

# Ações automatizadas - Instantâneo forense

## Contents

[Introduction](#)

[FAQ](#)

[O que é uma máquina comprometida?](#)

[O que é um compromisso?](#)

[O que acontece quando novas detecções ocorrem em uma máquina comprometida?](#)

[Onde posso ver e gerenciar comprometimentos?](#)

[Como uma ação automatizada\\* é acionada?](#)

[Como posso reativar uma ação automática?](#)

[Caso usado - Recriação de laboratório](#)

[Dica](#)

## Introduction

Este documento descreve a funcionalidade de ação automatizada no Secure Endpoint vinculada ao conceito de Compromissos. Compreender o ciclo de vida e o gerenciamento de compromissos são vitais para compreender a funcionalidade das ações automatizadas. Este artigo responde a perguntas sobre a terminologia e a funcionalidade desses conceitos.

## FAQ

### O que é uma máquina comprometida?

Uma máquina comprometida é um endpoint que tem um comprometimento ativo associado a ela. Uma máquina comprometida pode, por projeto, ter apenas um comprometimento ativo de uma vez.

### O que é um compromisso?

Um comprometimento é uma coleção de uma ou mais detecções em uma máquina. A maioria dos eventos de detecção (ameaça detectada, indicações de comprometimento etc.) pode gerar ou se tornar associada a um comprometimento. No entanto, há pares de eventos que podem não desencadear um novo compromisso. Por exemplo, quando ocorre um evento Detectado de Ameaça, mas logo após ele ter um evento associado de Quarentena de Ameaça, isso não gera um novo comprometimento. Logicamente, isso ocorre porque o Secure Endpoint lidou com o possível comprometimento (colocamos a ameaça em quarentena).

### O que acontece quando novas detecções ocorrem em uma máquina comprometida?

Os eventos de detecção são adicionados ao comprometimento existente. Nenhum novo compromisso é criado.

## Onde posso ver e gerenciar comprometerimentos?

Os comprometerimentos são gerenciados na guia Caixa de entrada do console do Secure Endpoint (que é <https://console.amp.cisco.com/compromises> para a nuvem da América do Norte). Uma máquina comprometida está listada na seção **Require Attention** e pode ser eliminada de seu comprometimento pressionando **Mark Resolved**. Além disso, os comprometerimentos são automaticamente eliminados após um mês.

## Como uma ação automatizada\* é acionada?

Ações automatizadas são acionadas com um comprometimento, ou seja, quando uma máquina sem comprometimento se torna uma máquina comprometida. Se uma máquina já comprometida encontrar uma nova detecção, essa detecção será adicionada ao comprometimento, mas como isso não é um novo comprometimento, ela não aciona uma ação automatizada.

## Como posso reativar uma ação automática?

É necessário "limpar" o comprometimento antes de tentar reativar uma ação automática. Lembre-se de que um evento de Ameaça Detectada + Ameaça em Quarentena não é suficiente para gerar um novo evento de comprometimento (e, portanto, não é suficiente para disparar uma nova ação automatizada).

\*Exceção: A ação automatizada "Enviar arquivo para o ThreatGrid" não é afiliada a comprometerimentos e é executada por detecção

## Caso usado - Recriação de laboratório

**Nº 1:** Como dissemos na seção de perguntas frequentes. Os snapshots forenses são obtidos somente em caso de "comprometimento". Em outras palavras, se tentarmos acessar e baixar um arquivo mal-intencionado de um site TEST e o arquivo for sinalizado durante o download e colocado em quarentena que não é considerado um comprometimento e não aciona a ação.

**Note:** Detecção de DFC, Falha de Quarentena e praticamente qualquer coisa que, pela lógica, se encaixe na categoria de evento de comprometimento deve criar Instantâneo Forense.

**Nº 2:** Você só pode gerar um Instantâneo Forense uma vez em um evento comprometido exclusivo que ele não gere um instantâneo, a menos que você resolva a máquina comprometida na caixa de entrada. Se você não resolver o evento comprometido, não gerará nenhum outro snapshot.

Exemplo: Neste laboratório, um script gera atividade mal-intencionada e, como o arquivo é excluído assim que é criado, o Secure Endpoint não conseguiu colocar o arquivo em quarentena na categoria de comprometimento.

Two screenshots of a security console showing file detection details for 'abcde.txt' as 'Win.Ransomware.Eicar:W32.EICAR.15ic'. The top screenshot shows a 'Quarantine: Failed' status, while the bottom screenshot shows a 'Threat Detected' status. Both screenshots include fields for File Name, File Path, File Size, and Parent Filename.

Agora, neste teste, você pode observar ações automatizadas e 3 coisas que aconteceram com base nas configurações.

- O instantâneo foi criado
- O envio foi enviado para o Threat Grid (TG)
- O endpoint foi movido para um grupo separado criado e chamado ISOLAMENTO

Você pode ver tudo isso nessa saída, como mostrado na imagem.

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

Agora, como esse endpoint está comprometido, o próximo teste para provar a teoria com um arquivo mal-intencionado semelhante, mas com um nome diferente, como mostrado na imagem.

