إجراءات مؤتمتة - لقطة الطب الشرعي

المحتويات

المقدمة
أسئلة شائعة
ما هي الآلة المشبوهة؟
ما هي التسوية؟
ماذا يحدث عندما تحدث اكتشافات جديدة على جهاز مخادع؟
أين يمكنني رؤية وإدارة التسويات؟
كيف يتم تشغيل إجراء مؤتمت*؟
كيف يمكنني إعادة تشغيل إجراء مؤتمت؟
الحالة المستخدمة - إعادة إنشاء Lab
طرف

المقدمة

يصف هذا المستند وظيفة الإجراء التلقائي في نقطة النهاية الآمنة مرتبطة بمفهوم التنازلات. يعد فهم دورة الحياة وإدارة التسويات أمرا حيويا لفهم وظائف الإجراءات المؤتمتة. تجيب هذه المقالة عن الأسئلة المتعلقة بمصطلحات ووظائف هذه المفاهيم.

أسئلة شائعة

ما هي الآلة المشبوهة؟

الجهاز الذي تم إختراقه هو نقطة نهاية تحتوي على تسوية نشطة مقترنة به. يمكن للجهاز الذي تم اكتشافه، من خلال التصميم، أن يكون لديه حل وسط واحد فقط نشط في وقت واحد.

ما هي التسوية؟

الحل الوسط هو مجموعة من واحد أو أكثر من عمليات الكشف على الجهاز. يمكن أن تولد معظم أحداث الكشف (التحديد الذي تم الكشف عنه، مؤشرات التسوية، وما إلى ذلك) أو تصبح مرتبطة بحل وسط. ومع ذلك، هناك أوجه من الأحداث التي قد لا تؤدي إلى حل وسط جديد. على سبيل المثال، عند حدوث حدث تم الكشف عنه لتحديد، ولكن بعد وقت قصير من ظهور حدث مرتبط تم وضعه في الحجر الصحي لتحديد ما، فإن هذا لا يؤدي إلى إصدار حل وسط جديد. ومنطقيا، يرجع السبب في ذلك إلى أن "نقطة النهاية الآمنة" قامت بمعالجة التسوية المحتملة (قمنا بوضع حد أدنى للتحديد).

ماذا يحدث عندما تحدث اكتشافات جديدة على جهاز مخادع؟

تتم إضافة حدث (أحداث) الكشف إلى الحل الوسط الموجود. لم يتم إنشاء أي حل وسط جديد.

أين يمكنني رؤية وإدارة التسويات؟

تتم إدارة التسويات في علامة التبويب "علبة الوارد" الخاصة بوحدة تحكم نقطة النهاية

الآمنة (وهي https://console.amp.cisco.com/compromises لسحابة أمريكا الشمالية). يتم إدراج الجهاز الذي تم إختراقه ضمن قسم **يتطلب الانتباه** ويمكن إلغاء تحديده من التسوية الخاصة به من خلال الضغط على **علامة تم حلها**. كما يتم مسح التنزيلات تلقائيا بعد شهر واحد.

كيف يتم تشغيل إجراء مؤتمت*؟

يتم تشغيل الإجراءات التلقائية عند الوصول إلى حل وسط يتمثل في عندما تصبح إحدى الأجهزة التي لا يمكن الوصول إليها بأي شكل من الأشكال جهازا تم التوصل إليه. وإذا صادفت آلة تم اكتشافها بالفعل، فإن هذا الكشف يضاف إلى الحل الوسط، ولكن بما أن هذا ليس حلا وسطا جديدا، فإنه لا يؤدي إلى عمل آلي.

كيف يمكنني إعادة تشغيل إجراء مؤتمت؟

ومن الضروري "تسوية" الحل الوسط قبل محاولة إعادة إطلاق إجراء مؤتمت. تذكر أن التهديد الذي تم الكشف عنه + التهديد الموجود في الحجر الصحي لا يكفي لتوليد حدث تسوية جديد (وبالتالي لا يكفي لإطلاق إجراء مؤتمت جديد).

*إستثناء: الإجراء التلقائي "إرسال الملف إلى ThreatGrid" غير مرتبط بالتنزيلات، ويعمل لكل كشف

