自动操作 — 取证快照

目录

简介

本文档介绍安全终端中的自动操作功能与危害的概念有关。 了解危害的生命周期和管理对于理解自动化操作的功能至关重要。本文回答有关这些概念的术语和功能的问题。

常见问题

什么是受危害的机器？

受感染的计算机是与其关联的活动危害的终端。按照设计，受感染的机器一次只能激活一个危害。

什么是妥协？

危害是计算机上一个或多个检测的集合。大多数检测事件（检测到威胁、危害表现等）都可以生成或与危害关联。但是，有对事件可能不会触发新的危害。例如，当检测到威胁事件发生，但在其发生关联的威胁隔离事件后不久，这不会触发新的危害。从逻辑上讲，这是因为安全终端已处理了潜在危害（我们隔离了威胁）。

在受感染的计算机上发生新检测时会发生什么情况？

检测事件将添加到现有危害。未创建新危害。

我在哪里可以看到和管理危害？

危害在安全终端控制台的“收件箱”(Inbox)选项卡中进行管理(北美云为 https://console.amp.cisco.com/compromises)。受损计算机列在“需要注**意”部**分下，可通过按“已解决标记”来清除**其危害**。此外，一个月后，威胁会自动消除。

如何触发自动操作*?

在危害（即未受危害的机器成为受危害的机器时）触发自动操作。如果已受损的计算机遇到新检测，则此检测会添加到危害中，但由于这不是新的危害，因此不会触发自动操作。

如何重新触发自动操作？

在尝试重新触发自动操作之前，必须“清除”危害。请记住，Threat Detected + Threat Quarantined事件不足以生成新的危害事件（因此不足以触发新的自动操作）。

*异常：“向ThreatGrid提交文件”自动操作与危害无关，并运行每次检测

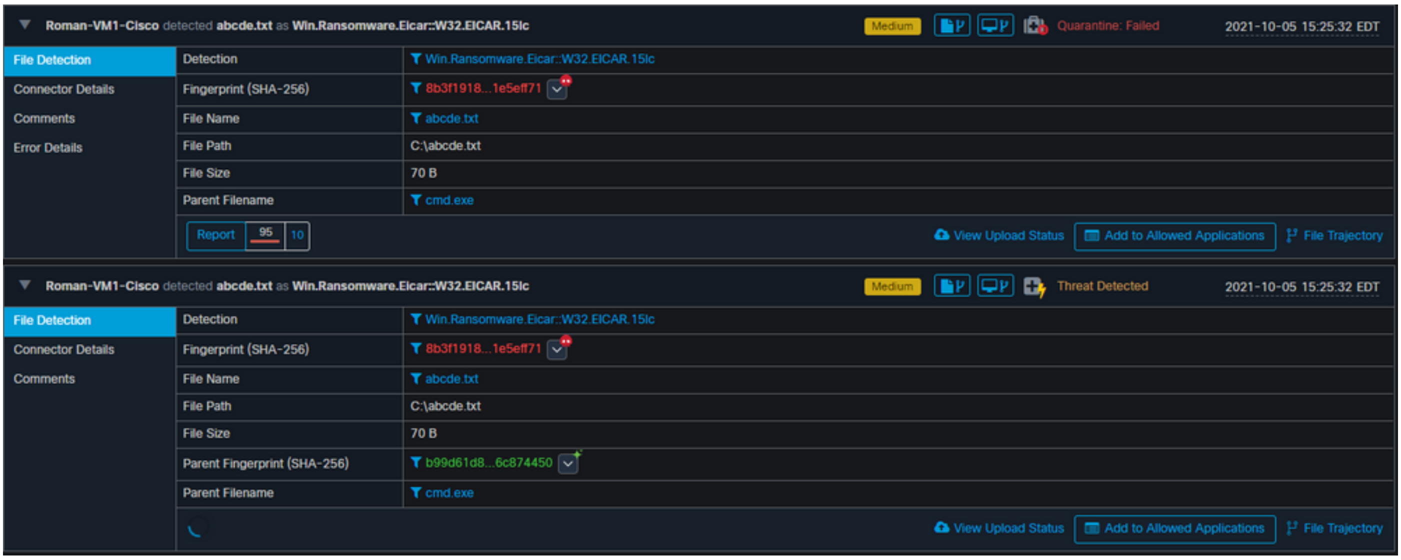
使用案例 — 实验重新创建

#1:正如我们在常见问题部分中所述。调查分析快照仅在“危害”时拍摄。换句话说，如果我们尝试从TEST站点访问和下载恶意文件，并且下载时会标记该文件并将其隔离，而不被视为危害，并且不会触发操作。

> **注意**：DFC检测、隔离故障以及几乎任何逻辑属于危害事件类别的内容都应创建取证快照。

#2:只能在唯一受危害事件上生成一次取证快照，它不会生成快照，除非您在收件箱中解析受危害的计算机。如果不解决受危害事件，则不生成任何其他快照。

示例：在本实验中，脚本会生成恶意活动，并且因为文件一旦创建即被删除，并且安全终端无法隔离其属于危害类别的文件。



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

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

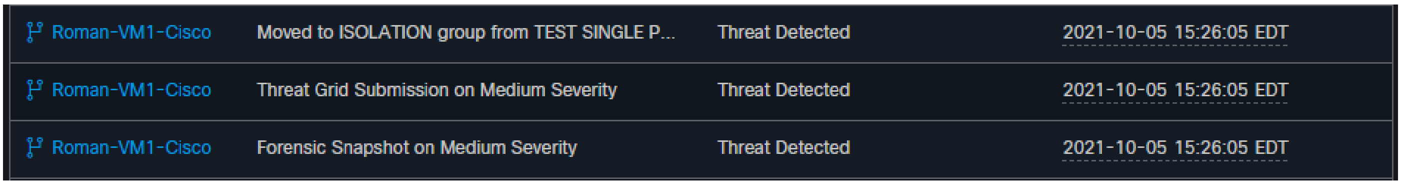
Roman-VM1-Cisco detected abcde.txt as Win.Ransomware.Eicar::W32.EICAR.15lc　Medium　Threat Detected　2021-10-05 15:25:32 EDT

