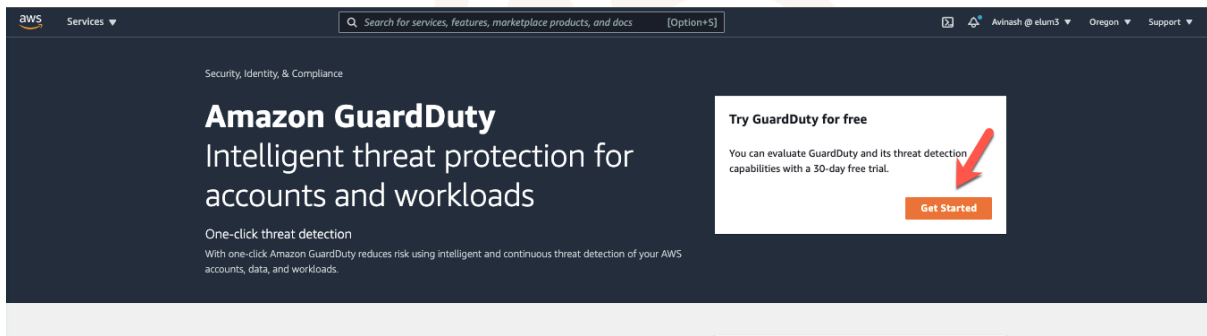# JJ Tech

AWS Guard Duty / Inspector Runbook

Protect your AWS accounts with intelligent threat detection

Enable GuardDuty

- Navigate to Amazon GuardDuty console

- If you are trying to enable GuardDuty in child accounts you can delegate this to Admin account
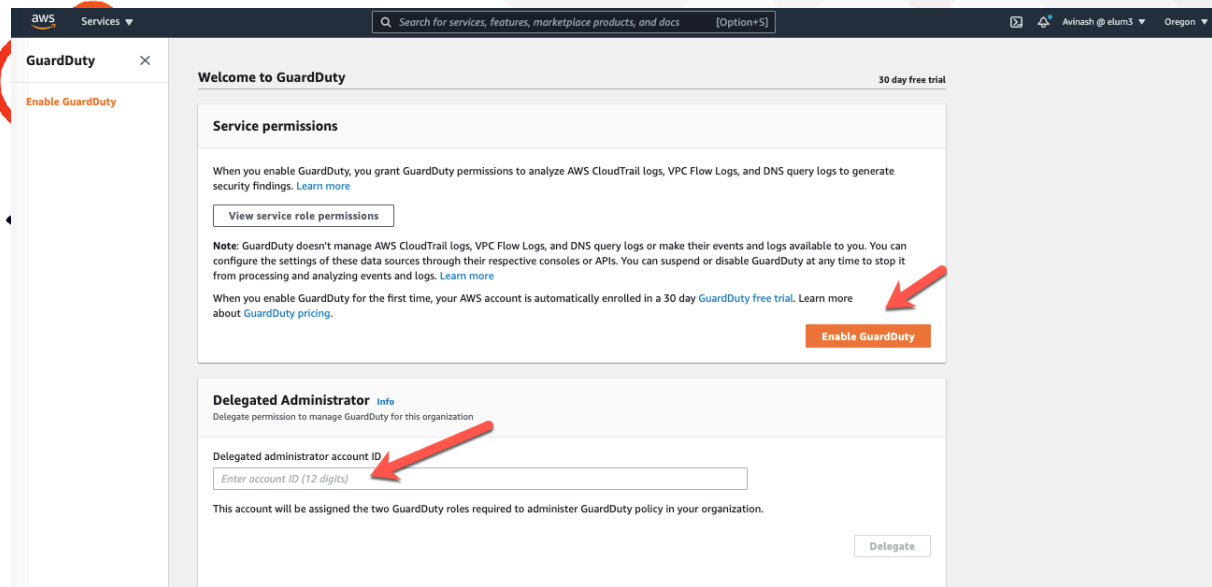- If you are doing this in an individual account , you are not required to delegate access

Demo:

