivi in AMP for Endpoints

Sommario

Introduzione

In questo documento viene descritto come raccogliere un'analisi di file dei falsi positivi in Advanced Malware Protection (AMP) for Endpoints.

Contributo di Jesus Javier Martinez, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Dashboard della console AMP
- Account con privilegi di amministratore

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco AMP for Endpoints versione 6.X.X e successive.

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.

Premesse

AMP for Endpoints può generare avvisi eccessivi su un determinato file/processo/SHA (Secure Hash Algorithm) 256. Se si sospetta la presenza di falsi positivi nella rete, è possibile contattare il Cisco Technical Assistance Center (TAC), il team di diagnostica procederà a un'analisi più approfondita dei file. Quando si contatta Cisco TAC, è necessario fornire le seguenti informazioni:

·Hash file SHA 256
·Copia di esempio dei file
·Acquisizione di eventi di allarme dalla console AMP
·Acquisizione dei dettagli sugli eventi da AMP Console
·Informazioni sul file (origine e motivo della presenza nell'ambiente)
·Spiegare perché si ritiene che il file/processo possa essere un falso positivo

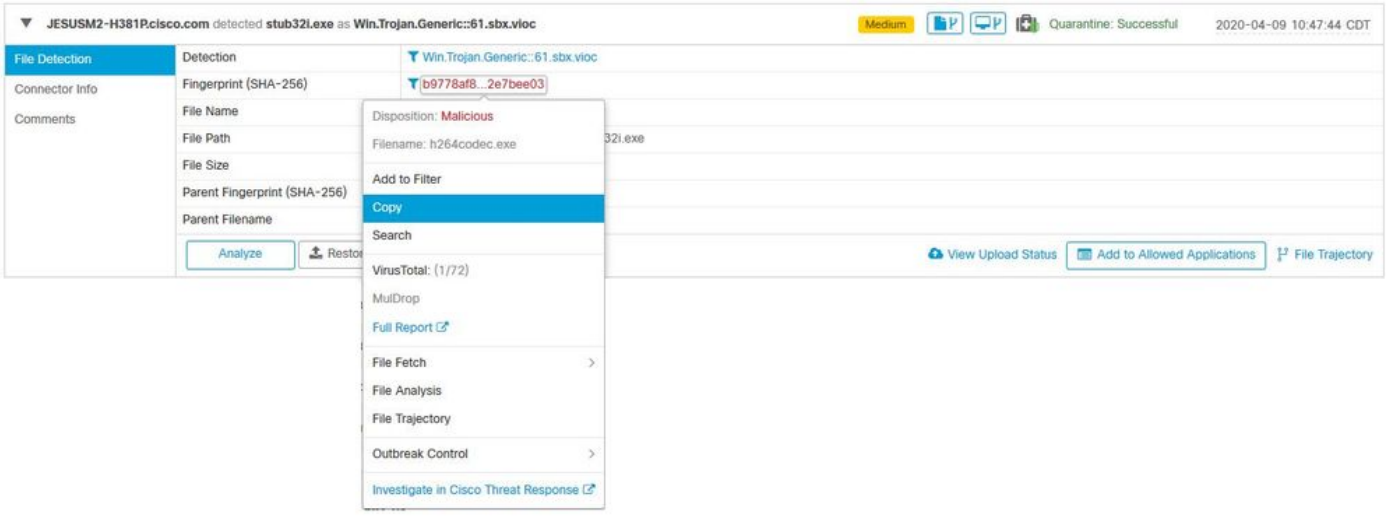
Risoluzione dei problemi relativi all'analisi dei file falsi positivi in AMP for Endpoints

In questa sezione vengono fornite informazioni che è possibile utilizzare per ottenere tutti i dettagli necessari per aprire un ticket Falso positivo con Cisco TAC.

