自動操作 — 調查分析快照

目錄

簡介

本文檔介紹了安全終端中的自動操作功能與危害概唸緊密相關。 瞭解危害的生命週期和管理對於理解自動化操作的功能至關重要。本文回答有關這些概念的術語和功能的問題。

常見問題

什麼是受損的機器？

受危害的電腦是與其關聯的活動危害的終結點。根據設計，受危害的電腦一次只能有一個危害處於活動狀態。

什麼是妥協？

危害是在電腦上一個或多個檢測的集合。大多數檢測事件（檢測到的威脅、危害表現等）可能會生成危害或與之關聯。但是，有成對的事件可能不會觸發新的危害。例如，當「檢測到威脅」事件發生，但發生相關威脅隔離事件後不久，不會觸發新的危害。從邏輯上講，這是因為安全端點已處理了潛在的危害（我們隔離了威脅）。

在受侵害的電腦上發生新檢測時，會發生什麼情況？

檢測事件會新增到現有危害中。不建立任何新的危害。

在哪裡可以檢視和管理折衷方案？

在安全終端控制檯的「收件箱」頁籤(北美雲為https://console.amp.cisco.com/compromises)中管理危害。受危害的電腦列在**需要注意**部分下，可以按**Mark Resolved**清除其危害。此外，在一個月後將自動清除危害行為。

如何觸發自動操作*?

在遭受危害時（即非受損電腦成為受損電腦）觸發自動操作。如果已經受損的電腦遇到新檢測，該檢測將被新增到危害中，但由於這不是新危害，因此不會觸發自動操作。

如何重新觸發自動操作？

在嘗試重新觸發自動操作之前，必須「清除」危害。請記住，檢測到的威脅+隔離威脅事件不足以生成新的危害事件（因此不足以觸發新的自動化操作）。

*異常：「向ThreatGrid提交檔案」自動操作與危害無關，並且根據檢測運行

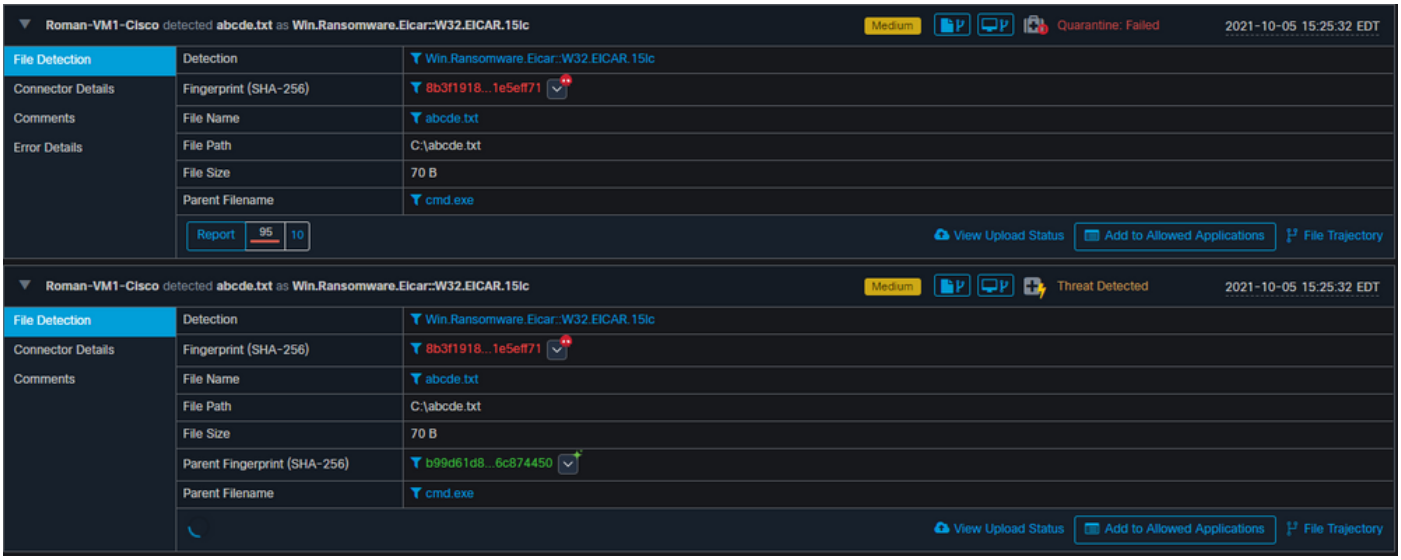
用例 — 實驗室重建

#1:如我們在FAQ部分中所述。只有在「洩露」的情況下才拍攝調查快照。換句話說，如果我們嘗試從TEST站點訪問和下載惡意檔案，並且該檔案在下載時被標籤並被隔離，這不會被視為危害並且不會觸發操作。

> **附註**：DFC檢測、隔離失敗以及邏輯上屬於危害事件類別的所有內容都應建立取證快照。

#2:您只能對唯一的受感染事件生成一次調查快照，除非您在收件箱中解析受感染電腦，否則不會生成快照。如果不解決受損事件，則不會生成任何其他快照。

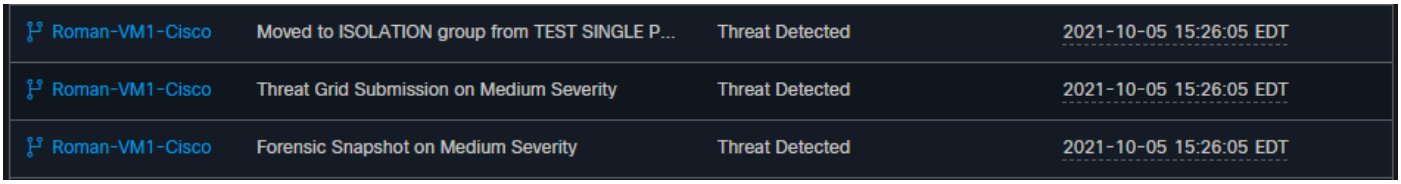
範例：在本實驗中，指令碼會生成惡意活動，而且由於檔案在建立後即被刪除，安全終結點無法隔離該檔案，因此該檔案屬於危害類別。



