

Behavior Group Level & Other Enhancements

Update Document

Publication Date: October 23, 2018

Abstract

This document will guide the users with the Behavior group level handled by EventTracker. It also includes detail information about the other enhancements in this update

Audience

User(s) who wish to monitor Behavior and set it at different group level.

The information contained in this document represents the current view of Netsurion. on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2018 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

Abstra	act	1
Audie	nce	1
Process 1	to be followed after applying the update	3
Behav	/ior Group Level	3
Α.	BEHAVIOR CORRELATION	4
В.	THREATS	6
C.	UNKNOWN PROCESSES	6
D.	SYSTEMS	7
Allow	the user to configure the Risk calculation based on Threat Level	8
Tile Da	ashboard: View the tile by risks	9
Ena	able/ Disable Syslog Relay	10
Enabli	ing or Disabling TLS Versions in VMWare	12

Process to be followed after applying the update

Behavior Group Level

This new feature processes and analyzes behavior data on group level.

For Example: IP activity in two group

Group- 1- TOONS

Group- 2- SIEM

So, if IP activity for an IP "192.168.X.XX" is found in TOONS group than a new activity gets generated for TOONS group only and the next occurrence activity count gets increased for the same IP.

On the otherhand, if IP activity for "192.168.X.XX" is found in SIEM group than a new activity gets generated for SIEM group only and the next occurrence activity count will get increased for the same IP.

1. Once the update is applied, login to EventTracker web; navigate to Admin and then Behavior Correlation Settings.

Behavior Correlation Settings								🔒 / Admin /	Behavior Correla	ation Settings	
User Activity		Top Activitie	es				Unknown Process Det	Jnknown Process Detection			
Monitor enterprise activity	Monitor enterprise activity			Top activities displayed							
Event Threshold	Purge Frequ	iency				Threshold Settings					
Event 3269 is generated when the total count of admin, no activities exceed the threshold. Set the maximum event the	Deletes the activity data, which is older than the configured number of days.			of	Minimum count	1000					
Event threshold [number of activities] per user 2500	user that is pertinent to your environment.		Purge user data older than 4 days				Variation Behavior Correlation	200		davs	
							learning period	3			
Enable DNS lookup for IP addresses	http://whois.do	maintools.com/IP-A	DDRESS								
Enable process lookup for applications	http://www.pro	cesslibrary.com/sea	rch/?q=								
Group Level			Reset Be	havior Corre	ation Data						
Enable group level			Reset	Click to reset the	e existing baseline of	behavior	correlation learning and start n	ew learning of be	havior correlatio	n data	
Note: Existing behavior data will reset if there is a change i	n Group level flag.										
									O	Cance	

Figure 1

- 2. Scroll-down and you can see a Group-Level pane.
- 3. Select the "Enable Group Level "checkbox, which will reset the existing behavior data.





Figure 2

4. Click **OK** to **Save** the changes.

Once the group level gets enabled, you can see the changes in the different EventTracker modules.

A. BEHAVIOR CORRELATION

In **Behavior Correlation**, you can see the **Group** field gets added which will display all the available groups in the drop down list.





- You can select the desired group and view the details for any Behavior activity.
- It will list the unique event ids for that particular group.

Example 1 Group: Custom Group 1 Rule: Event ID Activity



Behavior Group Level and Other Enhancements

Behavior Correlation Detail									🕈 / Dashbo	ard / Behavior	r Correlation / Be	ehavior Corre	elation Detail
Site	Group		Rule						Ad	tivities for			
NTPLDTBLR34	Custom Group 1	•	Event Id A	ctivity			٣			1 day			
Activities from Oct 11 03:52:09 PM - Oct 12 03:52:09 PM					Last refresh	ed Oct 12 03:5	57 PM						⊽C⊗
Sort By Event Id Count Unique Event Id: 18 Total Count: 1,210					Activities n 800 600 400	elated to : 351	3, Descrip	tion: Network	connection c	pened		_	₽
Event Id			Count 674 268	^	200	* 10/06	10/07	10/08	10/09	10/10	10/11	10/12	- []
√ 3523			62	L	System N	lame					Count		
√4670			47	L	✓ Com ³	Fech-Sqlsvr1					674		
▶1223			24	1									- 11
√1225			24										- 11
▶1267			24										- 11
√1268			24										- 11
₩4673			19	-									- 11
													•

