Identify Conditions to Trigger Automated Actions in Secure Endpoint

Contents

Introduction

This document describes conditions that need to be met in order to trigger Automated Actions.

Background Information

Automated Actions get triggered upon a compromise (means an un-compromised machine becomes a compromised machine). If an already-compromised machine triggers a new detection, this detection is added to the compromise, but since this is not a new compromise, it does not trigger an automated action.

One exception to this is the severity level. Automated actions get triggered based on criteria which is severity, nevertheless, compromises do not have severity by itself (onlyindividual detections do). If an Automated Action is configured to a severity level of high and a detection triggers as medium level, it does not trigger the action. If a subsequent event is added to the compromise that is high, the action triggers as this new detection is in the compromise that already exists.

What is a compromised machine?

A compromised machine is an endpoint that has an active compromise associated with it. A compromised machine can, by design, only have one compromise active at one time.

Applicability

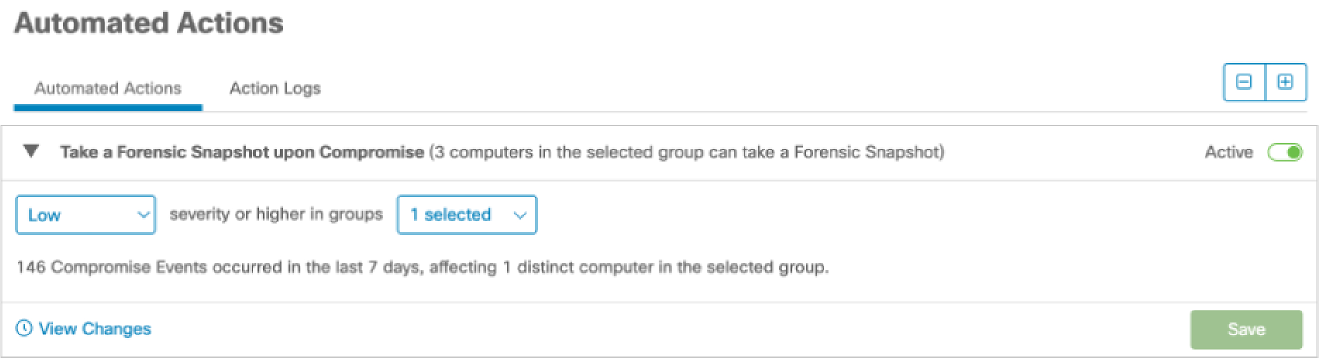
Windows, Mac

Automated Actions Available

1. Take a forensic snapshot upon Compromise: Takes a Forensic Snapshot of a computer when a compromise occurs. A compromise event is basically an event sent by a connector that notifies of something potentially malicious that happens.

   Conditions to trigger this automated action: Events that are the selected severity or higher,

trigger the automated
action.



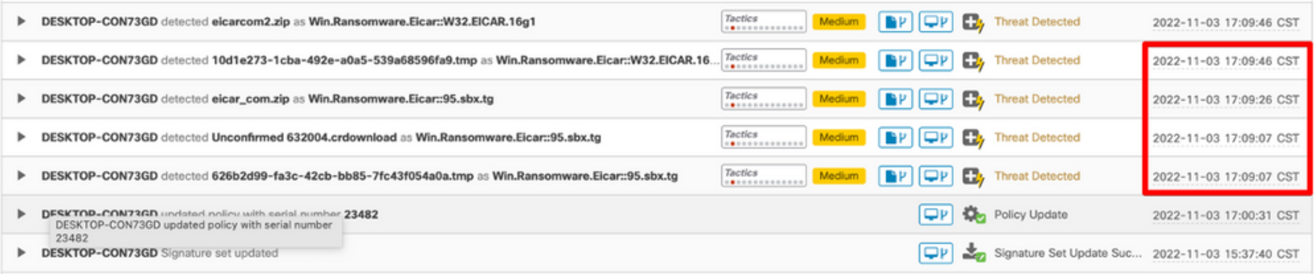
Automated Actions

▼ **Take a Forensic Snapshot upon Compromise** (3 computers in the selected group can take a Forensic Snapshot) Active

Low severity or higher in groups 1 selected

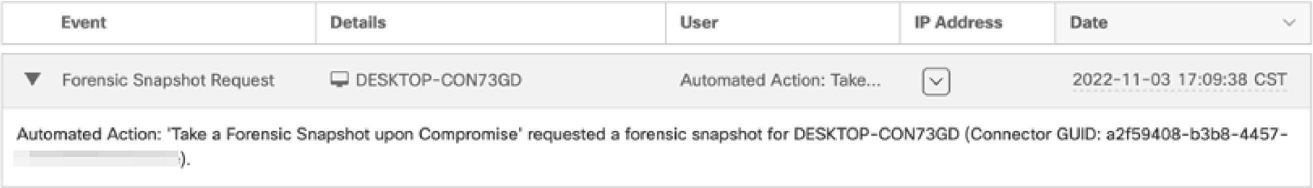
146 Compromise Events occurred in the last 7 days, affecting 1 distinct computer in the selected group.