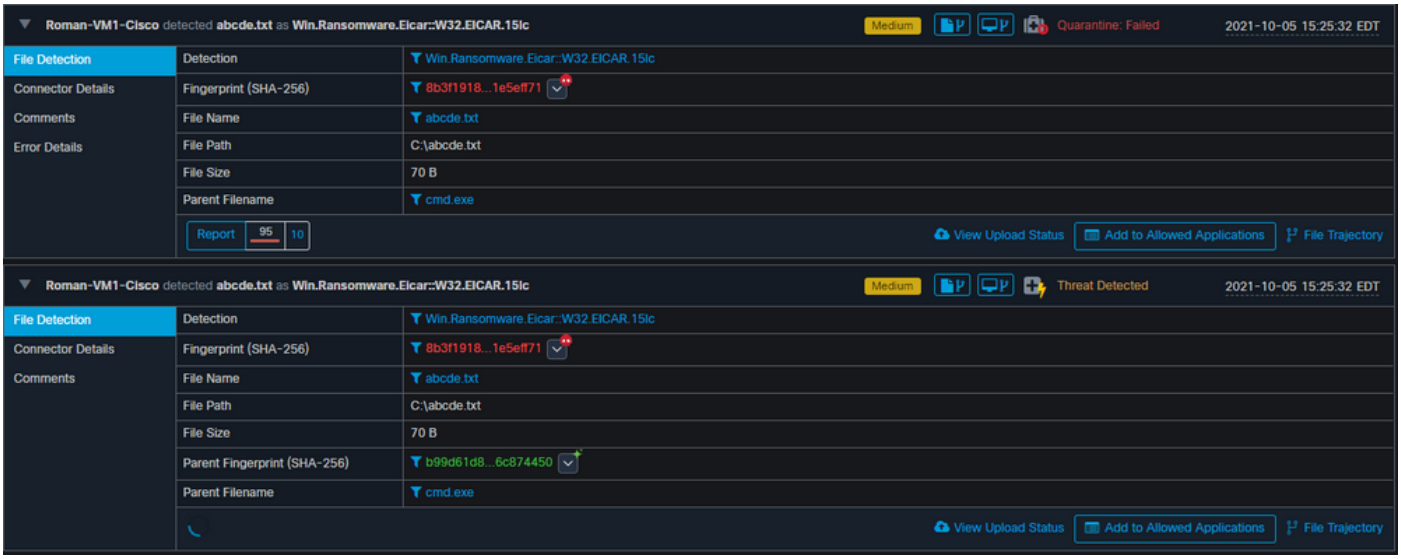
الحالة المستخدمة - إعادة إنشاء Lab

#1: كما ذكرنا في قسم الأسئلة المتداولة. والتي تم أخذ اللقطات السريعية إلا في حالة "المساومة". بمعنى آخر، إذا حاولنا الوصول إلى ملف صار من موقع إختبار وتنزيله وتم وضع علامة على الملف عند التنزيل ووضع حجر صحي لا يعتبر حلا وسطا ولا يشغل الإجراء.

> **ملاحظة**: اكتشاف DFC، فشل الحجر الصحي، أو شيء بدرجة كبيرة يندرج ضمن فئة الحدث الوسط حسب المنطق، يجب أن يؤدي إلى إنشاء لقطة جنائية.

#2: يمكن إنشاء لقطة Forensic مرة واحدة فقط على حدث فريد تم إختراقه لا تقوم بإنشاء لقطة ما لم تقم بحل الجهاز الذي تم إختراقه في علبة الوارد الخاصة بك. إذا لم تقم بحل الحدث الذي تم إختراقه، فلن تقوم بتوليد أي لقطة أخرى.

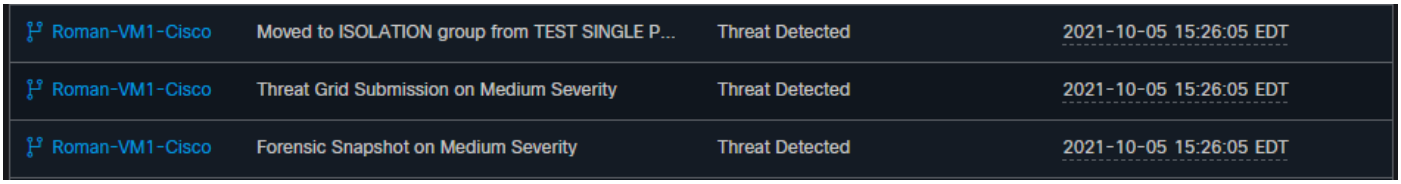
مثال: في هذا المختبر، يولد البرنامج النصي نشاط ضار، ولأن الملف يتم حذفه بمجرد إنشائه ولم تكن نقطة النهاية الآمنة قادرة على عزل الملف الذي يقع فيه إلى فئة التسوية.



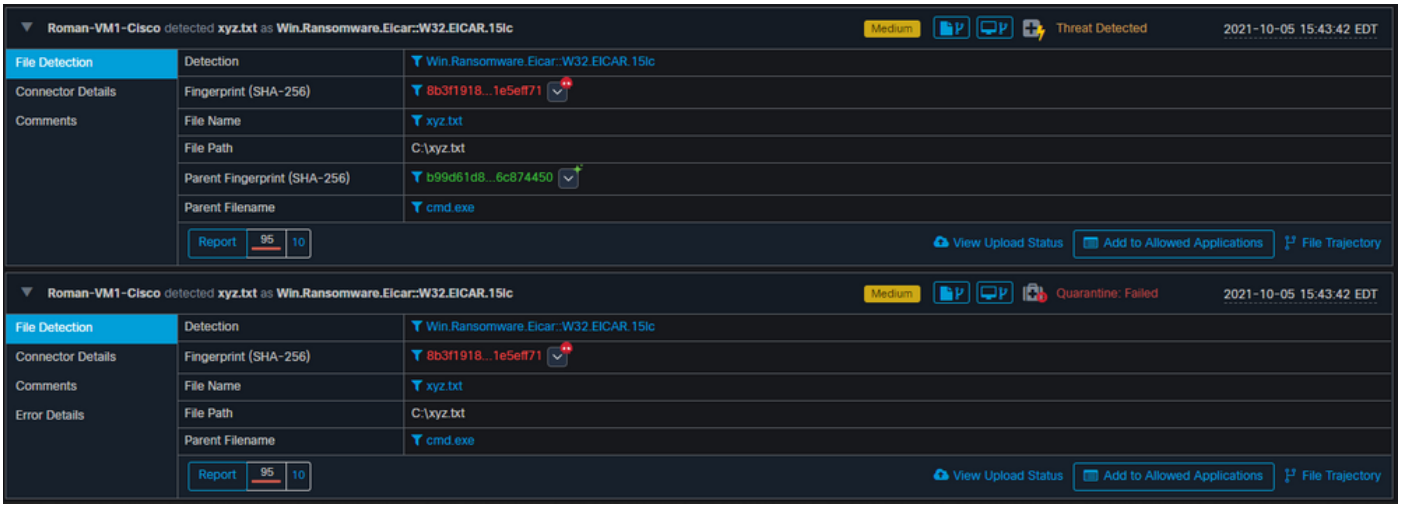
الآن في هذا الاختبار، يمكنك النظر تحت العمليات الآلية و 3 أشياء التي حدثت بناء على الإعدادات.

- تم إنشاء لقطة
- تم إرسال الإرسال إلى شبكة التهديدات (TG)
- تم نقل نقطة النهاية إلى مجموعة منفصلة تم إنشاؤها وتسمى "عزل"

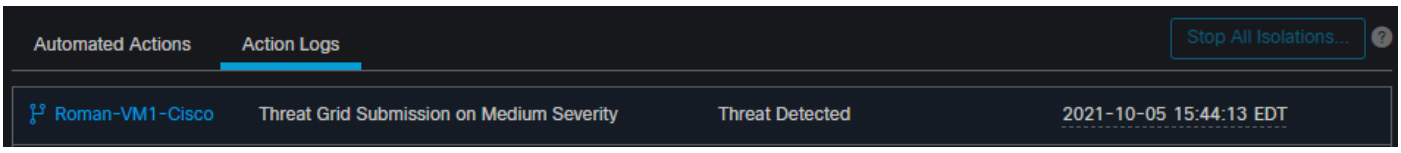
يمكنك رؤية كل ذلك في هذا المخرج، كما هو موضح في الصورة.



