Geautomatiseerde acties - Forensische Snapshot

Inhoud

Inleiding

Dit document beschrijft de functionaliteit voor geautomatiseerde actie in Secure Endpoint is gekoppeld aan het concept Compromiscue. Begrijp de levenscyclus en het beheer van compromissen zijn essentieel om de functionaliteit van geautomatiseerde acties te begrijpen. Dit artikel beantwoordt vragen over de terminologie en de functionaliteit van deze concepten.

FAQ

Wat is een gecompromitteerde machine?

Een gecompromitteerde machine is een eindpunt dat een actief compromis verbonden heeft. Een gecompromitteerde machine kan per ontwerp slechts één compromis tegelijk actief hebben.

Wat is een compromis?

Een compromis is een verzameling van een of meer detecties op een machine. De meeste detectiegebeurtenissen (bedreigingsdetectie, indicaties voor compromis, enz.) kunnen een compromis opleveren of sluiten. Er zijn echter paren van gebeurtenissen die wellicht geen nieuw compromis zullen opleveren. Wanneer er bijvoorbeeld een 'Threat Detected'-gebeurtenis plaatsvindt, maar kort nadat deze een bijbehorende Threat Quarantated-gebeurtenis heeft, veroorzaakt dit geen nieuw compromis. Logisch gezien is dit omdat Secure Endpoint met het mogelijke compromis is omgesprongen (we quarantaine de dreiging).

Wat gebeurt er als er nieuwe detecties optreden op een gecompromitteerde machine?

Het/de detectieevenement(en) wordt/worden toegevoegd aan het bestaande compromis. Er wordt geen nieuw compromis tot stand gebracht.

Waar kan ik compromissen zien en beheren?

Compromissen worden beheerd in het tabblad Inbox van de Secure Endpoint console (https://console.amp.cisco.com/compromises voor de Noord-Amerikaanse cloud). Een gecompromitteerde machine staat onder het gedeelte **Attire** Attire **Attentie** en kan worden gewist uit het compromis door op **Mark Resolved** te drukken. Bovendien worden compromissen automatisch na een maand gewist.

Hoe wordt een geautomatiseerde actie* geactiveerd?

Geautomatiseerde acties worden geactiveerd op een compromis dat wil zeggen wanneer een niet-gecompromitteerde machine een gecompromitteerde machine wordt. Als een al gecompromitteerde machine een nieuwe detectie tegenkomt, wordt deze detectie toegevoegd aan het compromis, maar aangezien dit geen nieuw compromis is, veroorzaakt het geen geautomatiseerde actie.

Hoe kan ik een geautomatiseerde actie opnieuw activeren?

Het compromis moet worden "gesneden" voordat wordt geprobeerd een geautomatiseerde actie opnieuw op gang te brengen. Houd in gedachten dat een bedreigde + bedreigde Garandeerde gebeurtenis niet voldoende is om een nieuw compromisevent op te zetten (en dus niet genoeg is om een nieuwe geautomatiseerde actie te starten).

*Uitzondering: De geautomatiseerde actie "Bestand indienen bij ThreatGrid" is niet aangesloten op compromissen, en wordt per detectie uitgevoerd

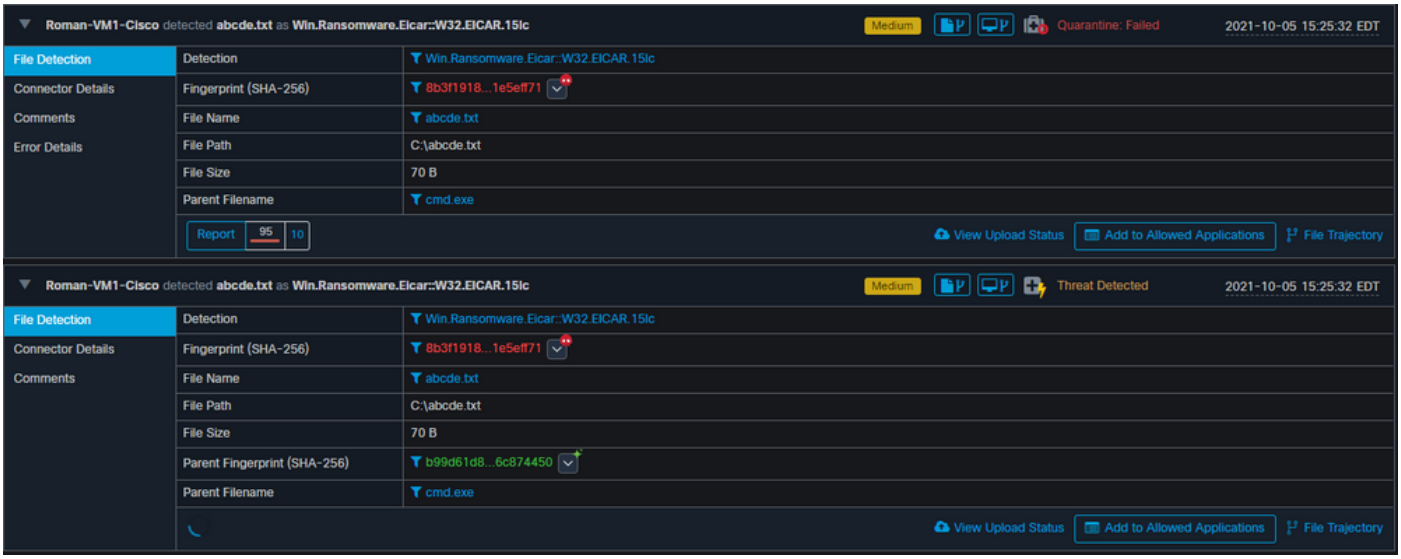
Gebruikte case - Lab Recreate

#1: Zoals we in het FAQ-gedeelte hebben aangegeven. Forensische momentopnamen worden alleen genomen in het geval van "compromis". Met andere woorden, als we proberen om een kwaadaardig bestand van een TEST-site te downloaden en te downloaden en het bestand wordt gesignaleerd bij download en quarantaine, dan wordt dat niet als een compromis beschouwd en wordt de actie niet geactiveerd.