Amazon GuardDuty Findings to SNS

Every GuardDuty finding is assigned a finding ID. For every finding with a unique finding ID, GuardDuty aggregates all subsequent occurrences of a particular finding that take place in six-hour intervals into a single event. GuardDuty then sends a notification about these subsequent occurrences based on this event. We can use this to push the notifications into SNS topic, and getting the security teams to investigate the findings.
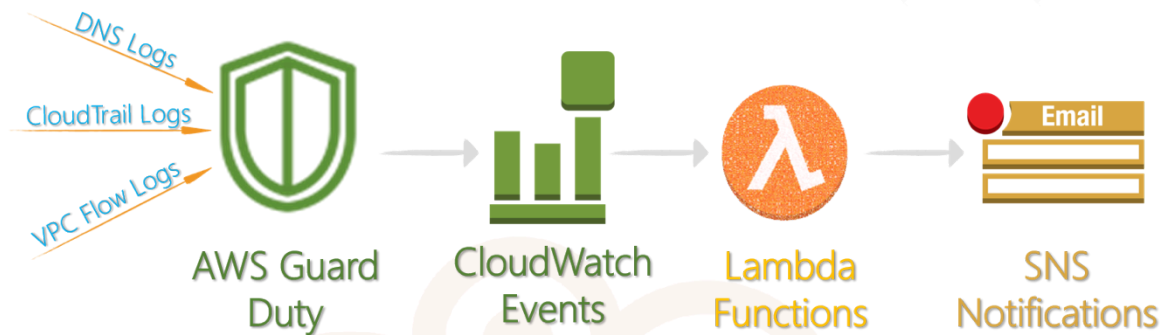
+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
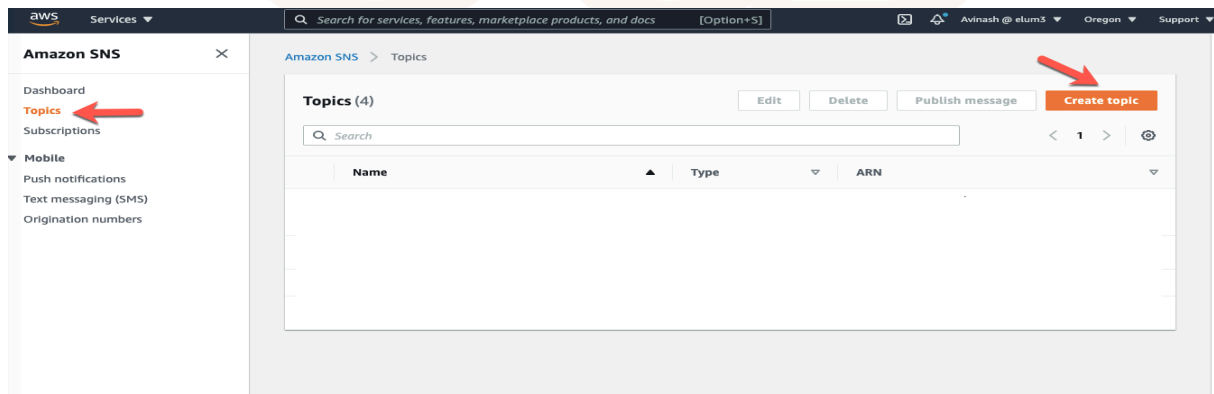14103 Hammermil Field Dr Bowie MD 20720

JJ Tech

This AWS Lambda function will help you to automatically push GuardDuty findings to an SNS topic which can be used by ITSM tools for their workflows.

Step-1

- Create a SNS Topic for Lambda to publish the GuardDuty Findings.
- Navigate to AWS SNS Console

Create topic

Details

Type Info
Topic type cannot be modified after topic is created

FIFO (first-in, first-out)	Standard
• Strictly-preserved message ordering	• Best-effort message ordering
• Exactly-once message delivery	• At-least once message delivery
• High throughput, up to 300 publishes/second	• Highest throughput in publishes/second
• Subscription protocols: SQS	• Subscription protocols: SQS, Lambda, HTTP, SMS, email, mobile application endpoints

Name

JJTech-GuarDuty-SNS

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

JJTech-GuarDuty-SNS

Maximum 100 characters, including hyphens (-) and underscores (_).

▶ **Encryption - optional**
Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic.

▶ **Access policy - optional**
This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic. Info

▶ **Delivery retry policy (HTTP/S) - optional**
The policy defines how Amazon SNS retries failed deliveries to HTTP/S endpoints. To modify the default settings, expand this section. Info

▶ **Delivery status logging - optional**
These settings configure the logging of message delivery status to CloudWatch Logs. Info

