Azioni automatizzate - Istantanea legale

Sommario

Introduzione

In questo documento viene descritta la funzionalità di azione automatizzata in Secure Endpoint legata al concetto di compromessi. Comprendere il ciclo di vita e la gestione dei compromessi sono fondamentali per comprendere la funzionalità delle azioni automatizzate. Questo articolo risponde alle domande relative alla terminologia e alle funzionalità di questi concetti.

Domande frequenti

Cos'è una macchina compromessa?

Un computer compromesso è un endpoint a cui è associato un compromesso attivo. Una macchina compromessa può, per progettazione, avere un solo compromesso attivo alla volta.

Che cos'è un compromesso?

Un compromesso è una raccolta di uno o più rilevamenti su una macchina. La maggior parte degli eventi di rilevamento (rilevamento minacce, segni di compromissione, ecc.) può generare o essere associata a un compromesso. Tuttavia, esistono coppie di eventi che potrebbero non attivare un nuovo compromesso. Ad esempio, quando si verifica un evento Rilevato minaccia, ma subito dopo che a esso è associato un evento In quarantena minaccia, non viene attivata una nuova compromissione. Logicamente, ciò è dovuto al fatto che Secure Endpoint ha gestito il potenziale compromesso (la minaccia è stata messa in quarantena).

Cosa succede quando si verificano nuovi rilevamenti su una macchina compromessa?

Gli eventi di rilevamento vengono aggiunti al compromesso esistente. Non viene creato alcun nuovo compromesso.

Dove posso vedere e gestire i compromessi?

I compromessi vengono gestiti nella scheda Posta in arrivo della console Secure Endpoint (https://console.amp.cisco.com/compromises per il cloud Nord America). Un computer compromesso è elencato nella sezione **Richiedi attenzione** e può essere eliminato premendo **Mark Resolved**. Inoltre, i compromessi vengono automaticamente cancellati dopo un mese.

In che modo viene attivata un'azione automatizzata*?

Le azioni automatizzate vengono attivate a seguito di un compromesso, ovvero quando una macchina senza compromessi diventa una macchina compromessa. Se una macchina già compromessa incontra un nuovo rilevamento, questo rilevamento viene aggiunto al compromesso, ma poiché non si tratta di un nuovo compromesso, non attiva un'azione automatica.

Come è possibile riattivare un'azione automatica?

Ènecessario "chiarire" il compromesso prima di tentare di riattivare un'azione automatizzata. Tenete presente che un evento Threat Detected + Threat Quarantined non è sufficiente per generare un nuovo evento di compromesso (e quindi non è sufficiente per attivare una nuova azione automatica).

*Eccezione: L'azione automatizzata "Invia file a ThreatGrid" non è associata a compromessi ed è eseguita per rilevamento

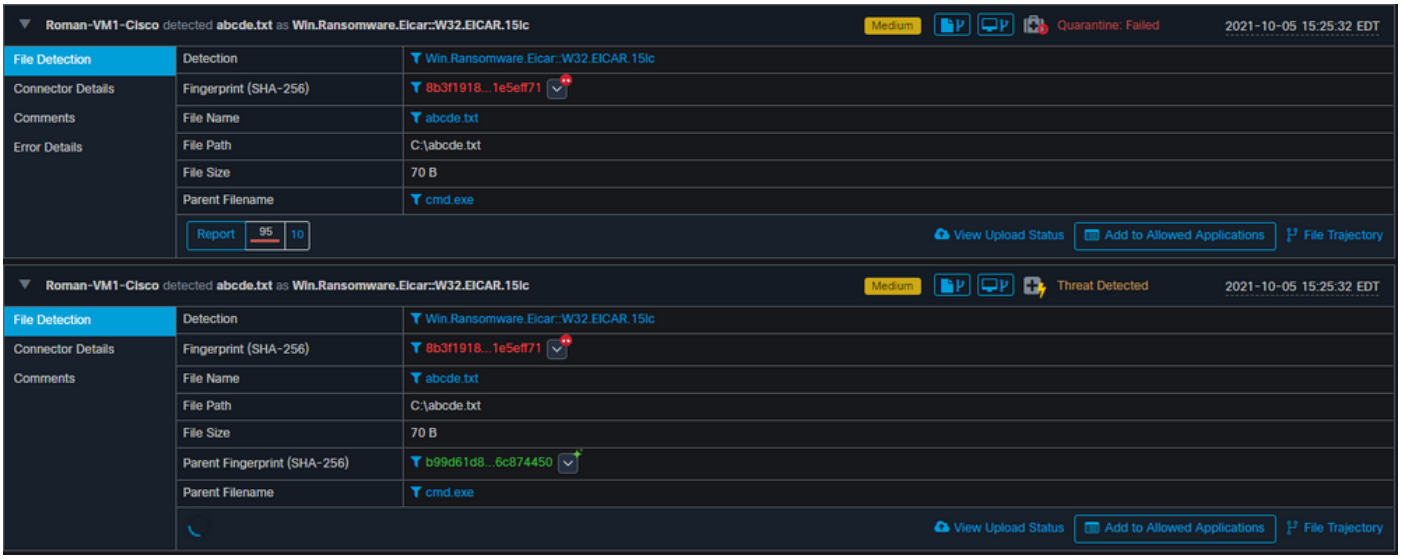
Custodia - Ricreazione in laboratorio

N. 1: Come indicato nella sezione FAQ. Le istantanee forensi sono prese solo in caso di "compromesso". In altre parole, se si tenta di accedere e scaricare un file dannoso da un sito TEST e il file viene contrassegnato al momento del download e messo in quarantena, ciò non è considerato un compromesso e non attiva l'azione.

> **Nota:** Rilevamento DFC, errore di quarantena e quasi tutto ciò che secondo la logica rientra nella categoria di evento di compromesso dovrebbe creare un'istantanea forense.

N. 2: È possibile generare un'istantanea solo una volta su un evento compromesso univoco. Non genera un'istantanea a meno che non si risolva il computer compromesso nella Posta in arrivo. Se l'evento compromesso non viene risolto, non verrà generata alcuna altra istantanea.

