自動化されたアクション：フォレンジックスナップショット

内容

概要

このドキュメントでは、セキュアエンドポイントの自動アクション機能をCompromisesの概念に関連付けて説明します。 自動化されたアクションの機能を理解するには、妥協のライフサイクルと管理が不可欠であることを理解する。この記事では、これらの概念の用語と機能に関する質問に回答します。

FAQ

感染したマシンとは何ですか。

侵害されたマシンは、アクティブな侵害が関連付けられているエンドポイントです。侵害されたマシンは、設計上、一度に1つの侵害しかアクティブにすることができません。

侵害とは何ですか。

侵害とは、マシン上の1つ以上の検出の集合です。ほとんどの検出イベント（Threat Detected、Indications of Compromiseなど）は、侵害を生成または関連付けることができます。ただし、新しい侵害を引き起こさない可能性があるイベントのペアがあります。たとえば、Threat Detectedイベントが発生しても、関連するThreat Quarantinedイベントが発生した直後は、新しい侵害は発生しません。論理的には、これは、セキュアエンドポイントが潜在的な侵害を処理したためです（脅威を隔離しました）。

侵害されたマシンで新しい検出が発生するとどうなりますか。

検出イベントが既存の侵害に追加されます。新しい妥協は作成されません。

妥協はどこで見て管理できますか。

セキュリティで保護されたエンドポイントコンソールの[受信トレイ]タブ(北米クラウド用[の](https://console.amp.cisco.com/compromises)
https://console.amp.cisco.com/compromises)でセキュリティ侵害を管理します。侵害されたマシンは「注意が必要」セクション**に表示され**、「解決済みのマーク」を押して侵入を**クリアできます**。また、1か月後には契約内容が自動的にクリアされます。

自動アクション*はどのようにトリガーされますか。

不正なマシンが不正なマシンになった場合に発生する侵入によって、自動アクションがトリガーされます。すでに侵害されているマシンで新しい検出が検出された場合、この検出は侵害に追加されますが、これは新しい侵害ではないため、自動アクションはトリガーされません。

自動アクションを再トリガーするにはどうすればよいですか。

自動アクションを再トリガーする前に、侵害を「クリア」する必要があります。Threat Detected + Threat Quarantinedイベントは、新しい侵害イベントを生成するには不十分です（したがって、新しい自動アクションをトリガーするには不十分です）。

*例外：「Submit File to ThreatGrid」自動化アクションは、セキュリティ侵害とは無関係であり、検出ごとに実行されます

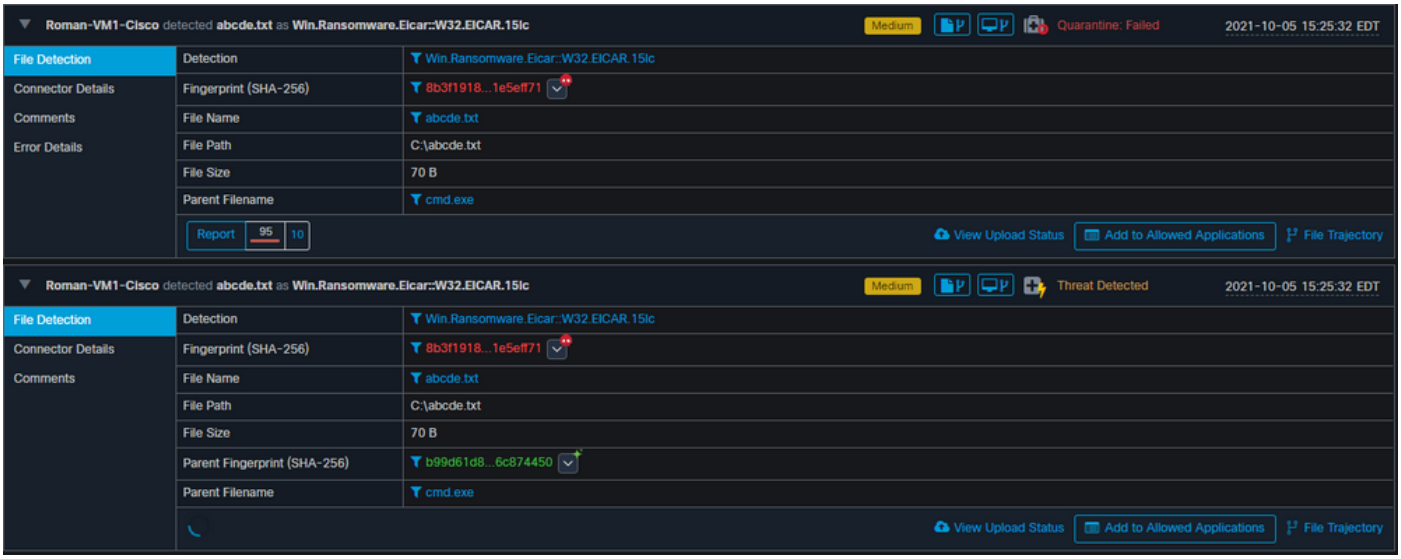
使用例：ラボ再現

#1:FAQセクションで述べたように。フォレンジックスナップショットは、「侵害」の場合にのみ取得されます。つまり、TESTサイトから悪意のあるファイルにアクセスしてダウンロードしようとすると、そのファイルはダウンロードと隔離の際にフラグが付けられ、侵害とは見なされず、アクションはトリガーされません。

> **注**：DFC検出、検疫障害、およびロジックによって侵害イベントのカテゴリに分類されるほとんどすべての情報がフォレンジックスナップショットを作成します。

#2:フォレンジックスナップショットを生成できるのは、受信箱で感染したマシンを解決しない限り、固有の侵害されたイベントではスナップショットを生成しません。侵害されたイベントを解決しない場合、他のスナップショットは生成されません。