▶ **Tags - optional**
A tag is a metadata label that you can assign to an Amazon SNS topic. Each tag consists of a key and an optional value. You can use tags to search and filter your topics and track your costs. Learn more ⬈
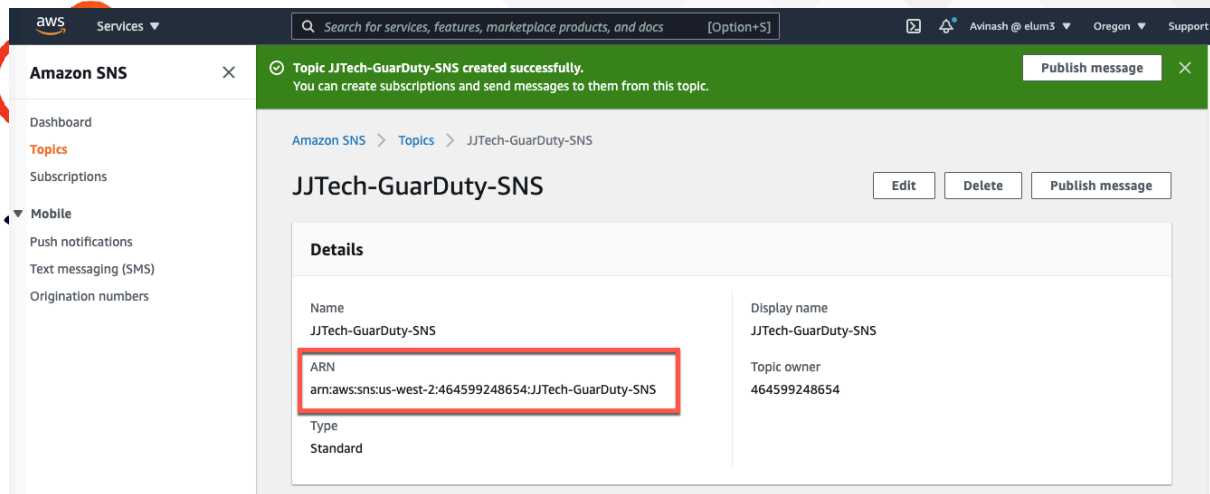
Cancel   **Create topic**
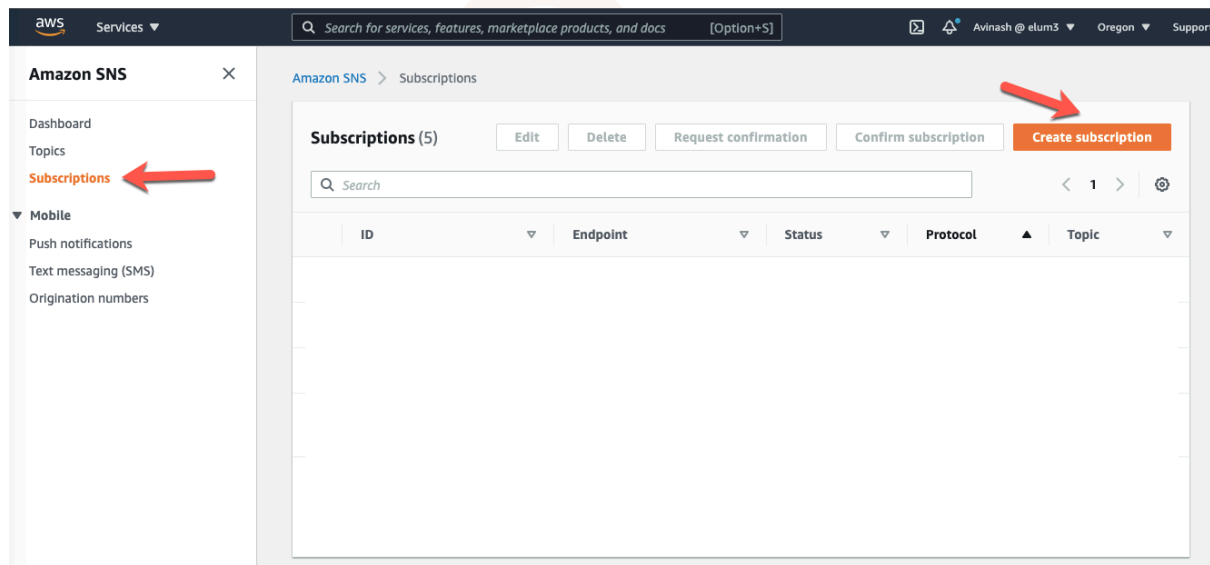
+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720

- Now you can subscribe the SNS topic with your mail id.

