Actions automatisées - Instantané médico-légal

Contenu

Introduction

Ce document décrit la fonctionnalité d'action automatisée dans Secure Endpoint est liée au concept de compromission. Comprendre le cycle de vie et la gestion des compromis est essentiel pour comprendre la fonctionnalité des actions automatisées. Cet article répond à des questions sur la terminologie et la fonctionnalité de ces concepts.

Forum aux questions

Qu'est-ce qu'une machine compromise ?

Une machine compromise est un terminal associé à un compromis actif. Une machine compromise ne peut, par conception, avoir qu'un seul compromis actif à la fois.

Qu'est-ce qu'un compromis ?

Un compromis est un ensemble de détections sur une machine. La plupart des événements de détection (menaces détectées, indicateurs de compromission, etc.) peuvent générer ou devenir associés à un compromis. Cependant, il existe des paires d'événements qui peuvent ne pas déclencher un nouveau compromis. Par exemple, lorsqu'un événement Threat Detected se produit, mais peu après qu'il ait un événement Threat Quarantined associé, cela ne déclenche pas de nouveau compromis. Logiquement, c'est parce que Secure Endpoint a géré le compromis potentiel (nous avons mis la menace en quarantaine).

Que se passe-t-il lorsque de nouvelles détections se produisent sur une machine compromise ?

Les événements de détection sont ajoutés au compromis existant. Aucun nouveau compromis n'est créé.

Où puis-je voir et gérer les compromis ?

Les compromis sont gérés dans l'onglet Boîte de réception de la console Secure Endpoint (https://console.amp.cisco.com/compromises pour le cloud nord-américain). Une machine compromise est répertoriée dans la section **Exiger l'attention** et peut être effacée de son compromis en appuyant sur **Mark Resolved**. En outre, les compromis sont automatiquement éliminés au bout d'un mois.

Comment déclencher une action automatisée* ?

Les actions automatisées sont déclenchées après un compromis, c'est-à-dire lorsqu'une machine sans compromis devient une machine compromise. Si une machine déjà compromise rencontre une nouvelle détection, cette détection est ajoutée au compromis, mais comme il ne s'agit pas d'un nouveau compromis, elle ne déclenche pas d'action automatisée.

Comment puis-je relancer une action automatisée ?

Il est nécessaire de « supprimer » le compromis avant de tenter de relancer une action automatisée. N'oubliez pas qu'un événement Threat Detected + Threat Quarantined n'est pas suffisant pour générer un nouvel événement de compromission (et donc pas suffisant pour déclencher une nouvelle action automatisée).

*Exception : L'action automatisée « Envoyer le fichier à ThreatGrid » n'est pas liée aux compromis et s'exécute par détection

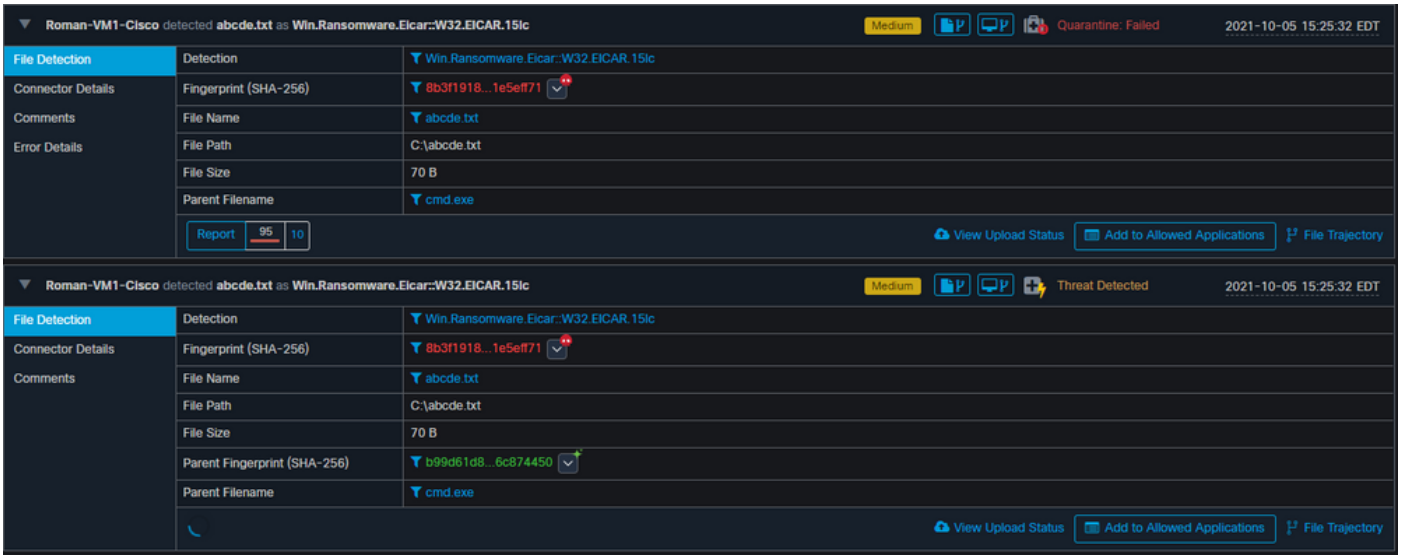
Cas d'utilisation - Récréation des travaux pratiques

N° 1 : Comme nous l'avons indiqué dans la section FAQ. Les clichés médico-légaux ne sont pris qu'en cas de ” de compromission “. En d'autres termes, si nous essayons d'accéder et de télécharger un fichier malveillant à partir d'un site TEST et que le fichier est marqué lors du téléchargement et de la mise en quarantaine, cela n'est pas considéré comme un compromis et ne déclenche pas l'action.

> **Note**: Détection DFC, échec de quarantaine, et à peu près tout ce qui, selon la logique, entre dans la catégorie des événements de compromission devrait créer un snapshot médico-légal.

