자동 작업 - 포렌식 스냅샷

목차

소개

이 문서에서는 보안 엔드포인트의 자동화된 조치 기능이 보안 침해 개념과 연계되어 있다는 설명을 제공합니다. 자동화된 작업의 기능을 이해하는 데 보안 침해의 라이프사이클 및 관리를 이해해야 합니다. 이 문서에서는 이러한 개념의 용어 및 기능에 대한 질문에 답변합니다.

FAQ

손상된 시스템이란 무엇입니까?

손상된 시스템은 연결된 활성 보안 침해 상태의 엔드포인트입니다. 보안이 침해된 머신은 한 번에 하나의 보안 침해만 활성화할 수 있습니다.

타협이란 무엇입니까?

보안침해는 시스템에서 하나 이상의 탐지를 수집하는 것입니다. 대부분의 탐지 이벤트(Threat Detected, Indications of Compromise 등)는 보안 침해를 생성 또는 연결할 수 있습니다. 그러나 새 보안 침해를 트리거하지 않을 수 있는 이벤트 쌍이 있습니다. 예를 들어, Threat Detected 이벤트가 발생하지만 관련 Threat Quarantined 이벤트가 발생한 직후 새로운 보안 침해가 발생하지 않습니다. 논리적으로 이는 보안 엔드포인트가 잠재적인 보안 침해를 처리했기 때문입니다(위협을 격리함).

손상된 시스템에서 새 탐지가 발생할 경우 어떻게 됩니까?

탐지 이벤트가 기존 보안 침해에 추가됩니다. 새로운 보안 침해 항목이 생성되지 않습니다.

보안 침해를 어디에서 확인하고 관리할 수 있습니까?

보안 엔드포인트 콘솔의 받은 편지함 탭에서 보안 침해가 관리됩니다(북미 클라우드의 경우 https://console.amp.cisco.com/compromises). 감염된 시스템은 주의 필요 섹션 아래에 **나열되며** Mark Resolved(해결됨 **표시)**를 눌러 보안 침해를 제거할 수 있습니다. 또한 보안 침해가 한 달 후에 자동으로 해결됩니다.

자동화된 작업*은 어떻게 트리거됩니까?

보안침해되지 않은 시스템이 손상된 시스템이 될 때 자동으로 작업이 트리거됩니다. 이미 손상된 시스템에서 새로운 탐지가 발생할 경우 이 탐지가 보안 침해에 추가되지만 새로운 보안이 아니므로 자동화된 조치를 트리거하지 않습니다.

자동화된 작업을 다시 트리거하려면 어떻게 해야 합니까?

자동화된 작업을 다시 트리거하기 전에 보안 침해를 "제거"해야 합니다. Threat Detected + Threat Quarantined 이벤트로 인해 새로운 보안 침해 이벤트를 생성할 수 없으므로 새로운 자동화된 작업을 트리거할 수 없습니다.

*예외: "Submit File to ThreatGrid(ThreatGrid에 파일 제출)" 자동화 작업은 보안 침해와 관련이 없으며 탐지별로 실행됩니다.

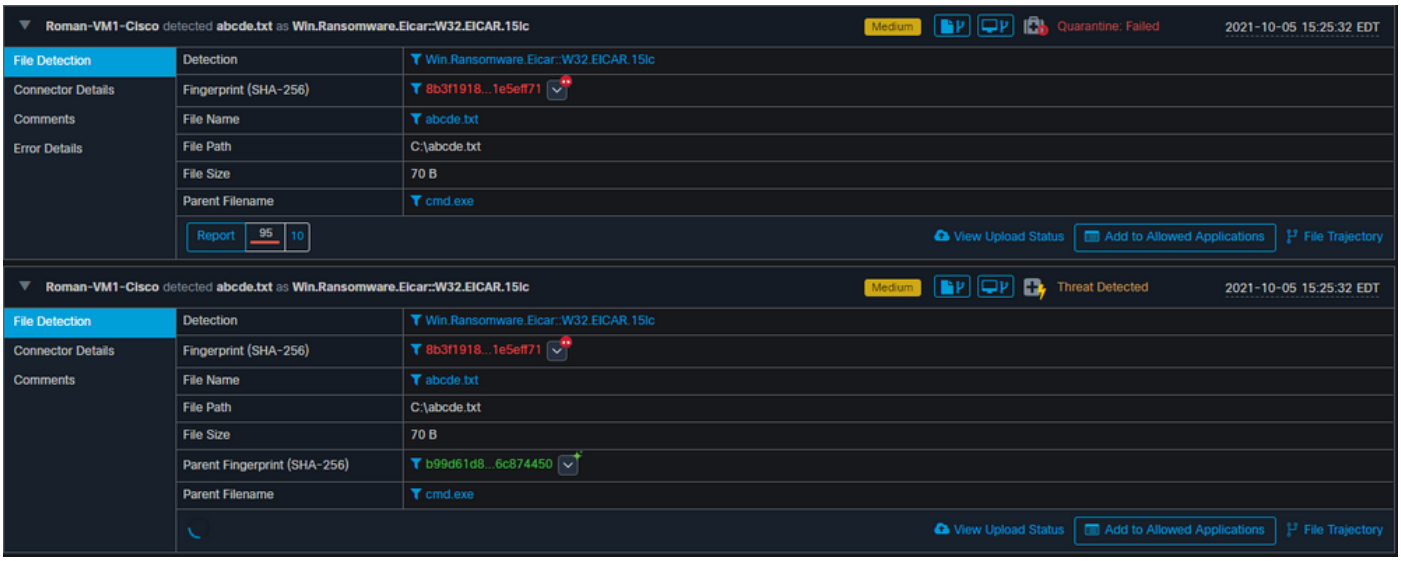
사용 사례 - Lab Recreate

#1: FAQ 섹션에서 설명한 대로 포렌식 스냅샷은 "손상"의 경우에만 촬영됩니다. 즉, TEST 사이트에서 악성 파일에 액세스하여 다운로드하려고 할 때 파일이 다운로드 시 플래그가 지정되고 격리되어 보안침해로 간주되지 않으며 작업을 트리거하지 않는 경우

> **참고:** DFC 탐지, 격리 실패, 그리고 논리로 인해 보안 침해 이벤트에 포함되는 거의 모든 것이 포렌식 스냅샷을 생성해야 합니다.

