Automated Actions - Forensic Snapshot

Contents

Introduction

This document describes Automated Action functionality in Secure Endpoint is tied to the concept of Compromises. Understand the lifecycle and management of Compromises are vital to comprehend the functionality of Automated Actions. This article answers questions about the terminology and functionality of these concepts.

FAQ

What is a compromised machine?

A compromised machine is an endpoint that has an active compromise associated with it. A compromised machine can, by design, only have one compromise active at one time.

What is a compromise?

A compromise is a collection of one or more detections on a machine. Most detection events (Threat Detected, Indications of Compromise, etc) can generate or become associated with a compromise. However, there are pairs of events that may not trigger a new compromise. For example, when a Threat Detected event occurs, but shortly after it has an associated Threat Quarantined event, this does not trigger a new compromise. Logically, this is because Secure Endpoint has handled the potential compromise (we quarantined the threat).

What happens when new detections occur on a compromised machine?

The detection event(s) are added to the existing compromise. No new compromise is created.

Where can I see and manage compromises?

Compromises are managed in the Inbox tab of the Secure Endpoint console (which is https://console.amp.cisco.com/compromises for the North America cloud). A compromised machine is listed under **Require Attention** section and can be cleared of its compromise by pressing **Mark Resolved**. Also, compromises are automatically cleared after one month.

How does an automated action* get triggered?

Automated actions get triggered upon a compromise that is to say when an uncompromised machine becomes a compromised machine. If an already-compromised machine encounters a new detection, this detection is added to the compromise, but since this is not a new compromise, it does not trigger an automated action.

How can I re-trigger an automated action?

It is necessary to "clear" the compromise prior to attempt to re-trigger an automated action. Keep in mind that a Threat Detected + Threat Quarantined event is not sufficient to generate a new compromise event (and thus not sufficient to trigger a new automated action).

*Exception: The "Submit File to ThreatGrid" automated action is unaffiliated with compromises, and runs per-detection

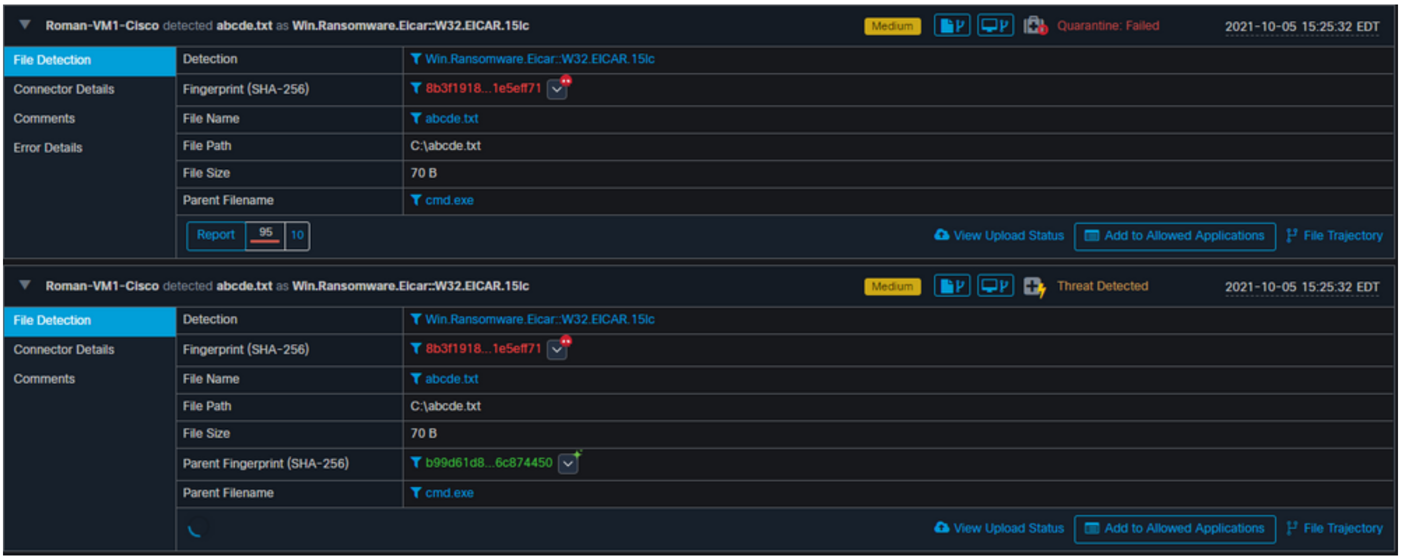
Used Case - Lab Recreate

#1: As we stated in FAQ section. Forensic snapshots are taken only in case of “compromise”. In other words, if we try to access and download a malicious file from a TEST site and the file is flagged upon download and quarantined that is not considered a compromise and does not trigger the action.

> **Note**: DFC Detection, Quarantine Failure, and pretty much anything that by the logic fall into the category of compromise event should create Forensic Snapshot.

#2: You can only generate Forensic Snapshot once on a unique compromised event it does not generate a snapshot unless you resolve the compromised machine in your inbox. If you don’t resolve the compromised event, you do not generate any other snapshot.

Example: In this lab, a script generates malicious activity, and because the file is deleted as soon as it is created and Secure Endpoint was not able to quarantine the file it falls in to compromise category.



Roman-VM1-Cisco detected abcde.txt as Win.Ransomware.Eicar::W32.EICAR.15lc — Medium — Quarantine: Failed — 2021-10-05 15:25:32 EDT

File Detection
Connector Details
Comments
Error Details

Detection	Win.Ransomware.Eicar::W32.EICAR.15lc
Fingerprint (SHA-256)	8b3f1918...1e5eff71
File Name	abcde.txt
File Path	C:\abcde.txt
File Size	70 B
Parent Filename	cmd.exe

Report 95 10 — View Upload Status — Add to Allowed Applications — File Trajectory

Roman-VM1-Cisco detected abcde.txt as Win.Ransomware.Eicar::W32.EICAR.15lc — Medium — Threat Detected — 2021-10-05 15:25:32 EDT

File Detection
Connector Details
Comments

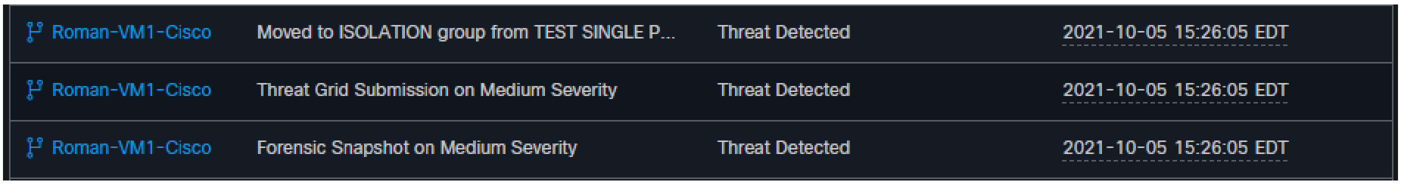
Detection	Win.Ransomware.Eicar::W32.EICAR.15lc
Fingerprint (SHA-256)	8b3f1918...1e5eff71
File Name	abcde.txt
File Path	C:\abcde.txt
File Size	70 B
Parent Fingerprint (SHA-256)	b99d61d8...6c874450
Parent Filename	cmd.exe

View Upload Status — Add to Allowed Applications — File Trajectory

Now in this test, you can look under automated actions and 3 things that happened based on the settings.

