

Azioni automatizzate - Istantanea legale

Sommario

[Introduzione](#)

[Domande frequenti](#)

[Cos'è una macchina compromessa?](#)

[Che cos'è un compromesso?](#)

[Cosa succede quando si verificano nuovi rilevamenti su una macchina compromessa?](#)

[Dove posso vedere e gestire i compromessi?](#)

[In che modo viene attivata un'azione automatizzata*?](#)

[Come è possibile riattivare un'azione automatica?](#)

[Custodia - Ricreazione in laboratorio](#)

[Suggerimento](#)

Introduzione

In questo documento viene descritta la funzionalità di azione automatizzata in Secure Endpoint legata al concetto di compromessi. Comprendere il ciclo di vita e la gestione dei compromessi sono fondamentali per comprendere la funzionalità delle azioni automatizzate. Questo articolo risponde alle domande relative alla terminologia e alle funzionalità di questi concetti.

Domande frequenti

Cos'è una macchina compromessa?

Un computer compromesso è un endpoint a cui è associato un compromesso attivo. Una macchina compromessa può, per progettazione, avere un solo compromesso attivo alla volta.

Che cos'è un compromesso?

Un compromesso è una raccolta di uno o più rilevamenti su una macchina. La maggior parte degli eventi di rilevamento (rilevamento minacce, segni di compromissione, ecc.) può generare o essere associata a un compromesso. Tuttavia, esistono coppie di eventi che potrebbero non attivare un nuovo compromesso. Ad esempio, quando si verifica un evento Rilevato minaccia, ma subito dopo che a esso è associato un evento In quarantena minaccia, non viene attivata una nuova compromissione. Logicamente, ciò è dovuto al fatto che Secure Endpoint ha gestito il potenziale compromesso (la minaccia è stata messa in quarantena).

Cosa succede quando si verificano nuovi rilevamenti su una macchina compromessa?

Gli eventi di rilevamento vengono aggiunti al compromesso esistente. Non viene creato alcun nuovo compromesso.

Dove posso vedere e gestire i compromessi?

I compromessi vengono gestiti nella scheda Posta in arrivo della console Secure Endpoint (<https://console.amp.cisco.com/compromises> per il cloud Nord America). Un computer compromesso è elencato nella sezione **Richiedi attenzione** e può essere eliminato premendo **Mark Resolved**. Inoltre, i compromessi vengono automaticamente cancellati dopo un mese.

In che modo viene attivata un'azione automatizzata*?

Le azioni automatizzate vengono attivate a seguito di un compromesso, ovvero quando una macchina senza compromessi diventa una macchina compromessa. Se una macchina già compromessa incontra un nuovo rilevamento, questo rilevamento viene aggiunto al compromesso, ma poiché non si tratta di un nuovo compromesso, non attiva un'azione automatica.

Come è possibile riattivare un'azione automatica?

È necessario "chiarire" il compromesso prima di tentare di riattivare un'azione automatizzata. Tenete presente che un evento Threat Detected + Threat Quarantined non è sufficiente per generare un nuovo evento di compromesso (e quindi non è sufficiente per attivare una nuova azione automatica).

*Eccezione: L'azione automatizzata "Invia file a ThreatGrid" non è associata a compromessi ed è eseguita per rilevamento