> **Opmerking:** DFC Detection, Quarantine Fail, en vrijwel alles wat door de logica in de categorie van compromisgebeurtenissen valt, zou Forensisch Snapshot moeten creëren.

#2: U kunt alleen Forensische Snapshot genereren op een uniek gecompromitteerd evenement als het geen snapshot genereert tenzij u de gecompromitteerde machine in uw inbox oplost. Als u de gecompromitteerde gebeurtenis niet oplost, genereert u geen andere momentopname.

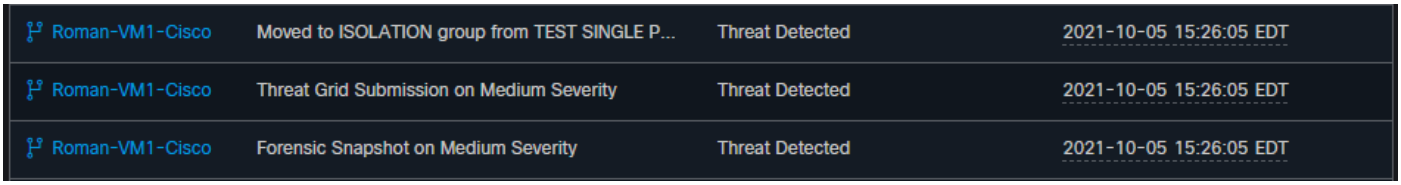
Voorbeeld: In dit lab genereert een script kwaadaardige activiteit en omdat het bestand gewist wordt zodra het gemaakt is en Secure Endpoint niet in staat is om het bestand in quarantaine te plaatsen voor een compromitterende categorie.



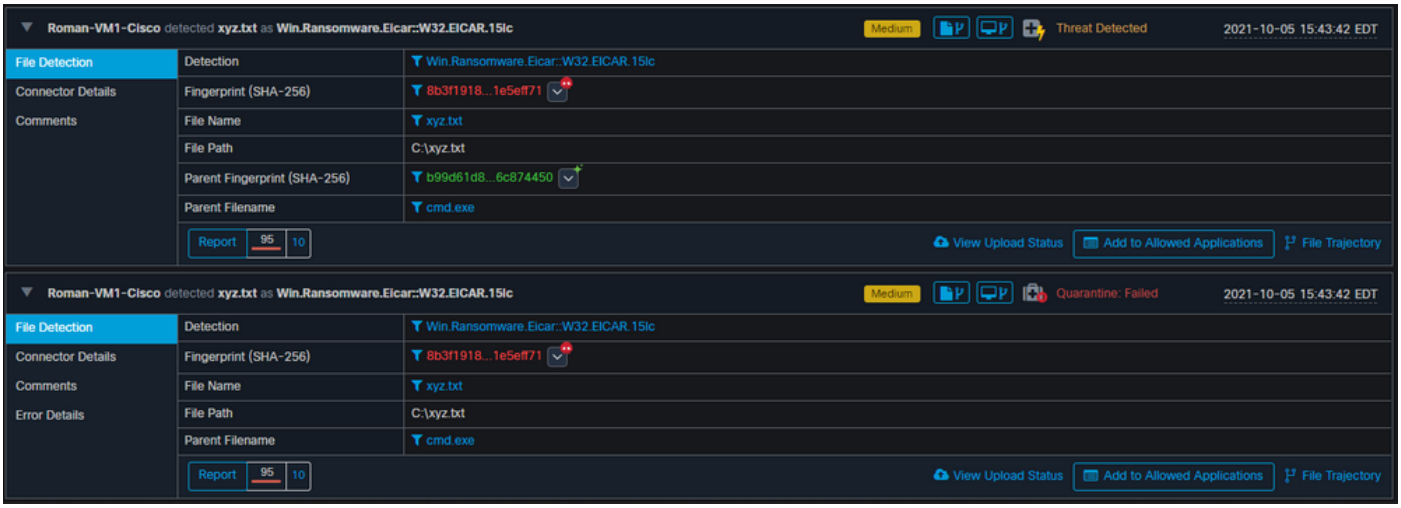
In deze test kan je onder geautomatiseerde handelingen kijken en 3 dingen die gebeurde gebaseerd op de instellingen.

- Snapshot werd gemaakt
- Indiening werd naar Threat Grid (TG) verzonden
- Het eindpunt werd verplaatst naar een afzonderlijke groep die ISOLATION werd gecreëerd en genoemd

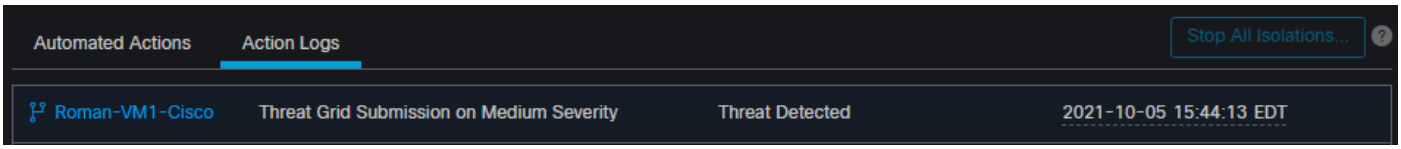
U kunt dit alles in deze uitvoer zien, zoals in de afbeelding wordt weergegeven.



Aangezien dit eindpunt gecompromitteerd is, de volgende test om de theorie met een soortgelijk kwaadaardig bestand maar met een andere naam aan te tonen, zoals in de afbeelding getoond wordt.

