Netsurion. EventTracker

Integrate Amazon Web Service (AWS) GuardDuty

EventTracker v9.2 and later

Publication Date: October 22, 2020

Abstract

This guide provides instructions to integrate AWS with EventTracker manager using AWS Lambda.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and Amazon AWS.

Audience

Administrators who are assigned the task to monitor Amazon AWS 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.	Pre	erequisites	. 3
2.	Ov	erview	. 3
3.	Int	egrating AWS GuarDuty using Lambda Function	. 4
4.	Eve	entTracker Knowledge Packs	. 7
	4.1	Saved Searches	. 7
	4.2	Alerts	. 9
	4.3	Flex Reports	10
	4.4	Dashboard	10
5.	Im	porting knowledge pack into EventTracker	13
	5.1	Alerts	14
	5.2	Token Template	15
	5.3	Flex Reports	17
	5.4	Knowledge Objects	18
	5.5	Dashboards	20
	5.6	Saved Searches	21
6.	Ve	rifying knowledge pack in EventTracker	22
	6.1	Alerts	22
	6.2	Token Template	23
	6.3	Flex Reports	23
	6.4	Knowledge Objects	24
	6.5	Dashboards	25
	6.6	Saved Searches	26

Netsurion. EventTracker[®]

1. Prerequisites

- EventTracker v9.2 and above/ EventTracker agent should be installed.
- Administrative access for AWS Account.
- EventTracker syslog VCP port / EventTracker syslog relay port (e.g. 514) should be allowed on public IP.
- GuardDuty should be enabled on your AWS account.
- CloudWatch Should be enabled on your AWS account.

2. Overview

Amazon GuardDuty is a threat detection service that continuously monitors malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3.

Amazon GuardDuty can be integrated with EventTracker using EventTracker Lambda function. After the logs are received from GuardDuty, EventTracker alerts you of the following finding types:

- Backdoor
- Crypto Currency
- Discovery
- Impact
- Pentest
- Persistence
- Policy
- Privilege Escalation
- Recon
- Resource Consumption
- Stealth
- Trojan
- Unauthorized Access

EventTracker dashboard will display the summarized view of GuardDuty findings based on Threat type, Source IP and Map view of suspicious activities source location.

EventTracker reports will provide activities summary on scheduled basis. These reports will also furnish details about all activities, resources affected, about the threat actor, etc.



3. Integrating AWS GuarDuty using Lambda Function

Before integrating AWS GuardDuty with EventTracker manager, we need to integrate AWS with EventTracker using Lambda function. Follow <u>this</u> guide before proceeding with the below instructions:

- 1. Login into AWS CloudWatch portal.
- 2. Click on the Rules tab under Events and create rule by clicking Create rule.

aws Services ▼								
CloudWatch Dashboards Alarms ALARM 0 INSUFFICIENT 0 OK 0 Billing Logs Log groups Insiahts	CloudWatt Amazon EventBr event-driven arch Amazon EventBr Rules Rules Rules route events to Create rule	CloudWatch Events is now Amazon EventBridge Amazon EventBridge (formerly CloudWatch Events) provides all functionality from CloudWatch Events and also launched new features such as Custom event buses, 3rd party event sources and Sc event-driven architecture and applications. Amazon EventBridge documentation Rules Rules Rules Create rule Actions						
Metrics								
Events	Status All	▼ Name						
Rules	Sta	tus Name			Description			
Event Buses								
ServiceLens								
Service Map								
Traces								
Resources								
Performance Monitoring								
Lambda Insights NEW								
Multi-function								
Single-function								
Synthetics								
Canaries								
Contributor Insights								
Settings								
Favorites								
O Add a dashboard								
				Figure 1				

3. In Create rule screen, select GuardDuty in Service Name and All Events in Event Types as Event Source.





Step 1: Create rule

Create rules to invoke Targets based on Events happening in your AWS environment.

Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

Event Pattern () Schedule ()								
Build event pattern to match even	Build event pattern to match events by service -							
Service Name	GuardDuty	•						
Event Type	All Events	•						
Build an event pattern to match all ev	vents from this service							
 Event Pattern Preview 		Copy to clipboard	Edit					
<pre>{ "source": ["aws.guardduty"] }</pre>								

Figure 2

4. In **Targets** section, click **Add Target** and select **Lambda** function created for EventTracker. If Lambda function for EventTracker is still not created. Follow <u>this</u> Instructions.

Targets

Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.

O Add target*

Figure 3





Keep the remaining section as default.