N° 2 : Vous ne pouvez générer de cliché médico-légal qu'une seule fois sur un événement compromis unique, il ne génère pas de cliché à moins de résoudre l'ordinateur compromis dans votre boîte de réception. Si vous ne résolvez pas l'événement compromis, vous ne générez aucun autre instantané.

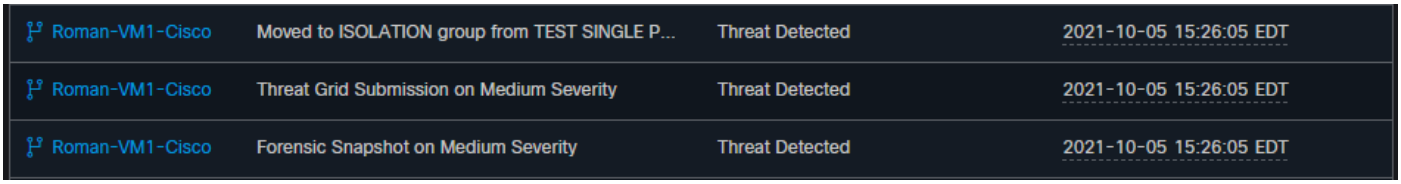
Exemple : Au cours de ces travaux pratiques, un script génère une activité malveillante et, parce que le fichier est supprimé dès sa création et que Secure Endpoint n'a pas pu mettre en quarantaine le fichier qu'il se trouve dans la catégorie compromis.



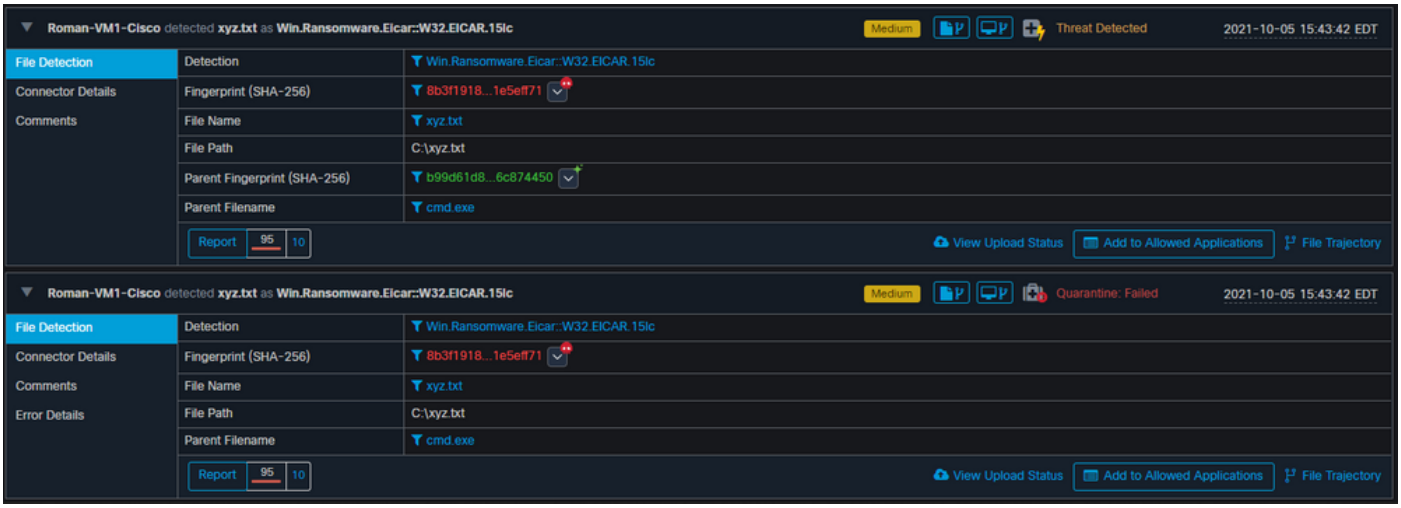
Dans ce test, vous pouvez regarder sous actions automatisées et 3 choses qui se sont produites en fonction des paramètres.

- Instantané créé
- L'envoi a été envoyé à Threat Grid (TG)
- Le point de terminaison a été déplacé vers un groupe distinct créé et appelé ISOLATION

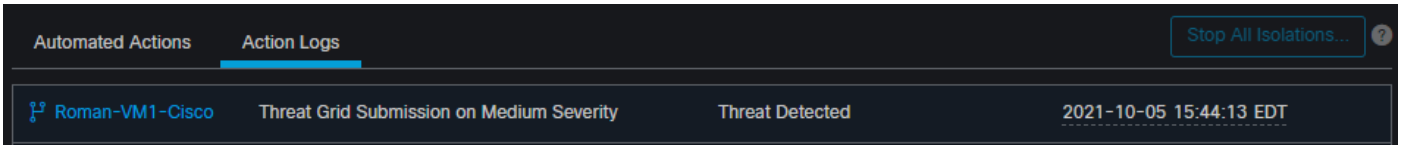
Vous pouvez voir tout cela dans cette sortie, comme le montre l'image.



Maintenant que ce point de terminaison est compromis, le prochain test pour prouver la théorie avec un fichier malveillant similaire mais avec un nom différent, comme illustré dans l'image.