الآن بما أن هذه النقطة النهائية تم إخراقها، الاختبار التالي لإثبات النظرية بملف ضار مماثل لكن باسم مختلف، كما هو موضح في الصورة.

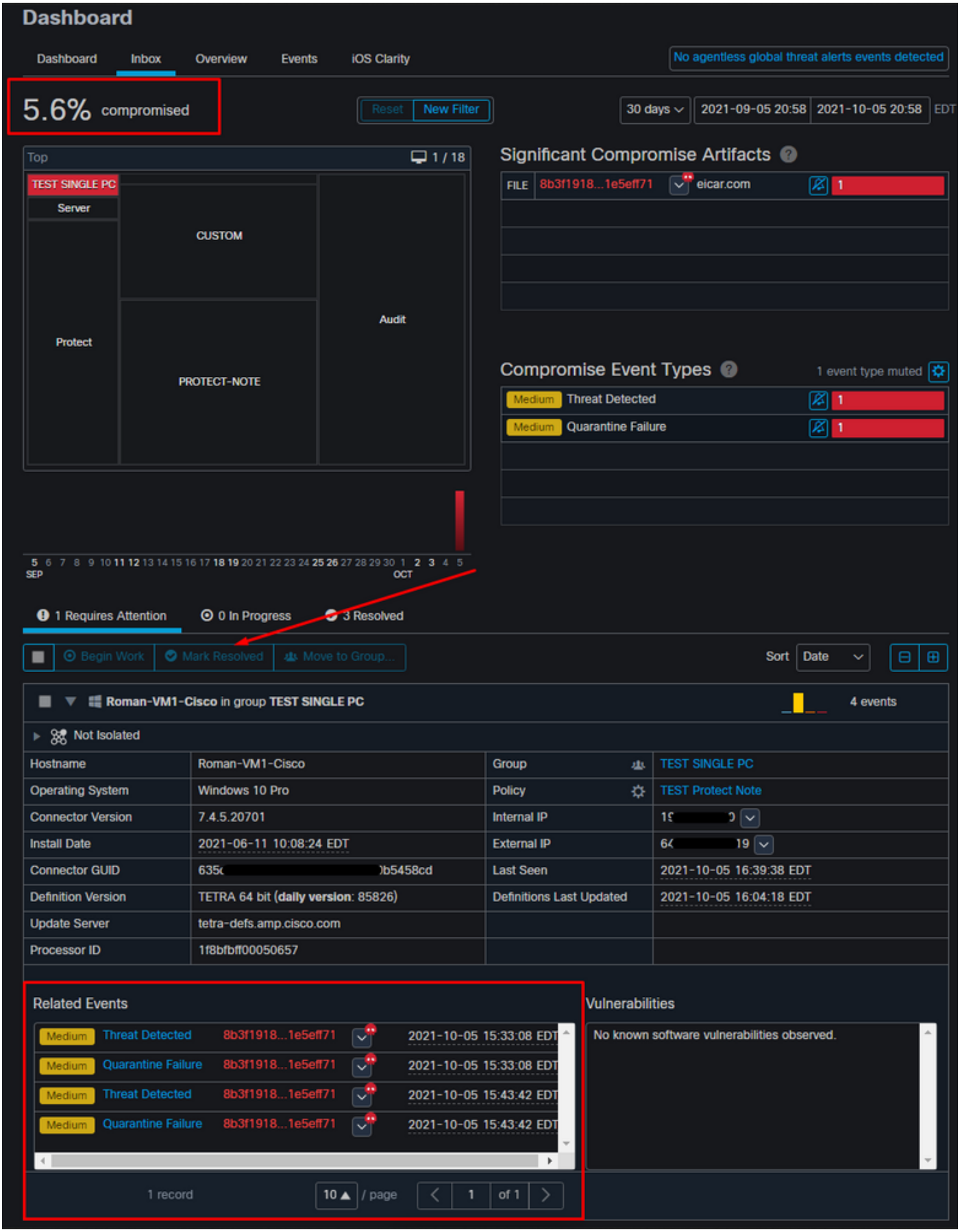


ومع ذلك، نظرا لعدم حل هذه التسوية، يمكنك إنشاء إرسال TG فقط. لم يتم تسجيل أي أحداث أخرى، قم أيضا بإيقاف تشغيل العزل قبل هذا الاختبار الثاني.