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720

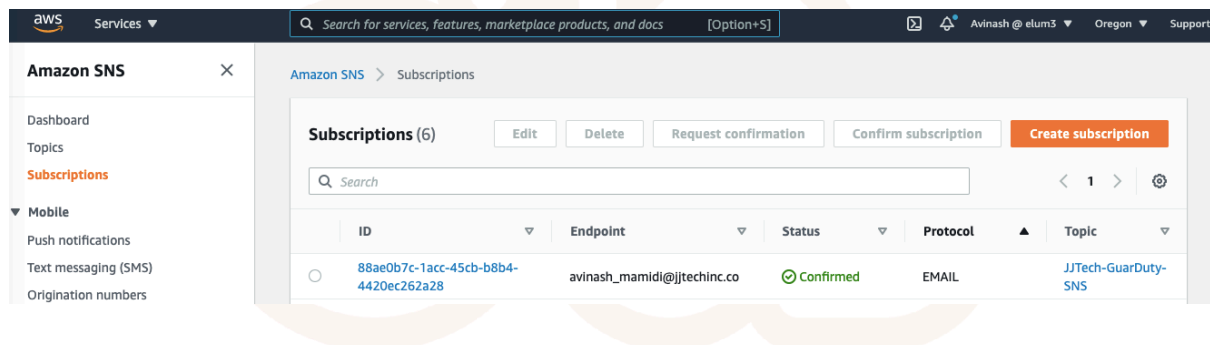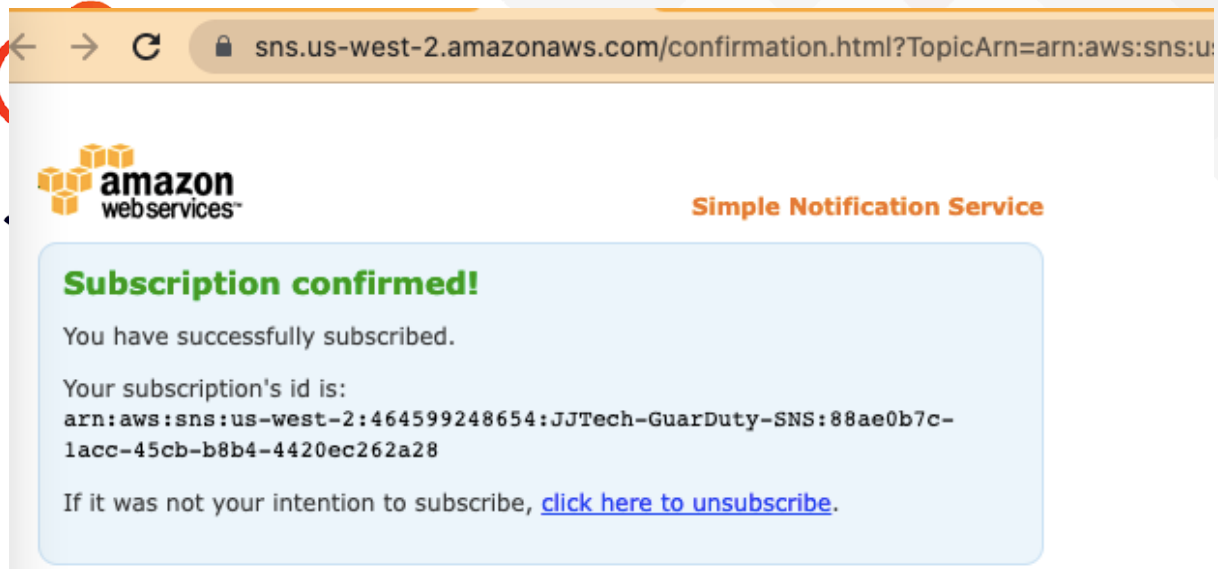- You will receive a mail to confirm the subscription to your mail
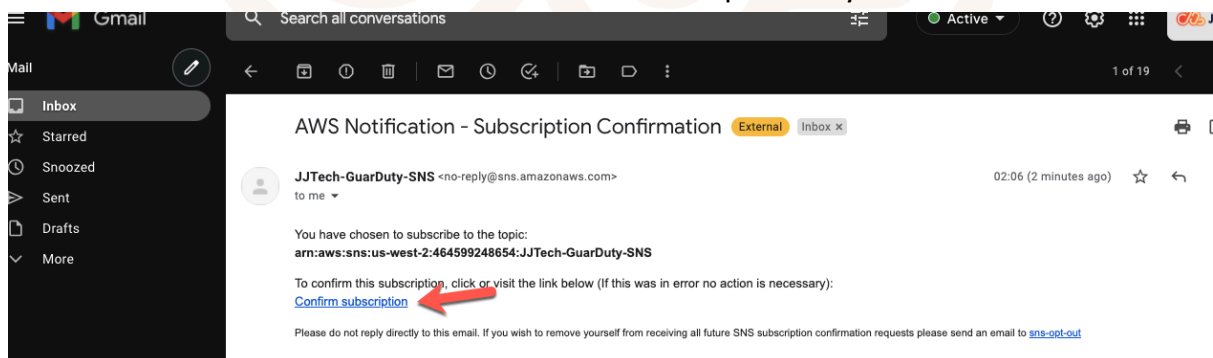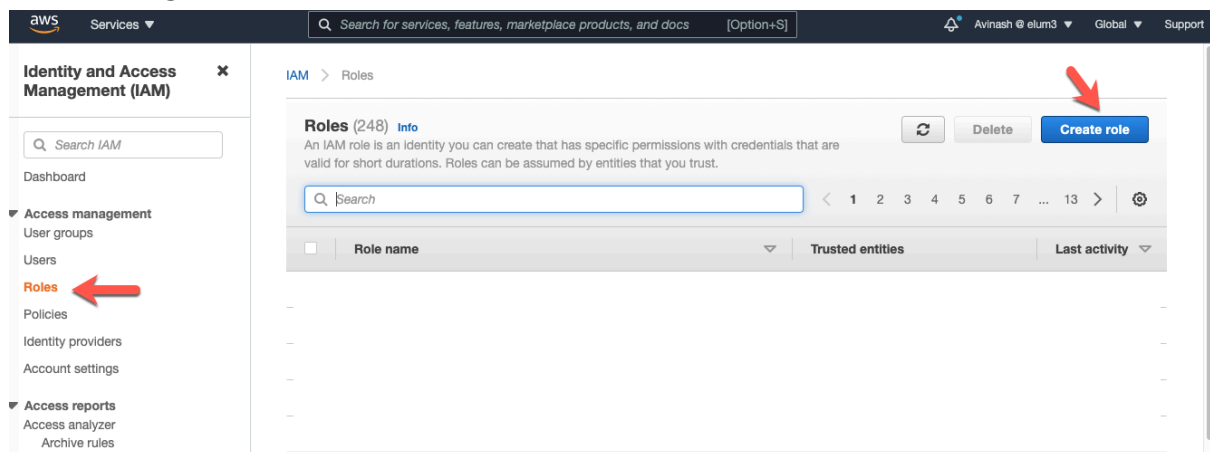
+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720

