

**ATTACK**  
**DEFENSE**  
by PentesterAcademy

<b>Name</b>	GuardDuty : CloudWatch Alerts
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=2479">https://attackdefense.com/challengedetails?cid=2479</a>
<b>Type</b>	AWS Cloud Security : Defense

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

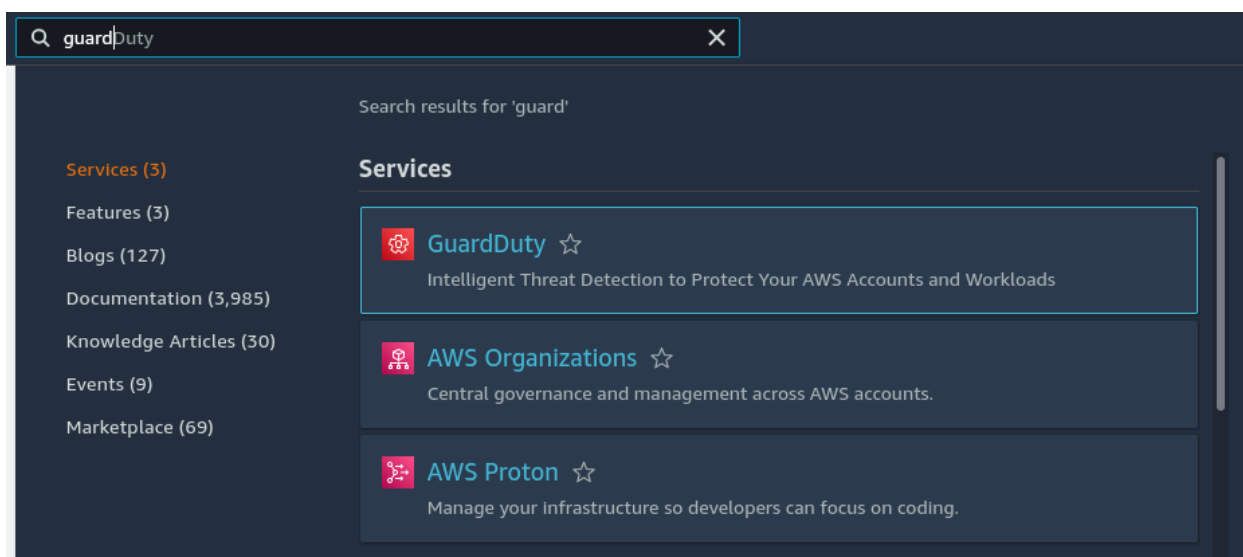
### Solution:

**Step 1:** Click the lab link button to get access credentials.

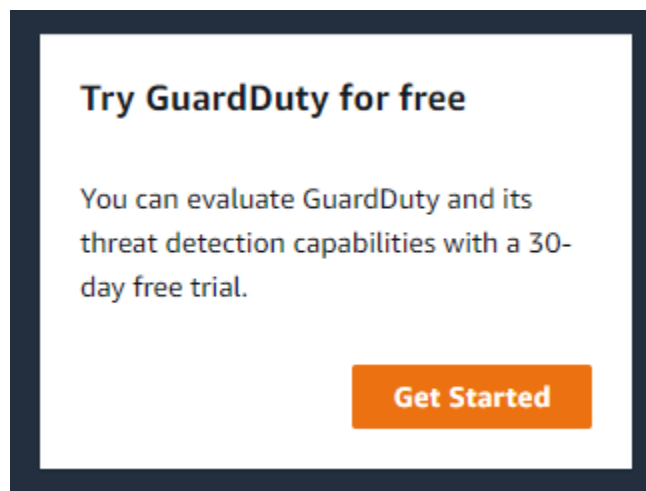
## Access Credentials to your AWS lab Account

Login URL	<a href="https://232168499015.signin.aws.amazon.com/console">https://232168499015.signin.aws.amazon.com/console</a>
Region	US East (N. Virginia) us-east-1
Username	student
Password	Ad80crvxYj4MLspo
Access Key ID	AKIATMDSSE5D72AMOB0A
Secret Access Key	yXWhf1hfC8BYjDBrJuk2N5wzmBGqgmVRB8ZwGc3N

**Step 2:** Enable GuardDuty from the console. Search for GuardDuty in the search bar and navigate to the GuardDuty dashboard.