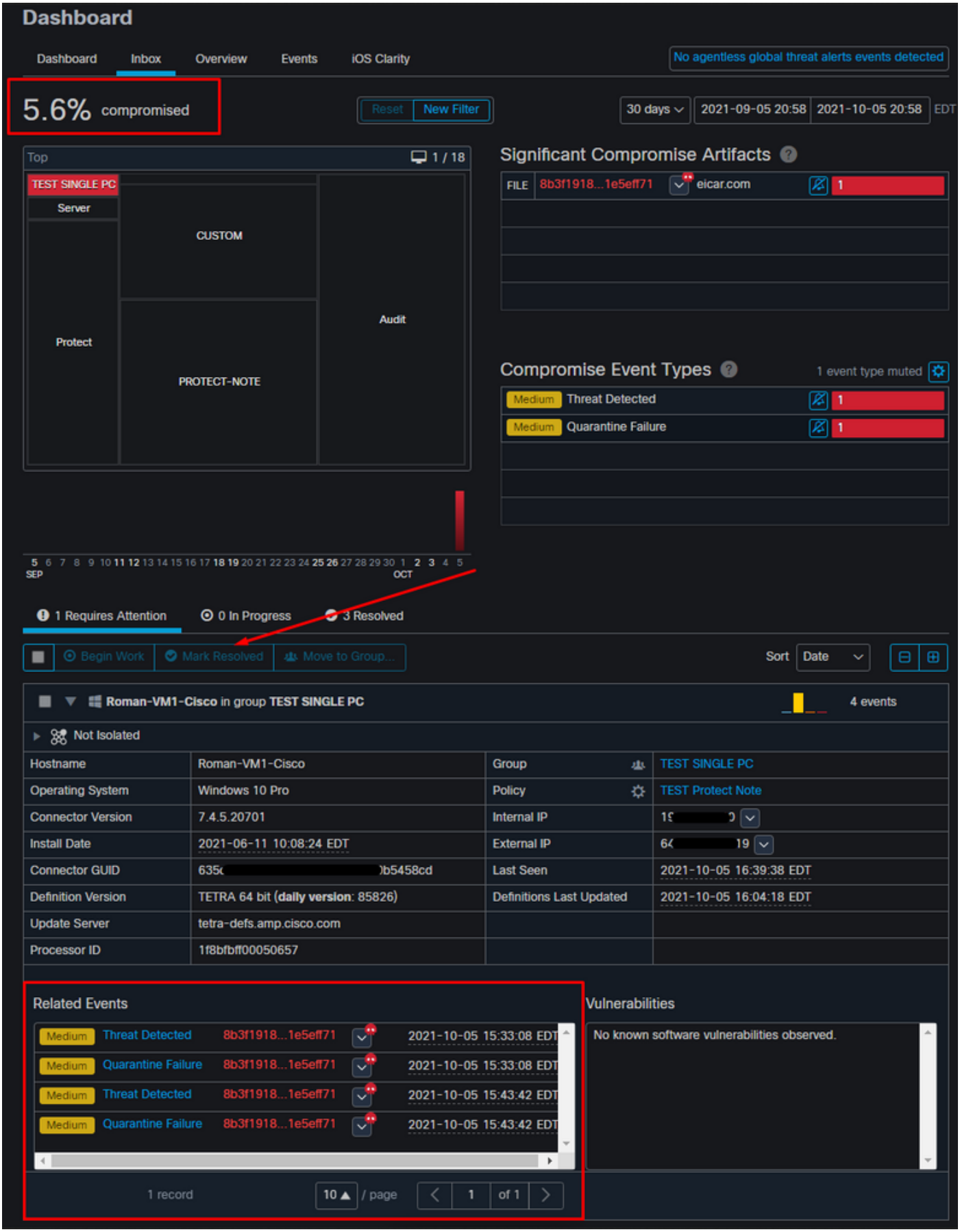


Aangezien dit compromis echter niet is opgelost, kunt u alleen een TG-voorstel opstellen. Er werden geen andere voorvallen geregistreerd en de isolatie werd ook uitgeschakeld voor deze 2e test.

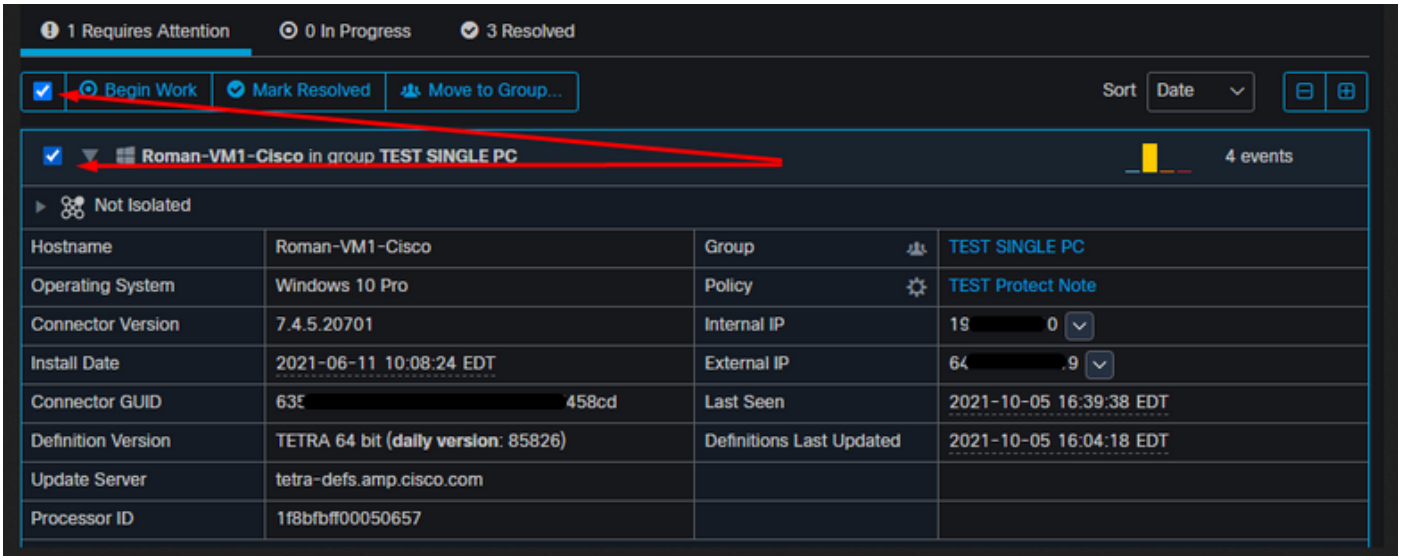


Opmerking: Let op het tijdstip waarop de dreiging is gedetecteerd en automatische actie triggers instelt.

