Acciones automatizadas: instantánea forense

Contenido

[Introducción](#)
[Preguntas frecuentes](#)
[¿Qué es una máquina en peligro?](#)
[¿Qué es un compromiso?](#)
[¿Qué ocurre cuando se producen nuevas detecciones en una máquina en peligro?](#)
[¿Dónde puedo ver y gestionar los compromisos?](#)
[¿Cómo se activa una acción automatizada*?](#)
[¿Cómo puedo volver a activar una acción automatizada?](#)
[Caso usado - Recreación de laboratorio](#)
[Recomendación](#)

Introducción

Este documento describe la funcionalidad de Acción Automatizada en el Terminal Seguro que está ligada al concepto de Compromisos. Entender el ciclo de vida y la gestión de los compromisos son vitales para comprender la funcionalidad de las acciones automatizadas. Este artículo responde preguntas sobre la terminología y funcionalidad de estos conceptos.

Preguntas frecuentes

¿Qué es una máquina en peligro?

Una máquina en peligro es un terminal que tiene un riesgo activo asociado. Una máquina en peligro sólo puede, por diseño, tener un riesgo activo a la vez.

¿Qué es un compromiso?

Un riesgo es una colección de una o más detecciones en una máquina. La mayoría de los eventos de detección (amenaza detectada, indicadores de compromiso, etc.) pueden generar o asociarse a un riesgo. Sin embargo, hay pares de acontecimientos que pueden no generar un nuevo compromiso. Por ejemplo, cuando se produce un evento Threat Detected, pero poco después de que tenga un evento Threat Quarantines asociado, esto no provoca un nuevo riesgo. Lógicamente, esto se debe a que el terminal seguro ha gestionado el riesgo potencial (pusimos en cuarentena la amenaza).

¿Qué ocurre cuando se producen nuevas detecciones en una máquina en peligro?

Los eventos de detección se agregan al riesgo existente. No se crea ningún nuevo compromiso.

¿Dónde puedo ver y gestionar los compromisos?

Los compromisos se gestionan en la ficha Bandeja de entrada de la consola de terminales

seguros (que es https://console.amp.cisco.com/compromises para la nube de Norteamérica). Una máquina en peligro aparece en la sección **Requerir atención** y se puede eliminar de su compromiso presionando **Marcar resuelto**. Además, los compromisos se eliminan automáticamente después de un mes.

¿Cómo se activa una acción automatizada*?

Las acciones automatizadas se activan cuando se produce un riesgo, es decir, cuando una máquina sin riesgos se convierte en una máquina en peligro. Si una máquina que ya se encuentra en peligro encuentra una nueva detección, esta detección se añade al riesgo, pero como no se trata de un nuevo riesgo, no activa una acción automatizada.

¿Cómo puedo volver a activar una acción automatizada?

Es necesario "aclarar" el compromiso antes de intentar volver a activar una acción automatizada. Tenga en cuenta que un evento Threat Detected + Threat Quarantines no es suficiente para generar un nuevo evento de compromiso (y, por lo tanto, no es suficiente para activar una nueva acción automatizada).

*Excepción: La acción automatizada "Enviar archivo a ThreatGrid" no está afiliada a riesgos y se ejecuta por detección

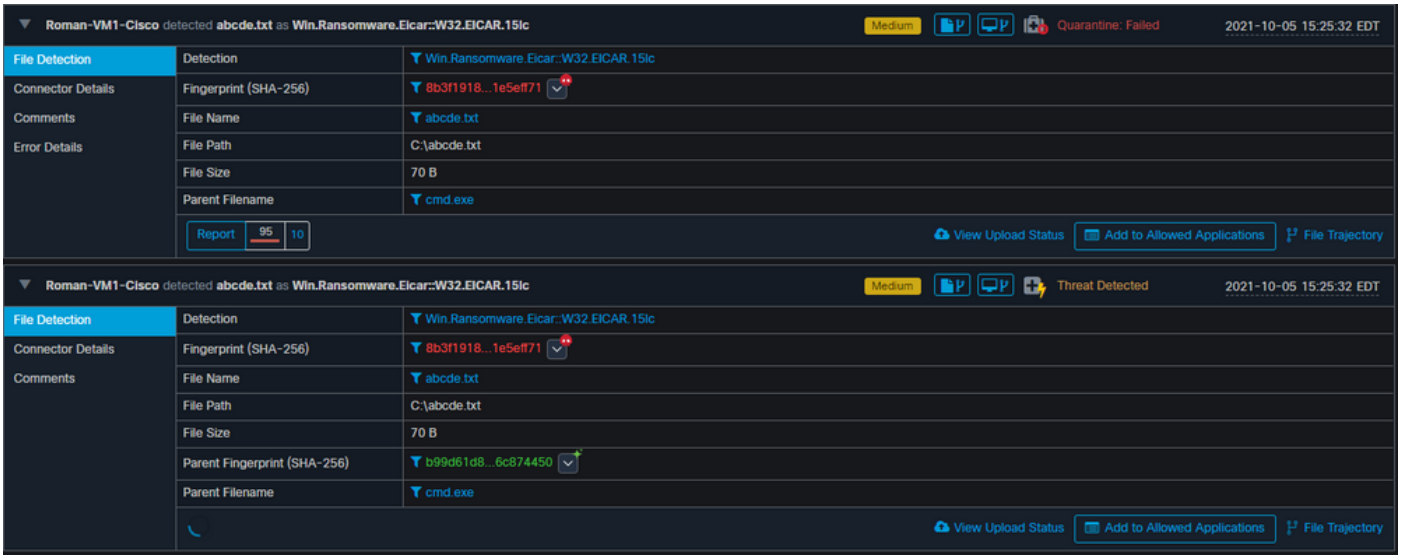
Caso usado - Recreación de laboratorio

N.º 1: Como hemos indicado en la sección Preguntas frecuentes. Las instantáneas forenses se toman sólo en caso de "compromiso". En otras palabras, si tratamos de acceder y descargar un archivo malicioso desde un sitio TEST y el archivo se marca al descargarlo y ponerlo en cuarentena que no se considera un riesgo y no activa la acción.