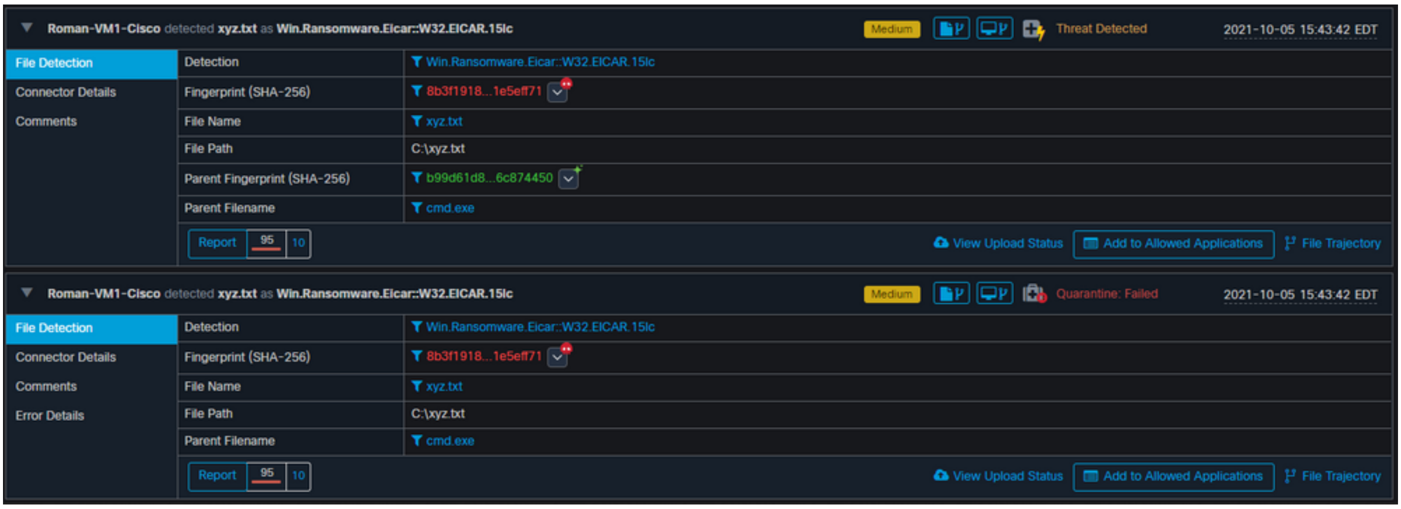
- Snapshot was created
- Submission was sent to Threat Grid (TG)
- The endpoint was moved to a separate group that was created and called ISOLATION

You can see all of that in this output, as shown in the image.



Roman-VM1-Cisco	Moved to ISOLATION group from TEST SINGLE P...	Threat Detected	2021-10-05 15:26:05 EDT
Roman-VM1-Cisco	Threat Grid Submission on Medium Severity	Threat Detected	2021-10-05 15:26:05 EDT
Roman-VM1-Cisco	Forensic Snapshot on Medium Severity	Threat Detected	2021-10-05 15:26:05 EDT

Now since this endpoint is compromised, the next test to prove the theory with a similar malicious file but with a different name, as shown in the image.



Roman-VM1-Cisco detected xyz.txt as Win.Ransomware.Eicar::W32.EICAR.15lc — Medium — Threat Detected — 2021-10-05 15:43:42 EDT

File Detection
Connector Details
Comments

Detection	Win.Ransomware.Eicar::W32.EICAR.15lc
Fingerprint (SHA-256)	8b3f1918...1e5eff71
File Name	xyz.txt
File Path	C:\xyz.txt
Parent Fingerprint (SHA-256)	b99d61d8...6c874450
Parent Filename	cmd.exe

Report 95 10 — View Upload Status — Add to Allowed Applications — File Trajectory

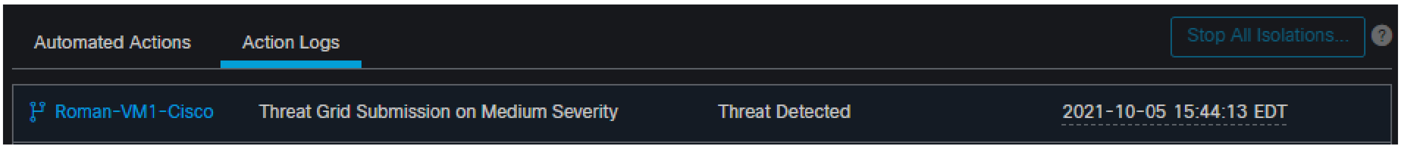
Roman-VM1-Cisco detected xyz.txt as Win.Ransomware.Eicar::W32.EICAR.15lc — Medium — Quarantine: Failed — 2021-10-05 15:43:42 EDT

File Detection
Connector Details
Comments
Error Details

Detection	Win.Ransomware.Eicar::W32.EICAR.15lc
Fingerprint (SHA-256)	8b3f1918...1e5eff71
File Name	xyz.txt
File Path	C:\xyz.txt
Parent Filename	cmd.exe

Report 95 10 — View Upload Status — Add to Allowed Applications — File Trajectory

However, since this compromise was not resolved, you can only be able to create a TG submission. No other events were recorded, also turn off the Isolation prior to this 2nd test.

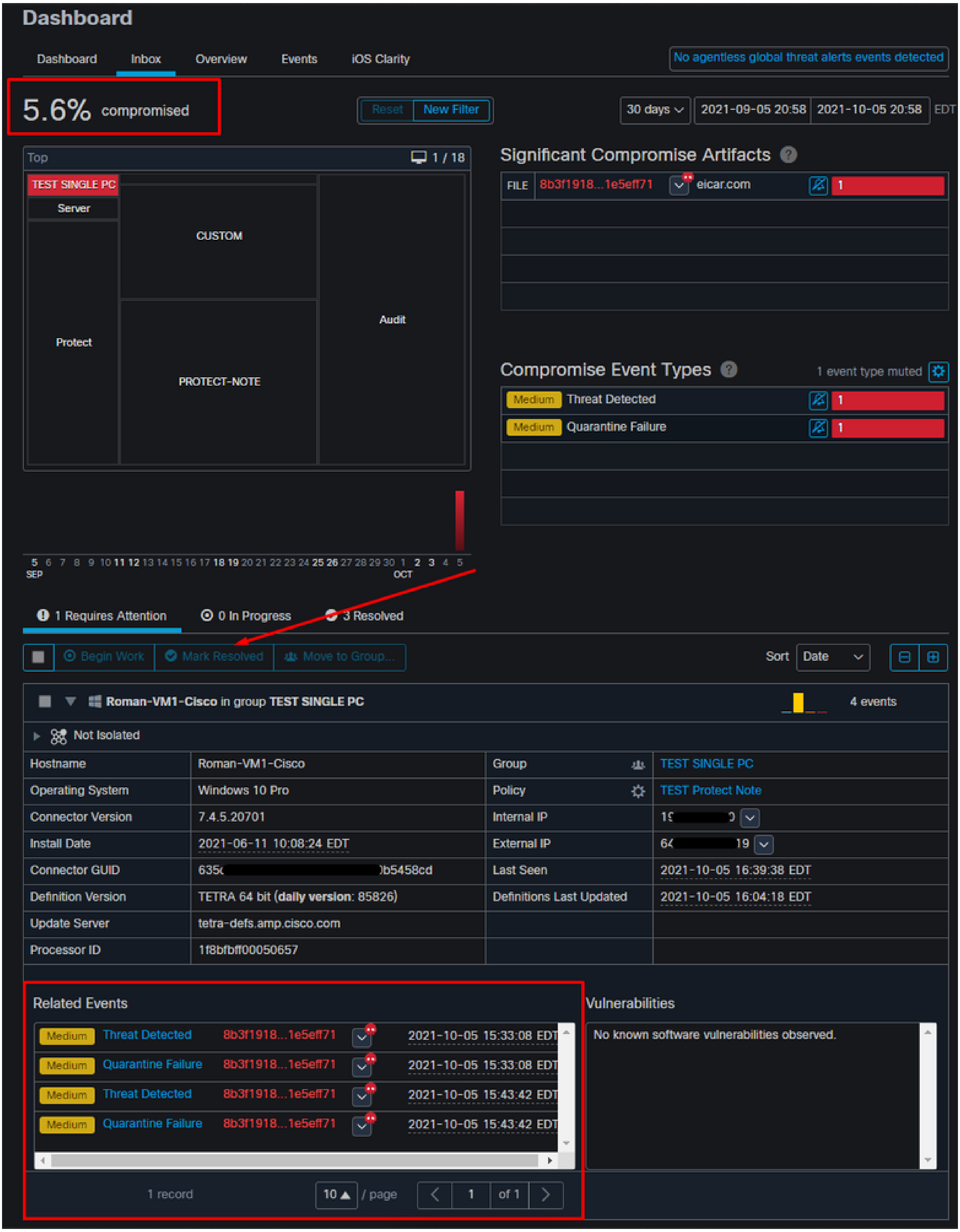


Automated Actions — Action Logs — Stop All Isolations...