De gebeurtenis kan niet opnieuw geactiveerd worden, tenzij het gecompromitteerde eindpunt is opgelost. In dit geval ziet het dashboard er zo uit. Let op het percentage en de knop Mark Resolved samen met de gecompromitteerde gebeurtenissen. Ongeacht het aantal gebeurtenissen dat wordt geactiveerd, kunt u slechts één momentopname maken en het grote procentuele aantal is nooit gewijzigd. Dat getal vertegenwoordigt compromissen binnen uw organisatie en is gebaseerd op de totale hoeveelheid eindpunten in uw organisatie. Het verandert alleen met een andere gecompromitteerde machine. In dit voorbeeld is het aantal hoog door slechts 16 apparaten in het lab. Houd er ook rekening mee dat compromisgebeurtenissen automatisch worden gewist zodra ze 31 dagen oud zijn.

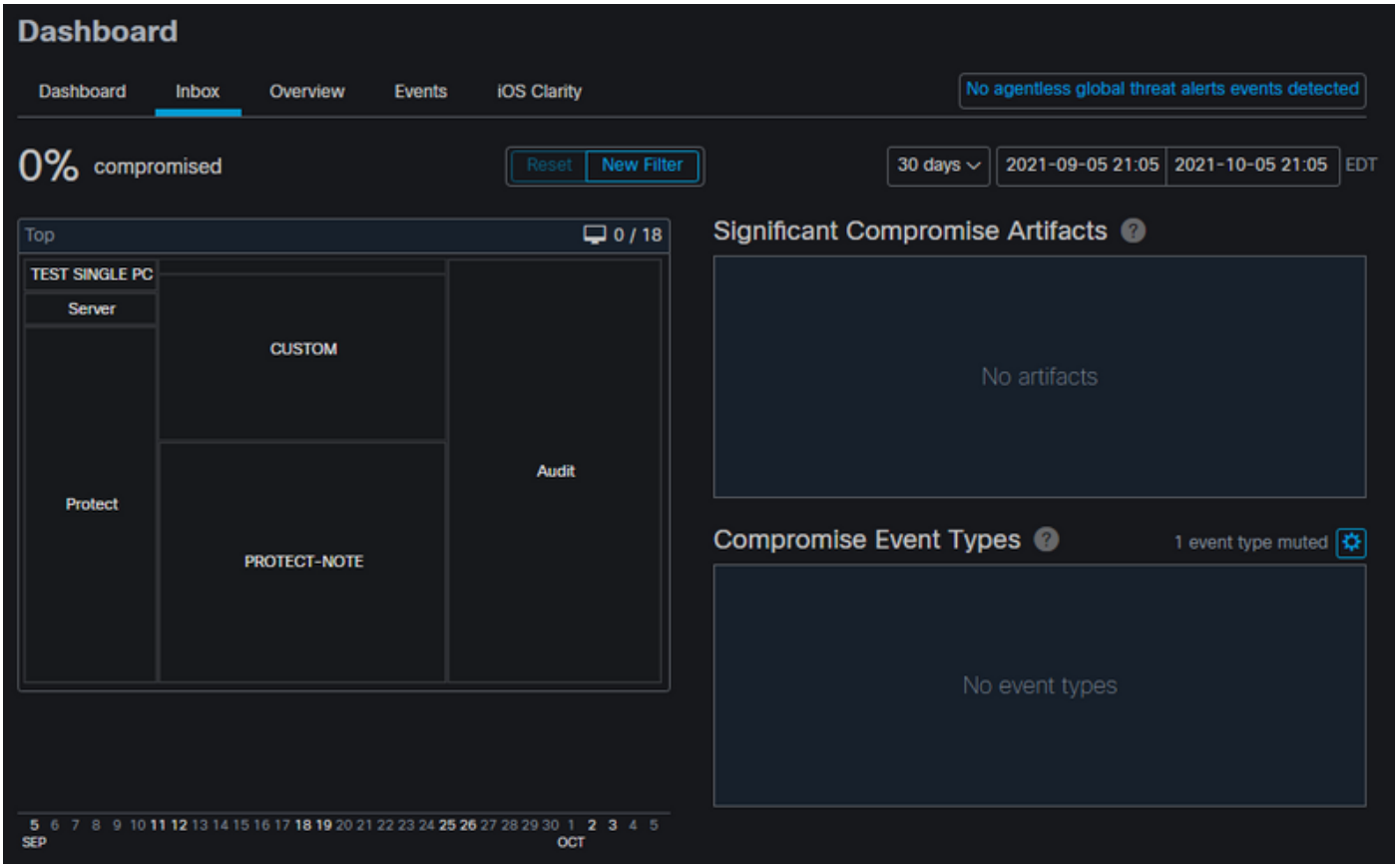


De volgende stap is het creëren van een andere gebeurtenis en het creëren van een forensische momentopname. De eerste stap is om dit compromis op te lossen, klikt u op de knop **Mark Resolved**. U kunt dit per eindpunt doen of u kunt alles in uw organisatie selecteren.

