Netsurion. EventTracker

Integrate SpamTitan Gateway

EventTracker v9.2 and above

Publication Date: July 14, 2020

Abstract

This guide provides instructions to configure SpamTitan Gateway to send its logs to EventTracker.

Scope

The configuration details in this guide are consistent with EventTracker version v9.2 or above and **SpamTitan Gateway**

Audience

Administrators who are assigned the task to monitor SpamTitan Gateway events using EventTracker.

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.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

1.	Ov	erview	. 3
2.	Pre	erequisites	. 3
3.	Int 3.1	egration of SpamTitan Gateway with EventTracker Configuring SpamTitan Gateway to send the logs to EventTracker	. 3 . 3
4.	Eve 4.1	entTracker Knowledge Pack Category	. 4 . 4
	4.2	Alerts	. 5
	4.3	Report	. 5
	4.4	Dashboards	. 7
5.	اlm 5.1	porting SpamTitan Gateway knowledge pack into EventTracker Category	10 11
	5.2	Alerts	12
	5.3	Token template	13
	5.4	Knowledge Object	14
	5.5	Report	16
	5.6	Dashboards	17
6.	Ve 6.1	rifying SpamTitan Gateway knowledge pack in EventTracker Category	20 20
	6.2	Alerts	21
	6.3	Token templates	22
	6.4	Knowledge Object	23
	6.5	Report	24
	6.6	Dashboards	25

Netsurion. EventTracker

1. Overview

SpamTitan Gateway is a powerful Anti-Spam appliance that equips network administrators with extensive tools to control mail flow and protect against unwanted email and malware.

EventTracker helps to monitor events from SpamTitan Gateway. EventTracker's reports provide detailed information of all events, alerts are helpful to determine and stop the attack and suspicious activities in real-time, and dashboards will help you to analyze all the security-related events in a single console. Also, we can create and save log search rules/queries under the saved search feature for real-time and historical log search.

2. Prerequisites

- Admin privileges for SpamTitan Gateway to configure logging.
- EventTracker should be installed in the system.
- Syslog Port 514 should be open.

3. Integration of SpamTitan Gateway with EventTracker

SpamTitan Gateway logs we can get by using syslog.

3.1 Configuring SpamTitan Gateway to send the logs to EventTracker

Syslog is the de facto standard for forwarding log messages in an IP network. All system log messages are written to local log files on SpamTitan Gateway using syslog and logs can be viewed in the Logs tab.

Besides, the log output can also be sent to a remote syslog server. This is useful for administrators who want to use EventTracker to view and analyze log files.

Go to **Settings > Remote syslog** to specify a remote syslog server for mail, interface, and messages log files. The remote servers defined must run a logging daemon compatible with the syslog protocol.

To specify a remote server:

- 1. Click Enable to turn the remote syslog status to ON.
- 2. Enter the EventTracker's address in the syslog Server: field.



Note:

To specify a port, put a colon after the remote syslog address, and add the port number. For example, **192.168.3.120:5826**

3. Click Save.

ON	Disable
	Save
	0
ON	Disable
	Save
g	Ø
ON	Disable
	Save
9	ON ON ON ON ON ON ON ON ON



4. EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support SpamTitan Gateway.

4.1 Category

Saved searches are designed to quickly parse/filter logs and allow the user to see only specific events related to:

- **SpamTitan Gateway Infected Emails:** This category for SpamTitan Gateway allows users to quickly filter and display the events related to Infected emails.
- **SpamTitan Gateway Noqueue Email:** Using this category for SpamTitan Gateway we can quickly filter and display the events related to Noqueue emails.



- **SpamTitan Gateway Passed Emails:** This category provides quick search and filter related to the Passed email events.
- **SpamTitan Gateway Spam Emails:** This category for SpamTitan Gateway allows users to quickly filter and display the events related to Spam emails.
- **SpamTitan Gateway Virus detected in the mail:** This category provides the quick filter and logs search related to Virus detected events.

4.2 Alerts

Alerts are triggered when an event received is identified as critical and requires immediate notification. Such as

- **SpamTitan Gateway Virus detected in Infected mails:** This alert is triggered by EventTracker when SpamTitan Gateways detect any Virus/Malware in mails.
- SpamTitan Gateway Mail with Coronavirus/Covid-19 subject: This alert is triggered by EventTracker when SpamTitan Gateways mail subject contains information of Coronavirus or Covid-19.

