

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](#)

[FAQ](#)

[感染したマシンとは何ですか。](#)

[侵害とは何ですか。](#)

[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。](#)

[妥協はどこで見て管理できますか。](#)

[自動アクション*はどのようにトリガーされますか。](#)

[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。](#)

[使用例：ラボ再現](#)

[ヒント](#)

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>)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。

Two screenshots of a security dashboard showing file detection results for 'abcde.txt' as a Win.Ransomware.Eicar threat. The top screenshot shows 'Quarantine: Failed' and the bottom one shows 'Threat Detected'.

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

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。

Source	Action	Severity	Timestamp
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

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。

Two screenshots of a security dashboard showing file detection results for 'xyz.txt' as a Win.Ransomware.Eicar threat. The top screenshot shows 'Threat Detected' and the bottom one shows 'Quarantine: Failed'.

Section	Field	Value
File Detection	Detection	Win.Ransomware.Eicar:W32.EICAR.15ic
	Fingerprint (SHA-256)	8b3f1918...1e5eff71
Connector Details	File Name	xyz.txt
	File Path	C:\xyz.txt
Error Details	File Size	70 B
	Parent Filename	cmd.exe
	Parent Fingerprint (SHA-256)	b99d61d8...6c874450

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。

Screenshot of the 'Automated Actions' section showing a 'Threat Grid Submission on Medium Severity' event.

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

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

ユ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。

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.

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。

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		

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。

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

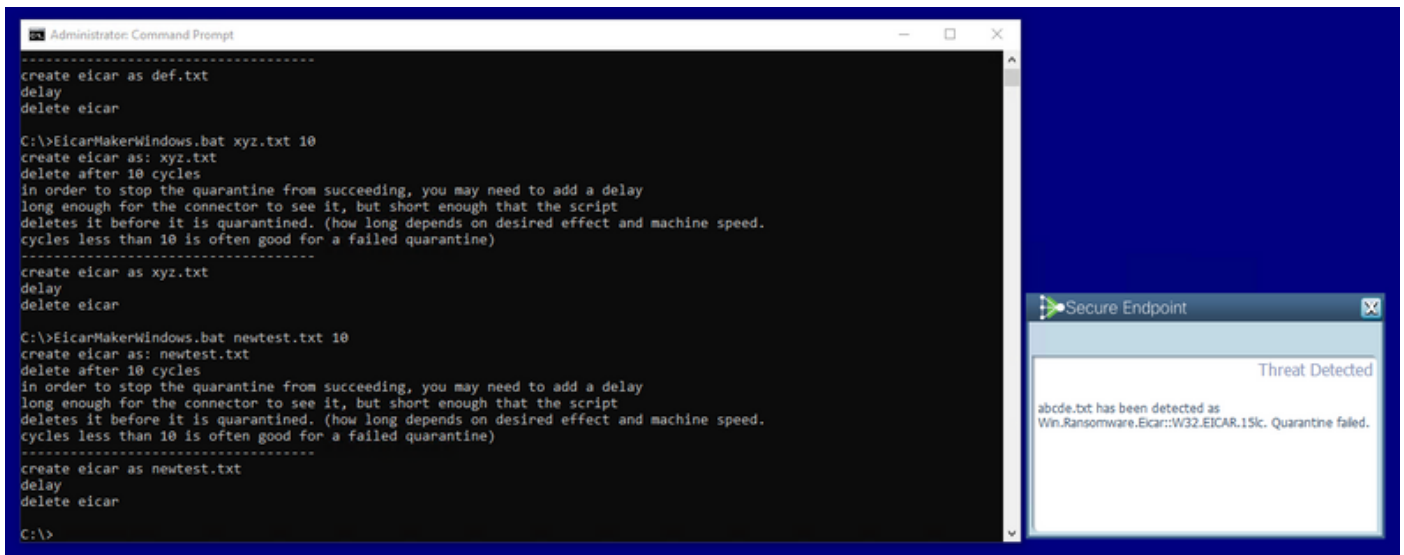
Compromise Event Types

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

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

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

TEST SINGLE PC

Server

CUSTOM

Protect

Audit

PROTECT-NOTE

Significant Compromise Artifacts ?

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

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

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

[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。

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

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。

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

表示されたデータを表示できます。

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

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。

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

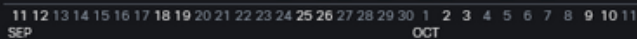


Significant Compromise Artifacts

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

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

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

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いないため、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。