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

在本测试中，您可以根据设置查看自动操作和发生的3件事。

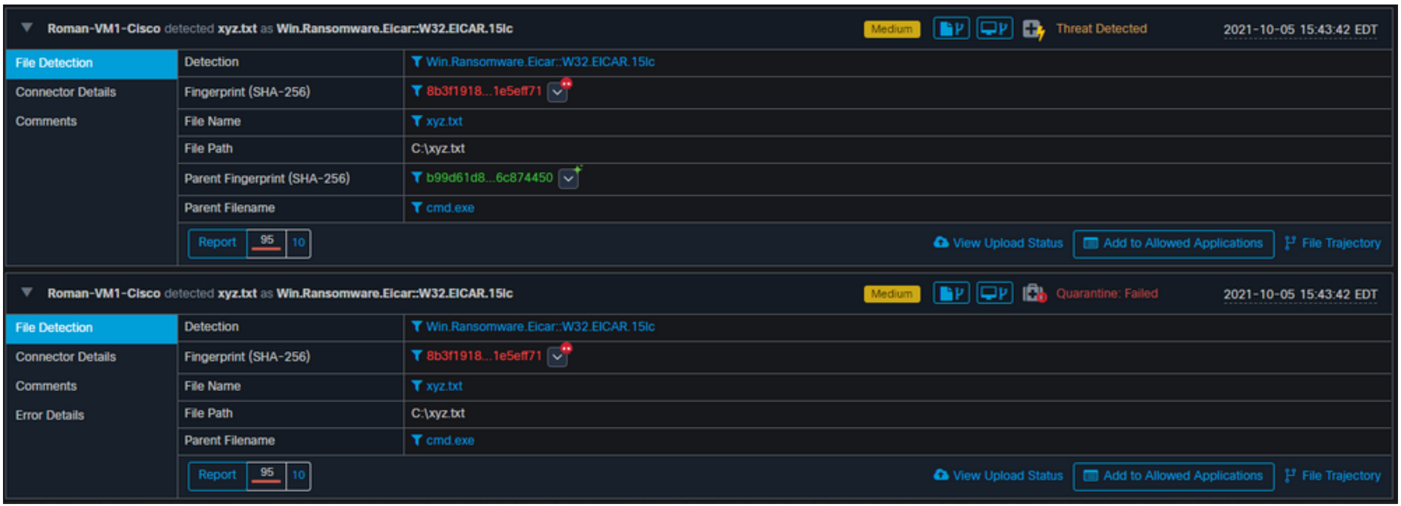
- 已创建快照
- 提交文件已发送到Threat Grid(TG)
- 终端已移至创建并称为ISOLATION的单独组

您可以在此输出中看到所有这些，如图所示。



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

现在，由于此终端已受到危害，下一次测试将用类似的恶意文件证明该理论，但名称不同，如图所示。



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

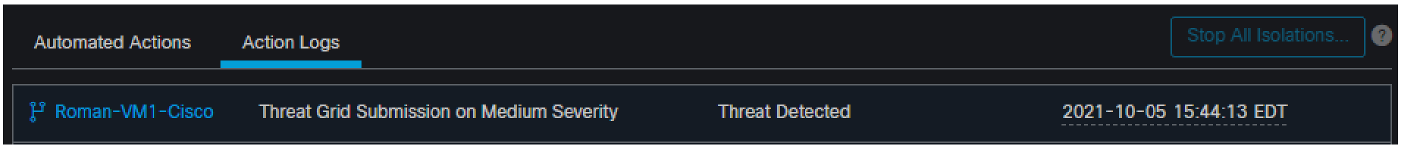
Report 95 10 View Upload Status Add to Allowed Applications File Trajectory

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

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

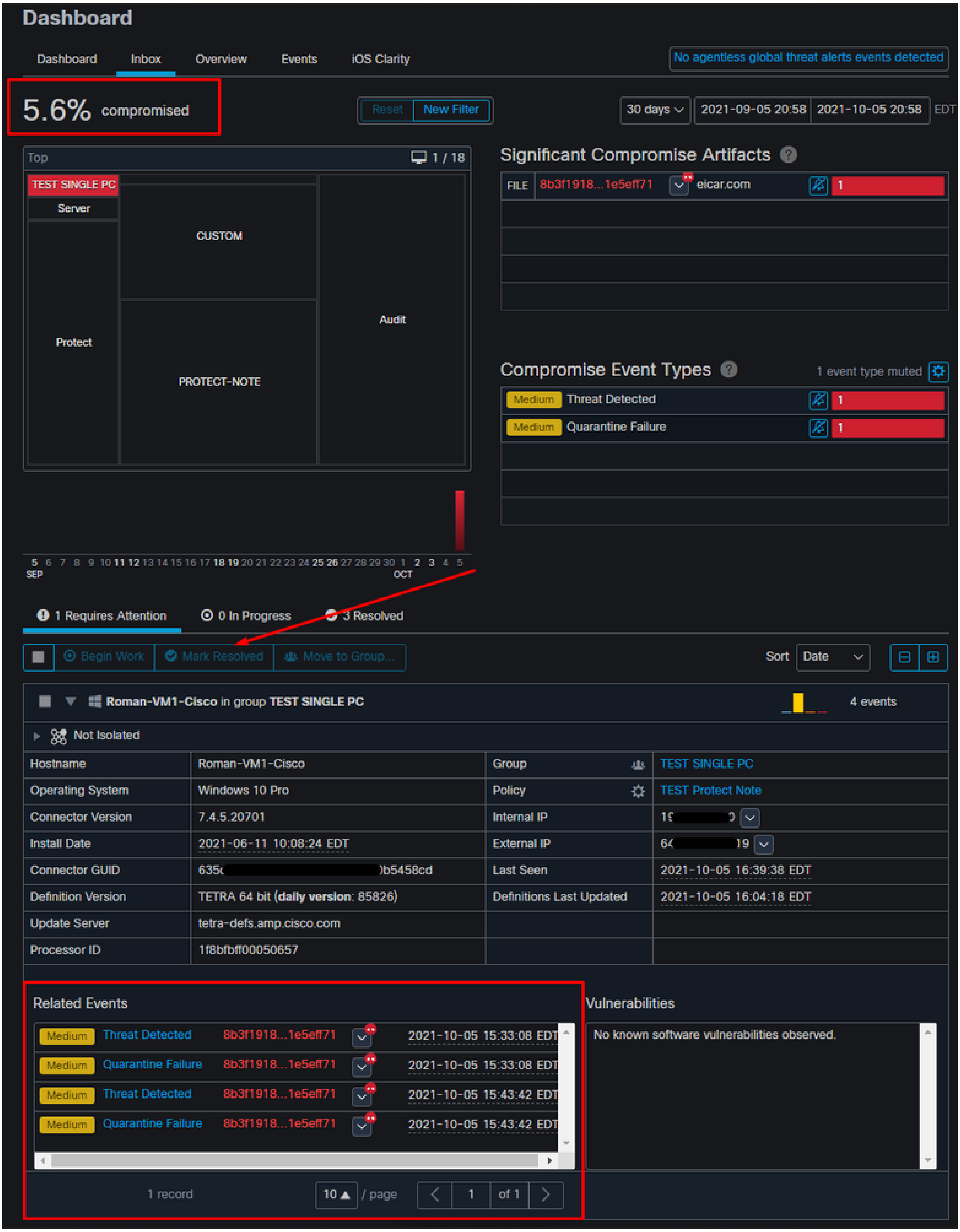
但是，由于此危害未解决，您只能创建TG提交。没有记录其他事件，也在此第2次测试之前关闭隔离。