Hash SHA 256 file

Passaggio 1. Per ottenere l'hash SHA 256, passare a **AMP Console > Dashboard > Eventi.**

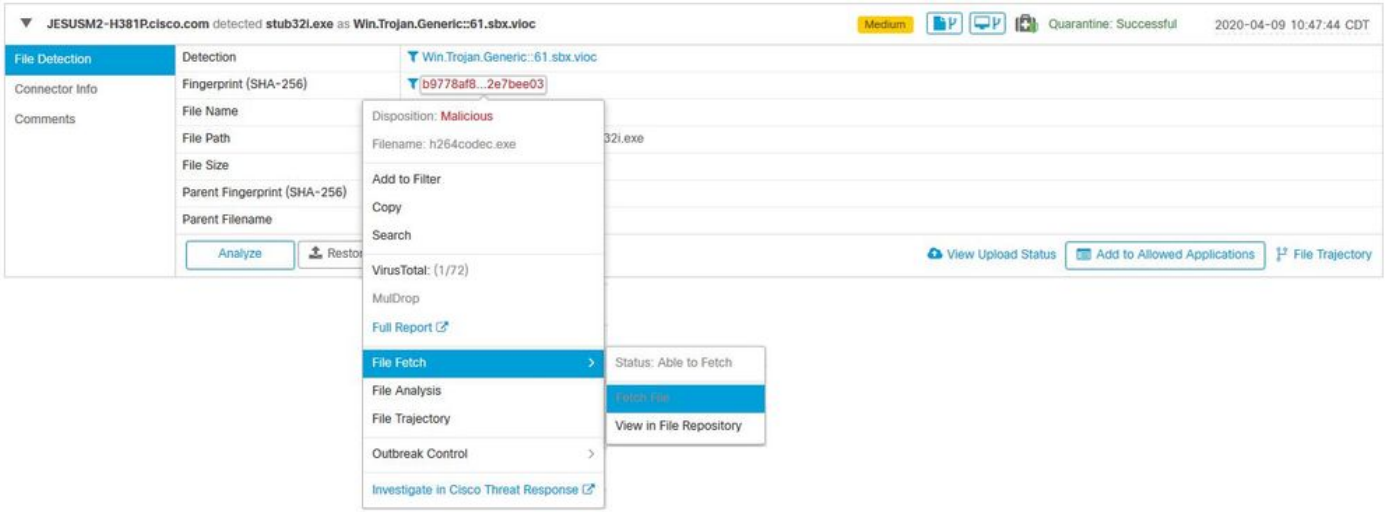
Passaggio 2. Selezionare l'**evento di avviso**, fare clic su **SHA256** e selezionare **Copia** come mostrato nell'immagine.