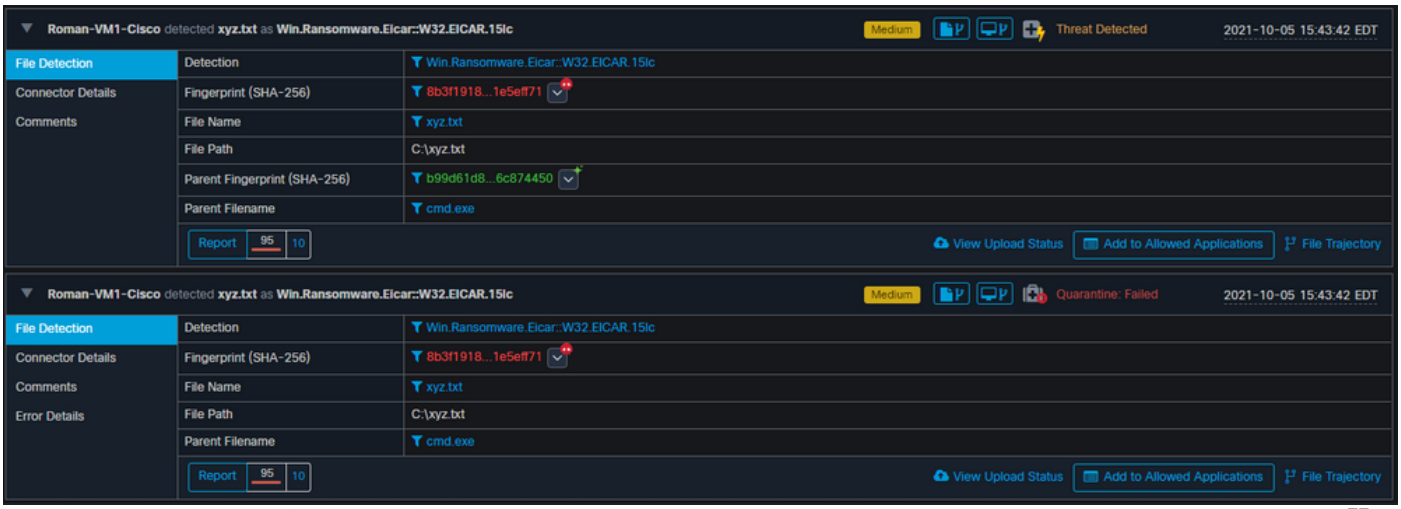
在此測試中，您可以檢視自動操作下的內容以及基於設定發生的3件事。

- 已建立快照
- 提交內容已傳送到Threat Grid(TG)
- 端點被移動到已建立並稱為ISOLATION的獨立組

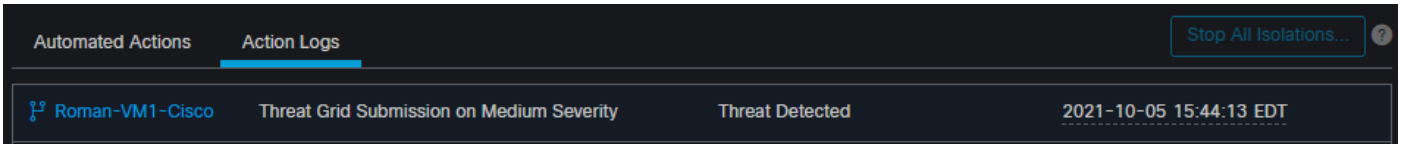
您可以在此輸出中看到所有這些內容，如下圖所示。



現在，由於此端點受到危害，下一步測試將用類似的惡意檔案使用不同的名稱來證明該理論，如下圖所示。

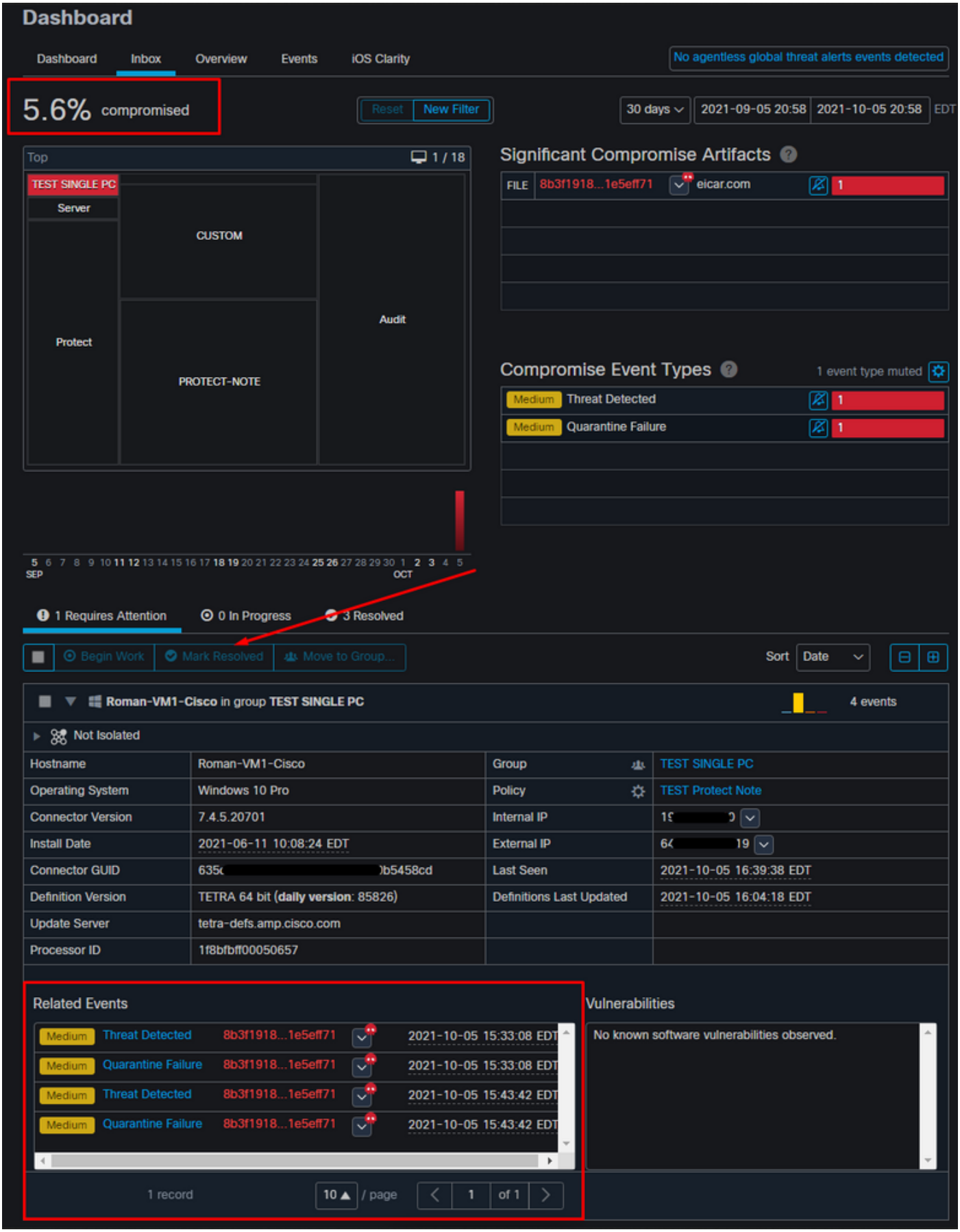