This is an example of a compromised
machine:



```
▶ DESKTOP-CON73GD detected eicarcom2.zip as Win.Ransomware.Eicar::W32.EICAR.16g1                       Tactics  Medium  Threat Detected            2022-11-03 17:09:46 CST
▶ DESKTOP-CON73GD detected 10d1e273-1cba-492e-a0a5-539a68596fa9.tmp as Win.Ransomware.Eicar::W32.EICAR.16...  Tactics  Medium  Threat Detected  2022-11-03 17:09:46 CST
▶ DESKTOP-CON73GD detected eicar_com.zip as Win.Ransomware.Eicar::95.sbx.tg                            Tactics  Medium  Threat Detected            2022-11-03 17:09:26 CST
▶ DESKTOP-CON73GD detected Unconfirmed 632004.crdownload as Win.Ransomware.Eicar::95.sbx.tg            Tactics  Medium  Threat Detected            2022-11-03 17:09:07 CST
▶ DESKTOP-CON73GD detected 626b2d99-fa3c-42cb-bb85-7fc43f054a0a.tmp as Win.Ransomware.Eicar::95.sbx.tg  Tactics  Medium  Threat Detected            2022-11-03 17:09:07 CST
▶ DESKTOP-CON73GD updated policy with serial number 23482                                                               Policy Update              2022-11-03 17:00:31 CST
    DESKTOP-CON73GD updated policy with serial number
    23482
▶ DESKTOP-CON73GD Signature set updated                                                                                 Signature Set Update Suc... 2022-11-03 15:37:40 CST
```

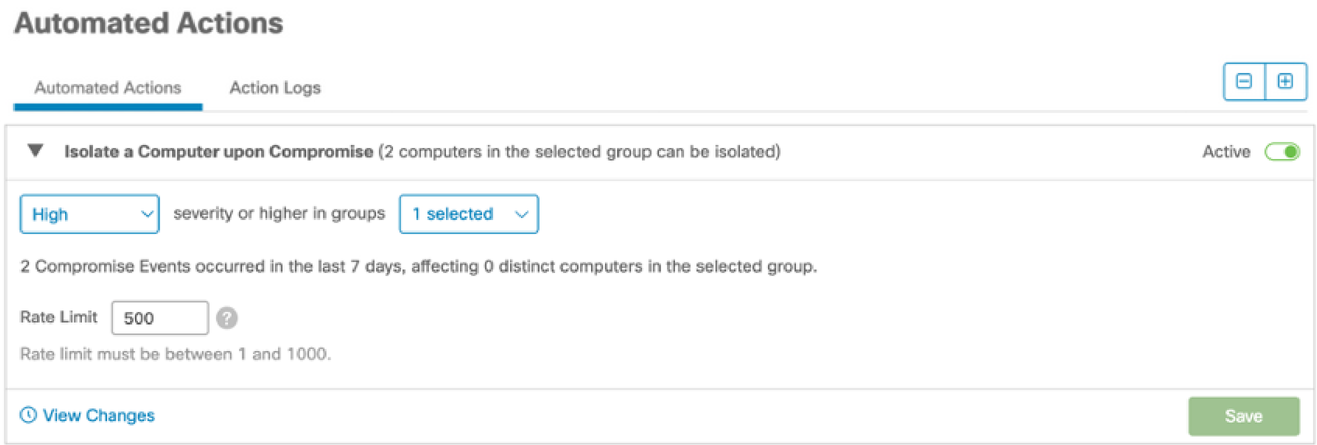
This is the Log of the automated action (from Audit Log
tab)



Event	Details	User	IP Address	Date
▼ Forensic Snapshot Request	DESKTOP-CON73GD	Automated Action: Take...		2022-11-03 17:09:38 CST

Automated Action: 'Take a Forensic Snapshot upon Compromise' requested a forensic snapshot for DESKTOP-CON73GD (Connector GUID: a2f59408-b3b8-4457-[redacted]).

2. Isolate a computer upon compromise: Isolates computers when a compromise occurs.Conditions to trigger this automated action: Events that are the selected severity or higher, trigger the automated action. The Rate Limit protects you against false positive detections. The Rate Limit feature looks at the total number of isolations in a 24 hour rolling window. If the number of isolations is greater than the limit, no further isolations are triggered. Computers are isolated again once the number of compromise events falls to fewer than the limit in the 24 hour rolling window or you stop isolation on computers that were automatically
isolated.