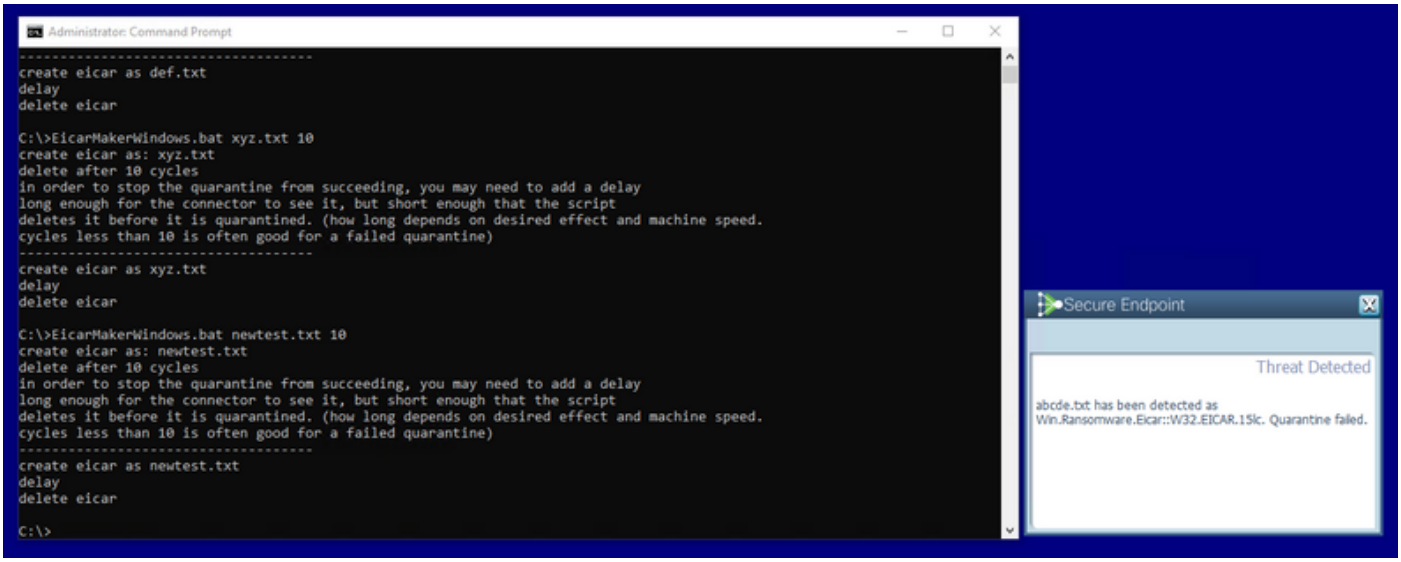


Opmerking: Als u alle compromissen selecteert, worden ze teruggezet op 0%.

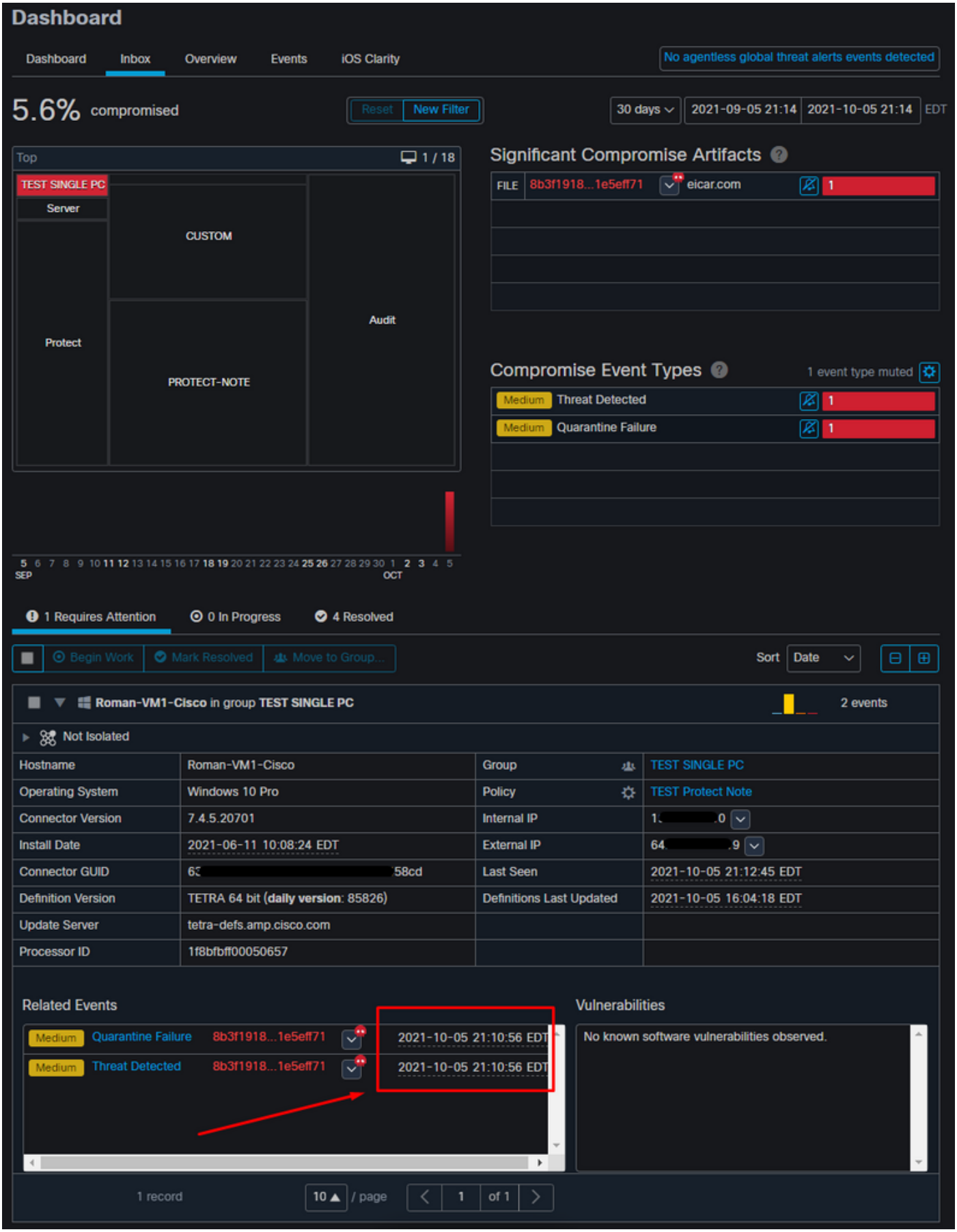
Zodra de knop Mark Resolved is geselecteerd en omdat slechts één eindpunt werd gecompromitteerd op het Secure Endpoint dashboard lijkt dit. Op dat moment werd een nieuw gecompromitteerd evenement op de testmachine geactiveerd.



