JJ Tech

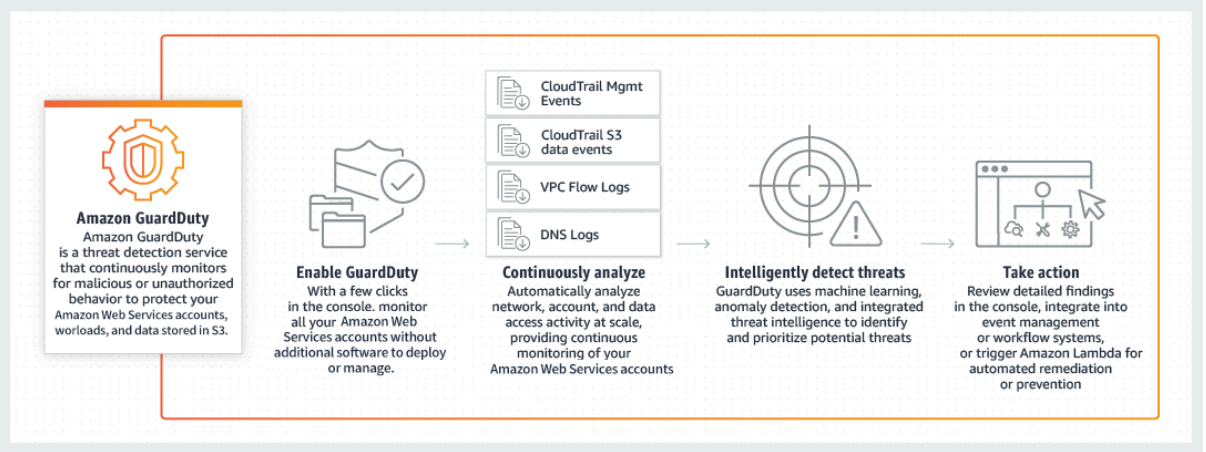
AWS Guard Duty

Protect your AWS accounts with intelligent threat detection

- Achieve organization-wide visibility into possible threats with only a few click
- Expose threats quickly with AWS threat intelligence, behavioural models, and third-party security feeds.
- Mitigate threats early by triggering automated responses.

How it works

Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.



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

JJ Tech

Terminology

Account
A standard Amazon Web Services (AWS) account that contains your AWS resources. You can sign in to AWS with your account and enable GuardDuty.
You can also invite other accounts to enable GuardDuty and become associated with your AWS account in GuardDuty. If your invitations are accepted, your account is designated as the **administrator** GuardDuty account, and the added accounts become your **member** accounts. You can then view and manage those accounts' GuardDuty findings on their behalf.
Users of the administrator account can configure GuardDuty as well as view and manage GuardDuty findings for their own account and all of their member accounts. You can have up to 5000 member accounts in GuardDuty.
Users of member accounts can configure GuardDuty as well as view and manage GuardDuty findings in their account (either through the GuardDuty management console or GuardDuty API). Users of member accounts can't view or manage findings in other members' accounts.
An AWS account can't be a GuardDuty administrator and member account at the same time. An AWS account can accept only one membership invitation. Accepting a membership invitation is optional.

Detector
All GuardDuty findings are associated with a detector, which is an object that represents the GuardDuty service. The detector is a regional entity, and a unique detector is required in each region GuardDuty operates in. When you enable GuardDuty in a region a new detector with a unique 32 alphanumeric detector ID is generated in that region. The detector ID format looks like this:

12abc34d567e8fa901bc2d34e56789f0

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

You can find your detector ID for your current region in the console from the **Settings** pane, or programmatically using the ListDetectors API.

JJ Tech

Note
In multiple account environments all findings for member accounts roll up to the administrator account's detector.
Some GuardDuty functionality is configured through the detector, such as configuring CloudWatch Events notification frequency and the enabling or disabling of optional data sources for GuardDuty to process.

Data source
The origin or location of a set of data. To detect unauthorized and unexpected activity in your AWS environment, GuardDuty analyzes and processes data from AWS CloudTrail event logs, VPC Flow Logs, and DNS logs.

Finding
A potential security issue discovered by GuardDuty.
Findings are displayed in the GuardDuty console and contain a detailed description of the security issue. You can also retrieve your generated findings by calling the GetFindings and ListFindings API operations.
You can also see your GuardDuty findings through Amazon CloudWatch events. GuardDuty sends findings to Amazon CloudWatch via HTTPS protocol. For more information.

Suppression rule
Suppression rules allow you to create very specific combinations of attributes to suppress findings. For example, you can define a rule through the GuardDuty filter to auto-archive Recon:EC2/Portscan from only those instances in a specific VPC, running a specific AMI, or with a specific EC2 tag. This rule would result in port scan findings being automatically archived from the instances that meet the criteria. However, it

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

still allows alerting if GuardDuty detects those instances conducting other malicious activity, such as crypto-currency mining.
Suppression rules defined in the GuardDuty administrator account apply to the GuardDuty member accounts. GuardDuty member accounts can't modify suppression rules.

With suppression rules, GuardDuty still generates all findings. Suppression rules provide suppression of findings while maintaining a complete and immutable history of all activity.
Typically suppression rules are used to hide findings that you have determined as false positives for your environment, and reduce the noise from low-value findings so you can focus on larger threats.

Trusted IP list
A list of trusted IP addresses for highly secure communication with your AWS environment. GuardDuty does not generate findings based on trusted IP lists.

Threat list
A list of known malicious IP addresses. GuardDuty generates findings based on threat lists.

GuardDuty Data Sources

- AWS CloudTrail Event Logs
- AWS CloudTrail Management Events
- AWS CloudTrail S3 Data Events
- VPC Flow Logs
- DNS logs

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

JJ Tech

Severity levels for GuardDuty findings

Each GuardDuty finding has an assigned severity level and value that reflects the potential risk the finding could have to your network as determined by our security engineers. The value of the severity can fall anywhere within the 0.1 to 8.9 range, with higher values indicating greater security risk. To help you determine a response to a potential security issue that is highlighted by a finding, GuardDuty breaks down this range into, High, Medium, and Low severity levels.

