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.

Table of Contents

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 this 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.**

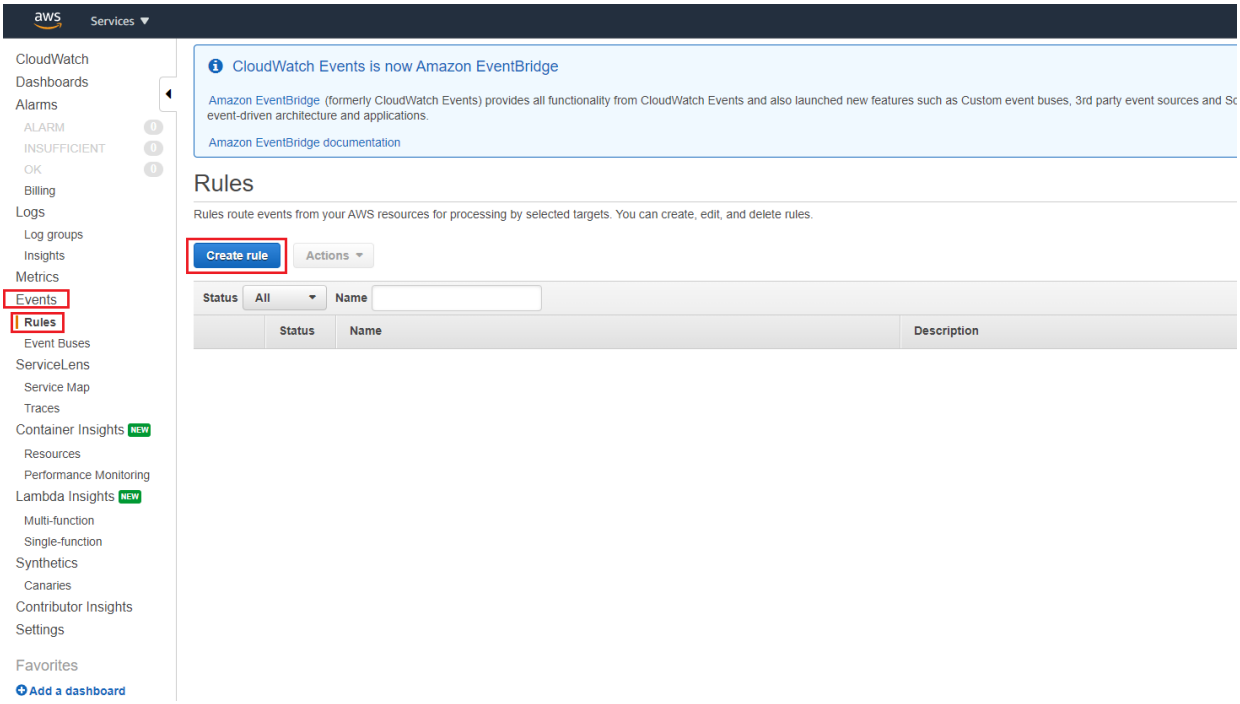

Figure 1

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

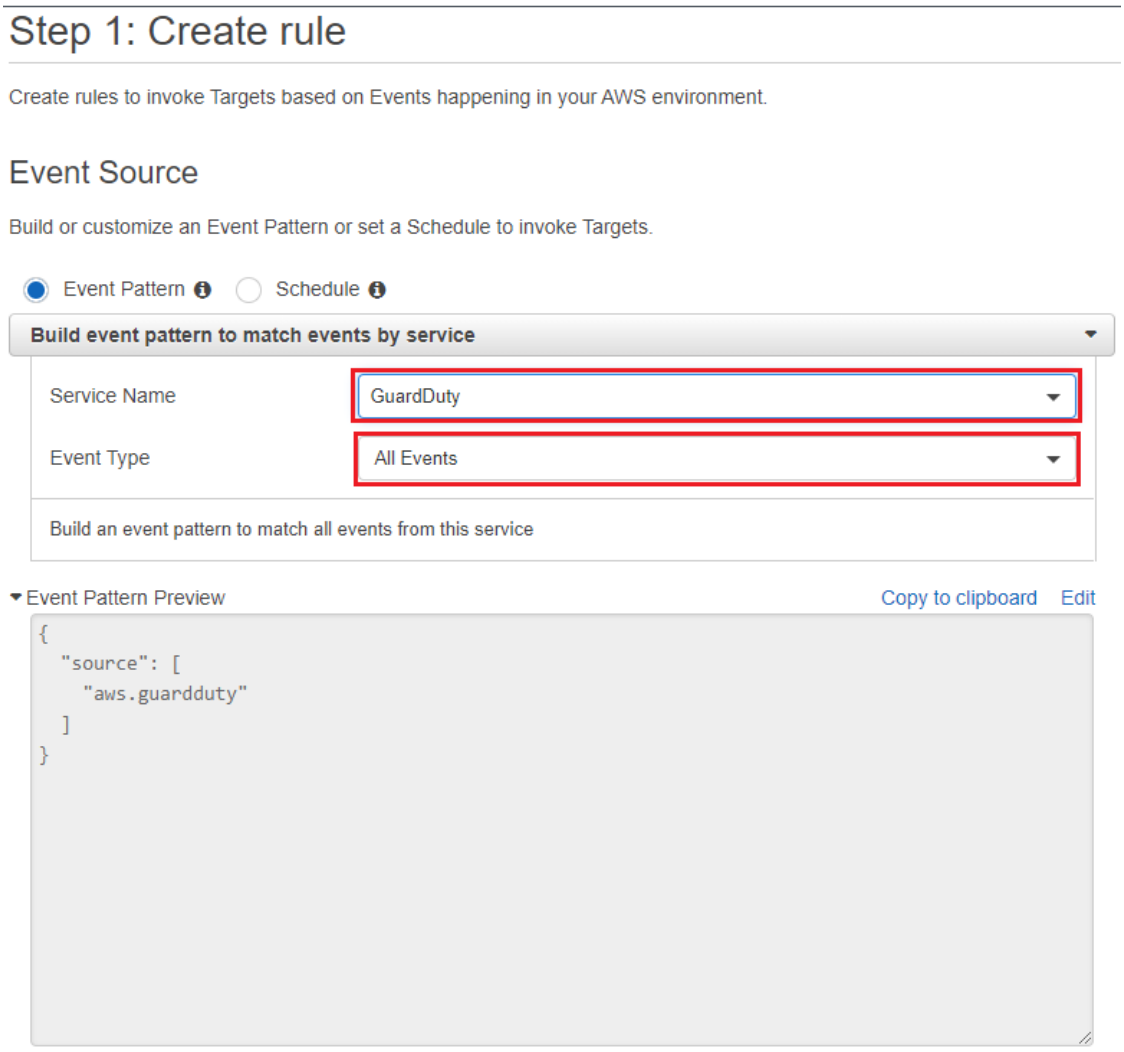

Figure 2

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

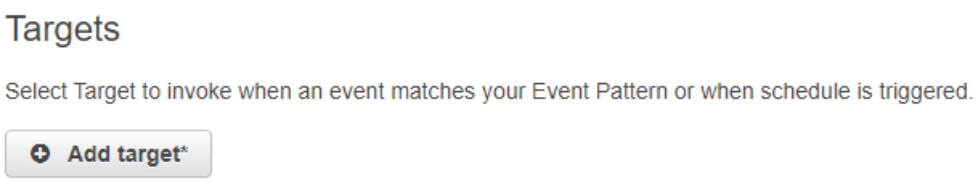

Figure 3

Keep the remaining section as default.