4.3 Report

 SpamTitan Gateway - Passed Emails: This report provides detailed information on SpamTitan Gateway Passed emails events generated by SpamTitan Gateway. This report contains information such as Source IP addresses, Mail sender information, Mail recipient, Mail Header information, Mail Subject, etc.

LogTime	Source IP	Mail Sender	Mail Recipient	From Header	Mail Subject	Rate
07/13/2020 03:22:02 PM	192.28.153.136	673-UWY- 229.0.464899.0.0.30 9332.9.13623248@b ounce1.xyz.com	Robert.p@conto so.com	Silicon Valley Business Journal <reply@news.bounce1.x yz.com.com></reply@news.bounce1.x 	Coronavirus Global News.	none
07/13/2020 03:22:02 PM	192.1688.153.136	673-UWY- 229.0.464899.0.0.30 9332.9.13623248@y ahoo.com	Peter.p@contos o.com	Silicon Valley Business Journal <reply@news.yahoo.com .com></reply@news.yahoo.com 	Covid-19 Vaccene update.	none

Figure 2

 SpamTitan Gateway - Spam Emails: This report provides detailed information on SpamTitan Gateway events generated by SpamTitan Gateway. This report contains information such as Source IP addresses, Source Port, Destination IP address, Mail Sender and Recipient address, Reason, Size, Action taken on spam mail, Quarantine details, etc.

LogTime	Source IP Address	Sourc e Port	Destinat ion IP	Sender Address	Recipient address	Reason	Size	Action	Quarantine	Hits
07/13/2020 03:22:01 PM	21.11.10.89 0	36912	21.11.10 .890	bounce- 9493_HTML- 61583723- 560396- 7234512- 22@bounce.repl y.ien.com	tim.cook@co ntoso.com	NoBounceInbound,Quara ntined	86058	Blocked	C/spam- CQmVjvelsdd x	4.93
07/13/2020 03:22:02 PM	22.11.10.20	36912	22.11.10 .20	Corona- VirusHTML- 61583723- 560396- 7234512- 22@abc.replyco m	tim.cook@co ntoso.com	NoBounceInbound,Quara ntined	86058	Blocked	C/spam- CQmVjvelsdd x	4.93



• **SpamTitan Gateway** - **Infected Emails with Virus:** This report provides detailed information on SpamTitan Gateway Response events generated by SpamTitan Gateway. This report contains information such as Scanner name, Sender-Recipient address, source IP address, source port, Virus name, size, hits and action taken on the mail, etc.

LogTime	Scan ner	Recipient address	Sender Address	Source IP	Sourc e Port	Destinati on IP	Virus Details	Size	Hits	Action	Quarantine	Reason
07/13/2020 04:42:42 PM	BitDef ender	Pter.s@co ntoso.com	grace.quinte ro@zoom.n et	200.7.10 0.32	57045	123.81.2 34.10	Trojan.C ryxos.40 60	141392	-	Blocked	H/virus- H5wyjc3l8_n 7	DiscardedInb ound,Quarant ined
07/13/2020 04:42:42 PM	BitDef ender	adam.s@c ontoso.co m	Hunter.X@Y amaha.net	12.7.100. 20	57045	230.81.2 34.113	Trojan.C ryxos.40 58	141392	-	Blocked	H/virus- H5wyjc3l8_n 7	DiscardedInb ound,Quarant ined

Figure 4

 SpamTitan Gateway - Noqueue Emails: This report provides detailed information on SpamTitan Gateway Noqueue events generated by SpamTitan Gateway. This report contains information such as Action taken on Noqueue mails, Protocol types, Mail Recipient and Sender addresses, source IP address, etc.

LogTime	Action	Protocol	Recipient address	Sender Address	Source IP
07/13/2020 03:22:02 PM	filter	ESMTP	Admin.Server@contoso.com	673-UWY- 229.0.464899.0.0.309332.9.1362324 8@bounce1.token.com	192.168.15.16
07/13/2020 03:22:02 PM	filter	ESMTP	Robert.wilson@contoso.com	673-UWY- 229.0.464899.0.0.309332.9.1362324 8@bounce12.gmail.com	192.168.15.16
07/13/2020 04:42:42 PM	filter	ESMTP	Admin.Server@contoso.com	673-UWY- 229.0.464899.0.0.309332.9.1362324 8@bounce1.token.com	<mark>192.168.15.16</mark>