Note
Values 0 and 9.0 to 10.0 are currently reserved for future use.
The following are the currently defined severity levels and values for the GuardDuty findings as well as general recommendations for each:

Severity level	**Value range**
High	8.9 - 7.0
A High severity level indicates that the resource in question (an EC2 instance or a set of IAM user credentials) is compromised and is actively being used for unauthorized purposes. We recommend that you treat any High severity finding security issue as a priority and take immediate remediation steps to prevent further unauthorized use of your resources. For example,	

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

clean up your EC2 instance or terminate it, or rotate the IAM credentials.	
Medium	6.9 - 4.0
A Medium severity level indicates suspicious activity that deviates from normally observed behavior and, depending on your use case, may be indicative of a resource compromise. We recommend that you investigate the implicated resource at your earliest convenience. Remediation steps will vary by resource and Finding family, but in general, you should be looking to confirm that the activity is authorized and consistent with your use case. If you cannot identify the cause, or confirm the activity was authorized, you should consider the resource compromised and follow Remediation Steps to secure the resource. Here are some things to consider when reviewing a Medium level finding: • Check if an authorized user has installed new software that changed the behavior of a resource (for example, allowed higher than normal traffic, or enabled communication on a new port). • Check if an authorized user changed the control panel settings, for example, modified a security group setting. • Run an anti-virus scan on the implicated resource to detect unauthorized software. • Verify the permissions that are attached to the implicated IAM role, user, group, or set of credentials. These might have to be changed or rotated.	
Low	3.9 - 1.0
A low severity level indicates attempted suspicious activity that did not compromise your network, for example, a port scan or a failed intrusion attempt. There is no immediate recommended action, but it is worth making note of this information as it may indicate someone is looking for weak points in your network.	

Findings by resource type

The following pages are broken down by each resource type GuardDuty currently generates findings for. The pages contain detailed information on all finding types for that resources type.

- EC2 finding types
- IAM finding types
- S3 finding types

Findings table

The following table lists all finding types by name, resource, data source and severity. A severity listed with an asterisk (*) indicates the finding has variable severities depending the circumstances of the finding, which are described in the details for that finding. Choose the finding name to open more info about that finding.

FINDING TYPE	RESOURCE	DATA SOURCE	SEVERITY
Backdoor:EC2/C&CActivity.B	EC2	VPC Flow Logs	High
Backdoor:EC2/C&CActivity.B!DNS	EC2	DNS logs	High
Backdoor:EC2/DenialOfService.Dns	EC2	VPC Flow Logs	High
Backdoor:EC2/DenialOfService.Tcp	EC2	VPC Flow Logs	High
Backdoor:EC2/DenialOfService.Udp	EC2	VPC Flow Logs	High
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	EC2	VPC Flow Logs	High
Backdoor:EC2/DenialOfService.UnusualProtocol	EC2	VPC Flow Logs	High
Backdoor:EC2/Spambot	EC2	VPC Flow Logs	Medium
Behavior:EC2/NetworkPortUnusual	EC2	VPC Flow Logs	Medium
Behavior:EC2/TrafficVolumeUnusual	EC2	VPC Flow Logs	Medium

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

CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail management event	Medium
CryptoCurrency:EC2/BitcoinTool.B	EC2	VPC Flow Logs	High
CryptoCurrency:EC2/BitcoinTool.B!DNS	EC2	DNS logs	High
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail management event	Medium
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail management event	Low
Discovery:S3/MaliciousIPCaller	S3	CloudTrail S3 data event	High
Discovery:S3/MaliciousIPCaller.Custom	S3	CloudTrail S3 data event	High
Discovery:S3/TorIPCaller	S3	CloudTrail S3 data event	Medium
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail management event	High
Exfiltration:S3/MaliciousIPCaller	S3	CloudTrail S3 data event	High
Exfiltration:S3/ObjectRead.Unusual	S3	S3 CloudTrail data event	Medium*
Impact:EC2/AbusedDomainRequest.Reputation	EC2	DNS logs	Medium
Impact:EC2/BitcoinDomainRequest.Reputation	EC2	DNS logs	High
Impact:EC2/MaliciousDomainRequest.Reputation	EC2	DNS logs	High
Impact:EC2/PortSweep	EC2	VPC Flow Logs	High
Impact:EC2/SuspiciousDomainRequest.Reputation	EC2	DNS logs	Low
Impact:EC2/WinRMBruteForce	EC2	VPC Flow Logs	Low*

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

Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail management event	High
Impact:S3/MaliciousIPCaller	S3	CloudTrail S3 data event	High
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail management event	Medium
PenTest:IAMUser/KaliLinux	IAM	CloudTrail management event	Medium
PenTest:IAMUser/ParrotLinux	IAM	CloudTrail management event	Medium
PenTest:IAMUser/PentooLinux	IAM	CloudTrail management event	Medium
PenTest:S3/KaliLinux	S3	CloudTrail S3 data event	Medium
PenTest:S3/ParrotLinux	S3	CloudTrail S3 data event	Medium
PenTest:S3/PentooLinux	S3	CloudTrail S3 data event	Medium
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail management event	Medium
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail management event or CloudTrail data event	Low
Policy:S3/AccountBlockPublicAccessDisabled	S3	CloudTrail management event	Low
Policy:S3/BucketAnonymousAccessGranted	S3	CloudTrail management event	High

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

Policy:S3/BucketBlockPublicAccessDisabled	S3	CloudTrail management event	Low
Policy:S3/BucketPublicAccessGranted	S3	CloudTrail management event	High
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail management event	Medium
Recon:EC2/PortProbeEMRUnprotectedPort	EC2	VPC Flow Logs	High
Recon:EC2/PortProbeUnprotectedPort	EC2	VPC Flow Logs	Low*
Recon:EC2/Portscan	EC2	VPC Flow Logs	Medium
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail management event	Medium
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail management event	Medium
Recon:IAMUser/TorIPCaller	IAM	CloudTrail management event	Medium
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail management event	Low
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail management event	Low
Stealth:S3/ServerAccessLoggingDisabled	S3	CloudTrail management event	Low
Trojan:EC2/BlackholeTraffic	EC2	VPC Flow Logs	Medium
Trojan:EC2/BlackholeTraffic!DNS	EC2	DNS logs	Medium
Trojan:EC2/DGADomainRequest.B	EC2	DNS logs	High
Trojan:EC2/DGADomainRequest.C!DNS	EC2	DNS logs	High
Trojan:EC2/DNSDataExfiltration	EC2	DNS logs	High