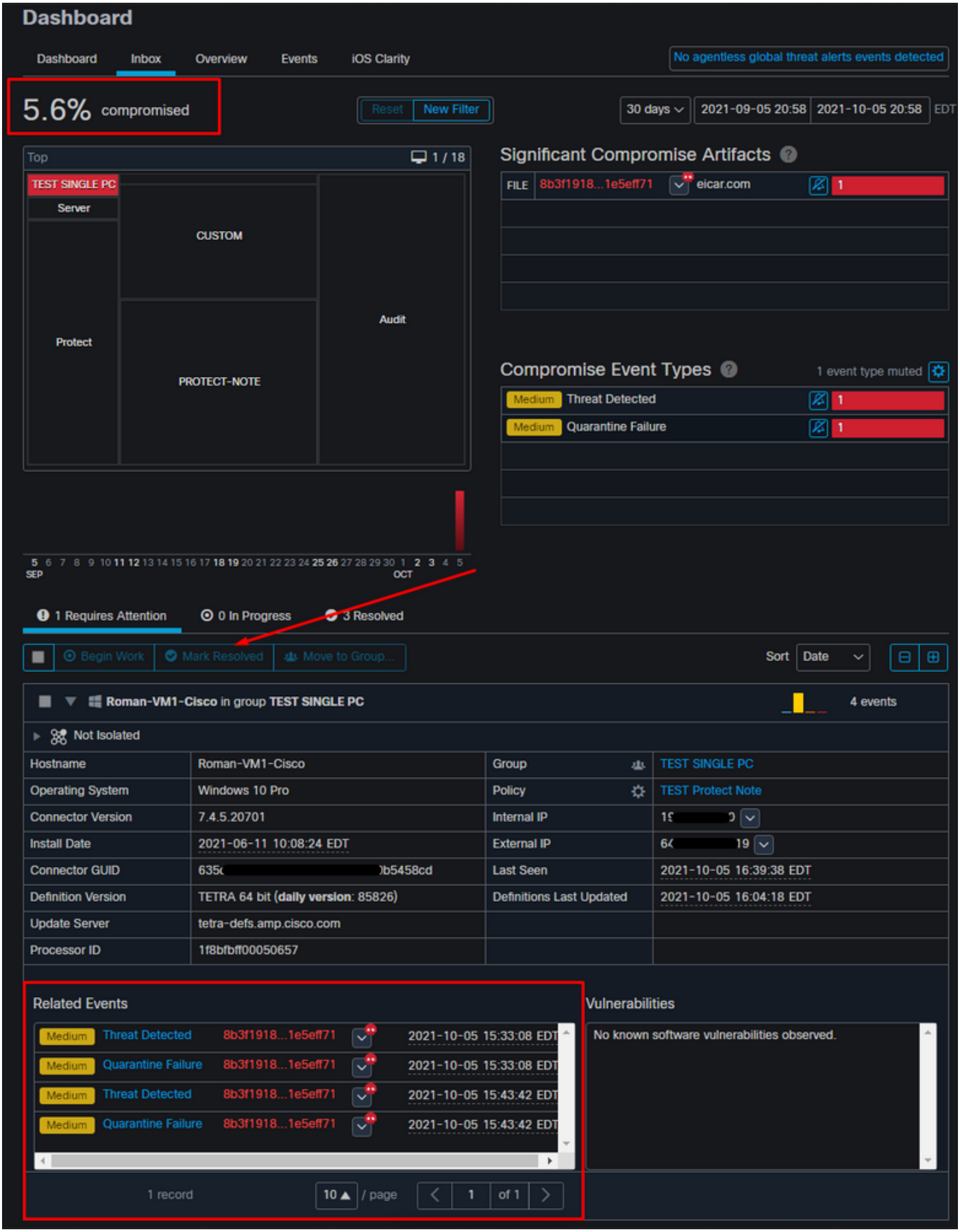


Cependant, comme ce compromis n'a pas été résolu, vous ne pouvez créer qu'une soumission TG. Aucun autre événement n'a été enregistré, aussi désactiver l'isolement avant ce 2ème test.

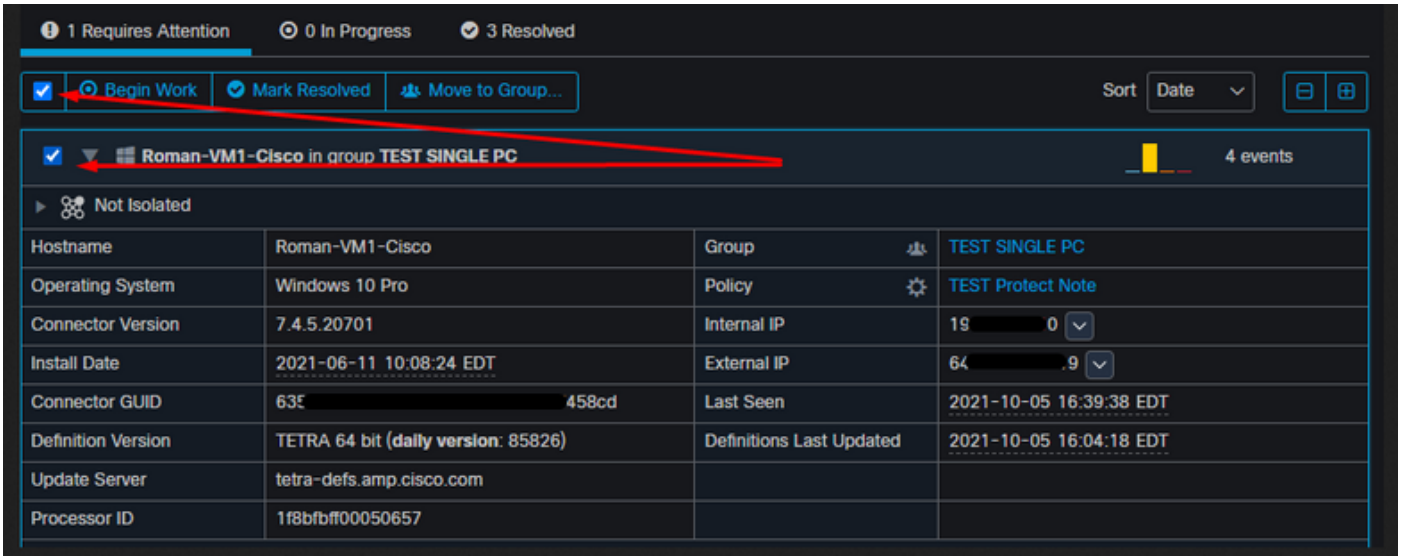


Note: Notez l'heure à laquelle la menace a été détectée et où les déclencheurs d'action automatisée ont été détectés.