Lambda function		- 0
Function*	EventTrackerSIEMIntegration	•
 Configure vers 	EventTrackerSIEMIntegration //alias Select version Select alias nt the the devent DN text)	
Default		
O Version	Select version	•
Alias	Select alias	•
 Configure input 	t	
Matched e	went 🚯	
Constant (JSON text) 🕤	
Input Tran	sformer 🚯	

Figure 4

5. Click Configure details.

reate rules to invoke Targets	s based on Events happening in your AWS environment				
Event Source			Targets		
uild or customize an Event F	Pattern or set a Schedule to invoke Targets.		Select Target to invoke	when an event matches your Event Pattern or when schedule is	triggered.
🔵 Event Pattern 🚯 🗌	Schedule ()		Lambda function		- 6
Build event pattern to ma	tch events by service	•	Function*	EventTrackerSIEMIntegration	•
Service Name	GuardDuty	-		n/alias	
Event Type	All Events	•	Default		
Build an event pattern to m	atch all events from this service		Version	Select version	Ť
Event Pattern Preview		Copy to clipboard Edit	Alias	Select alias	*
{ "source": ["aws.guardduty"] }			Configure input Matched eve Part of the m Constant (JS Input Transfo Add target*	nt ⊕ atched event ⊕ ON text) ⊕ rmer ⊕	
Show sample event(s)		h			

Figure 5





6. Provide Rule name (e.g. Guardduy ET Integration) and enable the State option and click Create rule for the completion of GuardDuty integration with EventTracker.

Step 2: Configure rule details Rule definition Name* Guardduty_ET_Integration Description State Enabled CloudWatch Events will add necessary permissions for target(s) so they can be invoked when this rule is trig * Required Figure 6								
Rule definition Name* Guardduty_ET_Integration Description								
		Name*	Guardduty_ET_Integratio	n				
		Description			li			
		State	Enabled					
CloudWatch Events will add necessary permissions for target(s) so they can be invoked when this rule is triggered. * Required Cancel Back Create rule								
* Required						Cancel Back	Create rule	
				Figure 6				
Rules								
Rules route ev	ents from y	our AWS resource	s for processing by se	lected targets. Yo	u can create, edit, and o	delete rules.		
Create rule	Act	ions 🔻					20	
Status All	•	Name			«	< Viewing 1 to 2	of 2 Rules > >>	
	Status	Name			Description			
		Guardduty_ET	_Integration					



4. EventTracker Knowledge Packs

4.1 Saved Searches

- AWS Guardduty: Backdoor This saved search will provide details about the backdoor activities attempting to happen on your AWS account. It provides detailed view of activities, resource affected, actor details and many more information.
- AWS Guardduty: Behavior This saved search will provide details about the unusual behavior activities attempting to happen on your AWS account. It provides detailed view of activities, resource affected, actor details and many more information.
- AWS Guardduty: Crypto Currency This saved search will provide details about the cryptocurrency • related activities (like EC2 instance is querying an IP address that is associated with bitcoin) which attempt to happen on your AWS account. It provides detailed view of activities, resource affected, actor details and many more information.



- AWS Guardduty: Discovery This saved search will provide details about the unusual discovery activities (like S3 API such as GetObjectAcl or ListObjects, was invoked from a Tor exit node IP address) which attempt to happen on your AWS account. It provides detailed view of activities, resource affected, actor details and many more information.
- AWS Guardduty: Impact This saved search will provide details about the unusual impactable activities (like IAM API call for changing permission on one or more buckets or objects.) happen on your AWS account. It provides detailed view of activities, resource affected, actor details and many more information.
- AWS Guardduty: PenTest This saved search will provide details about the pentest activities (like API invoked by parrot security Linux machine) happen on your AWS account. It provides detailed view of activities, resource affected, actor details and many more information.
- **AWS Guardduty: Persistence** This saved search will provide details about specific principal in your AWS environment is exhibiting different behavior from the established baseline. It provides detailed view of activities, resource affected, actor details and many more information.
- AWS Guardduty: Policy This saved search will provide details about the policy related activities (like root credential usage). It provides detailed view of activities, resource affected, actor details and many more information.
- AWS Guardduty: Privilege Escalation This saved search will provide details about the principal which has attempted to assign a highly permissive policy to themselves. It provides detailed view of activities, resource affected, actor details and many more information.
- AWS Guardduty: Recon This saved search will provide details about activities that can list or describe AWS resources in an account within your environment was invoked from an IP address that is included on an internal threat list. It provides detailed view of activities, resource affected, actor details and many more information.
- AWS Guardduty: Resource Consumption This saved search will provide details about the AWS environment are launched under suspicious circumstances. It provides detailed view of activities, resource affected, actor details and many more information.
- AWS Guardduty: Stealth This saved search will provide details about the attacker activities which attempt cover their tracks by eliminating any trace of their activity while gaining access to your AWS resources for malicious purposes. It provides detailed view of activities, resource affected, actor details and many more information.
- AWS Guardduty: Trojan This saved search will provide details about the trojan activities (DGA domain request, DNS data exfiltration, Drive by source traffic, etc.) happen on your AWS environment. It provides detailed view of activities, resource affected, actor details and many more information.

