

# 自動操作 — 調查分析快照

## 目錄

[簡介](#)

[常見問題](#)

[什麼是受損的機器？](#)

[什麼是妥協？](#)

[在受侵害的電腦上發生新檢測時，會發生什麼情況？](#)

[在哪裡可以檢視和管理折衷方案？](#)

[如何觸發自動操作\\*？](#)

[如何重新觸發自動操作？](#)

[用例 — 實驗室重建](#)

[提示](#)

## 簡介

本文檔介紹了安全終端中的自動操作功能與危害概念緊密相關。瞭解危害的生命週期和管理對於理解自動化操作的功能至關重要。本文回答有關這些概念的術語和功能的問題。

## 常見問題

### 什麼是受損的機器？

受危害的電腦是與其關聯的活動危害的終結點。根據設計，受危害的電腦一次只能有一個危害處於活動狀態。

### 什麼是妥協？

危害是在電腦上一個或多個檢測的集合。大多數檢測事件（檢測到的威脅、危害表現等）可能會生成危害或與之關聯。但是，有成對的事件可能不會觸發新的危害。例如，當「檢測到威脅」事件發生，但發生相關威脅隔離事件後不久，不會觸發新的危害。從邏輯上講，這是因為安全端點已處理了潛在的危害（我們隔離了威脅）。

### 在受侵害的電腦上發生新檢測時，會發生什麼情況？

檢測事件會新增到現有危害中。不建立任何新的危害。

### 在哪裡可以檢視和管理折衷方案？

在安全終端控制檯的「收件箱」頁籤(北美雲為<https://console.amp.cisco.com/compromises>)中管理危害。受危害的電腦列在**需要注意**部分下，可以按**Mark Resolved**清除其危害。此外，在一個月後將自動清除危害行為。

### 如何觸發自動操作\*？

在遭受危害時（即非受損電腦成為受損電腦）觸發自動操作。如果已經受損的電腦遇到新檢測，該檢測將被新增到危害中，但由於這不是新危害，因此不會觸發自動操作。

## 如何重新觸發自動操作？

在嘗試重新觸發自動操作之前，必須「清除」危害。請記住，檢測到的威脅+隔離威脅事件不足以生成新的危害事件（因此不足以觸發新的自動化操作）。

\*異常：「向ThreatGrid提交檔案」自動操作與危害無關，並且根據檢測運行

## 用例 — 實驗室重建

#1:如我們在FAQ部分中所述。只有在「洩露」的情況下才拍攝調查快照。換句話說，如果我們嘗試從TEST站點訪問和下載惡意檔案，並且該檔案在下载時被標籤並被隔離，這不會被視為危害並且不會觸發操作。

附註：DFC檢測、隔離失敗以及邏輯上屬於危害事件類別的所有內容都應建立取證快照。

#2:您只能對唯一的受感染事件生成一次調查快照，除非您在收件箱中解析受感染電腦，否則不會生成快照。如果不解決受損事件，則不會生成任何其他快照。

範例：在本實驗中，指令碼會生成惡意活動，而且由於檔案在建立後即被刪除，安全終結點無法隔離該檔案，因此該檔案屬於危害類別。

The image shows two screenshots of a security interface. The top screenshot shows a file detection result for 'abcde.txt' as 'Win.Ransomware.Eicar:W32.EICAR.15ic'. The detection is marked as 'Medium' and 'Quarantine: Failed'. The file path is 'C:\abcde.txt' and the parent filename is 'cmd.exe'. The bottom screenshot shows the same file detection result, but with a 'Threat Detected' status. The parent fingerprint (SHA-256) is 'b99d61d8...6c874450'. Both screenshots include a 'Report' button with a score of 95/10 and options to 'View Upload Status', 'Add to Allowed Applications', and 'File Trajectory'.