Roman-VM1-Cisco	Threat Grid Submission on Medium Severity	Threat Detected	2021-10-05 15:44:13 EDT

Note: Please notice the time when the threat was detected and automated action triggers.

The event is not able to retrigger unless the compromised endpoint is resolved. In this case, the dashboard looks like this. Please notice the percentage and the button Mark Resolved along with the compromised events. No matter how many events are triggered you are only able to create one snapshot and the big percentage number never changed. That number represents compromise inside of your organization and it is based on the total amount of endpoints in your organization. It changes only with another compromised machine. In this example, the number is high due to only 16 devices in the lab. Also, note that compromise events are auto cleared once they reach 31 days of age.



Significant Compromise Artifacts

FILE	8b3f1918...1e5eff71	eicar.com	1

Compromise Event Types

1 event type muted

Medium	Threat Detected	1
Medium	Quarantine Failure	1

Roman-VM1-Cisco in group TEST SINGLE PC — 4 events

Not Isolated

Hostname	Roman-VM1-Cisco	Group	TEST SINGLE PC
Operating System	Windows 10 Pro	Policy	TEST Protect Note
Connector Version	7.4.5.20701	Internal IP	1[redacted]0
Install Date	2021-06-11 10:08:24 EDT	External IP	64[redacted]19
Connector GUID	635[redacted]b5458cd	Last Seen	2021-10-05 16:39:38 EDT
Definition Version	TETRA 64 bit (**daily version**: 85826)	Definitions Last Updated	2021-10-05 16:04:18 EDT
Update Server	tetra-defs.amp.cisco.com		
Processor ID	1f8bfbff00050657		

Related Events

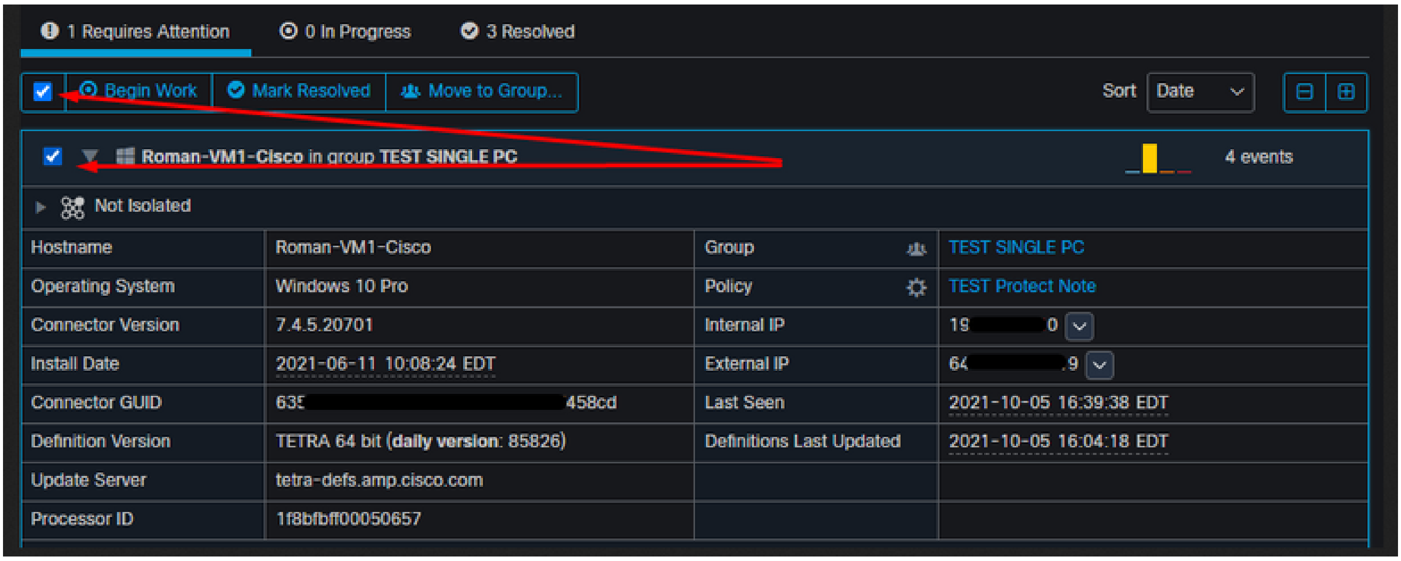
Medium	Threat Detected	8b3f1918...1e5eff71	2021-10-05 15:33:08 EDT
Medium	Quarantine Failure	8b3f1918...1e5eff71	2021-10-05 15:33:08 EDT
Medium	Threat Detected	8b3f1918...1e5eff71	2021-10-05 15:43:42 EDT
Medium	Quarantine Failure	8b3f1918...1e5eff71	2021-10-05 15:43:42 EDT

1 record 10 / page 1 of 1

Vulnerabilities

No known software vulnerabilities observed.

The next step is to create another event and generate a forensic snapshot. The first step is to resolve this compromise, click on the **Mark Resolved** button. You can do that per endpoint or you can select all in your organization.