Automated Actions

▼ **Isolate a Computer upon Compromise** (2 computers in the selected group can be isolated) Active

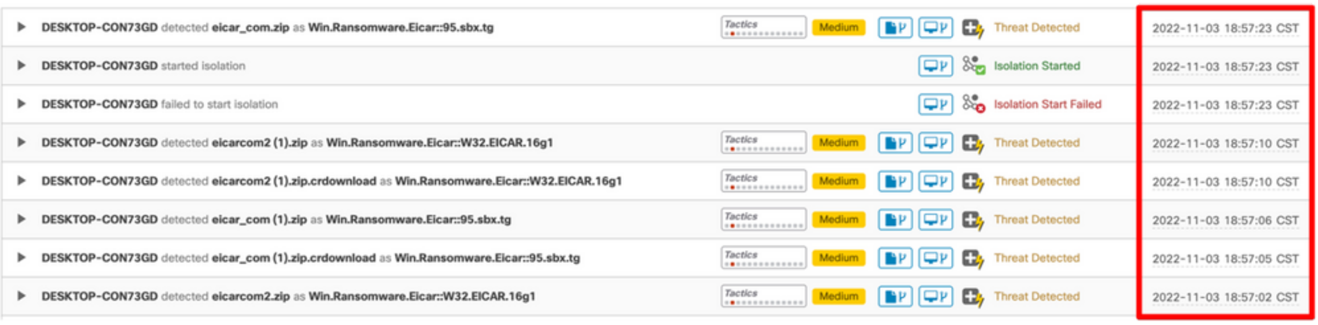
High severity or higher in groups 1 selected

2 Compromise Events occurred in the last 7 days, affecting 0 distinct computers in the selected group.

Rate Limit 500

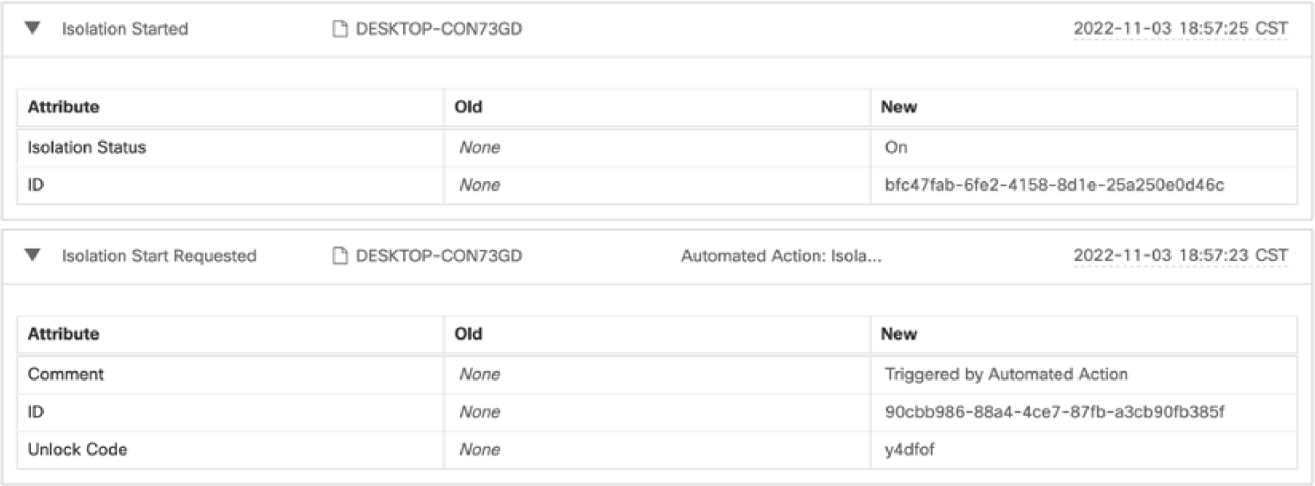
Rate limit must be between 1 and 1000.

This is an example of a compromised
machine:



▶ DESKTOP-CON73GD detected eicar_com.zip as Win.Ransomware.Eicar::95.sbx.tg	Tactics	Medium	Threat Detected	2022-11-03 18:57:23 CST
▶ DESKTOP-CON73GD started isolation			Isolation Started	2022-11-03 18:57:23 CST
▶ DESKTOP-CON73GD failed to start isolation			Isolation Start Failed	2022-11-03 18:57:23 CST
▶ DESKTOP-CON73GD detected eicarcom2 (1).zip as Win.Ransomware.Eicar::W32.EICAR.16g1	Tactics	Medium	Threat Detected	2022-11-03 18:57:10 CST
▶ DESKTOP-CON73GD detected eicarcom2 (1).zip.crdownload as Win.Ransomware.Eicar::W32.EICAR.16g1	Tactics	Medium	Threat Detected	2022-11-03 18:57:10 CST
▶ DESKTOP-CON73GD detected eicar_com (1).zip as Win.Ransomware.Eicar::95.sbx.tg	Tactics	Medium	Threat Detected	2022-11-03 18:57:06 CST
▶ DESKTOP-CON73GD detected eicar_com (1).zip.crdownload as Win.Ransomware.Eicar::95.sbx.tg	Tactics	Medium	Threat Detected	2022-11-03 18:57:05 CST
▶ DESKTOP-CON73GD detected eicarcom2.zip as Win.Ransomware.Eicar::W32.EICAR.16g1	Tactics	Medium	Threat Detected	2022-11-03 18:57:02 CST

This is the Log of the automated action (from Audit Log tab):