**Step 3:** Click on Get Started.



**Step 4:** Click on Enable GuardDuty.

in a 30 day [GuardDuty free trial](#). [Learn more](#)

[Enable GuardDuty](#)

There will not be any findings at first.



Resource

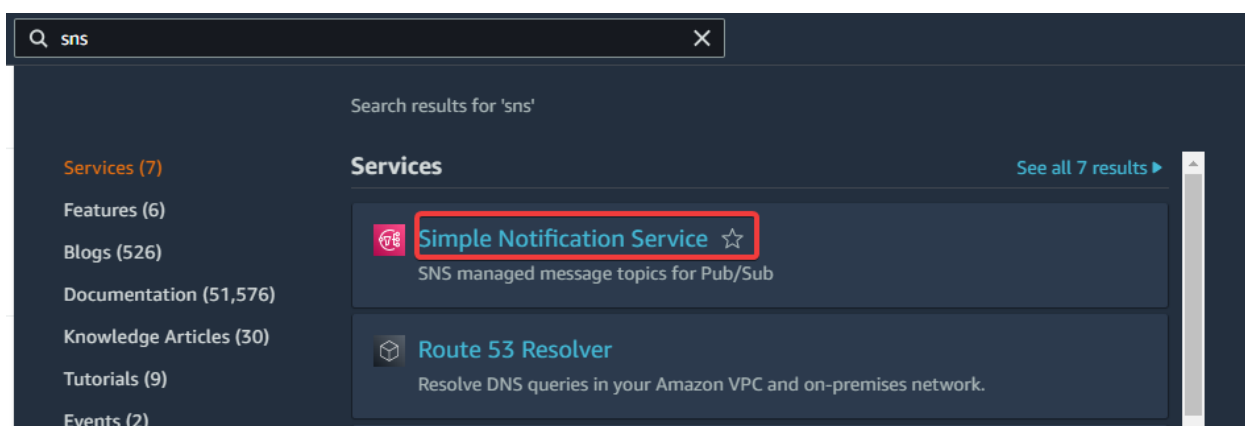


**You don't have any findings.**

GuardDuty continuously monitors your AWS environment and reports findings on this page.

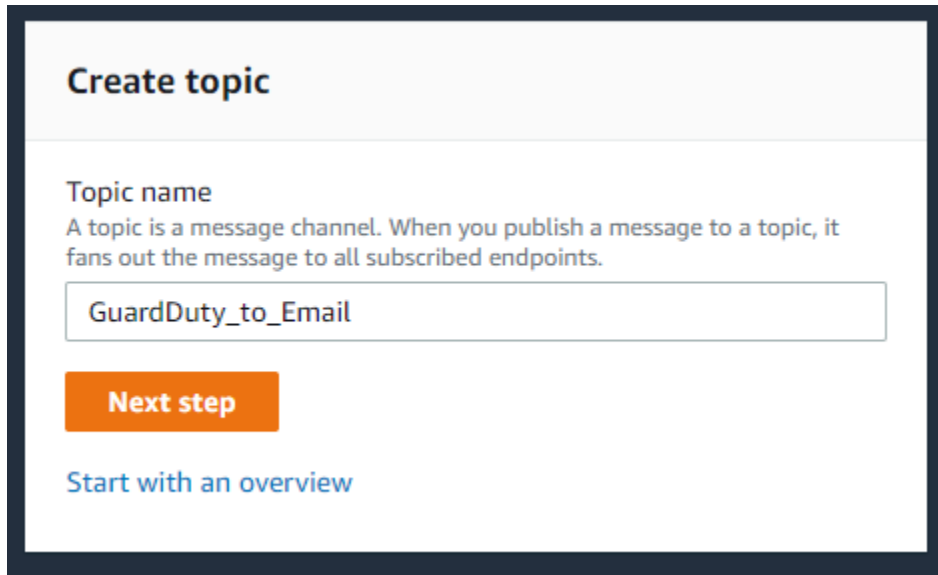
[Learn more](#)

**Step 5:** Create an SNS topic that will allow us to send notifications. Search for “SNS” in the search bar and navigate to “Simple Notification Service”.



