Ações automatizadas - Instantâneo forense

Contents

Introduction

Este documento descreve a funcionalidade de ação automatizada no Secure Endpoint vinculada ao conceito de Compromissos. Compreender o ciclo de vida e o gerenciamento de compromissos são vitais para compreender a funcionalidade das ações automatizadas. Este artigo responde a perguntas sobre a terminologia e a funcionalidade desses conceitos.

FAQ

O que é uma máquina comprometida?

Uma máquina comprometida é um endpoint que tem um comprometimento ativo associado a ela. Uma máquina comprometida pode, por projeto, ter apenas um comprometimento ativo de uma vez.

O que é um compromisso?

Um comprometimento é uma coleção de uma ou mais detecções em uma máquina. A maioria dos eventos de detecção (ameaça detectada, indicações de comprometimento etc.) pode gerar ou se tornar associada a um comprometimento. No entanto, há pares de eventos que podem não desencadear um novo compromisso. Por exemplo, quando ocorre um evento Detectado de Ameaça, mas logo após ele ter um evento associado de Quarentena de Ameaça, isso não gera um novo comprometimento. Logicamente, isso ocorre porque o Secure Endpoint lidou com o possível comprometimento (colocamos a ameaça em quarentena).

O que acontece quando novas detecções ocorrem em uma máquina comprometida?

Os eventos de detecção são adicionados ao comprometimento existente. Nenhum novo compromisso é criado.

Onde posso ver e gerenciar comprometimentos?

Os compromissos são gerenciados na guia Caixa de entrada do console do Secure Endpoint (que é https://console.amp.cisco.com/compromises para a nuvem da América do Norte). Uma máquina comprometida está listada na seção **Require Attention** e pode ser eliminada de seu comprometimento pressionando **Mark Resolved**. Além disso, os compromissos são automaticamente eliminados após um mês.

Como uma ação automatizada* é acionada?

Ações automatizadas são acionadas com um comprometimento, ou seja, quando uma máquina sem comprometimento se torna uma máquina comprometida. Se uma máquina já comprometida encontrar uma nova detecção, essa detecção será adicionada ao comprometimento, mas como isso não é um novo comprometimento, ela não aciona uma ação automatizada.

Como posso reativar uma ação automática?

Énecessário "limpar" o compromisso antes de tentar reativar uma ação automática. Lembre-se de que um evento de Ameaça Detectada + Ameaça em Quarentena não é suficiente para gerar um novo evento de comprometimento (e, portanto, não é suficiente para disparar uma nova ação automatizada).

*Exceção: A ação automatizada "Enviar arquivo para o ThreatGrid" não é afiliada a comprometimentos e é executada por detecção

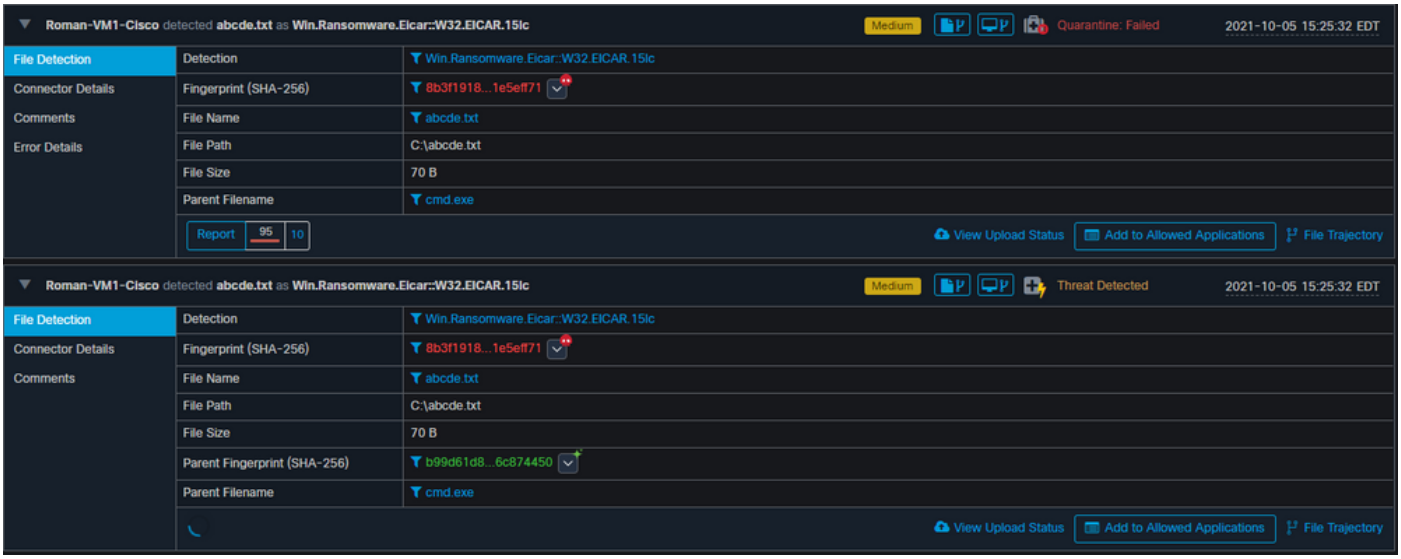
Caso usado - Recriação de laboratório

Nº 1: Como dissemos na seção de perguntas frequentes. Os snapshots forenses são obtidos somente em caso de "comprometimento". Em outras palavras, se tentarmos acessar e baixar um arquivo mal-intencionado de um site TEST e o arquivo for sinalizado durante o download e colocado em quarentena que não é considerado um comprometimento e não aciona a ação.

> **Note**: Detecção de DFC, Falha de Quarentena e praticamente qualquer coisa que, pela lógica, se encaixe na categoria de evento de comprometimento deve criar Instantâneo Forense.