▼ Isolation Started   DESKTOP-CON73GD   2022-11-03 18:57:25 CST

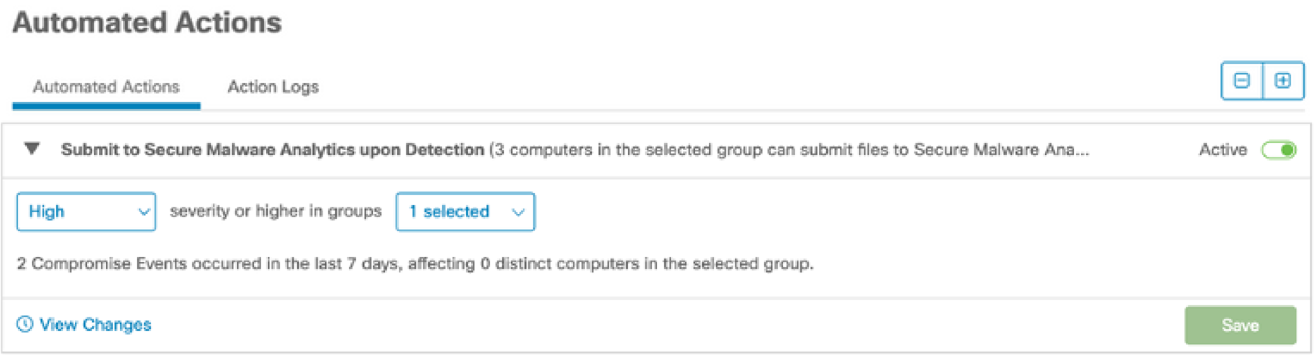
Attribute	Old	New
Isolation Status	*None*	On
ID	*None*	bfc47fab-6fe2-4158-8d1e-25a250e0d46c

▼ Isolation Start Requested   DESKTOP-CON73GD   Automated Action: Isola...   2022-11-03 18:57:23 CST

Attribute	Old	New
Comment	*None*	Triggered by Automated Action
ID	*None*	90cbb986-88a4-4ce7-87fb-a3cb90fb385f
Unlock Code	*None*	y4dfof

3. Submit to Secure Malware Analytics upon Detection: Submit a file to Secure Malware Analytics for File Analysis when a detection occurs.

   Conditions to trigger this automated action: Events that are the selected severity or higher, trigger the automated
   action.



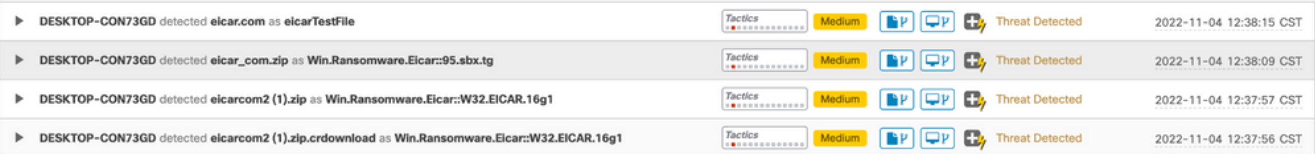
▼ **Submit to Secure Malware Analytics upon Detection** (3 computers in the selected group can submit files to Secure Malware Ana... Active

High severity or higher in groups 1 selected

2 Compromise Events occurred in the last 7 days, affecting 0 distinct computers in the selected group.

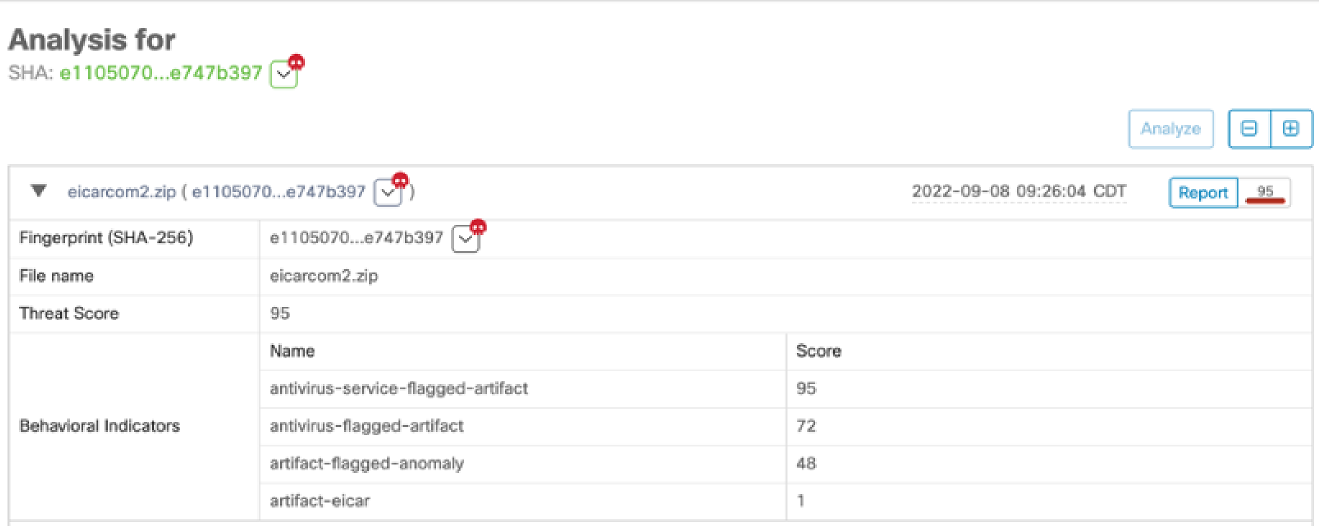
View Changes

Example of a compromised machine:



▶ DESKTOP-CON73GD detected eicar.com as eicarTestFile	Tactics	Medium	Threat Detected	2022-11-04 12:38:15 CST
▶ DESKTOP-CON73GD detected eicar_com.zip as Win.Ransomware.Eicar::95.sbx.tg	Tactics	Medium	Threat Detected	2022-11-04 12:38:09 CST
▶ DESKTOP-CON73GD detected eicarcom2 (1).zip as Win.Ransomware.Eicar::W32.EICAR.16g1	Tactics	Medium	Threat Detected	2022-11-04 12:37:57 CST
▶ DESKTOP-CON73GD detected eicarcom2 (1).zip.crdownload as Win.Ransomware.Eicar::W32.EICAR.16g1	Tactics	Medium	Threat Detected	2022-11-04 12:37:56 CST

In this case, the file was submitted to Secure Malware analytics previously, so the file analysis was already done. Example as follows:



Analysis for

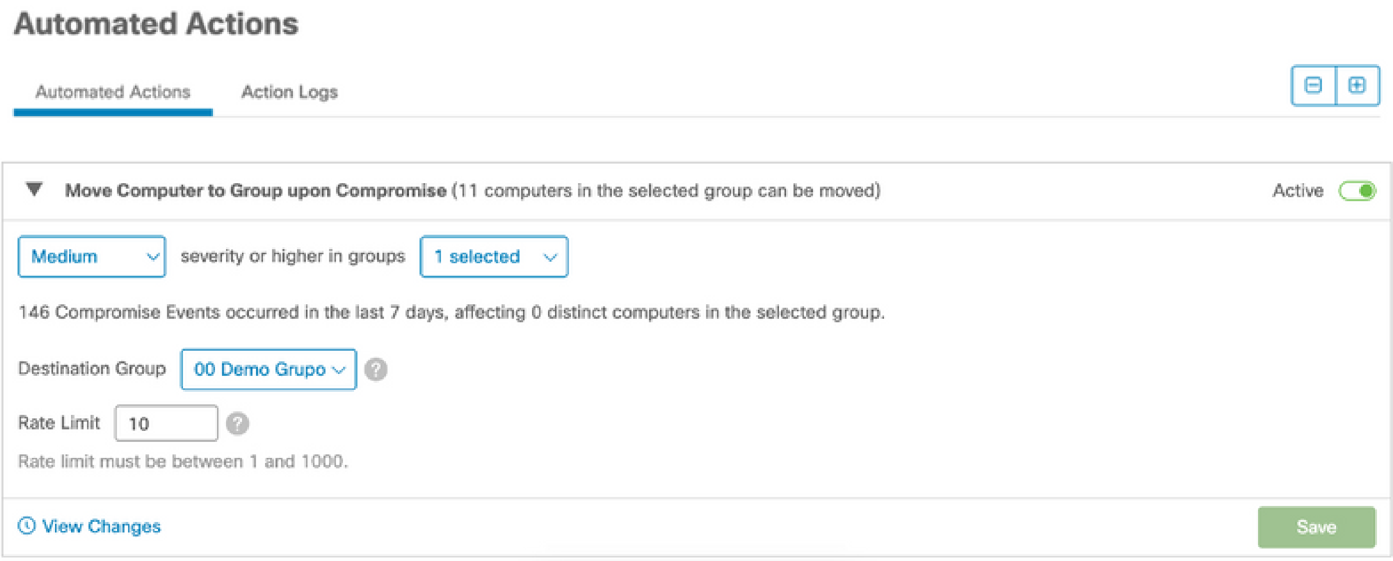
SHA: e1105070...e747b397

eicarcom2.zip (e1105070...e747b397) 2022-09-08 09:26:04 CDT

Fingerprint (SHA-256)	e1105070...e747b397	
File name	eicarcom2.zip	
Threat Score	95	
Behavioral Indicators	Name	Score
	antivirus-service-flagged-artifact	95
	antivirus-flagged-artifact	72
	artifact-flagged-anomaly	48
	artifact-eicar	1

4. Move Computer to group upon Compromise: Move computers from their current groups to another group when the action is triggered. This allows you to move compromised computers to a group with a policy that has more aggressive scanning and engine settings to remediate the compromise.

Conditions to trigger this automated action: Events that are the selected severity or higher, trigger the automated action.