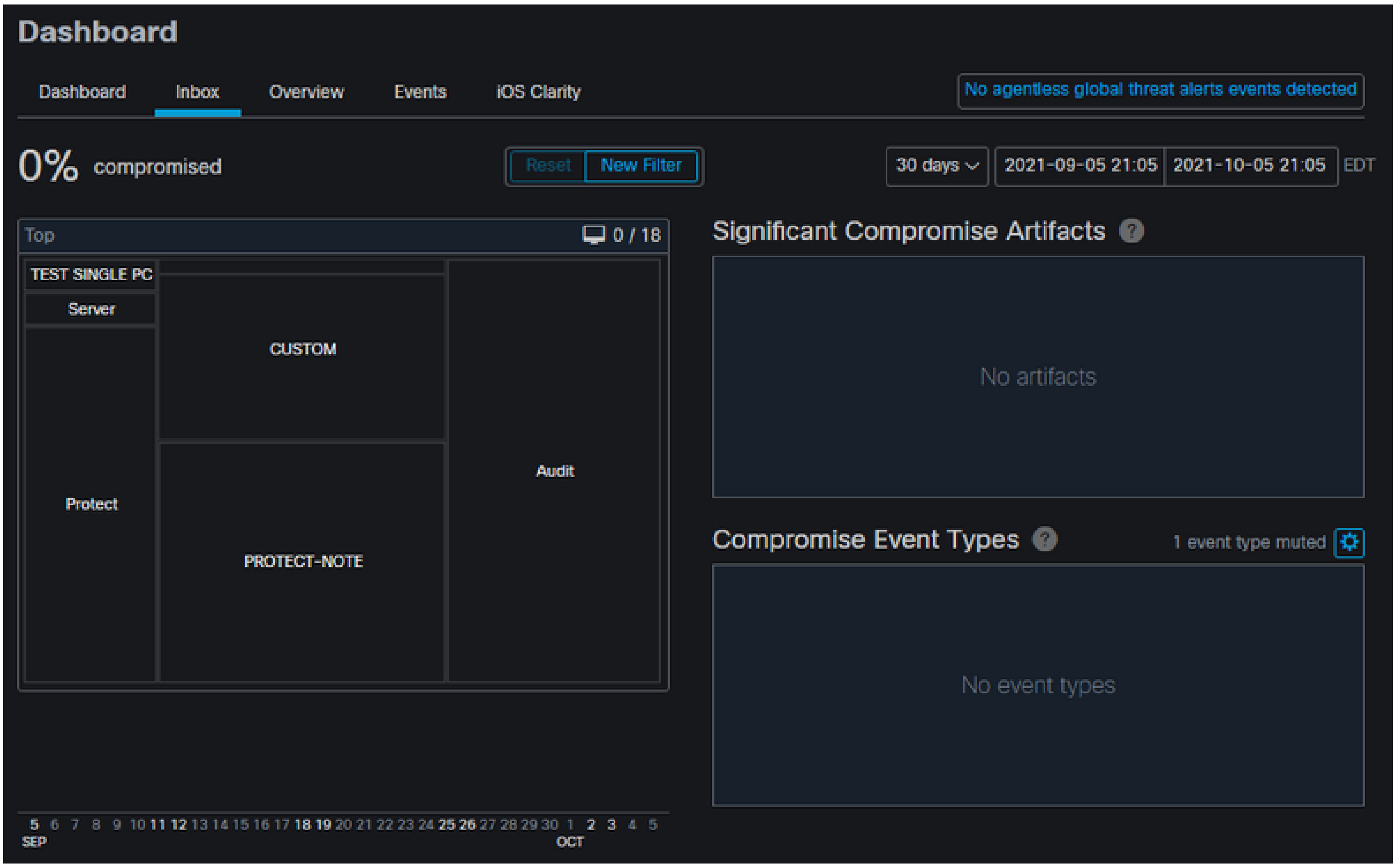
☑ Roman-VM1-Cisco in group TEST SINGLE PC

Not Isolated

Hostname	Roman-VM1-Cisco	Group	TEST SINGLE PC
Operating System	Windows 10 Pro	Policy	TEST Protect Note
Connector Version	7.4.5.20701	Internal IP	19[redacted]0
Install Date	2021-06-11 10:08:24 EDT	External IP	64[redacted].9
Connector GUID	63[redacted]458cd	Last Seen	2021-10-05 16:39:38 EDT
Definition Version	TETRA 64 bit (**daily version**: 85826)	Definitions Last Updated	2021-10-05 16:04:18 EDT
Update Server	tetra-defs.amp.cisco.com		
Processor ID	1f8bfbff00050657		

Note: If you select all the compromises are reset to 0%.

Once the Mark Resolved button is selected and since only one endpoint was compromised on the Secure Endpoint dashboard looks like this. And at this point, a new compromised event on the test machine was triggered.