Nº 2: Você só pode gerar um Instantâneo Forense uma vez em um evento comprometido exclusivo que ele não gere um instantâneo, a menos que você resolva a máquina comprometida na caixa de entrada. Se você não resolver o evento comprometido, não gerará nenhum outro snapshot.

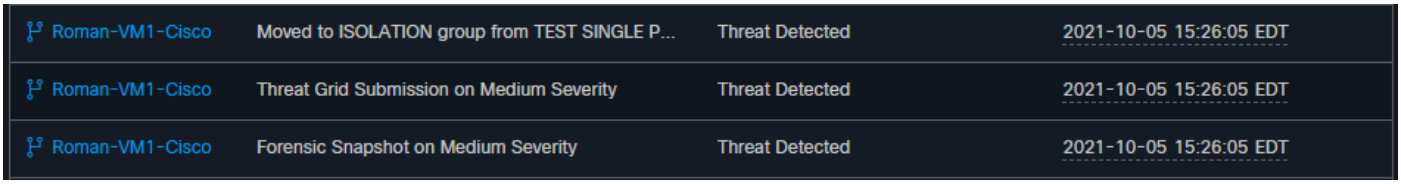
Exemplo: Neste laboratório, um script gera atividade mal-intencionada e, como o arquivo é excluído assim que é criado, o Secure Endpoint não conseguiu colocar o arquivo em quarentena na categoria de comprometimento.



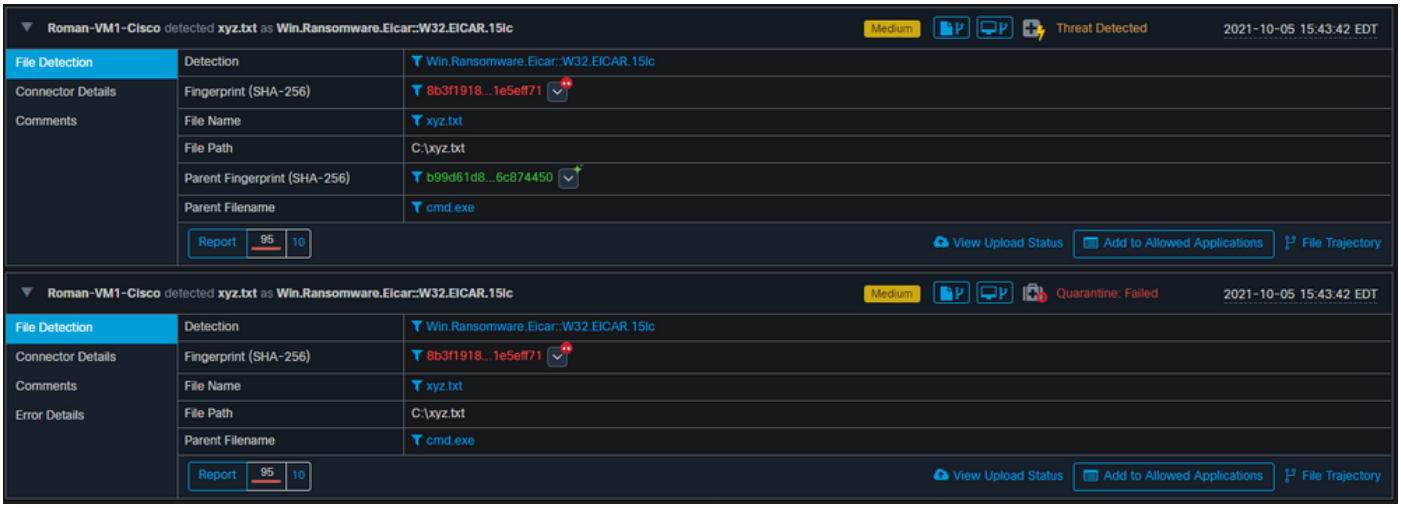
Agora, neste teste, você pode observar ações automatizadas e 3 coisas que aconteceram com base nas configurações.

- O instantâneo foi criado
- O envio foi enviado para o Threat Grid (TG)
- O endpoint foi movido para um grupo separado criado e chamado ISOLAMENTO

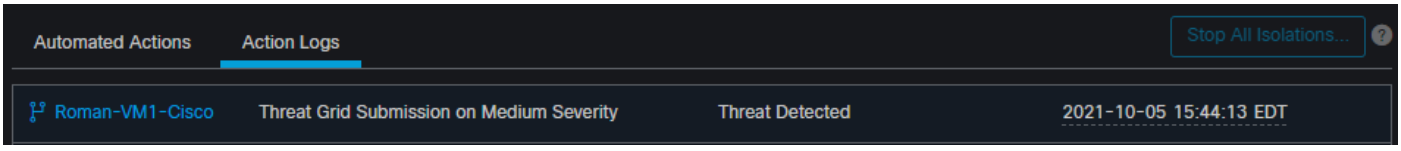
Você pode ver tudo isso nessa saída, como mostrado na imagem.



Agora, como esse endpoint está comprometido, o próximo teste para provar a teoria com um arquivo mal-intencionado semelhante, mas com um nome diferente, como mostrado na imagem.