Automated Actions

Move Computer to Group upon Compromise (11 computers in the selected group can be moved) Active

Medium severity or higher in groups 1 selected

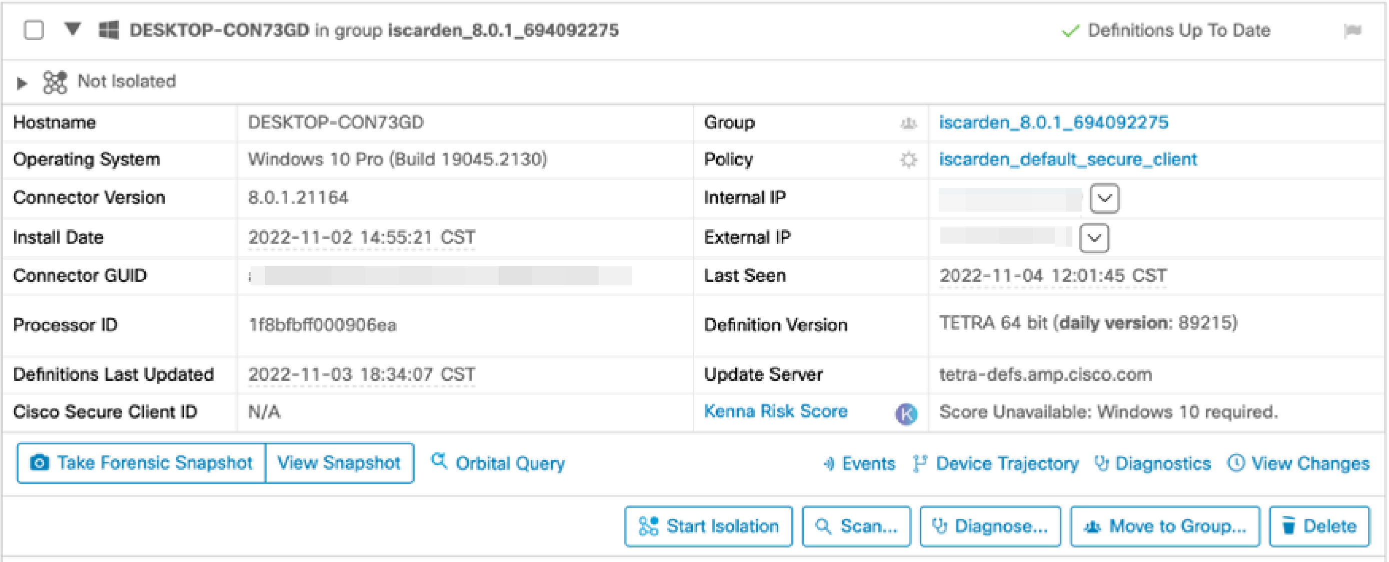
146 Compromise Events occurred in the last 7 days, affecting 0 distinct computers in the selected group.

Destination Group 00 Demo Grupo

Rate Limit 10

Rate limit must be between 1 and 1000.

This is the computer in the original group:

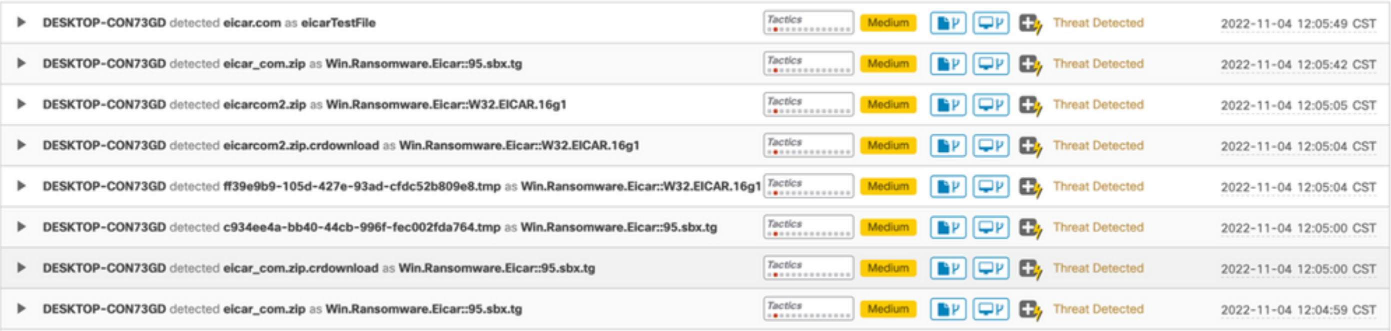


□ ▼ DESKTOP-CON73GD in group iscarden_8.0.1_694092275 ✓ Definitions Up To Date

▶ Not Isolated

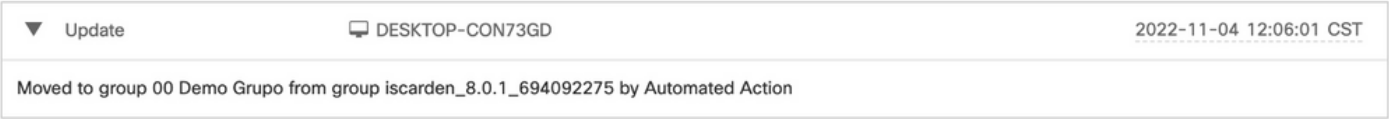
Hostname	DESKTOP-CON73GD	Group	iscarden_8.0.1_694092275
Operating System	Windows 10 Pro (Build 19045.2130)	Policy	iscarden_default_secure_client
Connector Version	8.0.1.21164	Internal IP	[redacted]
Install Date	2022-11-02 14:55:21 CST	External IP	[redacted]
Connector GUID	[redacted]	Last Seen	2022-11-04 12:01:45 CST
Processor ID	1f8bfbff000906ea	Definition Version	TETRA 64 bit (**daily version:** 89215)
Definitions Last Updated	2022-11-03 18:34:07 CST	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score	Score Unavailable: Windows 10 required.