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

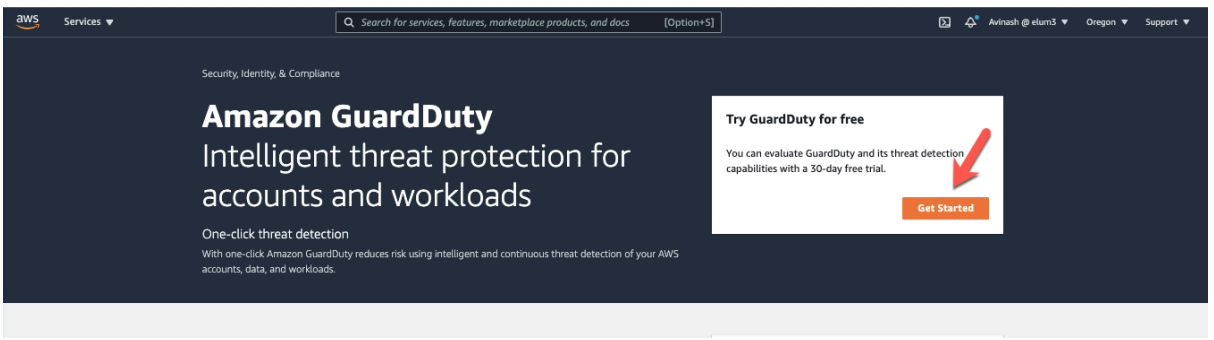
Trojan:EC2/DriveBySourceTraffic!DNS	EC2	DNS logs	High
Trojan:EC2/DropPoint	EC2	VPC Flow Logs	Medium
Trojan:EC2/DropPoint!DNS	EC2	DNS logs	Medium
Trojan:EC2/PhishingDomainRequest!DNS	EC2	DNS logs	High
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	EC2	VPC Flow Logs	Medium
UnauthorizedAccess:EC2/MetadataDNSRebind	EC2	DNS logs	High
UnauthorizedAccess:EC2/RDPBruteForce	EC2	VPC Flow Logs	Low*
UnauthorizedAccess:EC2/SSHBruteForce	EC2	VPC Flow Logs	Low*
UnauthorizedAccess:EC2/TorClient	EC2	VPC Flow Logs	High
UnauthorizedAccess:EC2/TorRelay	EC2	VPC Flow Logs	High
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail management event	Medium
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail management event	High
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail management event	Medium
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail management event	Medium
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail management event	Medium
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	S3	CloudTrail S3 data event	High
UnauthorizedAccess:S3/TorIPCaller	S3	CloudTrail S3 data event	

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

JJ Tech

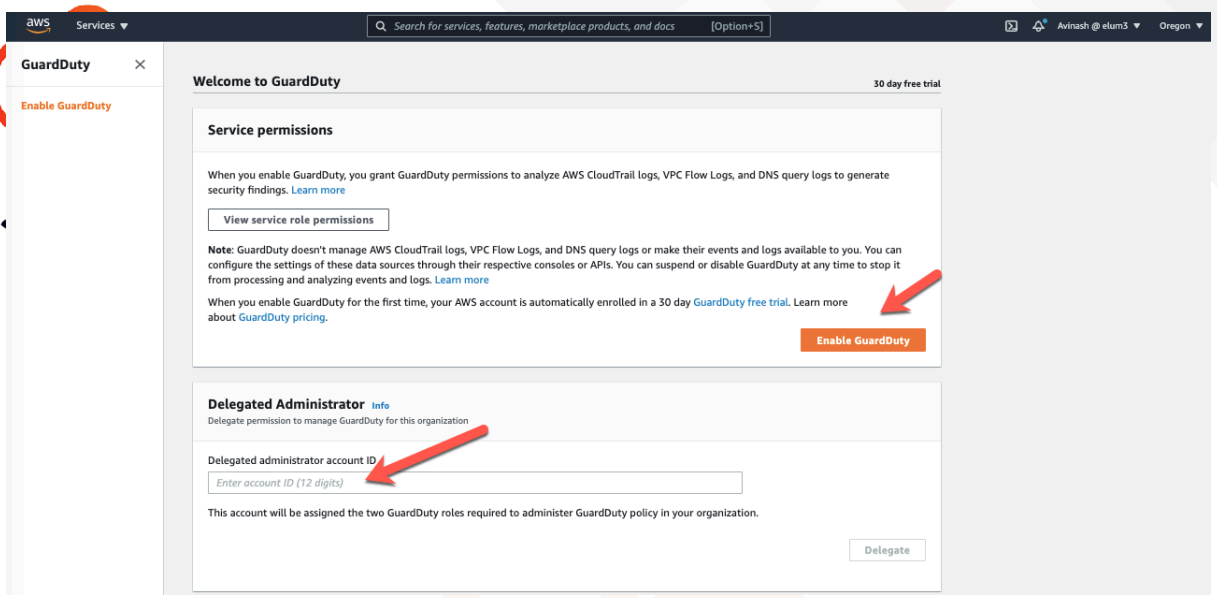
Enable GuardDuty

- 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

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



Demo:

