

Geautomatiseerde acties - Forensische Snapshot

Inhoud

[Inleiding](#)

[FAQ](#)

[Wat is een gecompromitteerde machine?](#)

[Wat is een compromis?](#)

[Wat gebeurt er als er nieuwe detecties optreden op een gecompromitteerde machine?](#)

[Waar kan ik compromissen zien en beheren?](#)

[Hoe wordt een geautomatiseerde actie* geactiveerd?](#)

[Hoe kan ik een geautomatiseerde actie opnieuw activeren?](#)

[Gebruikte case - Lab Recreate](#)

[Tip](#)

Inleiding

Dit document beschrijft de functionaliteit voor geautomatiseerde actie in Secure Endpoint is gekoppeld aan het concept Compromiscue. Begrijp de levenscyclus en het beheer van compromissen zijn essentieel om de functionaliteit van geautomatiseerde acties te begrijpen. Dit artikel beantwoordt vragen over de terminologie en de functionaliteit van deze concepten.

FAQ

Wat is een gecompromitteerde machine?

Een gecompromitteerde machine is een eindpunt dat een actief compromis verbonden heeft. Een gecompromitteerde machine kan per ontwerp slechts één compromis tegelijk actief hebben.

Wat is een compromis?

Een compromis is een verzameling van een of meer detecties op een machine. De meeste detectiegebeurtenissen (bedreigingsdetectie, indicaties voor compromis, enz.) kunnen een compromis opleveren of sluiten. Er zijn echter paren van gebeurtenissen die wellicht geen nieuw compromis zullen opleveren. Wanneer er bijvoorbeeld een 'Threat Detected'-gebeurtenis plaatsvindt, maar kort nadat deze een bijbehorende Threat Quarantated-gebeurtenis heeft, veroorzaakt dit geen nieuw compromis. Logisch gezien is dit omdat Secure Endpoint met het mogelijke compromis is omgesprongen (we quarantaine de dreiging).

Wat gebeurt er als er nieuwe detecties optreden op een gecompromitteerde machine?

Het/de detectieevenement(en) wordt/worden toegevoegd aan het bestaande compromis. Er wordt geen nieuw compromis tot stand gebracht.

Waar kan ik compromissen zien en beheren?

Compromissen worden beheerd in het tabblad Inbox van de Secure Endpoint console (<https://console.amp.cisco.com/compromises> voor de Noord-Amerikaanse cloud). Een gecompromitteerde machine staat onder het gedeelte **Attire Attire Attentie** en kan worden gewist uit het compromis door op **Mark Resolved** te drukken. Bovendien worden compromissen automatisch na een maand gewist.

Hoe wordt een geautomatiseerde actie* geactiveerd?

Geautomatiseerde acties worden geactiveerd op een compromis dat wil zeggen wanneer een niet-gecompromitteerde machine een gecompromitteerde machine wordt. Als een al gecompromitteerde machine een nieuwe detectie tegenkomt, wordt deze detectie toegevoegd aan het compromis, maar aangezien dit geen nieuw compromis is, veroorzaakt het geen geautomatiseerde actie.

Hoe kan ik een geautomatiseerde actie opnieuw activeren?

Het compromis moet worden "gesneden" voordat wordt geprobeerd een geautomatiseerde actie opnieuw op gang te brengen. Houd in gedachten dat een bedreigde + bedreigde Garandeerde gebeurtenis niet voldoende is om een nieuw compromisevent op te zetten (en dus niet genoeg is om een nieuwe geautomatiseerde actie te starten).

*Uitzondering: De geautomatiseerde actie "Bestand indienen bij ThreatGrid" is niet aangesloten op compromissen, en wordt per detectie uitgevoerd

Gebruikte case - Lab Recreate

#1: Zoals we in het FAQ-gedeelte hebben aangegeven. Forensische momentopnamen worden alleen genomen in het geval van "compromis". Met andere woorden, als we proberen om een kwaadaardig bestand van een TEST-site te downloaden en te downloaden en het bestand wordt gesignaleerd bij download en quarantaine, dan wordt dat niet als een compromis beschouwd en wordt de actie niet geactiveerd.

Opmerking: DFC Detection, Quarantine Fail, en vrijwel alles wat door de logica in de categorie van compromisgebeurtenissen valt, zou Forensisch Snapshot moeten creëren.