These are the events of compromise:



▶ **DESKTOP-CON73GD** detected **eicar.com** as **eicarTestFile**	Tactics	Medium	Threat Detected	2022-11-04 12:05:49 CST
▶ **DESKTOP-CON73GD** detected **eicar_com.zip** as **Win.Ransomware.Eicar::95.sbx.tg**	Tactics	Medium	Threat Detected	2022-11-04 12:05:42 CST
▶ **DESKTOP-CON73GD** detected **eicarcom2.zip** as **Win.Ransomware.Eicar::W32.EICAR.16g1**	Tactics	Medium	Threat Detected	2022-11-04 12:05:05 CST
▶ **DESKTOP-CON73GD** detected **eicarcom2.zip.crdownload** as **Win.Ransomware.Eicar::W32.EICAR.16g1**	Tactics	Medium	Threat Detected	2022-11-04 12:05:04 CST
▶ **DESKTOP-CON73GD** detected **ff39e9b9-105d-427e-93ad-cfdc52b809e8.tmp** as **Win.Ransomware.Eicar::W32.EICAR.16g1**	Tactics	Medium	Threat Detected	2022-11-04 12:05:04 CST
▶ **DESKTOP-CON73GD** detected **c934ee4a-bb40-44cb-996f-fec002fda764.tmp** as **Win.Ransomware.Eicar::95.sbx.tg**	Tactics	Medium	Threat Detected	2022-11-04 12:05:00 CST
▶ **DESKTOP-CON73GD** detected **eicar_com.zip.crdownload** as **Win.Ransomware.Eicar::95.sbx.tg**	Tactics	Medium	Threat Detected	2022-11-04 12:05:00 CST
▶ **DESKTOP-CON73GD** detected **eicar_com.zip** as **Win.Ransomware.Eicar::95.sbx.tg**	Tactics	Medium	Threat Detected	2022-11-04 12:04:59 CST

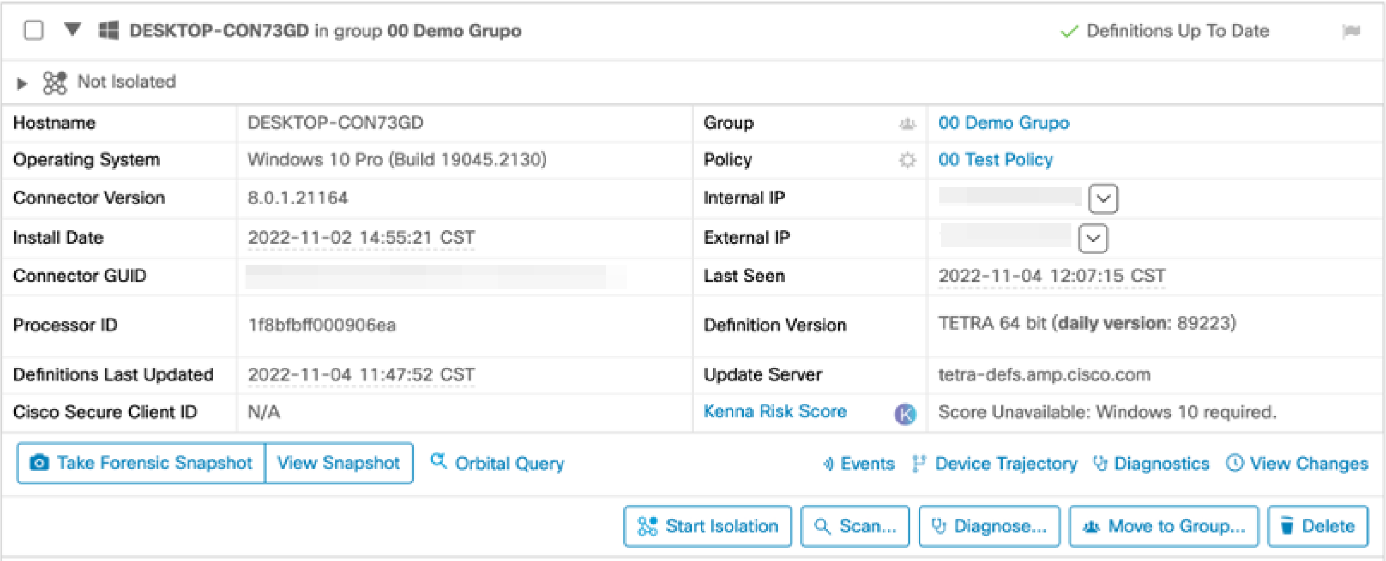
This is the Log of the automated action (from Audit Log tab):