但是，由於未解決此危害，因此您只能建立TG提交。未記錄其他事件，也在此第2次測試之前關閉隔離。

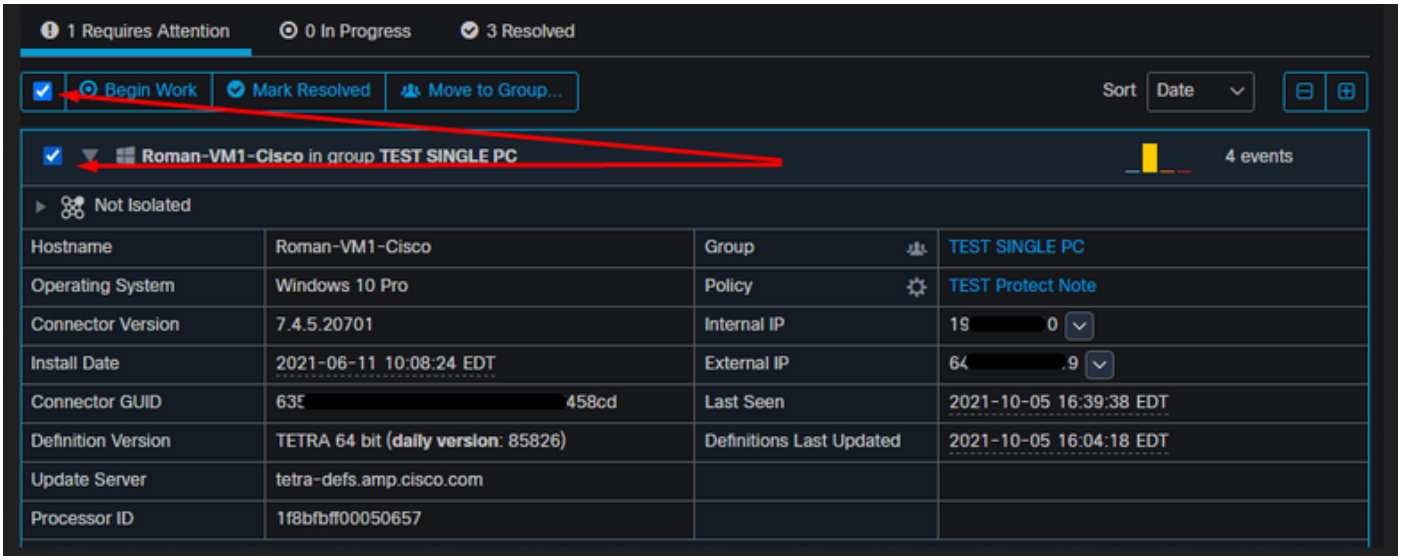


附註：請注意檢測到威脅並觸發自動操作的時間。

除非已解析損壞的終結點，否則無法重試事件。在這種情況下，儀表板如下所示。請注意百分比和「標籤已解決」按鈕以及受危害事件。無論觸發多少個事件，您都只能建立一個快照，並且大百分比的數字始終不變。該數字表示組織內部的危害，它基於組織中的終端總數。它只能用另一台受損的機器來改變。在本例中，由於實驗中只有16台裝置，因此該數字很高。另請注意，危害事件在達到31天時會自動清除。