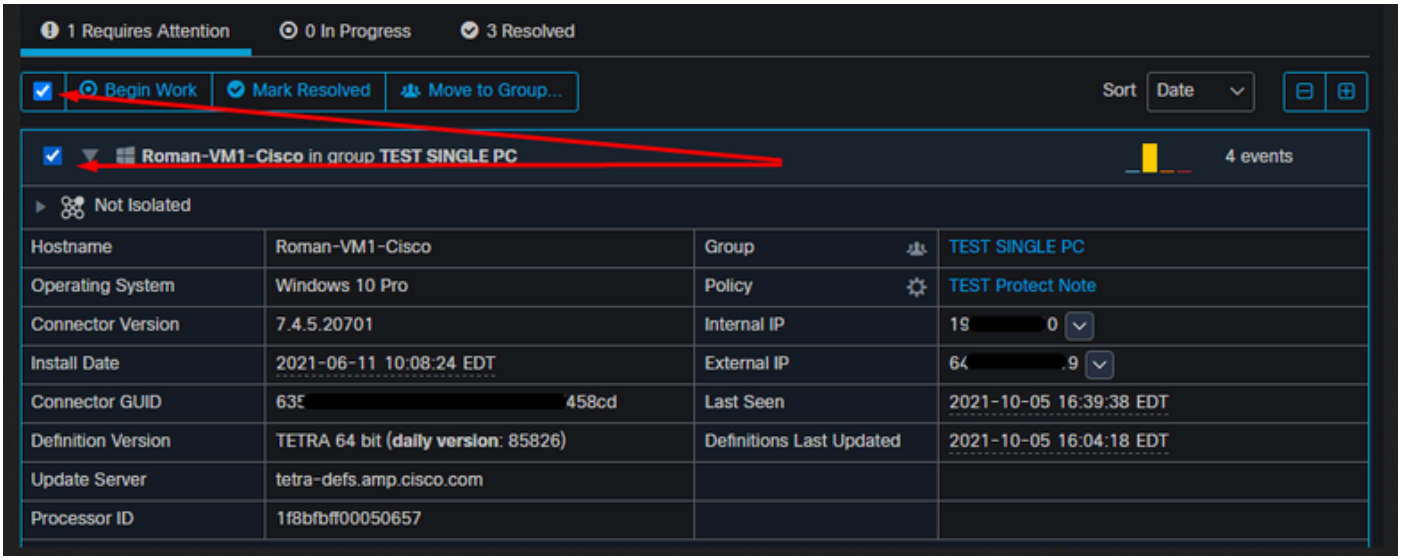


ملاحظة: الرجاء ملاحظة الوقت الذي تم فيه الكشف عن التهديد وبدء الإجراء التلقائي.

ال يمكن إستعادة الحدث ام لم يتم حل نقطة النهاية التي تم تعريضها للخطر. في هذه الحالة، تبدو لوحة المعلومات هكذا. الرجاء ملاحظة النسبة المئوية والعامة الزر التي تم حلها عم الأحداث التي تم إختراقها. بغض النظر عن عدد الأحداث التي تم تشغيلها، يمكن إنشاء نقطة واحدة فقط ولم يتم تغيير رقم النسبة المئوية الكبيرة مطلقا. يمثل هذا الرقم الحل وسط داخل مؤسستك ويقوم على المبلغ الإجمالي لنقاط النهاية في مؤسستك. إنها تتغير فقط مع جهاز آخر تم إختراقه. في هذا المثال، يكون الرقم مرتفعا بسبب وجود 16 جهازا في المختبر. لاحظ أيضا أنه يتم إلغاء تحديد الأحداث التي تمثل الحل وسط تلقائيا بمجرد بلوغها سن 31 يوما.

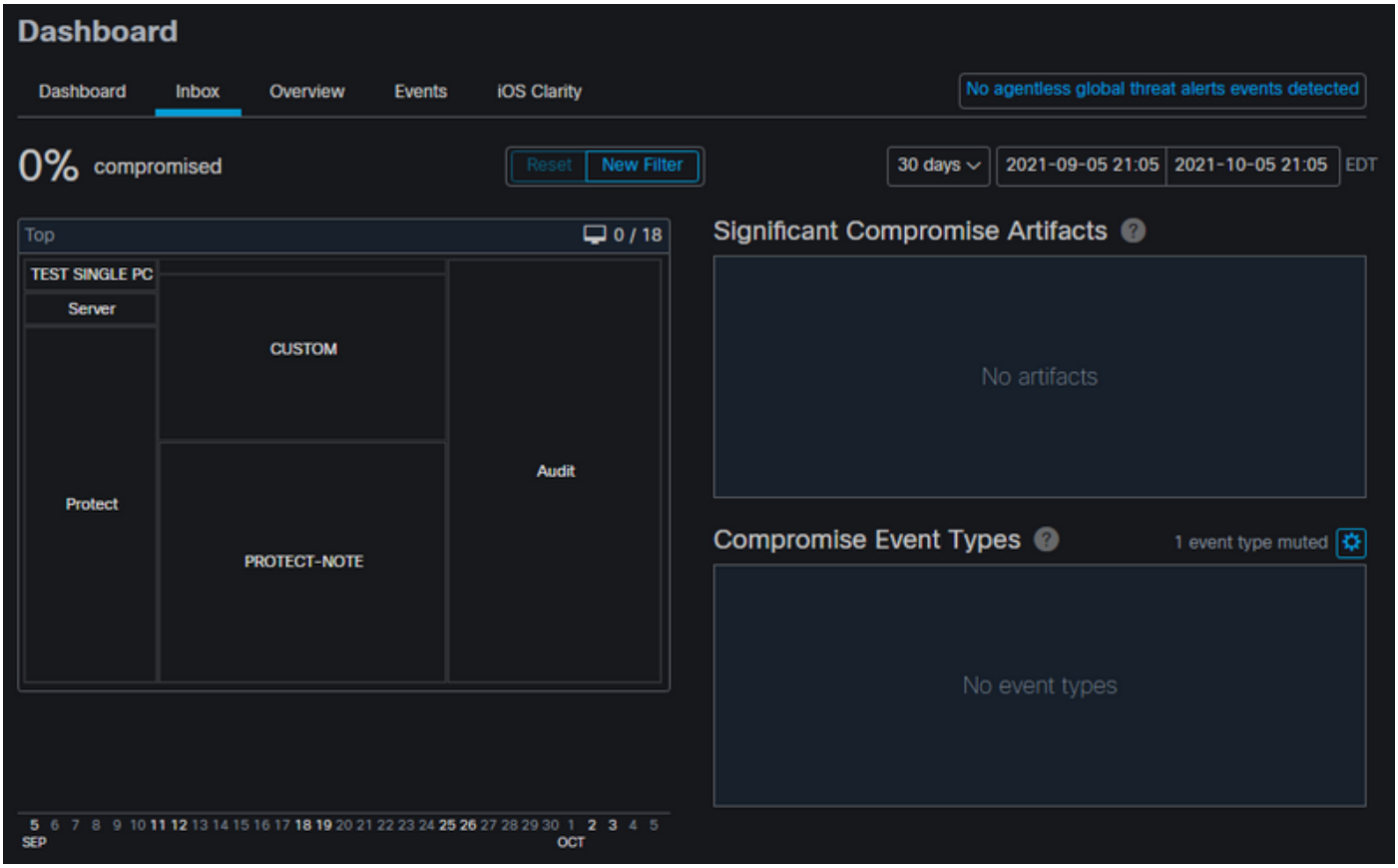


تتمثل الخطوة التالية في إنشاء حدث آخر وإنشاء لقطة جنائية. الخطوة الأولى هي حل هذه التسوية، انقر فوق زر **علامة الحل**". يمكنك القيام بذلك لكل نقطة نهاية أو يمكنك تحديد الكل في مؤسستك.