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

注意：请注意检测到威胁并触发自动操作的时间。

除非已解决受危害的终端，否则无法检索事件。在本例中，控制面板如下所示。请注意百分比和“标记已解决”按钮以及受危害事件。无论触发了多少个事件，您只能创建一个快照，且大百分比数量从未更改。该数字表示您组织内部的危害，并且取决于您组织中终端的总数量。它仅与另一台受危害的计算机一起更改。在本例中，由于实验中只有16台设备，因此该数字很高。另请注意，危害事件在达到31天时自动清除。



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

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]
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		

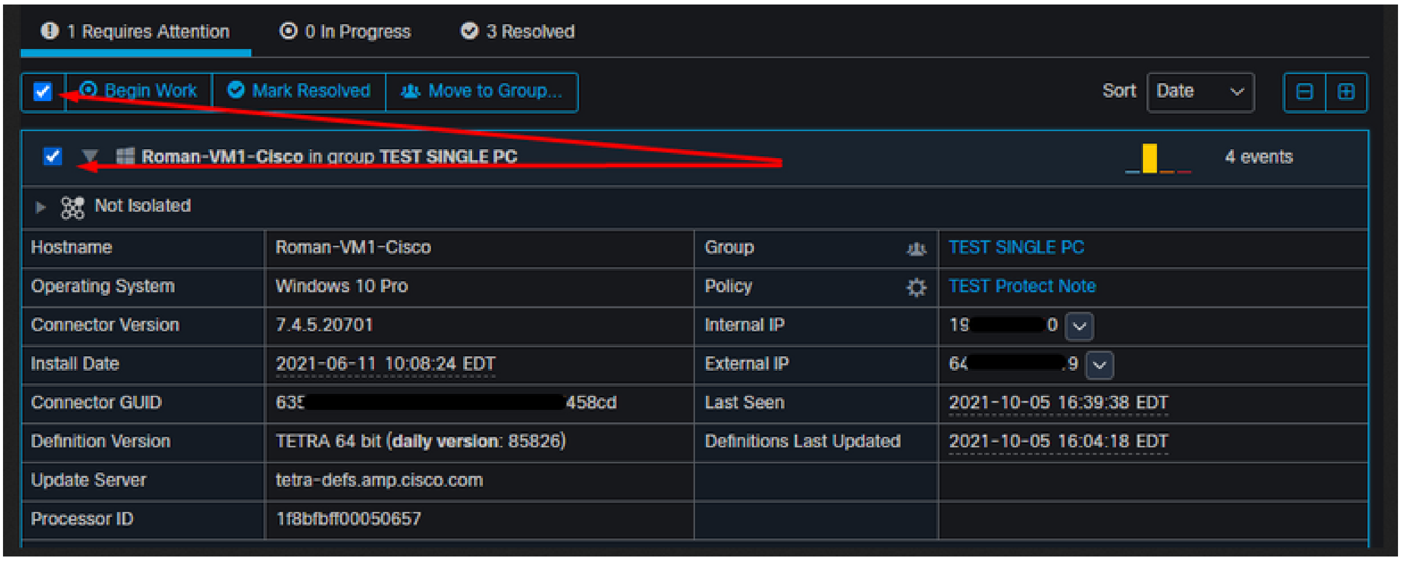
Related Events

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

Vulnerabilities

No known software vulnerabilities observed.