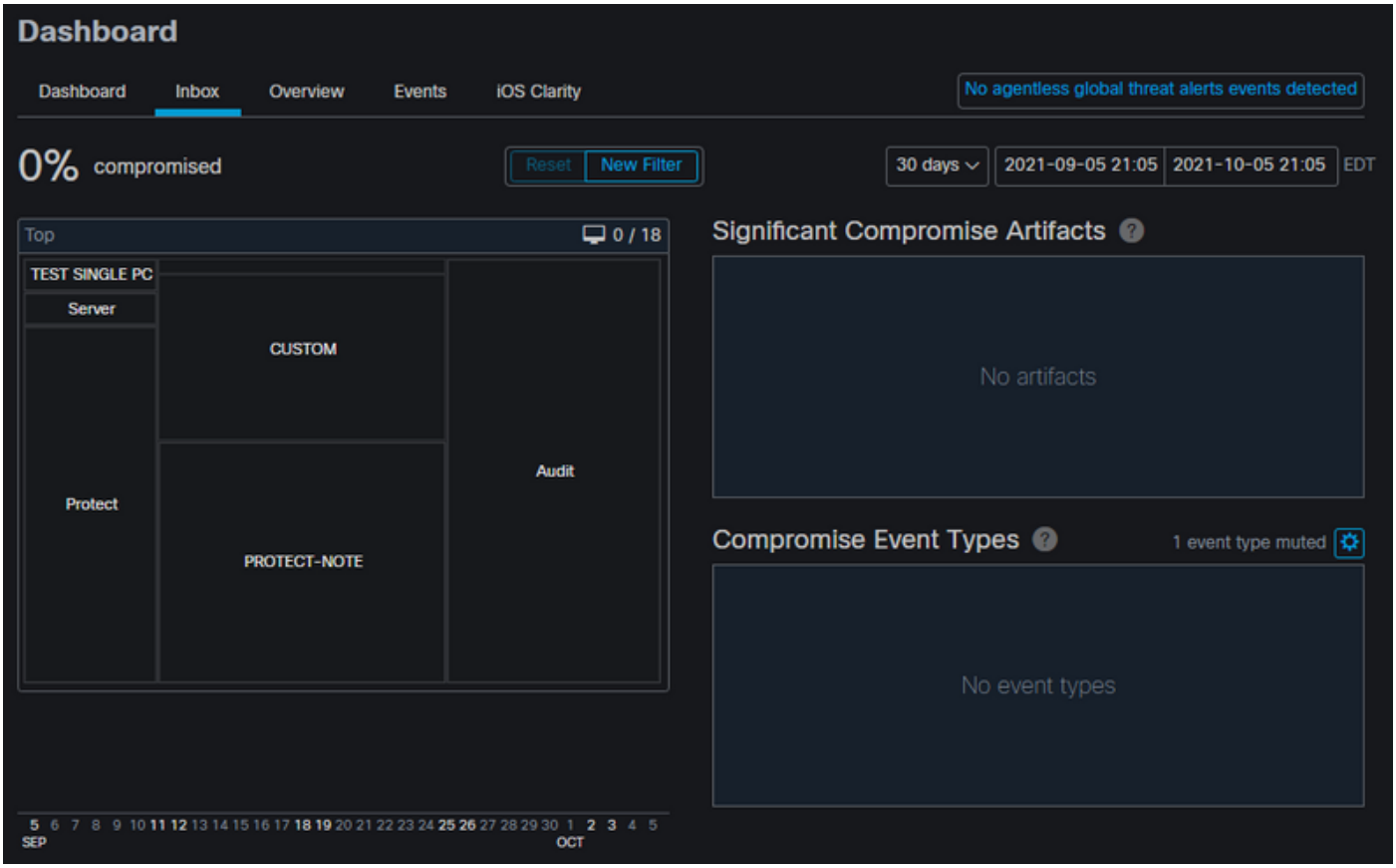


下一步是建立另一個事件並生成取證快照。第一步是解決此危害，按一下**Mark Resolved**按鈕。您可以按終端進行此操作，也可以選擇組織中的所有終端。

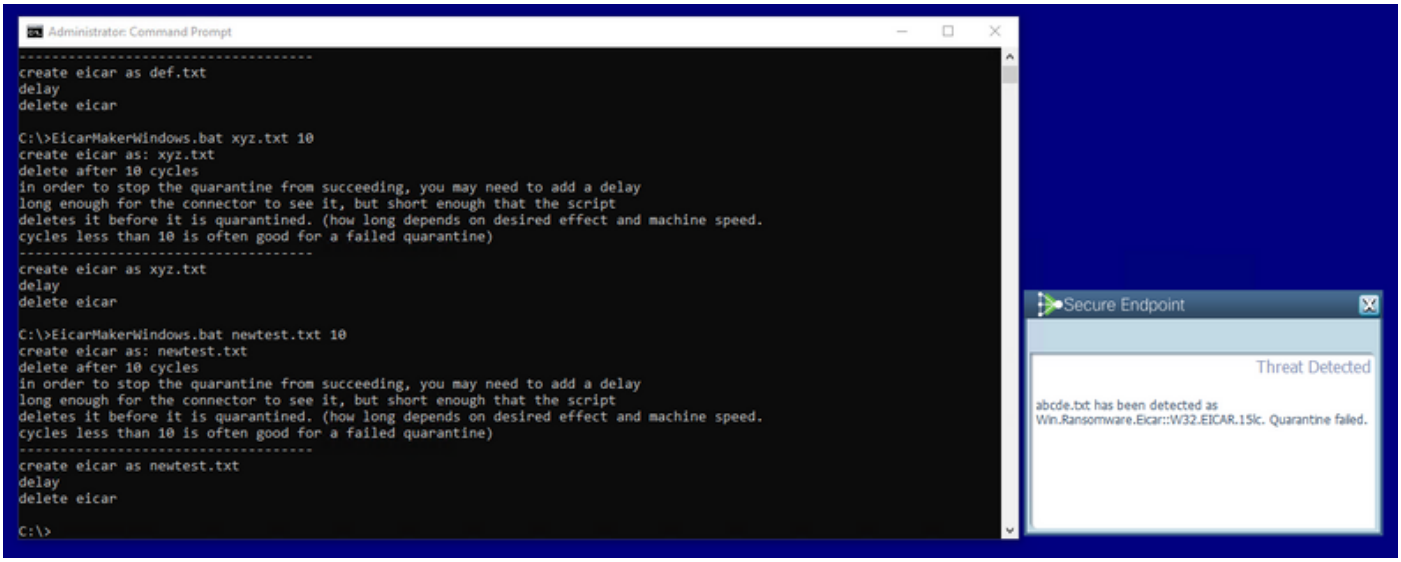