> **Nota:** La detección de DFC, la falla de cuarentena y prácticamente cualquier cosa que, según la lógica, caiga en la categoría de evento de compromiso debería crear una instantánea forense.

N.º 2: Solo puede generar una instantánea forense una vez en un evento comprometido único, no genera una instantánea a menos que resuelva el problema de la máquina en su bandeja de entrada. Si no resuelve el evento comprometido, no generará ninguna otra instantánea.

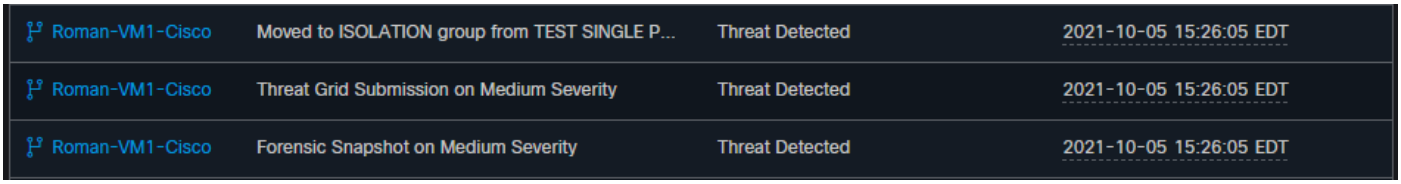
Ejemplo: En este laboratorio, una secuencia de comandos genera actividad maliciosa y, como el archivo se elimina tan pronto como se crea y el terminal seguro no pudo poner en cuarentena el archivo en el que se encuentra para poner en peligro la categoría.



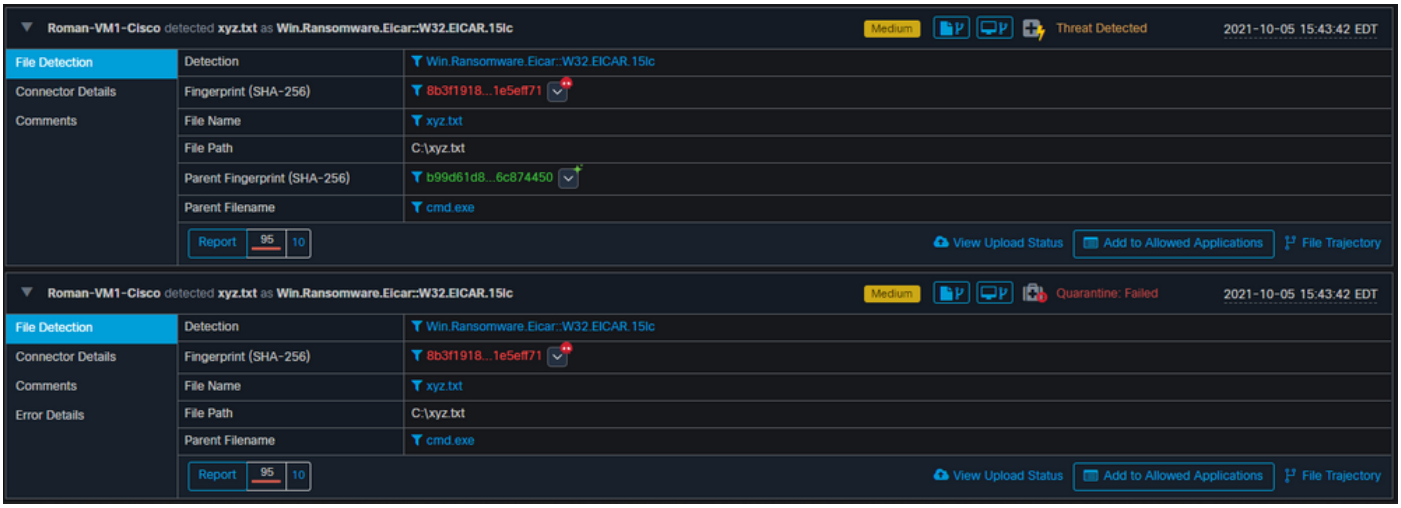
Ahora en esta prueba, puede ver las acciones automatizadas y 3 cosas que han ocurrido en función de la configuración.

- Se creó la instantánea
- El envío se envió a Threat Grid (TG)
- El punto final se trasladó a un grupo distinto que se creó y se llamó AISLAMIENTO

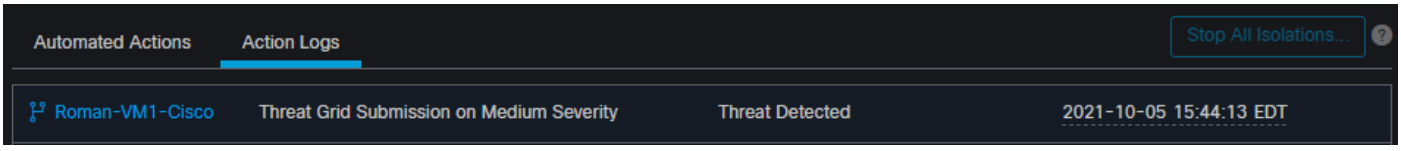
Puede ver todo eso en esta salida, como se muestra en la imagen.



Ahora que este terminal está comprometido, la siguiente prueba para probar la teoría con un archivo malintencionado similar pero con un nombre diferente, como se muestra en la imagen.