L'événement ne peut pas se déclencher à moins que le point de terminaison compromis ne soit résolu. Dans ce cas, le tableau de bord ressemble à ceci. Notez le pourcentage et le bouton Marquer résolu avec les événements compromis. Quel que soit le nombre d'événements déclenchés, vous ne pouvez créer qu'un seul instantané et le grand pourcentage n'a jamais changé. Ce nombre représente un compromis au sein de votre organisation et il est basé sur le nombre total de terminaux dans votre organisation. Il ne change qu'avec une autre machine compromise. Dans cet exemple, le nombre est élevé en raison de 16 périphériques seulement dans les travaux pratiques. Notez également que les événements de compromission sont automatiquement effacés lorsqu'ils atteignent l'âge de 31 jours.

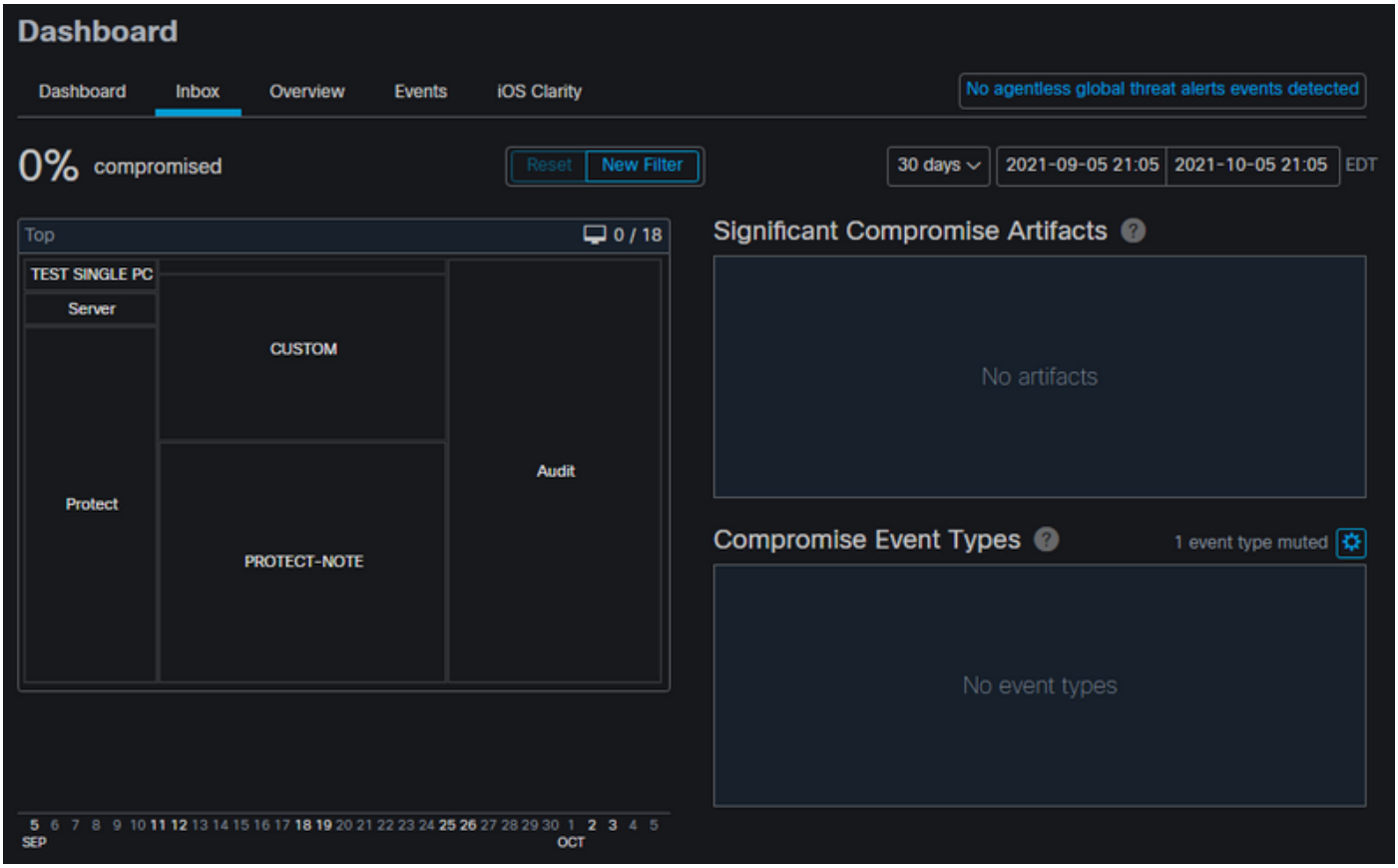


L'étape suivante consiste à créer un autre événement et à générer un cliché médico-légal. La première étape est de résoudre ce compromis, cliquez sur le bouton **Marquer résolu**. Vous pouvez le faire par point d'extrémité ou sélectionner tout dans votre organisation.