Step-2 : Create a IAM role for the Lambda function
- Navigate to IAM Console

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720

Create role

Select type of trusted entity

AWS service	Another AWS account	Web identity	SAML 2.0 federation
EC2, Lambda and others	Belonging to you or 3rd party	Cognito or any OpenID provider	Your corporate directory

Allows AWS services to perform actions on your behalf. Learn more

Choose a use case

Common use cases

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

API Gateway	CloudWatch Events	EMR	IoT SiteWise	RAM
AWS Backup	CodeBuild	EMR Containers	IoT Things Graph	RDS
AWS Chatbot	CodeDeploy	ElastiCache	KMS	Redshift
AWS Marketplace	CodeGuru	Elastic Beanstalk	Kinesis	Rekognition
AWS Support	CodeStar Notifications	Elastic Container Registry	Lake Formation	RoboMaker

* Required

Cancel   **Next: Permissions**

Create role

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Filter policies ⌄   🔍 AWSLambdaBasicExecutionRole   Showing 23 results

	Policy name ▲	Used as
☑ ▶	AWSLambdaBasicExecutionRole	Permissions policy (12)
☐ ▶	AWSLambdaBasicExecutionRole-0457599d-4b38-4305-b151-902785f8129f	Permissions policy (1)
☐ ▶	AWSLambdaBasicExecutionRole-0711a140-9353-49c2-b7c3-92f815022c2b	Permissions policy (1)
☐ ▶	AWSLambdaBasicExecutionRole-0c444622-3756-4643-9407-882745b780f6	Permissions policy (1)
☐ ▶	AWSLambdaBasicExecutionRole-22739936-14ff-4c3e-9d0b-86203c68ca4a	Permissions policy (1)
☐ ▶	AWSLambdaBasicExecutionRole-2a548e4d-30d7-411e-9dde-59eae2caf03a	Permissions policy (1)
☐ ▶	AWSLambdaBasicExecutionRole-33d56a2e-e2f6-449f-85a3-ea9995745d60	Permissions policy (1)
☐ ▶	AWSLambdaBasicExecutionRole-376732c7-5125-4ef2-a13a-acb539df12d8	Permissions policy (1)

▶ Set permissions boundary

* Required

Cancel   Previous   **Next: Tags**

Create role

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. Learn more

Key	Value (optional)	Remove
Add new key		

You can add 50 more tags.

Cancel   Previous   **Next: Review**

Create role

Review

Provide the required information below and review this role before you create it.

Role name*   JJTech-GuardDuty-Lambda-Role

Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

Role description   Allows Lambda functions to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities   AWS service: lambda.amazonaws.com

Policies   📦 AWSLambdaBasicExecutionRole ↗

Permissions boundary   Permissions boundary is not set

No tags were added.