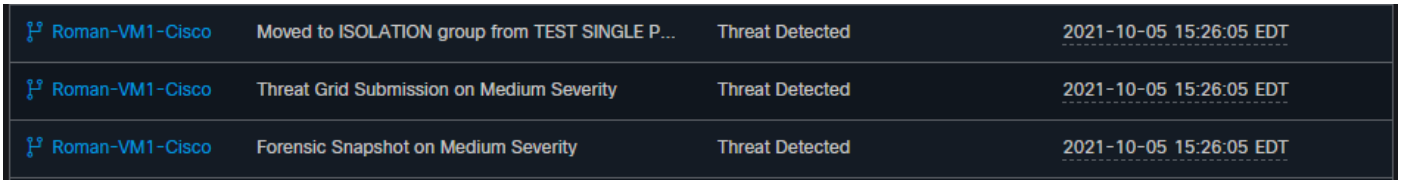
Esempio: In questa esercitazione uno script genera attività dannose e, poiché il file viene eliminato non appena creato e Endpoint protetto non è stato in grado di mettere in quarantena il file che rientra nella categoria compromissione.



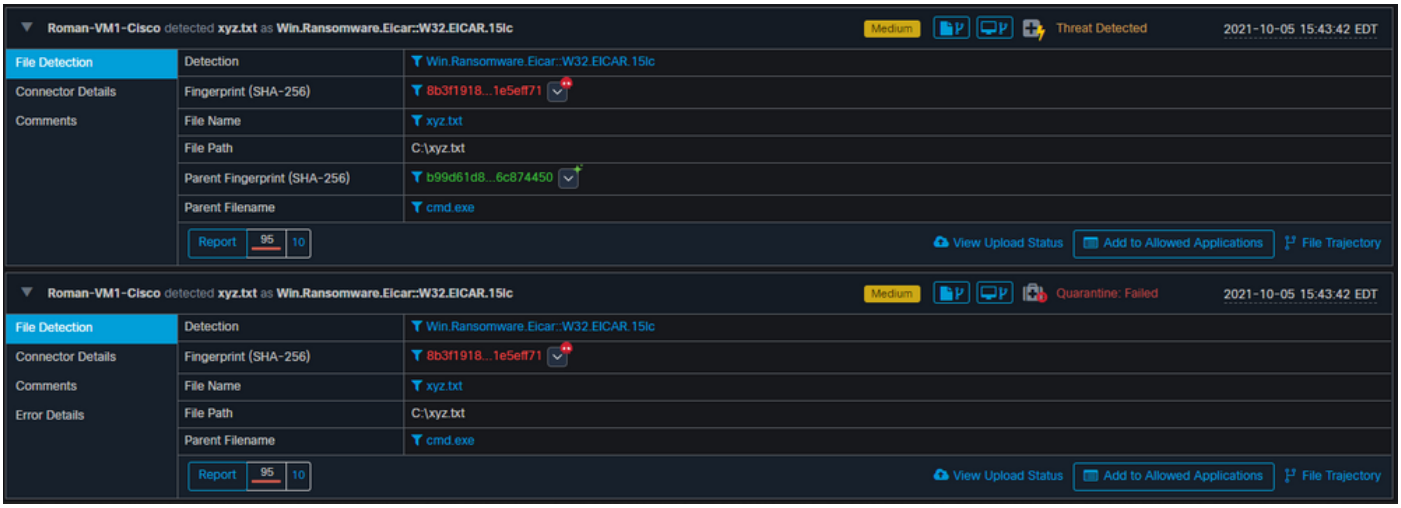
In questo test è possibile esaminare le operazioni automatizzate e le tre operazioni eseguite in base alle impostazioni.

- Snapshot creato
- Invio a Threat Grid (TG)
- L'endpoint è stato spostato in un gruppo separato creato e denominato ISOLATION

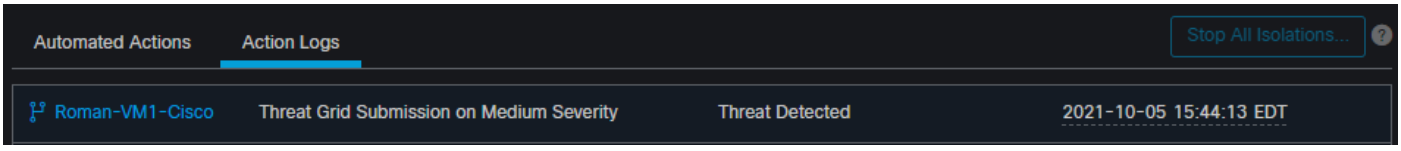
Potete vedere tutto questo in questo output, come mostrato nell'immagine.



Ora, dato che questo endpoint è compromesso, il prossimo test per provare la teoria con un simile file dannoso ma con un nome diverso, come mostrato nell'immagine.