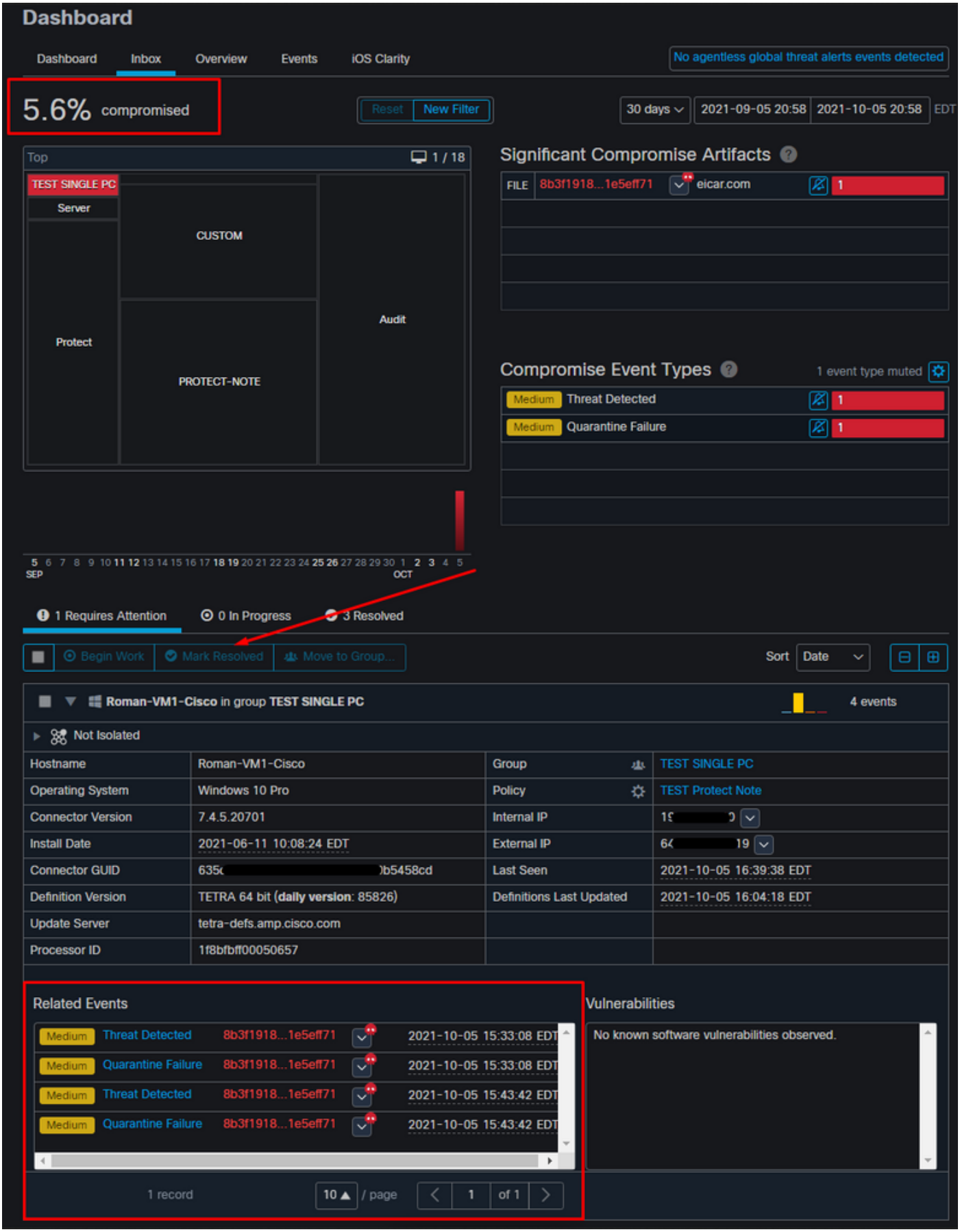


No entanto, como esse compromisso não foi resolvido, você só pode criar um envio de TG. Nenhum outro evento foi gravado, além de desligar o isolamento antes deste 2º teste.

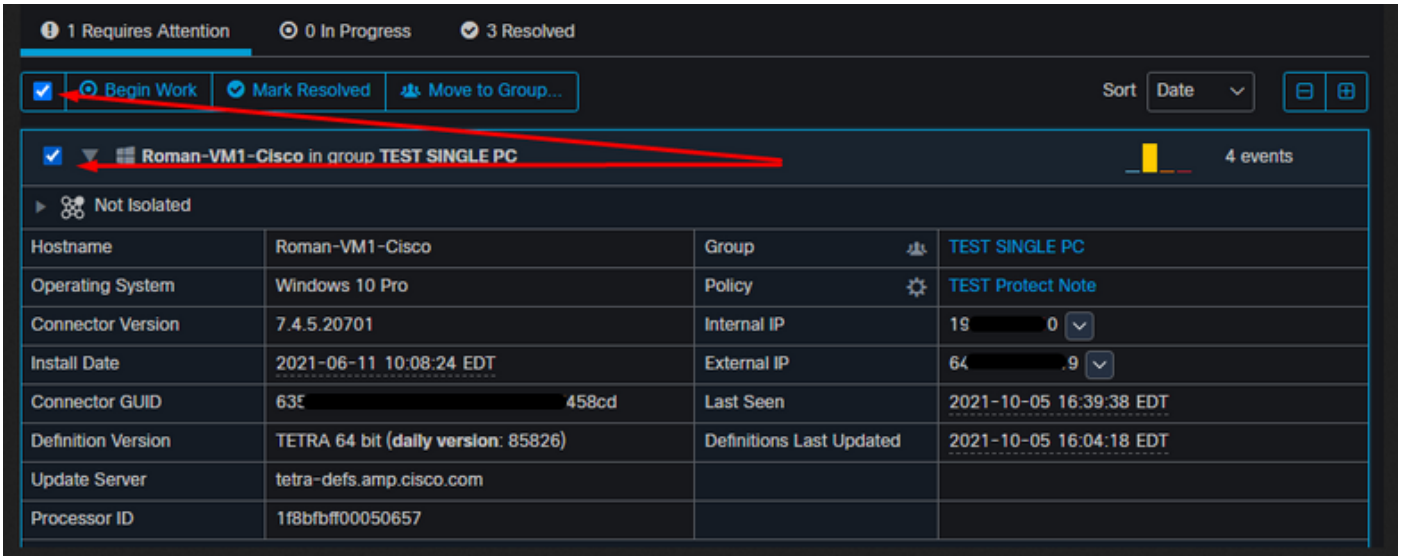


Note: Observe a hora em que a ameaça foi detectada e a ação automatizada é acionada.