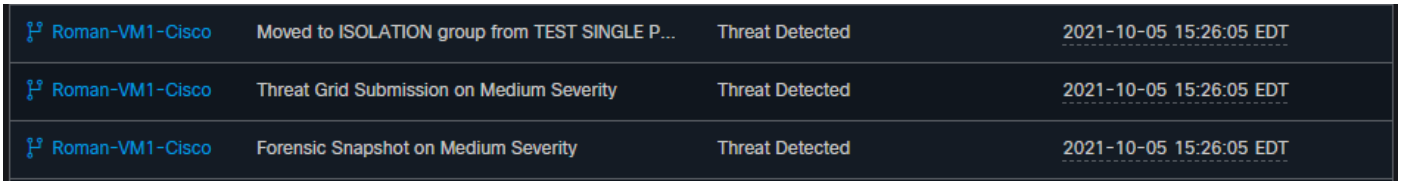
例：この実習では、スクリプトが悪意のあるアクティビティを生成します。ファイルが作成されるとすぐに削除され、セキュアエンドポイントが侵入カテゴリに分類されたファイルを検疫できなかったためです。



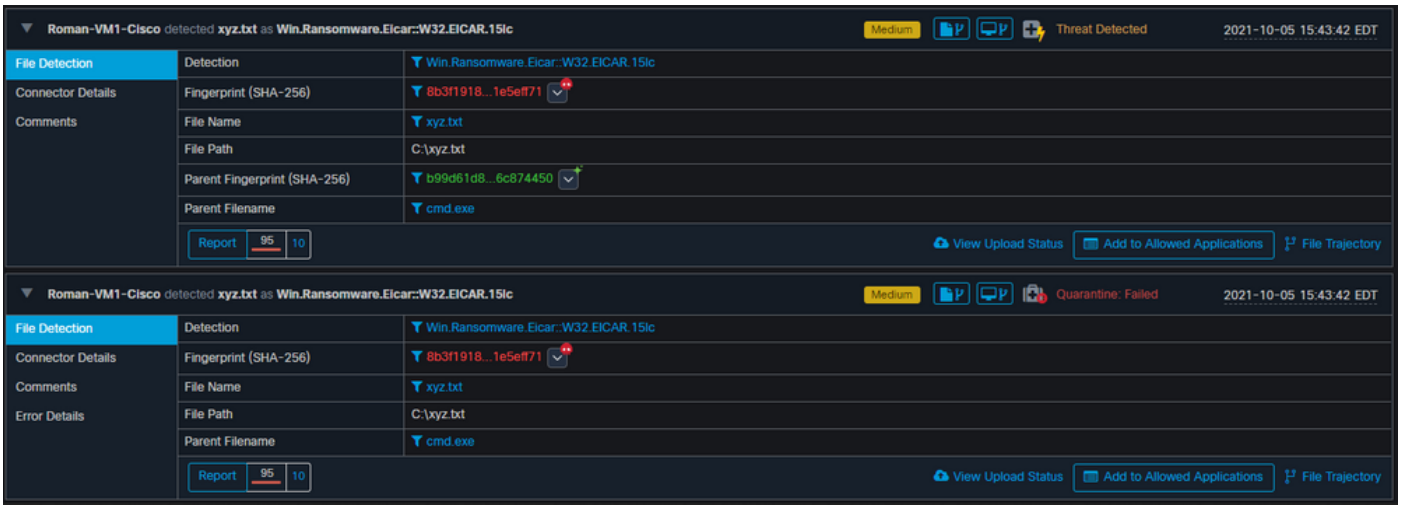
このテストでは、自動アクションと、設定に基づいて発生した3つのことを確認できます。

- スナップショットが作成されました
- 送信はThreat Grid(TG)に送信されました
- エンドポイントは、作成され、ISOLATIONと呼ばれる別のグループに移動されました