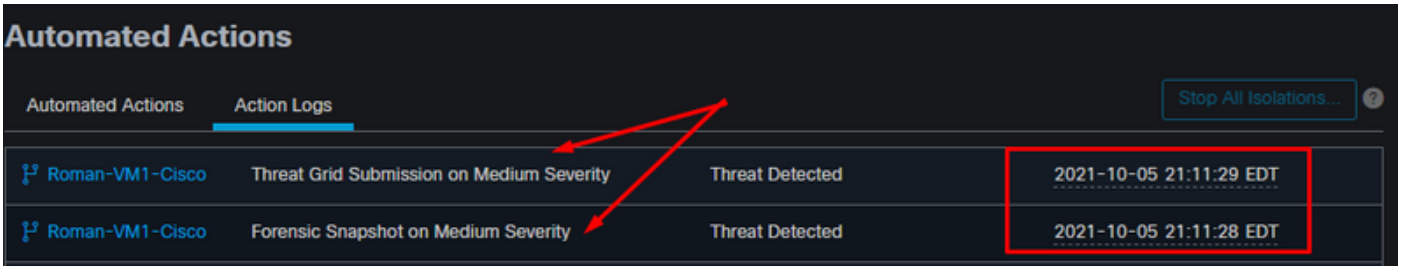
Het volgende voorbeeld veroorzaakt een gebeurtenis met een douane script dat een kwaadaardig bestand maakt en verwijdert.



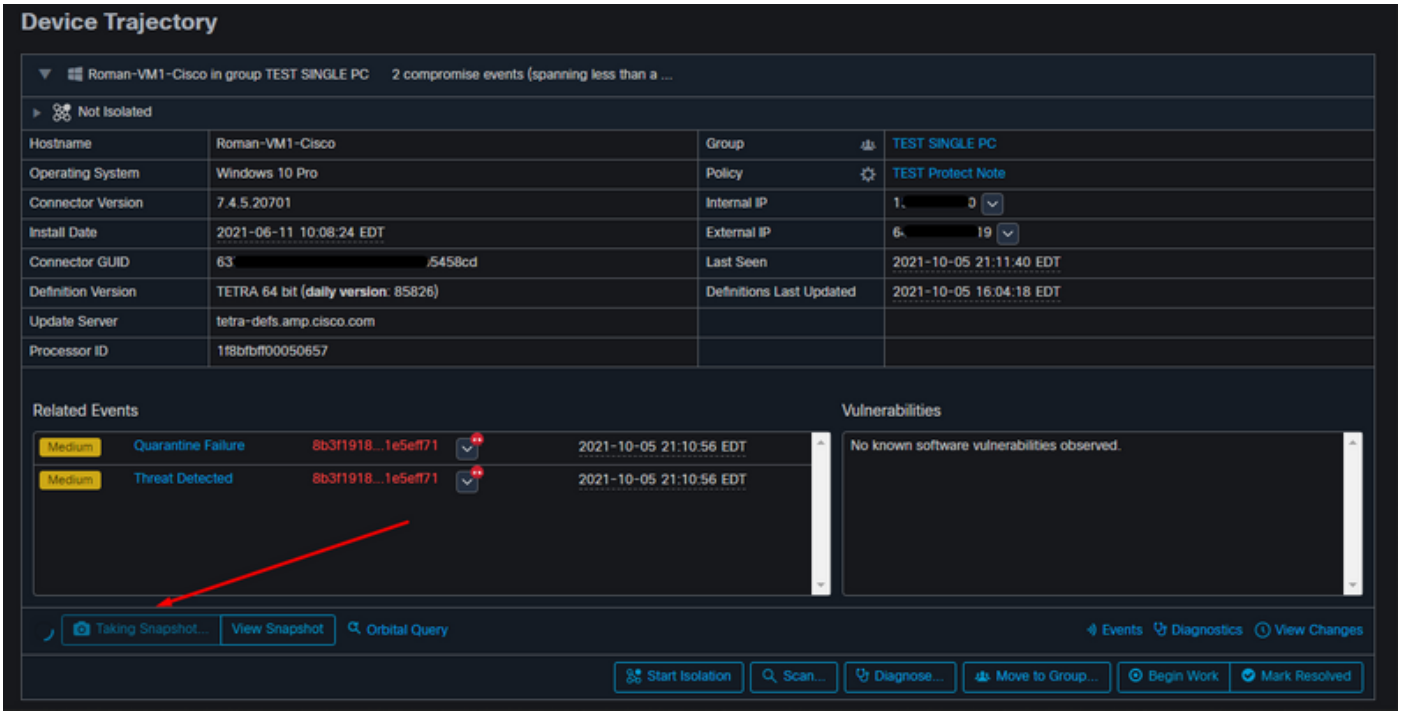
Secure Endpoint console opnieuw gecompromitteerd, zoals in de afbeelding getoond