在此測試中，您可以檢視自動操作下的內容以及基於設定發生的3件事。

- 已建立快照
- 提交內容已傳送到Threat Grid(TG)
- 端點被移動到已建立並稱為ISOLATION的獨立組

您可以在此輸出中看到所有這些內容，如下圖所示。

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

現在，由於此端點受到危害，下一步測試將用類似的惡意檔案使用不同的名稱來證明該理論，如下圖所示。

Roman-VM1-Cisco detected xyz.txt as Win.Ransomware.Eicar:W32.EICAR.151c Medium Threat Detected 2021-10-05 15:43:42 EDT

File Detection	Detection	Win.Ransomware.Eicar:W32.EICAR.151c
Connector Details	Fingerprint (SHA-256)	8b3f1918...1e5ef71
Comments	File Name	xyz.txt
	File Path	C:\xyz.txt
	Parent Fingerprint (SHA-256)	b99d51d8...6c874450
	Parent Filename	cmd.exe

View Upload Status Add to Allowed Applications File Trajectory

---

Roman-VM1-Cisco detected xyz.txt as Win.Ransomware.Eicar:W32.EICAR.151c Medium Quarantine: Failed 2021-10-05 15:43:42 EDT

File Detection	Detection	Win.Ransomware.Eicar:W32.EICAR.151c
Connector Details	Fingerprint (SHA-256)	8b3f1918...1e5ef71
Comments	File Name	xyz.txt
	File Path	C:\xyz.txt
Error Details	Parent Filename	cmd.exe

View Upload Status Add to Allowed Applications File Trajectory

但是，由於未解決此危害，因此您只能建立TG提交。未記錄其他事件，也在此第2次測試之前關閉隔離。

Stop All Isolations...

Automated Actions Action Logs

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

附註：請注意檢測到威脅並觸發自動操作的時間。

除非已解析損壞的終結點，否則無法重試事件。在這種情況下，儀表板如下所示。請注意百分比和「標籤已解決」按鈕以及受危害事件。無論觸發多少個事件，您都只能建立一個快照，並且大百分比的數字始終不變。該數字表示組織內部的危害，它基於組織中的終端總數。它只能用另一台受損的機器來改變。在本例中，由於實驗中只有16台裝置，因此該數字很高。另請注意，危害事件在達到31天時會自動清除。

**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	<b>TEST SINGLE PC</b>
Operating System	Windows 10 Pro	Policy	<b>TEST Protect Note</b>
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	118bfbff00050657		

**Related Events**

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

1 record 10 / page < 1 of 1 >

**Vulnerabilities**

No known software vulnerabilities observed.

下一步是建立另一個事件並生成取證快照。第一步是解決此危害，按一下**Mark Resolved**按鈕。您可以按終端進行此操作，也可以選擇組織中的所有終端。

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	63E...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		