Figure 5



4.4 Dashboards



• SpamTitan Gateway - All Events





• SpamTitan Gateway - Action taken on mails

Figure 7

Netsurion. EventTracker



• SpamTitan Gateway - Virus detected in infected mails



• SpamTitan Gateway – Virus detected by Source IP



Figure 9





• SpamTitan Gateway – Top Suspicious Mail Sender



• SpamTitan Gateway – Top Suspicious mail Recipient



Figure 11

Netsurion. EventTracker

action	email_subject	sender_address
Pass		willy.S@infosec.com
Pass		Nicole.S@technosoc.com
Blocked		bounce-9493_HTML-61583723-560396-7234512-22@bounce.reply.ie
Blocked		grace.quintero@zoom.net
Blocked		Hunter.X@Yamaha.net
PASS	Covid-19 Vaccene update.	673-UWY-229.0.464899.0.0.309332.9.13623248@yahoo.com
PASS	Coronavirus Global News.	673-UWY-229.0.464899.0.0.309332.9.13623248@bounce1.xyz.com
filter		bounce213.xyz.com[192.168.15.16]
filter		bounce213.xyz.com[192.168.15.16]
Blocked		Corona-VirusHTML-61583723-560396-7234512-22@abc.replycom
4		•

• SpamTitan Gateway - Top Spam mail with Subject and Sender SpamTitan Gateway

Figure 12

5. Importing SpamTitan Gateway knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Category
- Alert
- Token template
- Knowledge Object
- Report
- Dashboard
- 1. Launch the EventTracker Control Panel.
- 2. Double click Export Import Utility.



Figure 13

3. Click the **Import** tab.

5.1 Category

1. Click Category option, and then click Browse.

<u>в</u>	Export Import Utility	
Export Import		
1. Provide the path and file nam 2. Click the Import button.	e of the Categories file. Use the '' button to browse and locate the import file.	
Options	Location	
Category		
O Filters		
⊖ Alerts		
 Systems and Groups 	Source :	
O Token Value		
⊖ Reports		
O Behavior Correlation		
	Import	Close

Figure 14



- 2. Locate Categories_ SpamTitan Gateway.iscat file, and then click Open.
- 3. To import categories, click Import.

EventTracker displays a success message.

Export Import Utility	x
Selected category details are imported successfully.	
ОК	

Figure 15

4. Click **OK**, and then click **Close**.

5.2 Alerts

- 1. Once you have opened "Export-Import Utility" via "EventTracker Control Panel", click Alert option, and then click Browse
- 2. Navigate to the knowledge pack folder and select the file with the extension ".isalt", e.g. "Alerts_ SpamTitan Gateway.isalt" and then click "Import".

🐁 Export Imp	ort Utility			_		×
Export Import	t					
1. Provide th 2. Click the	ne path and file nam Import button.	e of the Alerts file. Use the '' butt	ton to browse and locate the import file.			
Options		Location				
Categor	Ŋ	Import E-mail settings				
O Filters		 Set Active Only if notifications set 	This setting is applicable only for imports Alert files. For v7 the active status will be	from Legacy (e set based or	v6x)	
Alerts]	O By default	"Active" key available in the configuratio	n section.		
O Systems	s and Groups	Watchlist Configuration				
	Value	Import Watchlist configuration	ion			
	Value	This setting is applicable only f Note: If this option is enabled t	or alerts which have Advanced watchlist co he user should make sure the watchlist grou	onfigured. ups are availa	ble	
 Reports 	3	on the console where the alert	s are imported.			
O Behavio	or Correlation					
		Source :		_	_	
		*.isalt				
				Import	Clo	se

Figure 16

3. EventTracker displays a success message:





5.3 Token template

1. Click the **Parsing rule** under the **Admin** option in the EventTracker manager page.

		🔎 Admin -
Active Watch Lists	FAQ Tile Configuration	🧭 Parsing Rules
Alerts	Group Management	Report Settings
Casebook Configuration	Q IP Lookup Configuration	Systems
● Category	· Q. Knowledge Objects	QQ Users
Diagnostics	Machine Learning Jobs	T Weights
Event Filters	🗞 Machine Learning Settings	
Eventvault	Manager	

Figure 18

2. Click Template.

Parsing Rule	S	
Parsing Rule	Template	
Groups		(+)
2725.00		



3. To import the token template, click **Import**.





4. Locate the **Templates_ SpamTitan Gateway.ettd** type file by clicking the **Browse** button, enable all the templates and click **import**.

mport				
Select file		🗁 Brow	se	
Note: Please select file of typ	e *.ettd (even	ttracker te	mplate das	hlets).