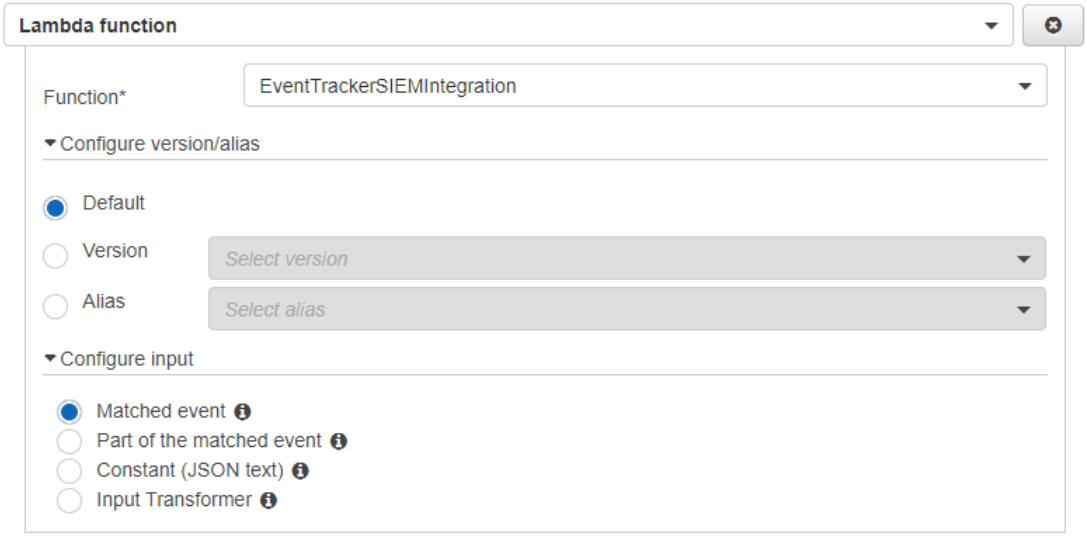

Figure 4

5. Click **Configure details.**

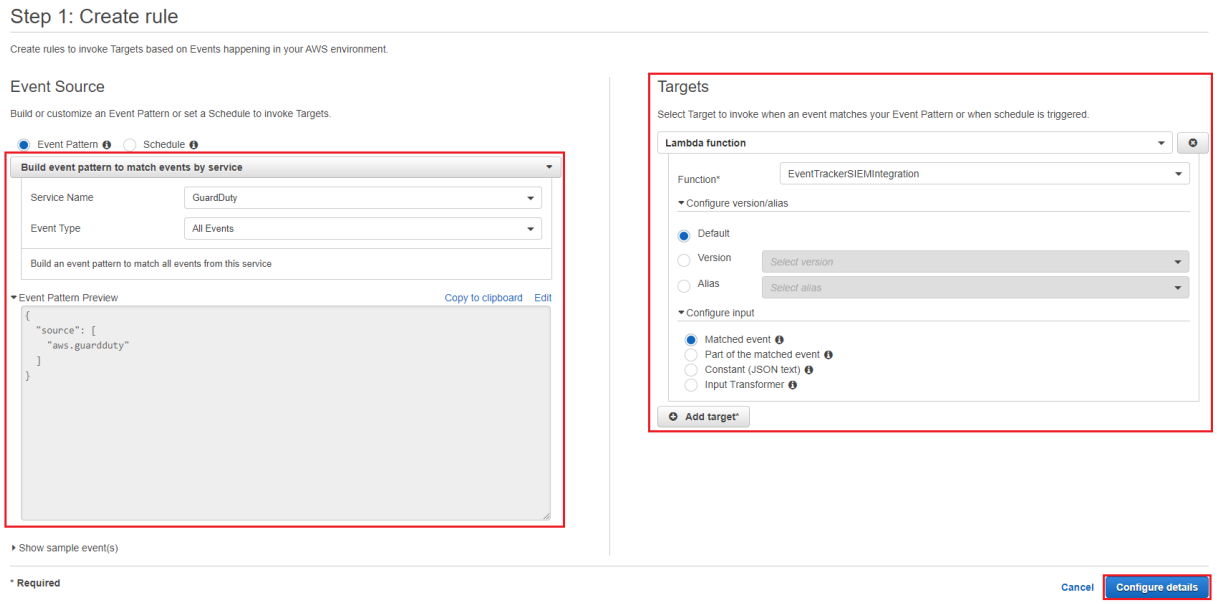

Figure 5

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.

Figure 6

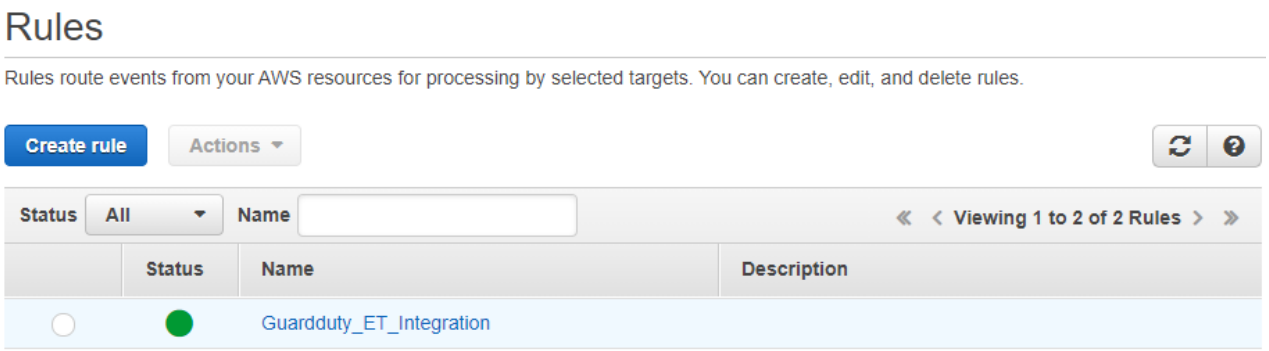

Figure 7

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

	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-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 01:59:50 AM	Unusual outbound communication seen from EC2 instance i-99999999 on server port 80.	Behavior:EC2/NetworkPortUnusual	828890237078	EC2 instance i-99999999 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-99999999 on server port 80.	Behavior:EC2/NetworkPortUnusual	828890237078	EC2 instance i-99999999 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:

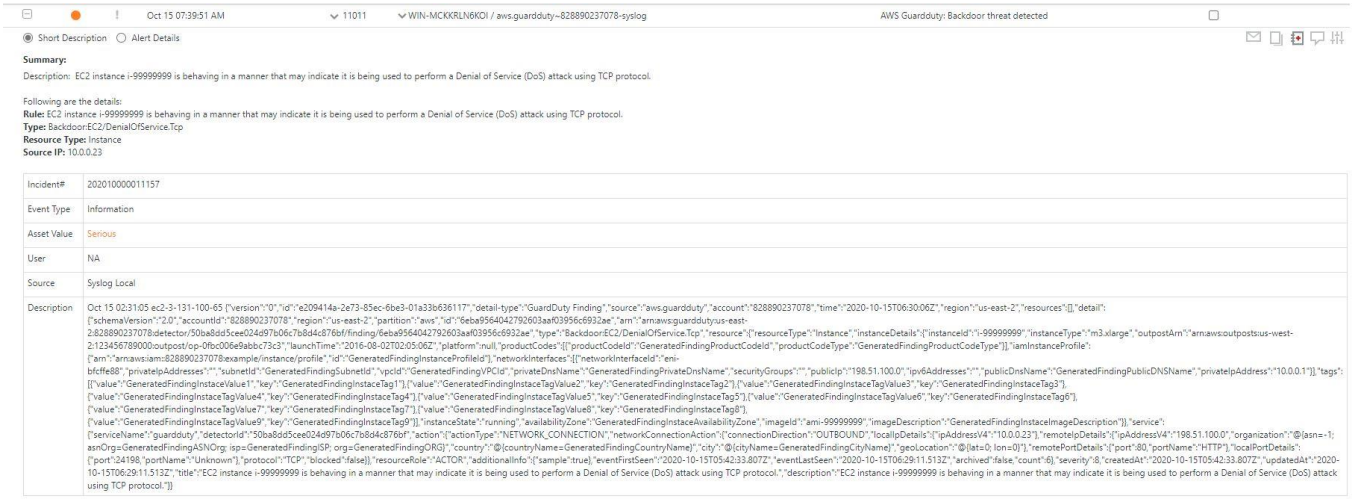

Figure 9

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	Type	Severity	Account	Remote IP	Resource Type	Resource Details	Finding Details
10/15/2020 01:38:21 AM	AWS.GUARDDUTY~828890237078	Unusual user permission reconnaissance activity by GeneratedFindingUserName.	Recon:IAMUser/UserPermissions	5	828890237078	198.51.100.0	AccessKey	"accessKeyId":"GeneratedFindingAccessKeyId","principalId":"GeneratedFindingPrincipalId","userType":"IAMUser","userName":"GeneratedFindingUserName"	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~828890237078-SYSLOG	API GeneratedFindingAPIName was invoked from a Tor exit node.	UnauthorizedAccess:S3/TorIPCaller	2	828890237078	198.51.100.0	S3Bucket	"accessKeyId":"GeneratedFindingAccessKeyId","principalId":"GeneratedFindingPrincipalId","userType":"IAMUser","userName":"GeneratedFindingUserName"	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~828890237078-SYSLOG	API GeneratedFindingAPIName was invoked from a Parrot Security Linux computer.	PenTest:IAMUser/ParrotLinux	5	828890237078	198.51.100.0	AccessKey	"accessKeyId":"GeneratedFindingAccessKeyId","principalId":"GeneratedFindingPrincipalId","userType":"IAMUser","userName":"GeneratedFindingUserName"	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.GUARDDUTY~828890237078-SYSLOG	EC2 instance i-99999999 is communicating with a Drop Point.	Trojan:EC2/DropPoint	5	828890237078	198.51.100.0	Instance	"instanceId":"i-99999999","instanceType":"m3.xlarge","outpostArn":"arn:aws:outposts:us-west-2:123456789000:outpost/op-0fbc006e9abbc73c3","launchTime":"2016-08-02T02:05:06Z","platform":null,"productCodes":[{"productCodeId":"GeneratedFindingProductCodeId","productCodeType":"GeneratedFindingProductCodeType"	EC2 instance i-99999999 is communicating with a remote host 198.51.100.0 that is known to hold credentials and other stolen data captured by malware.

Figure 10

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.

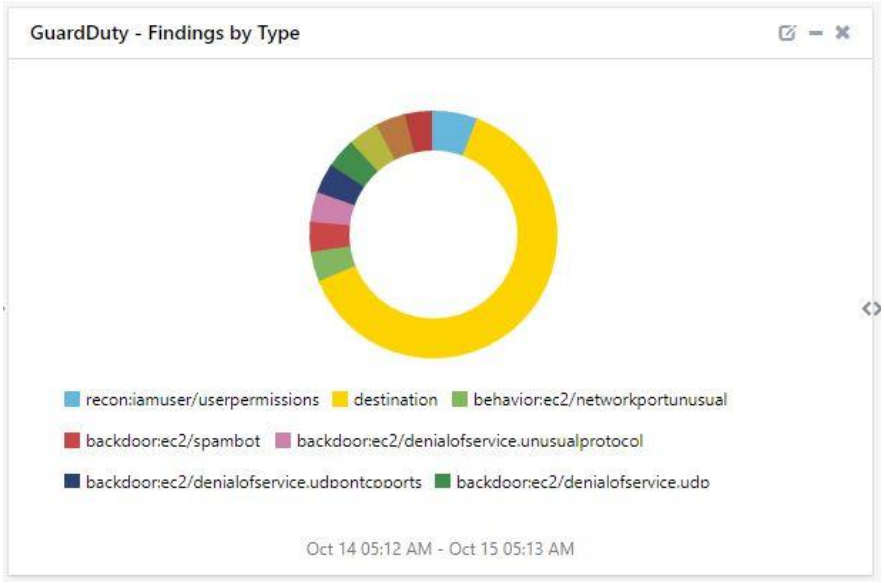

Figure 11

- **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.

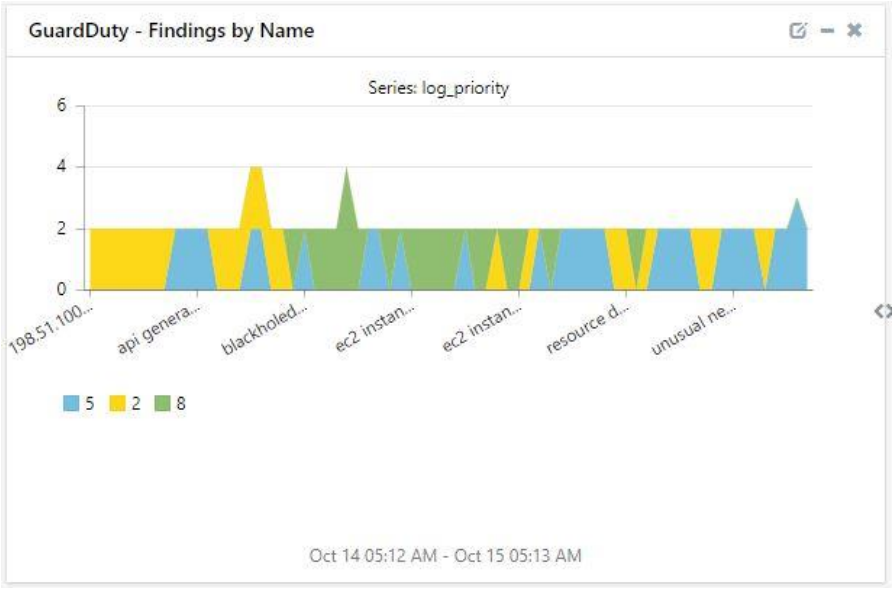

Figure 12

- **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.

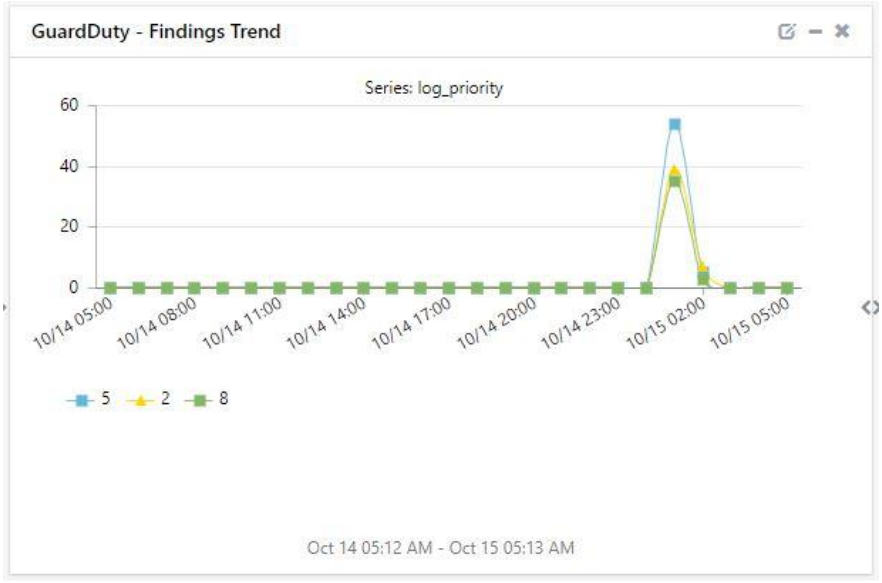

Figure 14

- **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.

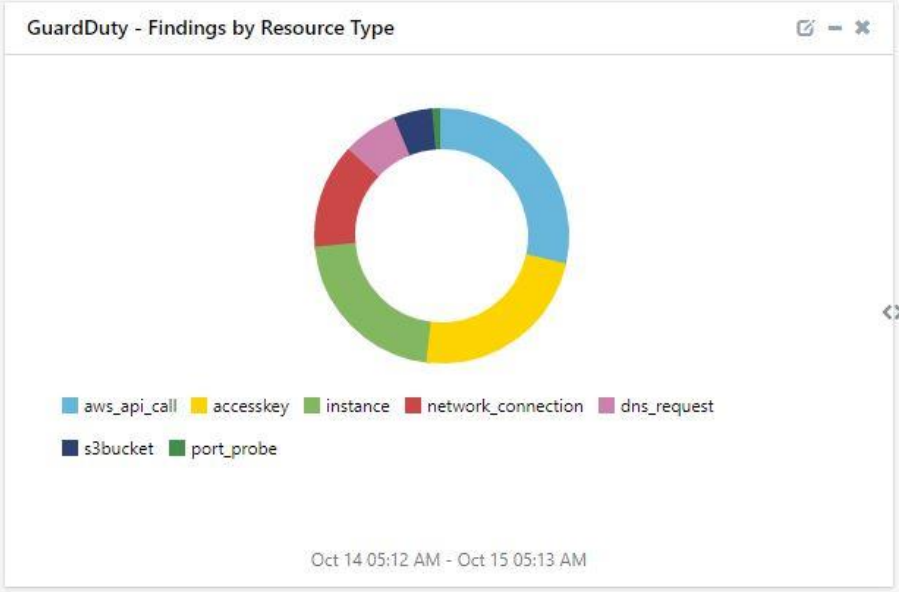

Figure 15

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 EventTracker support 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**.