Amazon Simple Notification Service (Amazon SNS) is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication. It enables you to send messages to users at scale via SMS, mobile push, and email.

**Step 6:** Set topic name as “GuardDuty\_to\_Email” and click on “Next step” button.



**Create topic**

**Topic name**  
A topic is a message channel. When you publish a message to a topic, it fans out the message to all subscribed endpoints.

GuardDuty\_to\_Email

**Next step**

[Start with an overview](#)

SNS topic is a logical access point that acts as a communication channel. A topic lets you group multiple endpoints.

**Step 7:** Select “Standard” as type and set name and display name as “GuardDuty\_to\_Email”.

## Details

### Type [Info](#)

Topic type cannot be modified after topic is created

☐ FIFO (first-in, first-out)

- Strictly-preserved message ordering
- Exactly-once message delivery
- High throughput, up to 300 publishes/second
- Subscription protocols: SQS

☒ Standard

- Best-effort message ordering
- At-least once message delivery
- Highest throughput in publishes/second
- Subscription protocols: SQS, Lambda, HTTP, SMS, email, mobile application endpoints

### Name

GuardDuty\_to\_Email

Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (\_).

### Display name - *optional*

To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message. [Info](#)

GuardDuty\_to\_Email

Maximum 100 characters.

Click on "Create topic".

and filter your topics and track your

Cancel Create topic

Successfully created SNS topic.

## GuardDuty\_to\_Email

### Details

Name

GuardDuty\_to\_Email

ARN

arn:aws:sns:us-east-1:232168499015:GuardDuty\_to\_Email

Type

Standard

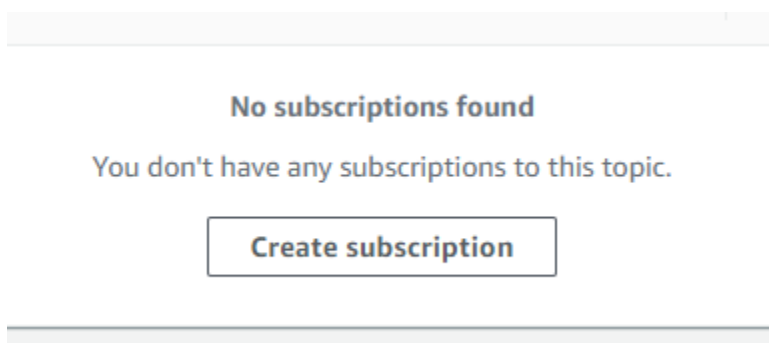
Display name

GuardDuty\_to\_Email

Topic owner

232168499015

**Step 8:** Create an SNS subscription for your topic. Click on “Create subscription”.



To receive messages published to a topic, you must subscribe to an endpoint to the topic. When you subscribe to an endpoint to a topic, the endpoint begins to receive messages published to the associated topic.

**Step 9:** Set protocol as email and provide an email to get notifications.

Amazon SNS > Subscriptions > Create subscription

## Create subscription

### Details

Topic ARN

Q am:aws:sns:us-east-1:232168499015:GuardDuty\_to\_Email

Protocol


The type of endpoint to subscribe

Email

Endpoint

An email address that can receive notifications from Amazon SNS.

besiwe6876@otodir.com

 After your subscription is created, you must confirm it. [Info](#)

Click on “Create subscription”.

Cancel

Create subscription

Successfully created subscription.

After subscribing to the endpoint, Amazon SNS will send a subscription confirmation message to the endpoint which is the provided email address.



Amazon SNS > Topics > GuardDuty\_to\_Email > Subscription: ec6effc7-060a-4b45-9e55-2144501b4771

## Subscription: ec6effc7-060a-4b45-9e55-2144501b4771

### Details

ARN

arn:aws:sns:us-east-1:232168499015:GuardDuty\_to\_Email:ec6effc7-060a-4b45-9e55-2144501b4771

Endpoint

besiwe6876@otodir.com

Topic

[GuardDuty\\_to\\_Email](#)

Status

⌚ Pending confirmation

Protocol

EMAIL

**Step 10:** Check the provided email account for subscription confirmation email. Click on “Confirm subscription” from the mail sent from the domain “sns.amazonaws.com”.