Figure 4

For Windows Applications Activity, it will list the unique application name for that particular group

Example 2 Group: Custom Group 2 Rule: Windows Applications Activity

Behavior Correlation Detail		_				f 2	/ Dashboard /	Behavior Corre	elation / Behavio	or Correlation Detail
Site	Group	Rule					Activiti	es for		
NTPLDTBLR34	Custom Group 2	Windows App	olications Activity		•	(i)	1 da	У		•
Activities from Oct 11 04:04:09 PM - Oct 12 04:04:09 PM			Last refreshe	ed Oct 12 04:0	09 PM					™ ∠ C ©
Search Q Q			Activities re	elated to : COI	NHOST.EXE					Q 🗠
ALL A B C D E F H I L M N R S T			300							
Sort By 🔘 Application Name 💿 Count			200							
Unique Application Name: 24			100							
Total Count: 387			0 —	10/06	10/07	10/08	10/09	10/10	10/11	10/12
Application Name		Count 🏛	System N	ame				(Count	
✓ CONHOST.EXE		215	V CDSI	-DC1				2	215	
✓ BCP.EXE		52								
✓ MMC.EXE		17								
✓ SSMS.EXE		16								
✓ CHROME.EXE		11								
➡ BACKGROUNDTASKHOST.EXE		11								
✓ SEARCHPROTOCOLHOST.EXE		10								
SEARCHFILTERHOST.EXE		9								
✓ DLLHOST.EXE		7 🗸								

Figure 5



The same functionality applies for the below Modules.

B. THREATS



Figure 5

C. UNKNOWN PROCESSES

hreats			🔶 / Dashboard / Threat	s / Processes / Unknown
Unknown Dormant Unsafe			Period: Oct 11 02:17 PM - Oct 12 02:17 PM Ref	reshed at: Oct 12 02:17 Pl
Site NTPLDTBLR31 •	Group	Period Last 1 day V	Total: 11	C 💠 İ 🖹
SIGNED 2 UNSIGNED	All Accenture Acer Allensolly AmericanExpress apple Doll	Search by file name	Q Q	æ
PUBLISHER NAME (3) Search by Publisher Name	BLISHER NAME (3) Domain Controllers V earch by Publisher Name EventTracker		SYSTEM NAME (2) Search by System Name	Q. Q.
SELECT ALL	Network Devices NTPL orange	Windows® Operating System 5	SELECT ALL	9
Notepad++	VmWare Win 7 and Server 2008 Above	Search 3	NTPLDTBLR38	2
Eclipse.org Foundation, Inc.	Win XP and Server 2003 Notepad Windows	++ 1 Installer - Unicode 1		

Figure 6

D. SYSTEMS

• In Admin->Systems, Behavior Correlation is not considered for the Default Group.

Systems								† /	Admin / Systen
1 Non Reporting Systems Systems not reporting since the last 24 hours	O Request Stat Status of various	O Request Status Status of various sensor requests			aged 12 aged 12 aged 12 em count	12 set EventTracker Ser Version by count	12 90 - Build 18 12 EventTracker Sensor Version Version by count		
< Groups		Systems							
Create Group Delete Group		Request Status	Non Reporting Systems	Search Compute	system Report	Auto Discover			
All Groups Accenture Acer	000	Default - Default	t Group			Page size	Sort by	Mar	naged: 2
Allensolly	0 0	Type here			Q	25	▼ Name		*
apple	0	Computer		Туре	Port	EventTracker Ve	rsion Change Audit Vers	ion Asset value	e
Blank group	0	NTPLDTBLR38		Win 7	14505	9.0 - Build 18		Low	
Default	0	NTPLDTBLR38-DL	A	Win 7	14505			Low	
Dell	0								
Documentation	0								
Domain Controllers	0								
Empty group	0								
EventTracker	0								
Firewall Devices									

Figure 7

- For any custom group, if you do not wish to consider for behavior correlation,
 - ✓ Click on **Create Group** or modify the existing group by clicking the gear icon and selecting **Edit**.