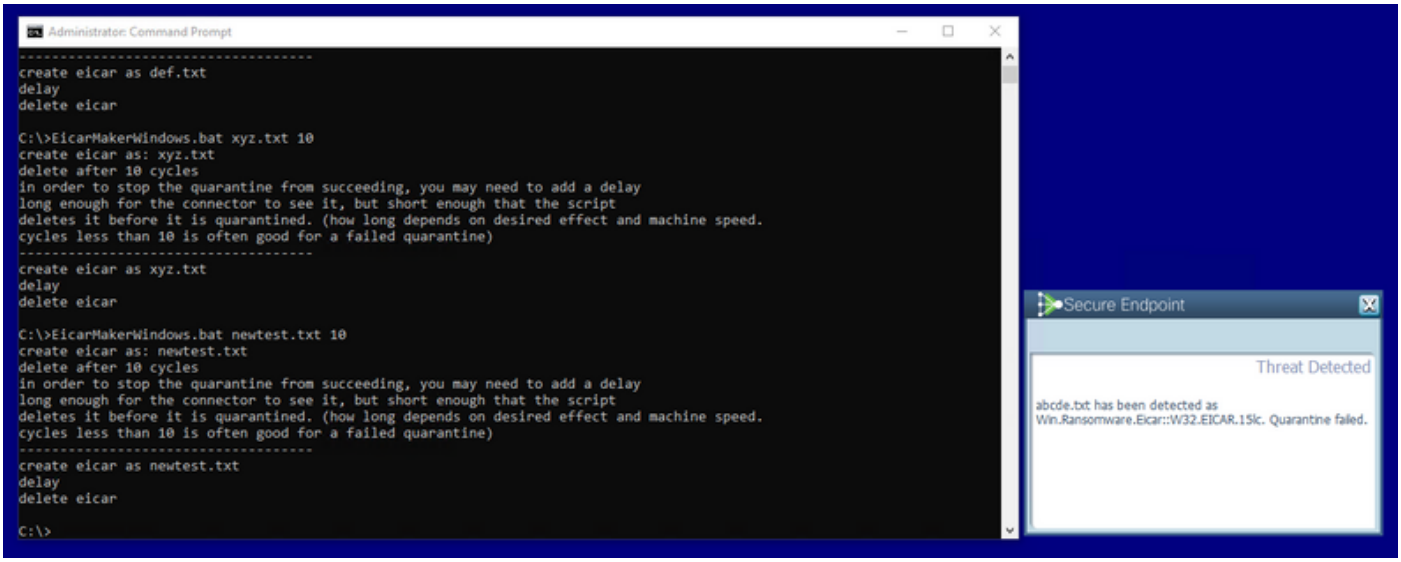


ملاحظة: إذا قمت بتحديد كافة التنازلات، يتم إعادة تعيينها إلى 0٪.

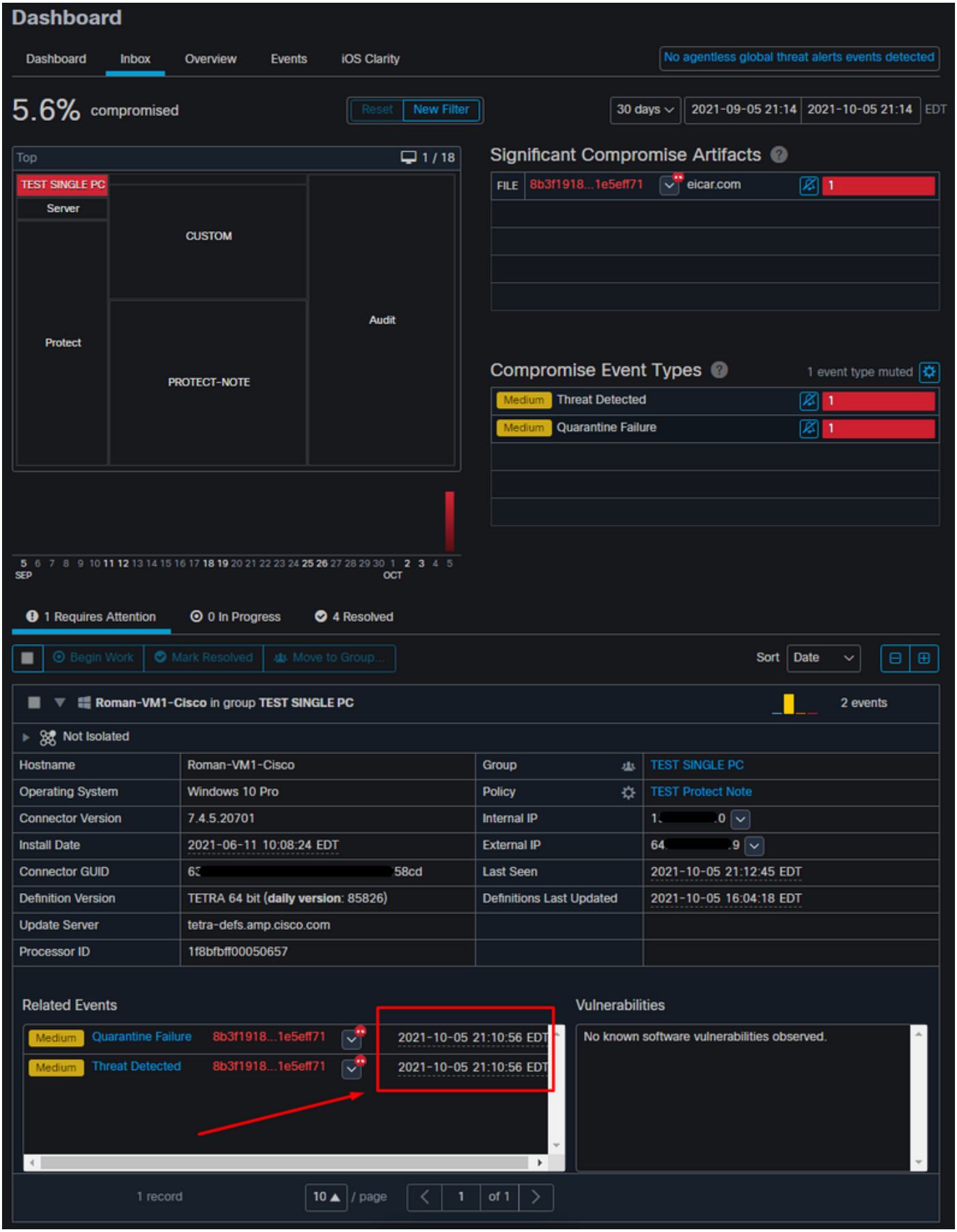
بمجرد تحديد زر "علامة الحل" ونظرا لأنه تم أختراق نقطة نهاية واحدة فقط على لوحة معلومات نقطة النهاية الآمنة تبدو بهذا الشكل. وعند هذه النقطة، تم تشغيل حدث جديد تم إختراقه على جهاز الاختبار.