GuardDuty\_to\_Email  
no-reply@sns.amazonaws.com

Date:

30-08-2022 16:37:30

Subject: AWS Notification - Subscription Confirmation

You have chosen to subscribe to the topic:

**arn:aws:sns:us-east-1:232168499015:GuardDuty\_to\_Email**

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):

[Confirm subscription](#)

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns-opt-out](#)

This will navigate to the subscription confirmation page.



You have successfully subscribed.

```
arn:aws:sns:us-east-1:232168499015:GuardDuty_to_Email:ec6effc7-060a-4b45-9e55-2144501b4771
```

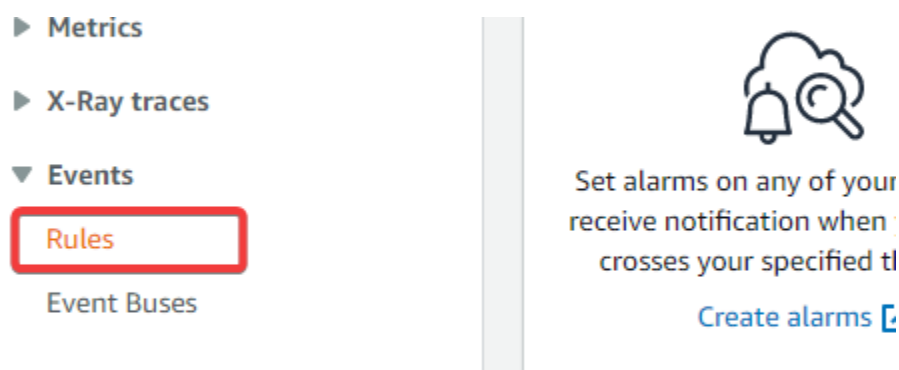
Subscription confirmed successfully.

**Step 11:** Create a CloudWatch Events rule to send events to the SNS topic. Search for “CloudWatch” in the search bar and navigate to the CloudWatch dashboard.

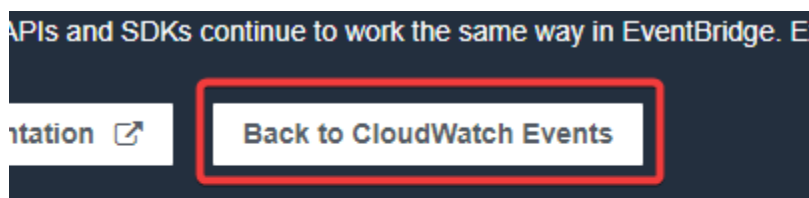


Amazon CloudWatch Events delivers a near real-time stream of system events that describe changes in AWS resources. Here we are creating custom responses to GuardDuty findings with Amazon CloudWatch Events.

**Step 12:** Click on “Rules” under events from the navigation pane.



**Step 13:** Click on “Back to CloudWatch Events” button.



**Step 14:** Click on “Create rule”.

In order to receive notifications about GuardDuty findings based on CloudWatch Events, you must create a CloudWatch Events rule and a target for GuardDuty. This rule enables CloudWatch to send notifications for findings that GuardDuty generates to the target that is specified in the rule.



Create rule    Actions ▾

Status    All ▾    Name

**Step 15:** Choose “Event pattern” and set service name as “GuardDuty” and event type as “GuardDuty Finding”.

## Event Source

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

☒ Event Pattern ⓘ    ☐ Schedule ⓘ

Build event pattern to match events by service ▾

Service Name

GuardDuty ▾

Event Type

GuardDuty Finding ▾

Click on “Edit”.