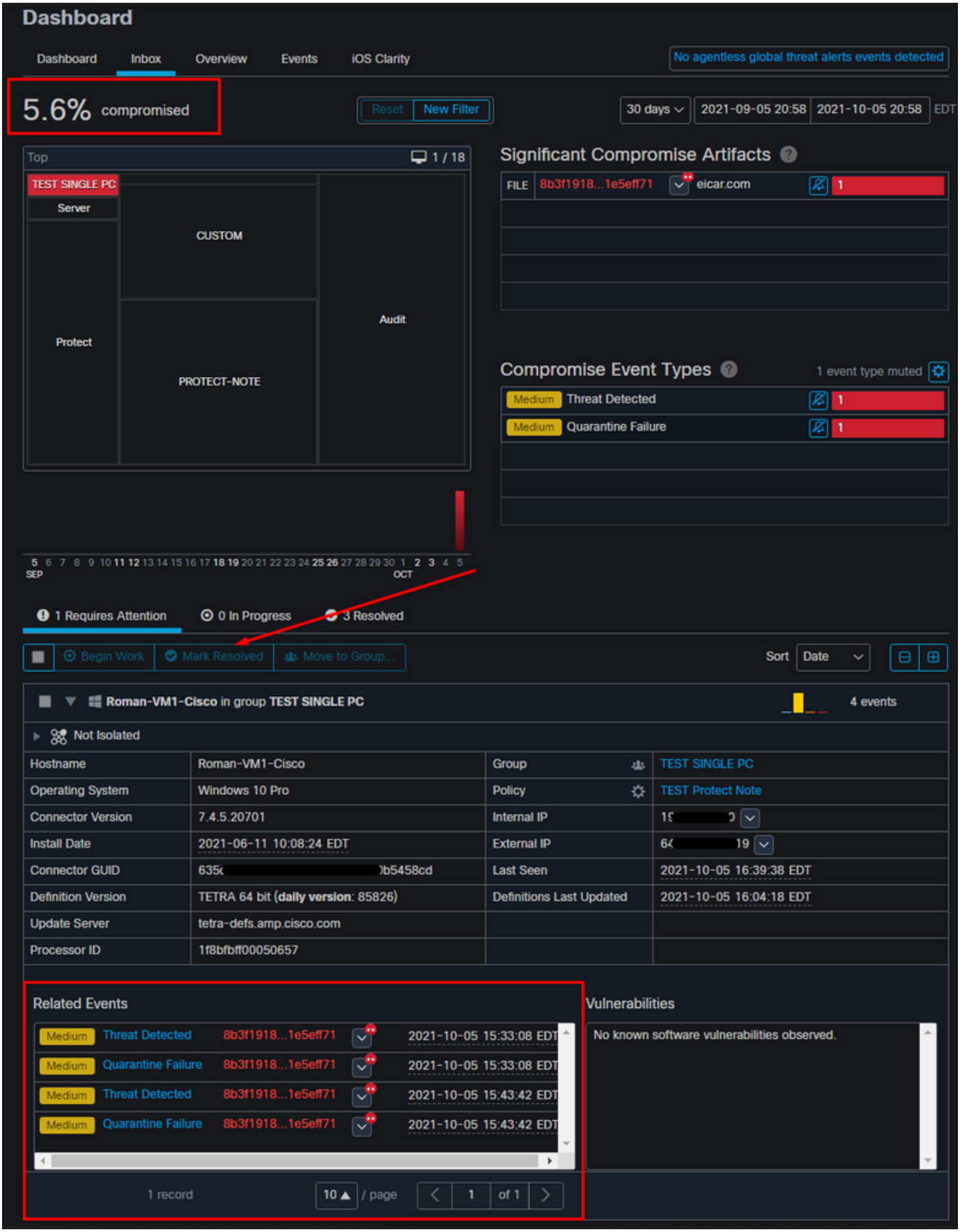


Sin embargo, como este compromiso no se resolvió, sólo puede crear un envío de TG. No se registraron otros eventos, también se apaga el aislamiento antes de esta 2ª prueba.

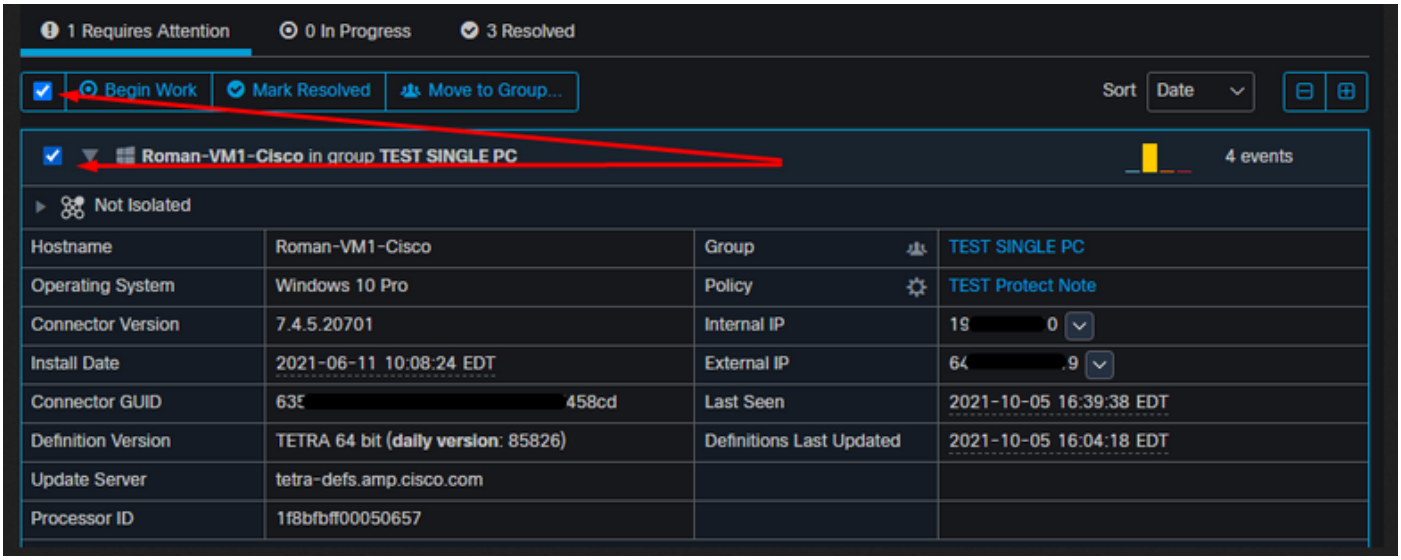


Nota: Observe el momento en que se detectó la amenaza y se activaron las acciones automatizadas.