5. Click **OK**.

5.4 Knowledge Object

1. Click **Knowledge objects** under the Admin option in the EventTracker manager page.

≡	Event Tracker ⊕					🐥 🛛 Admin-	Tools -
-	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
q		_	Alerts	© Correlation	Q IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	Diagnostics	🔆 Knowledge Objects	⊕ Weights	
k			🏷 Behavior Correlation Settings	⊽ Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Eventvault	🕖 Parsing Rules		
			e Category	FAQ Configuration	Report Settings		
	Attacker			– News			



2. Click **Import** \mathbb{T} as highlighted in the below image.



11	Knowledge Ob	jects		♠ / Admin / Knowledge Objects
Q R	Search objects	Q	Q Activate Now	Objects 🕀 耳 🏦 🌣
	Groups	0 🖉 🗊		1.
	Cylance			
	EventTracker			

Figure 23

3. Click Browse.

Import		×
Select file	🗁 Browse Upload	
	Close	•



- 4. Locate the file named **KO_ SpamTitan Gateway.etko**.
- 5. Now select the checkbox and then click \mathbb{I} Import.



Impo	rt		×
Sele	ect file		🖆 Browse Upload
	Object name	Applies to	Group name
	SpamTitan Gateway	Gateway Anti-spam Appliance	SpamTitan Gateway
			Import Close

Figure 25

6. Knowledge objects are now imported successfully.



5.5 Report

1. Click **Reports** option and select the **New (*.etcrx)** option.

	Export Import Utility	
xport Import 1. Provide the path and file n 2. Gick the import button Note : If report(s) contains ter Options Category Filters Alerts Systems and Groups Token Value Proports Behavior Correlation	ame of Schedule Report file. Use the '' button to browse and locate the import file. nplate, first import template and proceed with exportimport utility. Location Legacy (* issch) New (* etcos) Source : * issch	
	Import	Close

Figure 27

2. Locate the file named Reports_SpamTitan Gateway.etcrx and select the checkbox.



sct file				and and	Select file	
lable reports						
•		Frequency Stowal	· Q	Q		
	Title	Stes	Groups		Systems	Frequence
ICIT Test	n Titlen Galleway - Spart Dmails					Undefined
EDIT Sow	n Titan Gabeway - Infected Emails with Vis					Undefined
						,
far. Set nun fan	e spiton is not applicable for Dafne	1 Reports and Houdy Reports				,
te: Set run tere	region is not applicable for Define	ef Reports and Hourly Reports	ten 54 ()			,
te: Set von ten t nun time fo	e option is not applicable for Carline r report(p) from	t Reports and Hourly Reports M • at interval of minu	tes Set ()			Activat

Figure 28

3. Click Import \mathbb{T} to import the report. EventTracker displays a success message.



Figure 29

5.6 Dashboards

NOTE: Below steps given are specific to EventTracker 9 and later.

1. Open EventTracker in browser and logon.



	Home		
٩	My Dashboard		
k	Threats	1	
	Incidents	Indicators of Compromise USB activities, New services or software install	
	Behavior Correlation		
	Change Audit		-
	Compliance	Carlos and	



- 2. Navigate to My Dashboard option as shown above.
- 3. Click Import I as shown below:

	My Dashboard	🕈 / Dashboard / My Dashboard
۹		+ 🖉 Q 🌣 1 🎞 O ()

- 4. Import dashboard file Dashboard_ SpamTitan Gateway.etwd and select Select All checkbox.
- 5. Click **Import** as shown below.







6. Import is now completed successfully.





7. My Dashboard page selects to 🕀 add a dashboard.

Ш	Netsurion. EventTracker	4 2	Admin -	Tools -	💽 Ada
	My Dashboard			🔒 / Das	hboard / M
۹			(֯@	¢ ±



8. Choose an appropriate name for Title and Description. Click Save.

Add Dashboard	
Title	1
Product/Software Name	
Description	
Product/Software Description	
	Save Delete Cancel

Figure 35

9. In **My Dashboard** page Select to add dashlets.



Figure 36



10. Select imported dashlets and click Add.

C	ustomize dashlets			×
	spam			Q
	☑ SpamTitan Gateway - Action tak	☑ SpamTitan Gateway - Top Spam	☑ SpamTitan Gateway - Top Suspi	SpamTitan Gateway - Top Suspi
	SpamTitan Gateway - Virus dete	SpamTitan Gateway - Virus dete	SpamTitan Gateway- All Events	
				Add Delete Close

Figure 37

Verifying SpamTitan Gateway knowledge pack in EventTracker

6.1 Category

- 1. Logon to EventTracker.
- 2. Click Admin dropdown, and then click Category.