Below is one of the samples of Saved search

Netsurion. EventTracker

	Time	rule_name	service_type	object_id	log_info
+	Oct 15 02:00:04 AM	Unusually large amount of network traffic from EC2 instance i-999999999.	Behavior:EC2/TrafficVolumeUnusual	828890237078	EC2 instance i-99999999 is generating unusually large amounts of network traffic to remote host 198.51.100.0.
+	Oct 15 01:59:50 AM	Unusual outbound communication seen from EC2 instance i-99999999 on server port 80.	Behavior:EC2/NetworkPortUnusual	828890237078	EC2 instance i-999999999 is communicating with a remote host on an unusual server port 80.
+	Oct 15 01:43:04 AM	Unusually large amount of network traffic from EC2 instance i-99999999.	Behavior:EC2/TrafficVolumeUnusual	828890237078	EC2 instance i-99999999 is generating unusually large amounts of network traffic to remote host 198.51.100.0.
+	Oct 15 01:42:58 AM	Unusual outbound communication seen from EC2 instance i-999999999 on server port 80.	Behavior:EC2/NetworkPortUnusual	828890237078	EC2 instance i-999999999 is communicating with a remote host on an unusual server port 80.

Figure 8

4.2 Alerts

- AWS Guardduty: Backdoor detected This alert will be triggered when the backdoor activities happen on your AWS environment.
- AWS Guardduty: Cryptocurrency based threat detected This alert will be triggered when the cryptocurrency related activities (like EC2 instance is querying an IP address that is associated with bitcoin) attempt to happen on your AWS environment.
- AWS Guardduty: Discovery category threat detected This alert will be triggered when the unusual discover activities (like S3 API such as GetObjectAcl or ListObjects, was invoked from a Tor exit node IP address) happen on your AWS environment.
- AWS Guardduty: Impact category threat detected This alert will be triggered when the unusual impactable activities (like IAM API call for changing permission on one or more buckets or objects.) happen on your AWS environment.
- AWS Guardduty: Pentest activities detected This alert will be triggered when the pentest activities (like API invoked by parrot security Linux machine) happen on your AWS environment.
- **AWS Guardduty: Persistence activities detected** This alert will be triggered when specific principal in your AWS environment is exhibiting different behavior from the established baseline.
- AWS Guardduty: Policy based activities detected This alert will be triggered when the policy related activities (like root credential usage) happen on your AWS environment.
- **AWS Guardduty: Privilege Escalation detected** This alert will be triggered when the principal attempts to assign a highly permissive policy to itself.
- AWS Guardduty: Recon activities detected This alert will be triggered when activities that can list or describe AWS resources in an account within your environment was invoked from an IP address and is included on an internal threat list.
- AWS Guardduty: Stealth activities detected This alert will be triggered when the attacker activities attempt cover their tracks by eliminating any trace of their activity while gaining access to your AWS resources for malicious purposes.
- **AWS Guardduty: Trojan detected** This alert will be triggered when the trojan activities (DGA domain request, DNS data exfiltration, Drive by source traffic, etc.) happen on your AWS environment.
- AWS Guardduty: Unauthorized Access detected This alert will be triggered when the unauthorized activities (putobject or putobjectacl api was invoked from a Tor exit node IP address.) happen on your AWS environment.