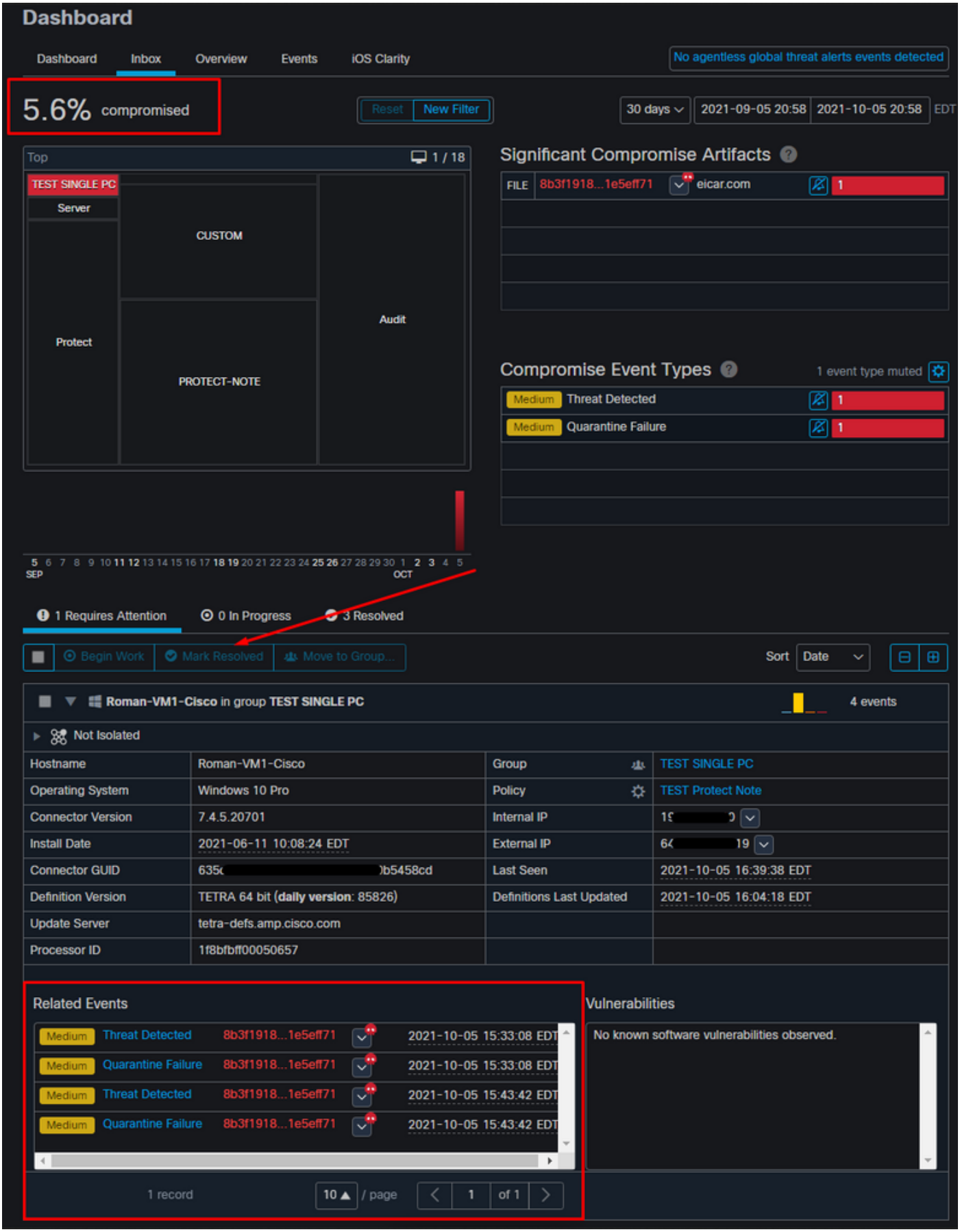


Tuttavia, poiché questo compromesso non è stato risolto, è possibile solo creare un invio TG. Non sono stati registrati altri eventi. Disattivare anche l'isolamento prima del 2° test.

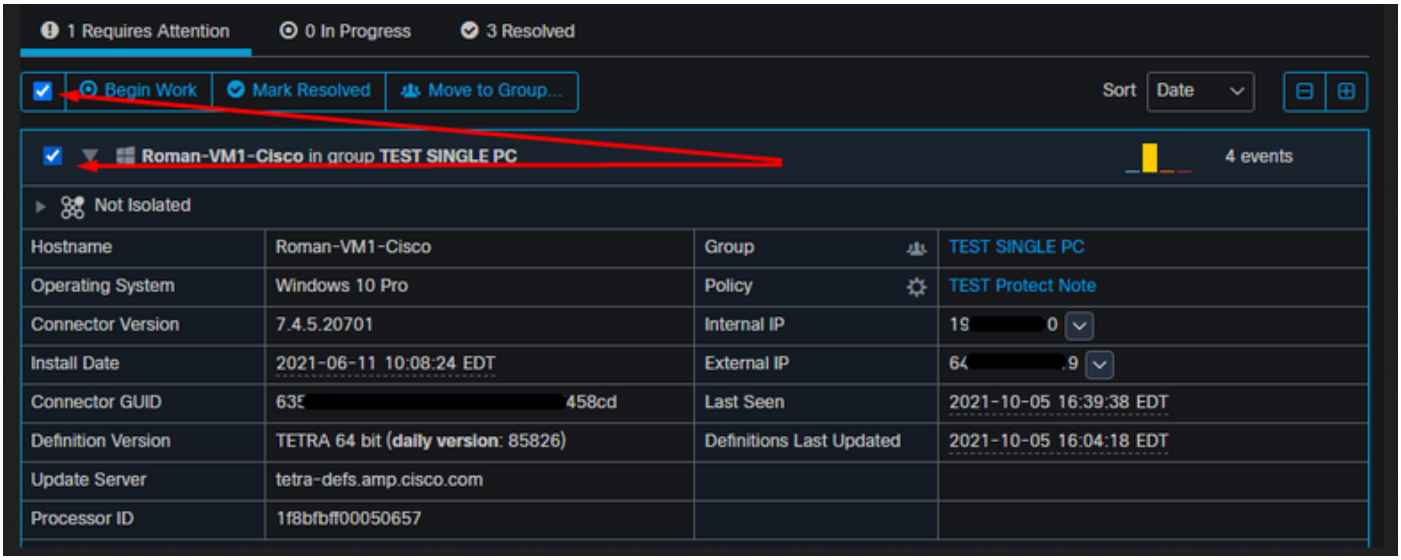


Nota: Si noti l'ora in cui la minaccia è stata rilevata e l'avvio automatico delle azioni.

L'evento non può essere riavviato a meno che non venga risolto l'endpoint compromesso. In questo caso, il dashboard avrà questo aspetto. Notare la percentuale e il pulsante Mark Risolto insieme agli eventi compromessi. Indipendentemente dal numero di eventi attivati, è possibile creare una sola istantanea e il numero percentuale elevato non è mai stato modificato. Tale numero rappresenta un compromesso all'interno dell'organizzazione e si basa sul totale degli endpoint nell'organizzazione. Cambia solo con un'altra macchina compromessa. Nell'esempio, il numero è alto perché il laboratorio dispone solo di 16 dispositivi. Inoltre, gli eventi di compromesso vengono cancellati automaticamente una volta raggiunti i 31 giorni di età.