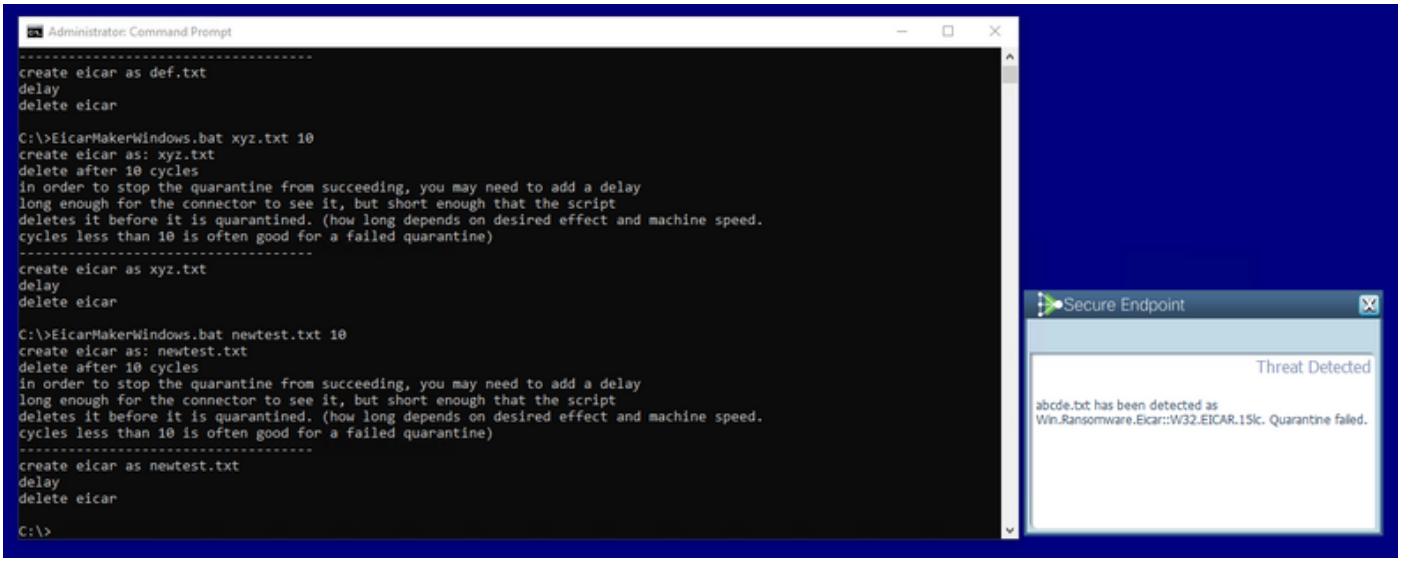


Remarque : si vous sélectionnez tous les compromis, ils sont réinitialisés à 0 %.

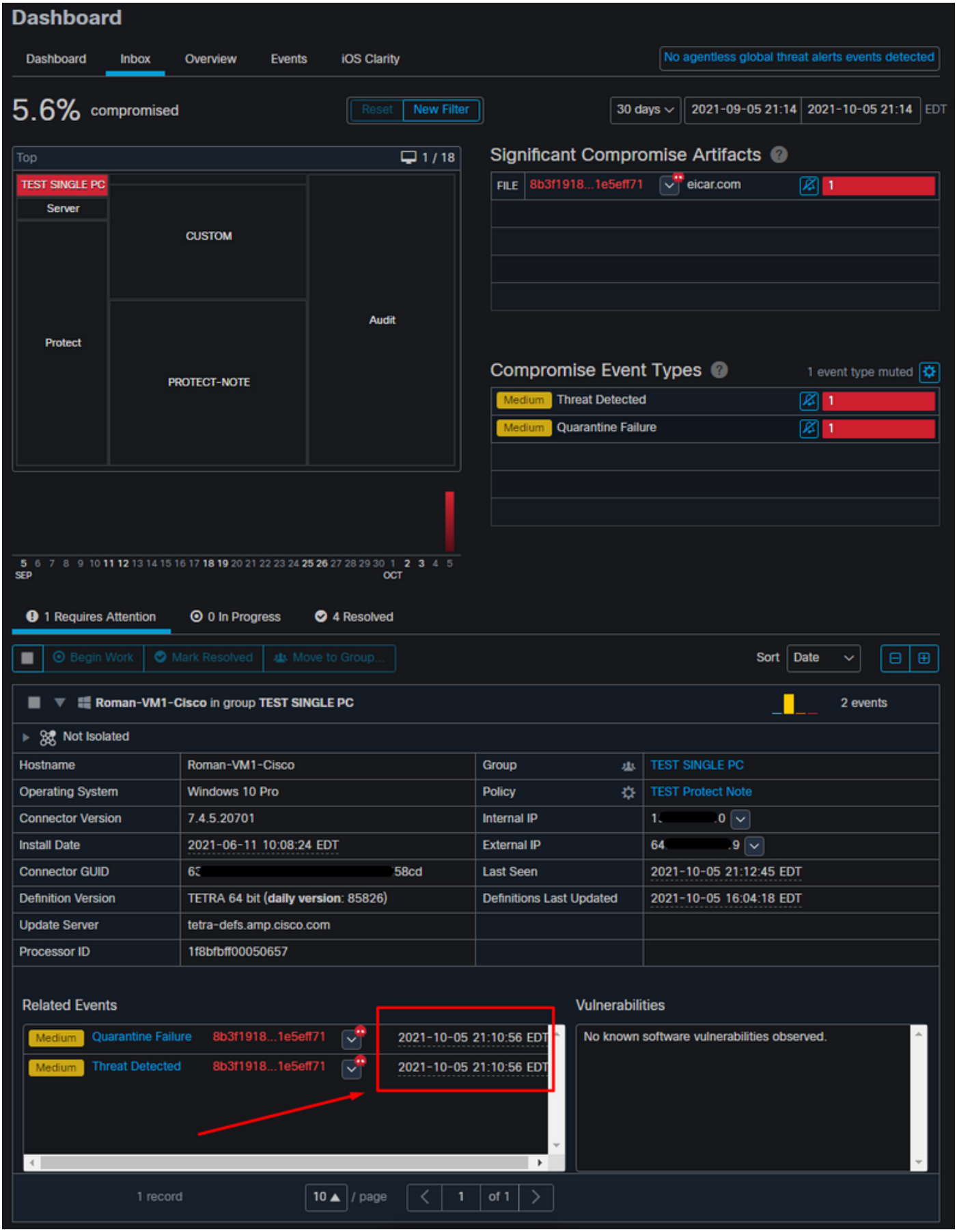
Une fois que le bouton Marquer résolu est sélectionné et qu'un seul point de terminaison a été compromis sur le tableau de bord de point de terminaison sécurisé ressemble à ceci. Et à ce stade, un nouvel événement compromis sur la machine à tester a été déclenché.