Below is the one of sample of alert:

- (Oct 15 07:39:51 AM	VII011 WIN-MCKKRLN6KOI / aws.guardduty~828890237078-syslog	AWS Guardduty: Backdoor threat detected	
Short Desi	scription 🔘 Alert Details			
Summary:				
Description: B	EC2 instance i-99999999 is behaving in a manner	that may indicate it is being used to perform a Denial of Service (DoS) attack using TCP protocol.		
Following are	the details:			
Rule: EC2 inst	tance i-99999999 is behaving in a manner that m	y indicate it is being used to perform a Denial of Service (DoS) attack using TCP protocol.		
Type: Backdo Resource Typ	sor:EC2/DenialOfService.Tcp			
Source IP: 10.	0.0.023			
Incident#	202010000011157			
Event Type	Information			
Asset Value	Serious			
User	NA			
Source	Syslog Local			
Description	Oct 19 021105 etc11311 100-65 [Presion1] Schemwission 120, "sccound" 82889023 2828802217078 detector/Solabald'sec2042 123456780000-topostic-p-0fic-0oleFable/7 [Panls" ramavaism8288902217078 asamplich (Panls" ChemateFindingInstace/luba") [Panls" GenerateFindingInstace/luba") (Panls" GenerateFindingInstace Isylauter (Panls" GenerateFindingInstace Isylauter (Panls" GenerateFindingInstace Isylauter (Panls" GenerateFindingInstace Isylauter (Panls" GenerateFindingInstace Isylauter (Panls" GenerateFindingInstace Isylauter (Panls" GenerateFindingInstace Isylauter (Panls") Gen	"In"":2004/14-2-27-345ec-08-20-10.32/05/8117"; "detail-type" "CaardOur"; Inding": "source"; "avays quarddshy": "escourd" 1007": regont": use-21"; "antition": "ava": "of "redeb/3564/2020/2004003/5566/32.av" in" annas quarddshy: "escourd" 1006/76/346/2760/finding/6eba9564/027302/3401/35966/32.av"; hype: "facedoorfic2/DenalOfService, Tey": "resource" 1006/76/346/2760/finding/6eba9564/027302/3401/37967 1007/1007/1007/1007/1007/1007/1007/1007	"828990237079" "time" "0220-10-13T06-30062", "region" /'us-east-2", "resources' []] 'detail"; ["resource'] bye ''Instance', "instance/Details', "instance'] bye ''m3.wileye'', add" ''product-doct ''post-10000', "post-30000', "instance'', "post-10000', "instance'', "post- add" ''post-10000', "post-10000', "instance'', "post-10000', "instance'', "post- uley' 'Cremented' Finding Instance ''goldward'', "key'', "Ceremented' Finding Instance'', "post- vie', "imageid '' ami-99999999', "ImageD exciption", "Generated Finding Instance'', "post- fiction Officed on ''OLI BOOKD', ''Could Octable', "key'', "Ceremented Finding Instance'', "post- etion Officed on ''OLI BOOKD', ''Could Octable', "I'post- fiction Officed on ''OLI BOOKD', ''Could Octable', "I'post- fiction Officed on ''OLI BOOKD', ''Could Octable', ''post- fiction Officed on ''OLI BOOKD', ''post- fiction Officed on ''OLI BOOKD', ''Could Octable', ''post- fiction Officed on ''OLI BOOKD', ''Could Octable', ''post- ont on ''Could ''Could Octable', ''post- Generated Finding Instance', ''post- ance'', ''post- ont officed on ''OLI BOOKD', ''Could Octable', ''post- ont on ''Could ''Could Octable', ''post- ance'', ''post- ance'', ''post- ance'', ''post- ''Could ''Could Octable', ''post- ''Could ''Could ''Could Octable', ''post- ''Could ''Could Octable', ''post- ''Could ''Could ''Could Octable', ''post- ''Could ''Could Octable', ''post- ''Could ''Could Octable', ''post- ''', ''otable', '''otable', ''post- ''', ''', '''otable', '''otable', ''', ''', ''', '''', '''', '''', '''', ''''', ''''', ''''', ''''', ''''''	outpostAm","amawsoutpostsus-west- blicDNSName", "privatelpAddress","10.00.17); "tags" envice"; "dress/44"198.51.100.01", organization, "t@(anne-1); 00.pont/luners"; "HTTP1, "tscalabutDetata"; "th" "2020 butDetata"; "dottedata"; "2020- th"; "2020 butDetata;"; "dottedata"; "2020- stata; "dottedata"; "dottedata; "2020- stata; "dottedata; "dottedata; "dottedata; "2020- stata; "dottedata; "dotte



4.3 Flex Reports

• AWS Guardduty : Findings – This report provides information about the findings detected by AWS GuardDuty. It will have details about rule name, its categories, resource affected, threat actor, identity of attacker like IP address, ASN, geolocation.