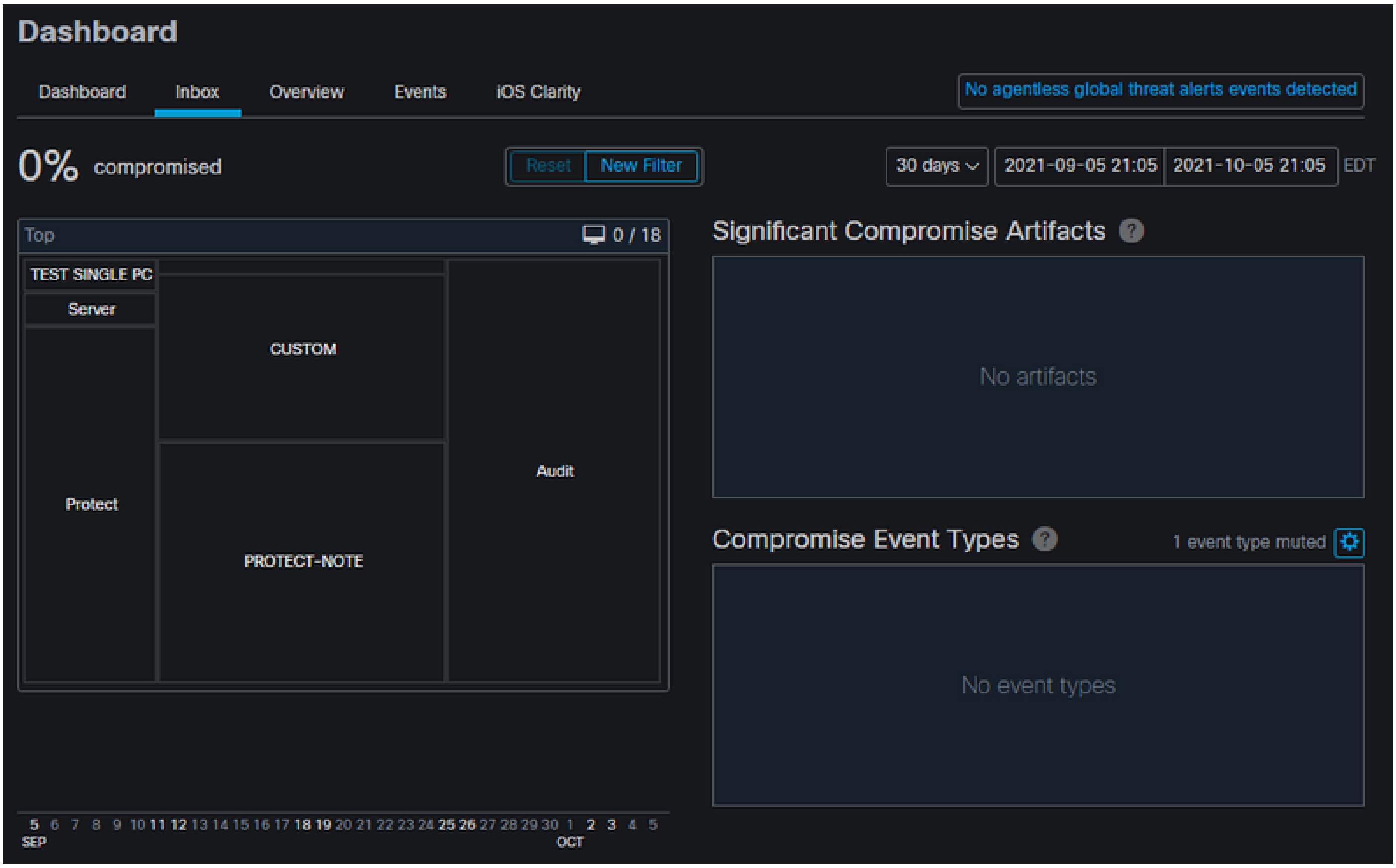
下一步是创建另一个事件并生成取证快照。第一步是解决此危害，单击“标记已解**决**”按钮。您可以按终端执行此操作，也可以在组织中选择所有。



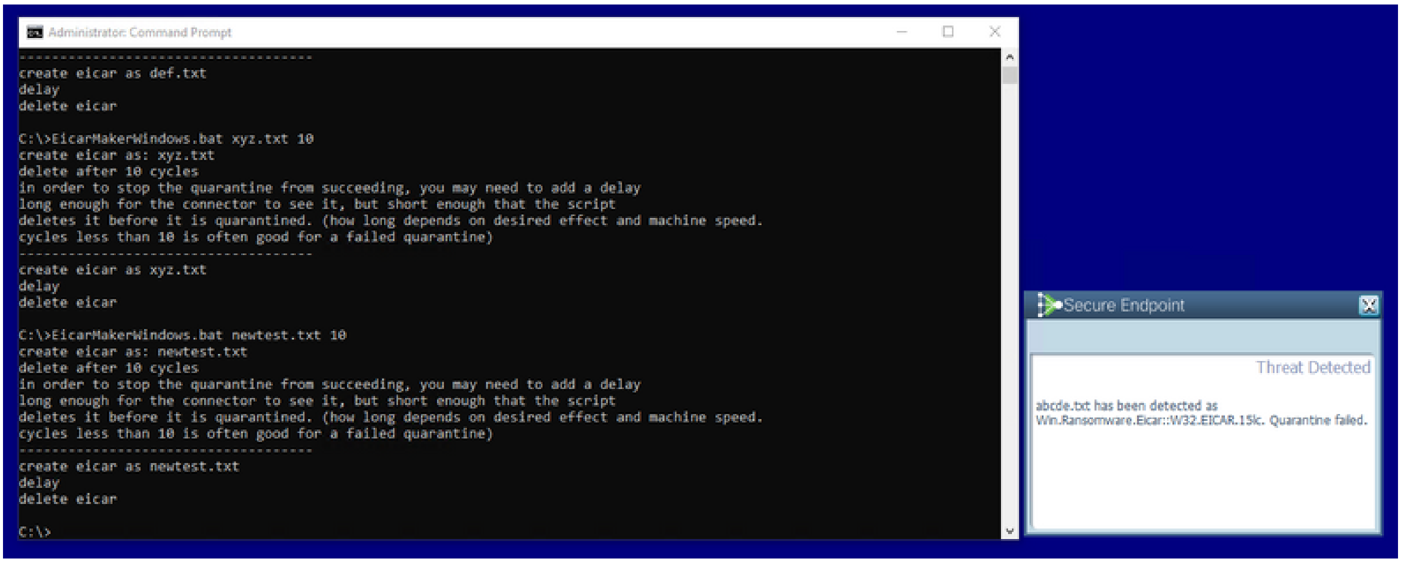
Hostname	Roman-VM1-Cisco	Group	TEST SINGLE PC
Operating System	Windows 10 Pro	Policy	TEST Protect Note
Connector Version	7.4.5.20701	Internal IP	19[redacted]0
Install Date	2021-06-11 10:08:24 EDT	External IP	64[redacted].9
Connector GUID	635[redacted]458cd	Last Seen	2021-10-05 16:39:38 EDT
Definition 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		