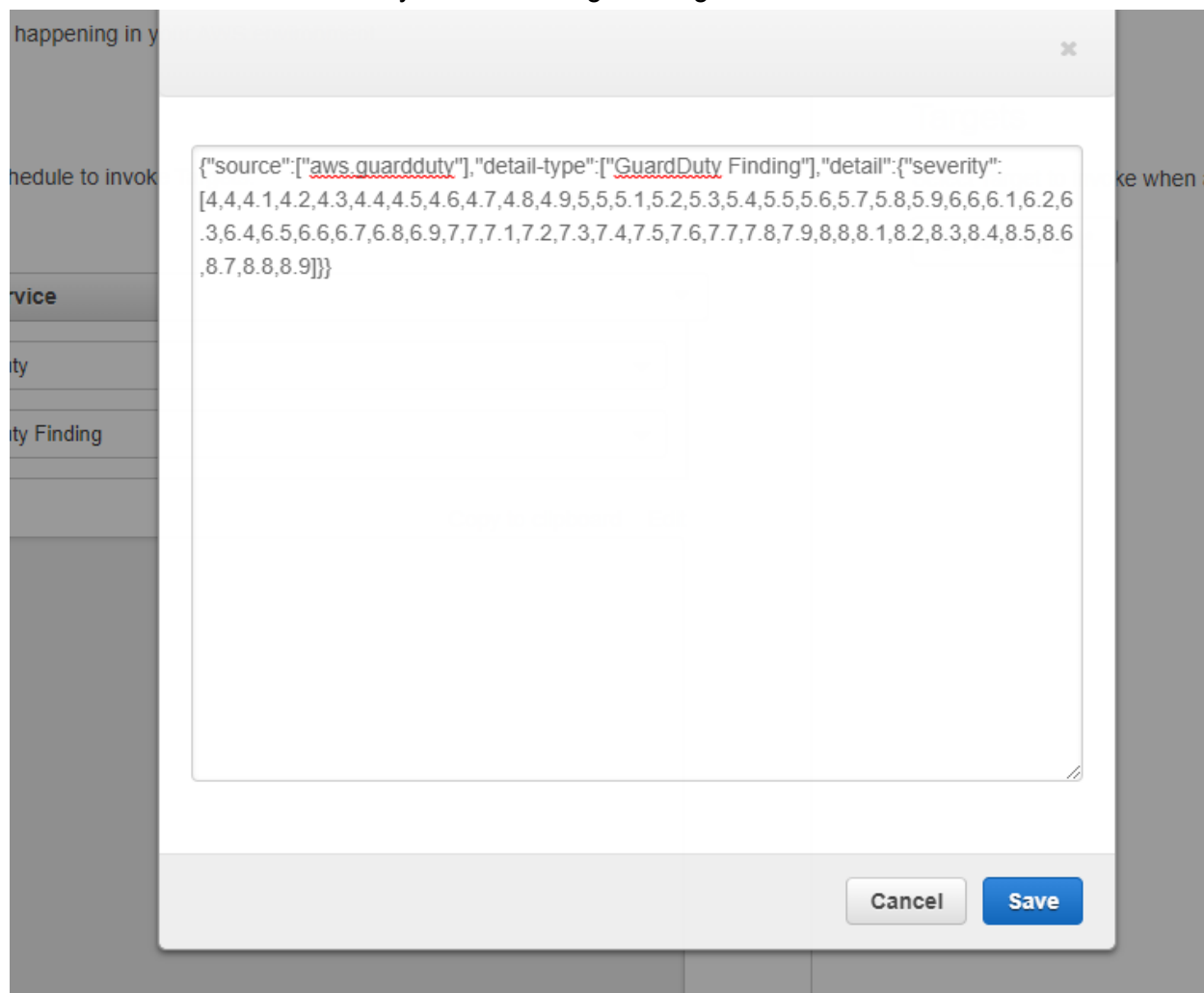
Copy to clipboard    **Edit**

**Step 16:** Copy and paste the provided JSON code and click on “Save”.

**JSON code:**

```
{"source":["aws.guardduty"],"detail-type":["GuardDuty Finding"],"detail":{"severity":["4,4,4.1,4.2,4.3,4.4,4.5,4.6,4.7,4.8,4.9,5,5.1,5.2,5.3,5.4,5.5,5.6,5.7,5.8,5.9,6,6.1,6.2,6.3,6.4,6.5,6.6,6.7,6.8,6.9,7,7.1,7.2,7.3,7.4,7.5,7.6,7.7,7.8,7.9,8,8.1,8.2,8.3,8.4,8.5,8.6,8.7,8.8,8.9"]}}
```


The above code will alert for any Medium to High finding.