Systems		Systems						
1		1	0					
Non Penorting Systems		Non Reporting Systems	Details					
Systems not reporting since the last 24 hours	OB	Systems not reporting since the last 24 hours	Edit					
	UTC	Groups	Install agent/Start poll					
< Groups		Groups	Uninstall agent/Stop poll					
		Create Group	Upgrade agent					
Create Group Delete Group		Create Group	Restart agent service					
			Agent service status					
		All Groups	Query for agent version					
All Groups		Accenture	Remove agent components					
Accenture	2	Acer	Delete systems					
Acer	2	Allensolly	Manage asset value					
Allensolly	>	AmericanExpress	Query for agent update info					
AmericanExpress	2	apple	Computer					

Figure 8

✓ Enable "Do not consider for behavior correlation" checkbox.

Create Gr	roup	×
Select Group Group C D Select O II O II O S	Act Group Name and Type up Name Custom Group 1 up Description	nbers manually.
		Cancel Back Next Finish



The particular group will not be considered for the Behavior Correlation.

Allow the user to configure the Risk calculation based on Threat Level

Earlier the EventTracker Risk calculation was based on (TVA) Threat, Vulnerability, and Asset value.

In this update, an option is provided which, if enabled will consider only the Threat level to calculate the risk.

Login to EventTracker web and navigate to Admin-> Manager.

Under the Alert Events pane, an option has been provided "Generate alert based only on threat level". If this particular option is enabled, the risk of an alert will only be considered based on the threat level. Disabling this option will take the earlier behavior into consideration and calculate the risk based on TVA.



Manager Configuration systog / Virtual Collection Point Direct Log Archiver Agent Settings E-mail	Elasticsearch	🏫 / Admin / Manager
Alert Events Image: Second S	🔲 Enable alert e-mail header	Fnable alert e-mail subject prefix
Turn off alerts Turn off filters C Enable alert events cache for analyzing alerts	Alert e-mail header	Alert e-mail subject prefix ① Netsurion (199999-9999)
Purge events from cache older than 7 days Suppress duplicate alerts Alert suppression interval	Enable alert e-mail footer Alert e-mail footer	HTML Template None Generate alert based only on threat level
Maximum number of alerts allowed 0		



Tile Dashboard: View the tile by risks

In the Tile Dashboard, an option is provided to filter tiles based on risks. The user can select the Risk options available from the dropdown list and get only those tiles in the dashboard.

- Navigate to Incidents-> Tile View.
- A new option field "Risk" is added.

Incidents				n /	Dashboard / Incidents / Tile	
Updated: Oct 15 03:58 PM Incidents from: Oct 14 03:5	8 PM - Oct 15 03:58 PM		() Total: 194 Duration Last 1 Day 💙			
Dashboard Graph Tabular Tile						
Group	Sort By	Rick	Top			
All V	Risk	All	20 🗸	Search Q Q	1	
EventTracker: Detected new bad reputation IP activity	Critical Potential Breach: A new process connecting to	Low Medium	hanged	*3221		
3 Oct 15 12:20:09 PM	1 O C 15 11:20:14 AM	Serious Critical		20 Oct 15 02:53:31 PM		
		□1 ♣ 1	# 2 ¢	□ 2 4 0	i	
EventTracker: Non reporting system(s) with low asset	3523_NewEventFound	*3221		*7024		
1 Oct 15 105203 AM ✓ 0 ♥ 0 ♥ 0 ♥ 0	O Oct 15 03/29:12 PM ✓ 0 ✓ 0 I 0	Oct 15 12:13:44 PM ✓ 35 ✓ 0 0		20 Oct 15 02:56:36 PM ✓ 0 ♂ 0 ! 0 ! 0		
🗆 1 🜲 0 🔠 🖉 🌣		□ 1 ♣ 0	i 🖉 🌣	□ 2 ♣ 0	ii 🖉 🌣	



• Select the severity from the dropdown list and it will display only those tiles.