注意： 如果选择所有危害，则重置为0%。

选择“标记已解析”(Mark Resolved)按钮后，由于安全终端控制面板上仅有一个终端受到危害，因此如下所示。此时，测试机上触发了新的入侵事件。



下一个示例使用创建和删除恶意文件的自定义脚本触发事件。

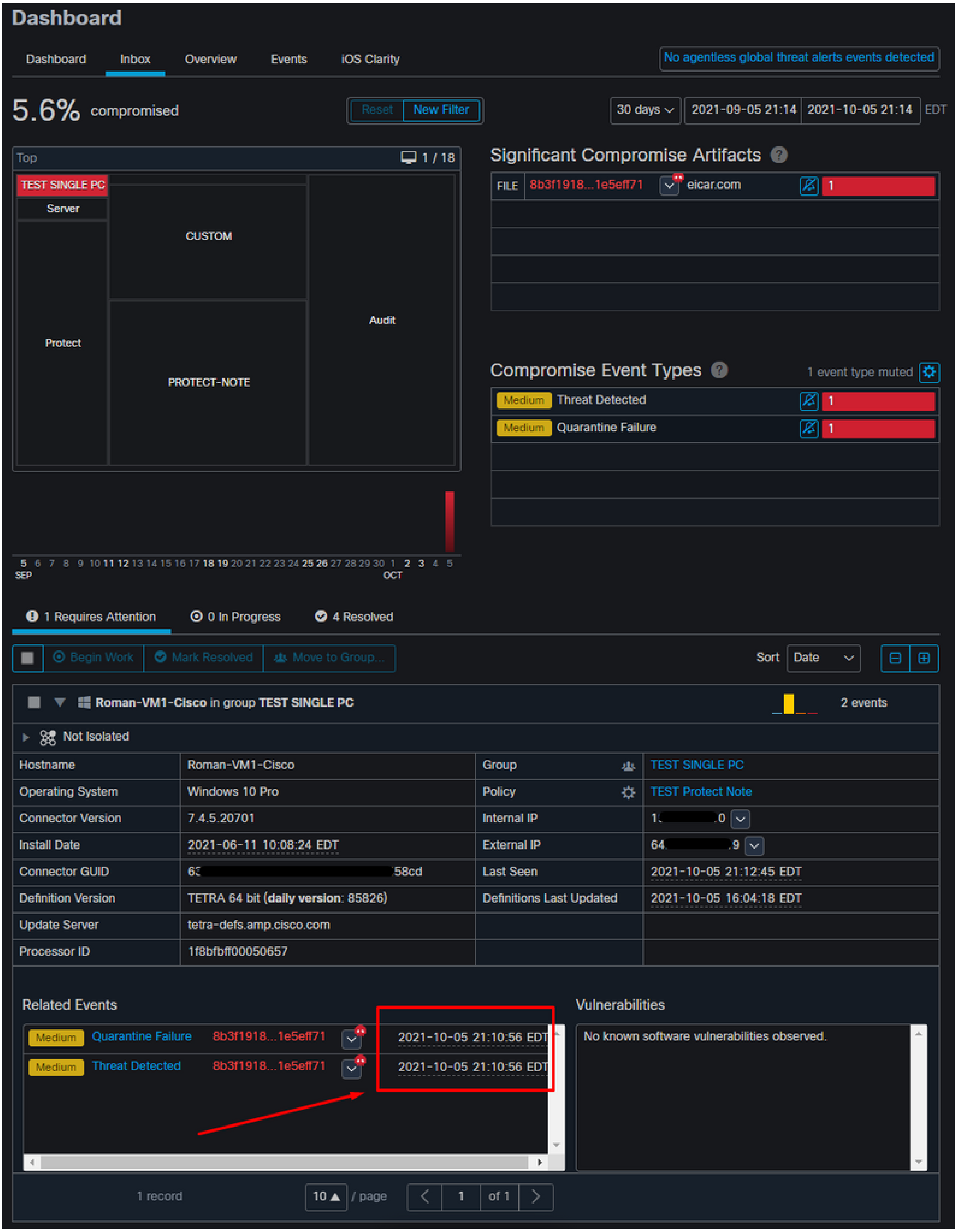


```
------------------------------------
create eicar as def.txt
delay
delete eicar

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:\>
```

Threat Detected

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

如图所示，安全终端控制台再次受到危害



Dashboard

Dashboard | Inbox | Overview | Events | iOS Clarity

No agentless global threat alerts events detected

5.6% compromised

Reset | New Filter

30 days | 2021-09-05 21:14 | 2021-10-05 21:14 | EDT

Significant Compromise Artifacts

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

Compromise Event Types

1 event type muted

Medium	Threat Detected	1
Medium	Quarantine Failure	1

1 Requires Attention | 0 In Progress | 4 Resolved

Begin Work | Mark Resolved | Move to Group...

Sort Date

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

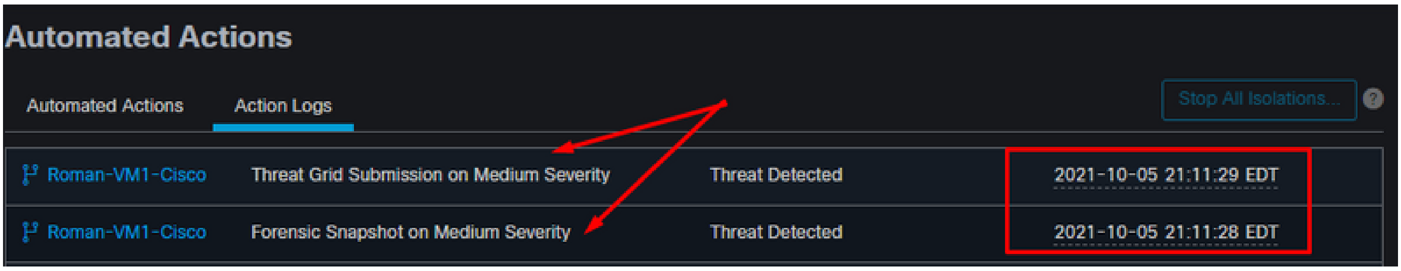
Medium	Quarantine Failure	8b3f1918...1e5eff71	2021-10-05 21:10:56 EDT
Medium	Threat Detected	8b3f1918...1e5eff71	2021-10-05 21:10:56 EDT

Vulnerabilities

No known software vulnerabilities observed.