附註： 如果選擇所有危害都會重置為0%。

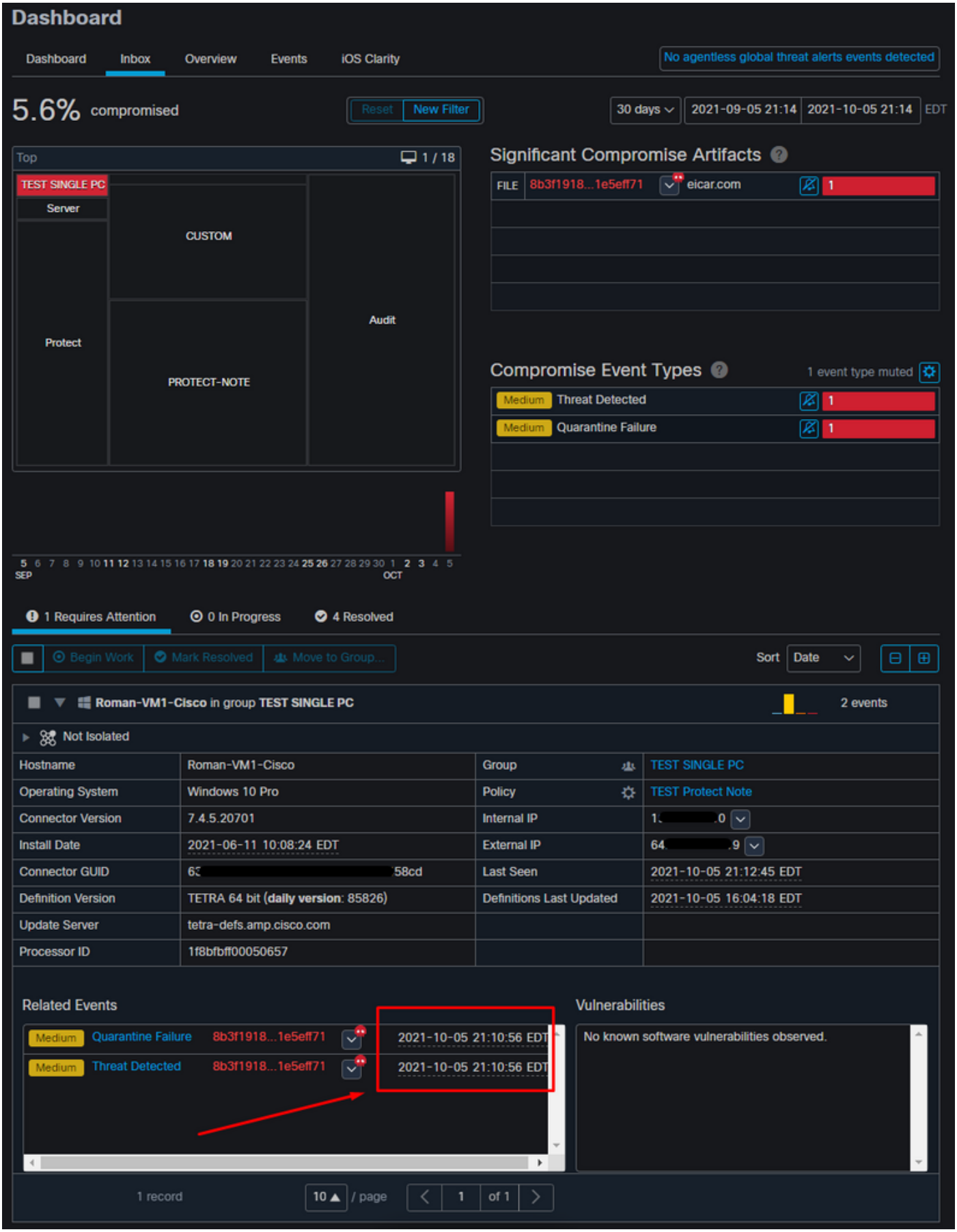
選中「標籤已解決」按鈕後，由於安全終結點控制面板上只有一個終結點受到危害，因此該按鈕將如下所示。這時，測試機上一個新的受損事件被觸發。