LogTime	Computer	Rule Name	Туре	Severity	Account	Remote IP	Resource Type	Resource Details	Finding Details
10/15/2020 01:38:21 AM	AWS.GUARDDUTY~82889023707 8	Unusual user permission reconnaissance activity by GeneratedFindingUserName.	Recon:IAMUser/UserPermissions	* 5	828890237078	198.51.100.0	AccessKey	"accessKeyld","CeneratedFinding AccessKeyld", principald","Gener atedFindingPrincipald","userType": "IAMUser","userName":"Generated FindingUserName"	APIs commonly used to discover the users, groups, policies and permissions in an account, was invoked by IAM principal GeneratedFindingUserName under unusual circumstances. Such activity is not typically seen from this principal.
10/15/2020 01:42:48 AM	AWS.GUARDDUTY~82889023707 8-SYSLOG	API GeneratedFindingAPIName was invoked from a Tor exit node.	UnauthorizedAccess:S3/TorIPCalle r	2	828890237078	198.51.100.0	S3Bucket	"accessKeyld":"GeneratedFinding AccessKeyld","principalld":"Gener atedFindingPrincipalld","userType": "AMUser","userName":"Generated FindingUserName"	API GeneratedFindingAPIName was used to access bucket GeneratedFindingS3Bucket from Tor exit node IP address 198.51.100.0.
10/15/2020 01:42:49 AM	AWS.GUARDDUTY~82889023707 8-SYSLOG	API GeneratedFindingAPIName was invoked from a Parrot Security Linux computer.	PenTest:IAMUser/ParrotLinux	5	828890237078	198.51.100.0	AccessKey	"accessKeyld": "GeneratedFinding AccessKeyld", "principalld": "Gener atedFindingPrincipalld", "userType": "IAMUser", "userName": "Generated FindingUserName"	API GeneratedFindingAPIName was invoked from a remote host with IP address 198.51.100.0 that is potentially running the Parrot Security Linux penetration testing tool.
10/15/2020 01.42.49 AM	AWS GUARDOUTY-8288023707 8-SYSLOG	EC2 Instance - 99999999 is communicating with a Drop Point.	Trojan EC2/DropPoint	-	* 828890237078	198.51.100.0	Instance	"Instance1""- 99999999", "InstanceType", "m3 xiar 99909999", "InstanceType", "m3 xiar 9212456780900 outpostop- 0fbc006e9abbc732", "aunorTime", 7016-08- 021702:05.692", "platform", null"prod ucCodes", ["productCode1", "prod ucCodes", "productCode1", "prod ucCodes", "productCode1", "prod ucCode1", "pre", "Generated1", indig	EC2 instance i-99999999 is communicating with a remote host 1985.11.00.0 that is known to hold credentials and other stolen data captured by malware.



4.4 Dashboard

• **GuardDuty** - **Findings by Type** - This dashboard provides the summarized details of suspicious activity type. On clicking, it provides more details like remote IP address, resource effected, etc.





Figure 11

• **GuardDuty** - **Findings by Name** - This provides rule-based summary of suspicious activities. Click on dashboard to find more details. Here, number represent severity of activities, higher the number, highly suspicious the activities is.





• **GuardDuty** - **Findings by User-agent** - This dashboard gives summarized view of user agent from where the suspicious activities happen. This user agent provides details about the system, browser, browser version from where the suspicious activities happen.





Figure 13

 GuardDuty - Findings Trend - This dashboard will provide daily basis trend of suspicious activities happening on your AWS environment.





• **GuardDuty - Findings by Resource Type** - This dashboard will help you to view the summarized details of resource types on which GuardDuty has found suspicious activities.





Figure 15

5. Importing knowledge pack into EventTracker

Getting Knowledge Packs

To get the knowledge packs, locate the knowledge pack folder. Follow the below steps:

- 1. Press "₩ + R".
- 2. Type "%et_install_path%\Knowledge Packs" and press "Enter".

(**Note** – If, not able to locate the file path as mentioned above, please contact <u>EventTracker support</u> to get assistance,).

NOTE: Import knowledge pack items in the following sequence:

- Saved Searches
- Alerts
- Token Template
- Flex Reports
- Knowledge Objects
- Dashboards
- 1. Launch the EventTracker Control Panel.
- 2. Double click Export-Import Utility.