1 record | 10 / page | 1 of 1

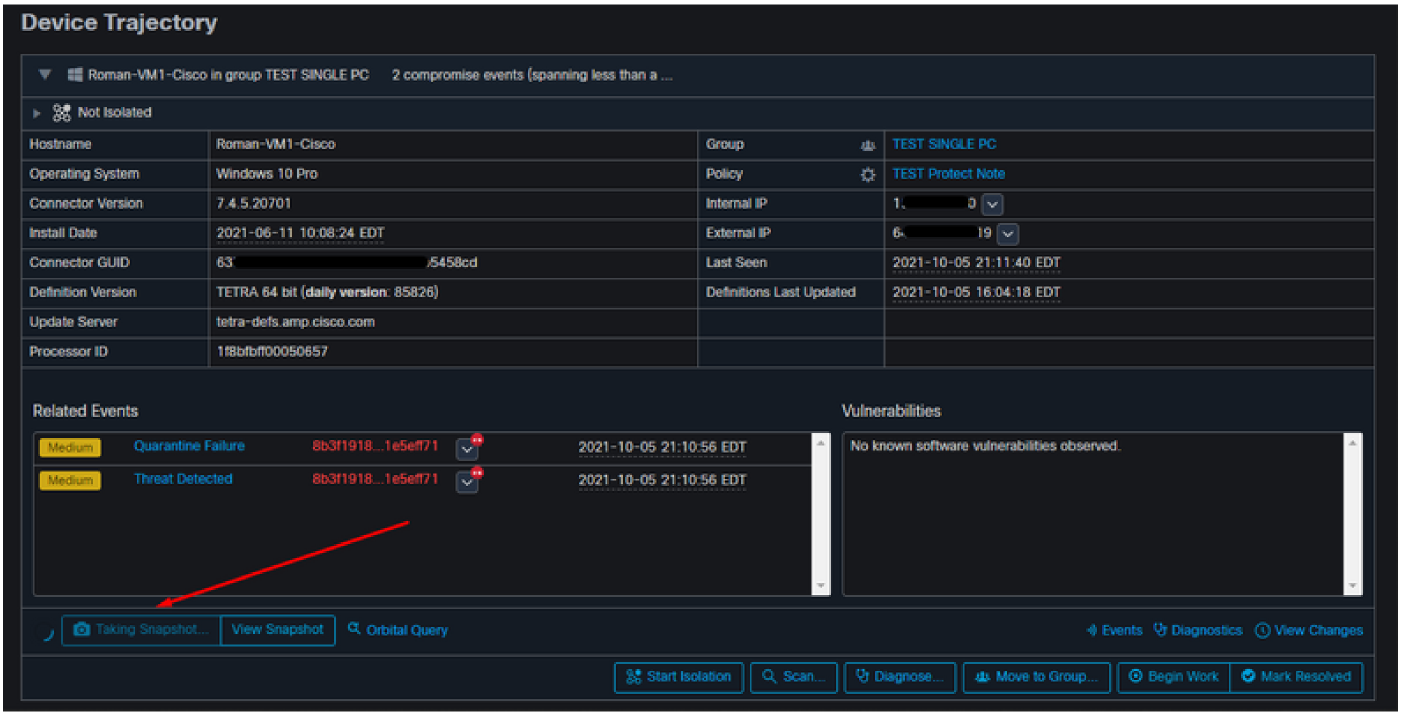
以下是自动操作下的新事件，如图所示。



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

选择“自动操作”下的主机名后，主机名将重定向到“设备轨迹”，在此可以观察展开计算机选项卡后创建的快照，如图所示。



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	1.[redacted]0
Install Date	2021-06-11 10:08:24 EDT	External IP	6.[redacted]19
Connector GUID	63[redacted]5458cd	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		

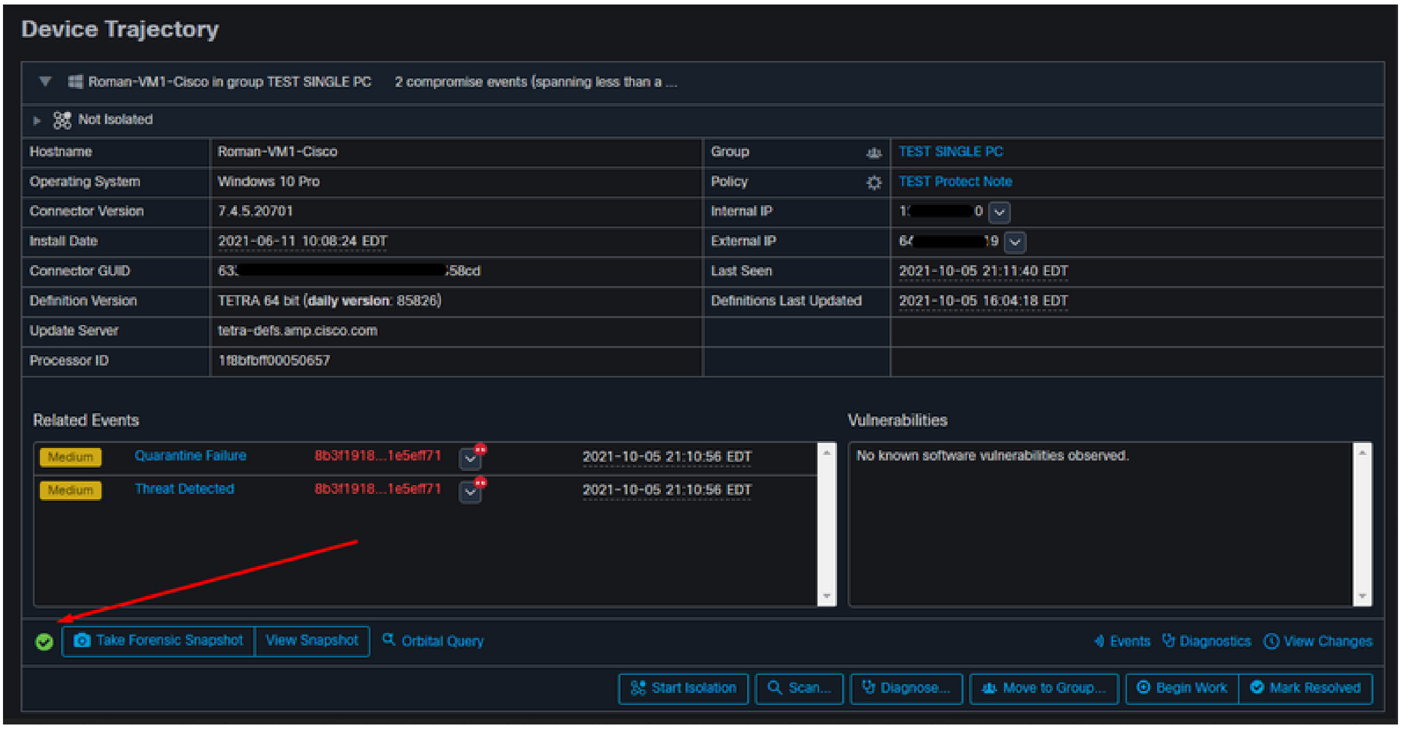
Related Events

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.