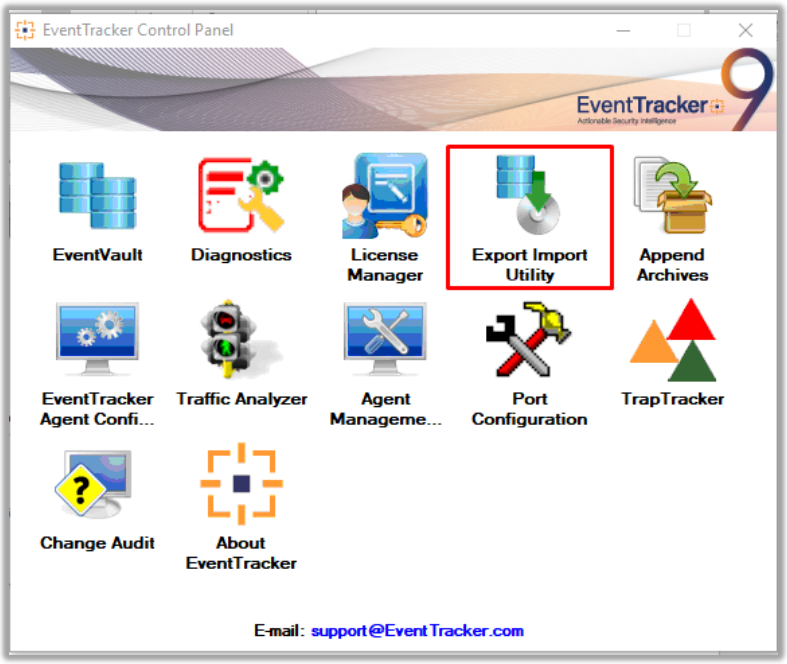

Figure 16

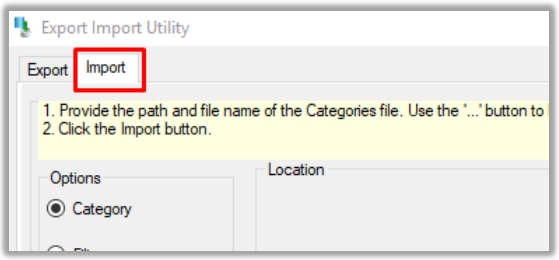

Figure 27

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**".

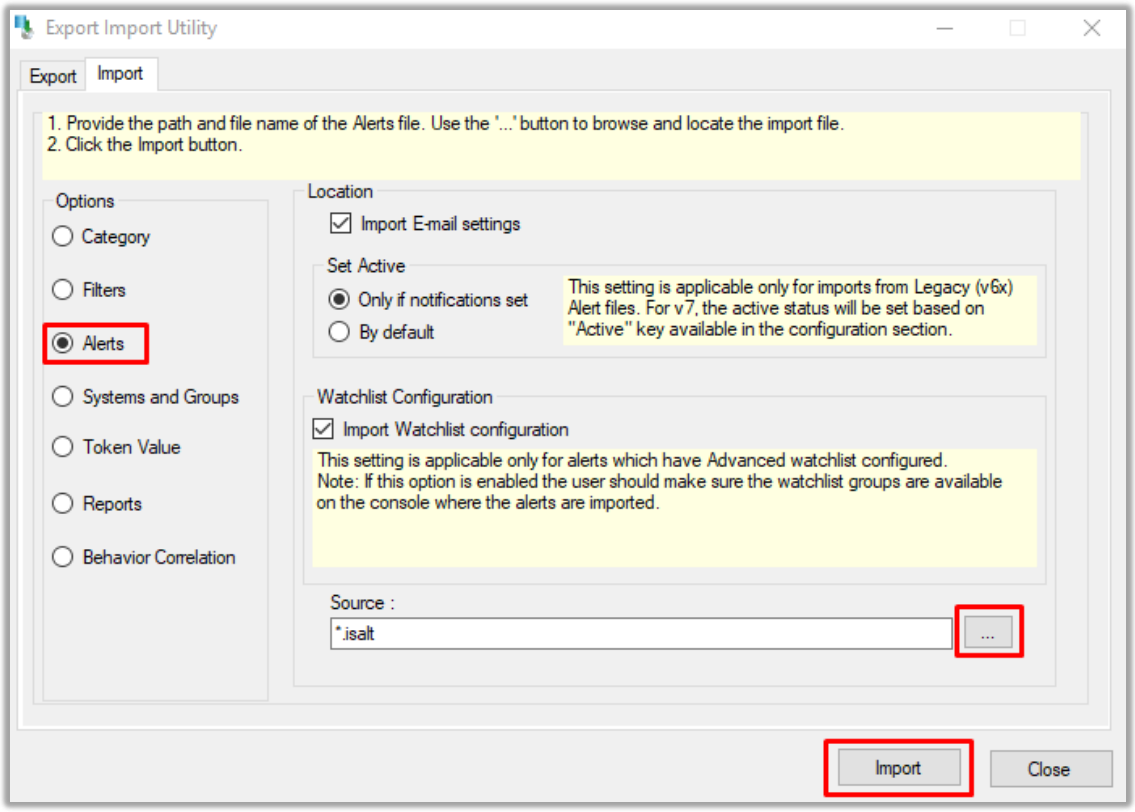

Figure 18

EventTracker displays a success message:

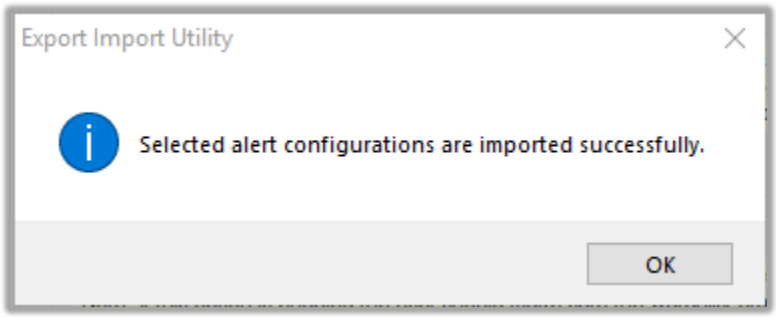

Figure 19

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.

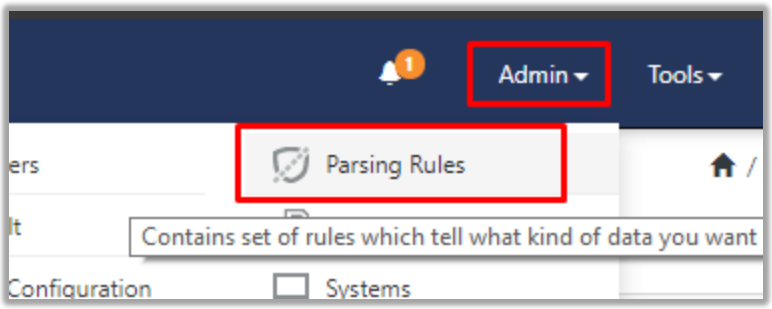

Figure 30

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

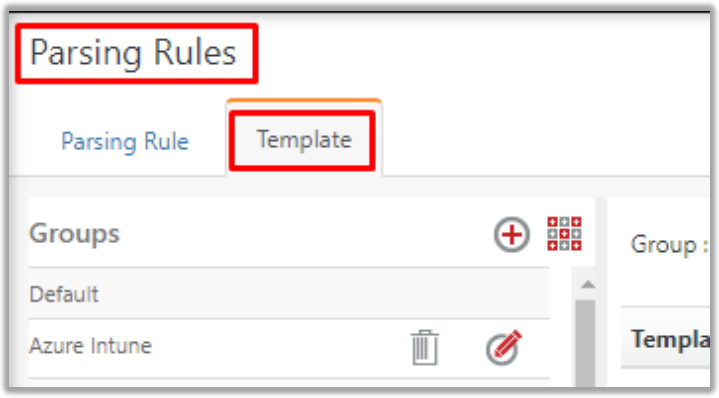

Figure 21

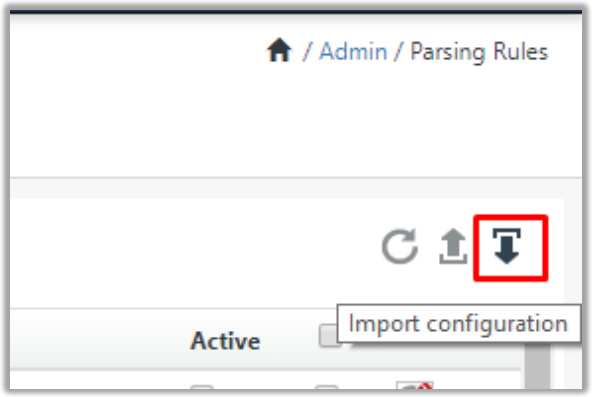

Figure 22

3. 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**".