El evento no se puede recuperar a menos que se resuelva el extremo comprometido. En este caso, el panel se ve así. Observe el porcentaje y el botón Marcar resuelto junto con los eventos comprometidos. No importa cuántos eventos se activen, solo podrá crear una instantánea y el número de porcentaje grande nunca cambiará. Ese número representa un riesgo dentro de su organización y se basa en la cantidad total de terminales de su organización. Sólo cambia con otra máquina comprometida. En este ejemplo, el número es alto debido a que sólo hay 16 dispositivos en el laboratorio. Además, tenga en cuenta que los eventos de compromiso se borran automáticamente una vez que alcanzan los 31 días de edad.

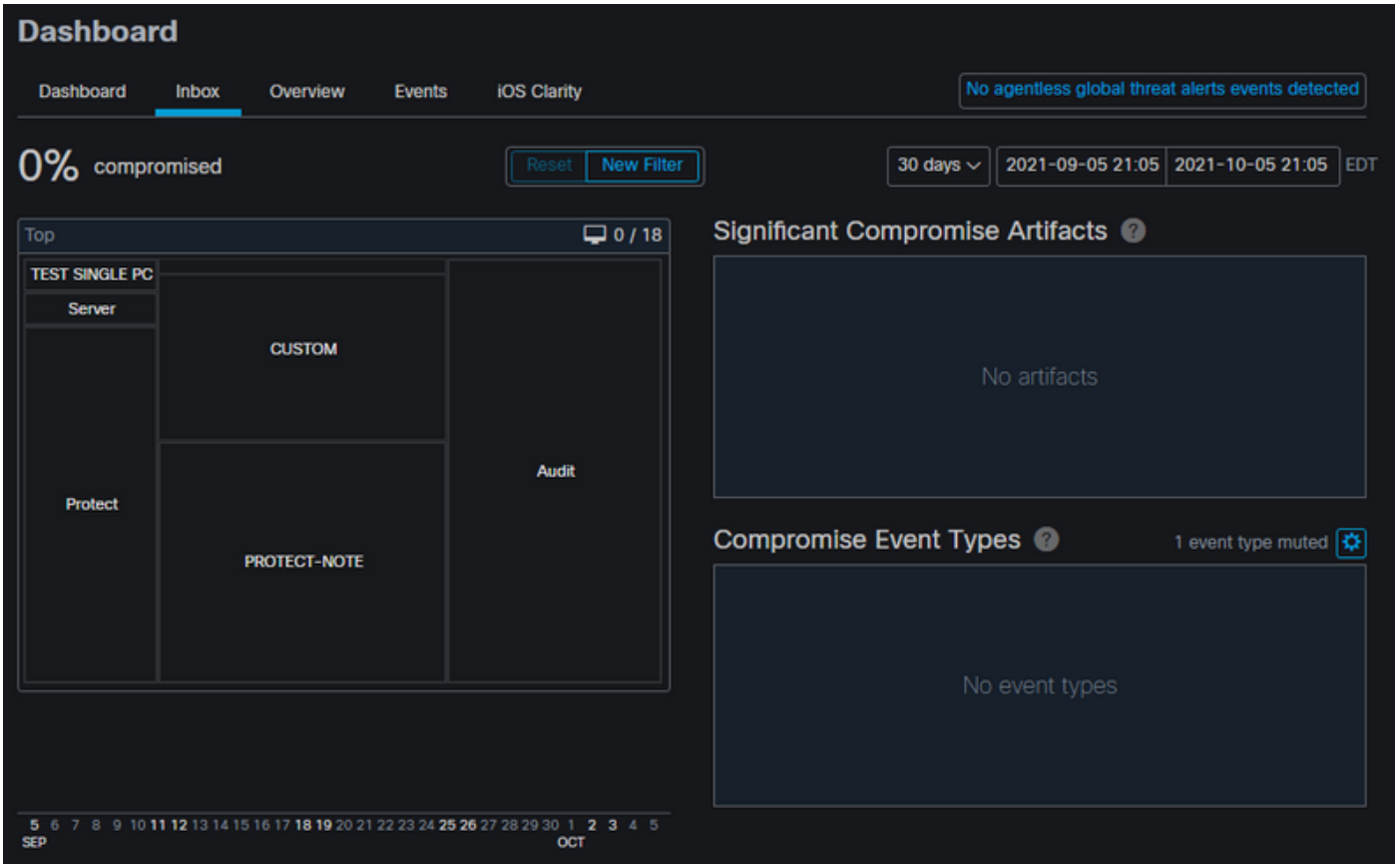


El siguiente paso es crear otro evento y generar una instantánea forense. El primer paso es resolver este problema, haga clic en el botón **Marcar resuelto**. Puede hacerlo por terminal o puede seleccionar todo en su organización.