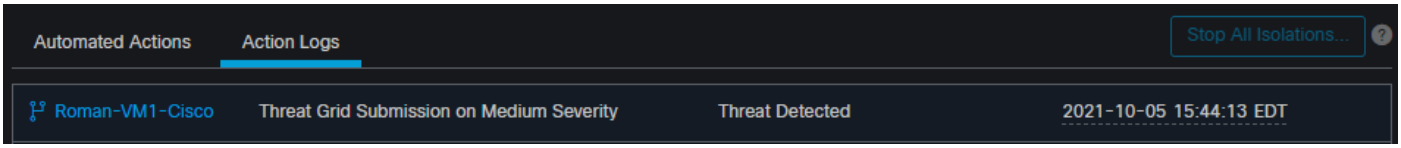
図に示すように、この出力では、これらすべてを確認できます。



このエンドポイントが侵害されたため、次のテストでは、図に示すように、類似の悪意のあるファイルが異なる名前の理論を証明します。



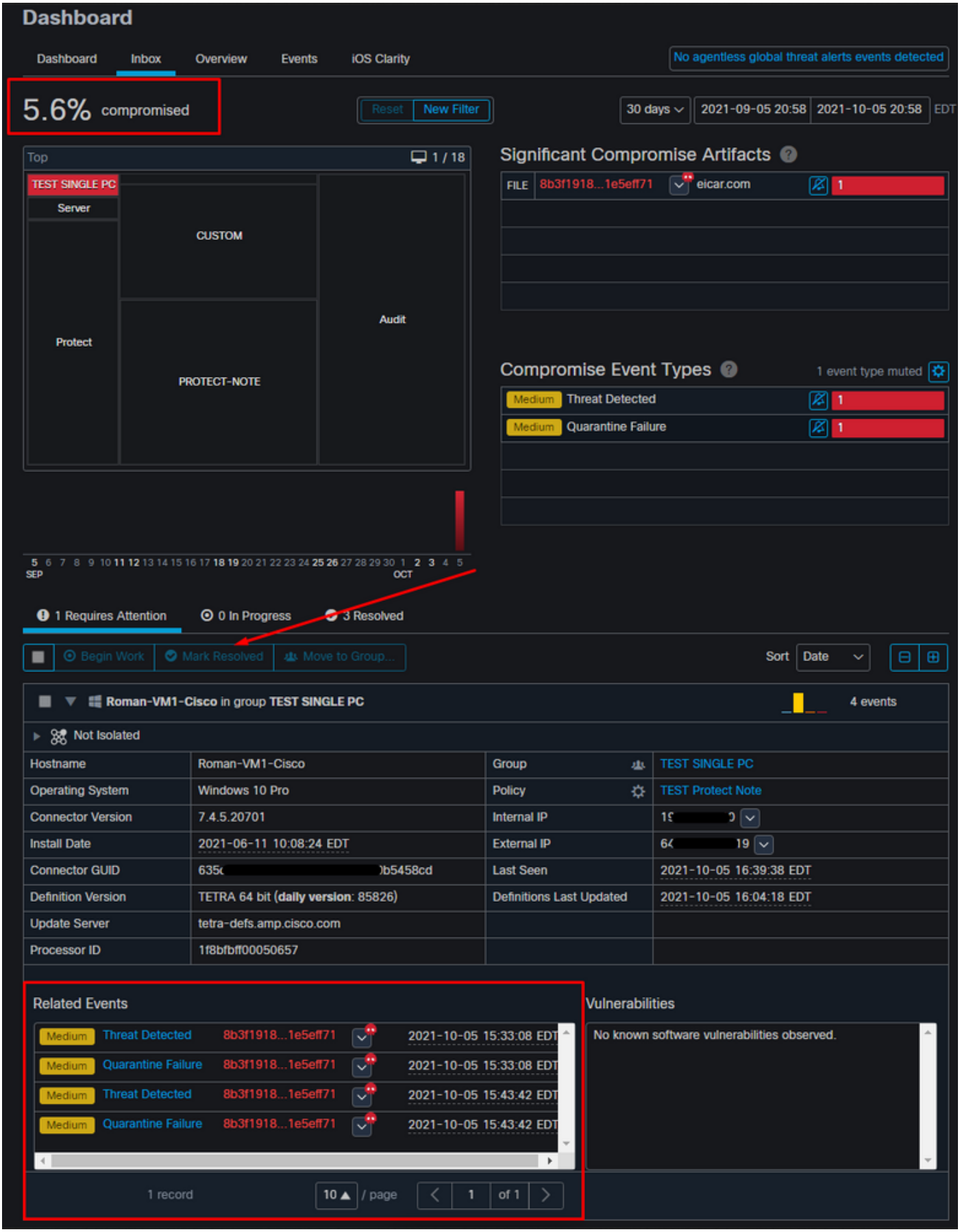
ただし、この侵害は解決されていないため、TG送信を作成することしかできません。その他のイベントは記録されず、この2回目のテストの前に[Isolation]もオフにしてください。



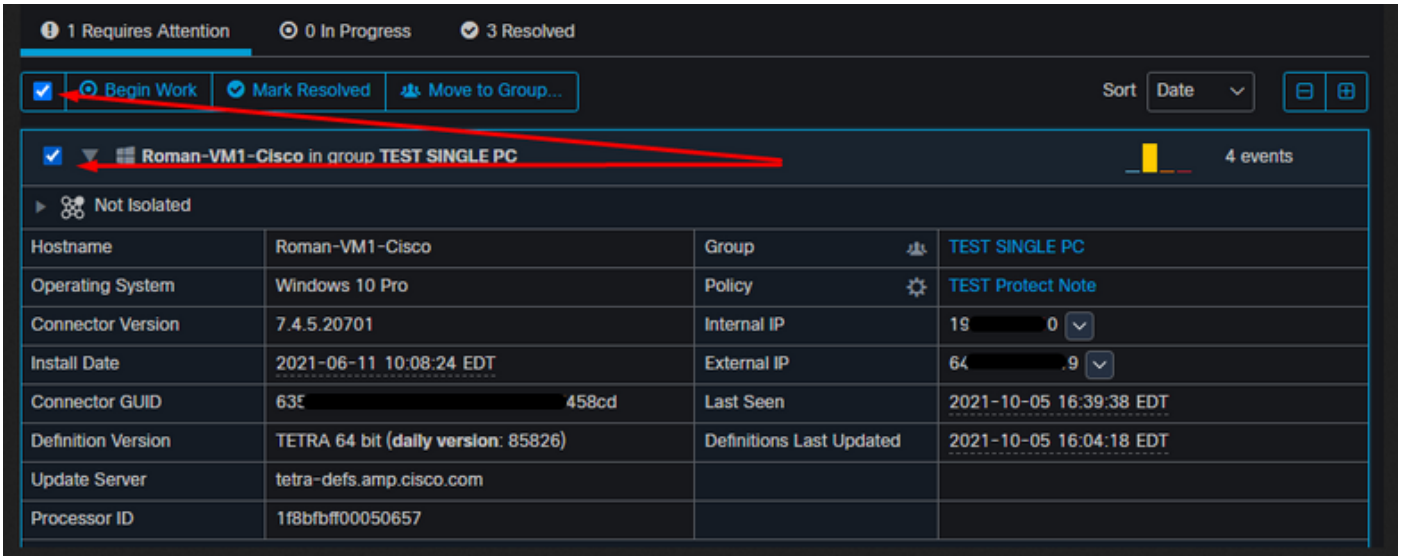
注：脅威が検出された時刻と自動アクショントリガーに注目してください。

侵害されたエンドポイントが解決されない限り、イベントを取得できません。この場合、ダッシ

ュボードは次のようになります。パーセンテージと[Mark Resolved]ボタンに、侵害されたイベントが表示されます。トリガーされるイベントの数に関係なく、1つのスナップショットのみを作成でき、大きなパーセンテージの数は変更されません。この数値は組織内のセキュリティ侵害を表し、組織内のエンドポイントの総量に基づいています。他の感染したマシンでのみ変更されます。この例では、ラボ内のデバイスが16台だけであるため、この数は多くなっています。また、侵入イベントは31日に達すると自動的にクリアされることに注意してください。