**Step 17:** Click on “Add target”.

## Targets

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

 **Add target\***

**Step 18:** Select “SNS topic” and choose topic “GuardDuty\_to\_Email” .Expand Configure input and then choose Input Transformer. Set Input Path and Input Template as the following and click on “Configure details”.

**Input Path:**

```
{
  "severity": "$.detail.severity",
  "Account_ID": "$.detail.accountId",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

**Input Template:**

"AWS <Account\_ID> has a severity <severity> GuardDuty finding type <Finding\_Type> in the <region> region."  
"Finding Description:"  
"<Finding\_description> . "  
"For more details open the GuardDuty console at  
[https://console.aws.amazon.com/guardduty/home?region=<region>#/findings?search=id=<Finding\\_ID>](https://console.aws.amazon.com/guardduty/home?region=<region>#/findings?search=id=<Finding_ID>)"

## Targets

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

SNS topic

GuardDuty\_to\_Email

▼ Configure Input

☐ Matched event ⓘ

☐ Part of the matched event ⓘ

☐ Constant (JSON text) ⓘ

☒ Input Transformer ⓘ

```
{
  "severity": "$.detail.severity",
  "Account_ID": "$.detail.accountId",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type <Finding_Type> in the <region>
region."
"Finding Description: "
"<Finding_description>."
"For more details open the GuardDuty console at https://console.aws.amazon.com/guardduty/home?
region=<region>#/findings?search=id=<Finding_ID>"
```

⊕ Add target\*

Cancel

Configure details

**Step 19:** Now set the rule name as “guardduty\_role” and description as “GuardDuty Rule” and make the state “Enabled”.



Name\* guardduty\_rule

Description	<u>GuardDuty</u> Rule
-------------	-----------------------

**State** ☒ Enabled

Id necessary permissions for target(s) so they can be invoked when this rule

Click on “Create rule”.

[Cancel](#) [Back](#) [Create rule](#)

Successfully created CloudWatch Events rule.

✓ Success  
Rule **guardduty\_rule** was created.

## Rules

Rules route events from your AWS resources for processing by selected targets. You can

Create rule

Actions ▾

Status

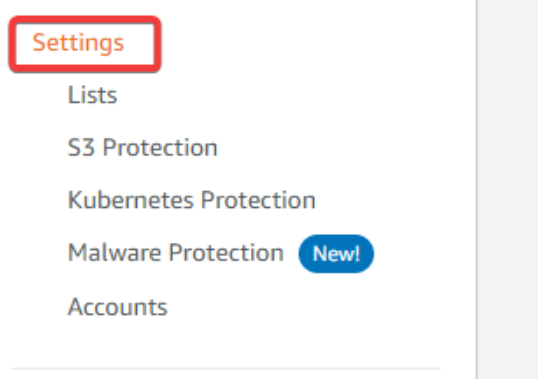
All ▾

Name

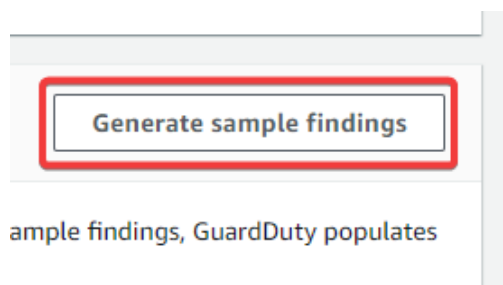
	Status	Name
<input type="radio"/>	<input checked="" type="radio"/>	guardduty_rule



**Step 20:** Navigate back to GuardDuty dashboard and create sample findings to check the notifications. Click on “Settings”.



**Step 21:** Click on the “Generate sample findings” button to generate sample findings.



Successfully created sample findings. The findings will be available in the findings dashboard and will trigger notifications.

<input type="checkbox"/>	▼	Finding type	▼	Resource	▼
<input type="checkbox"/>	▲	[SAMPLE] CryptoCurrency:EC2/BitcoinTool.B!DNS		Instance: i-999999999	
<input type="checkbox"/>	▲	[SAMPLE] UnauthorizedAccess:S3/MaliciousIPCaller.Custom		S3 Bucket: bucketName	
<input type="checkbox"/>	■	[SAMPLE] PenTest:S3/PentoolLinux		S3 Bucket: bucketName	
<input type="checkbox"/>	▲	[SAMPLE] Persistence:Kubernetes/TorIPCaller		EKSCluster: GeneratedFindingEKSClusterName	