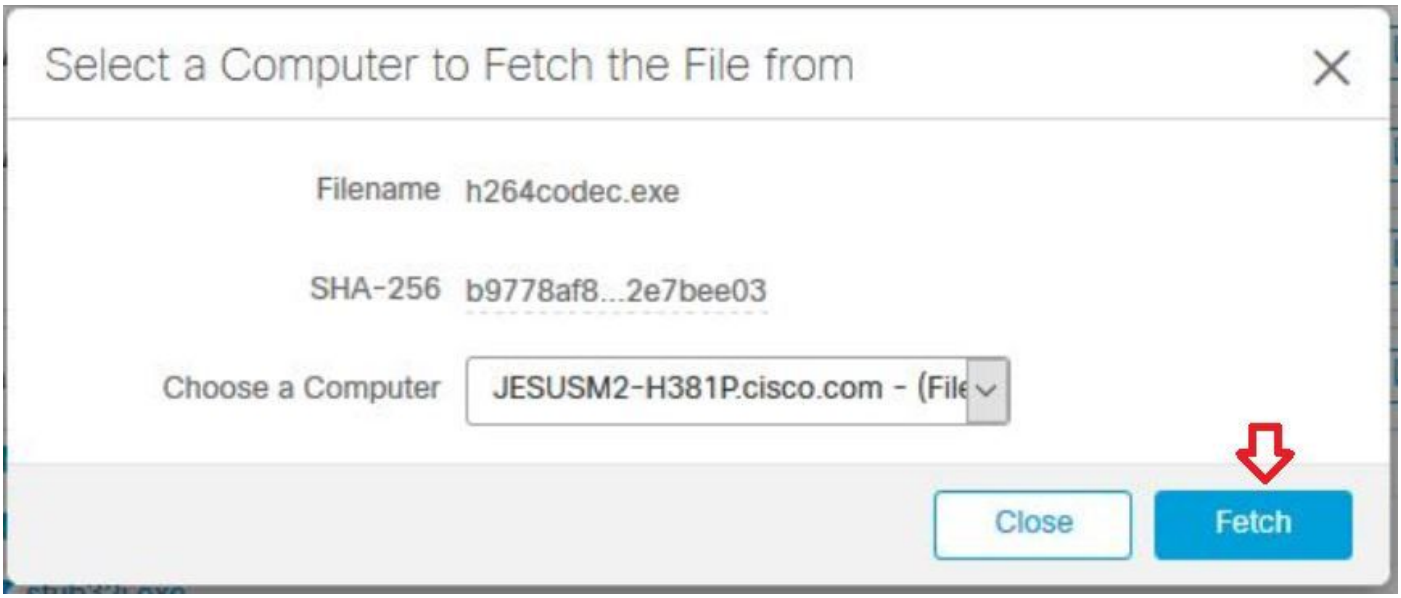
Copia di esempio file

Passaggio 1. È possibile ottenere il file di esempio da AMP Console, passare a **AMP Console > Dashboard > Events.**

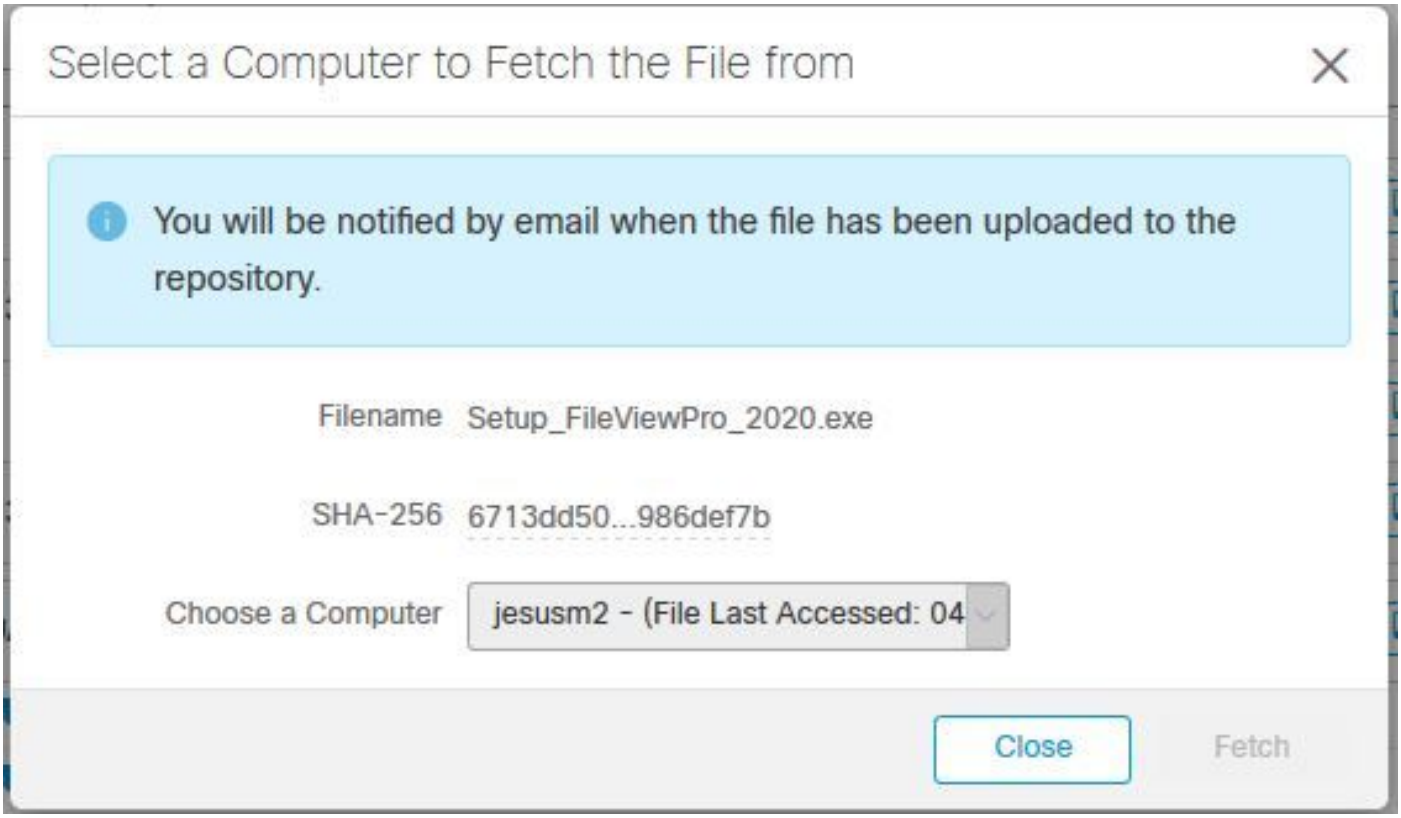
Passaggio 2. Selezionare l'**evento di avviso**, fare clic su **SHA256** e passare a **Recupero file> Recupero file** come mostrato nell'immagine.