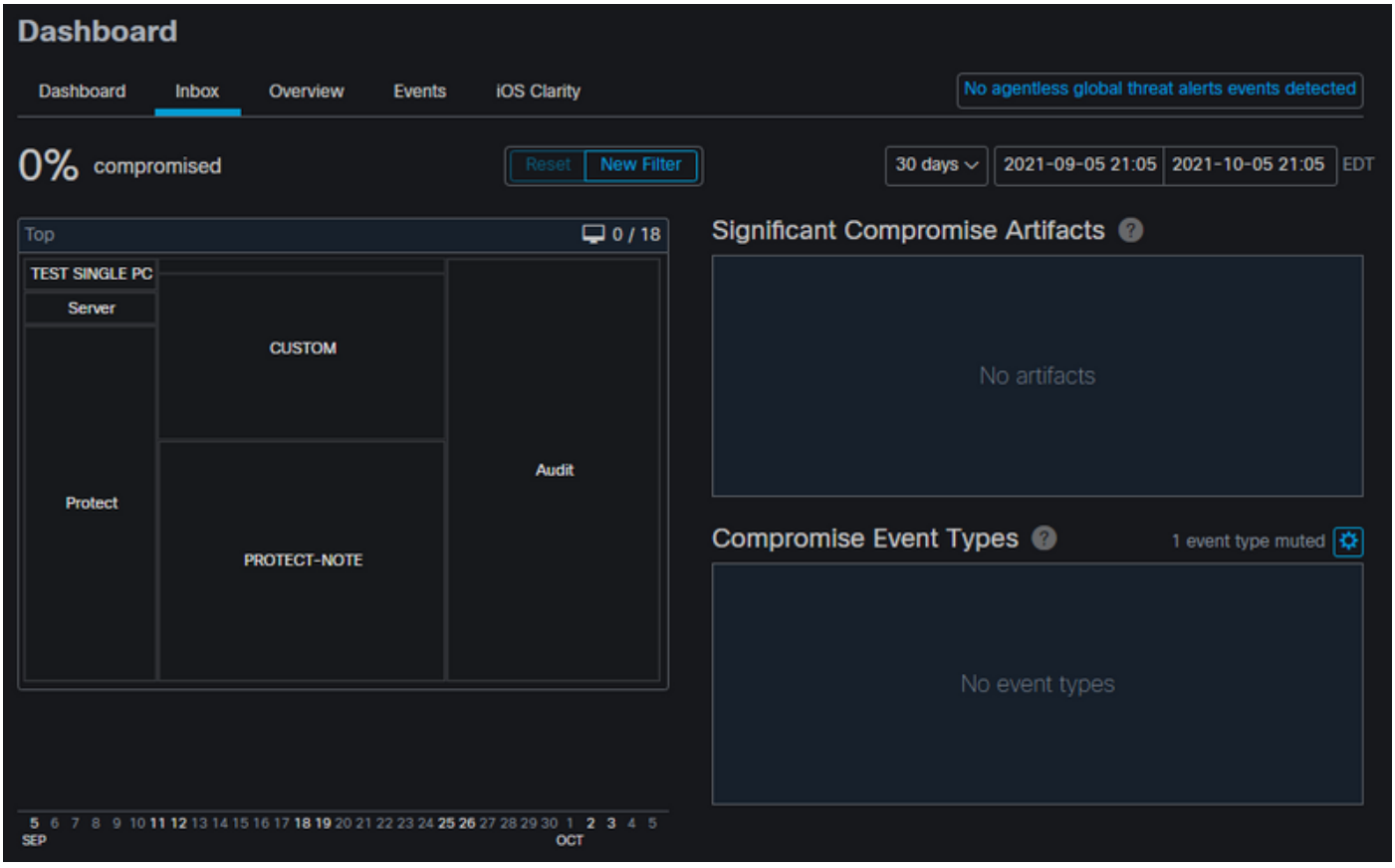


Il passaggio successivo consiste nel creare un altro evento e generare un'istantanea forense. Il primo passo è risolvere questo compromesso, fare clic sul pulsante **Segna come risolto**. È possibile eseguire questa operazione per ciascun endpoint oppure selezionare tutto nell'organizzazione.