#2: 받은 편지함에서 손상된 시스템을 확인하지 않는 한 포렌식 스냅샷이 생성되지 않는 고유한 손상 이벤트에 대해서만 포렌식 스냅샷을 생성할 수 있습니다. 손상된 이벤트를 해결하지 않으면 다른 스냅샷을 생성하지 않습니다.

예: 이 Lab에서는 스크립트가 악의적인 활동을 생성하며, 파일이 생성되자마자 삭제되고 보안 엔드포인트에서 손상 범주에 속하는 파일을 격리할 수 없기 때문입니다.

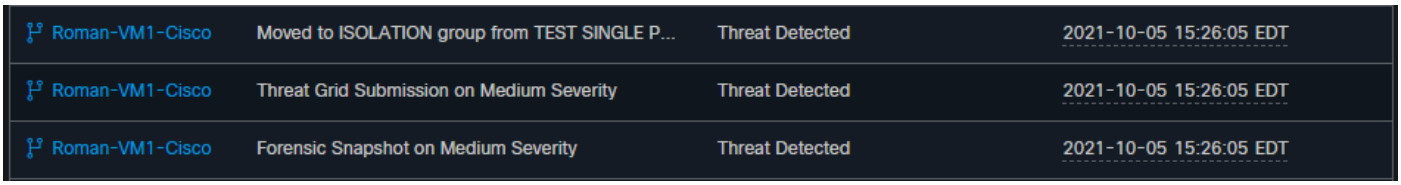


이 테스트에서는 자동화된 작업과 설정을 기반으로 발생한 3가지 사항을 확인할 수 있습니다.

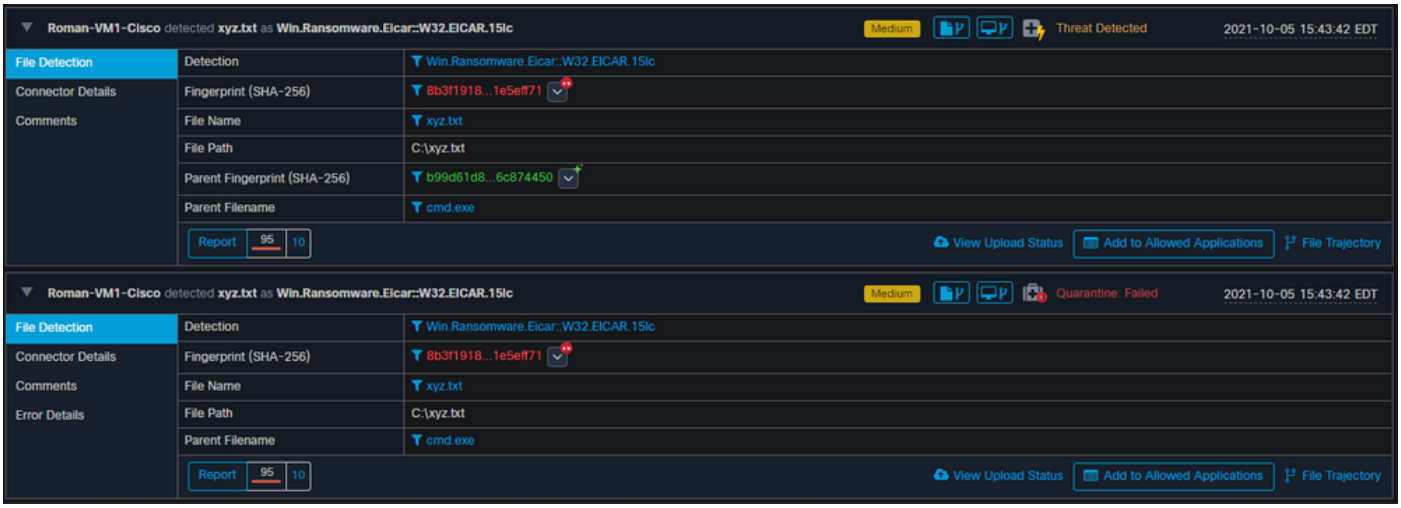
- 스냅샷이 생성되었습니다.

- TG(Threat Grid)로 제출
- 엔드포인트가 생성되어 ISOLATION이라고 하는 별도의 그룹으로 이동되었습니다.

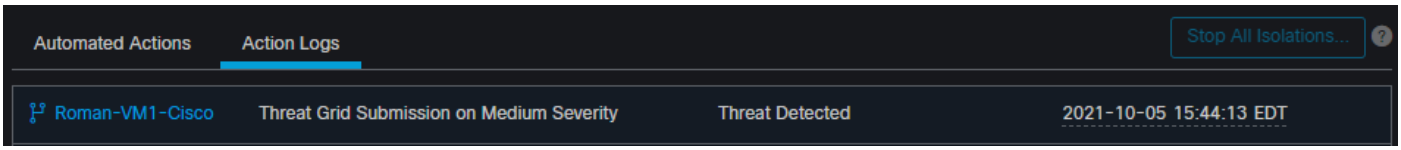
이미지에 표시된 대로 이 출력에서 모든 것을 볼 수 있습니다.



이제 이 엔드포인트가 손상되었으므로, 다음 테스트에서는 이미지에 표시된 것과 같이 유사한 악성 파일을 사용하지만 이름이 다른 이론을 입증합니다.