Incidents							🔒 / Dashboard / Incident	:s / Tile
Updated: Oct 15 03:59 PM	Incidents from: Oct 14 03:59 PM - Oct 15 03:59 PM				G) Total: 4 Dura	ation 🛛 Last 1 Day 💙	
Dashboard Graph Tabular Tile								
Group		Sort By		Risk	Тор			
All		Risk	~	Critical 🗸	20 🗸	Search	Q Q	1
Second Fraction Second Fra	activity Critical Potential Breas	h: A new process connecting to Oct 15 112014 AM ○ ② ○ 【 ○ 【 ○ 】 ○	~ ¢		1			

Figure 12



Enable/ Disable Syslog Relay

Earlier, if the EventTracker agents are running with syslog relay configuration then there was no indication in the Manager machine.

To avoid this, now in the System Manager the particular managed agent running with syslog relay configuration displays in green color. This helps the Admin to identify the managed agents with the syslog relay, easily.

Now, the Admin can even configure the syslog relay for any target machine from the System Manager.

- Login to EventTracker and navigate to Admin> Systems.
- Click the gear 🌞 icon beside the target system and select "Enable syslog relay" from the dropdown list.

S	ystems						🔒 / Admin / System
	0 Non Reporting Systems Systems not reporting since the list 24 hours	5 Managed Managed vs Unmanaged Managed/Ummanaged system count	s 3 Even Versio	90 - Buid 18 MTracker Sensor Version n by count			
	Systems Non Reporting Systems System Report C All Domain Computers						Managed: 5
	Type here	Q			Page size	Sort by Name	~
	Computer	Туре	Port	EventTracker Version	Change Audit Version	Asset value	
	NTPLDTBLR302	2016	14505	9.0 - Build 18	9.0 - Build 18	Serious	\$
	NTPLDTBLR302-DLA	2016	14505			Serious	\$
	NTPLDTBLR33	Win 8.1	14505	9.0 - Build 18		Low	\$
	NTPLDTBLR33-DLA	Win 8.1	14505			Low	\$
	R155-VM1	2016	14505	9.0 - Build 18		High Detail Maaia Enabl Disab	is ge asset value e syslog relay le syslog relay

Figure 13

In the Enable syslog relay dialog box, provide the **Regular Expression**, **Protocol** and **Port** and click **OK**.



This option allows EventTracker Agent to work as a syslog relay by receiving syslog messages from various devices and forwarding them to managers. A valid port which is not used by any other process should be configured. Based on the provided regular expression agent will e	
This option allows EventTracker Agent to work as a syslog relay by receiving syslog messages from various devices and forwarding them to managers. A valid port which is not used by any other process should be configured. Based on the provided regular expression agent will e	
value from event description and add the extracted value into computer name property of the event. Example: *devid=(?P <computer>["expression will extract devid from the event description and use it as computer name. Please provide named capture group as 'Computer' name, as shown in the example.</computer>	configured extract particular (w+])* for any field
Regular expression	
devid=(?P <computer>[\w+])</computer>	
Protocol	
UDP	~
Port	
514	

Figure 14

The Target system will turn "Orange" in color. This indicates that still syslog relay is not enabled on the target agent machine.

Systems						
Non Reporting Systems System Report						
All Domain Computers						Managed: 5
				Page size	Sort by	
Type here	Q			25	✓ Name	~
Computer	Тупа	Port	EventTracker Version	Change Audit Version	Arrativalua	
	and a second sec	1010			Asset value	
NTPEDTBER302	2010	14505	9.0 - Build 18	3/0 - Build 18	Serious	54
NTPLDTBLR302-DLA	2016	14505			Serious	
NTPLDTBLR33	Win 8.1	14505	9.0 - Build 18		Low	\$
NTPLDTBLR33-DLA	Win 8.1	14505			Low	\$
R1S5-VM1	2016	14505	9.0 - Build 18		High	0

Figure 15

Once the target system turns "Green" in color, it indicates that the syslog relay configuration is successfully enabled on the target agent machine.