Two screenshots of a security console showing file detection details for 'xyz.txt' as 'Win.Ransomware.Eicar:W32.EICAR.15ic'. The top screenshot shows a 'Threat Detected' status, while the bottom screenshot shows a 'Quarantine: Failed' status. Both screenshots include fields for File Name, File Path, File Size, and Parent Filename.

No entanto, como esse compromisso não foi resolvido, você só pode criar um envio de TG. Nenhum outro evento foi gravado, além de desligar o isolamento antes deste 2º teste.

Screenshot of the 'Automated Actions' section in the security console, showing an 'Action Logs' entry for 'Threat Grid Submission on Medium Severity' with a 'Threat Detected' status and a timestamp of 2021-10-05 15:44:13 EDT.

Note: Observe a hora em que a ameaça foi detectada e a ação automatizada é acionada.

O evento não poderá ser reacionado a menos que o ponto de extremidade comprometido seja resolvido. Nesse caso, o painel fica assim. Observe a porcentagem e o botão Mark Resolved junto com os eventos comprometidos. Não importa quantos eventos sejam disparados, você só pode criar um snapshot e o grande número percentual nunca mudou. Esse número representa um comprometimento dentro da sua empresa e se baseia na quantidade total de endpoints na sua empresa. Ele só muda com outra máquina comprometida. Neste exemplo, o número é alto devido a apenas 16 dispositivos no laboratório. Além disso, observe que os eventos de comprometimento são limpos automaticamente quando atingem 31 dias de idade.

# 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 20:58 2021-10-05 20:58 EDT

Top 1 / 18

**TEST SINGLE PC**

Server

CUSTOM

Protect

Audit

PROTECT-NOTE

### Significant Compromise Artifacts

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

### Compromise Event Types

1 event type muted

Medium	Threat Detected	1
Medium	Quarantine Failure	1

5 6 7 8 9 10 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  
SEP OCT

**1** Requires Attention **0** In Progress **3** Resolved

Begin Work  Mark Resolved  Move to Group... Sort Date

**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	192.168.1.10
Install Date	2021-06-11 10:08:24 EDT	External IP	64.100.1.19
Connector GUID	635c...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.

A próxima etapa é criar outro evento e gerar um snapshot forense. A primeira etapa é resolver esse compromisso, clique no botão **Marcar resolução**. Você pode fazer isso por endpoint ou selecionar tudo na sua organização.

1 Requires Attention 0 In Progress 3 Resolved

Begin Work
  Mark Resolved
  Move to Group...
 Sort Date

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	19...0
Install Date	2021-06-11 10:08:24 EDT	External IP	64...9
Connector GUID	63...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		

**Observação:** se você selecionar todos os comprometicos serão redefinidos para 0%.

Depois que o botão Marcar resolvido for selecionado e como apenas um endpoint foi comprometido no painel do Secure Endpoint é semelhante a este. E neste ponto, um novo evento comprometido na máquina de teste foi acionado.

Dashboard

Dashboard Inbox Overview Events iOS Clarity

No agentless global threat alerts events detected

0% compromised

Reset New Filter

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

Top 0 / 18

TEST SINGLE PC

Server

CUSTOM

Protect

Audit

PROTECT-NOTE

Significant Compromise Artifacts ?