O evento não poderá ser reacionado a menos que o ponto de extremidade comprometido seja resolvido. Nesse caso, o painel fica assim. Observe a porcentagem e o botão Mark Resolved junto com os eventos comprometidos. Não importa quantos eventos sejam disparados, você só pode criar um snapshot e o grande número percentual nunca mudou. Esse número representa um comprometimento dentro da sua empresa e se baseia na quantidade total de endpoints na sua empresa. Ele só muda com outra máquina comprometida. Neste exemplo, o número é alto devido a apenas 16 dispositivos no laboratório. Além disso, observe que os eventos de comprometimento são limpos automaticamente quando atingem 31 dias de idade.

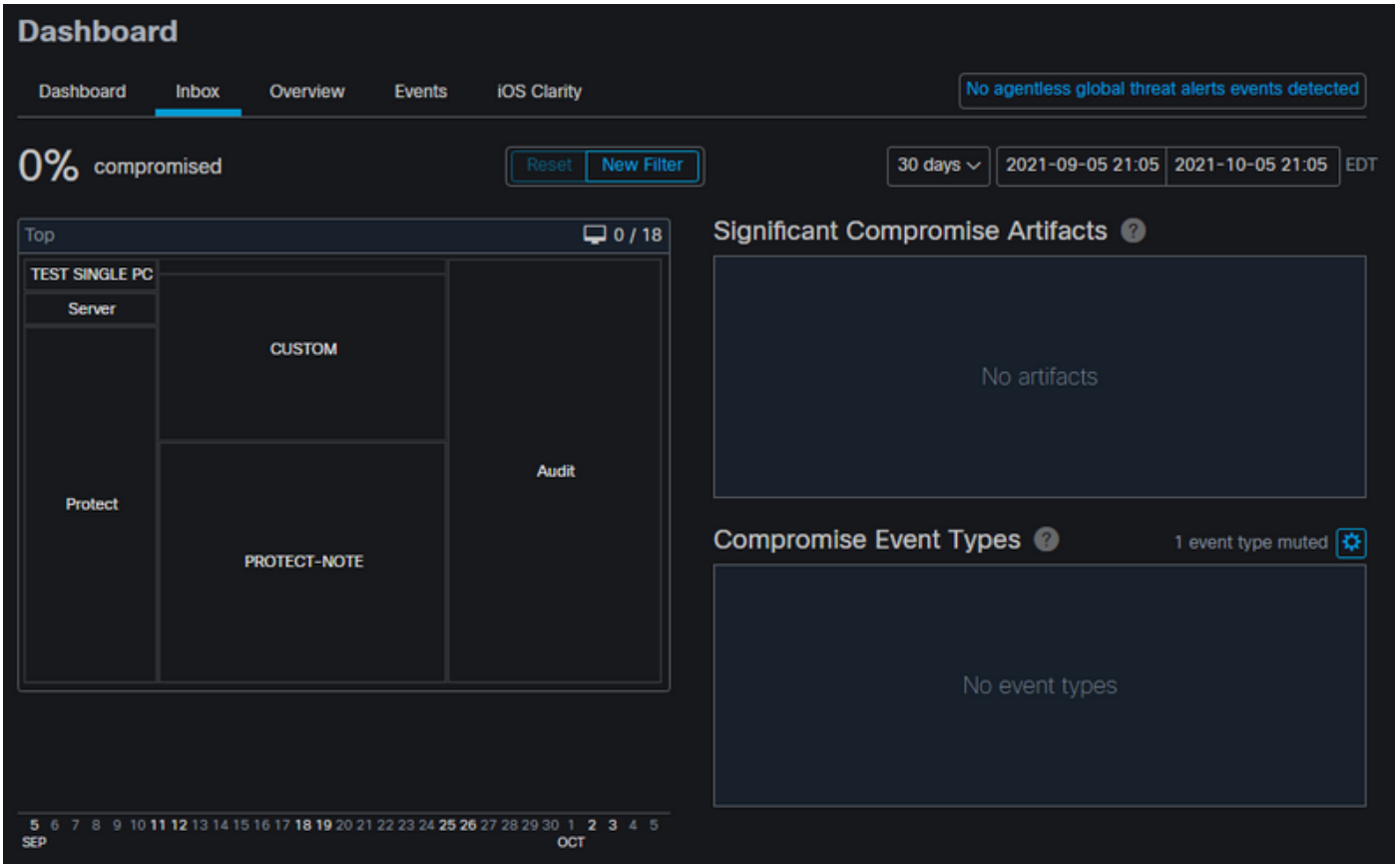


A próxima etapa é criar outro evento e gerar um snapshot forense. A primeira etapa é resolver esse compromisso, clique no botão **Marcar resolução**. Você pode fazer isso por endpoint ou selecionar tudo na sua organização.