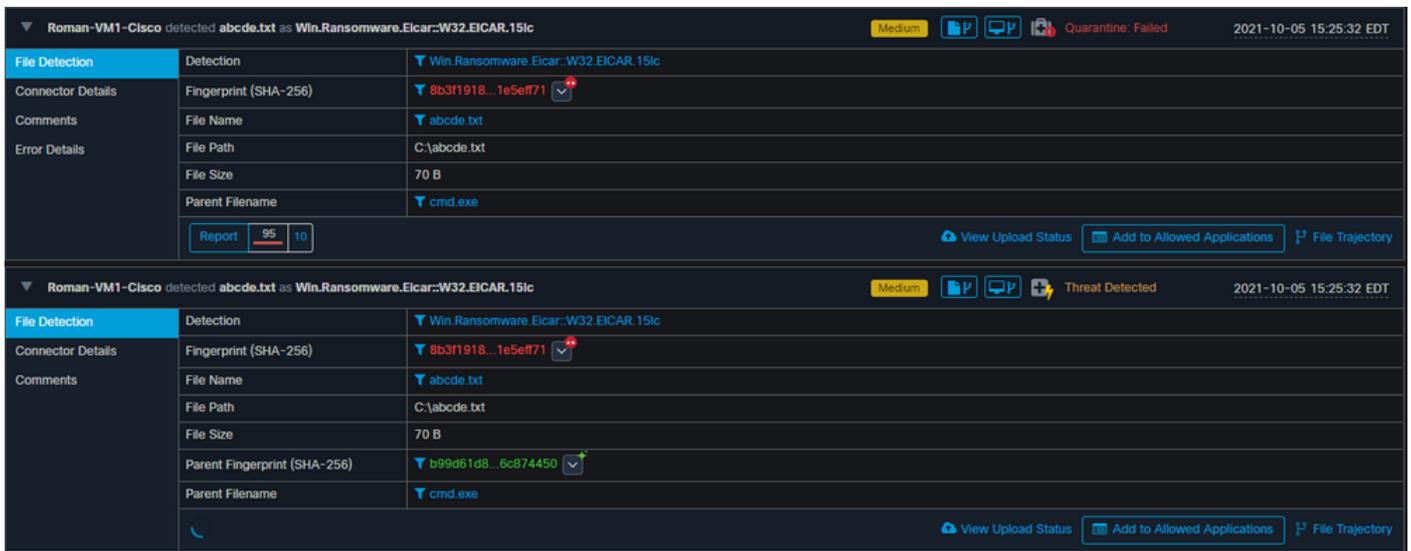
Custodia - Ricreazione in laboratorio

N. 1: Come indicato nella sezione FAQ. Le istantanee forensi sono prese solo in caso di "compromesso". In altre parole, se si tenta di accedere e scaricare un file dannoso da un sito TEST e il file viene contrassegnato al momento del download e messo in quarantena, ciò non è considerato un compromesso e non attiva l'azione.

Nota: Rilevamento DFC, errore di quarantena e quasi tutto ciò che secondo la logica rientra nella categoria di evento di compromesso dovrebbe creare un'istantanea forense.

N. 2: È possibile generare un'istantanea solo una volta su un evento compromesso univoco. Non genera un'istantanea a meno che non si risolva il computer compromesso nella Posta in arrivo. Se l'evento compromesso non viene risolto, non verrà generata alcuna altra istantanea.

Esempio: In questa esercitazione uno script genera attività dannose e, poiché il file viene eliminato non appena creato e Endpoint protetto non è stato in grado di mettere in quarantena il file che rientra nella categoria compromissione.



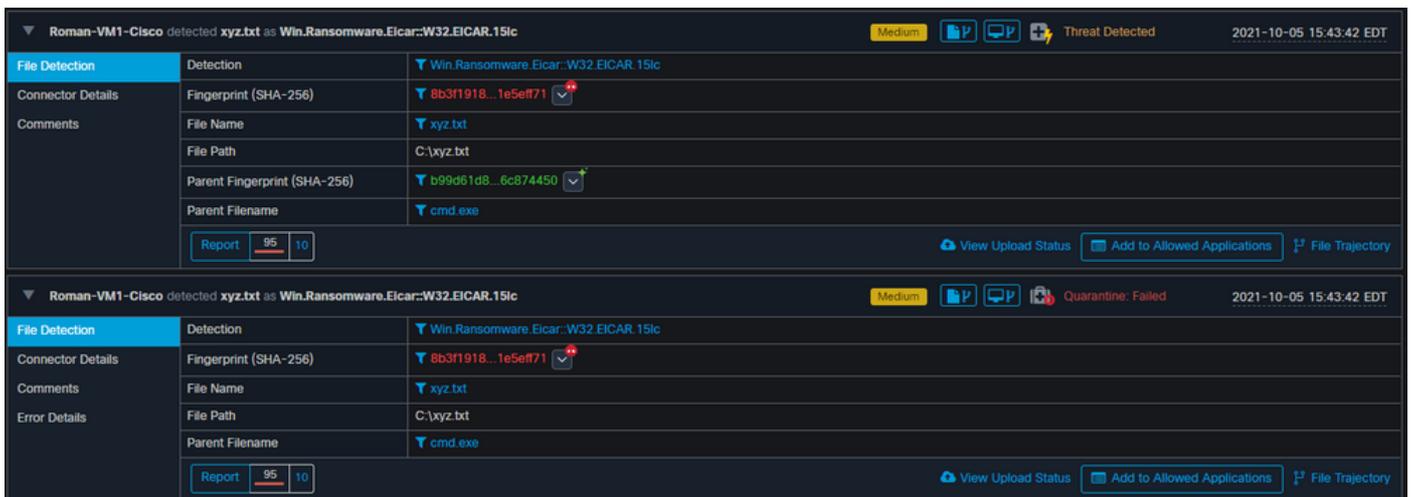
In questo test è possibile esaminare le operazioni automatizzate e le tre operazioni eseguite in base alle impostazioni.