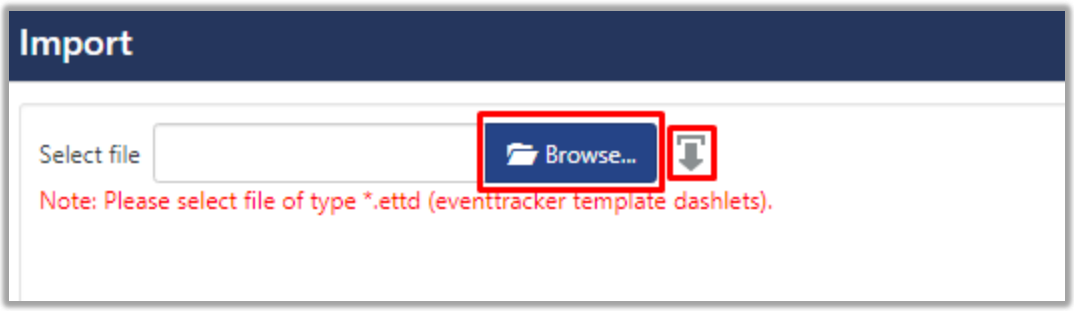

Figure 23

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)**":

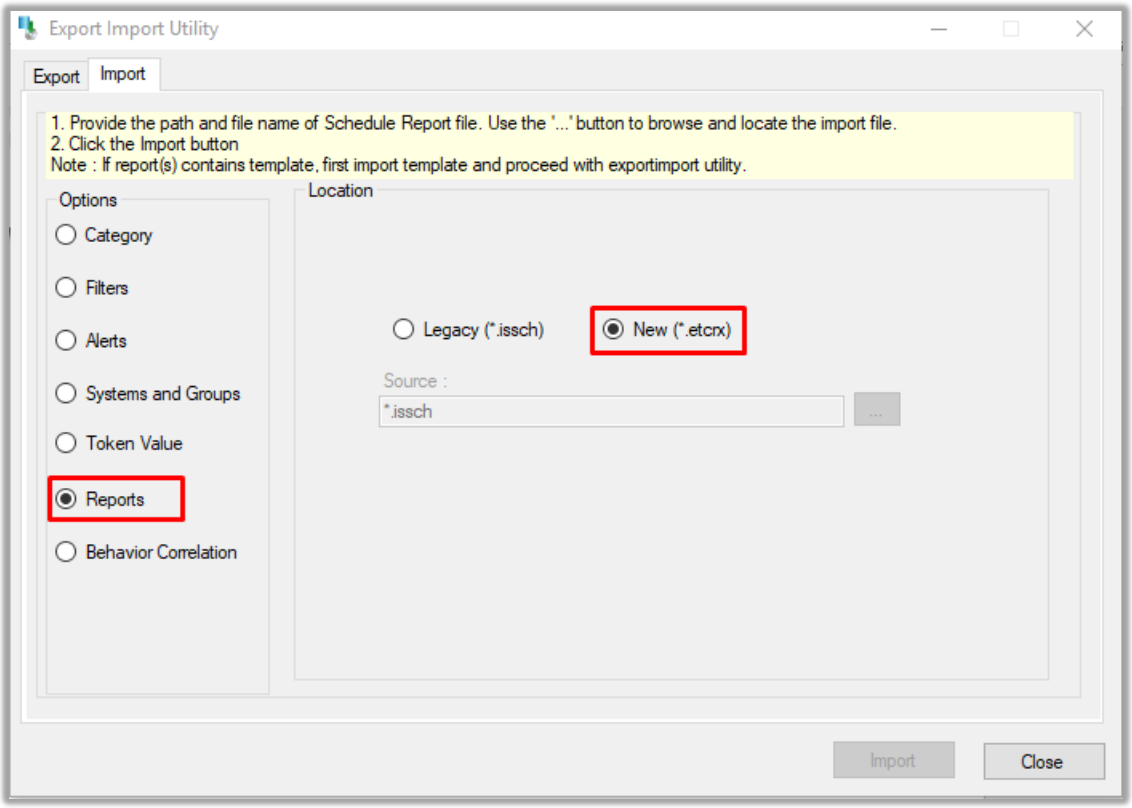

Figure 44

2. 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".**

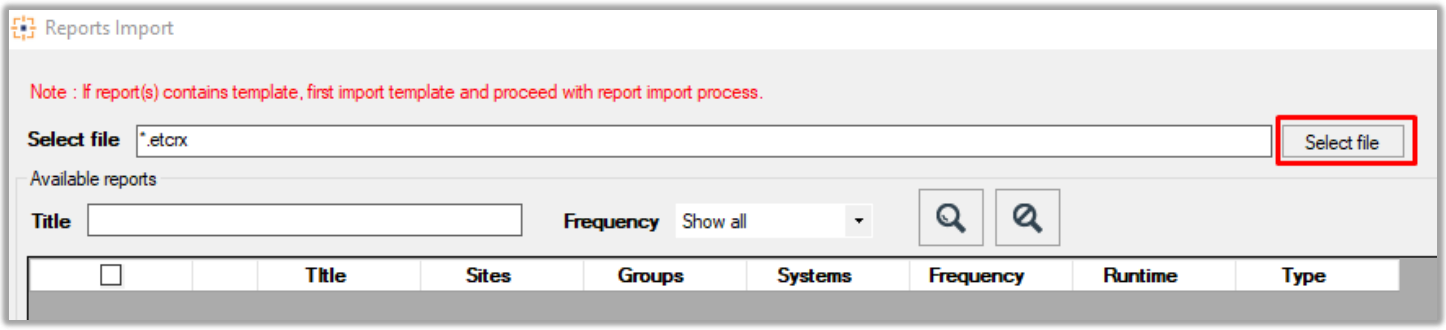

Figure 55

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

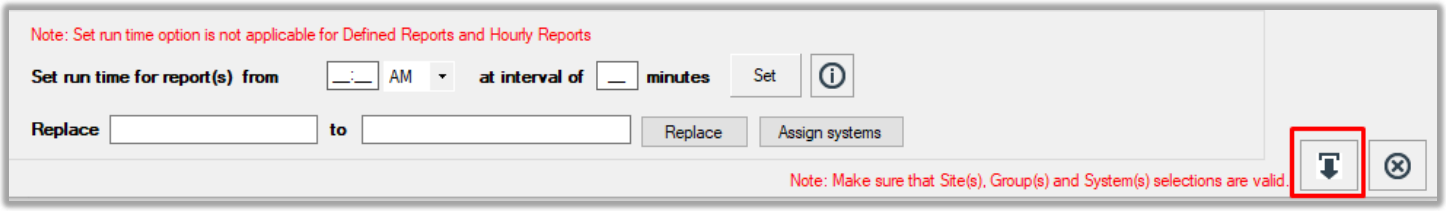

Figure 66

EventTracker displays a success message:

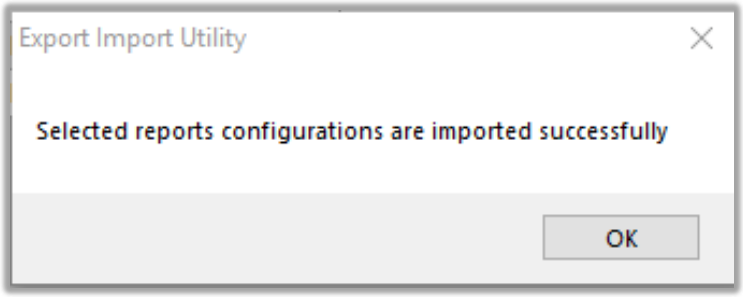

Figure 27

5.4 Knowledge Objects

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

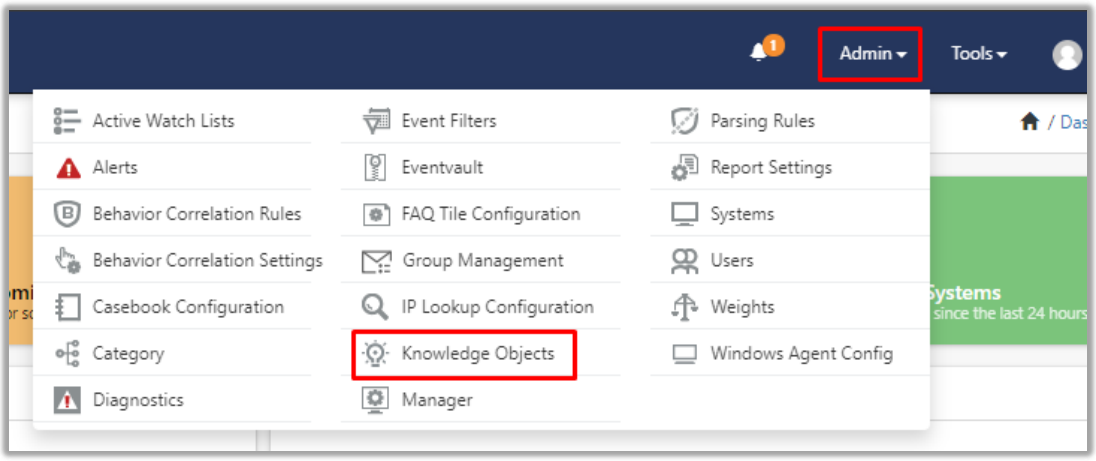

Figure 28

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

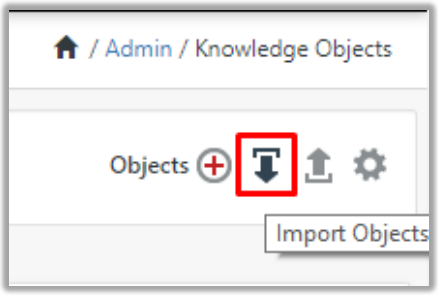

Figure 29

3. 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**".

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 → My Dashboard**.
3. In "My Dashboard", Click **Import**:

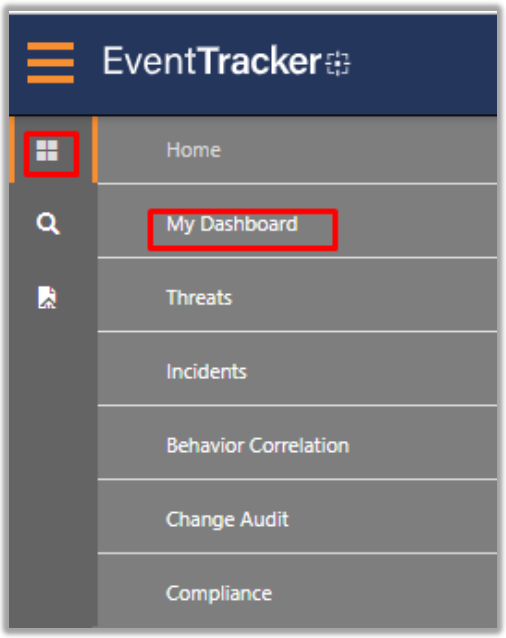

Figure 82

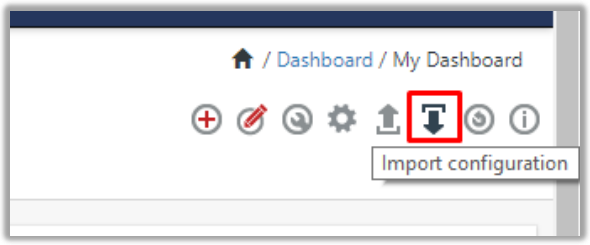

Figure 93

4. 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.

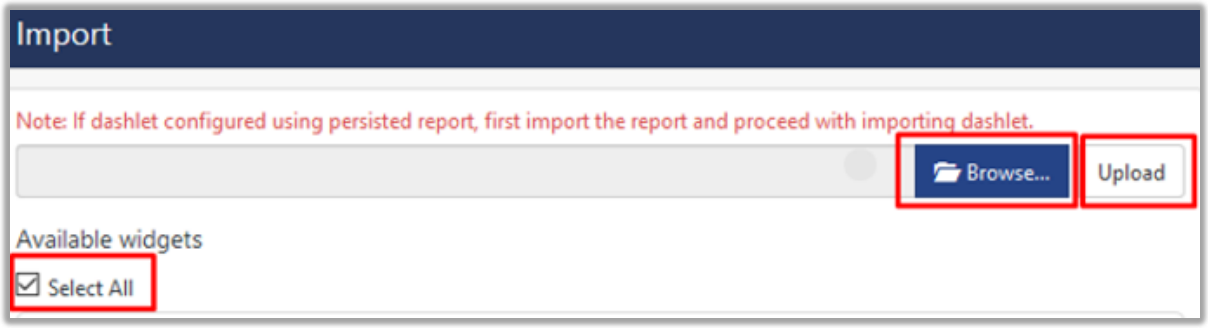

Figure 104

Figure 115

5.6 Saved Searches

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

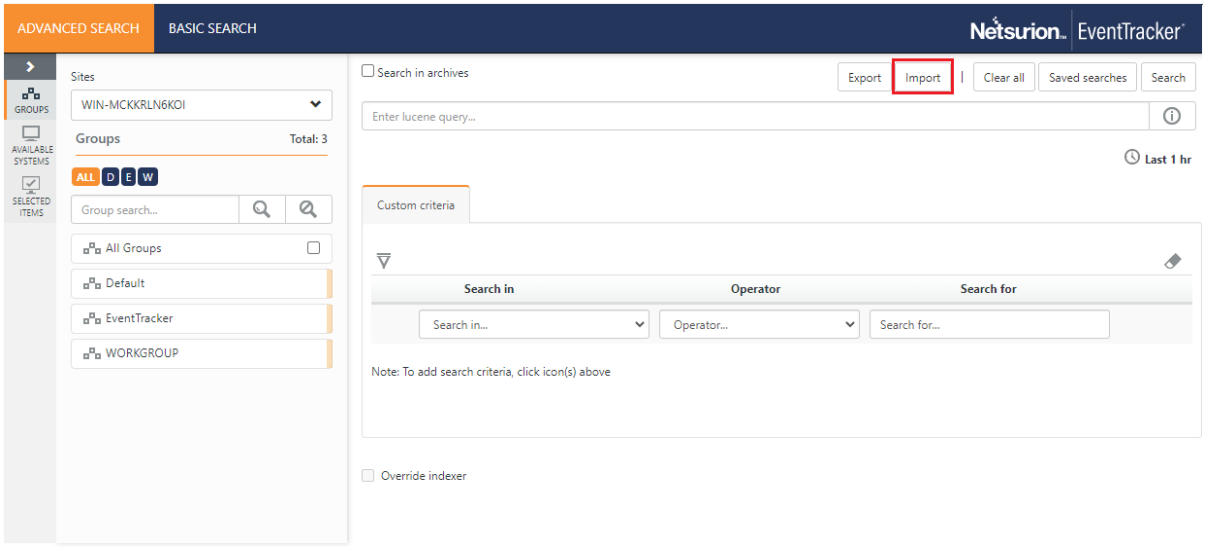

Figure 126

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.