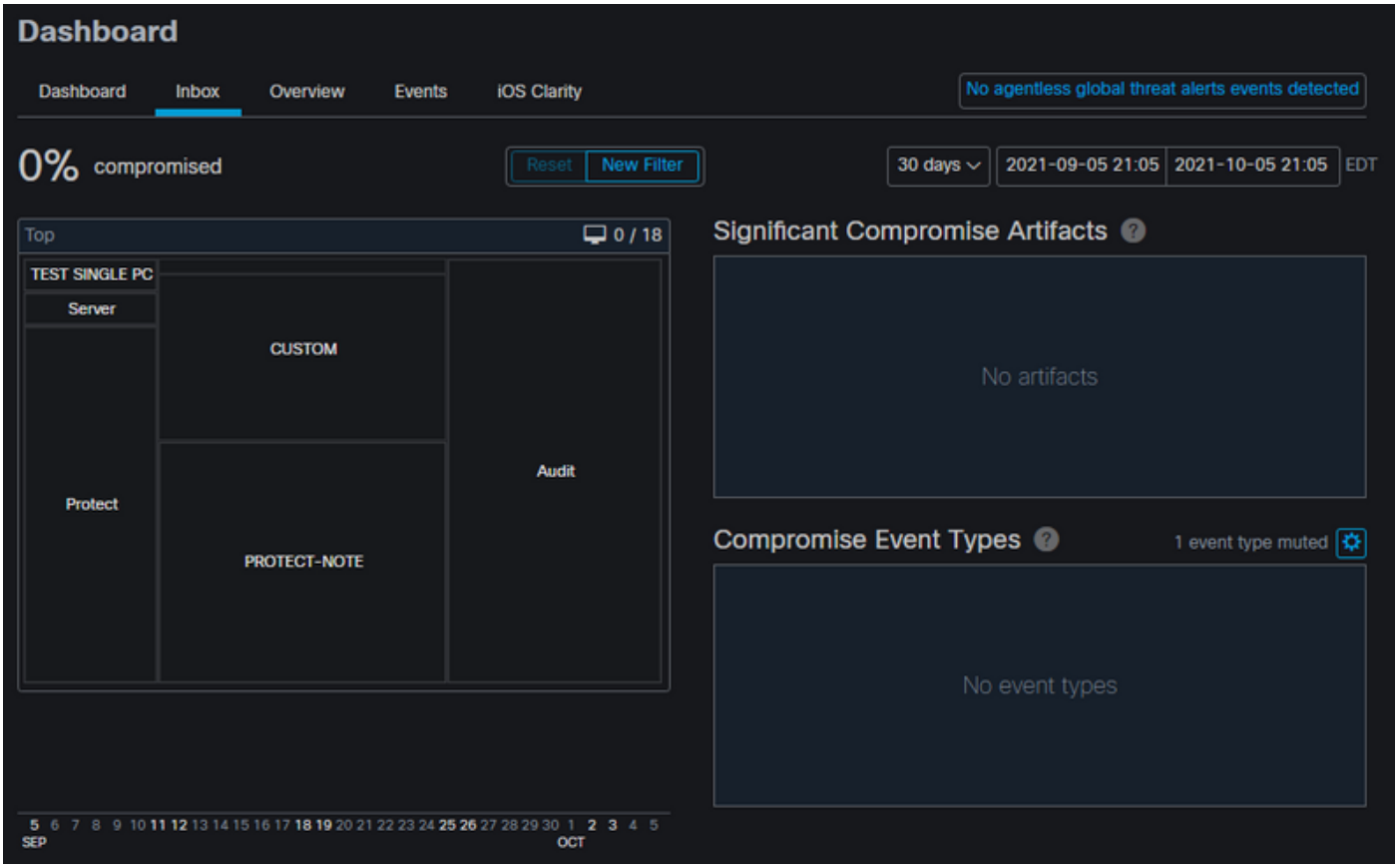


次のステップは、別のイベントを作成し、フォレンジックスナップショットを生成することです。最初のステップでは、この侵害を解決し、[Mark Resolved]ボタン**をクリック**します。エンドポイントごとに行うことも、組織内のすべての項目を選択することもできます。