<input type="checkbox"/>	●	[SAMPLE] UnauthorizedAccess:EC2/SSHBruteForce		Instance: i-999999999	
<input type="checkbox"/>	▲	[SAMPLE] Impact:Kubernetes/TorIPCaller		EKSCluster: GeneratedFindingEKSClusterName	
<input type="checkbox"/>	■	[SAMPLE] Recon:IAMUser/TorIPCaller		GeneratedFindingUserName: GeneratedFindingAcce	
<input type="checkbox"/>	■	[SAMPLE] Discovery:S3/TorIPCaller		S3 Bucket: bucketName	
<input type="checkbox"/>	■	[SAMPLE] PenTest:IAMUser/ParrotLinux		GeneratedFindingUserName: GeneratedFindingAcce	
<input type="checkbox"/>	▲	[SAMPLE] Exfiltration:S3/AnomalousBehavior		S3 Bucket: GeneratedFindingS3Bucket	

**Step 22:** Check the provided email account for the notification mails.

**Note:** GuardDuty sends a notification within 5 minutes of a finding.

GuardDuty_to_Email no-reply@sns.amazonaws.com	AWS Notification Message	>
GuardDuty_to_Email no-reply@sns.amazonaws.com	AWS Notification Message	>
GuardDuty_to_Email no-reply@sns.amazonaws.com	AWS Notification Message	>
GuardDuty_to_Email no-reply@sns.amazonaws.com	AWS Notification Message	>
GuardDuty_to_Email no-reply@sns.amazonaws.com	AWS Notification Message	>
GuardDuty_to_Email no-reply@sns.amazonaws.com	AWS Notification Message	>
GuardDuty_to_Email no-reply@sns.amazonaws.com	AWS Notification Message	>
GuardDuty_to_Email	AWS Notification Message	>

The email will be based on the template format that we set earlier while configuring CloudWatch Events rule.



GuardDuty\_to\_Email  
no-reply@sns.amazonaws.com

Date:

30-08-2022 17:06:11

---

Subject: AWS Notification Message

---

"AWS 232168499015 has a severity 5 GuardDuty finding type DefenseEvasion:IAMUser/AnomalousBehavior in the us-east-1 region."

"Finding Description:"

"APIs commonly used in DefenseEvasion tactics were invoked by user GeneratedFindingUserType : GeneratedFindingUserName, under anomalous circumstances. Such activity is not typically seen from this user.. "

"For more details open the GuardDuty console at <https://console.aws.amazon.com/guardduty/home?region=us-east-1#/findings?search=id=82c177430442cc84a03c613a50fe20e4>"

--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:

[https://sns.us-east-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:232168499015:GuardDuty\\_to\\_Email:ec6effc7-060a-4b45-9e55-2144501b4771&Endpoint=besiwe6876@otodir.com](https://sns.us-east-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:232168499015:GuardDuty_to_Email:ec6effc7-060a-4b45-9e55-2144501b4771&Endpoint=besiwe6876@otodir.com)

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at <https://aws.amazon.com/support>

Successfully created an SNS topic and subscription, and configured a CloudWatch Events rule that will send a message to the SNS topic depending on the results of GuardDuty.

## References:

1. Amazon GuardDuty  
([https://docs.aws.amazon.com/guardduty/latest/ug/guardduty\\_setup.html](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_setup.html))
2. GuardDuty findings with Amazon CloudWatch Events  
([https://docs.aws.amazon.com/guardduty/latest/ug/guardduty\\_findings\\_cloudwatch.html](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings_cloudwatch.html))