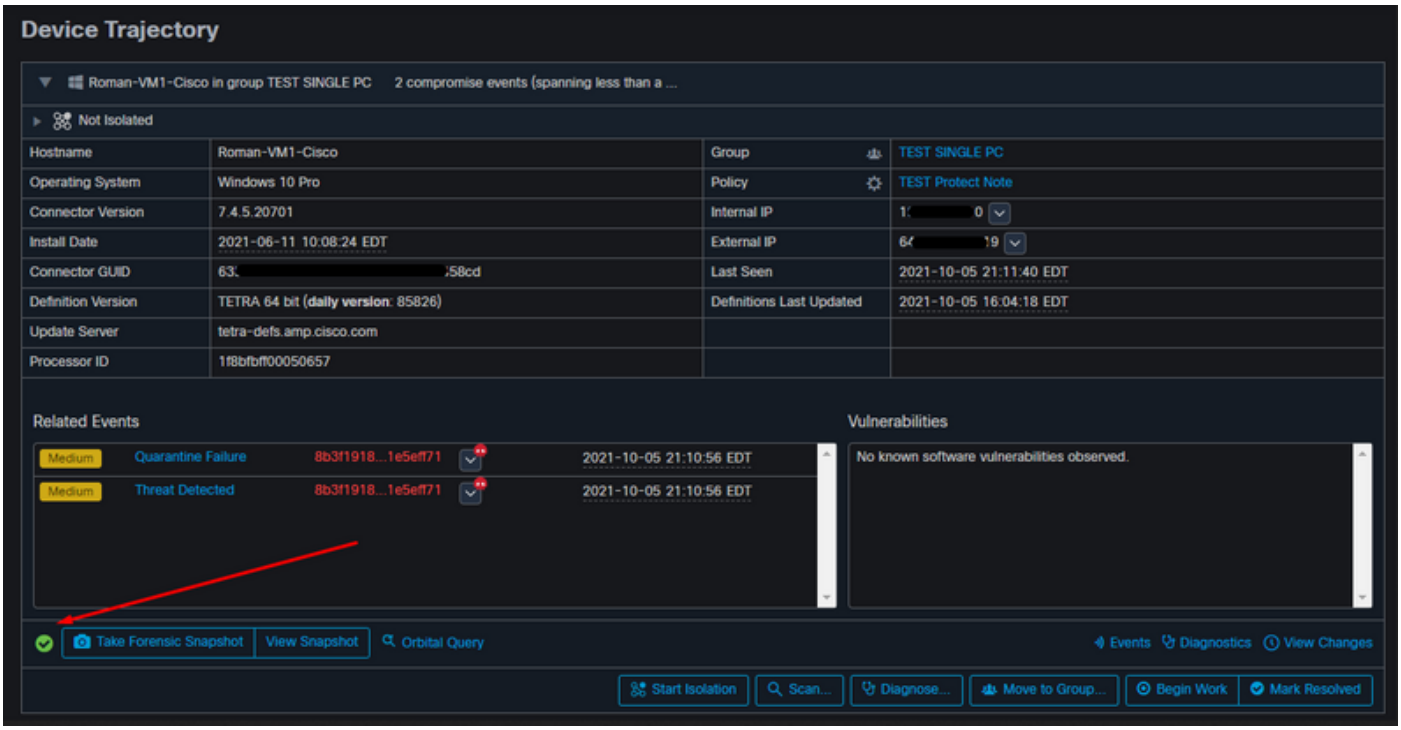
Hier zijn nieuwe gebeurtenissen onder Geautomatiseerde handelingen, zoals in de afbeelding weergegeven.



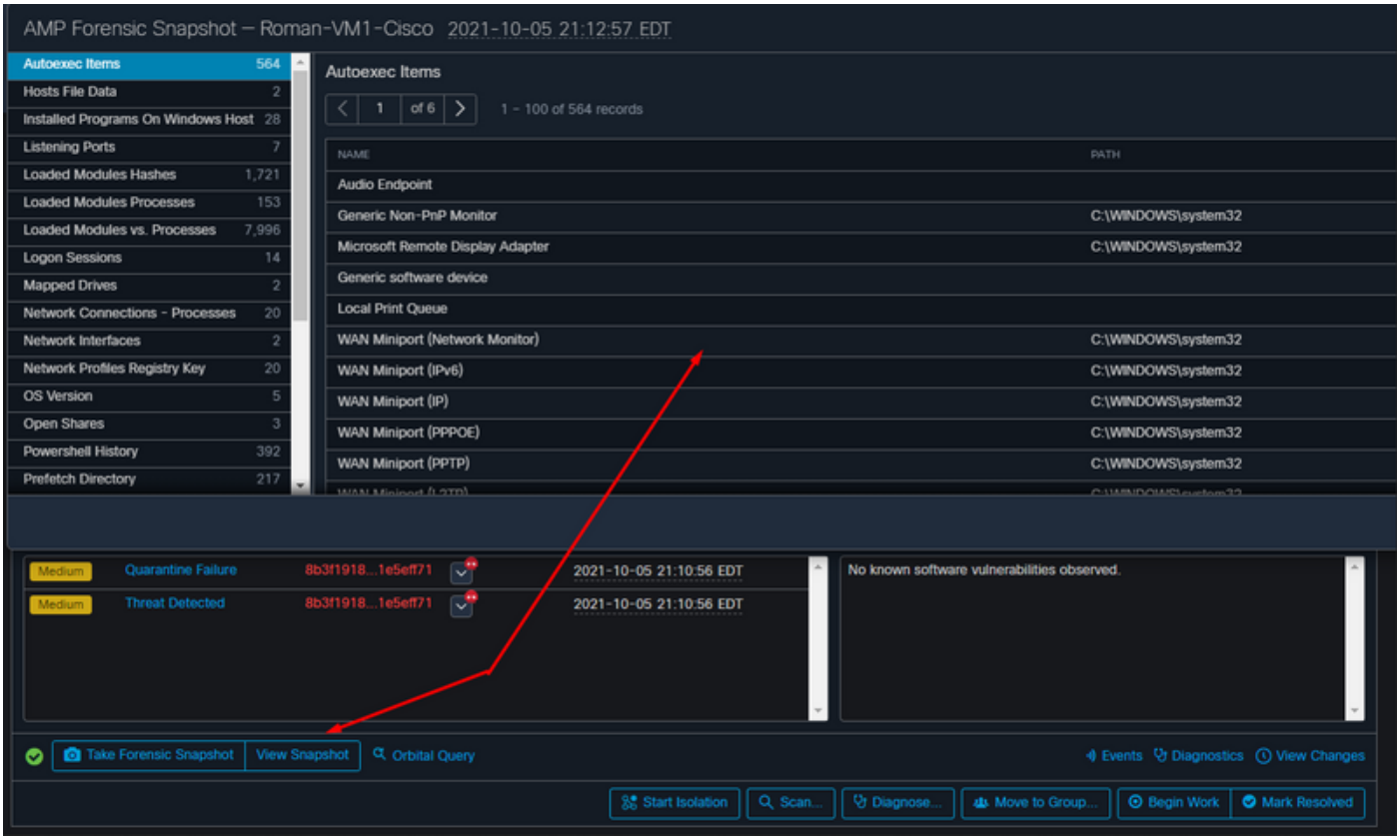
Wanneer de hostname onder Geautomatiseerde handelingen is geselecteerd, wordt deze omgeleid naar Apparaattraject waar u de snapshot kunt observeren die wordt gemaakt als u het computertabblad hebt uitvouwen, zoals in de afbeelding wordt getoond.