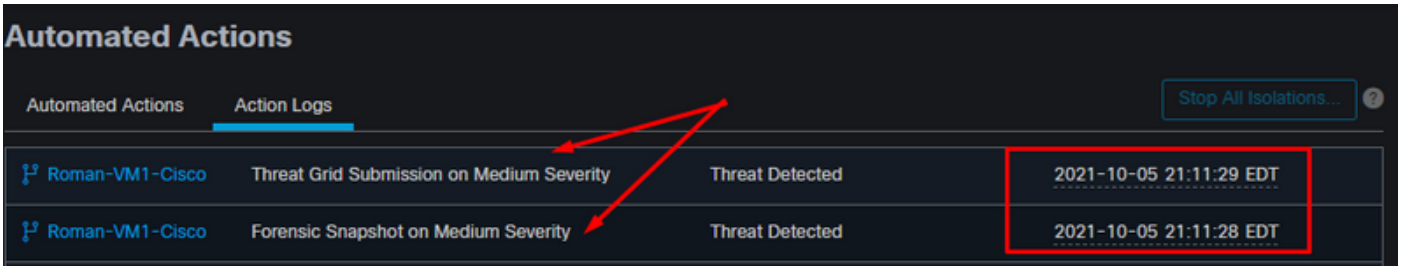
يقوم المثال التالي بتشغيل حدث باستخدام برنامج نصي مخصص يقوم بإنشاء وحذف ملف ضار.



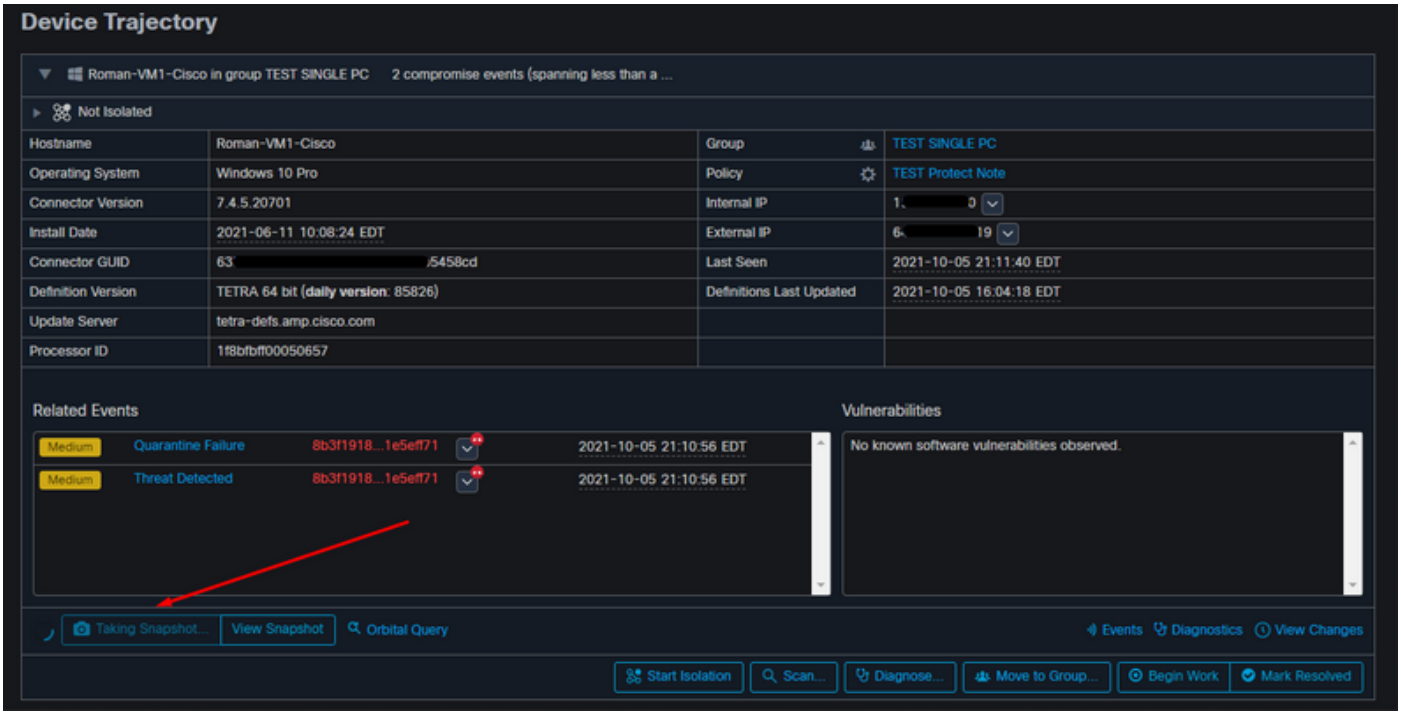
تم أختراق وحدة تحكم نقطة النهاية الآمنة مرة أخرى، كما هو موضح في الصورة