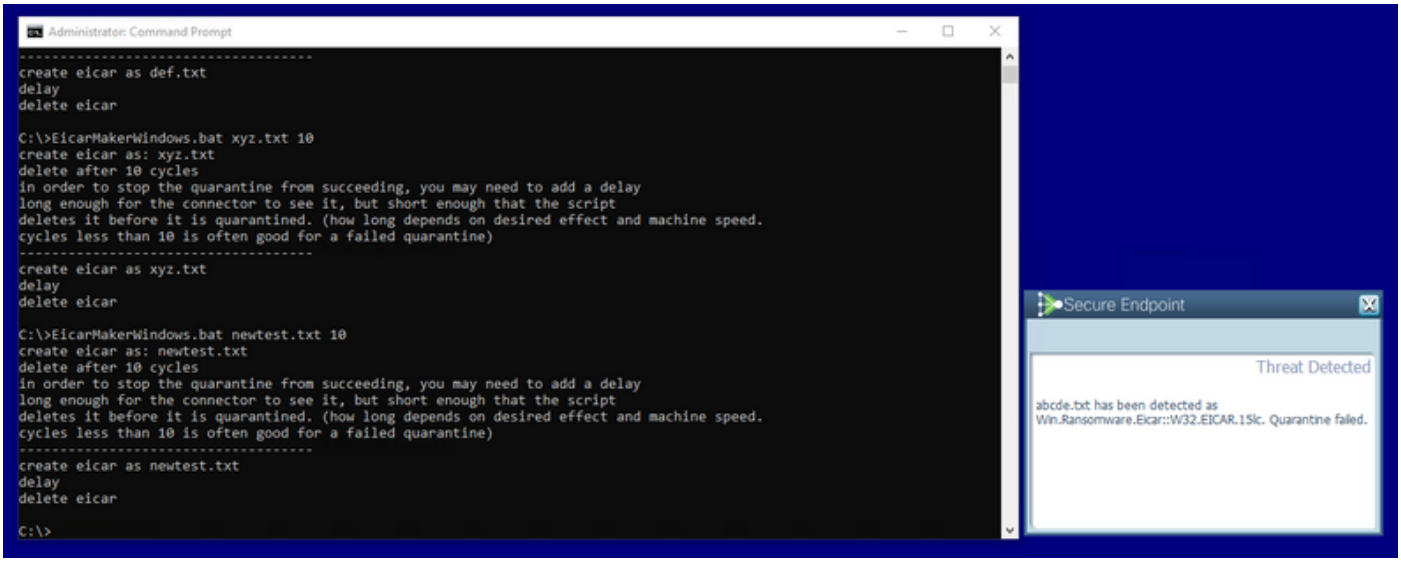


Nota: Si selecciona todos los compromisos, se restablecen al 0%.

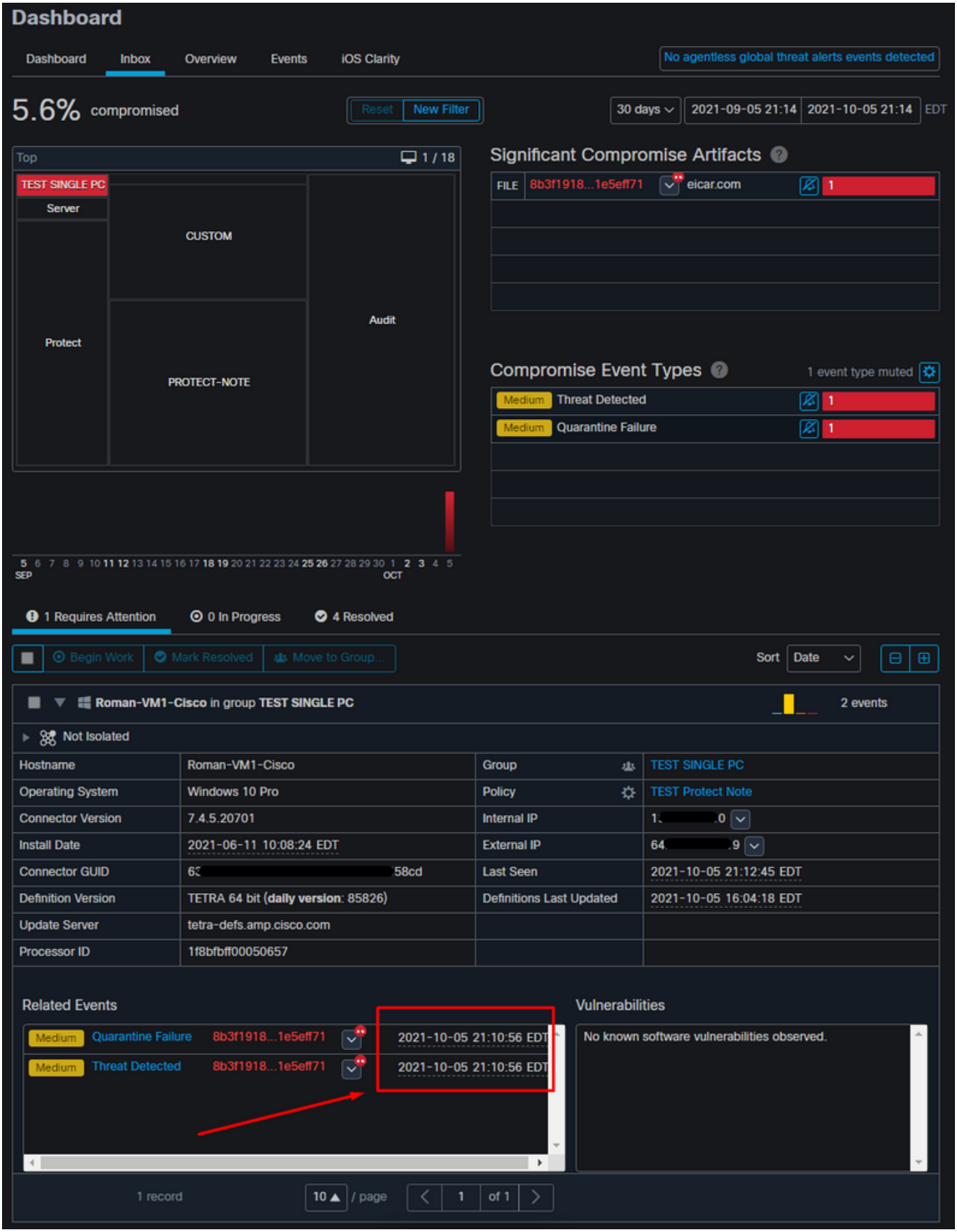
Una vez seleccionado el botón Marcar resuelto y puesto que sólo un terminal se vio comprometido en el panel de terminales seguros, se verá así. Y en este punto, se desencadenó un nuevo evento comprometido en la máquina de prueba.