附註： 如果選擇所有危害都會重置為0%。

選中「標籤已解決」按鈕後，由於安全終結點控制面板上只有一個終結點受到危害，因此該按鈕將如下所示。這時，測試機上一個新的受損事件被觸發。

### Dashboard

Dashboard   **Inbox**   Overview   Events   IOS Clarity

No agentless global threat alerts events detected

0% compromised  

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

Top   0 / 18

TEST SINGLE PC		
Server	CUSTOM	Audit
Protect	PROTECT-NOTE	

#### Significant Compromise Artifacts ?

No artifacts

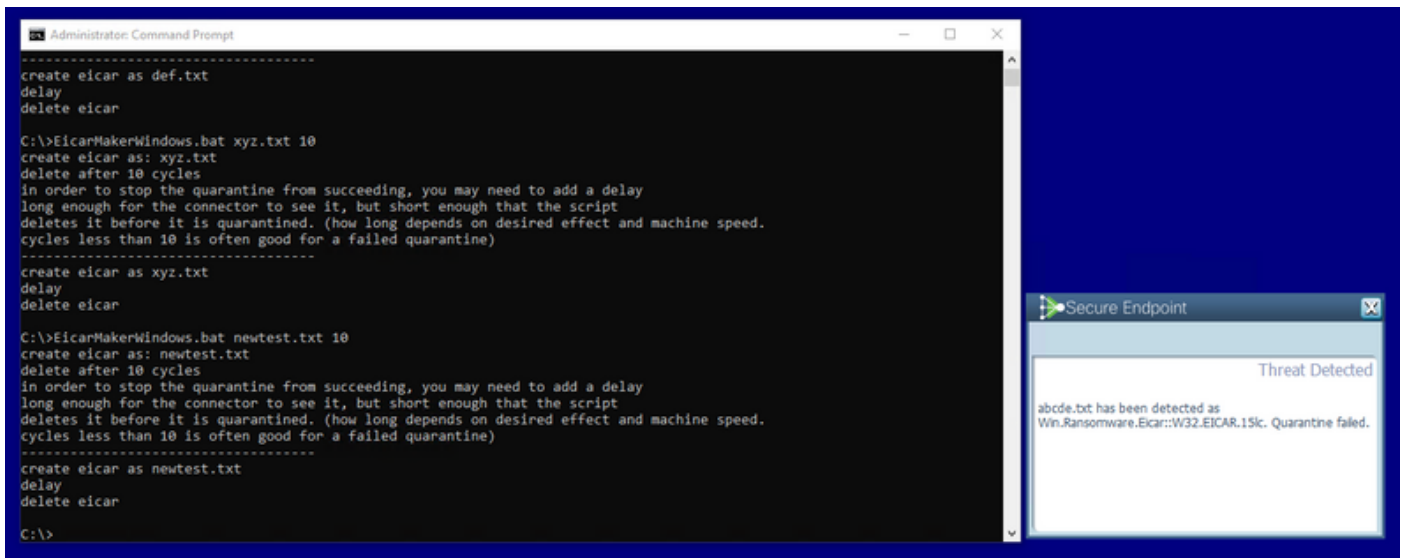
#### Compromise Event Types ?

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

下一個示例使用建立和刪除惡意檔案的自定義指令碼觸發事件。



安全終端控制檯再次受到損害，如下圖所示

**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

下面是「Automated Actions」下面的新事件，如下圖所示。



### Automated Actions

Automated Actions    Action Logs    Stop All Isolations... ?

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

選擇「Automated Actions (自動操作)」下的主機名後，它將重定向到「Device Trajectory (裝置軌跡)」，您可以在其中觀察在展開「computer (電腦)」頁籤後建立的快照，如圖所示。

### 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...1e5ef71	2021-10-05 21:10:56 EDT
Medium	Threat Detected	8b3f1918...1e5ef71	2021-10-05 21:10:56 EDT

Vulnerabilities

No known software vulnerabilities observed.

一分鐘後快照就會建立，如圖所示。

### 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] 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...1e5ef71	2021-10-05 21:10:56 EDT
Medium	Threat Detected	8b3f1918...1e5ef71	2021-10-05 21:10:56 EDT

Vulnerabilities

No known software vulnerabilities observed.

現在您可以檢視顯示的資料。



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

## 提示

在包含數千個端點且存在數百個危害的非常大的環境中，您可能會遇到難以導航到各個端點的情況。目前，唯一可用的解決方案是使用熱度圖，然後向下鑽取到您的危害終點所在的特定組，如下例所示。

# 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



## Significant Compromise Artifacts

FILE	Artifact Name	Count
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

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



11 Require Attention

1 In Progress

7 Resolved

Begin Work Mark Resolved Move to Group...

Sort Date

Group	Endpoint	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	ncaivaca-test-change	42 events
DESKTOP-K9THOUS in group	edubarre_7_2	1 event
DESKTOP-O78F5Q1 in group	Jesum2_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

在熱度圖中選擇組後，導航到危害事件的組。由於該組中只有一個終結點，請注意目前基於我們所在的特定組的100%已洩露。換句話說，如果本組中有2個終端，則一個終端已清除，另一個受危害的終端顯示50%的危害。