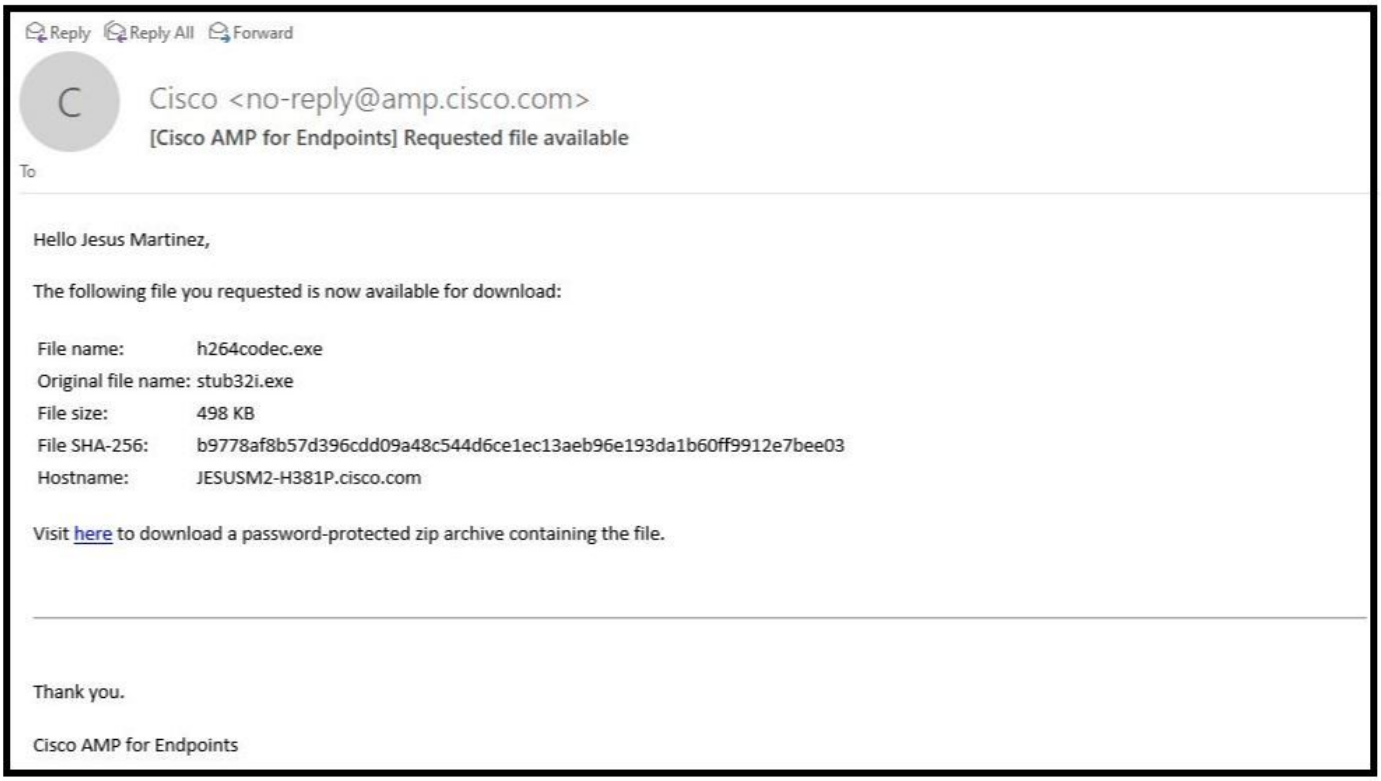
Passaggio 3. Selezionare la periferica in cui è stato rilevato il file e fare clic su **Fetch**, come mostrato nell'immagine (la periferica deve essere accesa **)**, come mostrato nell'immagine.