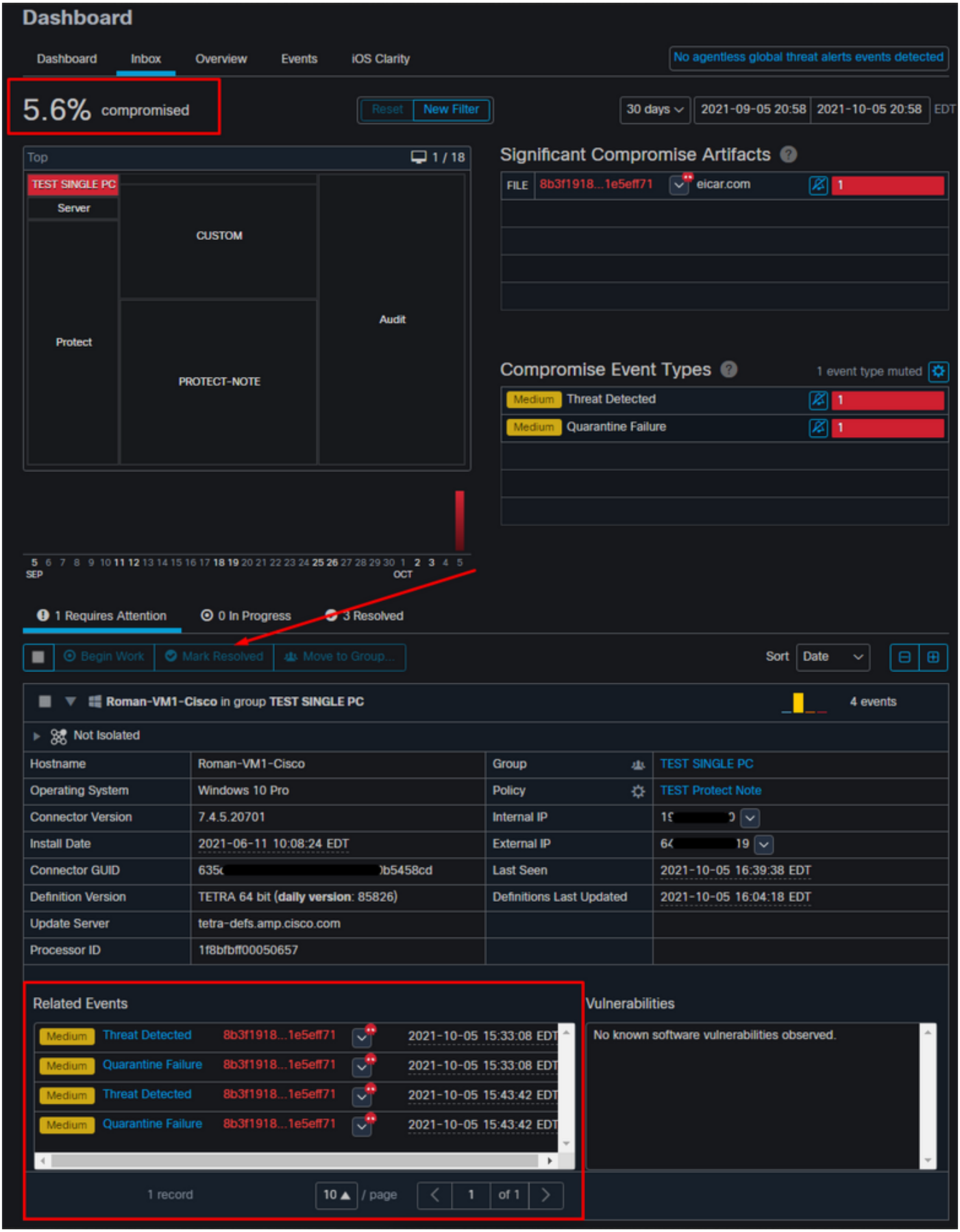


그러나 이 보안 침해 문제가 해결되지 않았으므로 TG 제출만 생성할 수 있습니다. 다른 이벤트가 기록되지 않았습니다. 이 2차 테스트 전에 격리를 해제하십시오.

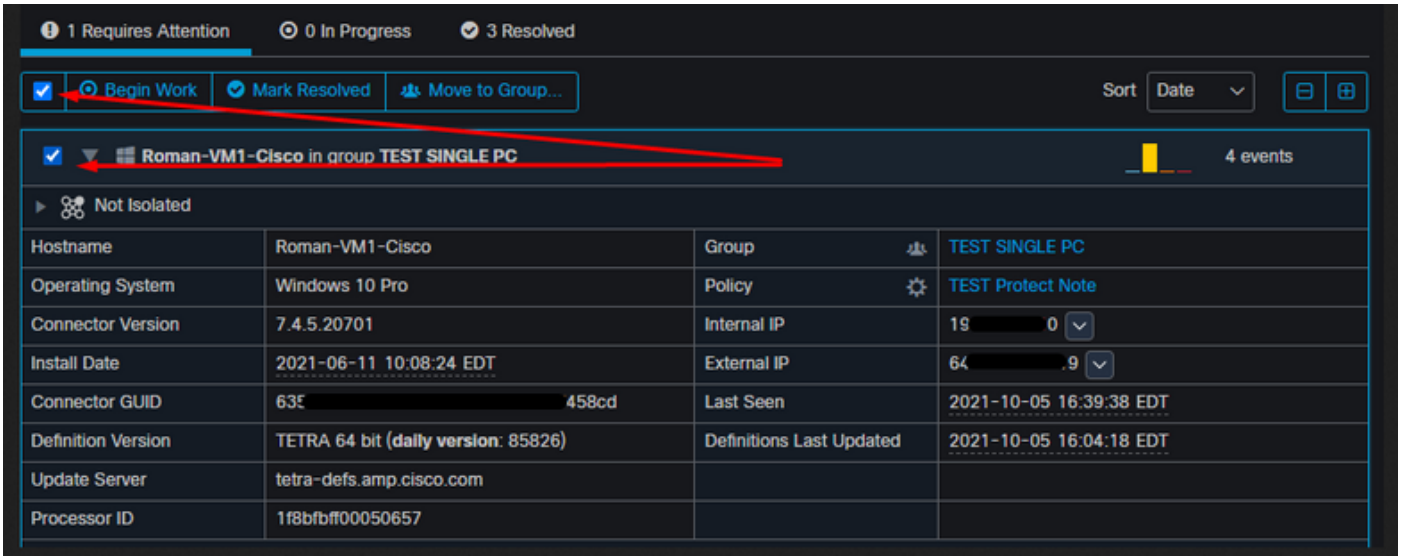


참고: 위협이 탐지되고 자동화된 작업이 트리거되는 시간을 확인하십시오.