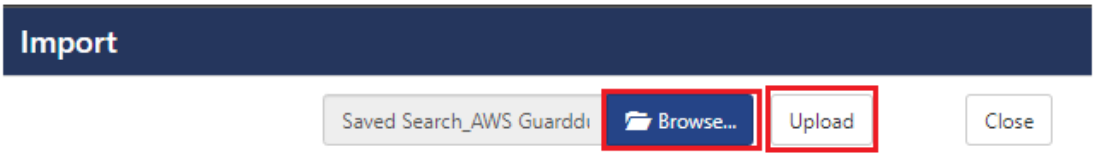

Figure 137

6. Verifying knowledge pack in EventTracker

6.1 Alerts

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

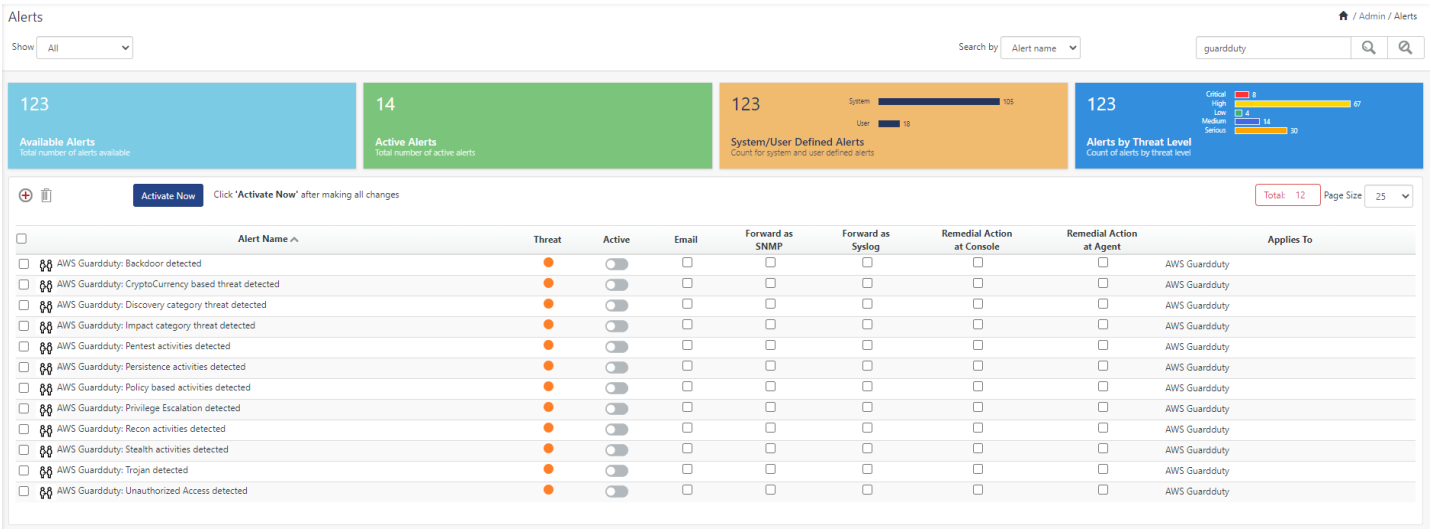

Figure 38

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.

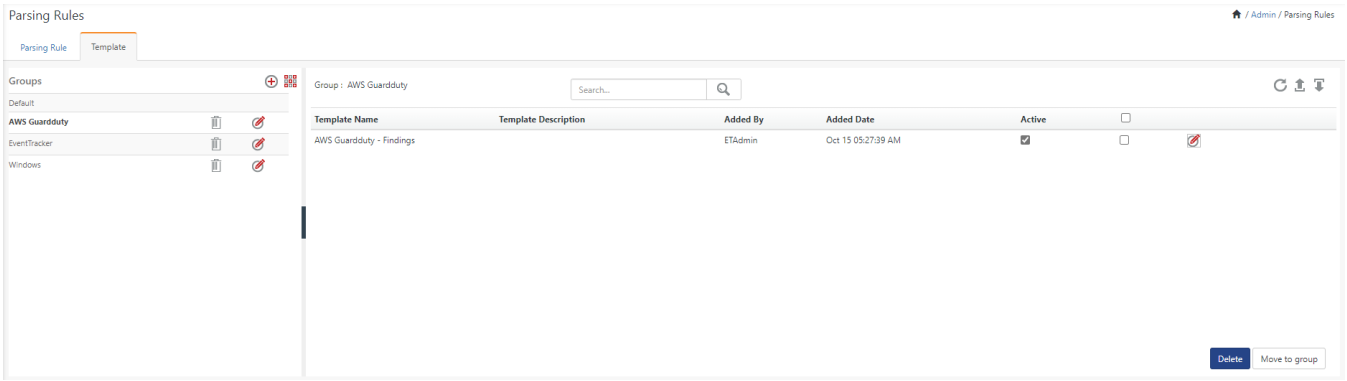

Figure 39

6.3 Flex Reports

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

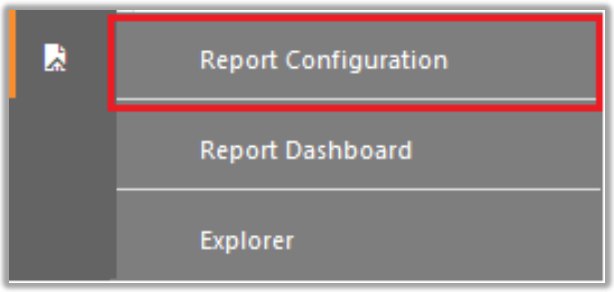

Figure 140

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

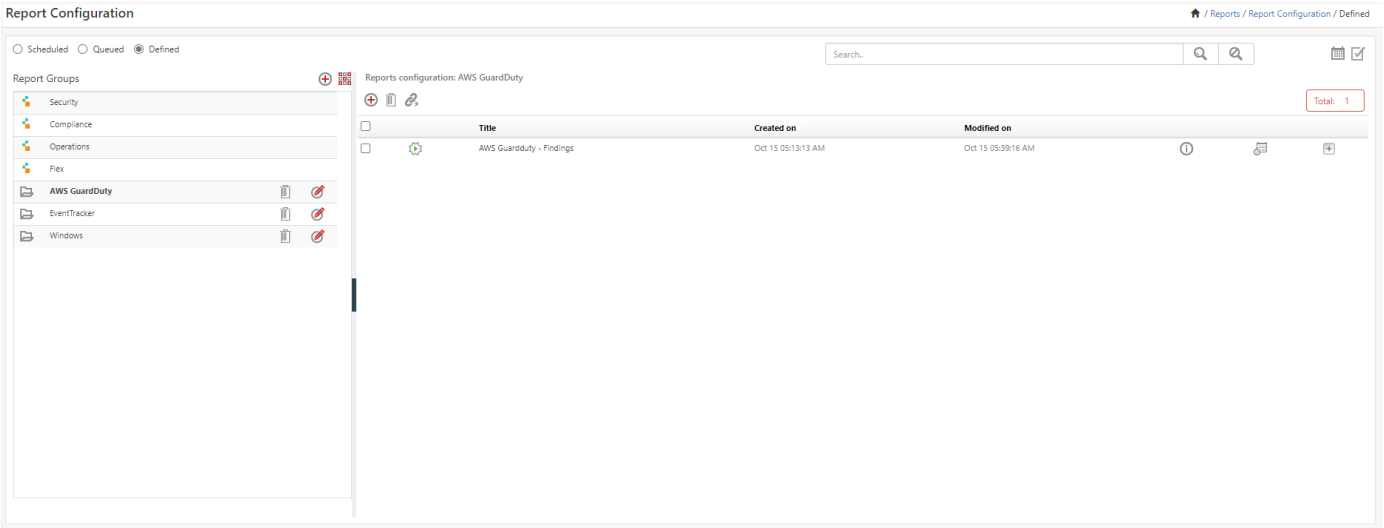

Figure 151

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.