En een minuut later momentopname wordt gecreëerd, zoals in de afbeelding wordt getoond.



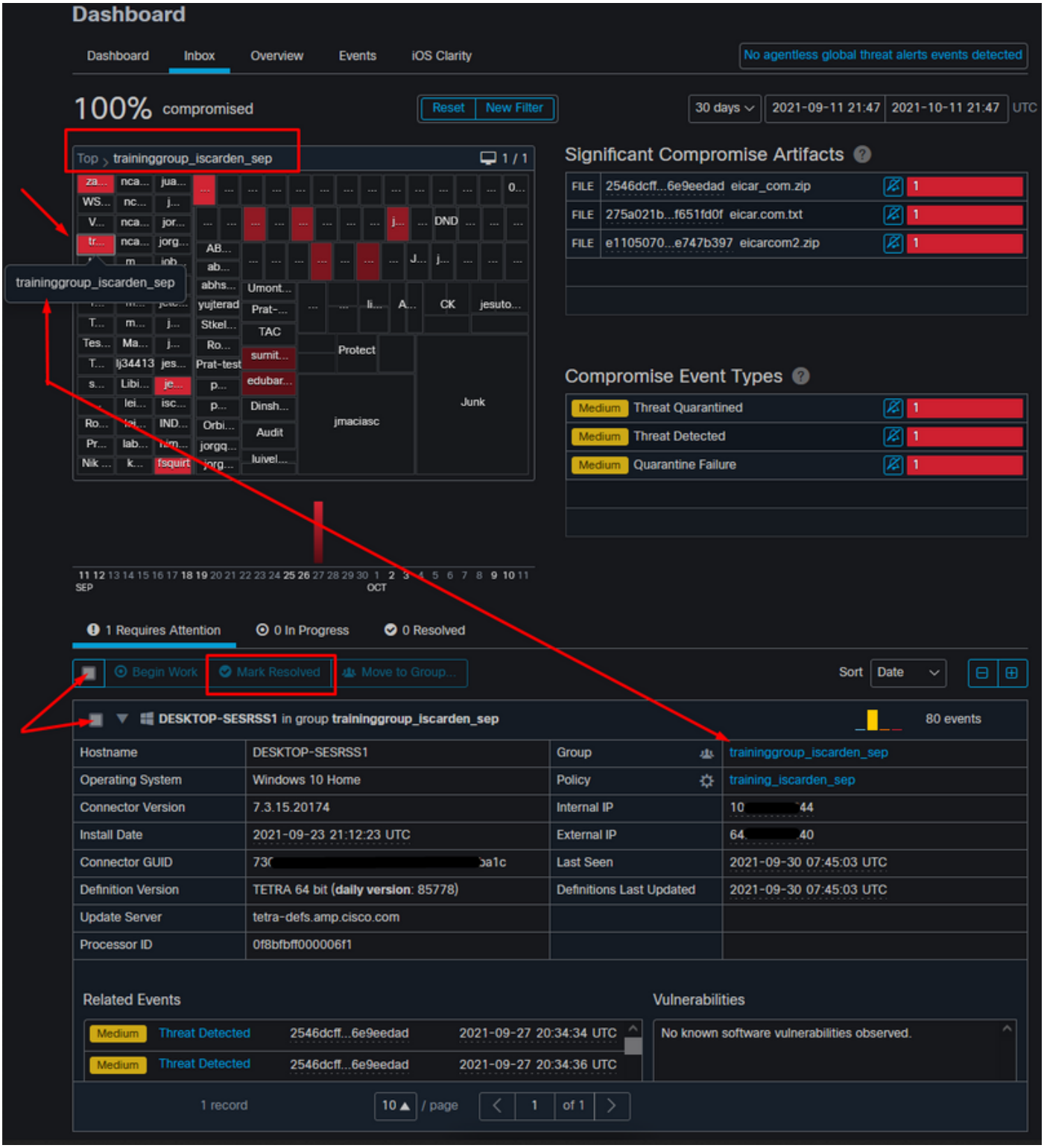
Nu kun je de weergegeven gegevens bekijken.



Tip

In zeer grote omgevingen met duizenden eindpunten en honderden compromissen, kan je in situaties lopen waar de navigatie naar het individuele eindpunt een uitdaging zou kunnen zijn. Op dit moment is de enige beschikbare oplossing: gebruik de hittekaart en boor vervolgens naar een specifieke groep waar uw compromiseindpunt is zoals in dit voorbeeld hieronder.

Zodra de groep geselecteerd is in de hittekaart navigeer naar die groep waarin we de gebeurtenis gecompromitteerd hebben. Aangezien er slechts één eindpunt in die groep is, merk ik op dat er 100% compromissen zijn gesloten, die nu gebaseerd zijn op de specifieke groep waarin wij ons bevinden. Met andere woorden, als we twee eindpunten in deze groep hebben, één schoon en het andere compromis geeft 50 procent compromis.


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