EventTracker Con	itrol Panel				\times		
	ale carata	No.	Eve	entTracker	9		
	5			2			
EventVault	Diagnostics	License Manager	Export Import Utility	Append Archives			
oQ.		X	*				
EventTracker Agent Confi	Traffic Analyzer	Agent Manageme	Port Configuration	TrapTracker			
?	-83						
Change Audit	About EventTracker						
E-mail: support@EventTracker.com							

Figure 16

🐁 Export Import Utility							
Export							
1. Provide the path and 2. Click the Import butto	file name of the Categories file. Use the '' button to n.						
Options	Location						
Category							

Figure 27

3. Click the **Import** tab.

5.1 Alerts

- 1. Open "Export Import Utility" via "EventTracker Control Panel", click Alert option, and then click the browse button.
- 2. Navigate to the knowledge pack folder and select the file with extension ".isalt", e.g. "Alerts_ AWS Guardduty.isalt" and then click "Import".

🐁 Export Import Utility			\times			
Export Import						
1. Provide the path and file nam 2. Click the Import button.	ne of the Alerts file. Use the '' butt	on to browse and locate the import file.				
Options	Location					
Category	✓ Import E-mail settings					
 Filters Alerts 	Set Active Only if notifications set By default	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.				
O Systems and Groups	Watchlist Configuration					
○ Token Value	Import Watchlist configuration					
0	This setting is applicable only for alerts which have Advanced watchlist configured. Note: If this option is enabled the user should make sure the watchlist groups are available					
Reports	on the console where the alert	s are imported.				
O Behavior Correlation						
	Source :					
	*.isalt					
		Import	Close			



EventTracker displays a success message:





5.2 Token Template

For importing "Token Template", navigate to EventTracker manager web interface.

1. Click **Parsing Rules** under the **Admin** option in the EventTracker manager web interface.



	🔎 Adr	min ↓ Tools ↓
ers	😥 Parsing Rules	^ /
lt Contains	set of rules which tell what k	kind of data you want
Configuration	Systems	_



2. Click the "Template" tab and then click the "Import Configuration" button.

Parsing Rules	5			
Parsing Rule	Template			
Groups			\oplus	Group :
Default			^	
Azure Intune		Ē	0	Templa







Click "Browse" and navigate to the knowledge packs folder (type "%et_install_path%\Knowledge Packs" in navigation bar) where ".ettd", e.g. "Templates_AWS Guardduty.ettd" file is located. Wait for the templates to load. After the templates are loaded, choose the required templates and click "Import".



Import	
Select file Note: Please select file	e of type *.ettd (eventtracker template dashlets).

Figure 23

5.3 Flex Reports

1. In EventTracker control panel, click "Export/ Import utility" and click the "Import" tab. Then, click Reports option, and choose "New (*.etcrx)":

 Export Import Utility Export Import 1. Provide the path and file nan 2. Click the Import button Note : If report(s) contains temp 		• ×
Options	Location	
Category		
⊖ Filters		
⊖ Alerts	◯ Legacy (*.issch)	
O Systems and Groups	Source : *issch	
O Token Value		
Reports		
O Behavior Correlation		
	Import	Close

Figure 44

 After selecting "New (*.etcrx)", a pop-up window appears. Click "Select File" and navigate to the knowledge pack folder and select file with extension ".etcrx", e.g. "Flex Reports_ AWS Guardduty.etcrx".

Reports Import								
Note : If repo	Note : If report(s) contains template, first import template and proceed with report import process. Select file Available reports							
	orts		Fi	requency Show all	•	Q Q		
		Title	Sites	Groups	Systems	Frequency	Runtime	Туре
		litle	Sites	Groups	Systems	Frequency	Runtime	Гуре

Figure 55

Wait while reports are being populated in below tables. Select all the relevant reports and then click Import .

Note: Set run time option is not applicable	e for Defined Reports and Hourly Reports		
Set run time for report(s) from	AM • at interval of minutes Set		
Replace	to Replace Assign systems		
	Note: Make sure that Site(s), Group(s) and System(s) selections are valid	d. 💶	\otimes

Figure 66

EventTracker displays a success message:

Export Import Utility	\times
Selected reports configurations are imported successful	у
ОК	



5.4 Knowledge Objects

1. Click Knowledge objects under the Admin option in the EventTracker manager web interface.

		🔎 🛛 Admin 🗸	Tools 👻 📀		
Active Watch Lists	Event Filters	🧭 Parsing Rules	📌 / Das		
Alerts	Eventvault	Report Settings			
Behavior Correlation Rules	FAQ Tile Configuration	Systems			
🗞 Behavior Correlation Settings	Group Management	QQ Users			
yr sc Casebook Configuration	🔍 IP Lookup Configuration	r Weights	Systems since the last 24 hour		
● Category	·☆ Knowledge Objects	Windows Agent Config			
Diagnostics	D Manager				



2. Click the **"import object"** icon:





 A pop-up box appears, click "Browse" and navigate to the knowledge packs folder (type "%et_install_path%\Knowledge Packs" in navigation bar) with the extension ".etko", e.g. "KO_ Amazon AWS.etko" and then click "Upload".