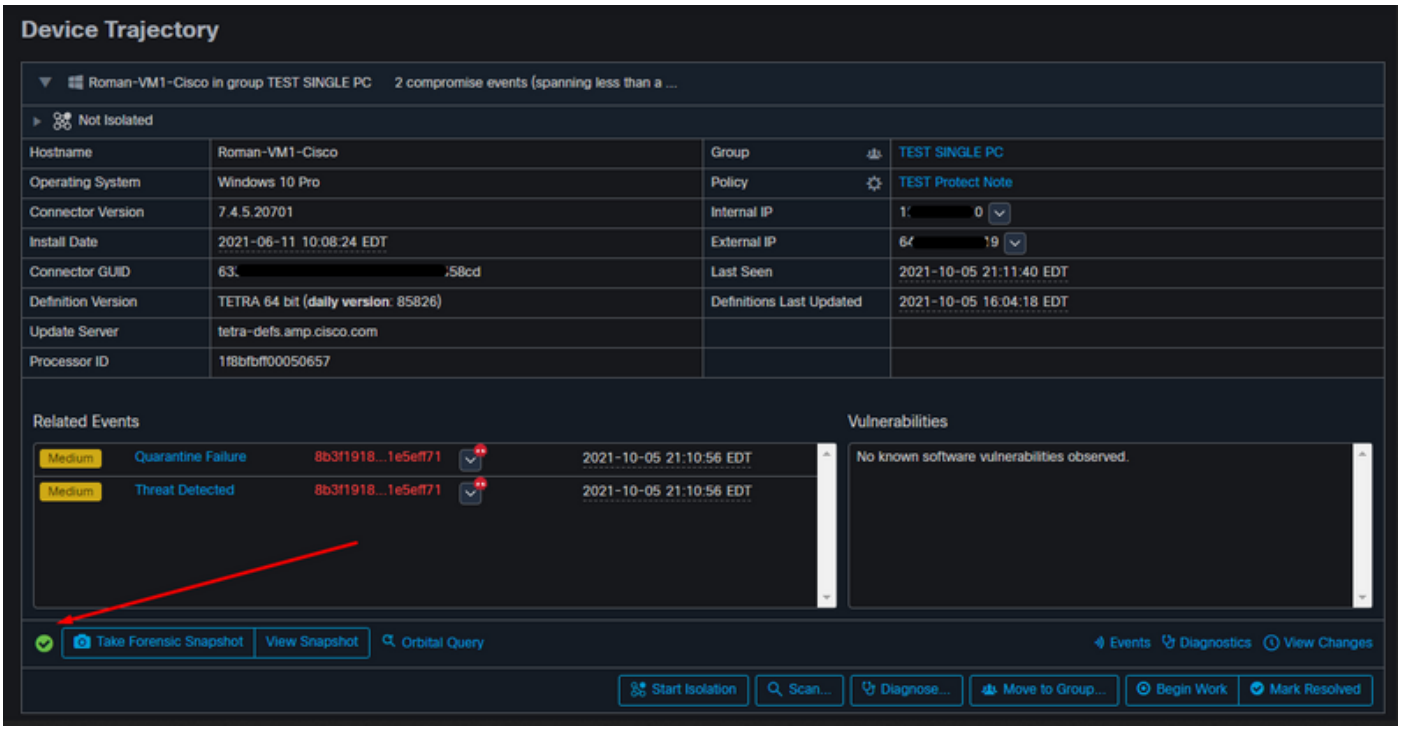
فيما يلي أحداث جديدة ضمن "إجراءات مؤتمتة"، كما هو موضح في الصورة.



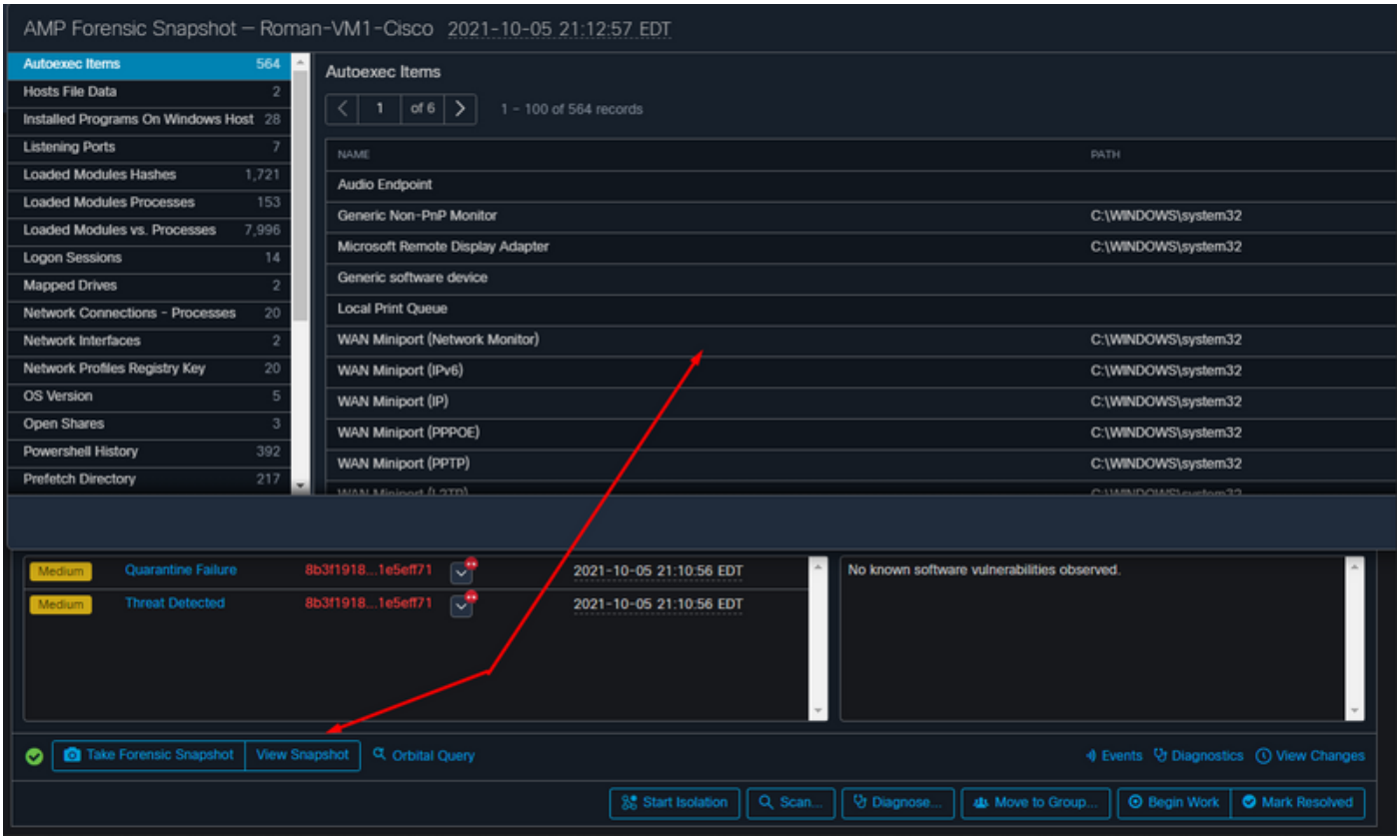
عندما يتم تحديد اسم المضيف تحت العمليات الآلية، فإنه يعيد توجيهه إلى مسار الجهاز حيث يمكنك ملاحظة اللقطة التي يتم إنشاؤها بمجرد توسيع علامة التبويب الكمبيوتر، كما هو موضح في الصورة.