▼ Update DESKTOP-CON73GD 2022-11-04 12:06:01 CST

Moved to group 00 Demo Grupo from group iscarden_8.0.1_694092275 by Automated Action

The computer was moved to specified group in the Automated Action setting:



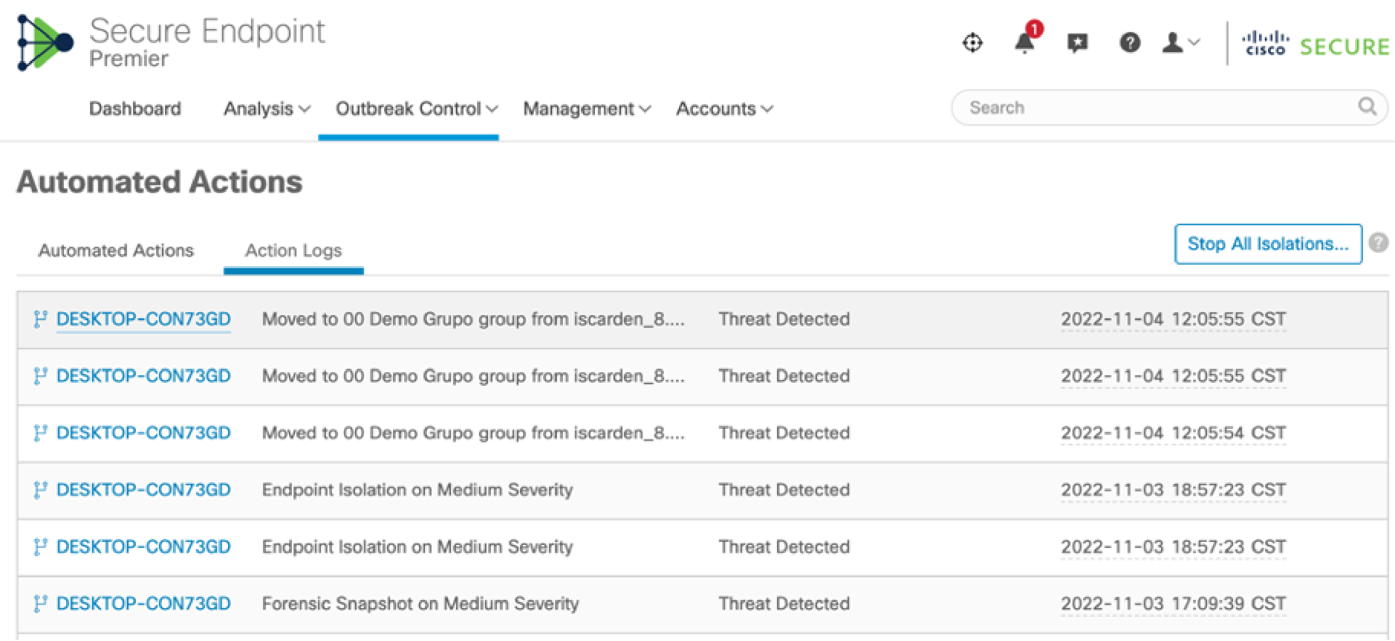
□ ▼ DESKTOP-CON73GD in group 00 Demo Grupo ✓ Definitions Up To Date

▶ Not Isolated

Hostname	DESKTOP-CON73GD	Group	00 Demo Grupo
Operating System	Windows 10 Pro (Build 19045.2130)	Policy	00 Test Policy
Connector Version	8.0.1.21164	Internal IP	[redacted]
Install Date	2022-11-02 14:55:21 CST	External IP	[redacted]
Connector GUID	[redacted]	Last Seen	2022-11-04 12:07:15 CST
Processor ID	1f8bfbff000906ea	Definition Version	TETRA 64 bit (**daily version:** 89223)
Definitions Last Updated	2022-11-04 11:47:52 CST	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score	Score Unavailable: Windows 10 required.

Action Logs

This is the full list of the Automated Action Logs from Automated Actions tab:



DESKTOP-CON73GD	Moved to 00 Demo Grupo group from iscarden_8....	Threat Detected	2022-11-04 12:05:55 CST
DESKTOP-CON73GD	Moved to 00 Demo Grupo group from iscarden_8....	Threat Detected	2022-11-04 12:05:55 CST
DESKTOP-CON73GD	Moved to 00 Demo Grupo group from iscarden_8....	Threat Detected	2022-11-04 12:05:54 CST
DESKTOP-CON73GD	Endpoint Isolation on Medium Severity	Threat Detected	2022-11-03 18:57:23 CST
DESKTOP-CON73GD	Endpoint Isolation on Medium Severity	Threat Detected	2022-11-03 18:57:23 CST
DESKTOP-CON73GD	Forensic Snapshot on Medium Severity	Threat Detected	2022-11-03 17:09:39 CST

Related Information

Secure Endpoint User Guide