Amazon GuardDuty Findings to SNS

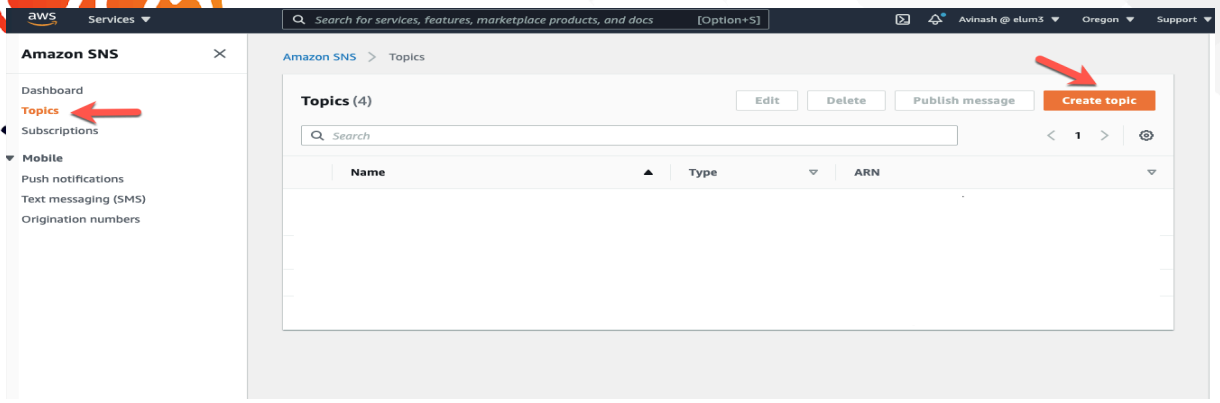
Every GuardDuty finding is assigned a finding ID. For every finding with a unique finding ID, GuardDuty aggregates all subsequent occurrences of a particular finding that take place in six-hour intervals into a single event. GuardDuty then sends a notification about these subsequent occurrences based on this event. We can use this to push the notifications into SNS topic, and getting the security teams to investigate the findings.

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.