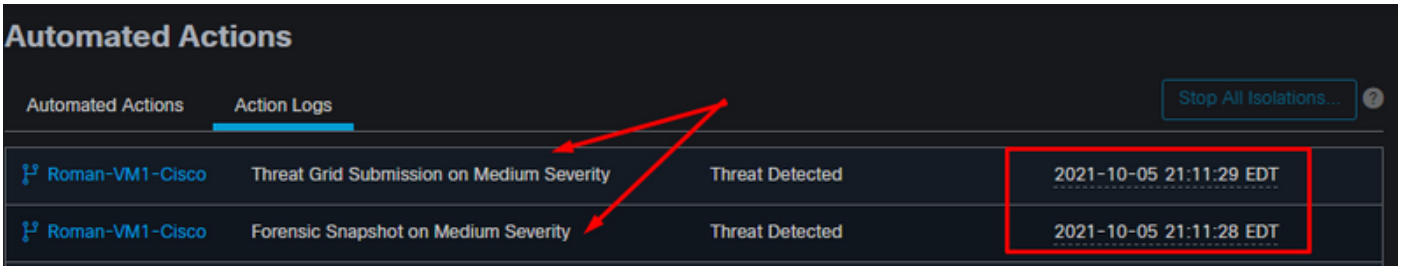
L'exemple suivant déclenche un événement avec un script personnalisé qui crée et supprime un fichier malveillant.



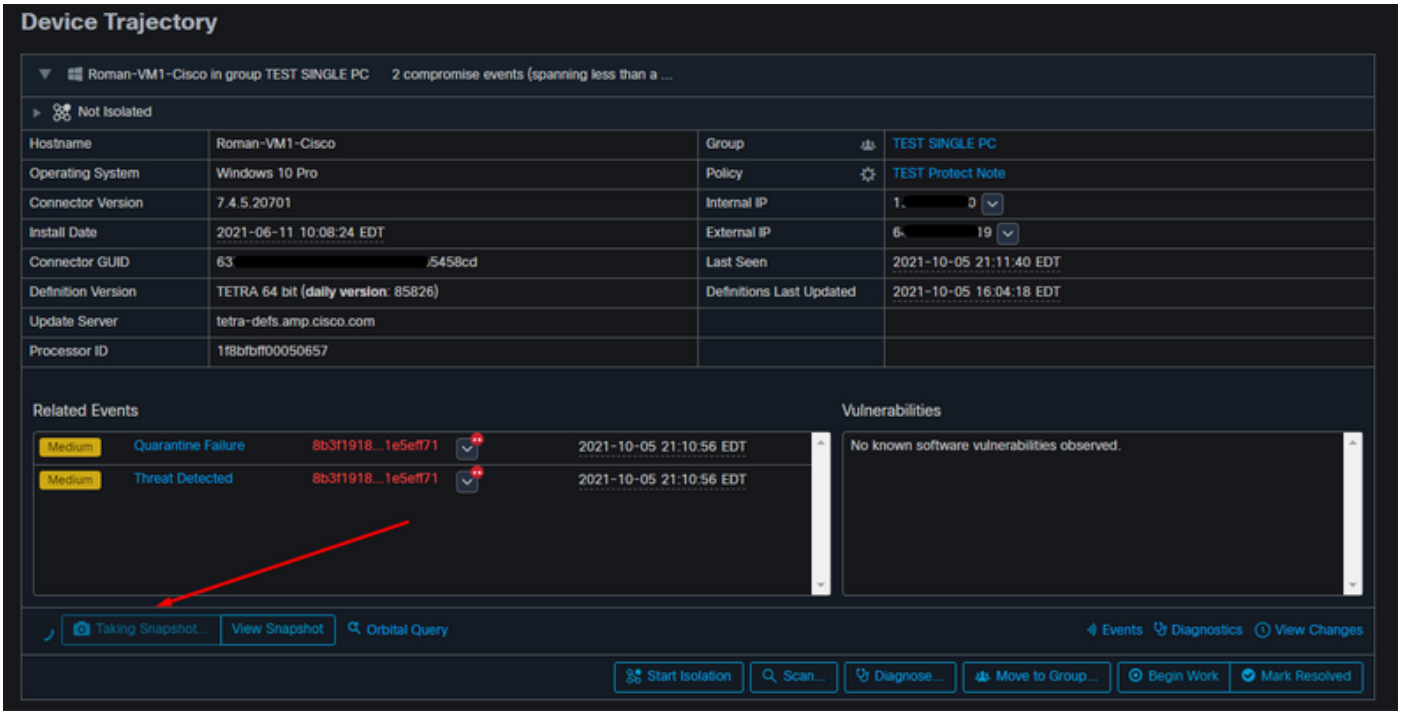
La console de point de terminaison sécurisé est une fois de plus compromise, comme l'illustre l'image