* Required   Cancel   Previous   **Create role**

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720

- Navigate to the role you created

- Update the SNS Topic ARN which was created in Step - 1

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "sns:Publish",
            "Resource": "<ARN-OF-YOUR-SNS-TOPIC>"
        }
    ]
}
```

Create policy

Review policy

Before you create this policy, provide the required information and review this policy.

Name* SNS-topic-access

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Service ▾	Access level	Resource	Request condition
Allow (1 of 299 services) Show remaining 298			
SNS	Limited: Write	TopicName | string like | JJTech-GuarDuty-SNS	None

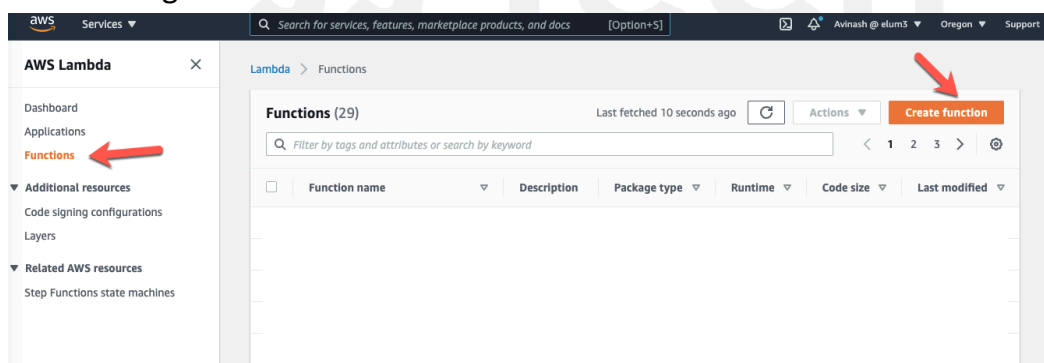* Required   Cancel   Previous   Create policy

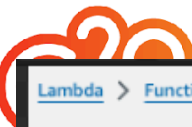## Step 3: Create Lambda Function

- Navigate to Lambda console

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720

Create function Info

Choose one of the following options to create your function.

- ● **Author from scratch**
  Start with a simple Hello World example.
- ○ **Use a blueprint**
  Build a Lambda application from sample code and configuration presets for common use cases.
- ○ **Container image**
  Select a container image to deploy for your function.

Basic information

Function name
Enter a name that describes the purpose of your function.

```
JJtech-GuardDuty-lambda
```

Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

```
Python 3.12                                          ▼
```

Architecture Info
Choose the instruction set architecture you want for your function code.

- ● x86_64
- ○ arm64

Permissions Info

By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

▼ **Change default execution role**

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the IAM console ↗.

- ○ Create a new role with basic Lambda permissions
- ● Use an existing role
- ○ Create a new role from AWS policy templates

Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.

```
lambdaGuardDuty                                      ▼
```

View the lambdaGuardDuty role ↗ on the IAM console.

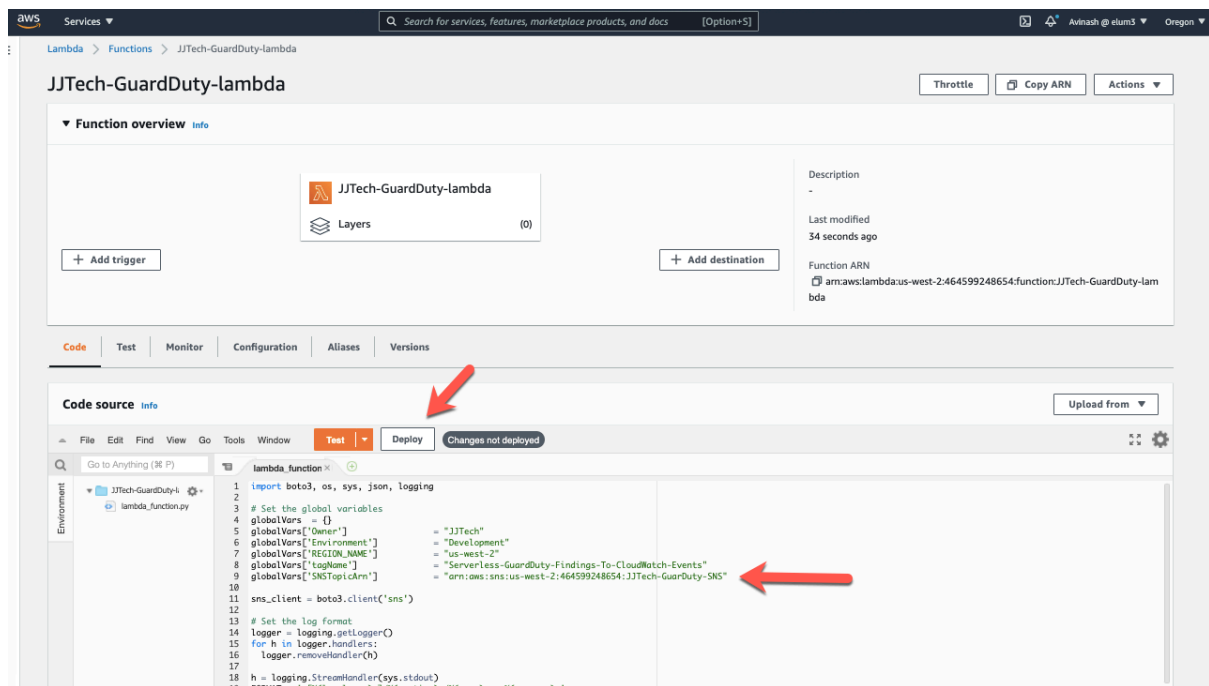▶ **Advanced settings**

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720

- Get the lambda code

- Change line 6 with your SNS topic ARN you created at Step 1
- Then Deploy the new code to the lambda function

- Now we have to increase the lambda timeout
  - select the lambda function > click on the configuration tab > General Configuration and click on Edit