손상된 엔드포인트가 해결되지 않으면 이벤트를 검색할 수 없습니다. 이 경우 대시보드는 다음과 같습니다. 감염된 이벤트와 함께 Mark Resolved(해결됨 표시) 버튼 및 백분율을 확인하십시오. 트리거되는 이벤트 수에 관계없이 하나의 스냅샷만 생성할 수 있으며, 큰 비율 수는 변경되지 않습니다. 이 수는 조직 내부의 보안 침해를 나타내며 조직의 총 엔드포인트 수를 기반으로 합니다. 다른 감염된 시스템에서만 변경됩니다. 이 예에서는 Lab에서 16개의 디바이스로 인해 숫자가 높습니다. 또한 보안 침해 이벤트는 31일이 지나면 자동으로 지워집니다.

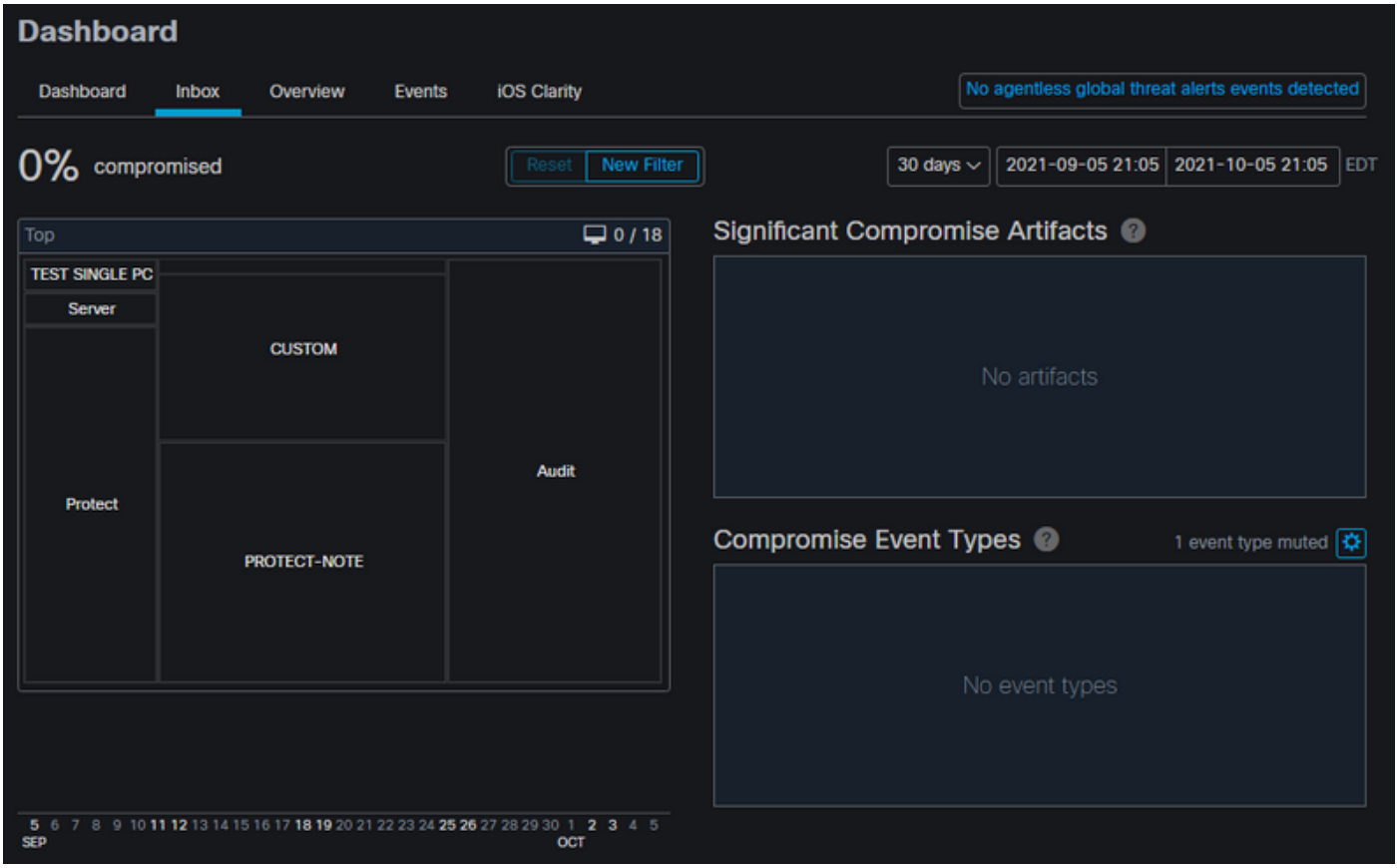


다음 단계는 다른 이벤트를 생성하고 포렌식 스냅샷을 생성하는 것입니다. 첫 번째 단계는 이 보안 침해를 해결하는 것입니다. Mark Resolved(해결됨 **표시**) 버튼을 클릭합니다. 엔드포인트별로 수행할 수도 있고 조직 내 모든 것을 선택할 수도 있습니다.