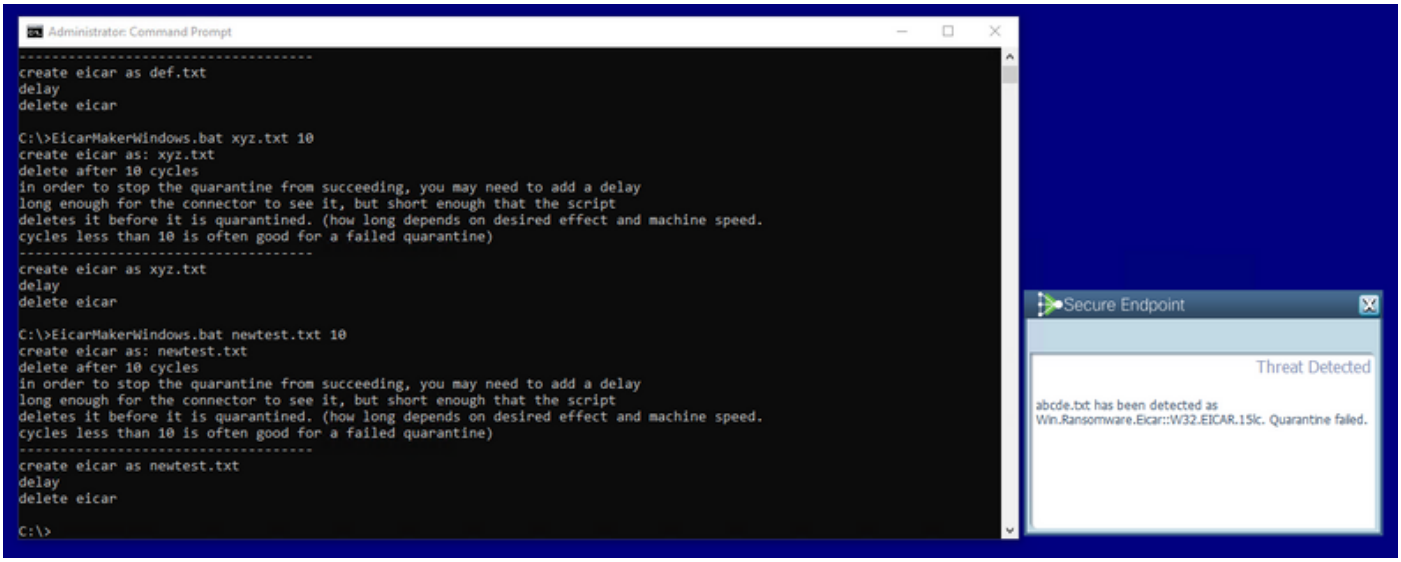


注： すべての妥協を選択すると、0 %にリセットされます。

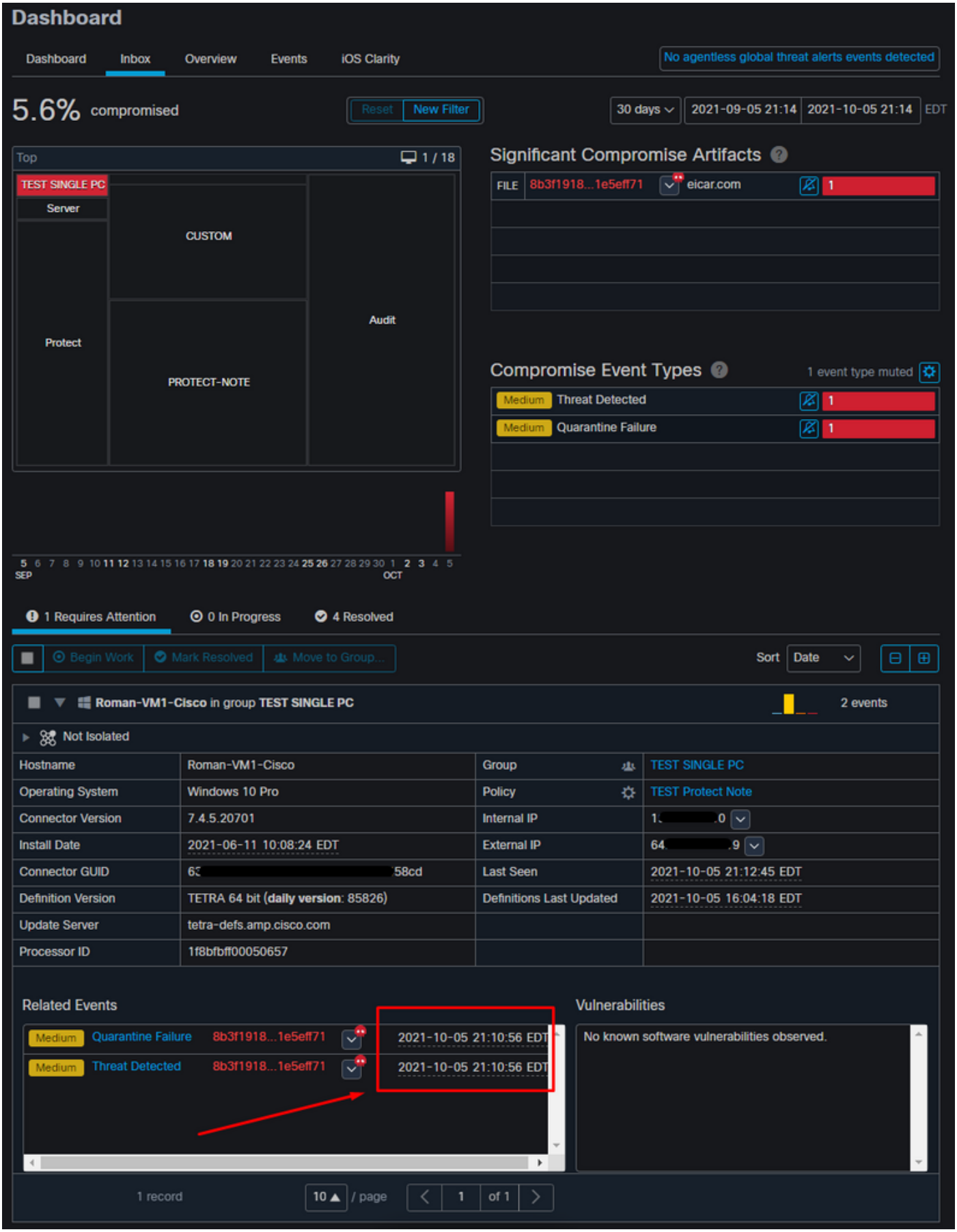
[解決済みのマーク(Mark Resolved)]ボタンを選択すると、セキュアエンドポイントダッシュボードで1つのエンドポイントだけが侵害されたため、次のようになります。この時点で、テストマシン上で新しい侵害イベントがトリガーされました。