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720

Lambda > Functions > lambda4GuardDuty

lambda4GuardDuty

Throttle | Copy ARN | Actions ▼

▼ Function overview Info

Export to Application Composer | Download ▼

Diagram | Template

lambda4GuardDuty

Layers (0)

EventBridge (CloudWatch Events)

+ Add trigger

+ Add destination

Description
-

Last modified
1 hour ago

Function ARN
arn:aws:lambda:us-east-1:666572520784:function:lambda4GuardDuty

Function URL Info
-

Code | Test | Monitor | Configuration | Aliases | Versions

General configuration

Triggers

Permissions

Destinations

Function URL

Environment variables

Tags

VPC

General configuration Info

Edit

Description
-

Timeout
15 min 0 sec

Memory
128 MB

SnapStart Info
None

Ephemeral storage
512 MB

Edit basic settings

Basic settings Info

Description - optional

[   ]

Memory (MB) Info
Your function is allocated CPU proportional to the memory configured.

[128] MB

Set memory to between 128 MB and 10240 MB

Timeout

[15] min [0] sec

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the IAM console.

◉ Use an existing role
◯ Create a new role from AWS policy templates

Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.

[JJTech-GuardDuty-Lambda-Role   ▼] [↻]

View the JJTech-GuardDuty-Lambda-Role role on the IAM console.

Cancel | Save

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720

![JJ Tech logo]

JJ Tech

STEP 4: Create Cloudwatch rule to trigger the lambda

- Create Cloudwatch rule to trigger lambda whenever New GuardDuty finding is available. So that we will get notified with the details to our mail
- Navigate to EventBridge console

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720

Create rule

A rule watches for certain events and then routes them to AWS targets that you choose. You can create a rule that performs an AWS action automatically when another AWS action happens, or a rule that performs an AWS action regularly on a set schedule.

Name and description

Name

JJTech-GuardDuty-Trigger

Maximum of 64 characters consisting of lower/upper case letters, ., -, _.

Description - optional

JJTech-GuardDuty-Trigger

Define pattern

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

◉ **Event pattern** Info
Build a pattern to match events

○ **Schedule** Info
Invoke your targets on a schedule

Event matching pattern
You can use pre-defined pattern provided by a service or create a custom pattern

◉ Pre-defined pattern by service
○ Custom pattern

Event pattern   [Copy]   [Edit]