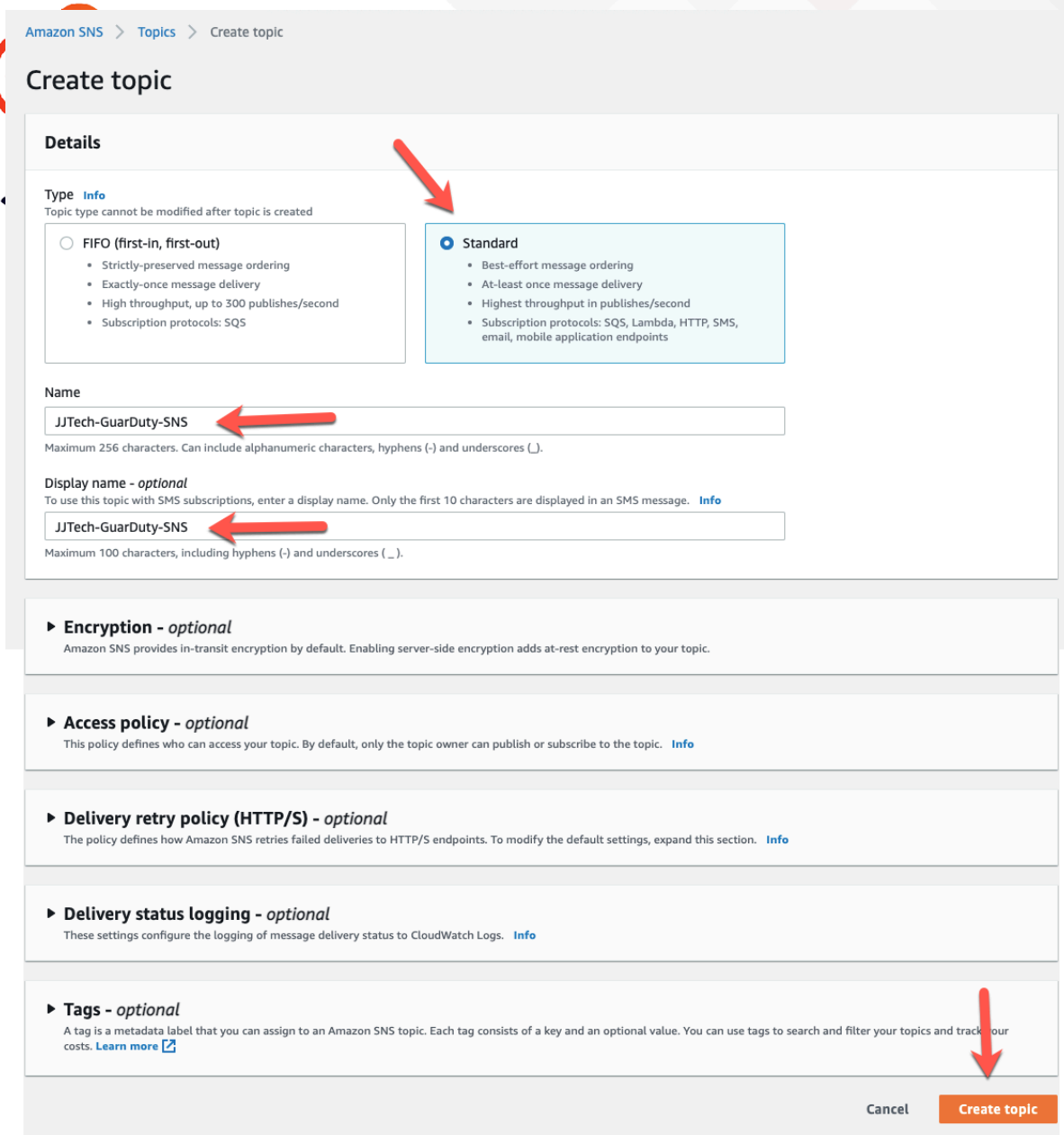
Step-1

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

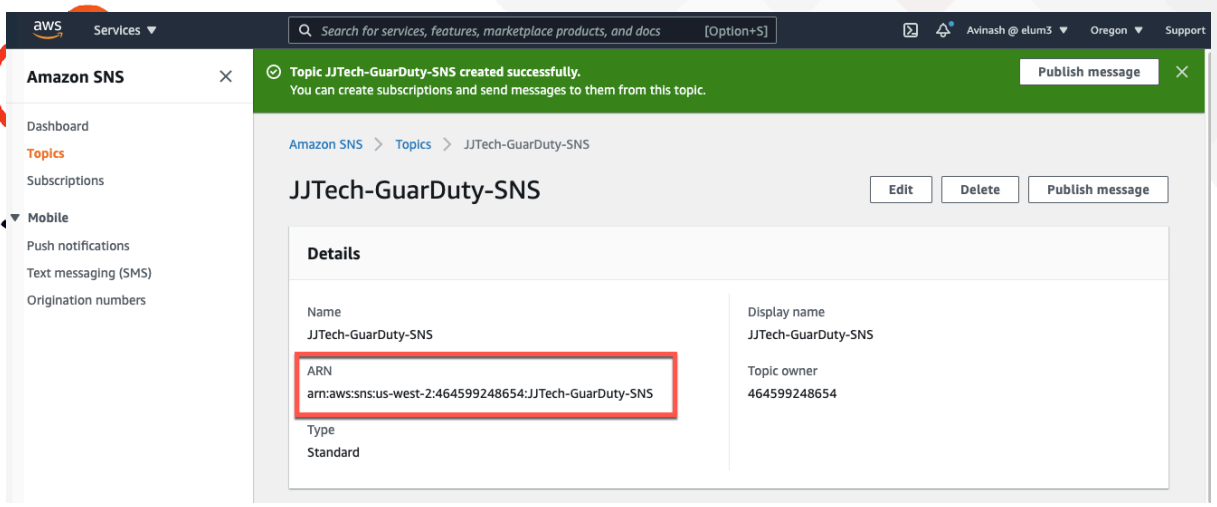
- Create a SNS Topic for Lambda to publish the GuardDuty Findings.
- Navigate to AWS SNS Console



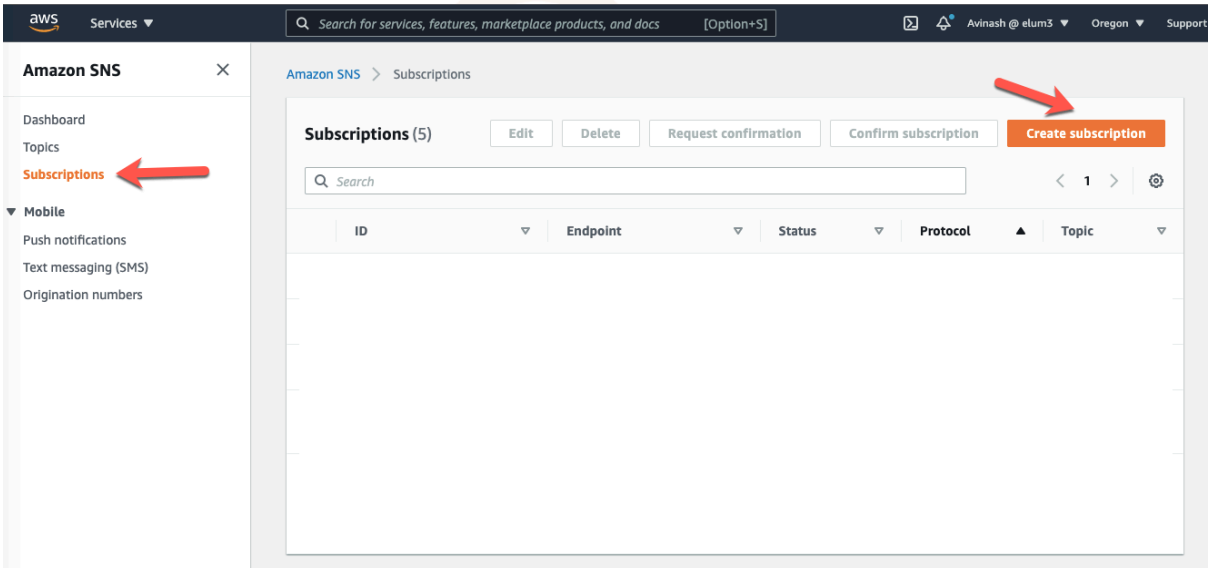
+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720



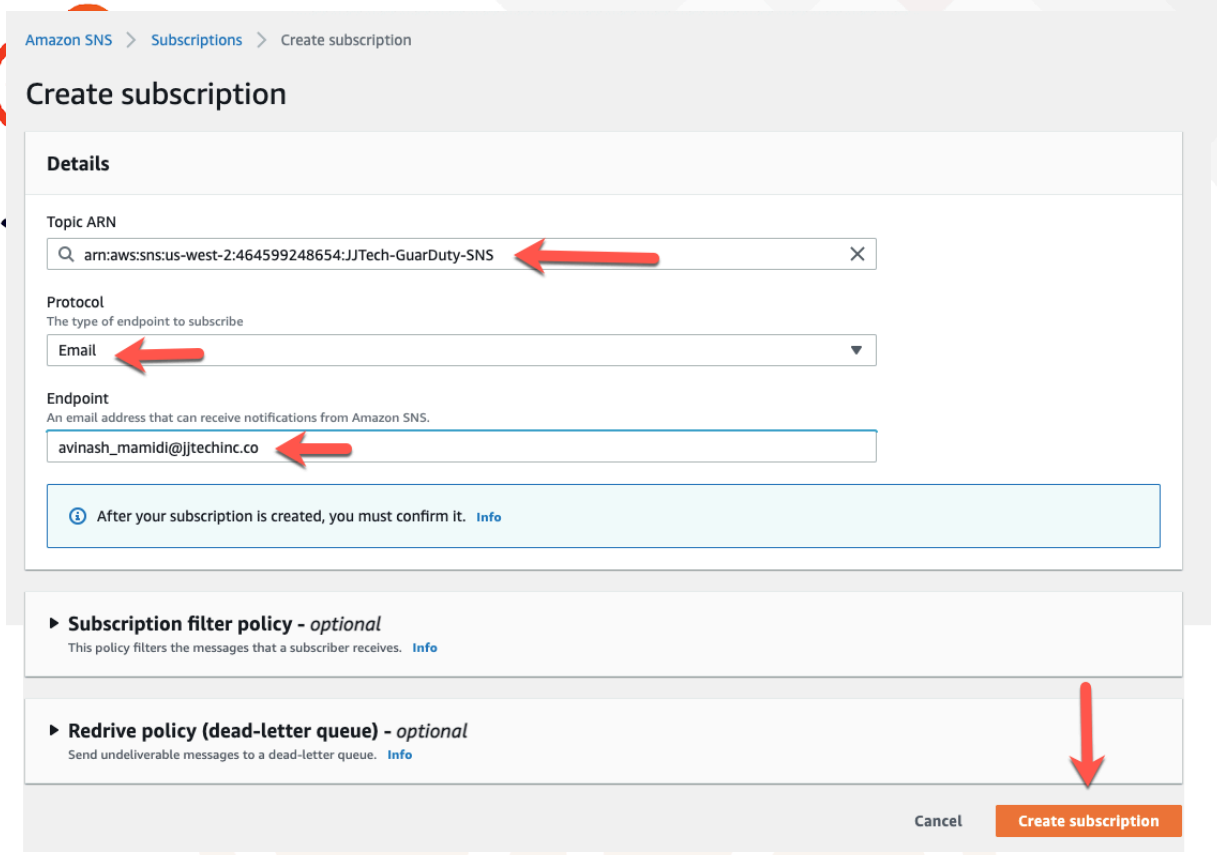
+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720