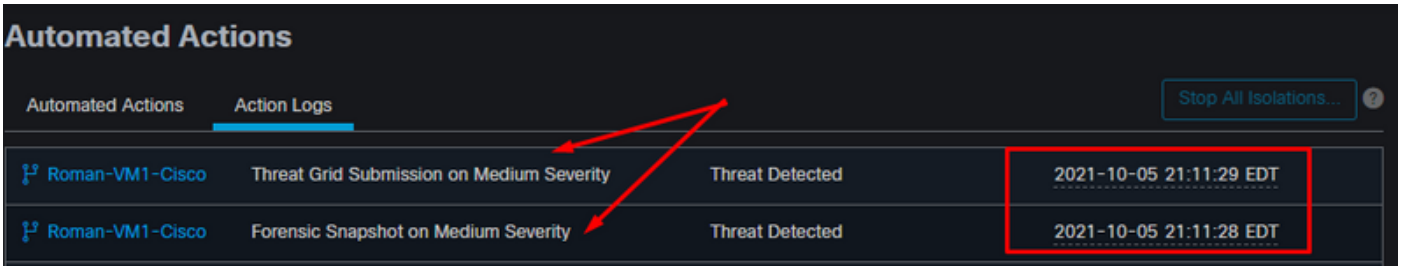
次の例は、悪意のあるファイルを作成および削除するカスタムスクリプトを使用してイベントをトリガーします。