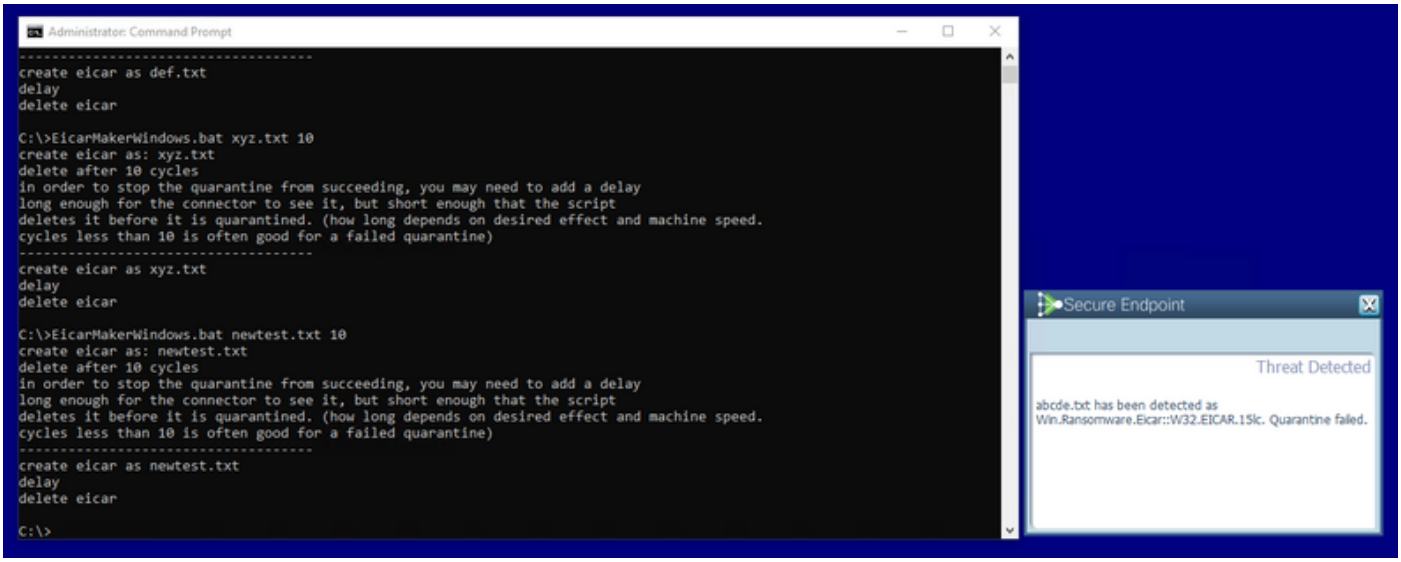


참고: 모든 보안 침해를 선택하면 0%로 재설정됩니다.

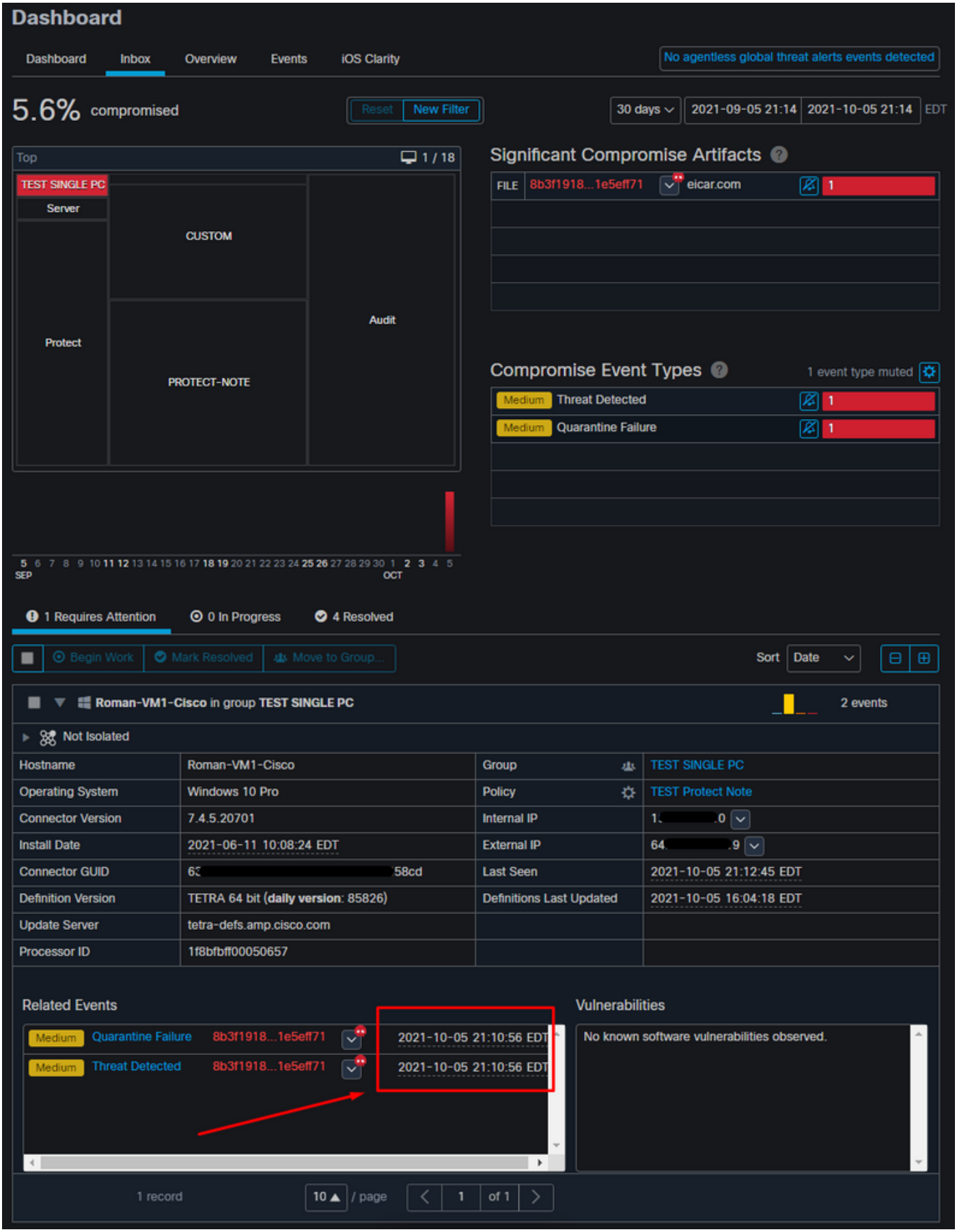
Mark Resolved(해결됨 표시) 버튼이 선택되고 Secure Endpoint(보안 엔드포인트) 대시보드에서 엔드포인트가 하나만 감염되었으므로 이 모양입니다. 그리고 이 시점에서 테스트 머신에서 새로운 감염 이벤트가 트리거되었습니다.