- Snapshot creato
- Invio a Threat Grid (TG)
- L'endpoint è stato spostato in un gruppo separato creato e denominato ISOLATION

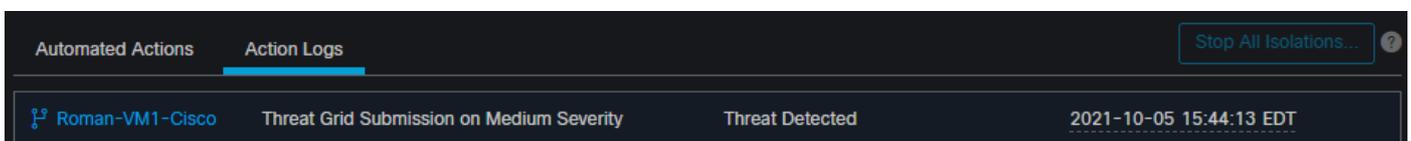
Potete vedere tutto questo in questo output, come mostrato nell'immagine.

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

Ora, dato che questo endpoint è compromesso, il prossimo test per provare la teoria con un simile file dannoso ma con un nome diverso, come mostrato nell'immagine.



Tuttavia, poiché questo compromesso non è stato risolto, è possibile solo creare un invio TG. Non sono stati registrati altri eventi. Disattivare anche l'isolamento prima del 2° test.



Nota: Si noti l'ora in cui la minaccia è stata rilevata e l'avvio automatico delle azioni.

L'evento non può essere riavviato a meno che non venga risolto l'endpoint compromesso. In questo caso, il dashboard avrà questo aspetto. Notare la percentuale e il pulsante Mark Risolto insieme agli eventi compromessi. Indipendentemente dal numero di eventi attivati, è possibile creare una sola istantanea e il numero percentuale elevato non è mai stato modificato. Tale numero rappresenta un compromesso all'interno dell'organizzazione e si basa sul totale degli endpoint nell'organizzazione. Cambia solo con un'altra macchina compromessa. Nell'esempio, il numero è alto perché il laboratorio dispone solo di 16 dispositivi. Inoltre, gli eventi di compromesso vengono cancellati automaticamente una volta raggiunti i 31 giorni di età.

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

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	64.155.78.19
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	118bfbff00050657		

Compromise Event Types ? 1 event type muted

Medium	Threat Detected	1
Medium	Quarantine Failure	1

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.

Il passaggio successivo consiste nel creare un altro evento e generare un'istantanea forense. Il primo passo è risolvere questo compromesso, fare clic sul pulsante **Segna come risolto**. È possibile eseguire questa operazione per ciascun endpoint oppure selezionare tutto nell'organizzazione.

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		

Nota: Se si selezionano tutti i compromessi, viene ripristinato lo 0%.

Dopo aver selezionato il pulsante Segna come risolto e poiché nel dashboard dell'endpoint protetto è stato compromesso un solo endpoint, avrà l'aspetto seguente. E a questo punto, è scattato un nuovo evento compromesso sulla macchina di test.