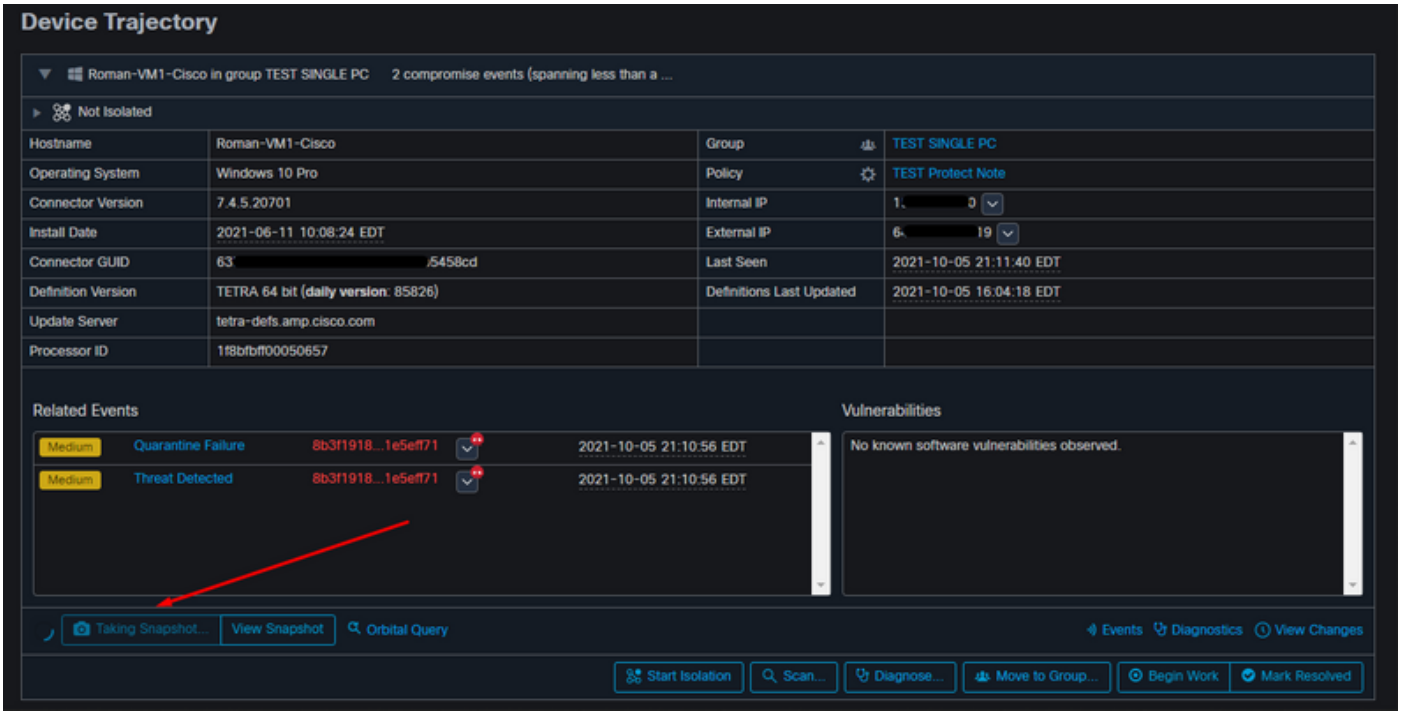
図に示すように、Secure Endpointコンソールが再度侵害されました



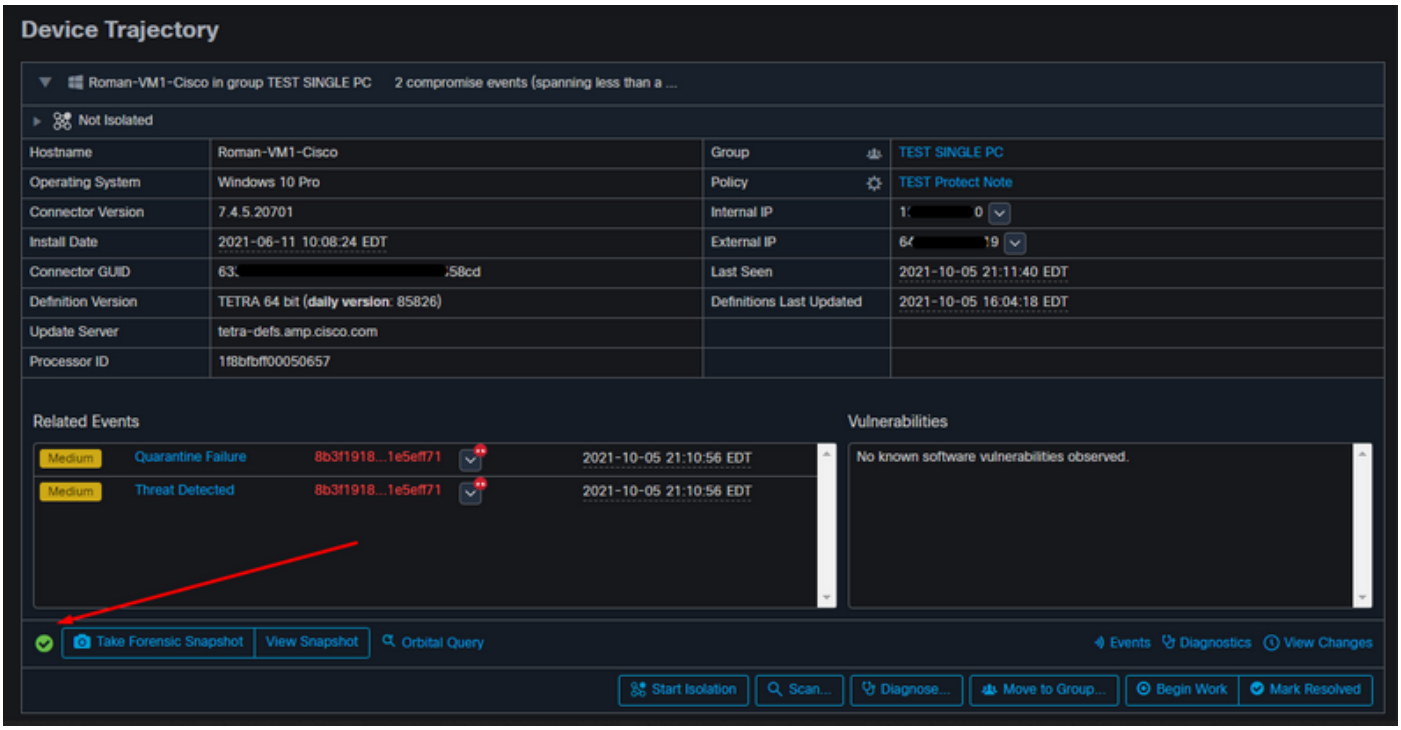
図に示すように、[Automated Actions]の下に新しいイベントがあります。



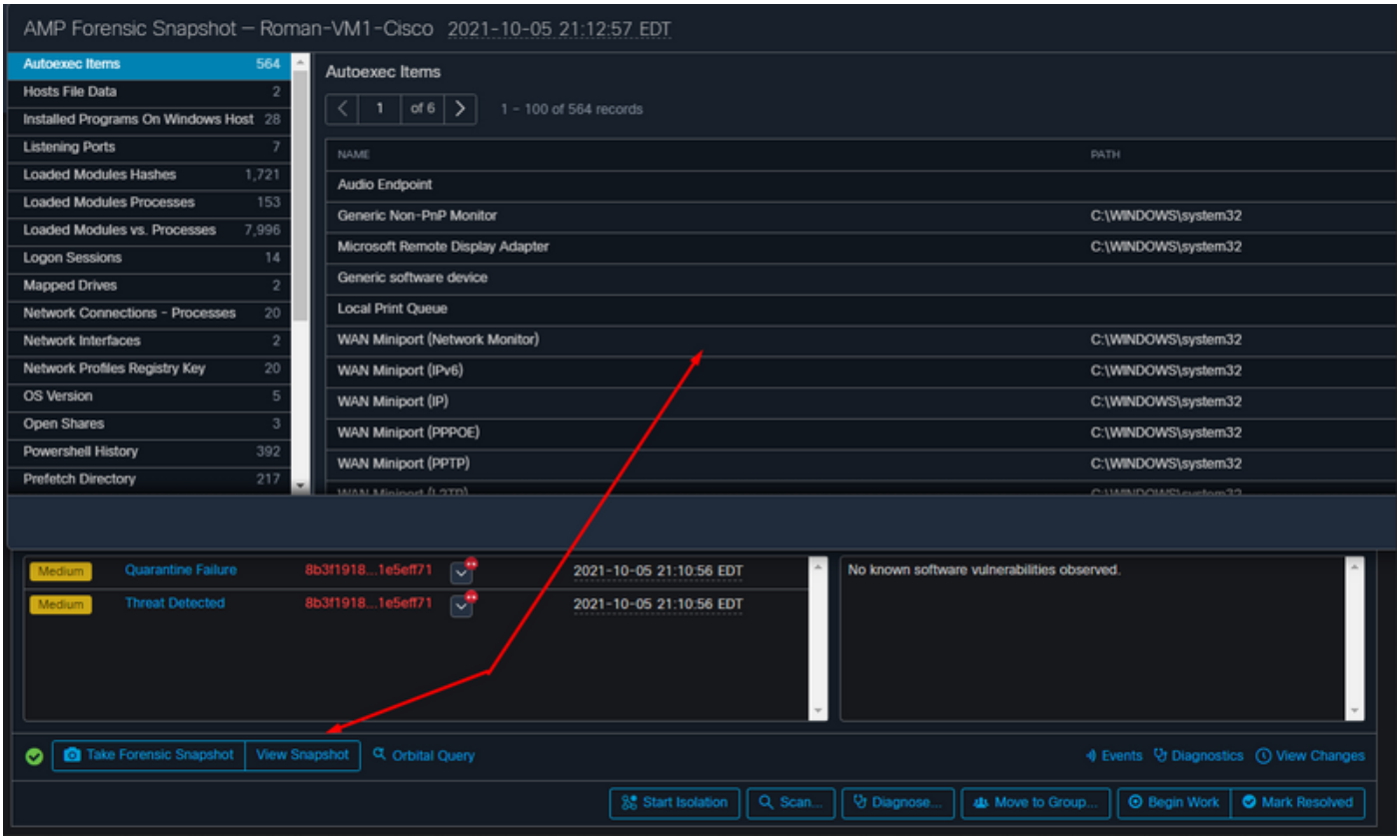
[自動アクション(Automated Actions)]の下のホスト名を選択すると、[デバイストラジェクトリー(Device Trajectory)]にリダイレクトされます。この図に示すように、[コンピュータ(Computer)]タブを展開すると、スナップショットが作成されます。