然后，将创建快照，如图所示。



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	1[redacted]0
Install Date	2021-06-11 10:08:24 EDT	External IP	64[redacted]19
Connector GUID	63[redacted]58cd	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		

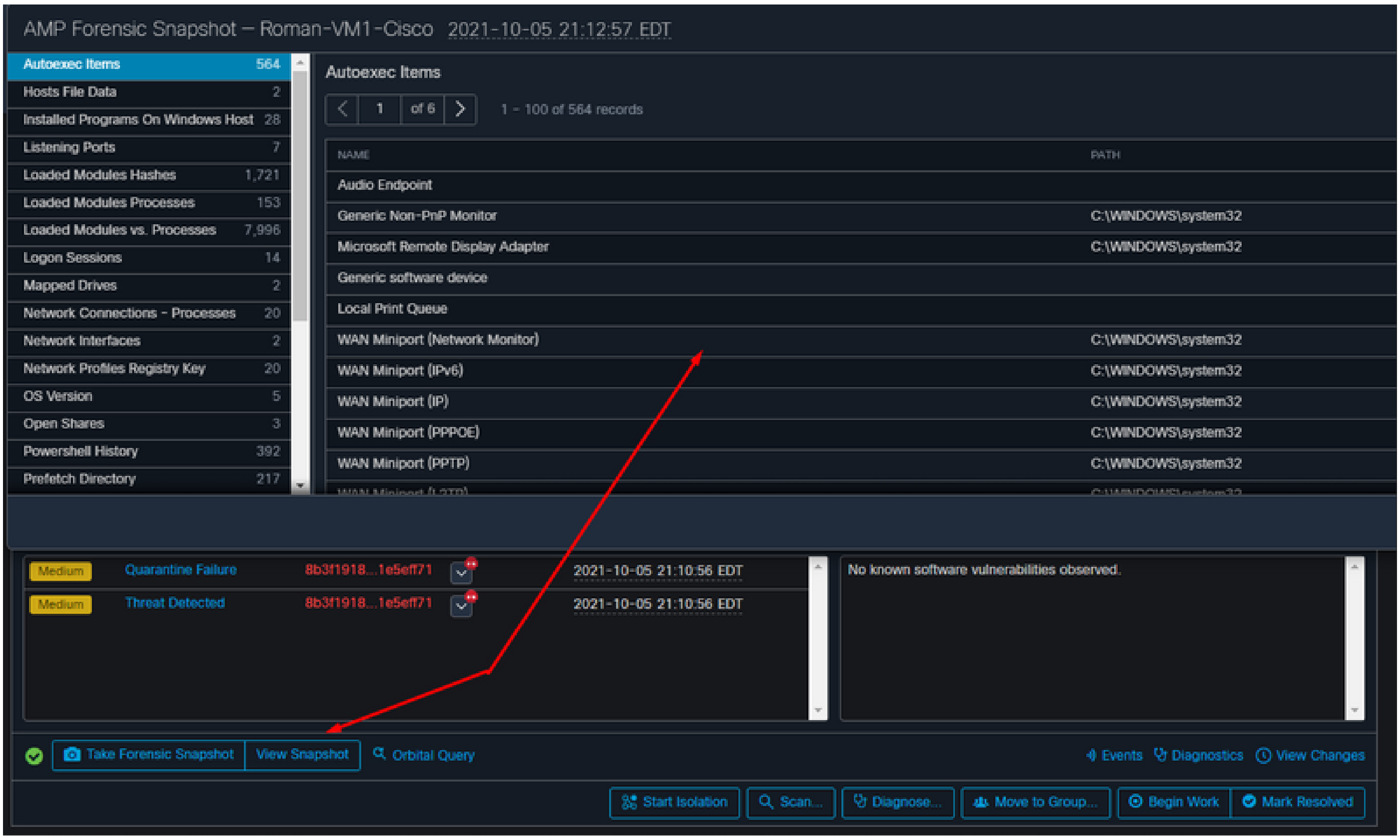
Related Events

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.

现在，您可以查看显示的数据。



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

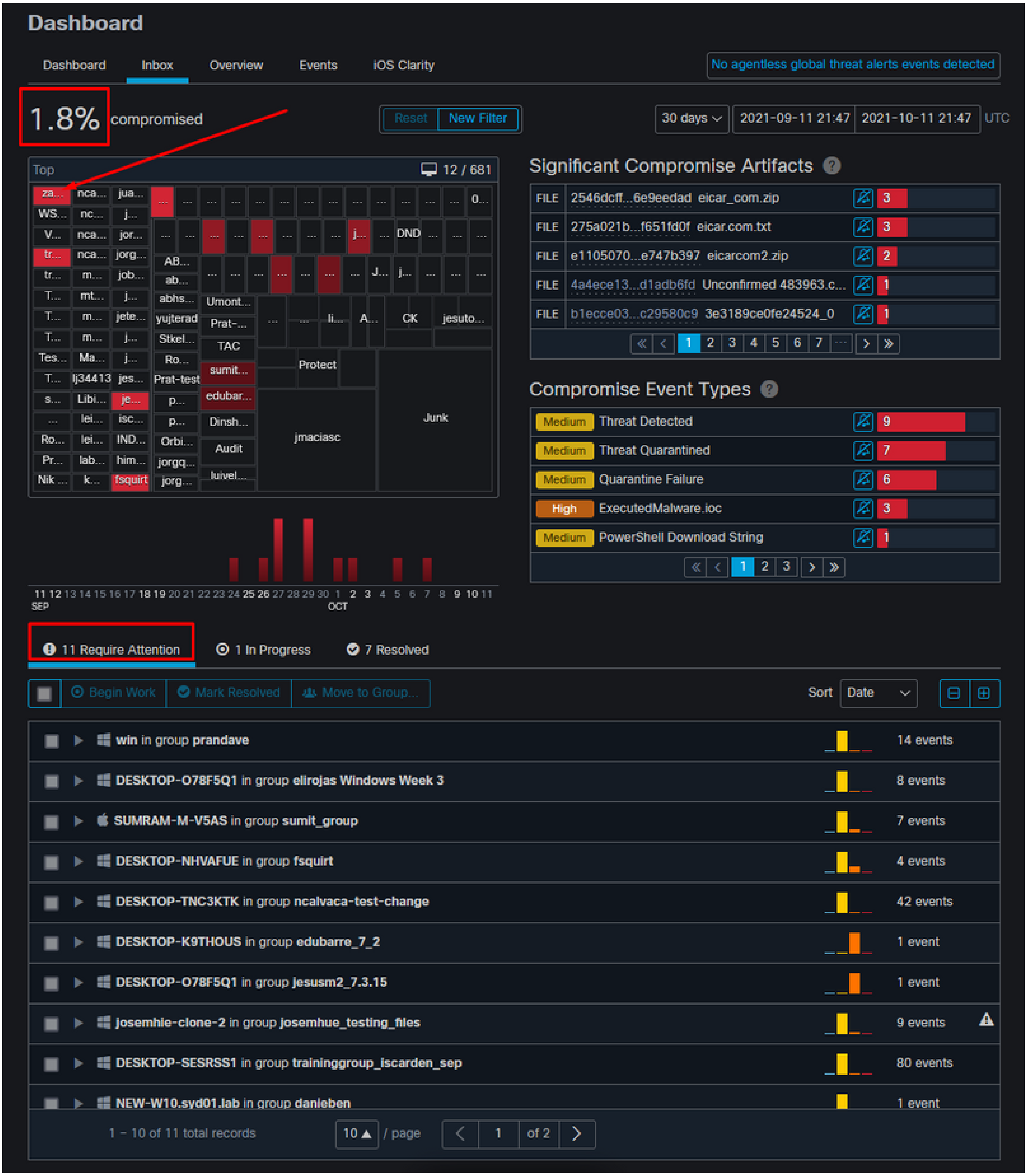
NAME	PATH
Audio Endpoint	
Generic Non-PnP Monitor	C:\WINDOWS\system32
Microsoft Remote Display Adapter	C:\WINDOWS\system32
Generic software device	
Local Print Queue	
WAN Miniport (Network Monitor)	C:\WINDOWS\system32
WAN Miniport (IPv6)	C:\WINDOWS\system32
WAN Miniport (IP)	C:\WINDOWS\system32
WAN Miniport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