Sy	stems						Admin / Systems
(1	0 Non Reporting Systems Systems not reporting since the last 24 hours	5 Managed Managed vs Unmanaged Managed Vsmanaged system court	s 3 EventTi Version b	90 - Build 18 racker Sensor Version y count	3		
>	Systems System Report C						Managarti 5
	All Domain Computers				Page size	Sort by	Manageo: 5
	Type here	Q			25	✓ Name	~
	Computer	Туре	Port	EventTracker Version	Change Audit Version	Asset value	
	NTPLDTBLR302	2016	14505	9.0 - Build 18	9.0 - Build 18	Serious	\$
	NTPLDTBLR302-DLA	2016	14505			Serious	\$
	NTPLDTBLR33	Win 8.1	14505	9.0 - Build 18		Low	\$
	NTPLDTBLR33-DLA	Win 8.1	14505			Low	\$
	R1SS-VM1	2016	14505	9.0 - Build 18		High	\$

Figure 16

If at any point you wish to disable the syslog relay configuration option, click the gear ^{*} icon beside the target system and select "**Disable syslog relay**" from the dropdown list.

Systems					
Non Reporting Systems System Report C					
All Domain Computers					Managed: 5
				Page size	Sort by
Type here	Q			25 🗸	Name 🗸
Computer	Туре	Port	EventTracker Version	Change Audit Version	Asset value
NTPLDTBLR302	2016	14505	9.0 - Build 18	9.0 - Build 18	Serious Details
NTPLDTBLR302-DLA	2016	14505			Serious Manage asset value
NTPLDTBLR33	Win 8.1	14505	9.0 - Build 18		Low Enable syslog relay
NTPLDTBLR33-DLA	Win 8.1	14505			Low Disable syslog relay
R155-VM1	2016	14505	9.0 - Build 18		High



Enabling or Disabling TLS Versions in VMWare

Managing TLS Protocol Configuration with the TLS Configurator Utility

Starting with vSphere 6.7, only TLS 1.2 is enabled, by default. TLS 1.0 and TLS 1.1 are disabled by default. Whether you do a fresh install, upgrade, or migration, vSphere 6.7 disables TLS 1.0 and TLS 1.1. You can use the TLS Configurator utility to enable older versions of the protocol temporarily on vSphere 6.7 systems. You can then disable the older less secure versions after all connections use TLS 1.2.

As part of the process, you can disable TLS 1.0, and enable TLS 1.1 and TLS 1.2. Or, you can disable TLS 1.0 and TLS 1.1, and enable only TLS 1.2.

NOTE:

Starting with vSphere 6.7, the TLS Configurator utility is included in VCenter/VSphere.

You no longer have to download it separately.

If you are not able to find utility then use the below procedure:



Prerequisites

Ensure that the hosts and services that the vCenter Server manages can communicate using a version of TLS that remains enabled. For products that communicate only using TLS 1.0, connectivity becomes unavailable.

1. Login to the vCenter Server system with the username and password for administrator@vsphere.local, or as another member of the vCenter Single Sign-On Administrators group who can run scripts.

2. Go to the directory where the script is located.

Windows:

cd %VMWARE_CIS_HOME%\TIsReconfigurator\VcTIsReconfigurator

Linux:

cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator

3. Run the command, depending on your operating system and on which version of TLS you want to use.

✓ To disable TLS 1.0 and enable both TLS 1.1 and TLS 1.2, run the following command.

Windows:

directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2

Linux:

directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2

✓ To disable TLS 1.0 and TLS 1.1, and enable only TLS 1.2, run the following command.