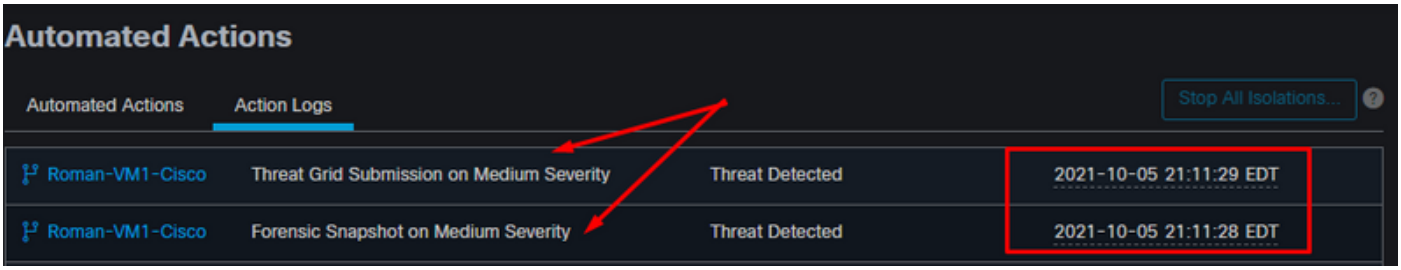
下一個示例使用建立和刪除惡意檔案的自定義指令碼觸發事件。



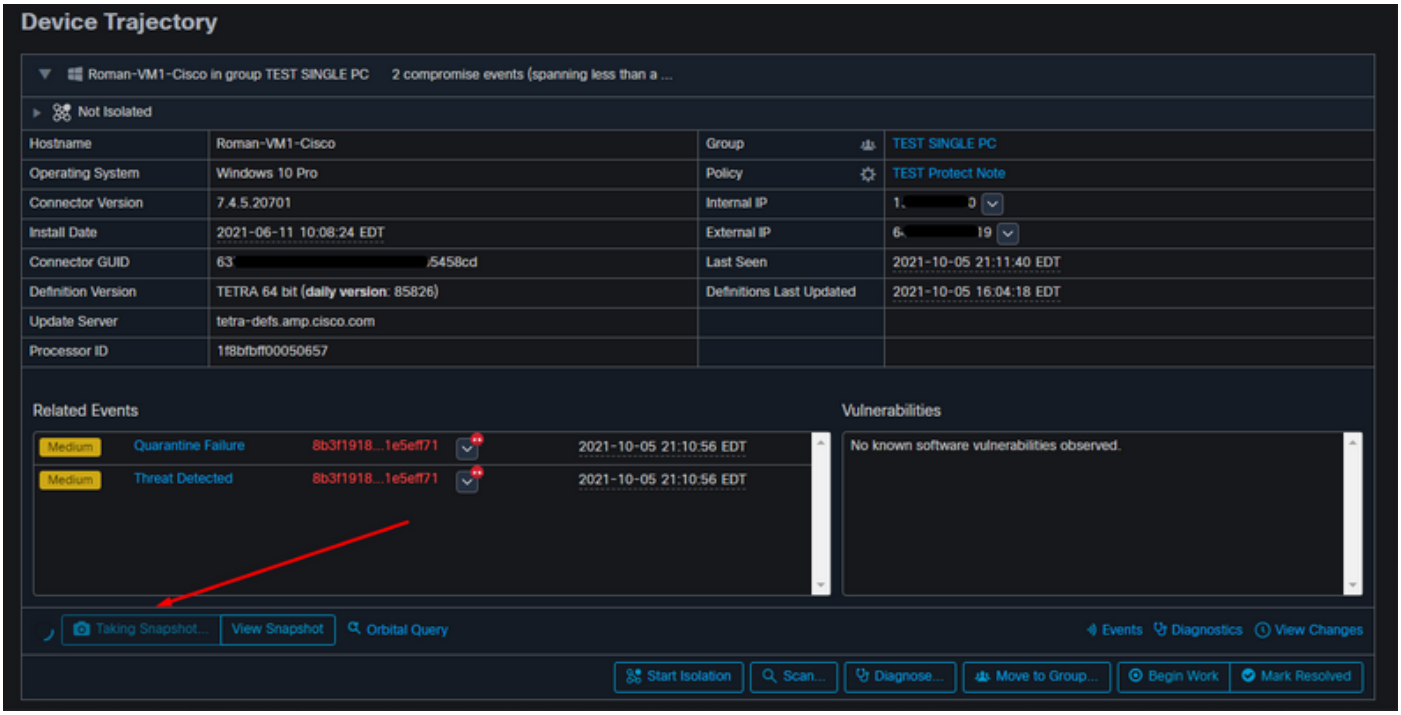
安全終端控制檯再次受到損害，如下圖所示



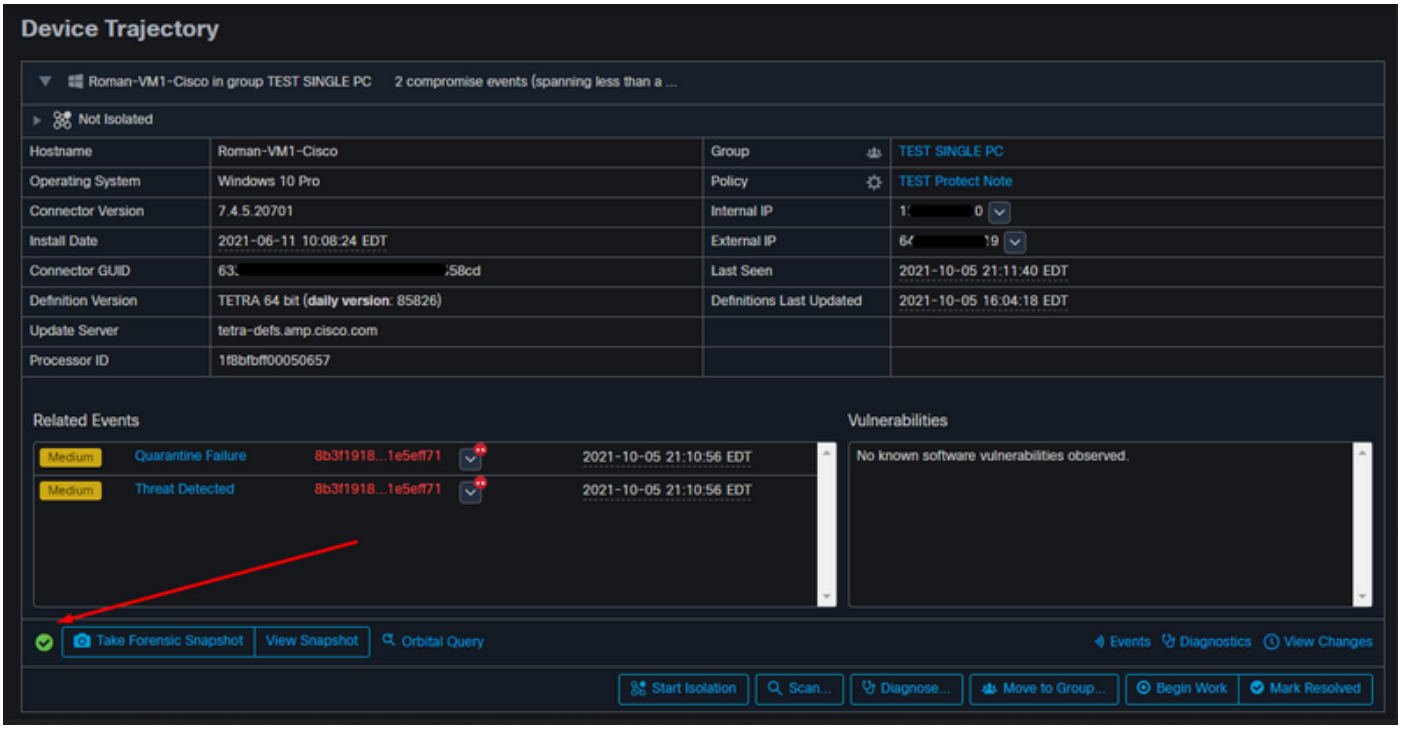