#2: U kunt alleen Forensische Snapshot genereren op een uniek gecompromitteerd evenement als het geen snapshot genereert tenzij u de gecompromitteerde machine in uw inbox oplost. Als u de gecompromitteerde gebeurtenis niet oplost, genereert u geen andere momentopname.

Voorbeeld: In dit lab genereert een script kwaadaardige activiteit en omdat het bestand gewist wordt zodra het gemaakt is en Secure Endpoint niet in staat is om het bestand in quarantaine te plaatsen voor een compromitterende categorie.

The screenshots show the following details:

- File Detection:** Detection: Win.Ransomware.Eicar:W32.EICAR.15ic
- Connector Details:** Fingerprint (SHA-256): 8b3f1918...1e5ef771
- Comments:** File Name: abcde.txt
- Error Details:** File Path: C:\abcde.txt, File Size: 70 B, Parent Filename: cmd.exe

Buttons: Report (95/10), View Upload Status, Add to Allowed Applications, File Trajectory.

In deze test kan je onder geautomatiseerde handelingen kijken en 3 dingen die gebeurde gebaseerd op de instellingen.

- Snapshot werd gemaakt
- Indiening werd naar Threat Grid (TG) verzonden
- Het eindpunt werd verplaatst naar een afzonderlijke groep die ISOLATION werd gecreëerd en genoemd

U kunt dit alles in deze uitvoer zien, zoals in de afbeelding wordt weergegeven.

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

Aangezien dit eindpunt gecompromitteerd is, de volgende test om de theorie met een soortgelijk kwaadaardig bestand maar met een andere naam aan te tonen, zoals in de afbeelding getoond wordt.

The screenshots show the following details:

- File Detection:** Detection: Win.Ransomware.Eicar:W32.EICAR.15ic
- Connector Details:** Fingerprint (SHA-256): 8b3f1918...1e5ef771
- Comments:** File Name: xyz.txt
- Error Details:** File Path: C:\xyz.txt, Parent Fingerprint (SHA-256): b99d61d8...6c874450, Parent Filename: cmd.exe

Buttons: Report (95/10), View Upload Status, Add to Allowed Applications, File Trajectory.

Aangezien dit compromis echter niet is opgelost, kunt u alleen een TG-voorstel opstellen. Er werden geen andere voorvallen geregistreerd en de isolatie werd ook uitgeschakeld voor deze 2^e test.

Automated Actions	Action Logs	Stop All Isolations...
Roman-VM1-Cisco	Threat Grid Submission on Medium Severity	Threat Detected
		2021-10-05 15:44:13 EDT

Opmerking: Let op het tijdstip waarop de dreiging is gedetecteerd en automatische actie triggers instelt.

De gebeurtenis kan niet opnieuw geactiveerd worden, tenzij het gecompromitteerde eindpunt is opgelost. In dit geval ziet het dashboard er zo uit. Let op het percentage en de knop Mark Resolved samen met de gecompromitteerde gebeurtenissen. Ongeacht het aantal gebeurtenissen dat wordt geactiveerd, kunt u slechts één momentopname maken en het grote procentuele aantal is nooit gewijzigd. Dat getal vertegenwoordigt compromissen binnen uw organisatie en is gebaseerd op de totale hoeveelheid eindpunten in uw organisatie. Het verandert alleen met een andere gecompromitteerde machine. In dit voorbeeld is het aantal hoog door slechts 16 apparaten in het lab. Houd er ook rekening mee dat compromisgebeurtenissen automatisch worden gewist zodra ze 31 dagen oud zijn.

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	64.100.100.19
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		

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.

1 record 10 / page < 1 of 1 >

De volgende stap is het creëren van een andere gebeurtenis en het creëren van een forensische momentopname. De eerste stap is om dit compromis op te lossen, klikt u op de knop **Mark Resolved**. U kunt dit per eindpunt doen of u kunt alles in uw organisatie selecteren.

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		

Opmerking: Als u alle compromissen selecteert, worden ze teruggezet op 0%.

Zodra de knop Mark Resolved is geselecteerd en omdat slechts één eindpunt werd gecompromitteerd op het Secure Endpoint dashboard lijkt dit. Op dat moment werd een nieuw gecompromitteerd evenement op de testmachine geactiveerd.