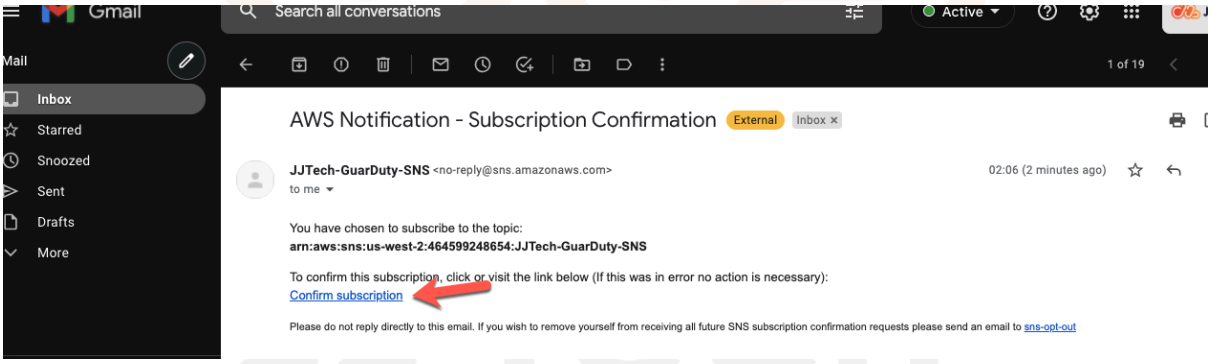
- Now you can subscribe the SNS topic with your mail id.



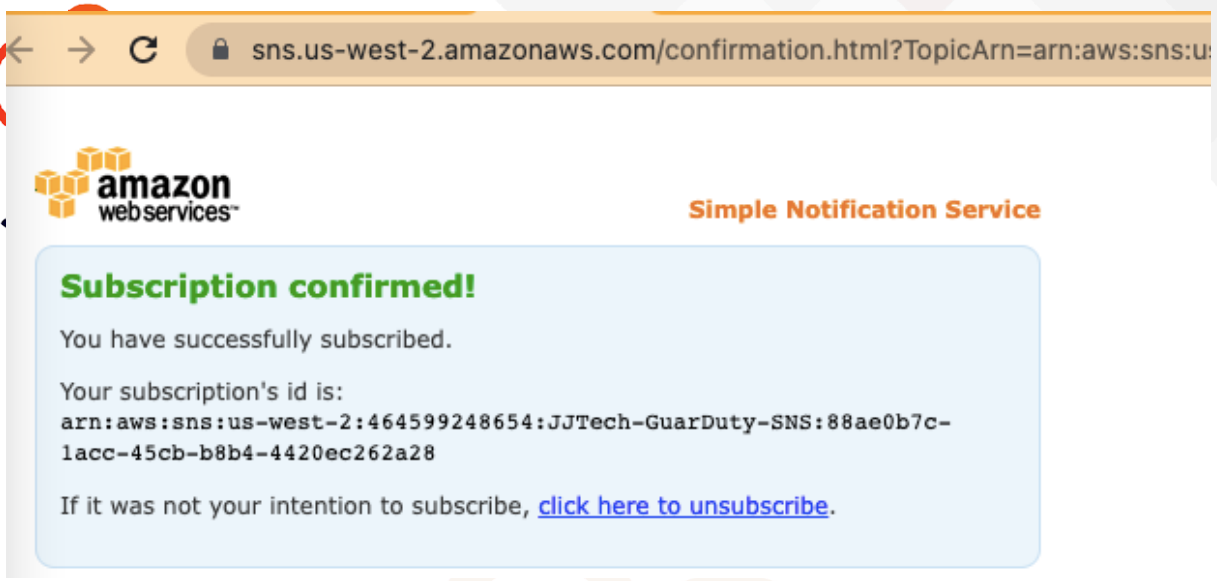
+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720