下面是「Automated Actions」下面的新事件，如下圖所示。



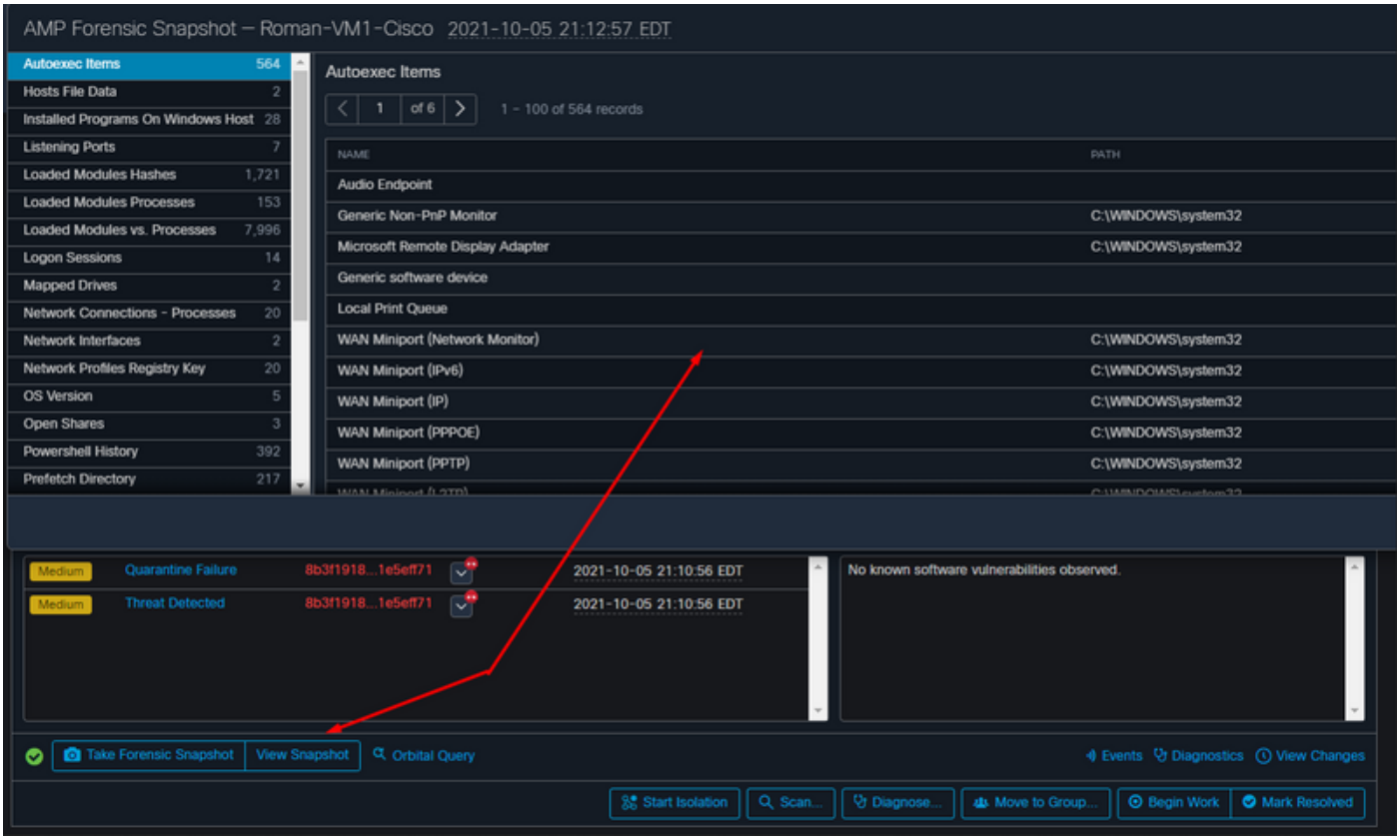
選擇「Automated Actions（自動操作）」下的主機名後，它將重定向到「Device Trajectory（裝置軌跡）」，您可以在其中觀察在展開「computer（電腦）」頁籤後建立的快照，如圖所示。