Import	
KO_ <product name="">.etko</product>	🗁 Browse Upload

Figure 70

4. Wait while EventTracker populates all the relevant knowledge objects. After the objects are displayed, select the required ones and click on "**Import**" button:





Figure 31

5.5 Dashboards

- 1. Login to EventTracker manager web interface.
- 2. Navigate to **Dashboard** \rightarrow **My Dashboard**.
- 3. In "My Dashboard", Click Import:



Figure 82



Figure 93



- Click Browse and navigate to knowledge pack folder (type "%et_install_path%\Knowledge Packs" in navigation bar) where ".etwd", e.g. "Dashboards_AWS Guardduty.etwd" is saved and click on "Upload" button.
- 5. Wait while EventTracker populates all the available dashboards. Now, choose "Select All" and click on "Import" Button.

Import
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.
Available widgets Select All
Figure 104



5.6 Saved Searches

- 1. Login to EventTracker Manager.
- 2. Navigate to Search -> Import.



ADVAN	CED SEARCH	BASIC SEARCH						Netsurion	EventTracker*	
> Sites			Search in archives		[Export Import	Clear all Sa	wed searches Search	٦	
GROUPS	WIN-MCKKRLN6KOI			Enter lucene query					(i)	
AVAILABLE	Groups Total: 3							0		
SYSTEMS								🕓 Last 1 hr	r	
SELECTED	Group search.	Q,	Q	Custom criteria						
	∎ [®] All Groups		$\overline{\nabla}$							
	∎ ⁿ ∎ Default			Search in		Operator		Search for		
	B ^B B EventTrac	:ker		Search in	~	Operator	 Search for 			
	B WORKGR	OUP		Note: To add search criteria, cli	:k icon(s) above					



3. Click on **Browse** and choose the file **"Saved searches_AWS Guardduty.etss"** under

%et_install_path%/Knowledge Packs. After selecting .etss file click upload to finish the saved search importing.



6. Verifying knowledge pack in EventTracker

6.1 Alerts

- 1. In the EventTracker manager web interface, click the Admin dropdown, and then click Alerts.
- In search box enter "<search criteria> e.g. "GuardDuty" and then click the Search button. EventTracker displays an alert related to "AWS GuardDuty":

Alerts	5 Admin / Alerts								
Show All						Search by Alert name	*	guardduty Q	Q
123 Available Alerts Tota number of alerts available	14 Active Alerts Total number of active alerts			123 System/User Defir Count for system and us	System User 18 ned Alerts er defined alerts	105	123 Alerts by Thre Count of alerts by	Critical is of the second seco	
Activate Now Click 'Activate Now' after making a	l changes							Total: 12 Page Size 25	5 🗸
Alert Name A	Threat	Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To	
□ δδ AWS Guardduty: Backdoor detected	•						Ū.	AWS Guardduty	
AWS Guardduty: CryptoCurrency based threat detected	•							AWS Guardduty	
AWS Guardduty: Discovery category threat detected	•							AWS Guardduty	
βδ AWS Guardduty: Impact category threat detected	•							AWS Guardduty	
AWS Guardduty: Pentest activities detected	•							AWS Guardduty	
AWS Guardduty: Persistence activities detected	•							AWS Guardduty	
ββ AWS Guardduty: Policy based activities detected	•							AWS Guardduty	
AWS Guardduty: Privilege Escalation detected	•							AWS Guardduty	
AWS Guardduty: Recon activities detected	•							AWS Guardduty	
AWS Guardduty: Stealth activities detected	•							AWS Guardduty	
B& AWS Guardduty: Trojan detected	•							AWS Guardduty	
BAWS Guardduty: Unauthorized Access detected	•							AWS Guardduty	

Figure 38

6.2 Token Template

- 1. In the EventTracker web interface, click the Admin dropdown, and then click Parsing Rules.
- 2. In the **Template** tab, click on the **"<product name/ report group name>"** e.g. **"AWS Guardduty**" group folder to view the imported Templates.