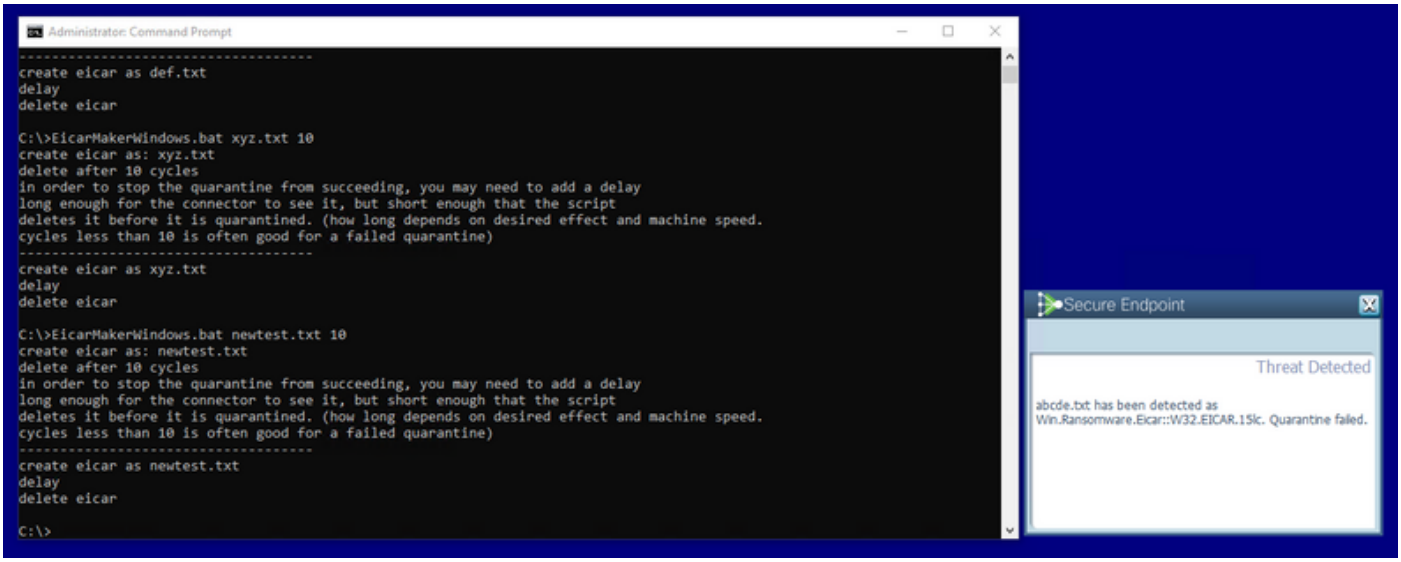


Nota: Se si selezionano tutti i compromessi, viene ripristinato lo 0%.

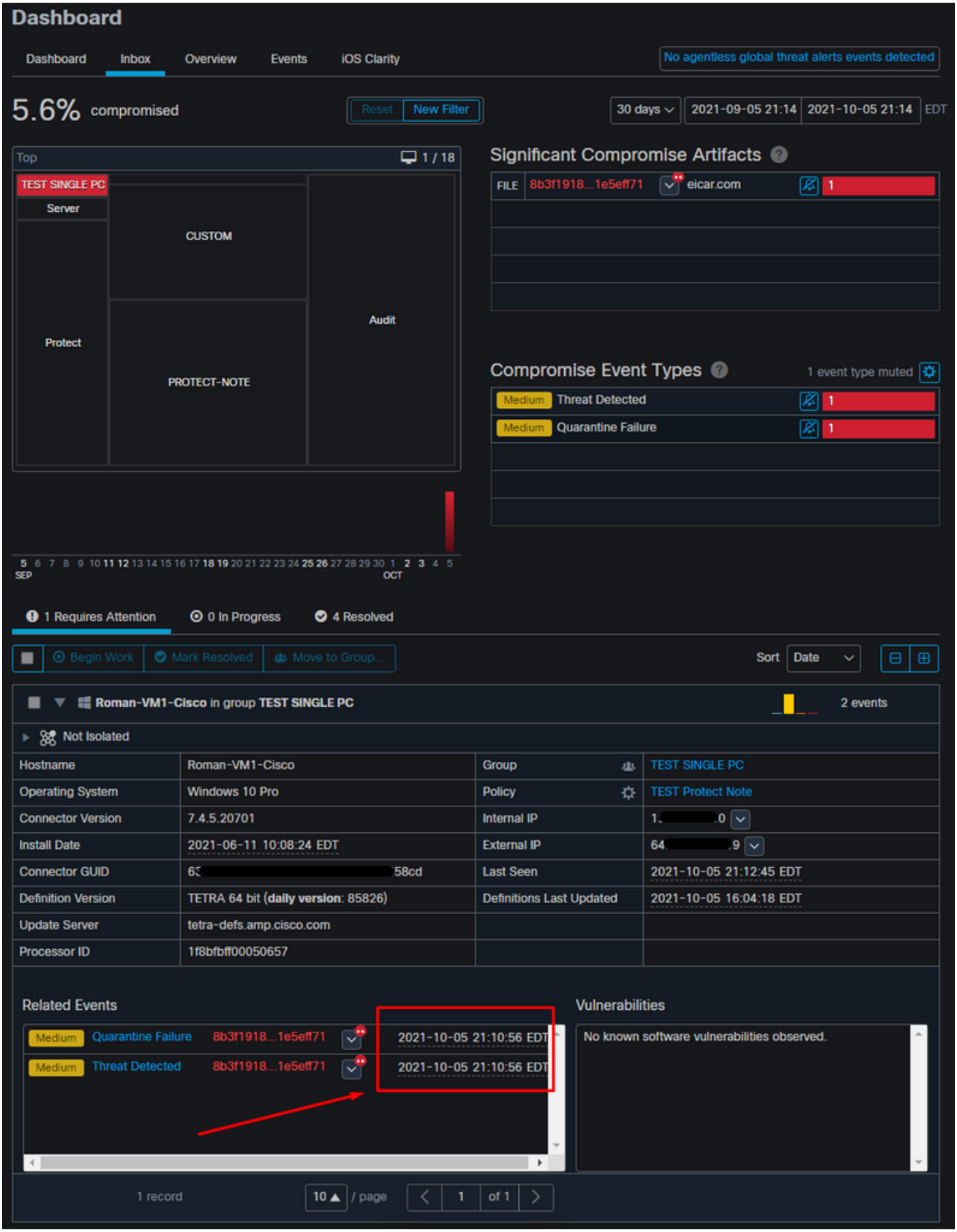
Dopo aver selezionato il pulsante Segna come risolto e poiché nel dashboard dell'endpoint protetto è stato compromesso un solo endpoint, avrà l'aspetto seguente. E a questo punto, è scattato un nuovo evento compromesso sulla macchina di test.



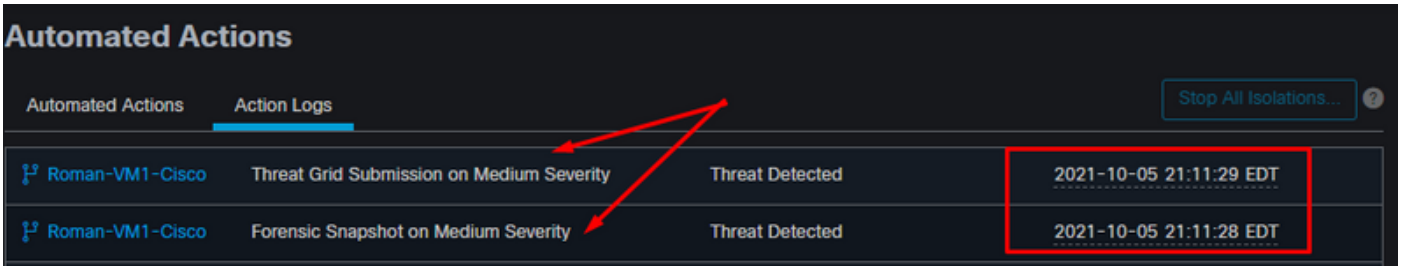
Nell'esempio successivo viene attivato un evento con uno script personalizzato che crea ed elimina un file dannoso.