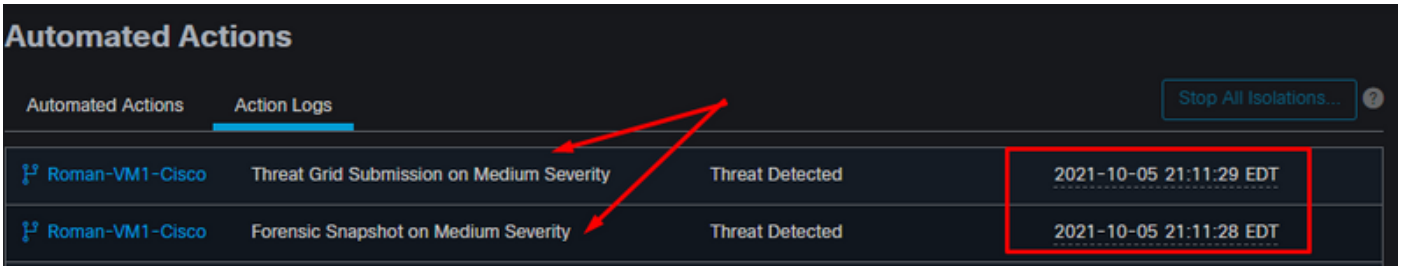
다음 예에서는 악성 파일을 만들고 삭제하는 사용자 지정 스크립트를 사용하여 이벤트를 트리거합니다.