≡	Event Tracker ⊕					🐥 🛛 Admin 🚽	Tools -
	Home		Active Watch Lists	Collection Master	🚰 Group Management	Systems	🕈 / Dashb
Q				Correlation	Q IP Lookup Configuration	Q Users	
_	O Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	1 Indicators of Cc USB activities, New sen	Behavior Correlation Rules	Tiagnostics 🔅 Knowledge Object		r Weights	
~			🗞 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config	
			Casebook Configuration	Seventvault	D Parsing Rules		
		-	el ^o Category	FAQ Configuration	Report Settings		
	Attacker			- News			



3. In **Category Tree** to view the imported category, scroll down and expand the **SpamTitan Gateway** group folder to view the imported category.



	Category	
Q R	Category Tree Search	
	All Categories *All error events *All information events *All warning events *All warning events *All warning events *All security events *Compe Audit *Comp	
	 SpamTitan Gateway SpamTitan Gateway - Infected Emails SpamTitan Gateway - Noqueue Email SpamTitan Gateway - Passed Emails SpamTitan Gateway - Spam Emails SpamTitan Gateway: Virus detected in m Windows 	

Figure 39

6.2 Alerts

- 1. In the EventTracker Manager web interface, click the Admin dropdown, and then click Alerts.
- 2. In search box enter "e.g. "SpamTitan" and then click Search. EventTracker displays an alert related to "SpamTitan Gateway":



	Alerts				
۹	Show All 🗸				
	119	15			
	Available Alerts Total number of alerts available	Active Alerts Total number of active alerts			
	Activate Now Click 'Activate Now'	after making all changes			
	Alert Name 🔨		Threat	Active	Email
	🗌 និ្តភ្លិ SpamTitan Gateway: Mail with Coronavirus/Covid-1	9 subject	•		
	📄 🖧 SpamTitan Gateway: Virus detected in Infected mail	5	•		

Figure 40

6.3 Token templates

1. In the EventTracker web interface, click the Admin dropdown, and then click Parsing rules.

≡	EventTracker @					🐥 🛛 Admin 🗸	Tools -
	Home		Active Watch Lists	Collection Master	🖙 Group Management	Systems	🕈 / Dashb
a		_	Alerts	© Correlation	Q IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	r Weights	
~		Indicators of Cc USB activities, New sen	🍓 Behavior Correlation Settings	😨 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point		Casebook Configuration	Seventvault	🧭 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker		- News				



2. On the **Template** tab, click on the **SpamTitan Gateway** group folder to view the imported token values.



	Parsing Rules			
۹	Parsing Rule Template			
2	Groups Default		(+)	Group : SpamTitan Gateway
	EventTracker	Ē	1	Template Name
	MSSQL Server	Ē	Ø	SpamTitan Gateway - Infected Email
	SpamTitan Gateway		Ø	SpamTitan Gateway - Noqueue
	windows		0	
				Email
				SpamTitan Gateway - Spam Email



6.4 Knowledge Object

1. In the EventTracker web interface, click the Admin dropdown, and then select Knowledge Objects.

≡	Event Tracker #					🐥 🛛 Admin 🗸	Tools +
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
٩			Alerts	Correlation	🔍 IP Lookup Configuration	QQ Users	
	0	1 Indicators of Cc USB activities, New sen	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	A Weights	
2			🗞 Behavior Correlation Setting	🔛 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point		Casebook Configuration	Eventvault	🧭 Parsing Rules		
			• Category	FAQ Configuration	Report Settings		
	Attacker			 News 			



2. In the Knowledge Object tree, expand the **SpamTitan Gateway** group folder to view the imported knowledge object.

Netsurion. EventTracker

	Knowledge Objects	
Q R	Search objects	Q Activate Now
	Groups 🕂 🧭 🗓	Object name SpamTitan Gateway Applies to Gateway Anti-spam Appliance
	Cisco ASA Firewall EventTracker	Rules
		Title
	Microsoft DHCP Server	SpamTitan Gateway events Message Signature:
	MSSQL Server	Message Exception:
	SpamTitan Gateway	Expressions
	Spamilitan Gateway	Expression type Expression 1 Regular Expression (?<=\<).*?(?=\>