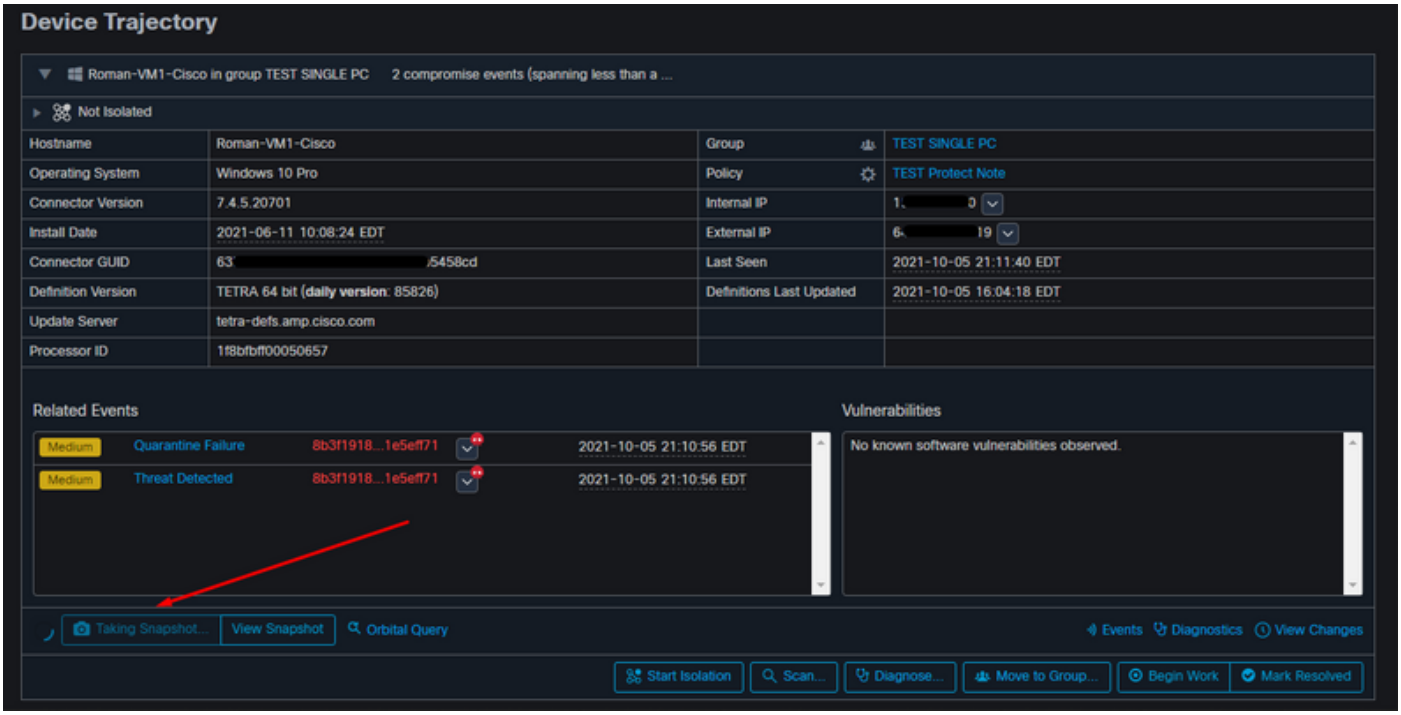
La console dell'endpoint sicuro è ancora una volta compromessa, come mostrato nell'immagine



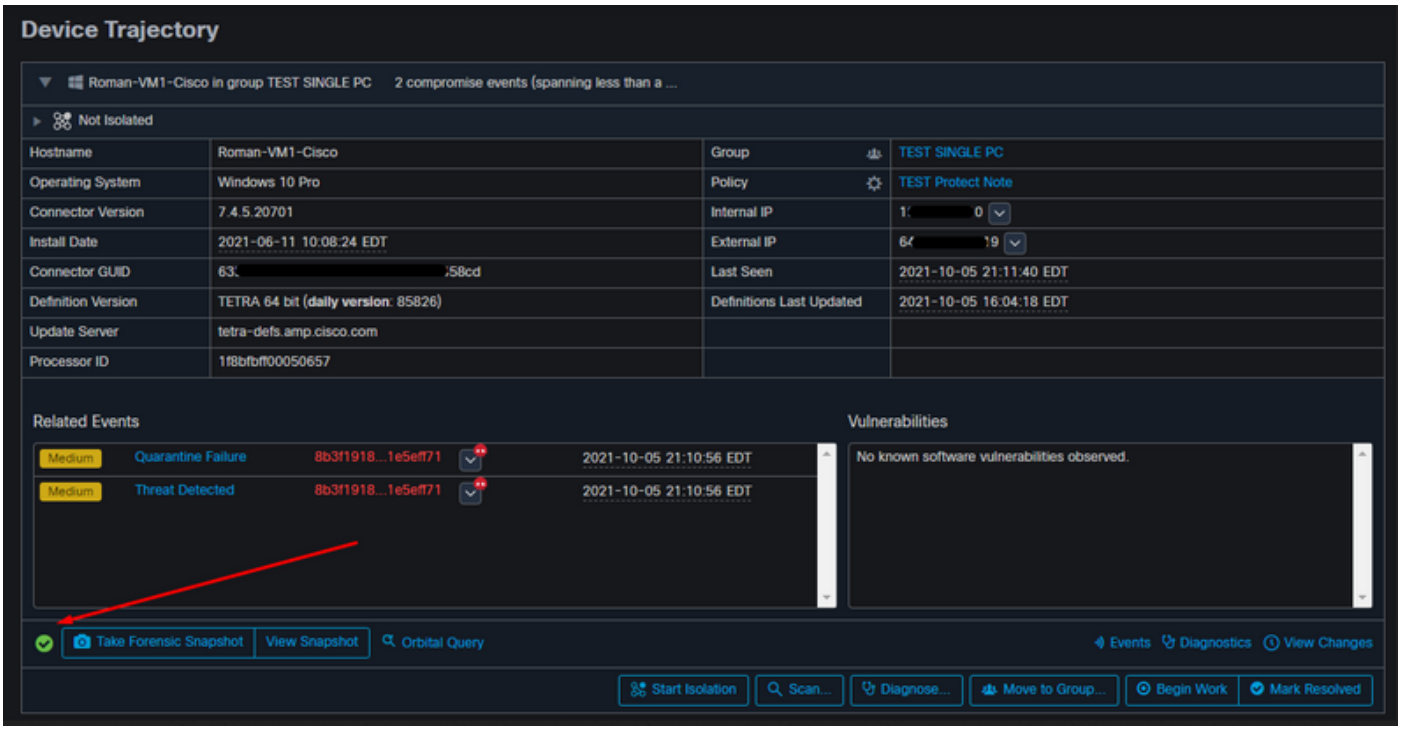
Di seguito sono riportati i nuovi eventi in Azioni automatiche, come mostrato nell'immagine.