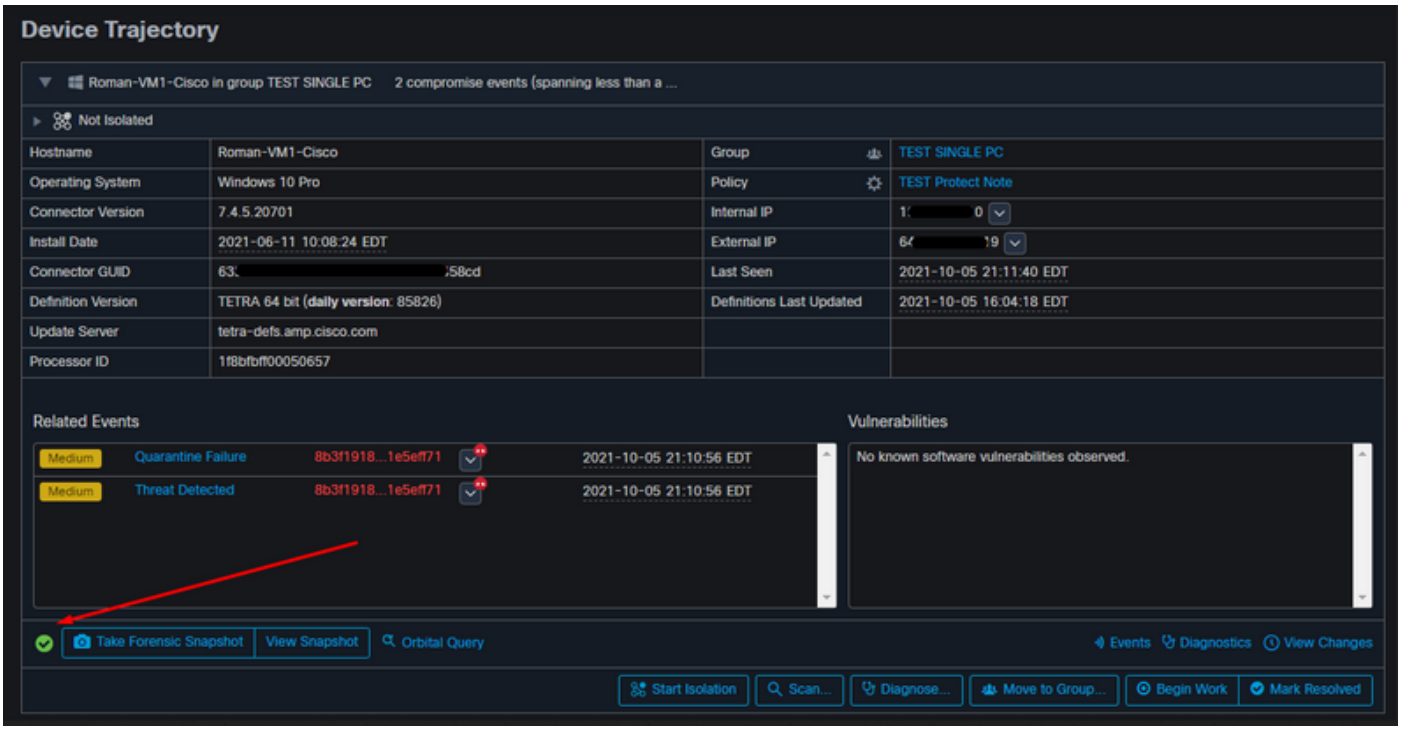
Voici de nouveaux événements sous Actions automatisées, comme l'illustre l'image.



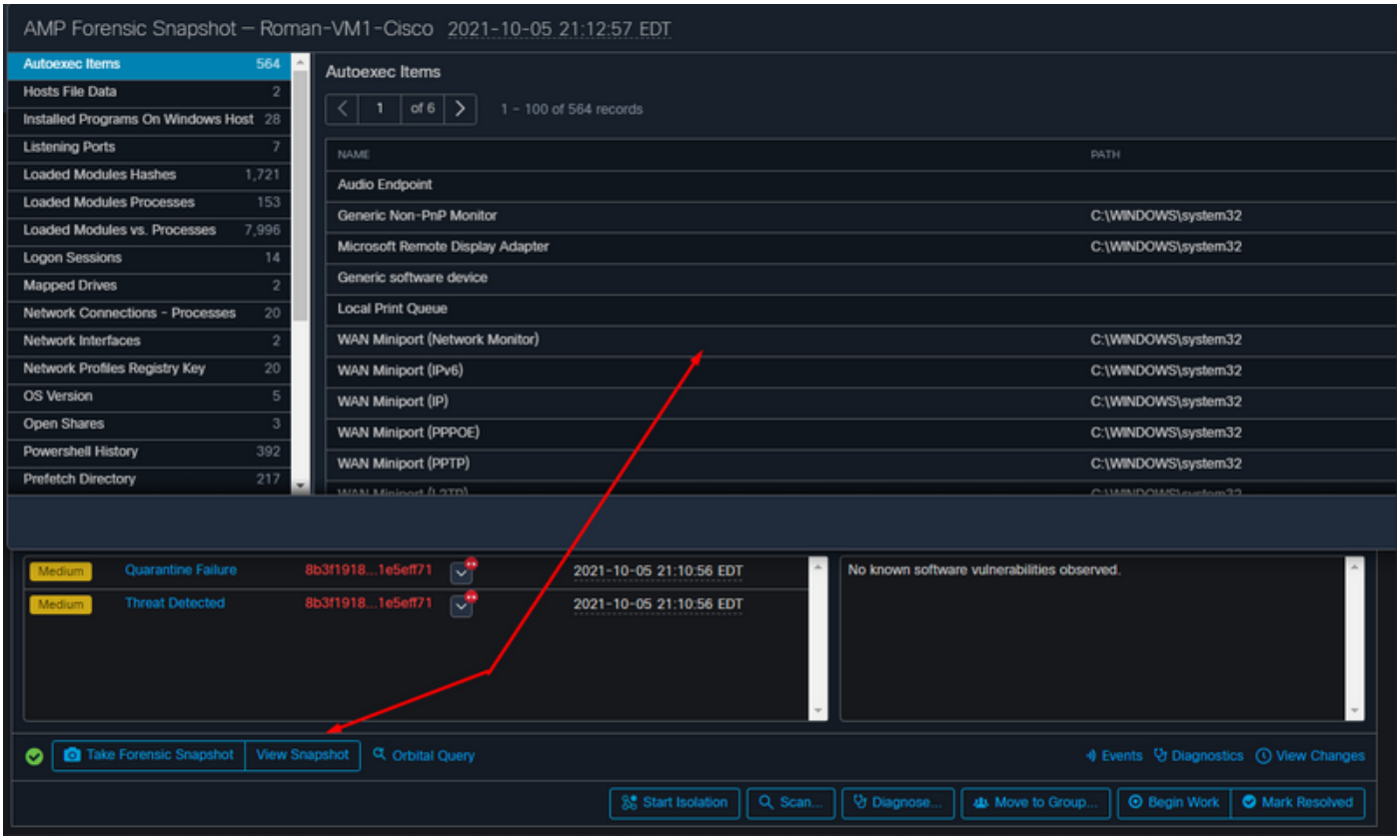
Lorsque le nom d'hôte sous Actions automatisées est sélectionné, il est redirigé vers la trajectoire du périphérique, où vous pouvez observer la création de l'instantané une fois que vous avez développé l'onglet de l'ordinateur, comme illustré dans l'image.