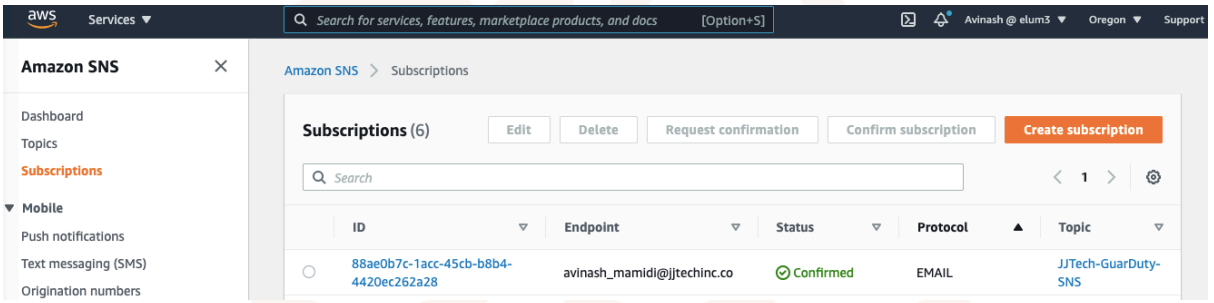


- You will receive a mail to confirm the subscription to your mail



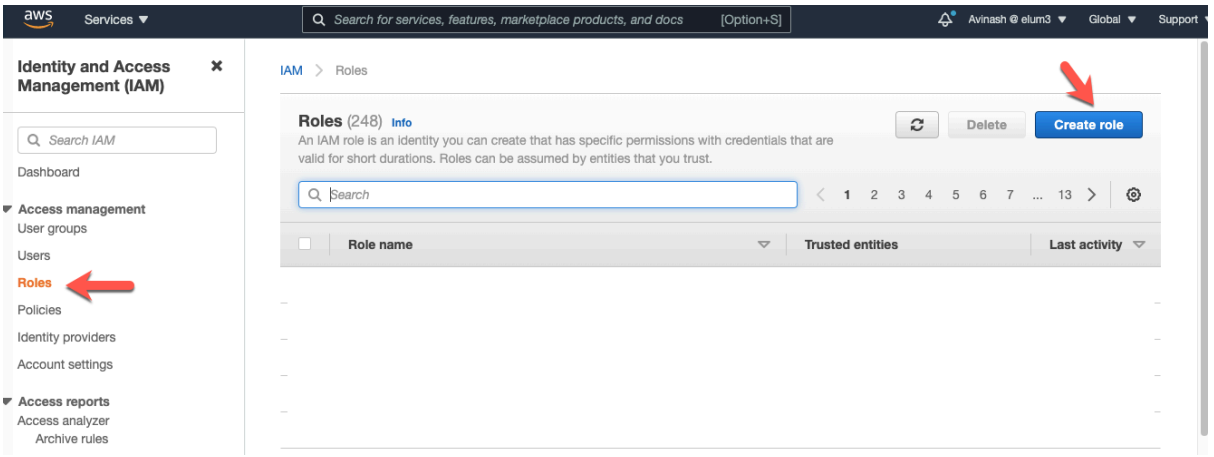
+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720