```
1 {
2   "source": ["aws.guardduty"],
3   "detail-type": ["GuardDuty Finding"]
4 }
```

Service provider
AWS services or custom/partner services

AWS ▼

Service name
The name of partner service selected as the event source

GuardDuty ▼

Event type
The type of events as the source of the matching pattern

GuardDuty Finding ▼

▶ Sample event(s)

▶ Test event pattern

Select event bus

Select an event bus for this rule.

◉ AWS default event bus
○ Custom or partner event bus

🔘 Enable the rule on the selected event bus

410) 8887049
@jjtechinc.co
.jjtechinc.co
e MD 20720

Select targets

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule).

Target   `Remove`

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule).

Lambda function	▼

Function

JJTech-GuardDuty-lambda	▼

▶ **Configure version/alias**

▶ **Configure input**

▶ **Retry policy and dead-letter queue**

`Add target`

Tags - *optional*

Key   Value

Enter key	Enter value	`Remove tag`

`Add tag`

`Cancel`   `Create`

- Now if you navigate to Lambda console you should see below trigger to be configured

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720
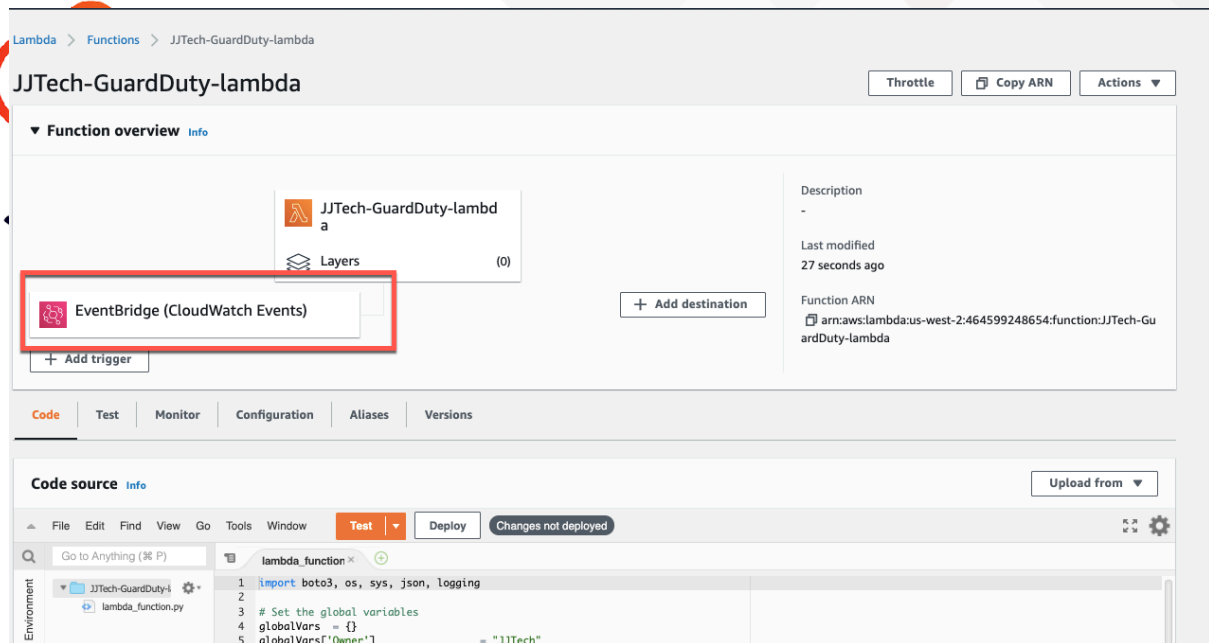
Step 5: Test the solution

- Navigate to Amazon GuardDuty console
- Let's create some sample findings in Guardduty

- You will receive mails whenever new finding is available in GuardDuty
- Based on the issue you have to fix them
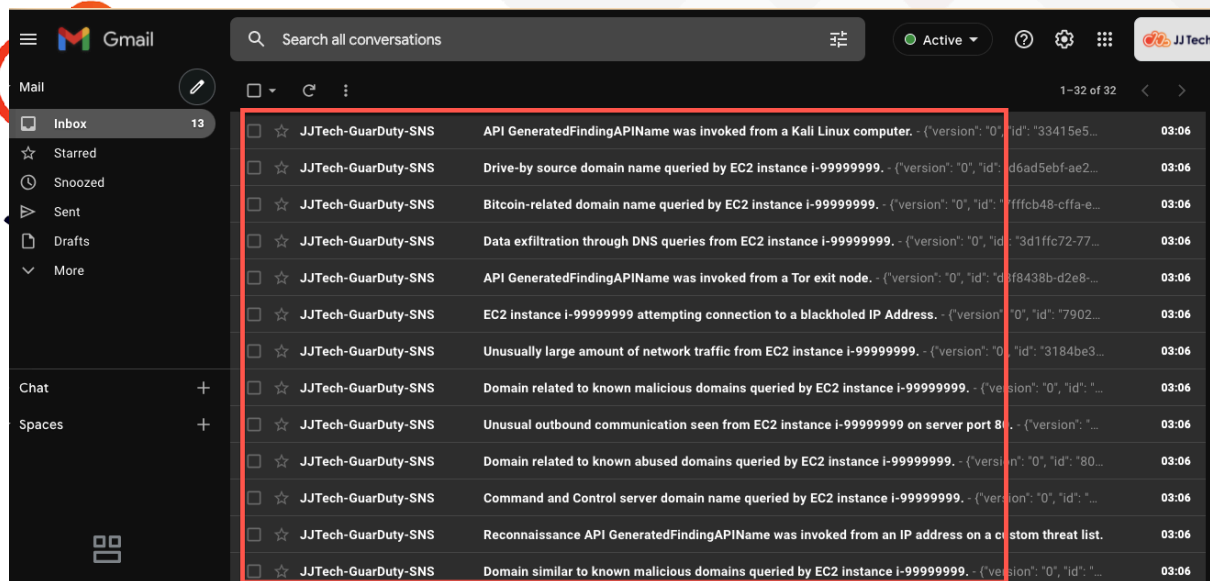
- For example If an EC2 instance got compromised try to terminate
- If an EC2 instance is getting malicious traffic try to block them in NACL or restrict access to respective networks in Security group and so on

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720

GOAL: USE AMAZON Inspector to inspect the security posture of EC2 instances based on CIS benchmarks

steps:

1. **Enable Amazon Inspector in the region**
2. **launch 3 Amazon Linux 2 instance with necessary SSM permissions to enable these instance to be "managed Instances"**
3. **create a one time scan and view the Inspector results**

Enable Inspector in your Region

we have to enable inspector in the Account and region

Once enabled, then we can see the details of inspector in the inspector console.

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720

Launch 3 EC2 managed instances.

- navigate to EC2 console and launch 3 EC2 instances based on Amazon Linux 2 ami
- Attach an Instance Profile (role) with SSM permissions so Systems Manager can manage these nodes.
- ensure all instance have a common tag (for simplicity)

  e.g **Name: inspectorInstance**

Create an inspector check based on CIS level 2 (supported CIS level for Amazon Linux 2).

- navigate to the inspector console
- click on "On-demand scans" and "create new scan"
- Provide necessary details
  - name: CIS-test-scan
  - key= **Name** , Value= **inspectorInstance** (based on the tag on EC2 instances)
  - CIS Benchmark Level = LEVEL_2
  - Target accounts = self
  - schedule = One time scan
- Click on "create"
- All tag instances are scanned after the create is complete.

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720