ويتم إنشاء لقطة بعد دقيقة، كما هو موضح في الصورة.



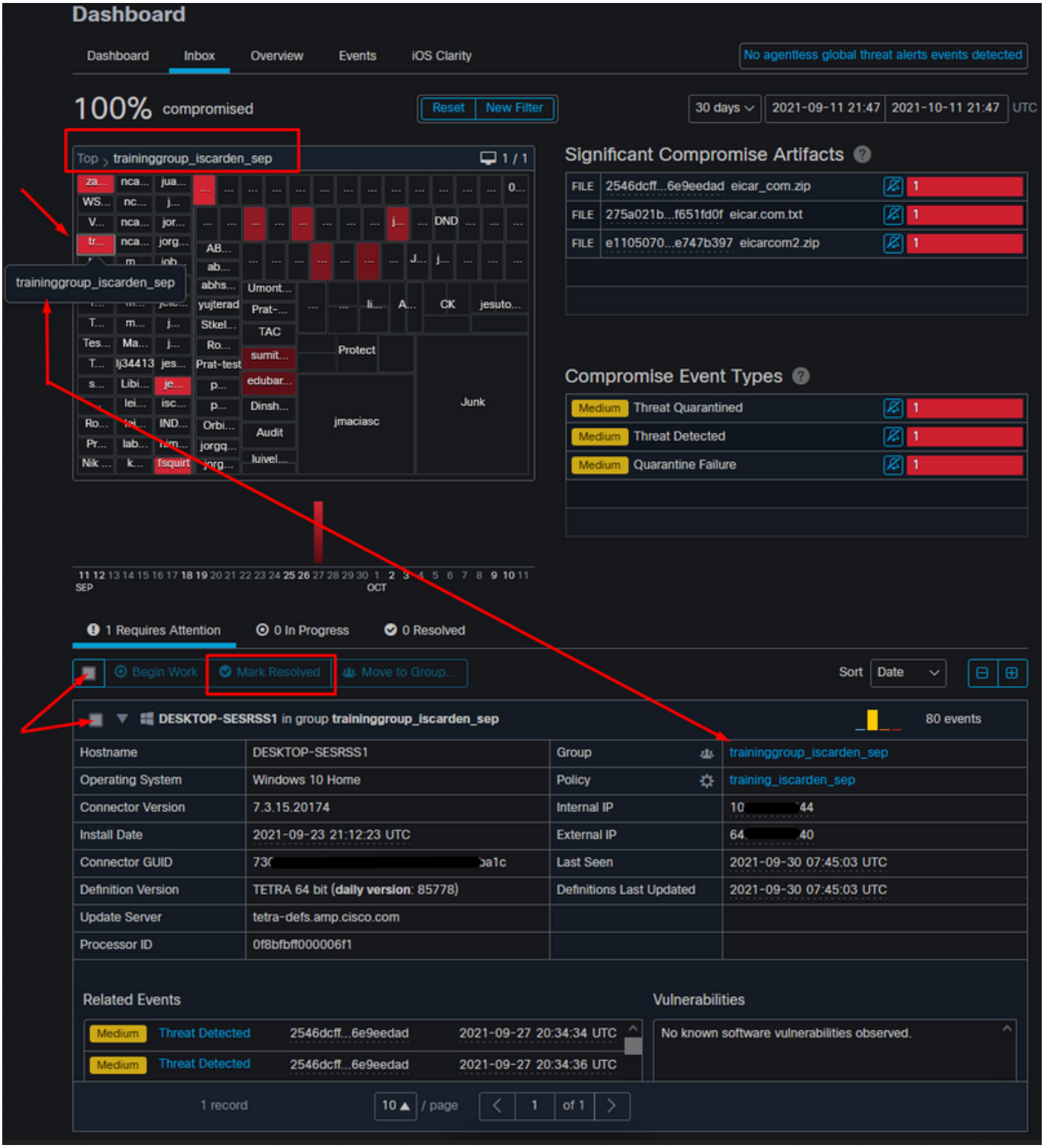
والآن يمكنك عرض البيانات المعروضة.



طرف

في البيئات الكبيرة جدا التي تحتوي على آلاف من نقاط النهاية ومئات من التنازلات، يمكنك أن تواجه مواقف حيث قد يشكل التنقل إلى نقطة النهاية الفردية تحديا. حاليا، الحل الوحيد المتاح هو إستخدام خريطة الحرارة ثم التنقل لأسفل إلى مجموعة محددة حيث تكون نقطة النهاية للتسويات الخاصة بك كما هو موضح في هذا المثال أدناه.

بمجرد تحديد المجموعة في خريطة الحرارة، انتقل إلى تلك المجموعة التي قمنا فيها بتقويض الحدث. ونظرًا لوجود نقطة نهاية واحدة فقط في هذه المجموعة، يجب ملاحظة النقطة التي تم التفريط فيها بنسبة 100٪ والتي تستند الآن إلى المجموعة المحددة التي نحن فيها. بمعنى آخر، إذا كان لديك 2 نقطة نهاية في هذه المجموعة واحدة نظيفة وأخرى تعرض تسوية 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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).