3. Click Activate Now to apply imported knowledge objects.

6.5 Report

1. In the EventTracker web interface, click the Reports menu, and then select the Report Configuration.

≡	EventTracker									
	Home									
Q R	Report Configuration		1							
	Report Dashboard	ntry point	Indicators of Compromise USB activities, New services or software install							
	Explorer									
	Attacker			-						



- 2. In Reports Configuration pane, select the Defined option.
- 3. Click on the **SpamTitan Gateway** group folder to view the imported reports.



	Repo	ort Configuration					
٩	O so	:heduled 🔘 Queued 💽 D	efined				
Å	Repo	ort Groups		(+)	Rep	figuration: SpamTitan Gateways	
	1.5	Security			Ð	Î d	>
	1.5	Compliance					Title
	1.5	Operations				2.23	SpamTitan Gateway - Noqueue Email
	1.1	Flex				233	SpamTitan Gateway - Infected Emails with Virus
		Amazon AWS	Ē	0		2	SpamTitan Gateway - Spam Emails
		EventTracker	١.	1		243	SpamTitan Gateway - Passed Emails
		Microsoft DHCP	Ē	1	-	W	
		Microsoft SQL	Ĩ	1			
		MSSQL Server	Ĩ	1			
		SpamTitan Gateways	Ī	1			
	D	Windows	Ĩ	0			

Figure 46

6.6 Dashboards

1. In the EventTracker web interface, Click Home and select "My Dashboard".





2. In the "SpamTitan Gateway" dashboard you should be now able to see something like this.

≡	Netsurion. EventTracker							🔎 Admin = Tools = 🔘			
-	MSSQL Spanitan.										
۹.	SpamTitan Gateway- All Events	6 - ×	SpamTit	n Gateway - Action taken on	© - ×	SpamTitan Gateway - Virus detected i	© - ×	SpamTitan Gateway - Virus detected	© - ×		
	e infecter e requeur e pas e span		Series log_category		peri	en e			٩		
					spam			12.7.100.20 200.7.100.32			
	Jul 07 11:56 AM - Jul 14 11:57 AM			Jul 07 11:56 AM - Jul 14 1	1:57 AM	Jul 07 11:56 AM - Jul 14 11:57 AM		Jul 07 11:56 AM - Jul 14 11:57 AM			
	SpamTitan Gateway - Top Suspicious	0 - ×	SpamTitan Gateway - Top Spam mail with Subject and Sender 🛛 🕲 — 🕊					SpamTitan Gateway - Top Suspicious	© - ×		
			action	email_subject	sender_address						
			Pass		willy.S@infosec.com						
			Blocked		hounce-9493 HTML-615837	23-560306-7234512-22@bounce.renk.ien.com					
			Blocked		grace.quintero@zoom.net						
			Blocked		Hunter.X@Yamaha.net						
		\diamond	PASS	Covid-19 Vaccene update.	673-UWY-229.0.464899.0.0.3	309332.9.13623248@yahoo.com	0		0		
			PASS	PASS Coronavirus Global News. 673-UWY-229.0.464899.0.0.309332.9.13623248@bounce1.x		309332.9.13623248@bounce1.xyz.com					
	673-uwy-229.0.464899.0.0.309332.9.13623248@bounce1.xyz.com	om	filter		bounce213.xyz.com[192.168	.15.16]		kavin.tsur@contoso.com 📒 tim.cook@contoso.com			
	673-uwy-229.0.464899.0.0.309332.9.13623248@yahoo.com		filter bounce213.xyz.com[192.168.15.16]				📕 adam.s@contoso.com 📕 admin.server@contoso.com				
	bounce-9493 html-61583723-560396-7234512-22@bounce.re	83 html-61583723-560396-7234512-22@bounce.reolv.ier		Blocked			Corona-VirusHTML-61583723-560396-7234512-22@abc.replycom			eter.o@contoso.com eter.s@contoso.com	_
	Jul 07 11:56 AM - Jul 14 11:57 AM				Jul 07 11:56 AM	- Jul 14 11:57 AM		Jul 07 11:56 AM - Jul 14 11:57 AM	<u>^</u>		



Netsurion. EventTracker