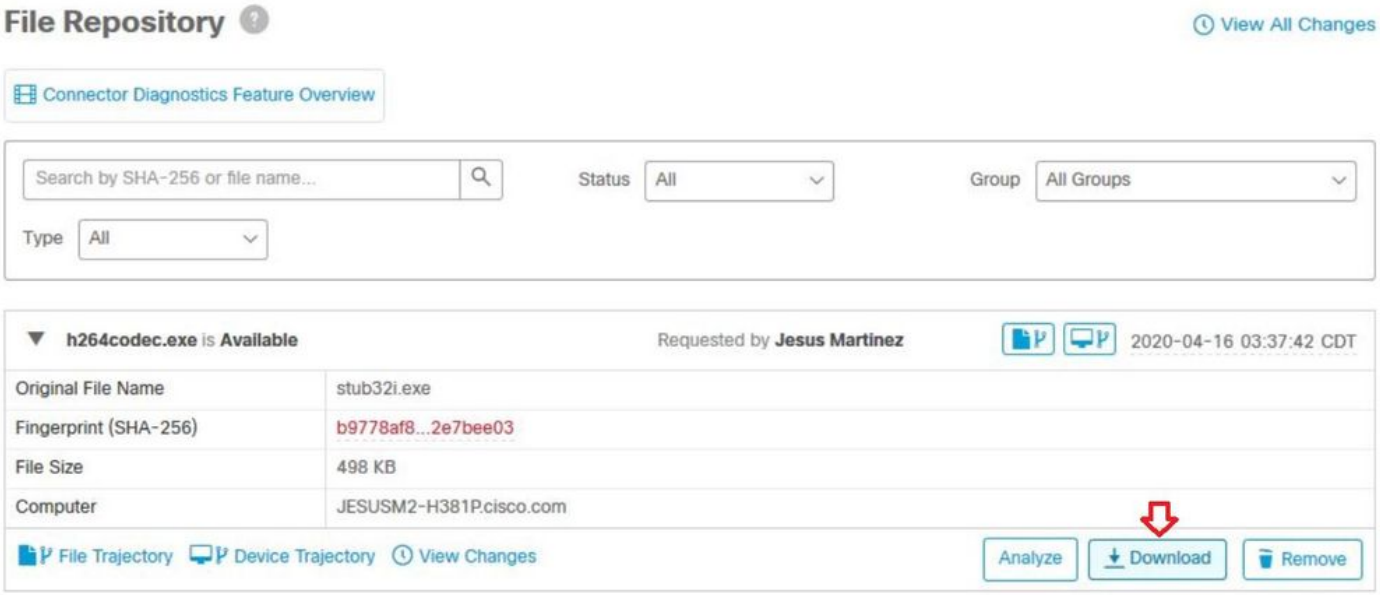
Passaggio 4. Si riceve il messaggio come mostrato nell'immagine.



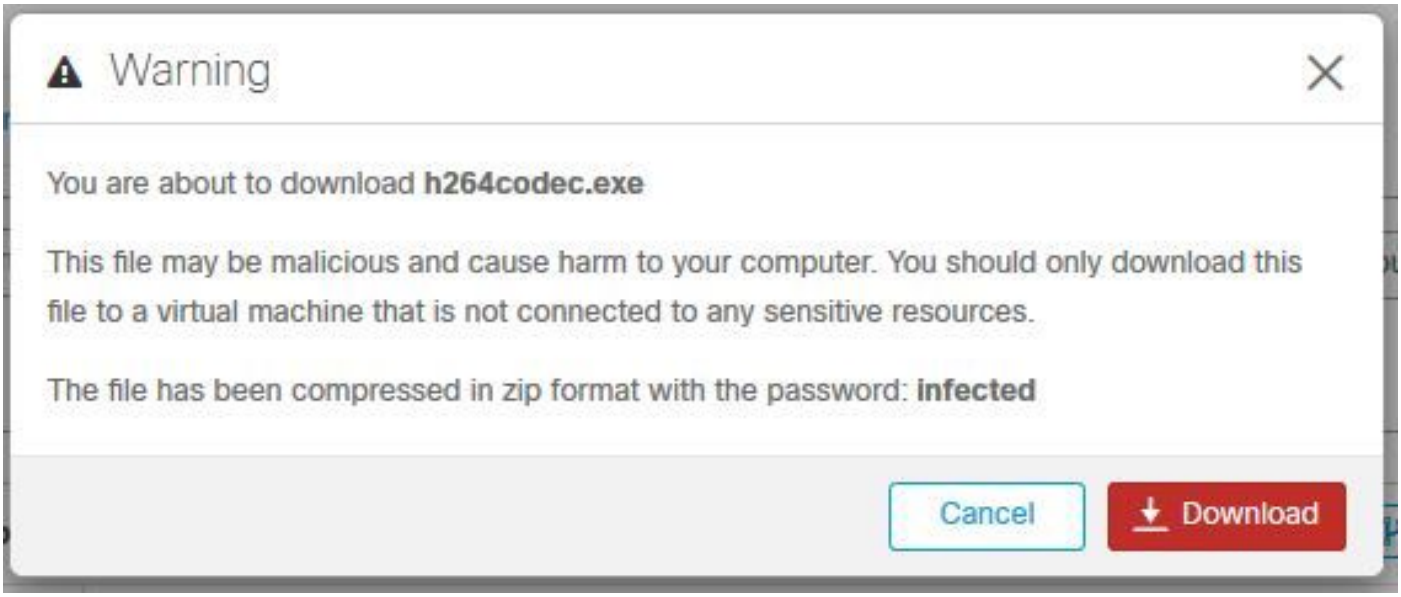
Dopo alcuni minuti si riceverà una notifica e-mail quando il file sarà disponibile per il download, come mostrato nell'immagine.