提示

在拥有数千个端点和数百个危害的超大型环境中，您可能会遇到导航到单个端点可能是一项挑战的情况。目前，唯一可用的解决方案是使用热图，然后深入到您的危害终端所在的特定组，如下例所示。



Dashboard

No agentless global threat alerts events detected

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

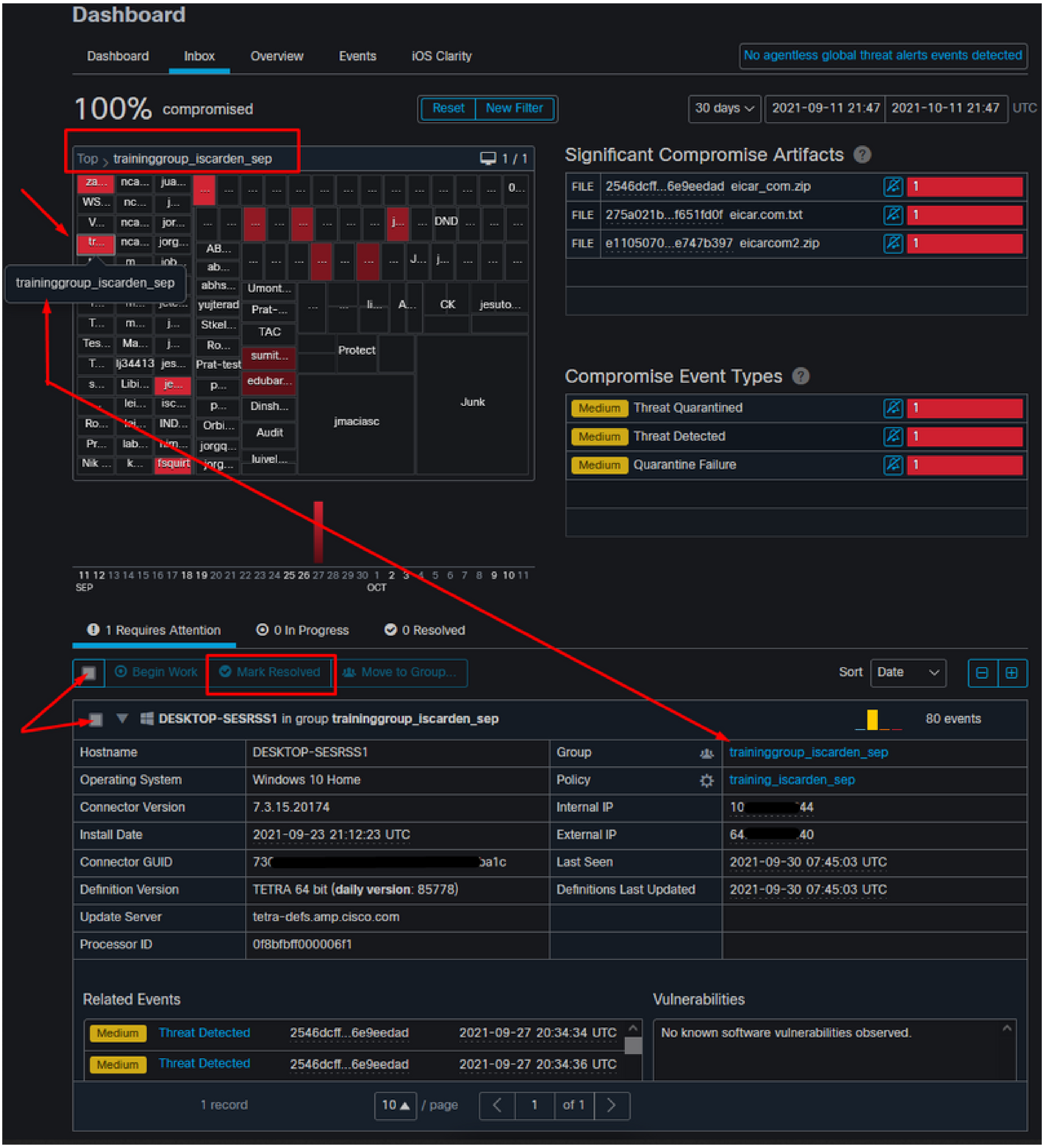
Compromise Event Types

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

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 ›

在热图中选择组后，导航到我们危害了事件的组。由于该组中只有一个终端，请注意100%受感染，这取决于我们所在的特定组。换句话说，如果此组中有2个终端，一个是干净的，另一个受感染的终端显示50%的危害。



100% compromised

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

DESKTOP-SESRSS1 in group traininggroup_iscarden_sep

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]a1c	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.