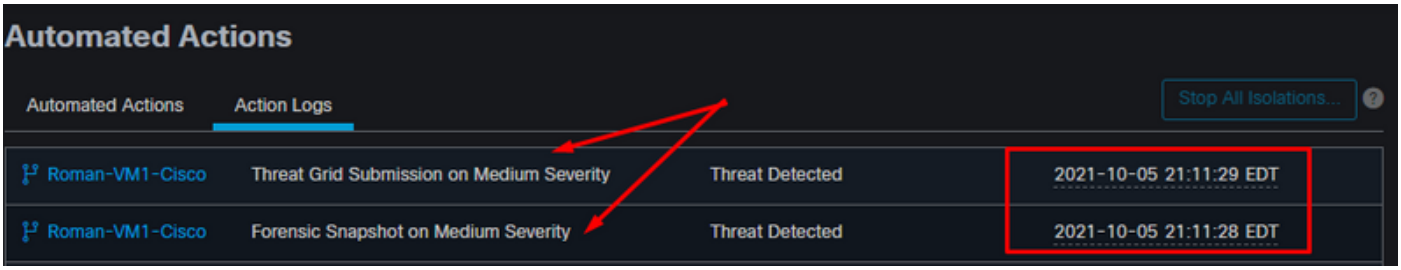
El siguiente ejemplo activa un evento con un script personalizado que crea y elimina un archivo malintencionado.



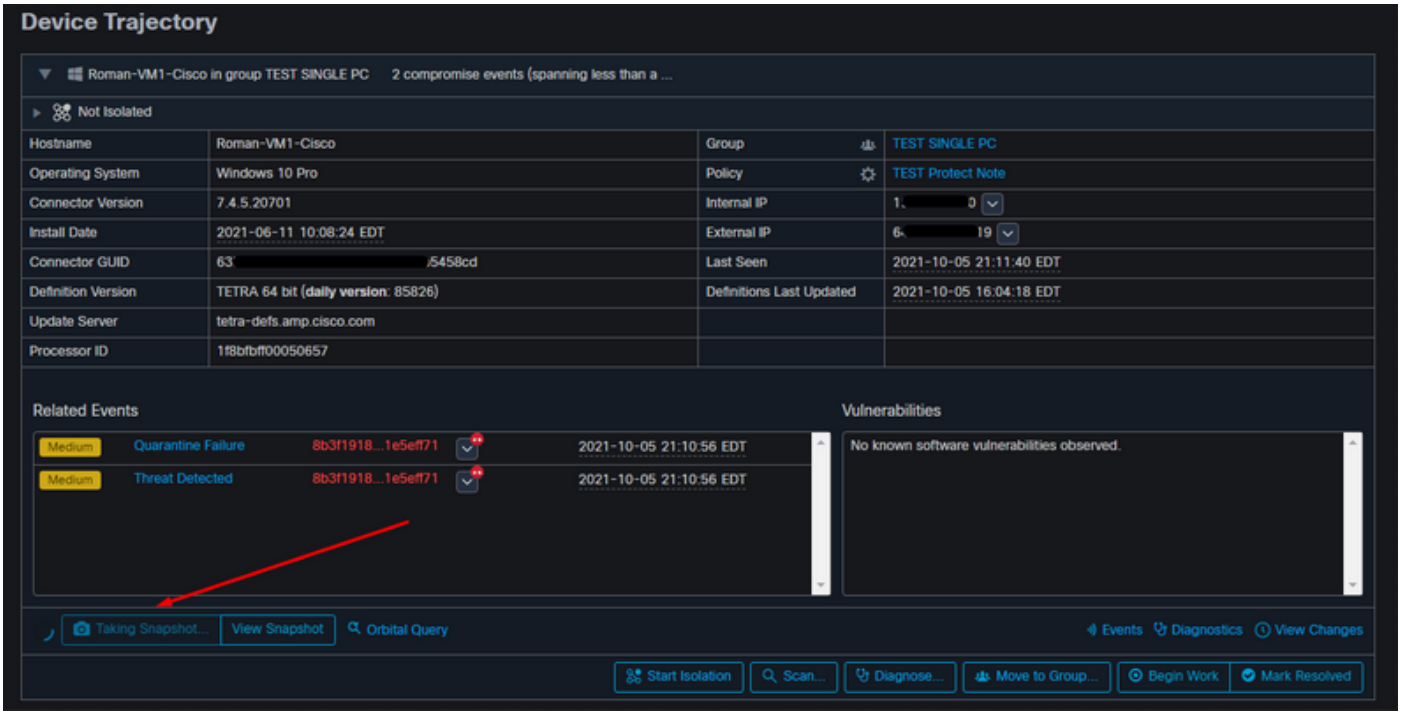
Una vez más, la consola de terminales seguros se vio comprometida, como se muestra en la imagen