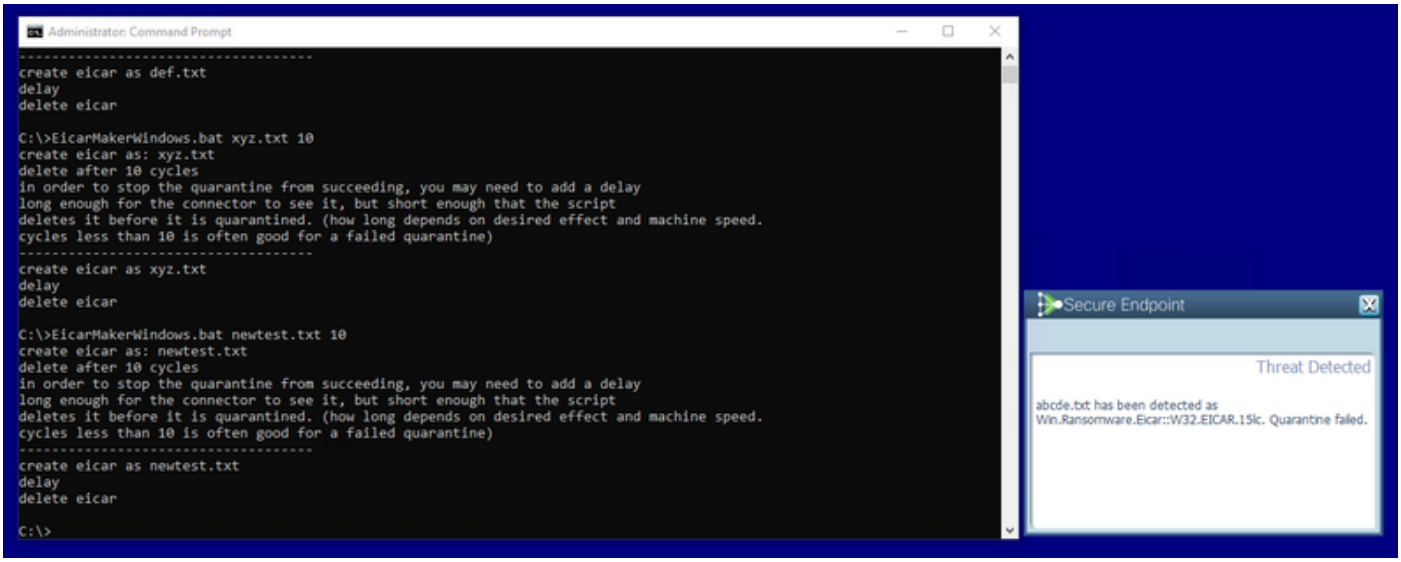


Observação: se você selecionar todos os comprometimentos serão redefinidos para 0%.

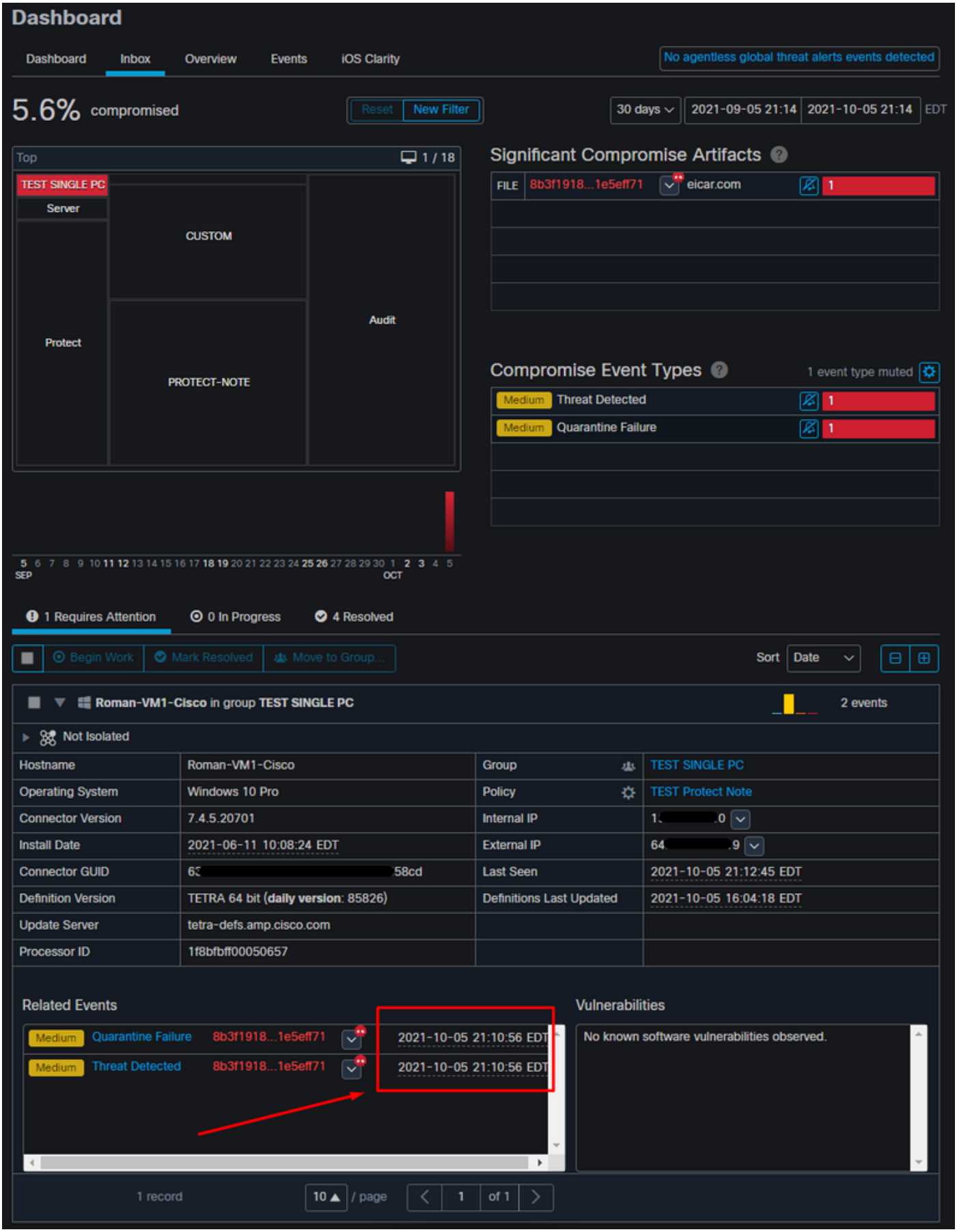
Depois que o botão Marcar resolvido for selecionado e como apenas um endpoint foi comprometido no painel do Secure Endpoint é semelhante a este. E neste ponto, um novo evento comprometido na máquina de teste foi acionado.