Dashboard

0% compromised

2021-09-05 21:05 – 2021-10-05 21:05

Significant Compromise Artifacts

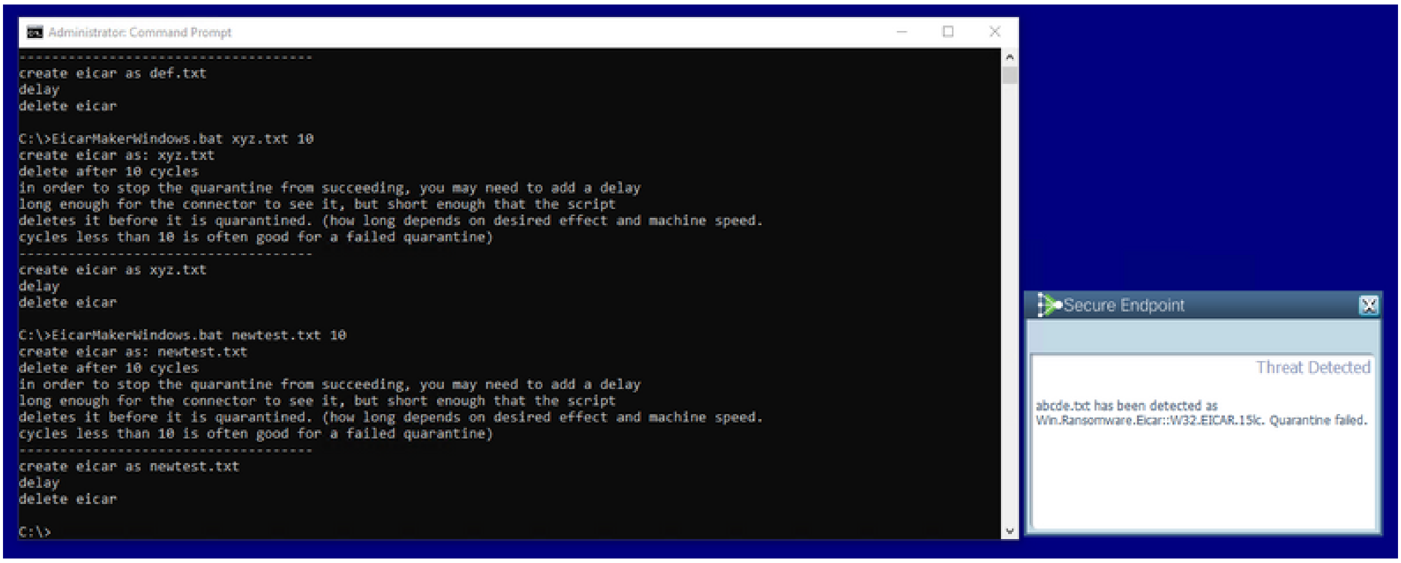
No artifacts

Compromise Event Types

1 event type muted

No event types

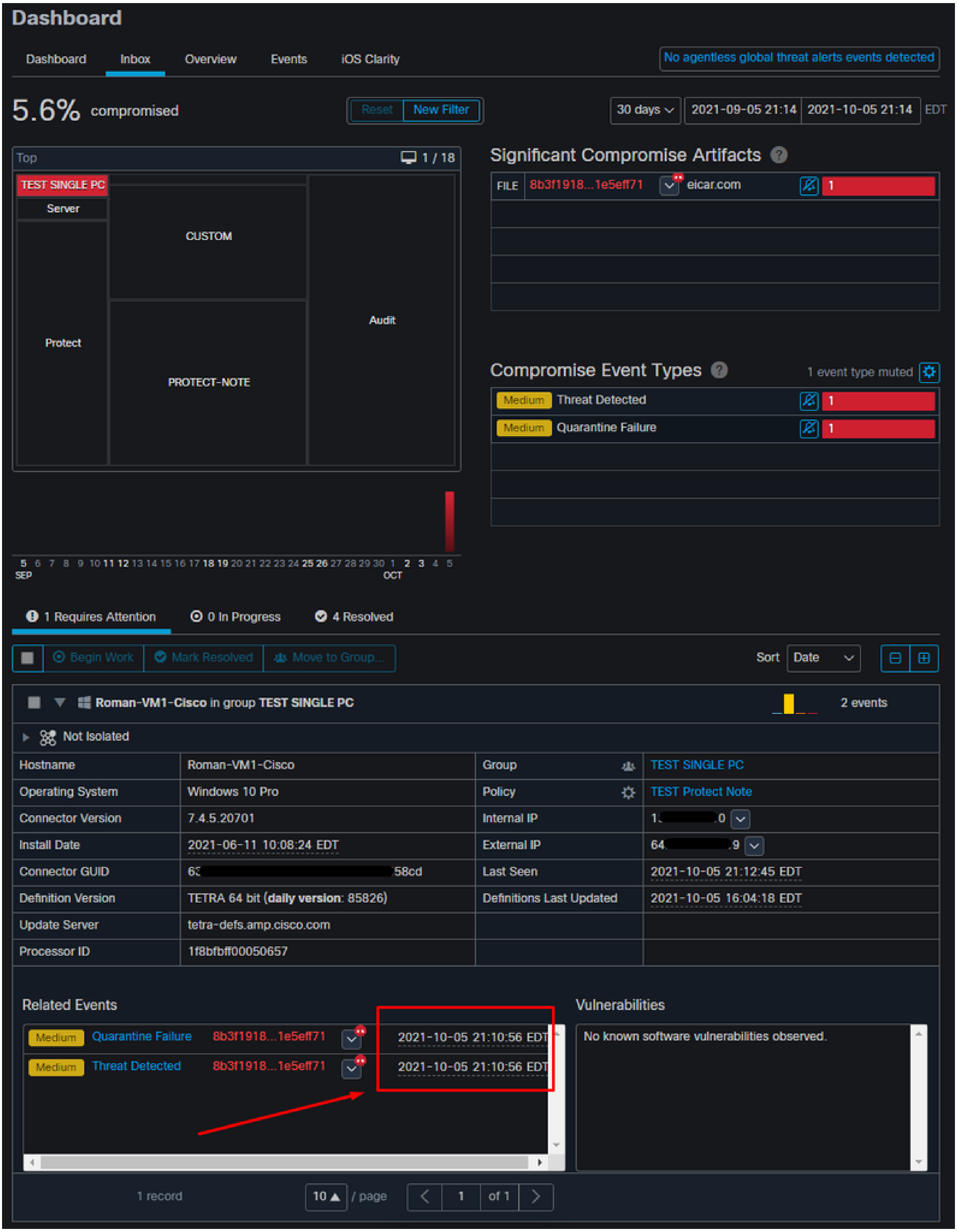
The next example triggers an event with a custom script that creates and deletes a malicious file.



```
-------------------------------------
create eicar as def.txt
delay
delete eicar

C:\>EicarMakerWindows.bat xyz.txt 10
create eicar as: xyz.txt
delete after 10 cycles
in order to stop the quarantine from succeeding, you may need to add a delay
long enough for the connector to see it, but short enough that the script
deletes it before it is quarantined. (how long depends on desired effect and machine speed.
cycles less than 10 is often good for a failed quarantine)
-------------------------------------
create eicar as xyz.txt
delay
delete eicar

C:\>EicarMakerWindows.bat newtest.txt 10
create eicar as: newtest.txt
delete after 10 cycles
in order to stop the quarantine from succeeding, you may need to add a delay
long enough for the connector to see it, but short enough that the script
deletes it before it is quarantined. (how long depends on desired effect and machine speed.
cycles less than 10 is often good for a failed quarantine)
-------------------------------------
create eicar as newtest.txt
delay
delete eicar

C:\>
```

abcde.txt has been detected as Win.Ransomware.Eicar::W32.EICAR.15lc. Quarantine failed.

Secure Endpoint console once again compromised, as shown in the image



5.6% compromised

Significant Compromise Artifacts

FILE	8b3f1918...1e5eff71	eicar.com	1

Compromise Event Types

Medium	Threat Detected	1
Medium	Quarantine Failure	1

Roman-VM1-Cisco in group **TEST SINGLE PC** 2 events

Not Isolated

Hostname	Roman-VM1-Cisco	Group	TEST SINGLE PC
Operating System	Windows 10 Pro	Policy	TEST Protect Note
Connector Version	7.4.5.20701	Internal IP	1[redacted]0
Install Date	2021-06-11 10:08:24 EDT	External IP	64[redacted]9
Connector GUID	63[redacted]58cd	Last Seen	2021-10-05 21:12:45 EDT
Definition Version	TETRA 64 bit (**daily version**: 85826)	Definitions Last Updated	2021-10-05 16:04:18 EDT
Update Server	tetra-defs.amp.cisco.com		
Processor ID	1f8bfbff00050657		

Related Events

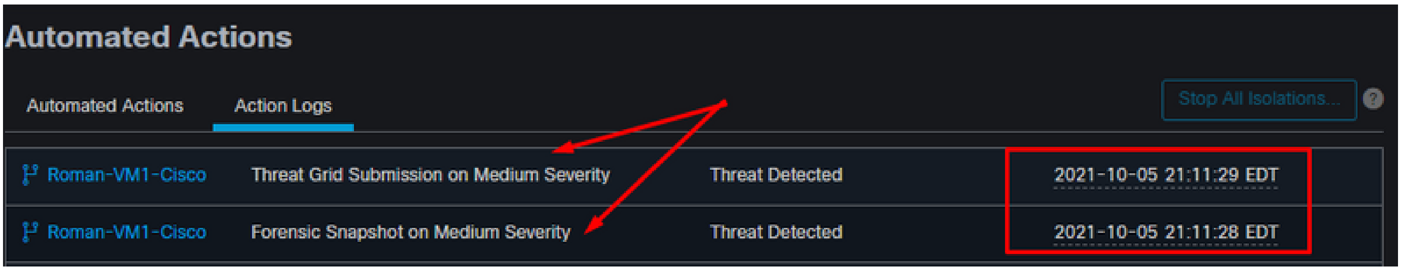
Medium	Quarantine Failure	8b3f1918...1e5eff71	2021-10-05 21:10:56 EDT
Medium	Threat Detected	8b3f1918...1e5eff71	2021-10-05 21:10:56 EDT

Vulnerabilities

No known software vulnerabilities observed.

1 record 10 / page 1 of 1

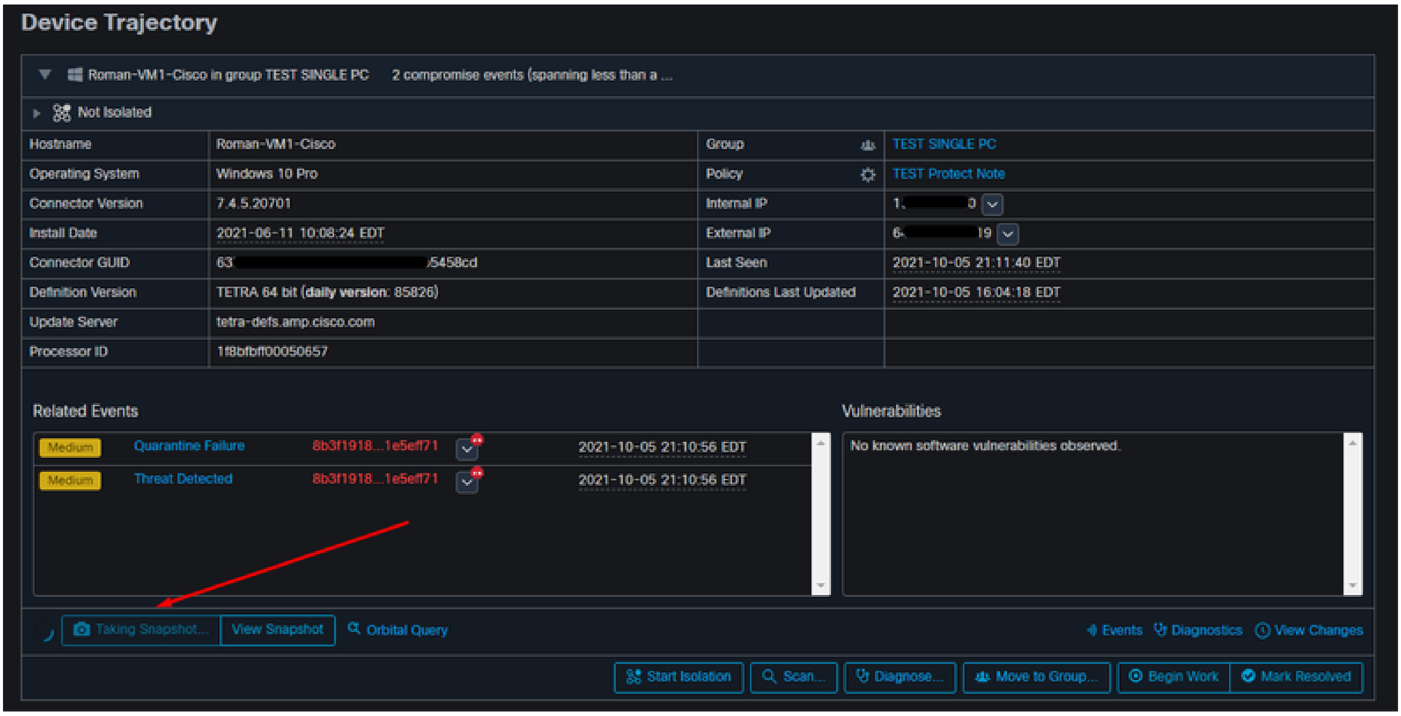
Here are new events under Automated Actions, as shown in the image.