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

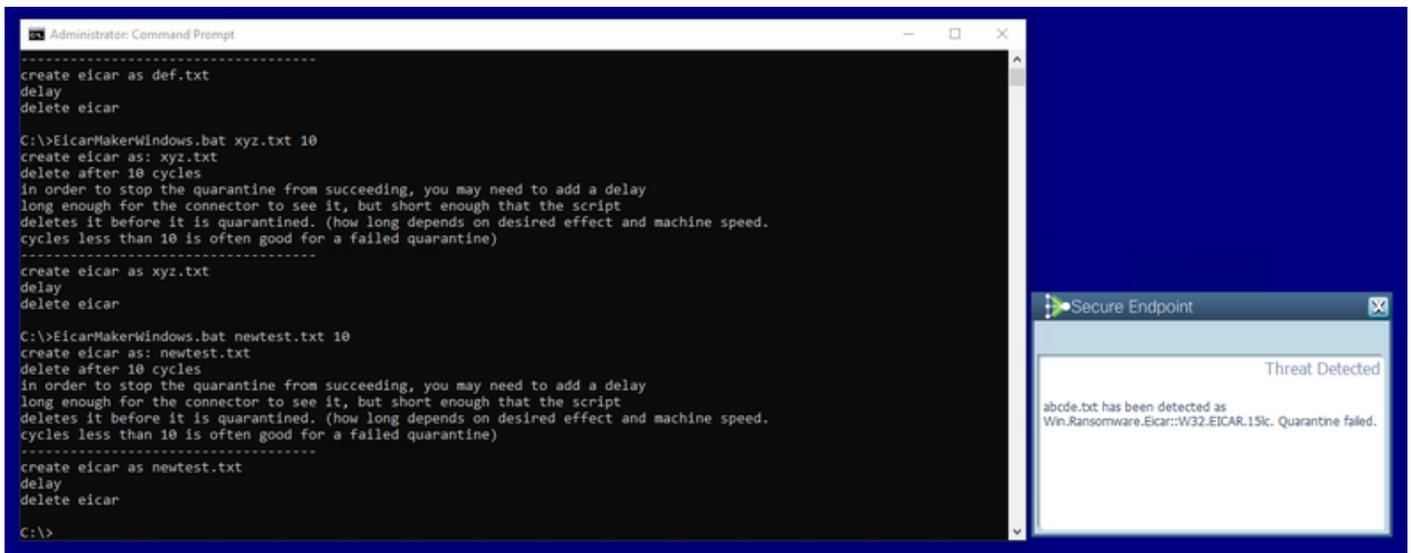
Compromise Event Types

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

Nell'esempio successivo viene attivato un evento con uno script personalizzato che crea ed elimina un file dannoso.



La console dell'endpoint sicuro è ancora una volta compromessa, come mostrato nell'immagine

Dashboard

Dashboard **Inbox** Overview Events iOS Clarity

No agentless global threat alerts events detected

5.6% compromised

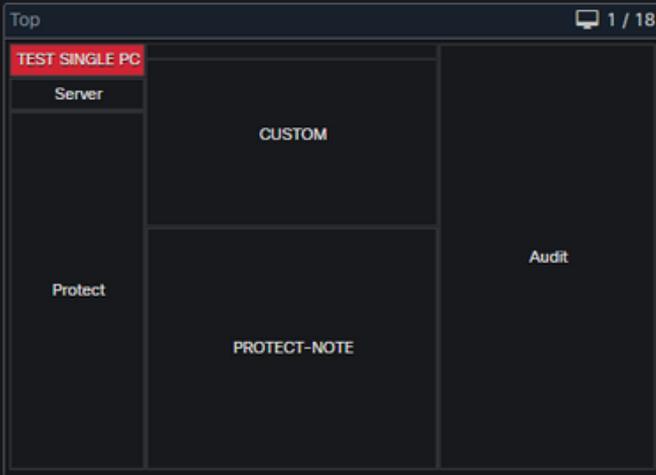
Reset New Filter

30 days

2021-09-05 21:14

2021-10-05 21:14

EDT



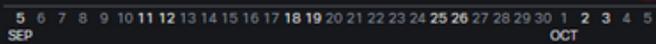
Significant Compromise Artifacts

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

Grid List

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	6558cd	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

Di seguito sono riportati i nuovi eventi in Azioni automatiche, come mostrato nell'immagine.

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 il nome host in Azioni automatiche è selezionato, viene reindirizzato alla traiettoria del dispositivo dove è possibile osservare la copia istantanea creata dopo aver espanso la scheda del computer, come mostrato nell'immagine.

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 minuto dopo viene creata una copia istantanea, come mostrato nell'immagine.

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

Ora è possibile visualizzare i dati visualizzati.

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

Suggerimento

In ambienti molto grandi con migliaia di endpoint e centinaia di compromessi, è possibile trovarsi in situazioni in cui la navigazione verso il singolo endpoint potrebbe rappresentare una sfida. Al momento, l'unica soluzione disponibile consiste nell'utilizzare la mappa termica e quindi eseguire il drilling verso il basso a un gruppo specifico in cui l'endpoint di compromesso è come nell'esempio seguente.

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 Require Attention 1 In Progress 7 Resolved

Begin Work Mark Resolved Move to Group...

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

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

Una volta selezionato il gruppo nella mappa termica, spostatevi sul gruppo in cui l'evento è stato compromesso. Dato che c'è un solo endpoint in quel gruppo, vi preghiamo di notare il 100% compromesso che si basa ora sul gruppo specifico in cui ci troviamo. In altre parole, se abbiamo due endpoint in questo gruppo uno pulito e l'altro compromesso mostra un compromesso del 50%.