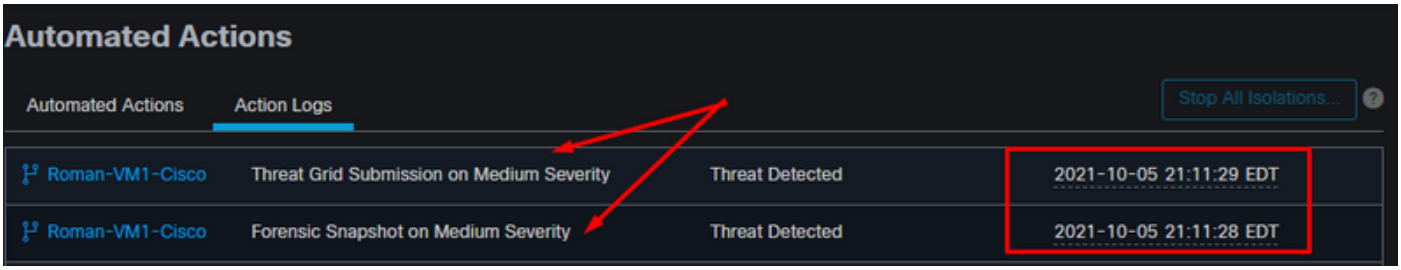
O próximo exemplo aciona um evento com um script personalizado que cria e exclui um arquivo mal-intencionado.



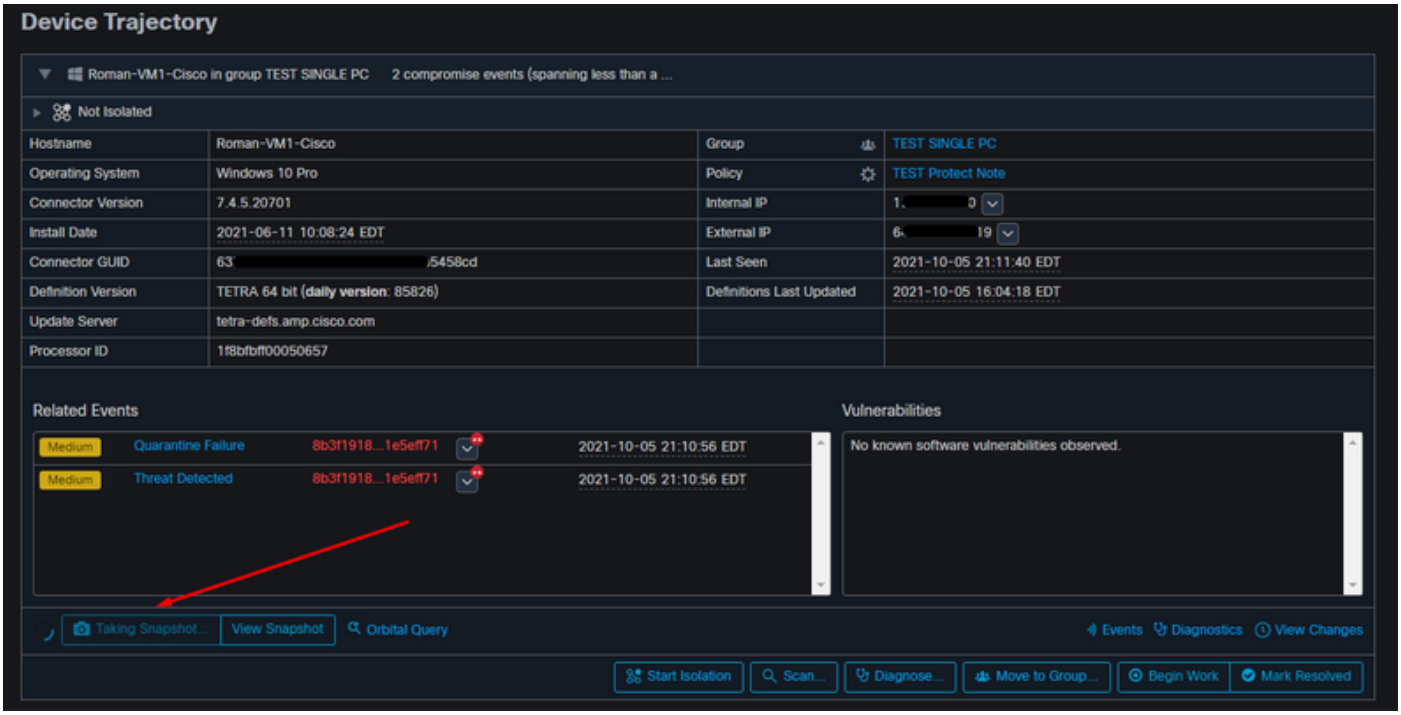
O console do Endpoint seguro novamente está comprometido, como mostrado na imagem