Passaggio 5. Passare a **AMP Console > Analisi > Archivio file** e selezionare il file e fare clic su **Scarica** come mostrato nell'immagine.



Passaggio 6. Viene visualizzata la finestra di notifica, fare clic su **Download** come mostrato nell'immagine, e il file viene scaricato in un file ZIP.



Acquisizione di eventi di avviso dalla console AMP

Passaggio 1. Passare a **AMP Console > Dashboard > Eventi.**

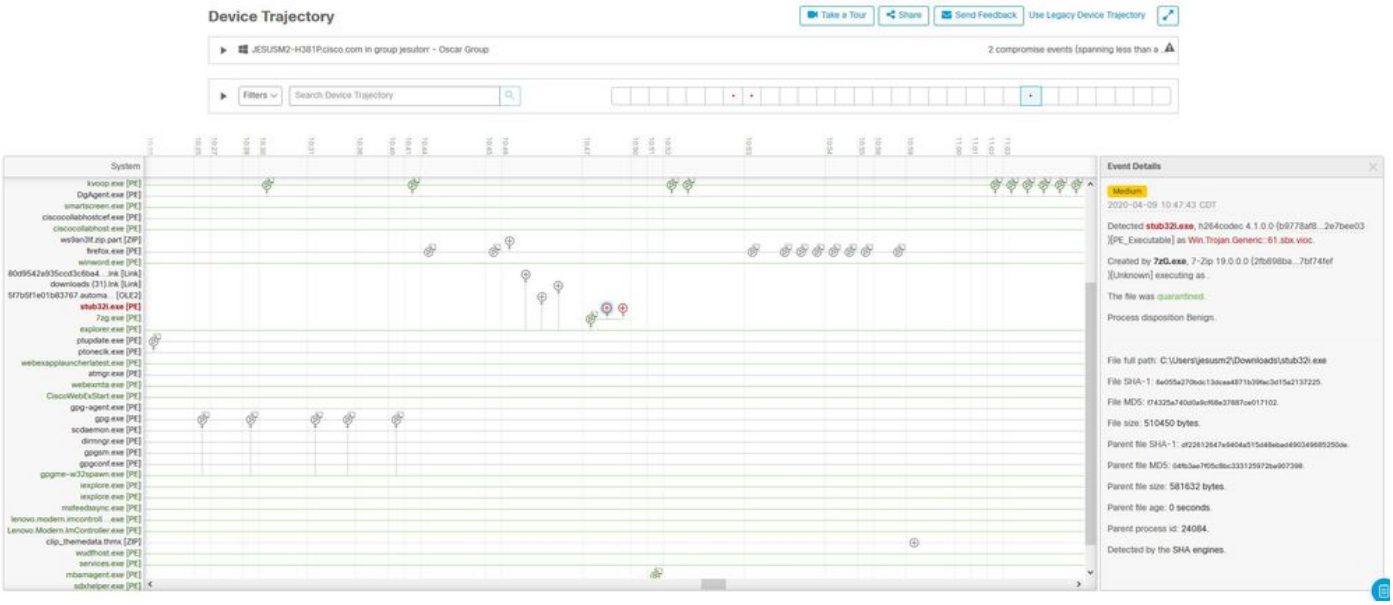
Passaggio 2. Selezionare l'**evento di avviso** ed eseguire l'acquisizione come mostrato nell'immagine.