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

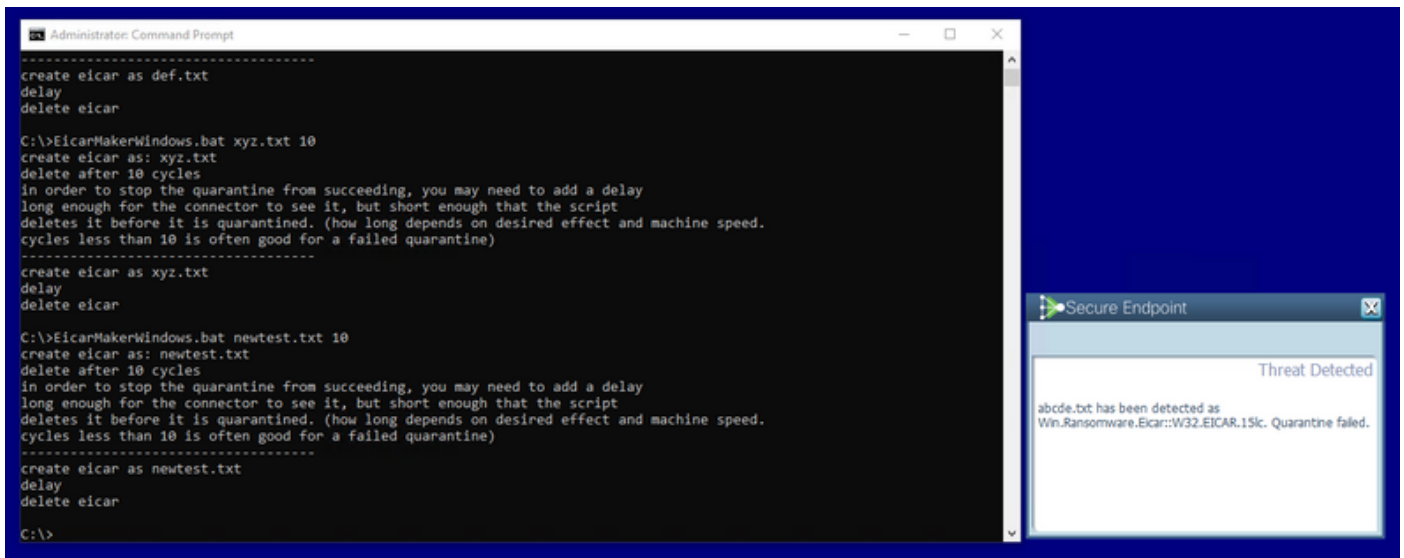
Compromise Event Types

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

Het volgende voorbeeld veroorzaakt een gebeurtenis met een douane script dat een kwaadaardig bestand maakt en verwijdert.



Secure Endpoint console opnieuw gecompromitteerd, zoals in de afbeelding getoond

Dashboard

Dashboard **Inbox** Overview Events iOS Clarity

No agentless global threat alerts events detected

5.6% compromised

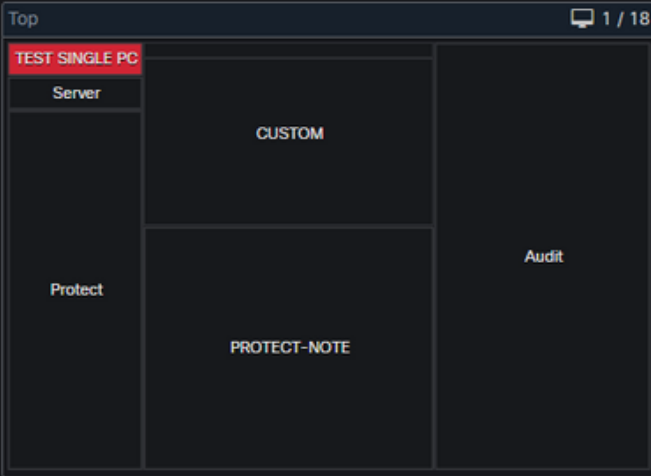
Reset New Filter

30 days

2021-09-05 21:14

2021-10-05 21:14

EDT



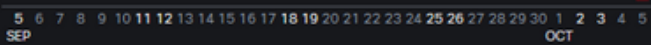
Significant Compromise Artifacts

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	1.0
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

Hier zijn nieuwe gebeurtenissen onder Geautomatiseerde handelingen, zoals in de afbeelding weergegeven.