Automated Actions

Roman-VM1-Cisco	Threat Grid Submission on Medium Severity	Threat Detected	2021-10-05 21:11:29 EDT
Roman-VM1-Cisco	Forensic Snapshot on Medium Severity	Threat Detected	2021-10-05 21:11:28 EDT

When the hostname under Automated Actions is selected, it redirects to Device Trajectory where you can observe the snapshot being created once you expand the computer tab, as shown in the image.



Device Trajectory

Roman-VM1-Cisco in group TEST SINGLE PC 2 compromise events (spanning less than a ...

Not Isolated

Hostname	Roman-VM1-Cisco	Group	TEST SINGLE PC
Operating System	Windows 10 Pro	Policy	TEST Protect Note
Connector Version	7.4.5.20701	Internal IP	[redacted]
Install Date	2021-06-11 10:08:24 EDT	External IP	[redacted]
Connector GUID	[redacted]	Last Seen	2021-10-05 21:11:40 EDT
Definition Version	TETRA 64 bit (**daily version**: 85826)	Definitions Last Updated	2021-10-05 16:04:18 EDT
Update Server	tetra-defs.amp.cisco.com		
Processor ID	1f8bfbff00050657		

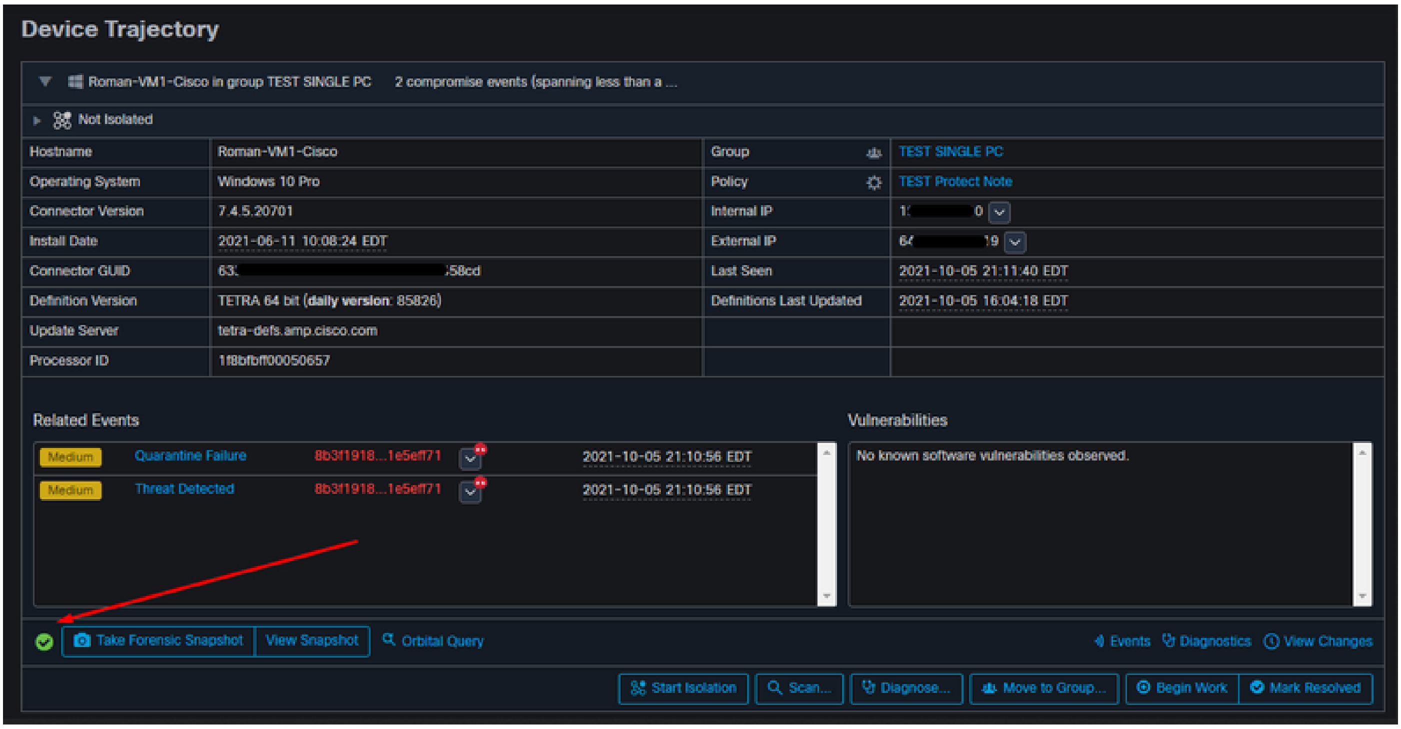
Related Events

Medium	Quarantine Failure	8b3f1918...1e5eff71	2021-10-05 21:10:56 EDT
Medium	Threat Detected	8b3f1918...1e5eff71	2021-10-05 21:10:56 EDT

Vulnerabilities

No known software vulnerabilities observed.

And minute later snapshot is created, as shown in the image.



Device Trajectory

Roman-VM1-Cisco in group TEST SINGLE PC 2 compromise events (spanning less than a ...

Not Isolated

Hostname	Roman-VM1-Cisco	Group	TEST SINGLE PC
Operating System	Windows 10 Pro	Policy	TEST Protect Note
Connector Version	7.4.5.20701	Internal IP	[redacted]
Install Date	2021-06-11 10:08:24 EDT	External IP	[redacted]
Connector GUID	[redacted]	Last Seen	2021-10-05 21:11:40 EDT
Definition Version	TETRA 64 bit (**daily version**: 85826)	Definitions Last Updated	2021-10-05 16:04:18 EDT
Update Server	tetra-defs.amp.cisco.com		
Processor ID	1f8bfbff00050657		