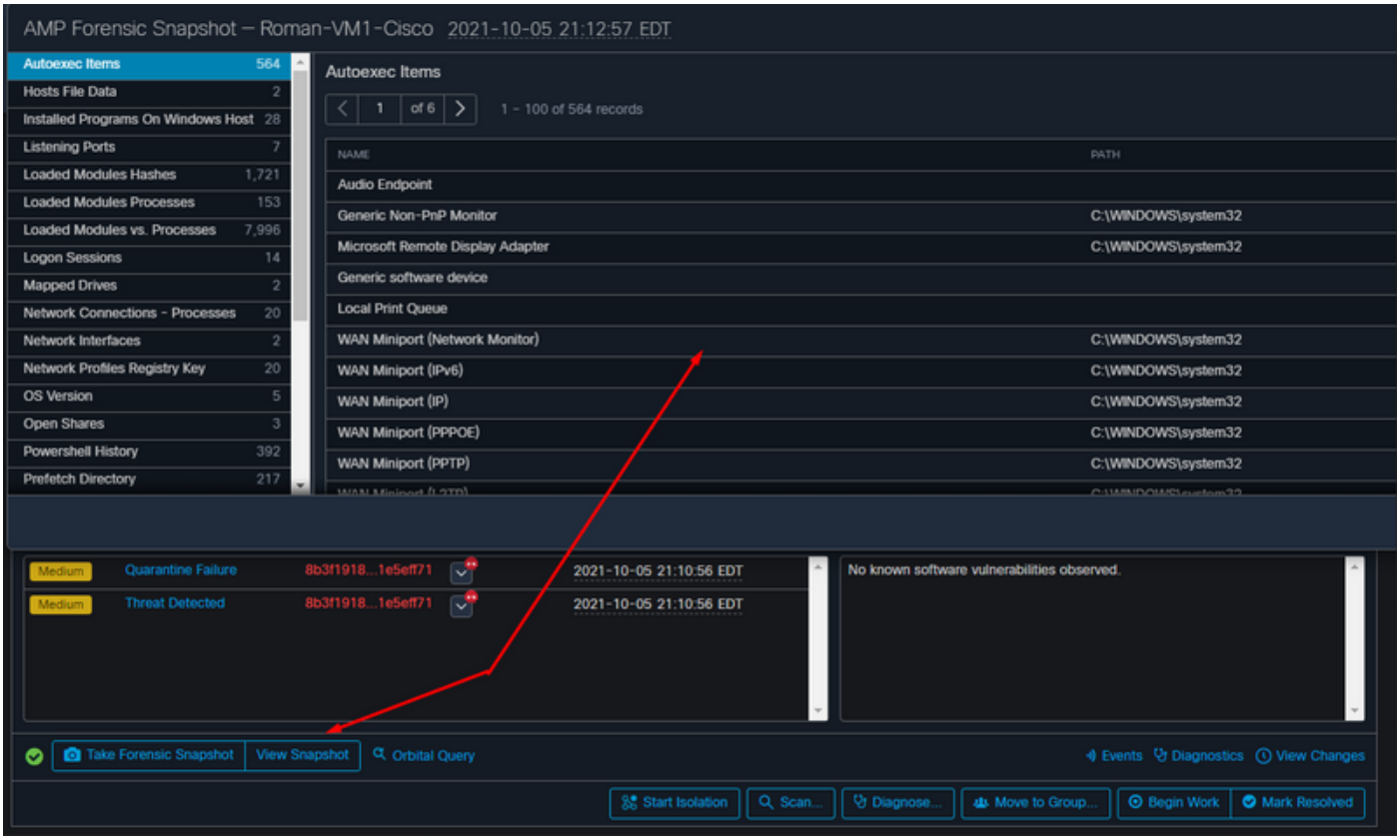
Quando il nome host in Azioni automatiche è selezionato, viene reindirizzato alla traiettoria del dispositivo dove è possibile osservare la copia istantanea creata dopo aver espanso la scheda del computer, come mostrato nell'immagine.



E minuto dopo viene creata una copia istantanea, come mostrato nell'immagine.