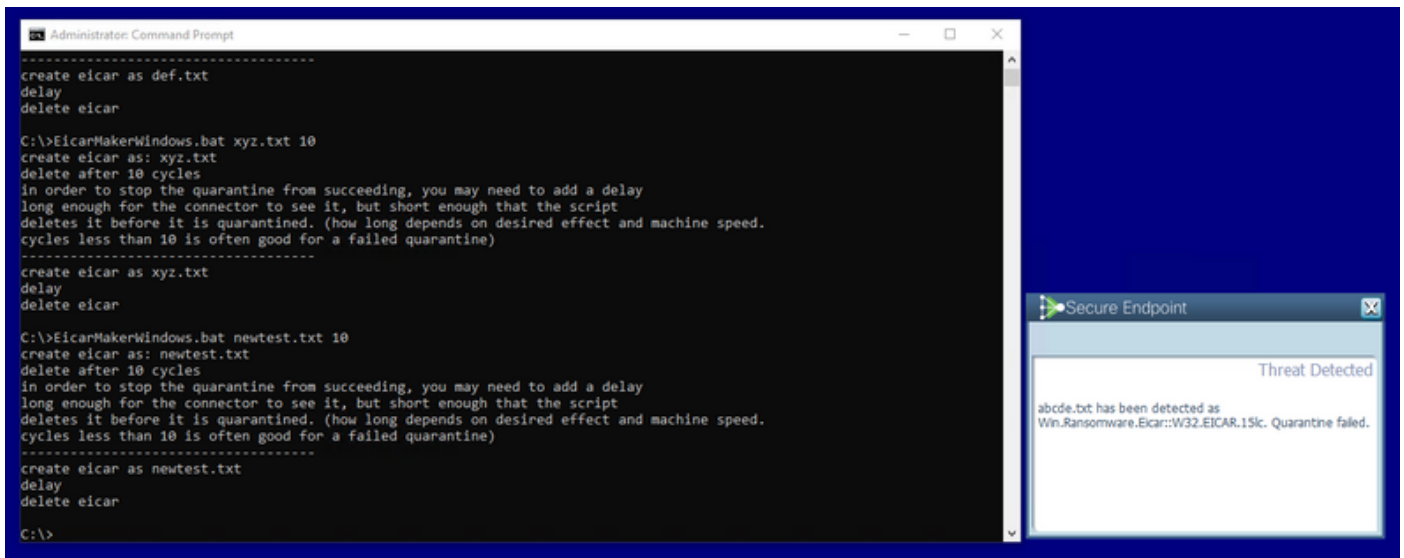
No artifacts

Compromise Event Types ? 1 event type muted

No event types

5 6 7 8 9 10 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  
SEP OCT

O próximo exemplo aciona um evento com um script personalizado que cria e exclui um arquivo mal-intencionado.



O console do Endpoint seguro novamente está comprometido, como mostrado na imagem

**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

Top 1 / 18

5 6 7 8 9 10 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  
SEP OCT

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. .... .0
Install Date	2021-06-11 10:08:24 EDT	External IP	64. .... .9
Connector GUID	65 ..... 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 >

**Significant Compromise Artifacts**

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

**Compromise Event Types** 1 event type muted

Medium	Threat Detected	1
Medium	Quarantine Failure	1

Aqui estão novos eventos em Ações automatizadas, como mostrado na imagem.



## Automated Actions

Automated Actions	Action Logs			
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

Quando o nome de host em Ações automatizadas é selecionado, ele redireciona para a trajetória do dispositivo, onde você pode observar o snapshot que está sendo criado quando você expande a guia Computador, como mostrado na imagem.

### 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. .... 0
Install Date	2021-06-11 10:08:24 EDT	External IP	6. .... 19
Connector GUID	63.....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	1f8bf00050657		

#### 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.

Taking Snapshot... View Snapshot Orbital Query

Start Isolation Scan... Diagnose... Move to Group... Begin Work Mark Resolved

E o instantâneo mais recente é criado, como mostrado na imagem.

### 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. .... 0
Install Date	2021-06-11 10:08:24 EDT	External IP	6. .... 19
Connector GUID	63.....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	1f8bf00050657		

#### 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.

Take Forensic Snapshot View Snapshot Orbital Query

Start Isolation Scan... Diagnose... Move to Group... Begin Work Mark Resolved

E agora você pode ver os dados exibidos.

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.

Take Forensic Snapshot View Snapshot Orbital Query Events Diagnostics View Changes

Start Isolation Scan... Diagnose... Move to Group... Begin Work Mark Resolved

## Dica

Em ambientes muito grandes com milhares de endpoints e centenas de comprometimentos, você pode se deparar com situações em que a navegação para o endpoint individual pode ser um desafio. Atualmente, a única solução disponível é usar o mapa de calor e depois detalhar para um grupo específico em que seu endpoint de comprometimento é como neste exemplo abaixo.

# Dashboard

Dashboard **Inbox** Overview Events iOS Clarity

No agentless global threat alerts events detected

1.8% compromised

Reset New Filter

30 days

2021-09-11 21:47

2021-10-11 21:47

UTC



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

11 Require Attention 1 In Progress 7 Resolved

Begin Work Mark Resolved Move to Group...

Sort Date

Group	Events
win in group prandave	14 events
DESKTOP-O78F5Q1 in group ellrojas 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

## Significant Compromise Artifacts

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

## Compromise Event Types

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

Quando o grupo for selecionado no mapa de calor, navegue até o grupo no qual o evento foi comprometido. Como há apenas um endpoint nesse grupo, observe os 100% comprometidos que agora se baseiam no grupo específico em que estamos. Em outras palavras, se tivermos dois endpoints nesse grupo, um limpo e o outro comprometido mostrarão 50% de comprometimento.

# Dashboard

Dashboard **Inbox** Overview Events iOS Clarity

No agentless global threat alerts events detected

100% compromised

[Reset](#) [New Filter](#)

30 days   UTC

Top > traininggroup_iscarden_sep	
za...	nca...
WS...	nc...
V...	nca...
tr...	nca...
AB...	
abhs...	
yujterad	Umont...
Stkel...	TAC
Tes...	Ma...
T...	lj34413
s...	Libi...
lei...	isc...
Ro...	lei...
Pr...	lab...
Nik...	k...

### Significant Compromise Artifacts

FILE	Artifact	Count
FILE	2546dcff...6e9eedad eicar_com.zip	1
FILE	275a021b...f651fd0f eicar.com.txt	1
FILE	e1105070...e747b397 eicarcom2.zip	1

### Compromise Event Types

Severity	Event Type	Count
Medium	Threat Quarantined	1
Medium	Threat Detected	1
Medium	Quarantine Failure	1

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

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...44	
Install Date	2021-09-23 21:12:23 UTC	External IP	64...40	
Connector GUID	73c...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	0f8bf000006f1			

#### 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  of 1