図に示すように、数分後にスナップショットが作成されます。



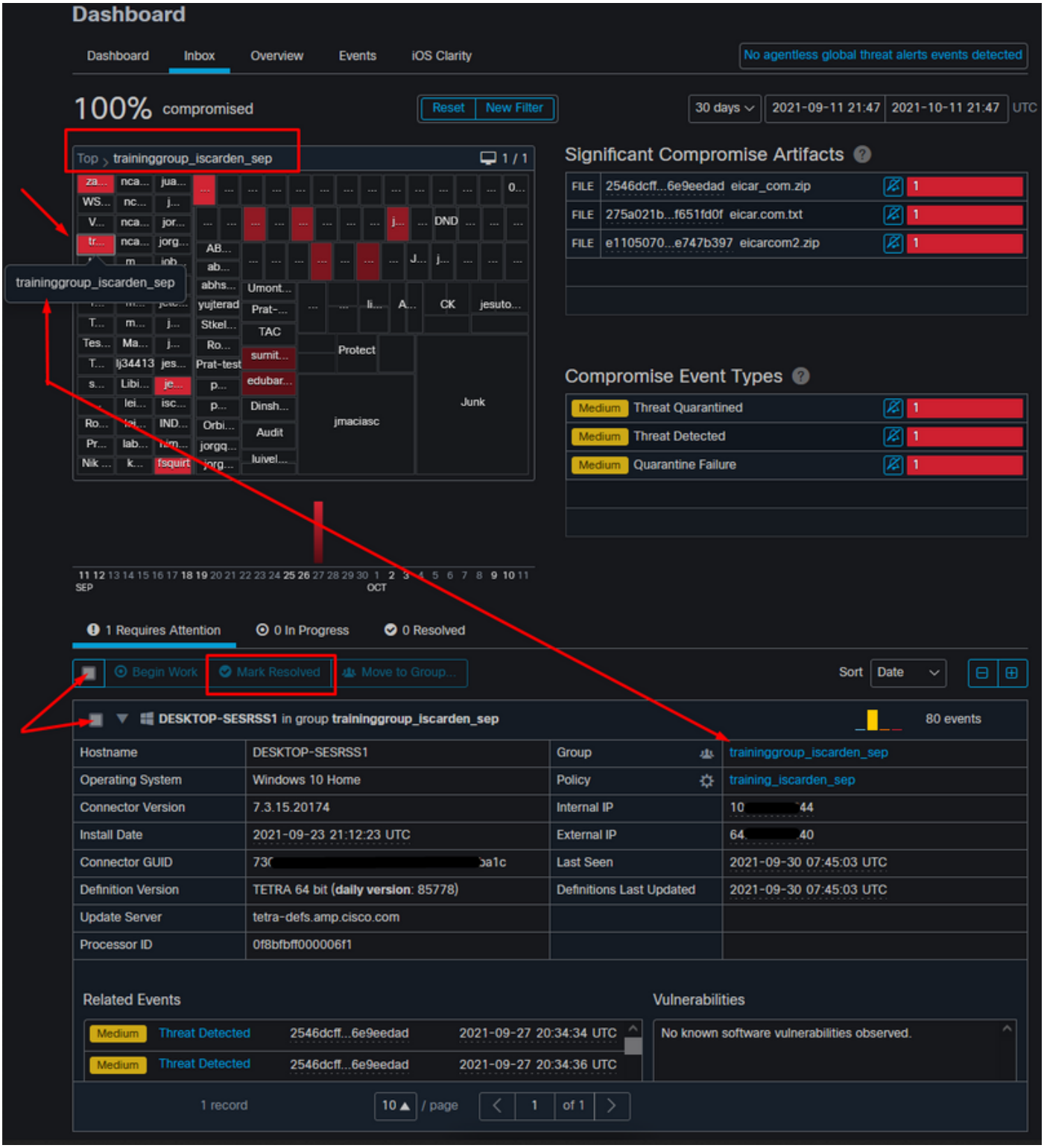
表示されたデータを表示できます。



ヒント

何千ものエンドポイントと数百もの妥協がある非常に大規模な環境では、個々のエンドポイントへのナビゲーションが課題となる可能性がある状況に遭遇できます。現在、利用できる唯一の解決策は、ヒートマップを使用し、次の例のように侵入エンドポイントがある特定のグループにドリルダウンすることです。

ヒートマップでグループを選択したら、イベントを侵害したグループに移動します。そのグループには1つのエンドポイントしかないため、現在は自分が属している特定のグループに基づいて100%が侵害されていることに注意してください。つまり、このグループに2つのエンドポイントがある場合、1つはクリーンで、もう1つは侵害されたエンドポイントは50 %の侵入を示します。


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