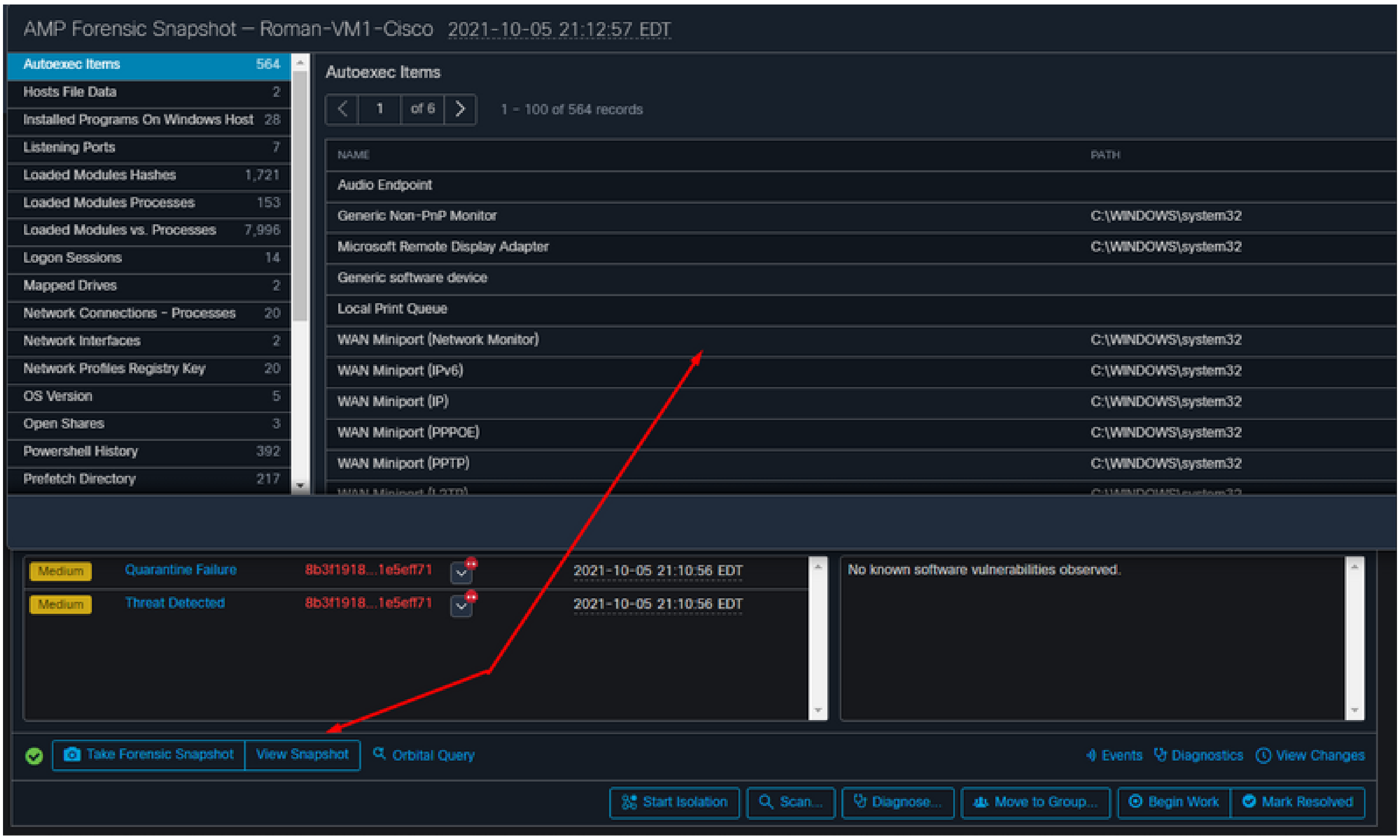
Related Events

Medium	Quarantine Failure	8b3f1918...1e5eff71	2021-10-05 21:10:56 EDT
Medium	Threat Detected	8b3f1918...1e5eff71	2021-10-05 21:10:56 EDT

Vulnerabilities

No known software vulnerabilities observed.

And now you can view the data displayed.



AMP Forensic Snapshot – Roman-VM1-Cisco 2021-10-05 21:12:57 EDT

Autoexec Items	564
Hosts File Data	2
Installed Programs On Windows Host	28
Listening Ports	7
Loaded Modules Hashes	1,721
Loaded Modules Processes	153
Loaded Modules vs. Processes	7,996
Logon Sessions	14
Mapped Drives	2
Network Connections - Processes	20
Network Interfaces	2
Network Profiles Registry Key	20
OS Version	5
Open Shares	3
Powershell History	392
Prefetch Directory	217

Autoexec Items

1 of 6 1 - 100 of 564 records

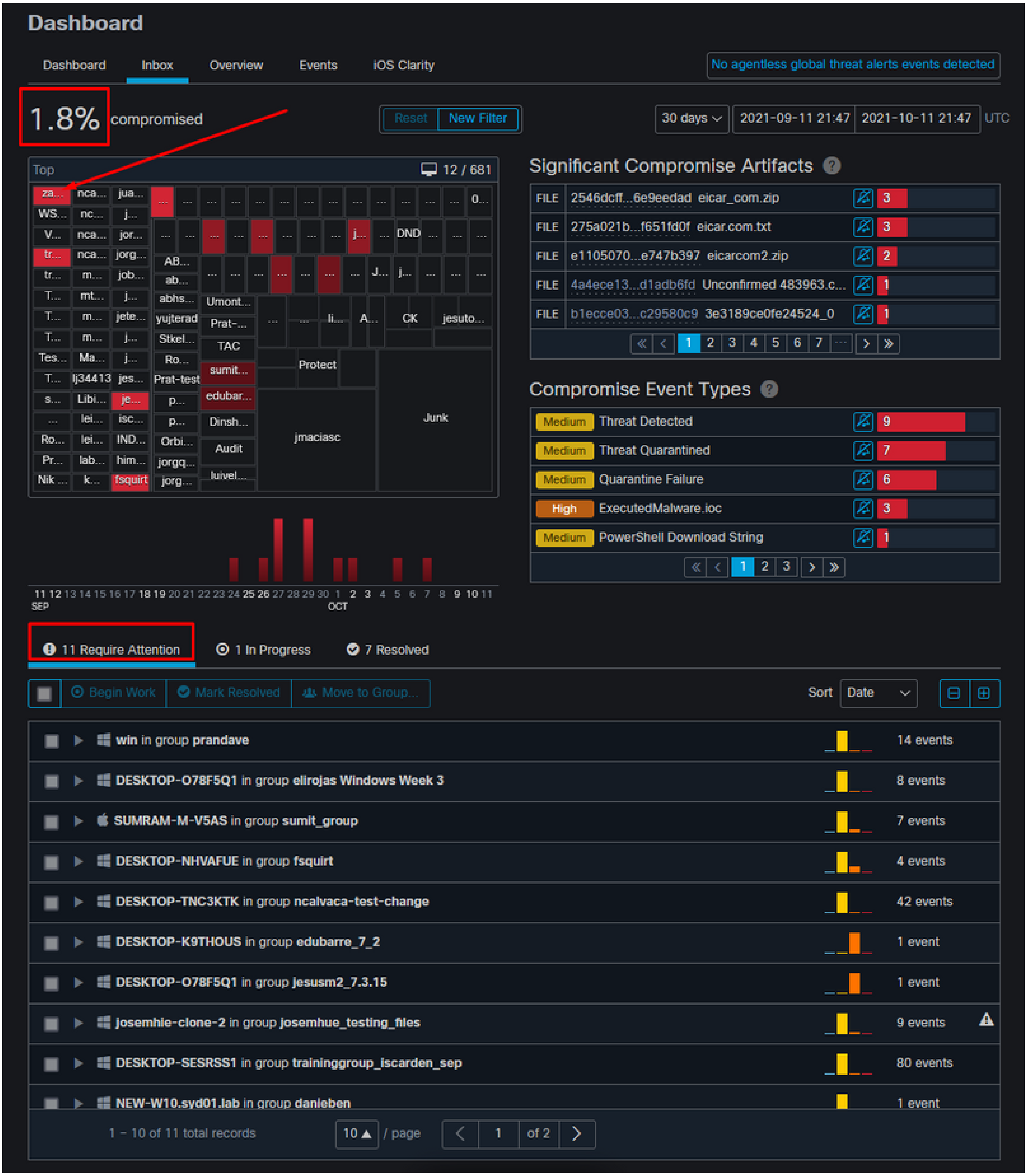
NAME	PATH
Audio Endpoint	
Generic Non-PnP Monitor	C:\WINDOWS\system32
Microsoft Remote Display Adapter	C:\WINDOWS\system32
Generic software device	
Local Print Queue	
WAN Miniport (Network Monitor)	C:\WINDOWS\system32
WAN Miniport (IPv6)	C:\WINDOWS\system32
WAN Miniport (IP)	C:\WINDOWS\system32
WAN Miniport (PPPOE)	C:\WINDOWS\system32
WAN Miniport (PPTP)	C:\WINDOWS\system32
WAN Miniport (L2TP)	C:\WINDOWS\system32

Medium	Quarantine Failure	8b3f1918...1e5eff71	2021-10-05 21:10:56 EDT
Medium	Threat Detected	8b3f1918...1e5eff71	2021-10-05 21:10:56 EDT

No known software vulnerabilities observed.