Une minute plus tard, un instantané est créé, comme l'illustre l'image.



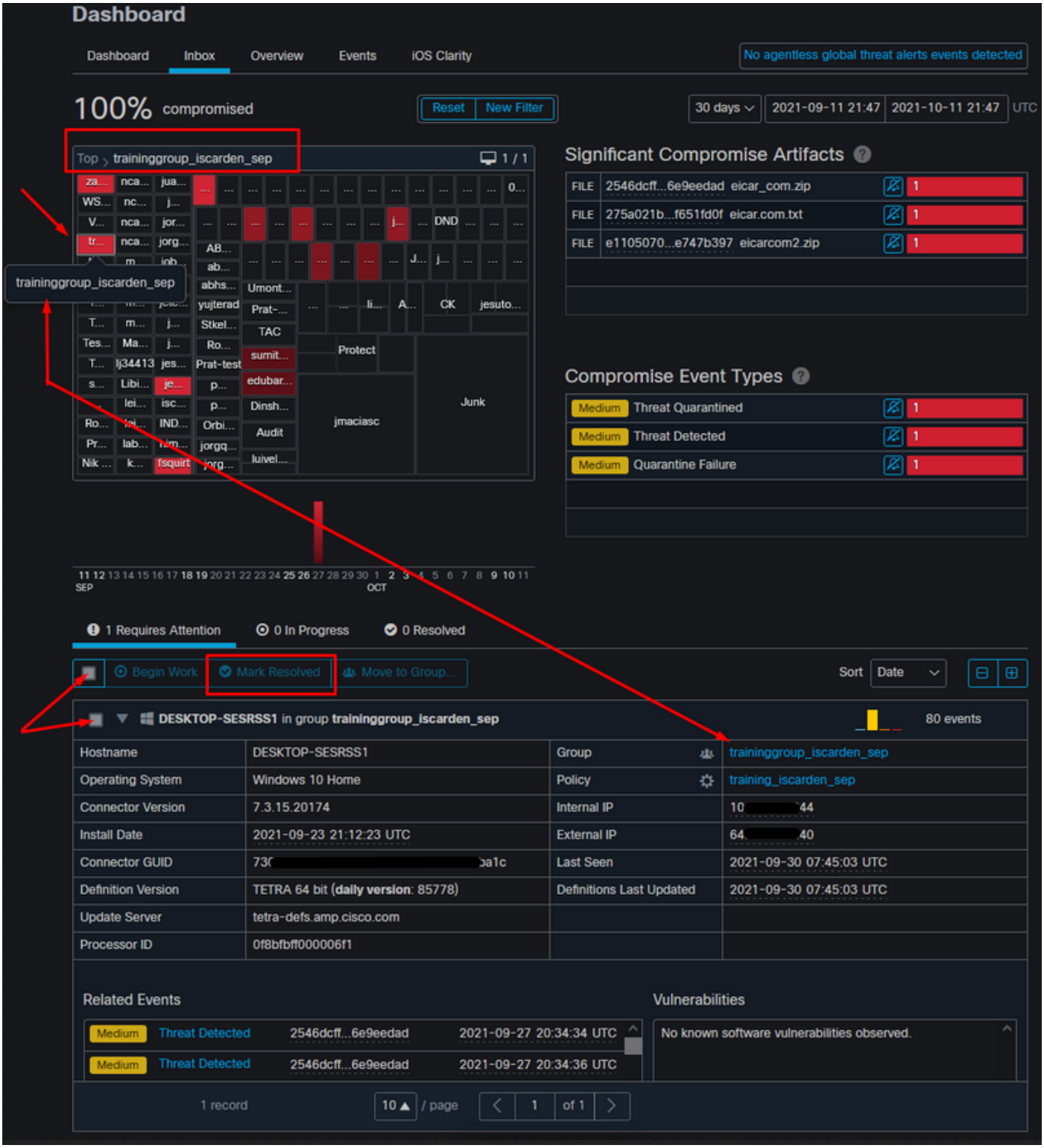
Et maintenant vous pouvez voir les données affichées.



Conseil

Dans des environnements très étendus avec des milliers de terminaux et des centaines de compromis, vous pouvez faire face à des situations où la navigation vers chaque terminal peut être un défi. Actuellement, la seule solution disponible est d'utiliser la carte thermique, puis d'effectuer une hiérarchisation vers le bas vers un groupe spécifique où se trouve votre point de terminaison de compromis, comme dans cet exemple ci-dessous.

Une fois le groupe sélectionné dans la carte thermique, naviguez jusqu'au groupe dans lequel nous avons compromis l'événement. Puisqu'il n'y a qu'un seul terminal dans ce groupe, veuillez noter le compromis à 100 % qui est basé maintenant sur le groupe spécifique dans lequel nous sommes. En d'autres termes, si nous avons 2 points de terminaison dans ce groupe, l'un est propre et l'autre est compromis et affiche un compromis de 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