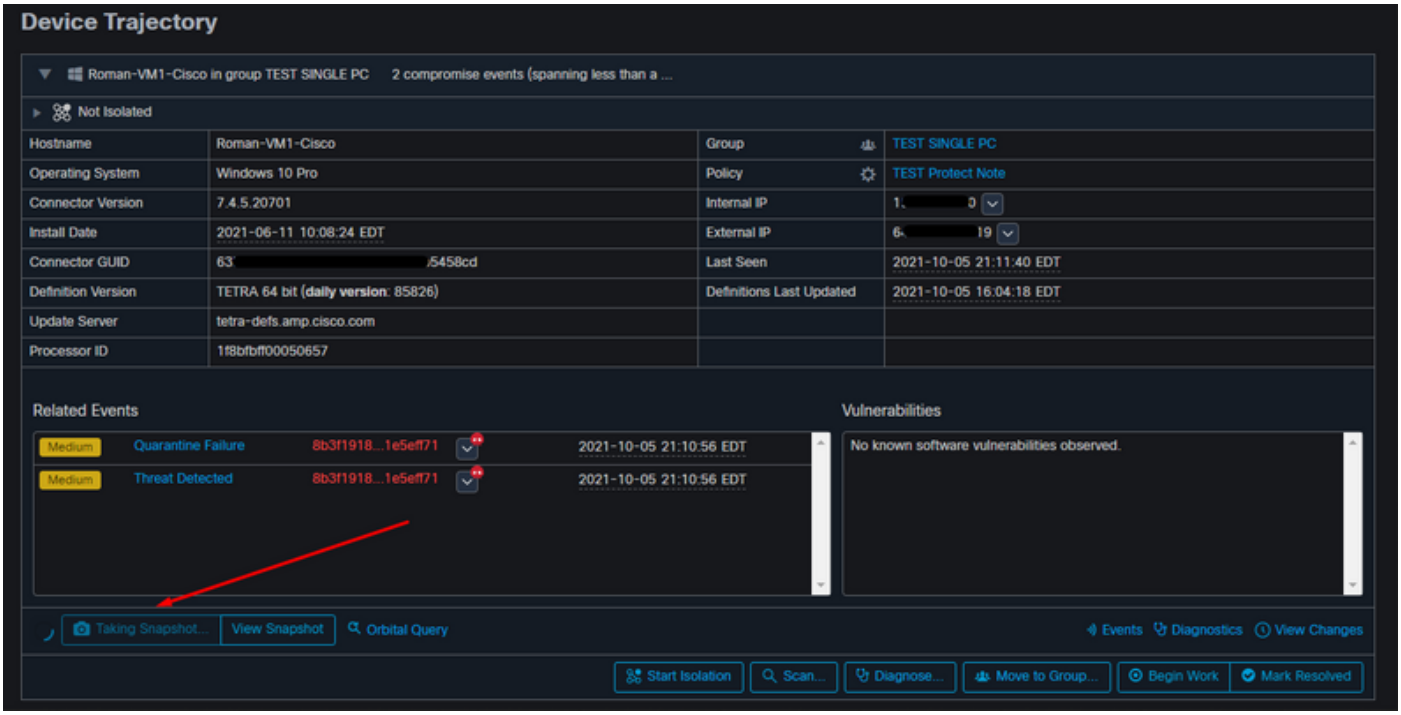
이미지에 표시된 대로 보안 엔드포인트 콘솔이 다시 한번 손상됨



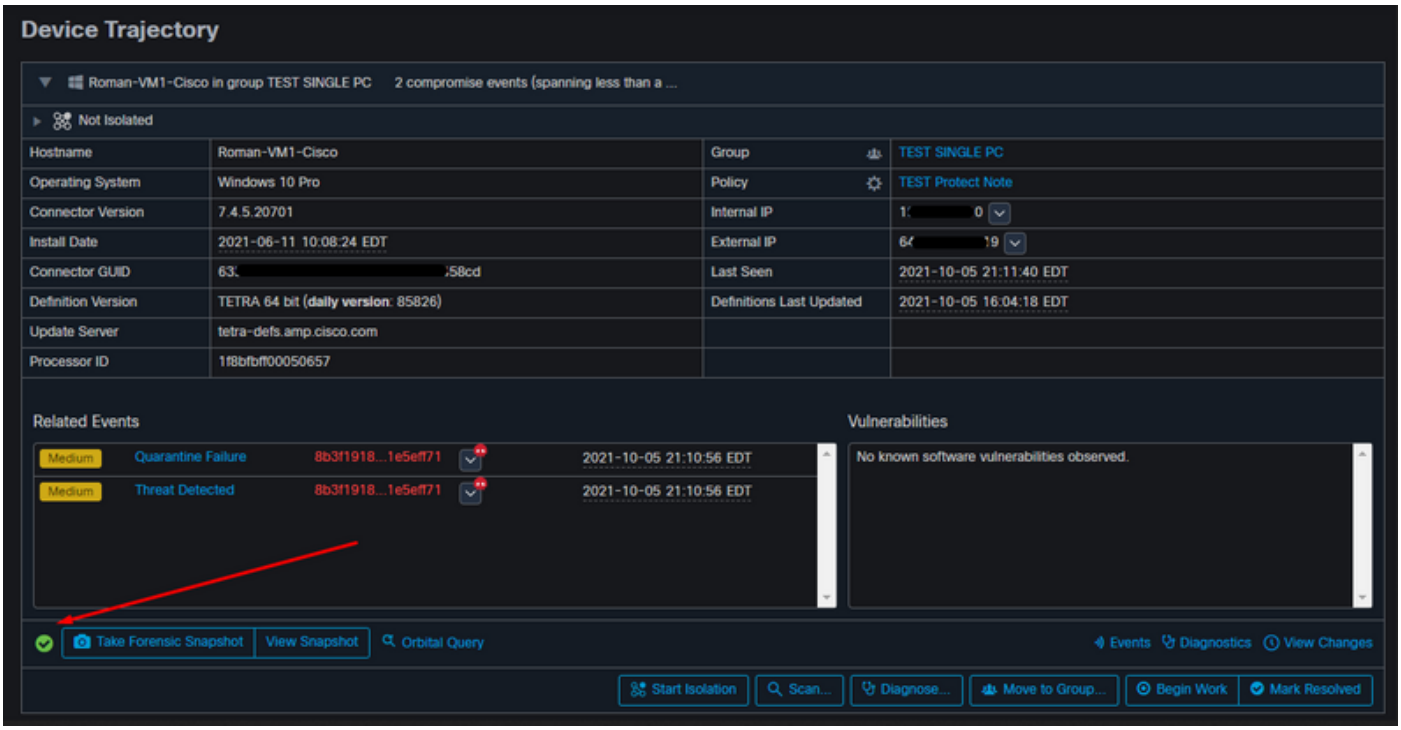
이미지에 표시된 대로 Automated Actions(자동 작업) 아래에 새 이벤트가 있습니다.



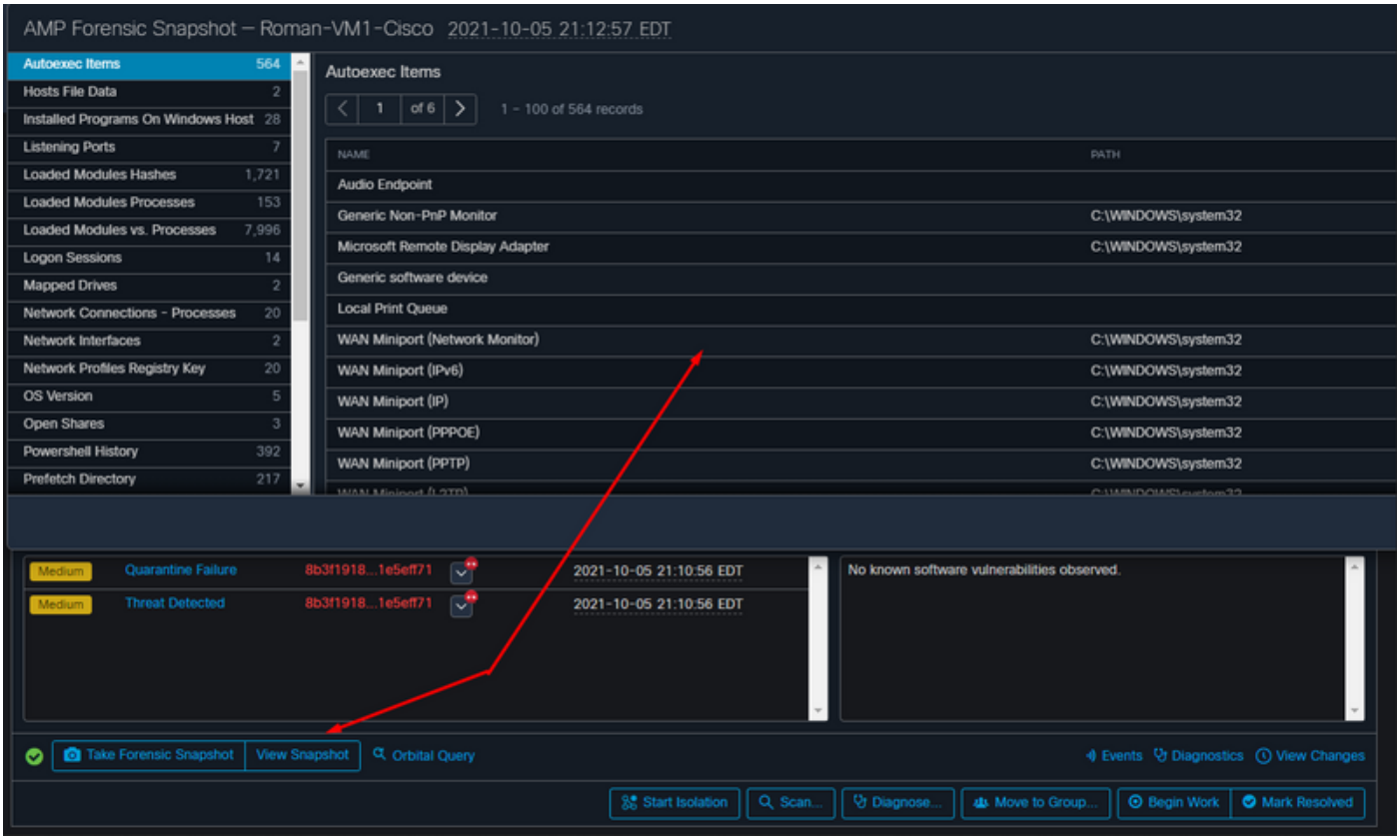
Automated Actions(자동 작업) 아래의 호스트 이름을 선택하면 이미지에 표시된 대로 컴퓨터 탭을 확장하면 생성되는 스냅샷을 관찰할 수 있는 Device Trajectory(디바이스 전파 흔적 분석)로 리디렉션됩니다.