Tip

In very large environments with thousands of endpoints and hundreds of compromises, you can run into situations where the navigation to the individual endpoint might be a challenge. Currently, the only available solution is to use the heat map and then drill down to a specific group where your compromise endpoint is as in this example below.



1.8% compromised

Significant Compromise Artifacts

FILE	2546dcff...6e9eedad eicar_com.zip		3
FILE	275a021b...f651fd0f eicar.com.txt		3
FILE	e1105070...e747b397 eicarcom2.zip		2
FILE	4a4ece13...d1adb6fd Unconfirmed 483963.c...		1
FILE	b1ecce03...c29580c9 3e3189ce0fe24524_0		1

« ‹ 1 2 3 4 5 6 7 ··· › »

Compromise Event Types

Medium	Threat Detected		9
Medium	Threat Quarantined		7
Medium	Quarantine Failure		6
High	ExecutedMalware.ioc		3
Medium	PowerShell Download String		1

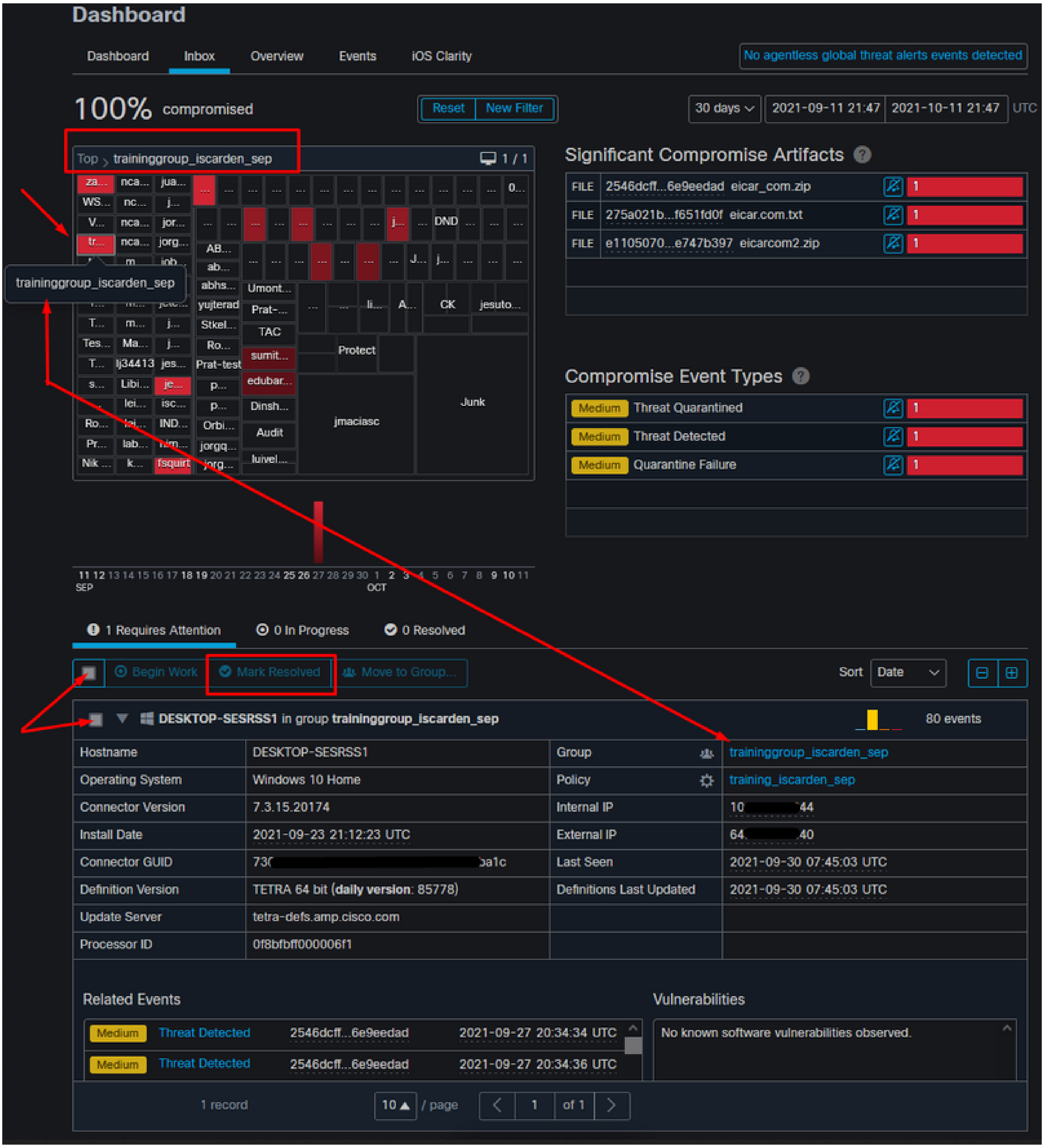
« ‹ 1 2 3 › »

11 Require Attention | 1 In Progress | 7 Resolved

□ ▶ win in group prandave	14 events
□ ▶ DESKTOP-O78F5Q1 in group elirojas Windows Week 3	8 events
□ ▶ SUMRAM-M-V5AS in group sumit_group	7 events
□ ▶ DESKTOP-NHVAFUE in group fsquirt	4 events
□ ▶ DESKTOP-TNC3KTK in group ncalvaca-test-change	42 events
□ ▶ DESKTOP-K9THOUS in group edubarre_7_2	1 event
□ ▶ DESKTOP-O78F5Q1 in group jesusm2_7.3.15	1 event
□ ▶ josemhie-clone-2 in group josemhue_testing_files	9 events ⚠
□ ▶ DESKTOP-SESRSS1 in group traininggroup_iscarden_sep	80 events
□ ▶ NEW-W10.syd01.lab in group danleben	1 event

1 - 10 of 11 total records 10 ▲ / page ‹ 1 of 2 ›

Once the group is selected in the heat map navigate to that group in which we have compromised the event. Since there is only one endpoint in that group please notice the 100% compromised which is based now on the specific group that we are in. In other words, if we have 2 endpoints in this group one clean and the other compromised displays 50% compromise.



Dashboard

100% compromised

Top > traininggroup_iscarden_sep

traininggroup_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

1 Requires Attention   0 In Progress   0 Resolved

DESKTOP-SESRSS1 in group **traininggroup_iscarden_sep**   80 events

Hostname	DESKTOP-SESRSS1	Group	traininggroup_iscarden_sep
Operating System	Windows 10 Home	Policy	training_iscarden_sep
Connector Version	7.3.15.20174	Internal IP	10[redacted]44
Install Date	2021-09-23 21:12:23 UTC	External IP	64[redacted]40
Connector GUID	73([redacted]ba1c	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