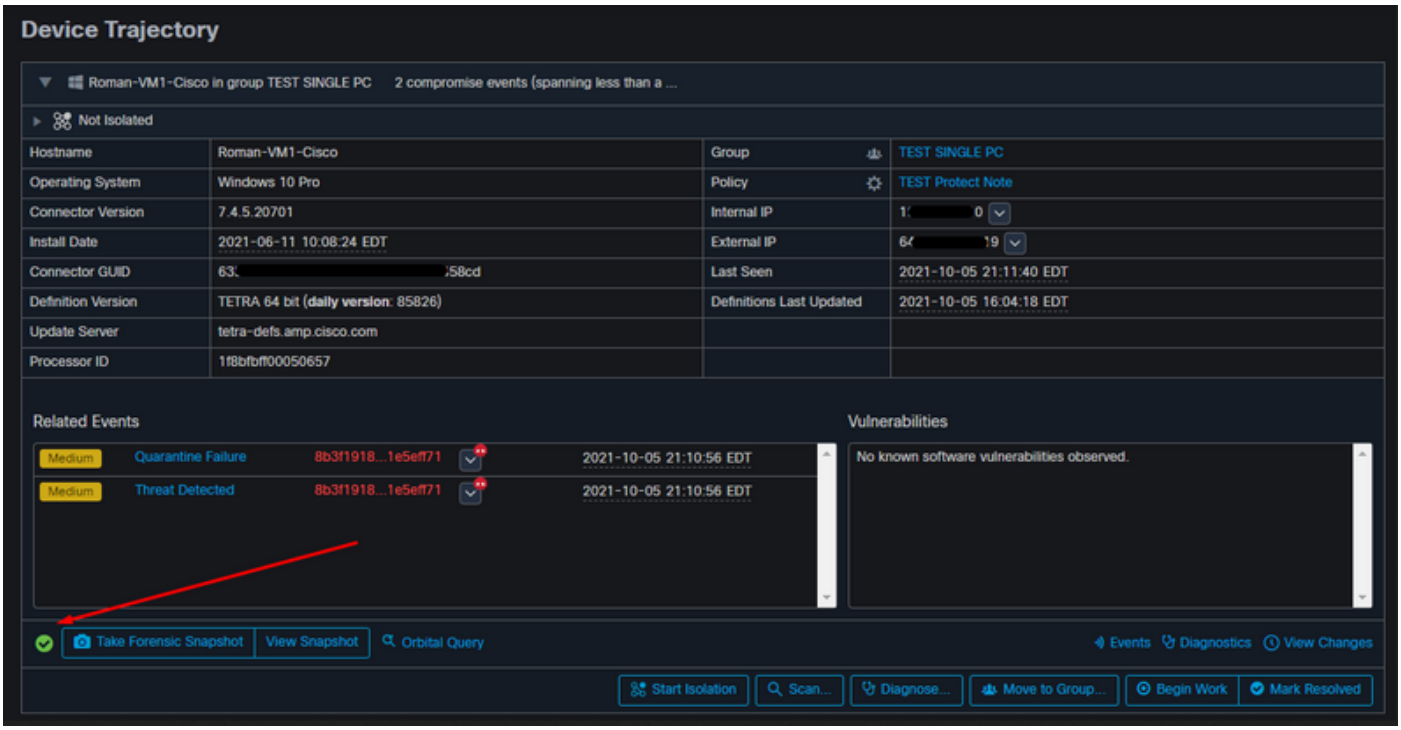
Estos son los nuevos eventos en Acciones automatizadas, como se muestra en la imagen.



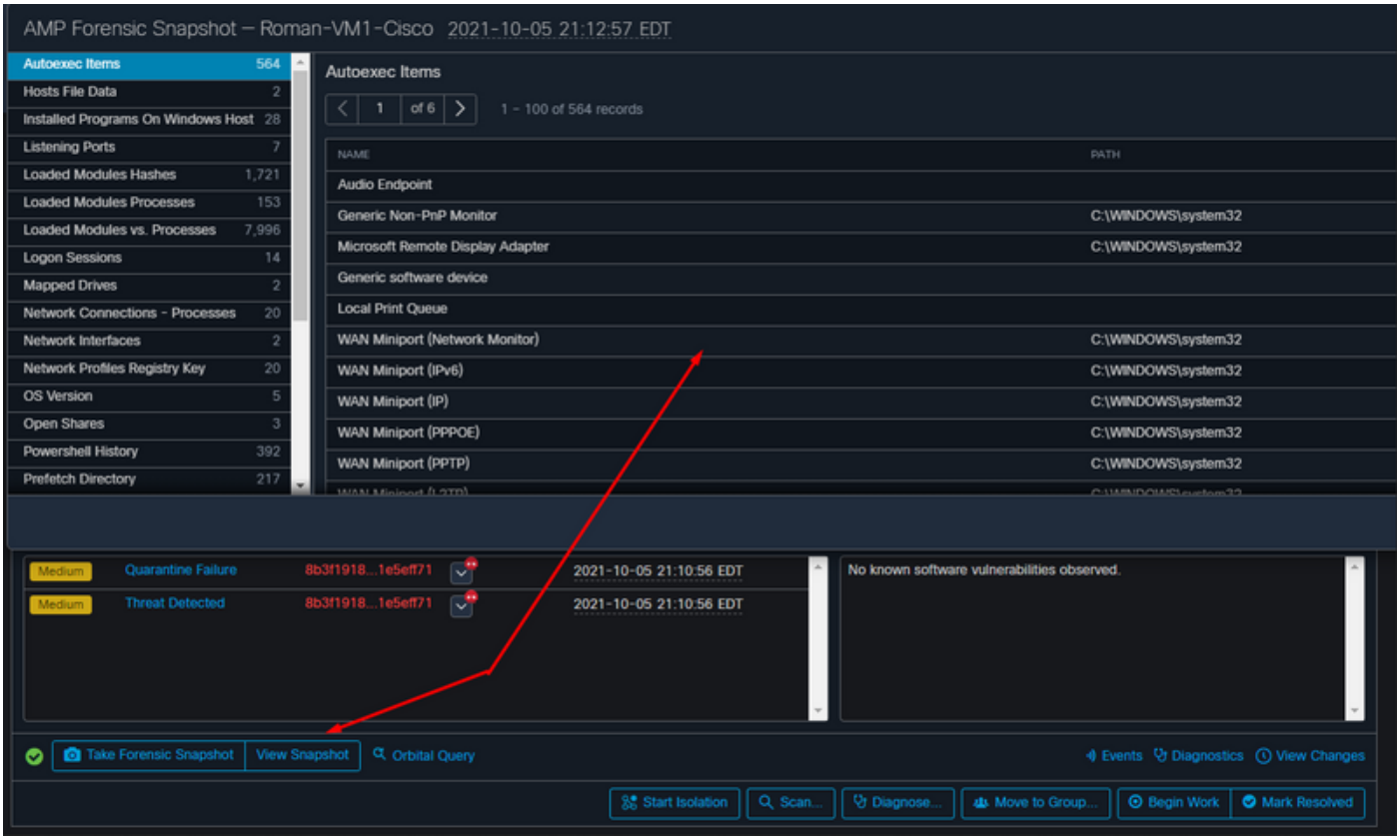
Cuando se selecciona el nombre de host en Acciones automatizadas, se redirige a la trayectoria del dispositivo, donde puede observar la instantánea que se crea una vez que expande la ficha del equipo, como se muestra en la imagen.