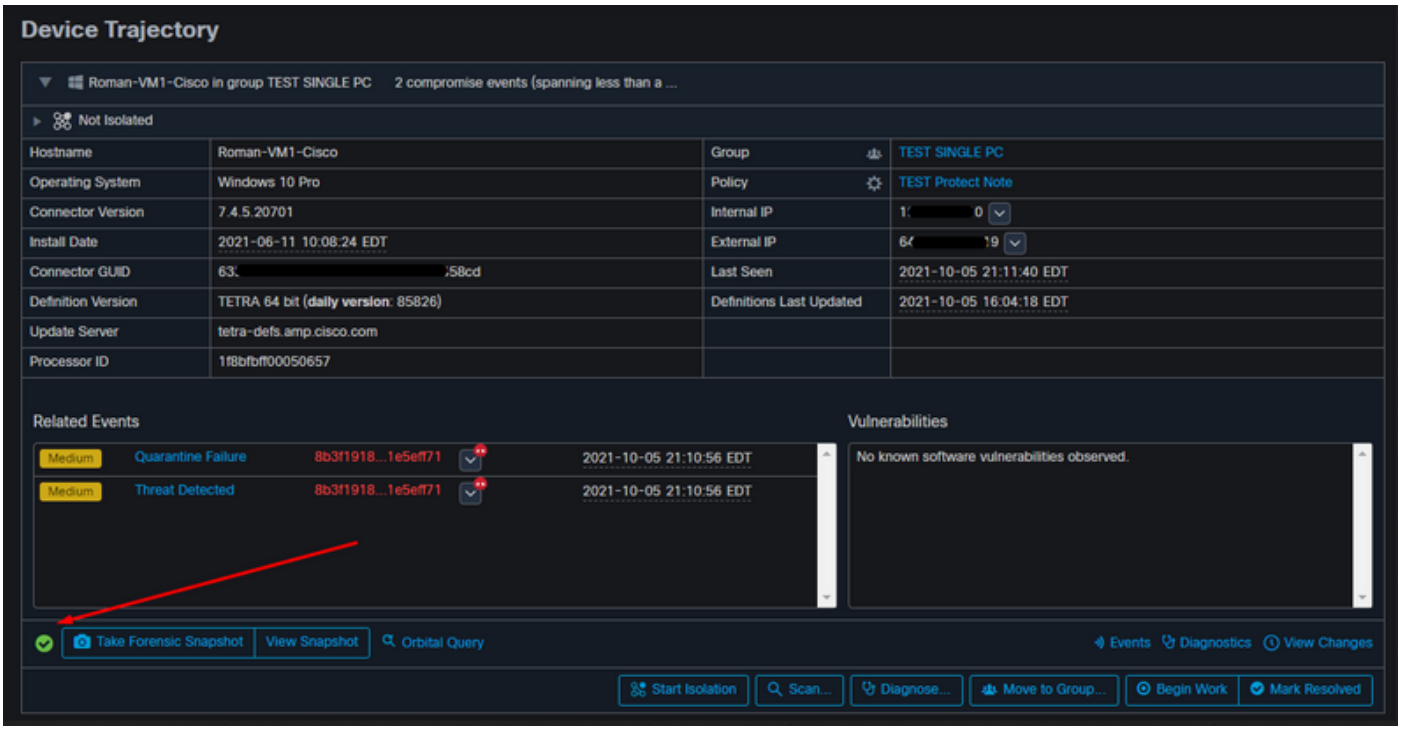
Aqui estão novos eventos em Ações automatizadas, como mostrado na imagem.



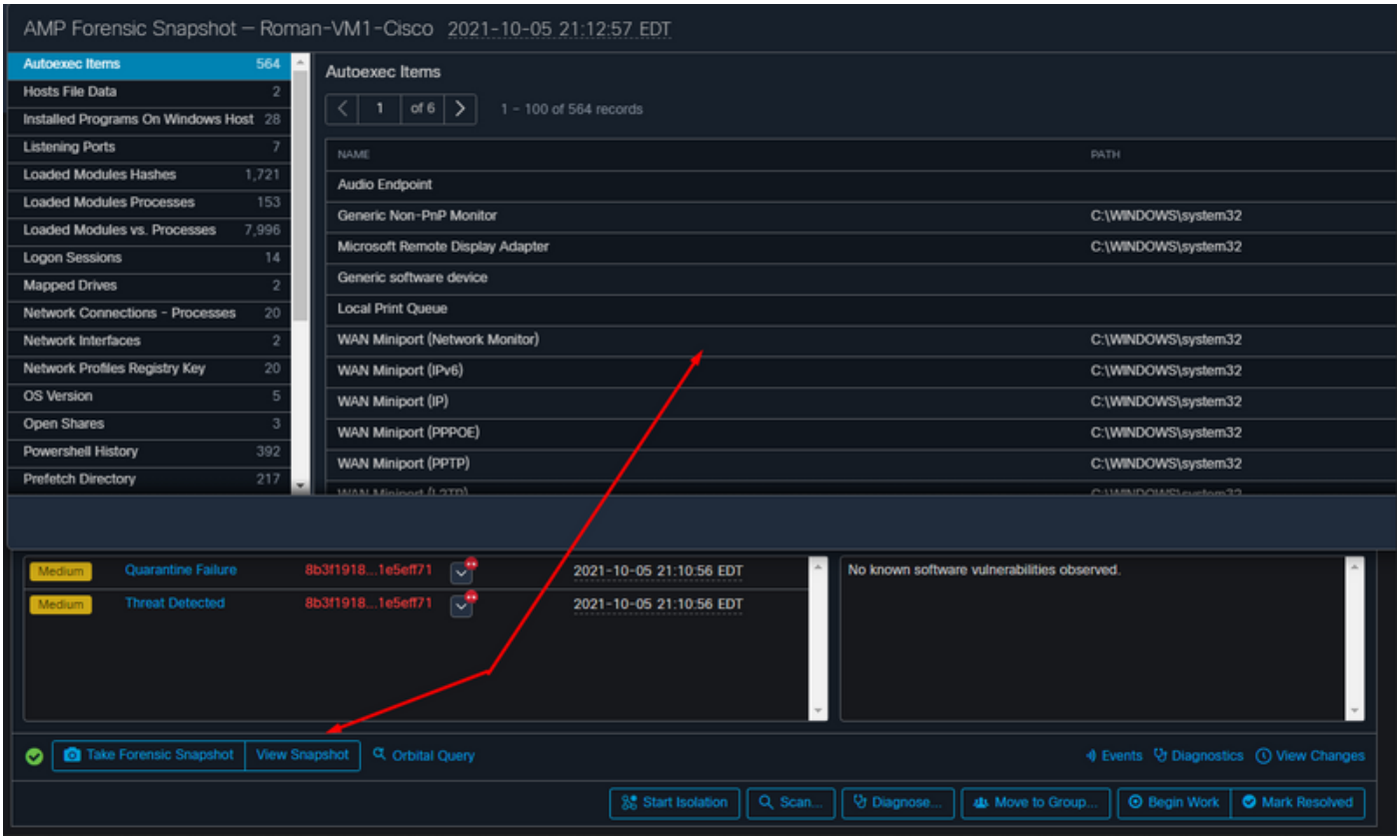
Quando o nome de host em Ações automatizadas é selecionado, ele redireciona para a trajetória do dispositivo, onde você pode observar o snapshot que está sendo criado quando você expande a guia Computador, como mostrado na imagem.