Parsing Rules								† /	Admin / Parsing Rules
Parsing Rule Template									
Groups		+ :::	Group : AWS Guardduty	Search	Q				CİŢ
Default									
AWS Guardduty	Ű	1	Template Name	Template Description	Added By	Added Date	Active		
EventTracker	Û	1	AWS Guardduty - Findings		ETAdmin	Oct 15 05:27:39 AM		Ø	
Windows	Û	1							
								Delete	Move to group



6.3 Flex Reports

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



Netsurion. EventTracker°





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

Repor	rt Configuration									A / Reports	/ Report Config	uration / Defined
O Sch	neduled 🔿 Queued 🖲 Defined							Search		Q, e		
Repor	rt Groups		+	Reports	configuration: AV	VS GuardDuty						
1.5	Security			🕂 🗓	<i>0</i> ,							Total: 1
1.5	Compliance					Title	Created on		Modified on			
S.,	Operations				(2)	AWS Guardduty - Findings	Oct 15 05:13:13 AN	1	Oct 15 05:39:16 AM	<u>(</u>)	8	+
1.5	Flex											
	AWS GuardDuty	Ē	1									
	EventTracker	Û	0									
	Windows	Ü	1									



6.4 Knowledge Objects

- 1. In the EventTracker web interface, click the Admin dropdown, and then click Knowledge Objects.
- 2. In the **Knowledge Object** tree, expand the "**AWS Guardduty**" group folder to view the imported Knowledge objects.

Knowledge Objects								Admin / Knowledge Objects
aws	Q Q	Activate Now						Objects 🕀 ፒ 🏦 🌣
Groups	⊕ Ø Î	Object name Amazon AWS Applies to Amazon AWS						⊕ ± \$
AUGLULARIS		Rules Title Amazon AWS Message Signature: Message Exception: Exception:	Event source Syslog	Source Type Amazon AWS	Log type	Event id	Event type	C 🔍 🗓 L,
		Expressions Expression type Regular Expression	Expression 1 "(? <key>{^*})``?(?<value>{^*})</value></key>	-)		Expression 2	Format string	0 i



6.5 Dashboards

1. In the EventTracker web interface, click on the Home Button and select "My Dashboard".





2. Select the **"Customize daslets**" Substitution and type **"GuardDuty**" in the search bar.







Custo	mize dashlets			×
guard	duty			Q
Gu	ardDuty - Findings by Name	GuardDuty - Findings by Resour	GuardDuty - Findings by Type	GuardDuty - Findings by User-a
Gu	ardDuty - Findings Trend			
				Add Delete Close

Figure 45

6.6 Saved Searches

- 1. Login to EventTracker manager web interface.
- 2. Navigate to Search -> Saved Searches.

ADVAN	ICED SEARCH	BASIC SEARCH					Netsurio	on EventTra	icker⁻
>	Sites			Search in archives		E	xport Import Clear all	Saved searches	Search
GROUPS	WIN-MCKKRL	N6KOI	~	Enter lucene guery			•		(i)
AVAILABLE	Groups Total: 3							0	
SYSTEMS	ALL DE W)						0	Last I nr
SELECTED	Group search.	Q	Q	Custom criteria					
	Ba All Group	55		$\overline{\nabla}$					۲
	Default			Sear	ch in	Operator	Search for		_
	B ^B B EventTra	cker		Search in	~	Operator 🗸	Search for		
	UNRKGF	OUP		Note: To add search crit	iteria, click icon(s) above				
				Override indexer					

Figure 46

3. Click on Saved Searches and search for "GuardDuty".



Saved Searches

Us	er defi	ned Pre defined				
Gu	ardduty	/			6	2
	Ì 🔒					
		Title	Added by			-
		Last search	ETAdmin	Ø	Q	
	٤Q	AWS Guardduty: Backdoor	ETAdmin	Ø	Q	
	٤Q	AWS Guardduty: Behavior	ETAdmin	Ø	Q	
	٤Q	AWS Guardduty: Crypto Currency	ETAdmin	Ø	Q	
	٤Q	AWS Guardduty: Discovery	ETAdmin	Ø	Q	
	٤Q	AWS Guardduty: Impact	ETAdmin	Ø	Q	
	٤Q	AWS Guardduty: PenTest	ETAdmin	Ø	Q	
	٤Q	AWS Guardduty: Persistence	ETAdmin	Ø	Q	
	Ð	AWS Guardduty: Policy	ETAdmin	0	Q	
	٤Q	AWS Guardduty: Privilege Escalation	ETAdmin	0	Q	
	Б	AWS Guardduty: Recon	ETAdmin	Ø	Q	•

Close

 \times

Figure 47

Netsurion. EventTracker*