Acquisizione di dettagli evento dalla console AMP

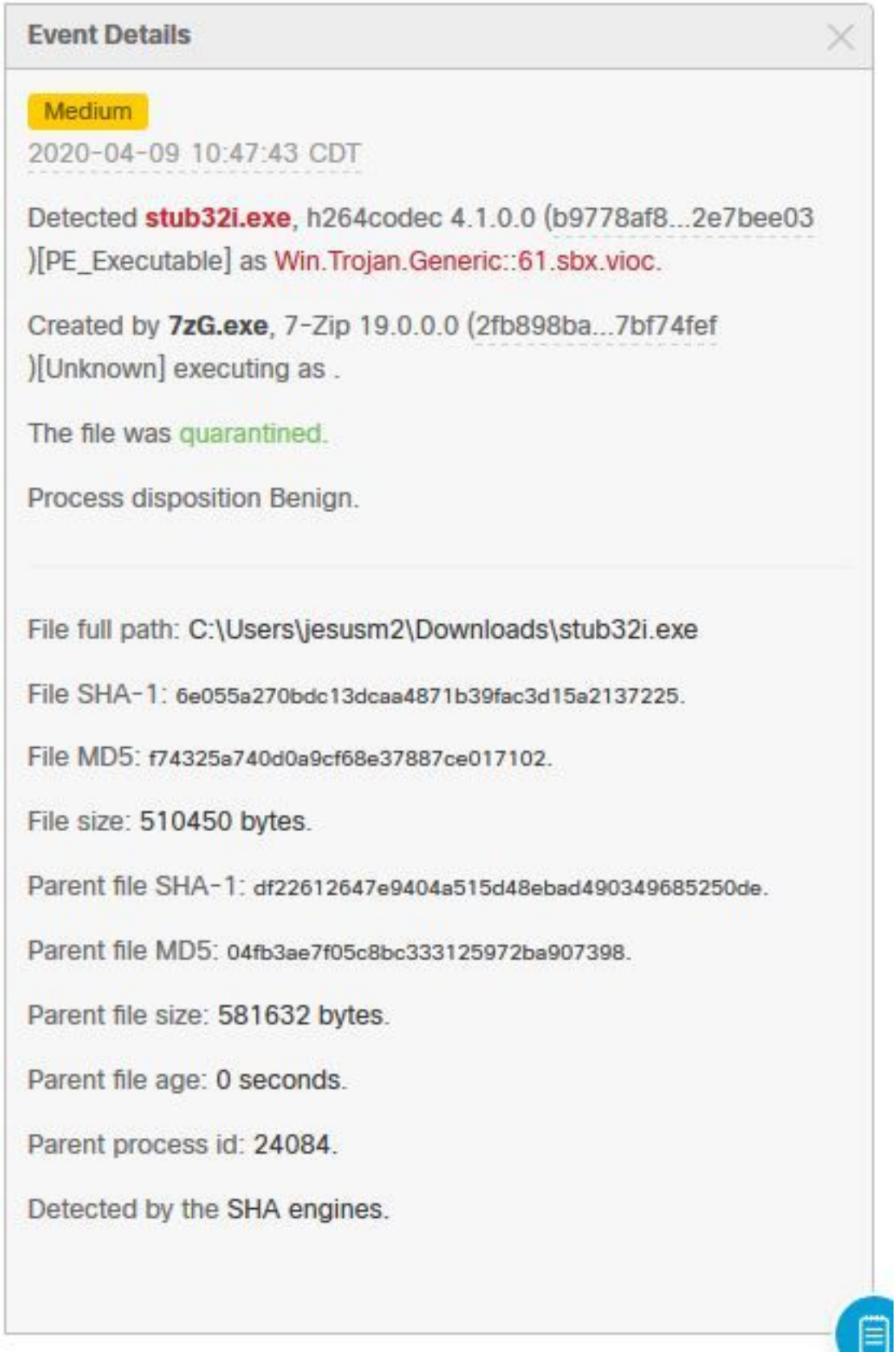
Passaggio 1. Passare a **AMP Console > Dashboard > Eventi.**

Passaggio 2. Selezionare l'evento di allarme e fare clic sull'opzione **Traiettoria periferica** come mostrato nell'immagine.