E o instantâneo mais recente é criado, como mostrado na imagem.



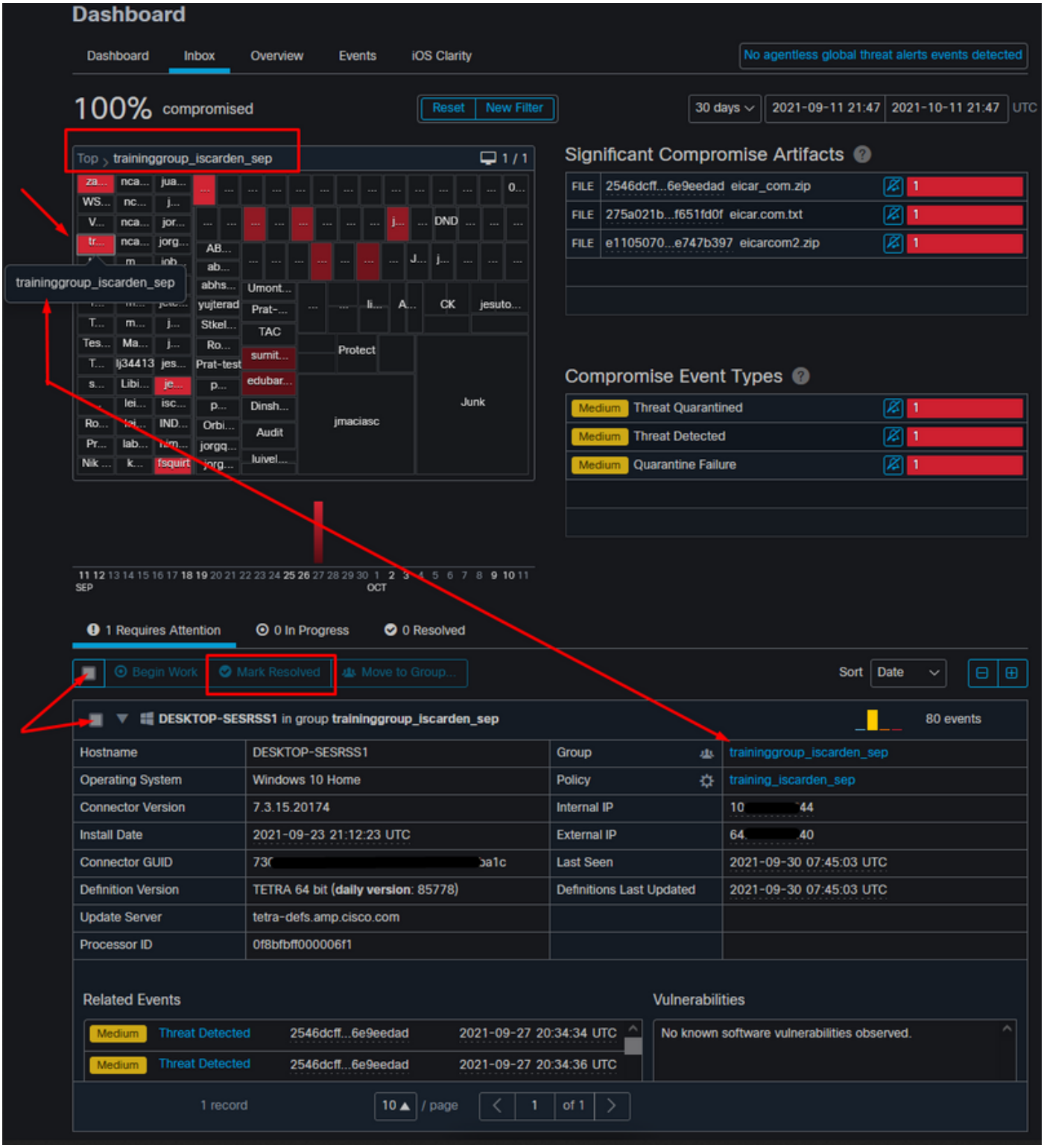
E agora você pode ver os dados exibidos.



Dica

Em ambientes muito grandes com milhares de endpoints e centenas de comprometimentos, você pode se deparar com situações em que a navegação para o endpoint individual pode ser um desafio. Atualmente, a única solução disponível é usar o mapa de calor e depois detalhar para um grupo específico em que seu endpoint de comprometimento é como neste exemplo abaixo.

Quando o grupo for selecionado no mapa de calor, navegue até o grupo no qual o evento foi comprometido. Como há apenas um endpoint nesse grupo, observe os 100% comprometidos que agora se baseiam no grupo específico em que estamos. Em outras palavras, se tivermos dois endpoints nesse grupo, um limpo e o outro comprometido mostrarão 50% de comprometimento.


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