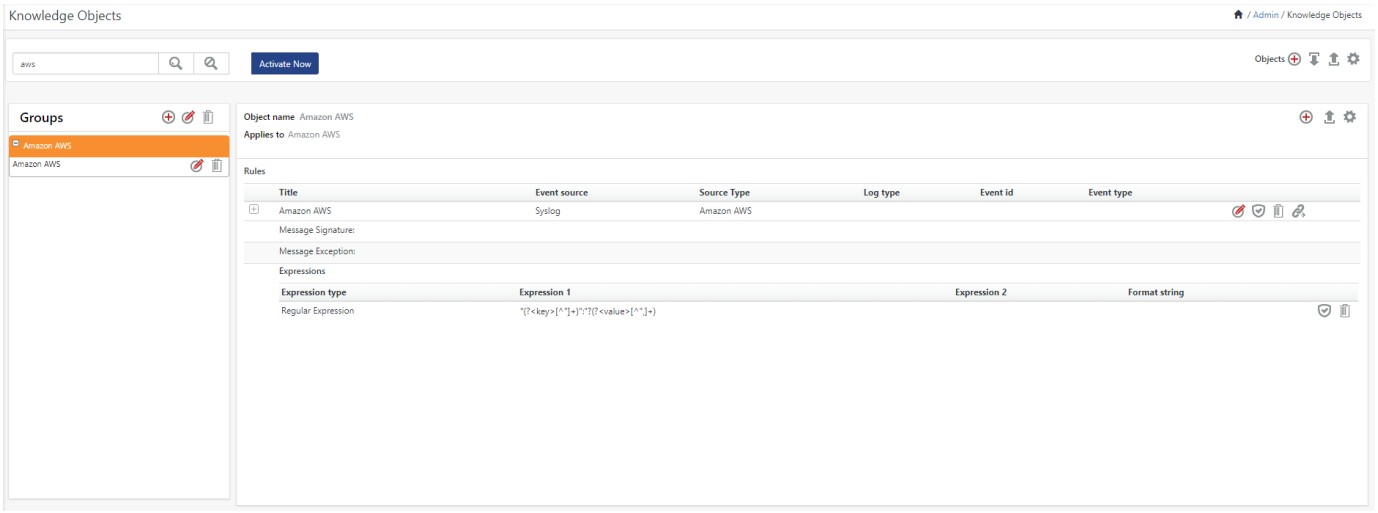

Figure 162

6.5 Dashboards

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

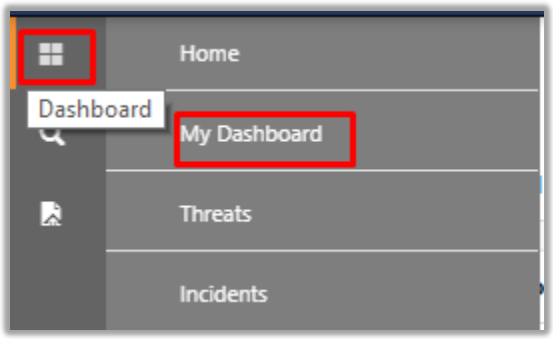

Figure 43

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

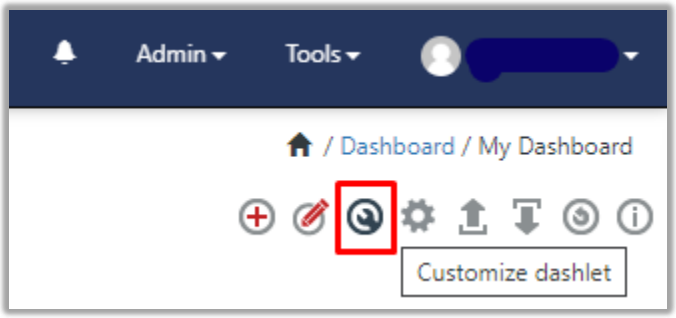

Figure 174

Figure 45

6.6 Saved Searches

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

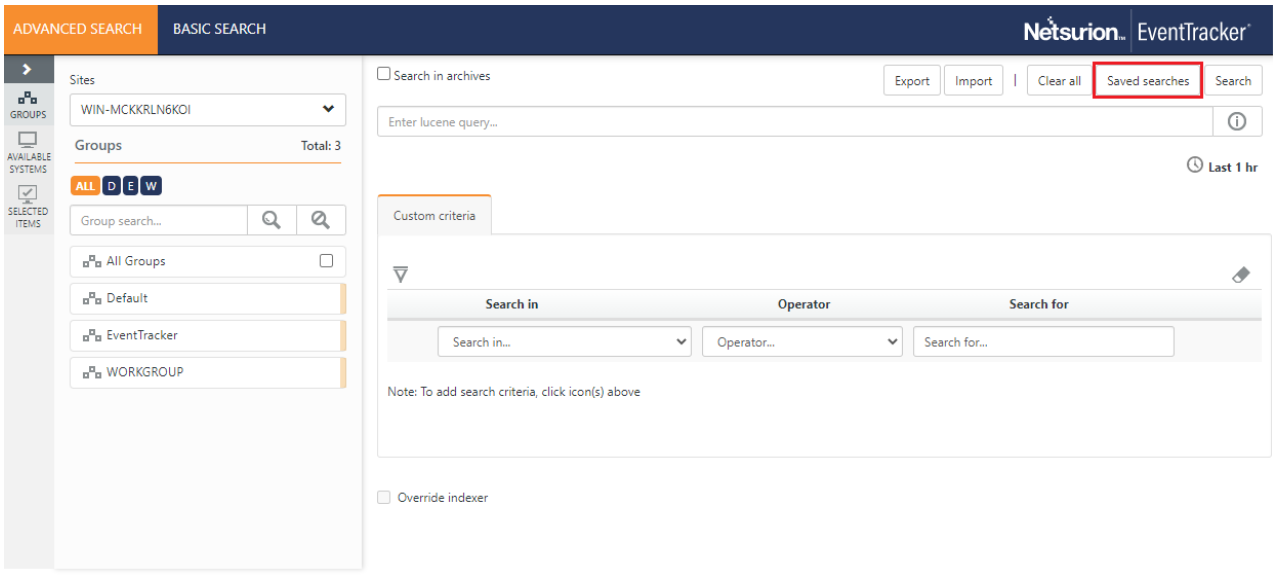

Figure 46

3. Click on **Saved Searches** and search for “GuardDuty”.

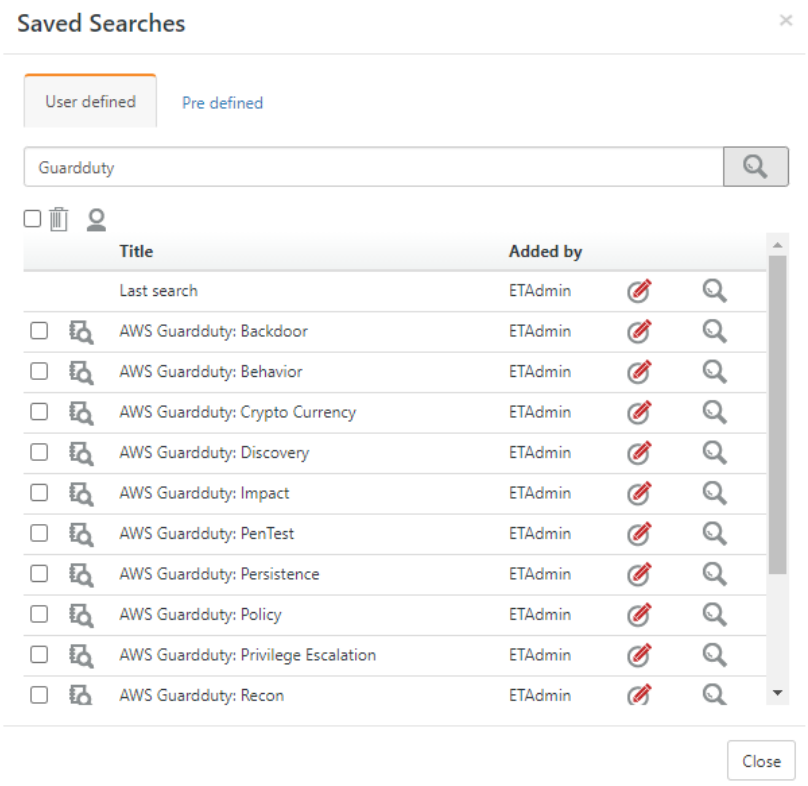
Saved Searches
User defined
Pre defined
Guardduty
Title
Added by
Last search
ETAdmin
AWS Guardduty: Backdoor
AWS Guardduty: Behavior
AWS Guardduty: Crypto Currency
AWS Guardduty: Discovery
AWS Guardduty: Impact
AWS Guardduty: PenTest
AWS Guardduty: Persistence
AWS Guardduty: Policy
AWS Guardduty: Privilege Escalation
AWS Guardduty: Recon
Close

Figure 47