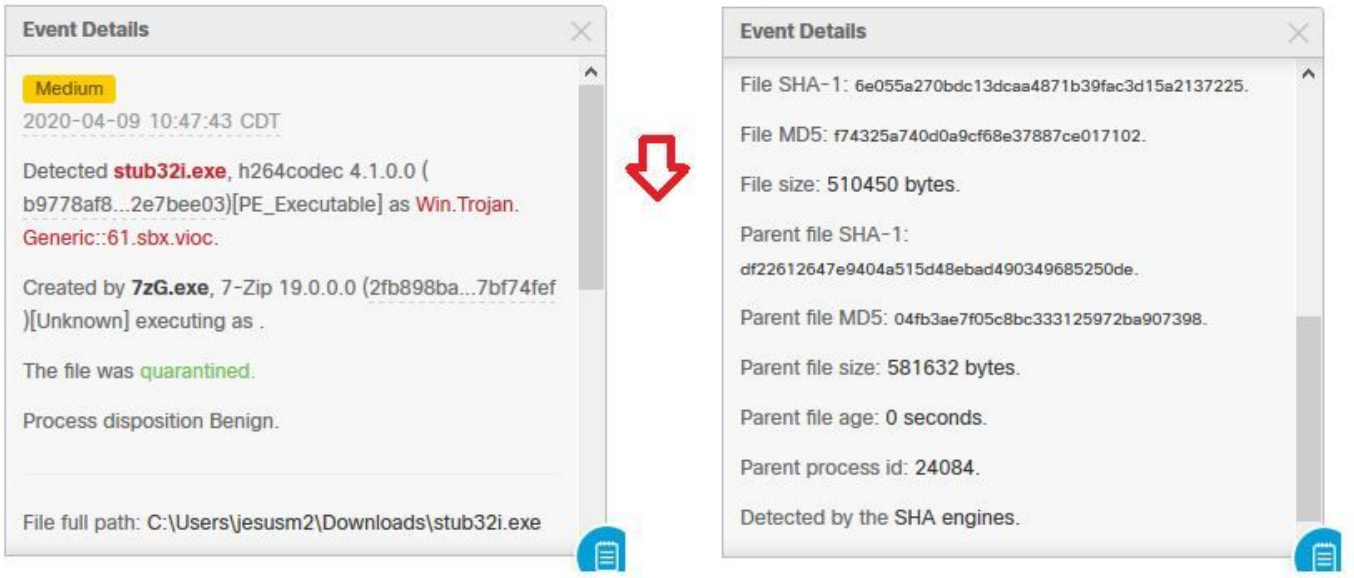
Viene reindirizzato ai dettagli della **traiettoria periferica**, come mostrato nell'immagine.



Passaggio 3. Acquisire la casella **Dettagli evento** come mostrato nell'immagine.



Passaggio 4. Se necessario, scorrere verso il basso ed eseguire alcune acquisizioni per ottenere tutte le informazioni **Dettagli eventi** come mostrato nell'immagine.



Informazioni sul file

- Informazioni sulla provenienza del file.
- Se il file proviene da un sito Web, condividere l'URL Web.
- Condividere una breve descrizione del file e spiegare la funzione del file.

Spiegazione

- Perché ritieni che l'elaborazione dei file possa essere un falso positivo?
- Condividere i motivi dell'attendibilità del file.

Fornisci informazioni

- Dopo aver raccolto tutti i dettagli, caricare tutte le informazioni richieste su https://cway.cisco.com/csc/.
- Accertarsi di fare riferimento al numero della richiesta di assistenza.

Conclusioni

Cisco si impegna sempre a migliorare ed espandere le funzionalità di intelligence delle minacce della tecnologia AMP for Endpoints. Tuttavia, se la soluzione AMP for Endpoints attiva un avviso erroneamente, è possibile adottare alcune misure per evitare ulteriori impatti sull'ambiente. Questo documento offre linee guida per ottenere tutti i dettagli necessari per aprire una richiesta in Cisco TAC in relazione a un problema di falso positivo. In base all'analisi dei file del team di diagnostica, la disposizione dei file può cambiare per arrestare gli eventi di allarme attivati su AMP Console oppure Cisco TAC può fornire la correzione appropriata per consentire l'esecuzione del file/processo senza problemi nell'ambiente.