Windows:

directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2

Linux:

directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2

4. If your environment includes other vCenter Server systems, repeat the process on each vCenter Server system.

5. Repeat the configuration on each ESXi host and each Platform Service Controller.

Behavior Group Level and Other Enhancements

192.168.1.31 - PuTTY			- 0 x
wxr-x 7 vaphere-	-client cis	4096 Aug 31 06:23 vmware-waphere-client	
		212 Aug 15 2017 mml2Conf.sh	
		195 Jul 18 2017 xsltConf.sh	
tephoton-machine [/usr/lib vmware	Reconfigurator/	
h: vmware-IlsReconf	figurator/: Is a di:		
otentorementine [/usr/lib/wwware-Tl	informator 1/ /reconfigureVe undate -n 713v1.1 714v1.2	
ab: ./reconfigureVo:	No such file or d	MATY TATA TATA TATA TATA TATA TATA TATA	
ot@photon-machine [/usr/lib/vmware-Tl	onfigurator 11 dir	
TlsReconfigurator			
		configurator]# cd VcTlsReconfigurator/	
	/usr/lib/vmware-Tl:	onfigurator/VcTlsReconfigurator 👭 ./reconfigureVc update -p TLSv1.1 TLSv1.2	
nter Transport Laye	er Security reconfig	cor, version=6.7.0, build=8832884	
more information r	refer to the follow:	article: https://kb.vmware.com/kb/2147669	
file: "/Var/log/vm	nware/vSphere-Tiske	Igurator/VClasseconfigurator.log".	
HICET SELVET IS GOIN	ig to be restarced.	you want to contrate (1/m)? y	
na backup directory	/rmp/20180913T09		
king up: vmware-vpx			
king up: vmware-upd			
cing up: vsphere-cl	lient		
king up: Vami-light	t por contra		
king up: vmware-rnt	S-wat obdog		
king up: vmware-spa			
king up: rsyslog			
	Scanning vCenter Se:	TLS endpoints managements	
Service Name	TLS Endpoint Port	TLS Version(a)	
mware-vpxd	1 8089	TLSv1.2	
mware-updatemgr			
Ware-updatemgr			
		NOT RUNNING	
sdird			
ware-stad		1L5v1.2 I	
phere-client	1 9443	TLSv1.2 I	
mi-lighttp	1 5480	ILDVIJ I	
ware-rbd-watchdow		ANT DINNING	
Storage Clients	I NOT APPLICABLE	LSv1.2	
syslog	1814	TLSv1.2	
ating vCenter Serve	er TLS configuration	aupport: ['TLSw1.1', 'TLSw1.2']	
ating: vmware-vpad			
ating: vmware-updat	temgr		
ting: vmcam			
ting: vmmare-sted			
ting: vaphere-clie			
ting: vami-lighttp			
	Restarting VC		
ping services			
O Tune here to a	tearch		A 171 dx 2:36 PM
- The mere to i	and the second sec		9/13/2018

Figure 18 (Before updating TLS Version)

•	++		+		,
Service Name	1	TLS Endpoint Port	1	TLS Version(s)	
vmware-voxd	+	8089	+	TLSv1.1 TLSv1.2	
vmware-updatemgr	i,	8084	1	TLSv1.1 TLSv1.2	
vmware-updatemgr	ĥ	9087	1	TLSv1.1 TLSv1.2	
vmcam	1		1	NOT RUNNING	1
vmdird	i.	636	1	TLSv1.1 TLSv1.2	
vmware-stsd	1	7444	1	TLSv1.1 TLSv1.2	
vsphere-client	1	9443	1	TLSv1.1 TLSv1.2	
vami-lighttp	1	5480	1	TLSv1.1 TLSv1.2	
vmware-rhttpproxy	1	443	1	TLSv1.1 TLSv1.2	
vmware-rbd-watchdog	1		1	NOT RUNNING	
VC Storage Clients	1	NOT APPLICABLE	1	TLSv1.1 TLSv1.2	
rsyslog	1	1514	1	TLSv1.1 TLSv1.2	

Figure 19 (After updating TLS Version)