그리고 1분 후에 이미지에 표시된 대로 스냅샷이 생성됩니다.



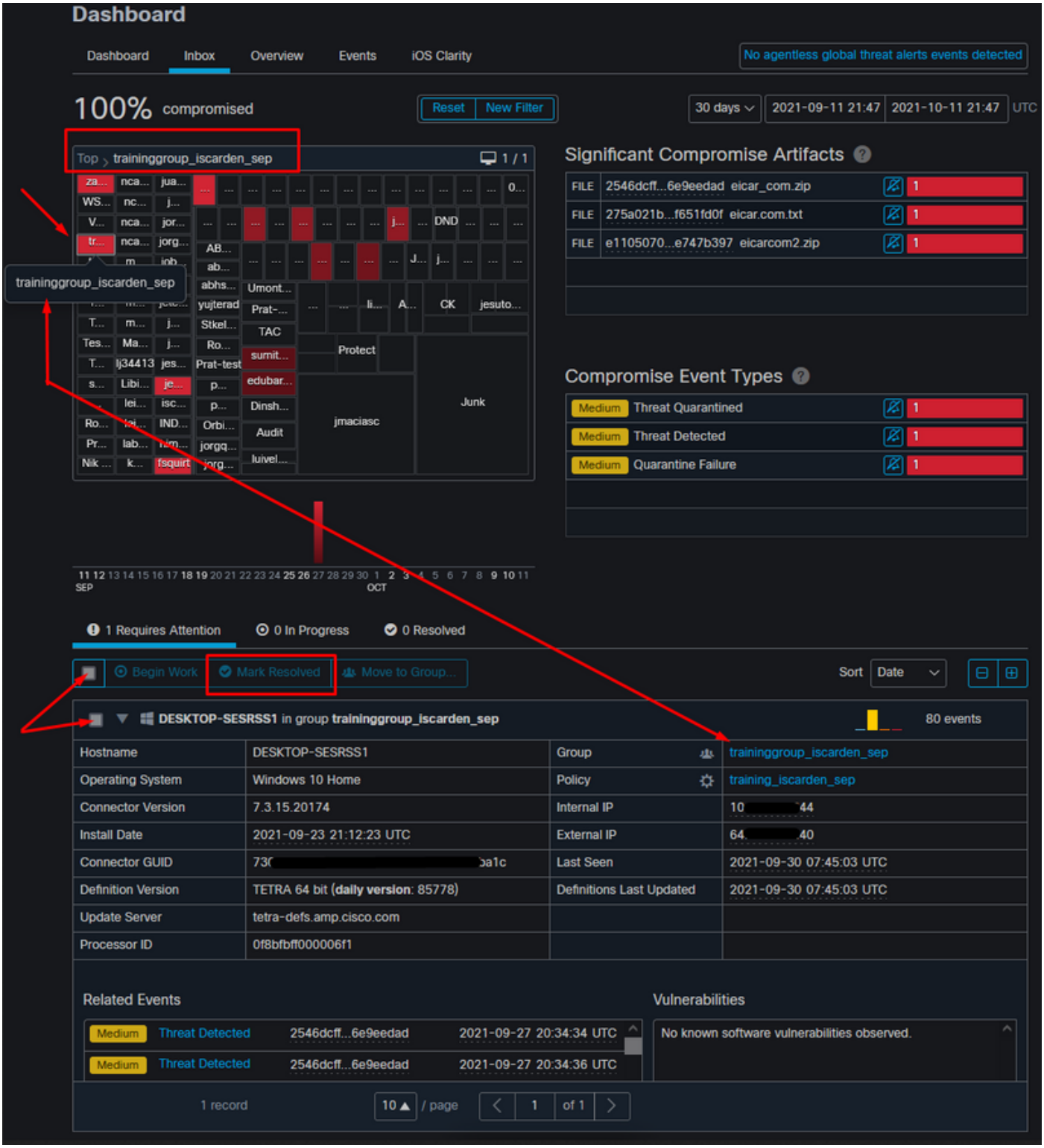
이제 표시된 데이터를 볼 수 있습니다.



팁

수천 개의 엔드포인트와 수백 개의 보안 침해가 있는 매우 큰 환경에서는 개별 엔드포인트로의 탐색이 문제가 될 수 있는 상황에 처할 수 있습니다. 현재 사용 가능한 유일한 솔루션은 히트맵을 사용한 다음 아래 예와 같이 보안 침해 엔드포인트가 있는 특정 그룹으로 드릴다운하는 것입니다.

히트 맵에서 그룹이 선택되면 이벤트를 감염시킨 그룹으로 이동합니다. 해당 그룹에 엔드포인트가 하나뿐이므로 100% 보안이 침해된 것은 현재 Cisco가 속한 특정 그룹을 기반으로 합니다. 다시 말해, 이 그룹에 엔드포인트가 2개인 경우 하나는 깨끗하며 다른 하나는 손상된 것으로 50%가 감염됩니다.


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