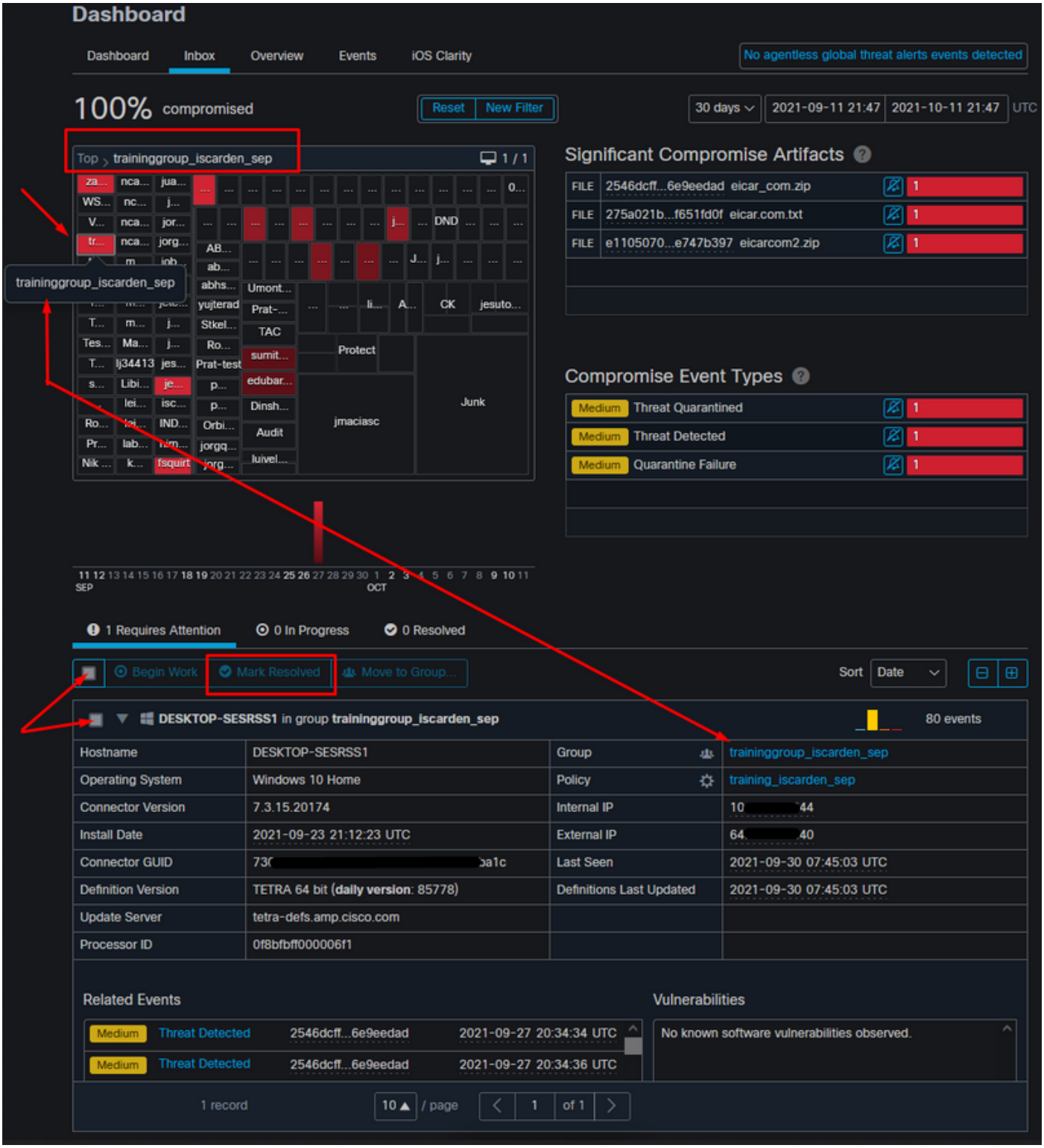
Ora è possibile visualizzare i dati visualizzati.



Suggerimento

In ambienti molto grandi con migliaia di endpoint e centinaia di compromessi, è possibile trovarsi in situazioni in cui la navigazione verso il singolo endpoint potrebbe rappresentare una sfida. Al momento, l'unica soluzione disponibile consiste nell'utilizzare la mappa termica e quindi eseguire il drilling verso il basso a un gruppo specifico in cui l'endpoint di compromesso è come nell'esempio seguente.

Una volta selezionato il gruppo nella mappa termica, spostatevi sul gruppo in cui l'evento è stato compromesso. Dato che c'è un solo endpoint in quel gruppo, vi preghiamo di notare il 100% compromesso che si basa ora sul gruppo specifico in cui ci troviamo. In altre parole, se abbiamo due endpoint in questo gruppo uno pulito e l'altro compromesso mostra un compromesso del 50%.


Dashboard
Dashboard
Inbox
Overview
Events
iOS Clarity
No agentless global threat alerts events detected
100% compromised
Reset
New Filter
30 days
2021-09-11 21:47
2021-10-11 21:47
UTC
Top
trainninggroup_iscarden_sep
1 / 1
trainninggroup_iscarden_sep
Significant Compromise Artifacts
FILE 2546dcff...6e9eedad eicar_com.zip 1
FILE 275a021b...f651fd0f eicar.com.txt 1
FILE e1105070...e747b397 eicarcom2.zip 1
Compromise Event Types
Medium Threat Quarantined 1
Medium Threat Detected 1
Medium Quarantine Failure 1
Protect
Junk
jmaciasc
11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 1 2 3 4 5 6 7 8 9 10 11
SEP
OCT
1 Requires Attention
0 In Progress
0 Resolved
Begin Work
Mark Resolved
Move to Group...
Sort
Date
DESKTOP-SESRSS1 in group trainninggroup_iscarden_sep
80 events
Hostname
DESKTOP-SESRSS1
Group
trainninggroup_iscarden_sep
Operating System
Windows 10 Home
Policy
training_iscarden_sep
Connector Version
7.3.15.20174
Internal IP
Install Date
2021-09-23 21:12:23 UTC
External IP
Connector GUID
Last Seen
2021-09-30 07:45:03 UTC
Definition Version
TETRA 64 bit (daily version: 85778)
Definitions Last Updated
2021-09-30 07:45:03 UTC
Update Server
tetra-defs.amp.cisco.com
Processor ID
0f8bfbff000006f1
Related Events
Medium Threat Detected 2546dcff...6e9eedad 2021-09-27 20:34:34 UTC
Medium Threat Detected 2546dcff...6e9eedad 2021-09-27 20:34:36 UTC
Vulnerabilities
No known software vulnerabilities observed.
1 record
10
/ page
1
of 1