一分鐘後快照就會建立，如圖所示。



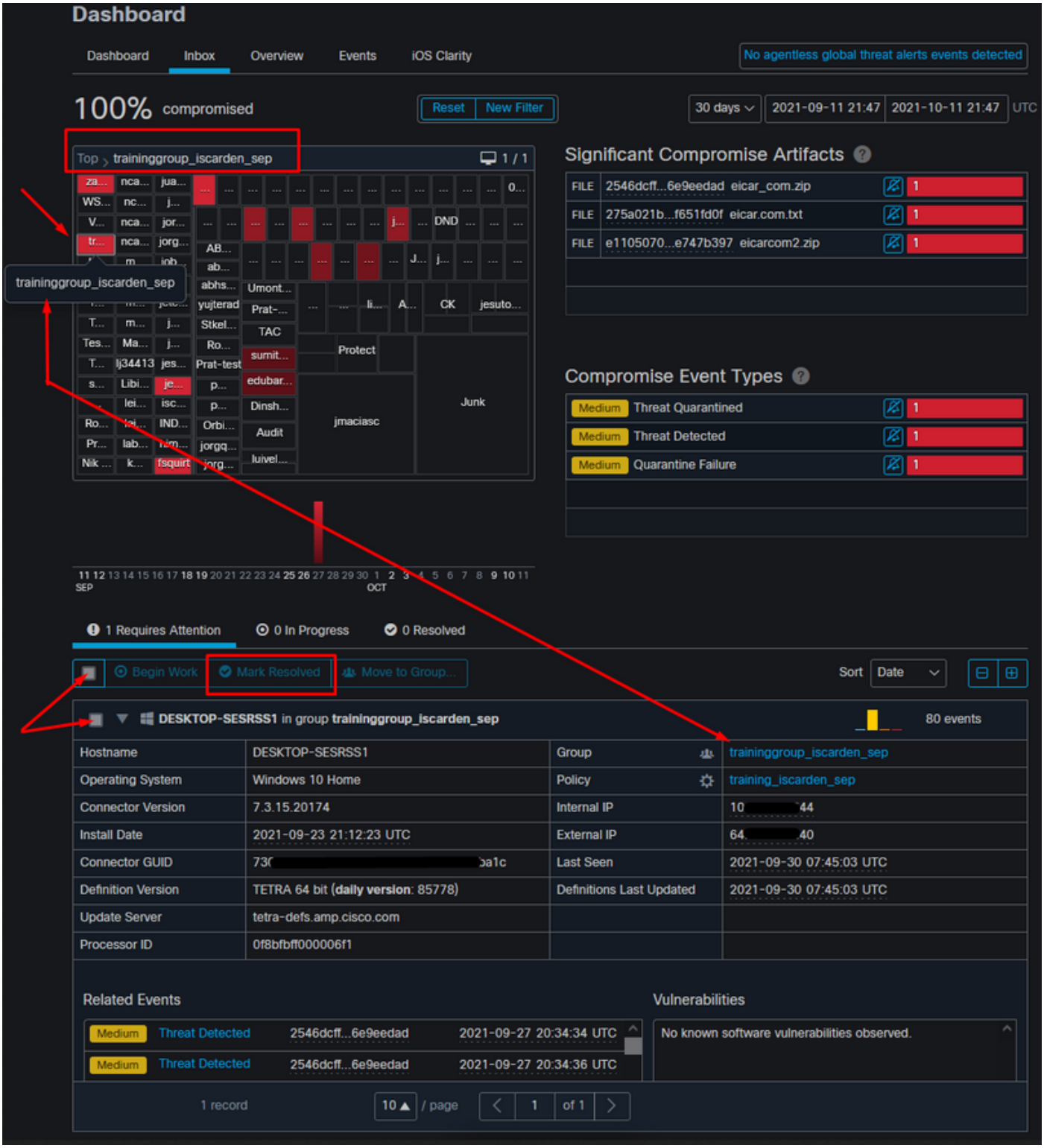
現在您可以檢視顯示的資料。



提示

在包含數千個端點且存在數百個危害的非常大型的環境中，您可能會遇到難以導航到各個端點的情況。目前，唯一可用的解決方案是使用熱度圖，然後向下鑽取到您的危害終點所在的特定組，如下例所示。

在熱度圖中選擇組後，導航到危害事件的組。由於該組中只有一個終結點，請注意目前基於我們所在的特定組的100%已洩露。換句話說，如果本組中有2個終端，則一個終端已清除，另一個受危害的終端顯示50%的危害。


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