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	

Wanneer de hostname onder Geautomatiseerde handelingen is geselecteerd, wordt deze omgeleid naar Apparaattraject waar u de snapshot kunt observeren die wordt gemaakt als u het computertabblad hebt uitgevouwen, zoals in de afbeelding wordt getoond.

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

En een minuut later momentopname wordt gecreëerd, zoals in de afbeelding wordt getoond.

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

Nu kun je de weergegeven gegevens bekijken.

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

Tip

In zeer grote omgevingen met duizenden eindpunten en honderden compromissen, kan je in situaties lopen waar de navigatie naar het individuele eindpunt een uitdaging zou kunnen zijn. Op dit moment is de enige beschikbare oplossing: gebruik de hittekaart en boor vervolgens naar een specifieke groep waar uw compromiseindpunt is zoals in dit voorbeeld hieronder.

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

Top 12 / 681

za...	nca...	jua...	0...
WS...	nc...	j...
V...	nca...	jor...	DND
tr...	nca...	jorg...	AB...
tr...	m...	job...	ab...	J...	J...
T...	mt...	j...	abhs...	Umont...
T...	m...	jete...	yujterad	Prat-
T...	m...	j...	Stkel...	TAC
Tes...	Ma...	j...	Ro...	sumit...	Protect
T...	lj34413	jes...	Prat-test	edubar...	Junk
s...	Libi...	je...	p...	Dinsh...
...	lei...	isc...	p...	Dinsh...
Ro...	lei...	IND...	Orbi...	Audit
Pr...	lab...	him...	jorgq...	luivel...
Nik...	k...	fsquirt	jorg...

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

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

Zodra de groep geselecteerd is in de hittekaart navigeer naar die groep waarin we de gebeurtenis gecompromitteerd hebben. Aangezien er slechts één eindpunt in die groep is, merk ik op dat er 100% compromissen zijn gesloten, die nu gebaseerd zijn op de specifieke groep waarin wij ons bevinden. Met andere woorden, als we twee eindpunten in deze groep hebben, één schoon en het andere compromis geeft 50 procent compromis.

Dashboard

Dashboard **Inbox** Overview Events iOS Clarity

No agentless global threat alerts events detected

100% compromised

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

30 days v 2021-09-11 21:47 2021-10-11 21:47 UTC

Top > **traininggroup_iscarden_sep** 1 / 1

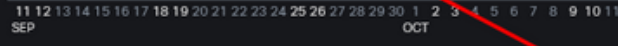
za...	nca...	jua...	0...
WS...	nc...	j...
V...	nca...	jor...	DND
tr...	nca...	jorg...
...	AB...
...	abhs...
...	Umont...
...	yujterad	Prat...
T...	m...	j...	Stkel...	TAC
Tes...	Ma...	j...	Ro...	sumit...	Protect
T...	lj34413	jes...	Prat-test	edubar...
s...	Libi...	je...	p...	Dinsh...	Junk
...	lei...	isc...	p...
Ro...	lei...	IND...	Orbi...
Pr...	lab...	...	jorgq...	Audit
Nik...	k...	fsquirt	jorg...	luivel...

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



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

[Begin Work](#) **Mark Resolved** [Move to Group...](#) Sort Date v

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...3a1c	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	Vulnerabilities								
<table border="1"><tr><td>Medium</td><td>Threat Detected</td><td>2546dcff...6e9eedad</td><td>2021-09-27 20:34:34 UTC</td></tr><tr><td>Medium</td><td>Threat Detected</td><td>2546dcff...6e9eedad</td><td>2021-09-27 20:34:36 UTC</td></tr></table>	Medium	Threat Detected	2546dcff...6e9eedad	2021-09-27 20:34:34 UTC	Medium	Threat Detected	2546dcff...6e9eedad	2021-09-27 20:34:36 UTC	No known software vulnerabilities observed.
Medium	Threat Detected	2546dcff...6e9eedad	2021-09-27 20:34:34 UTC						
Medium	Threat Detected	2546dcff...6e9eedad	2021-09-27 20:34:36 UTC						

1 record 10 / page < 1 of 1 >