Y minutos después se crea una instantánea, como se muestra en la imagen.



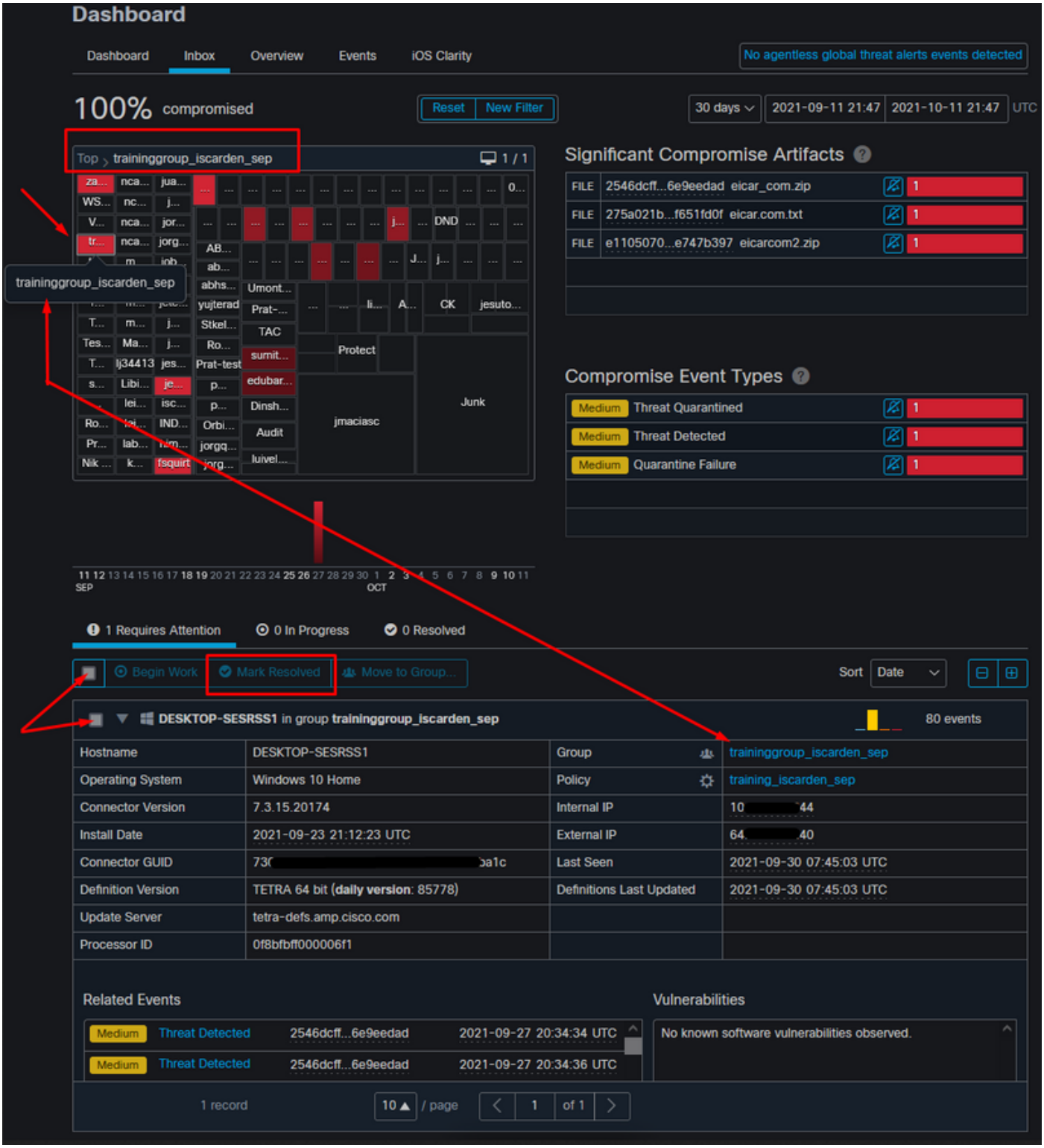
Y ahora puede ver los datos mostrados.



Recomendación

En entornos muy grandes con miles de terminales y cientos de compromisos, puede encontrarse con situaciones en las que la navegación hacia el terminal individual puede suponer un reto. Actualmente, la única solución disponible es utilizar el mapa de calor y, a continuación, profundizar en un grupo específico en el que su terminal de riesgo es como en este ejemplo a continuación.

Una vez seleccionado el grupo en el mapa de calor, navegue hasta ese grupo en el que hemos comprometido el evento. Dado que solo hay un terminal en ese grupo, observe el 100% comprometido que se basa ahora en el grupo específico en el que estamos. En otras palabras, si tenemos dos terminales en este grupo, uno limpio y el otro comprometido muestra un compromiso 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