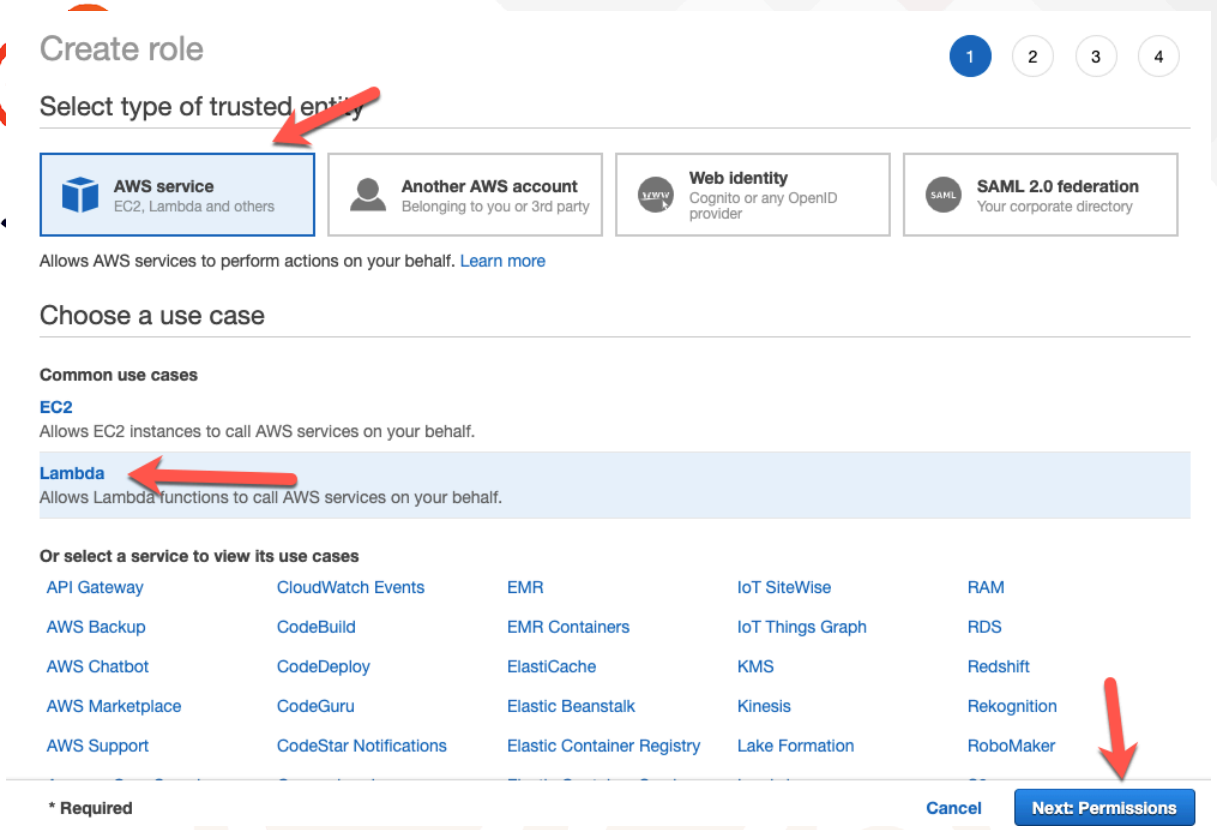


Step-2 : Create a IAM role for the Lambda function

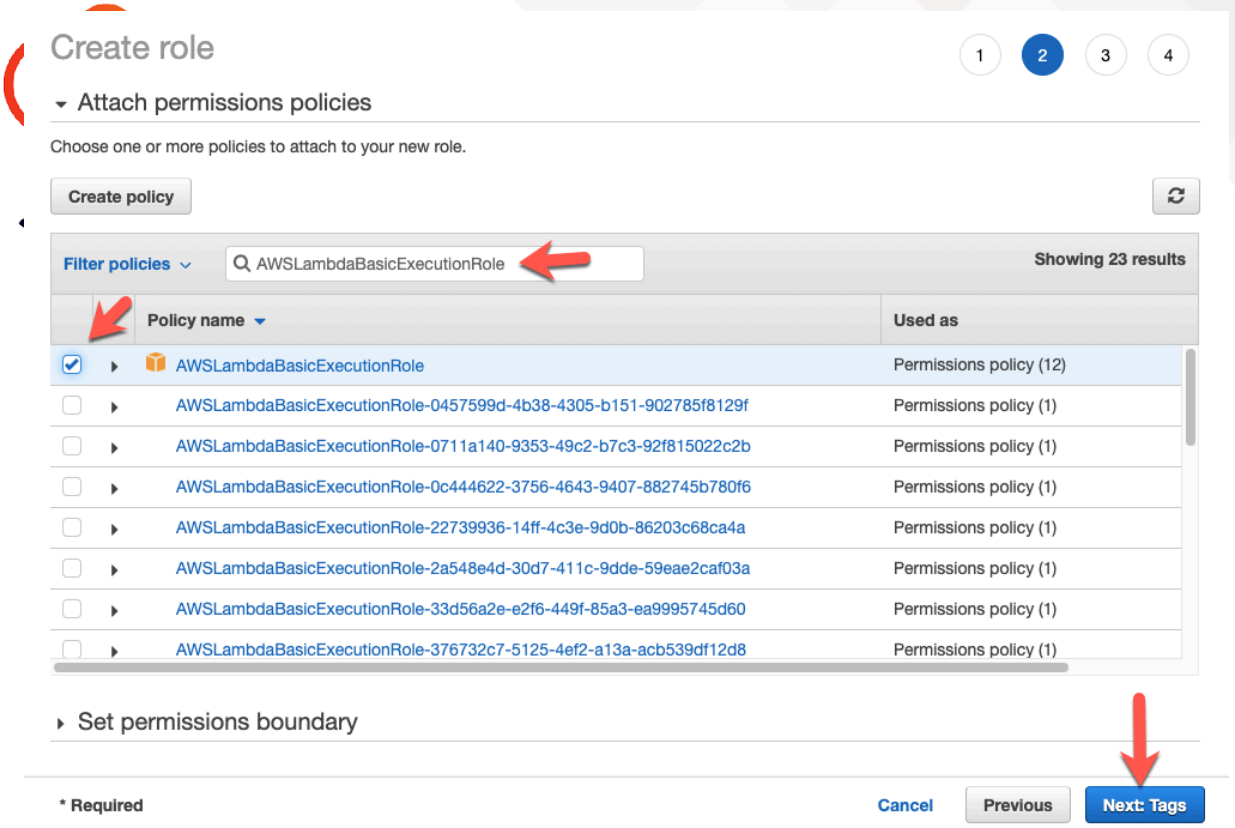
- Navigate to IAM Console



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

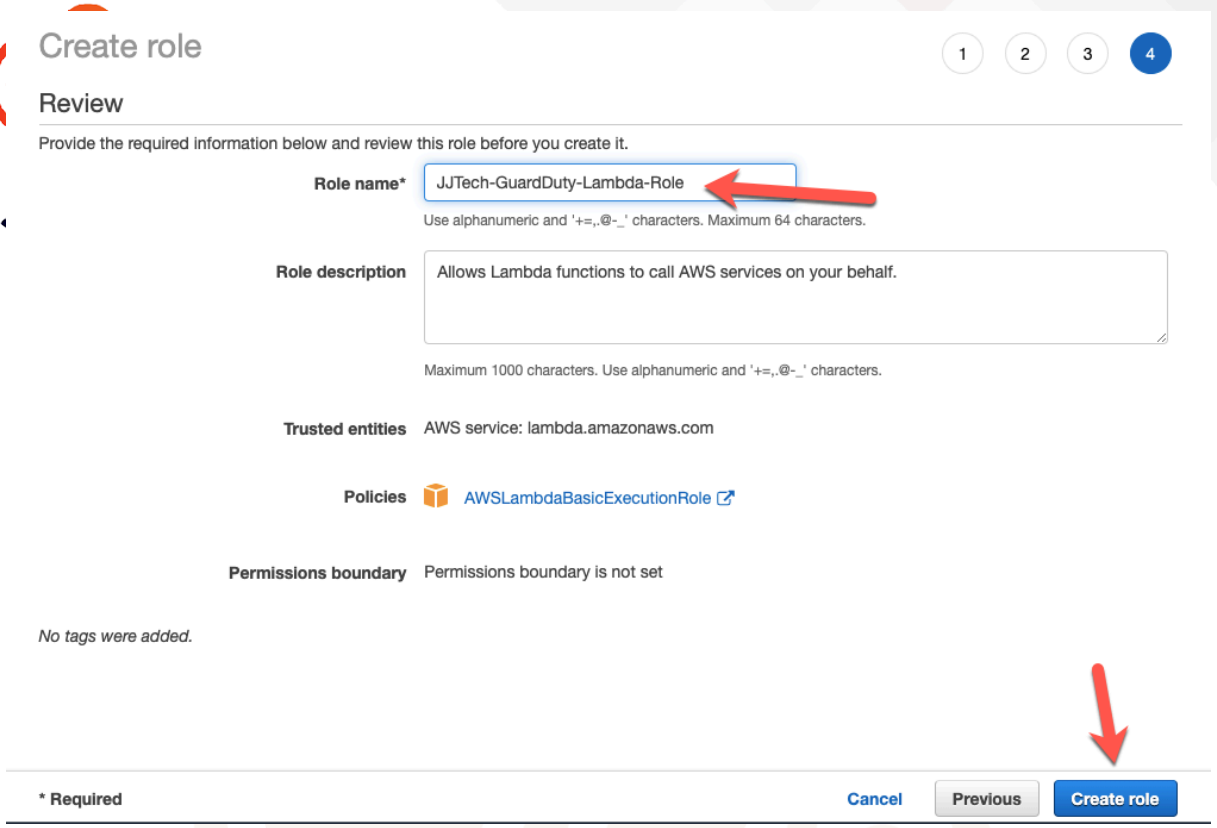


+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720



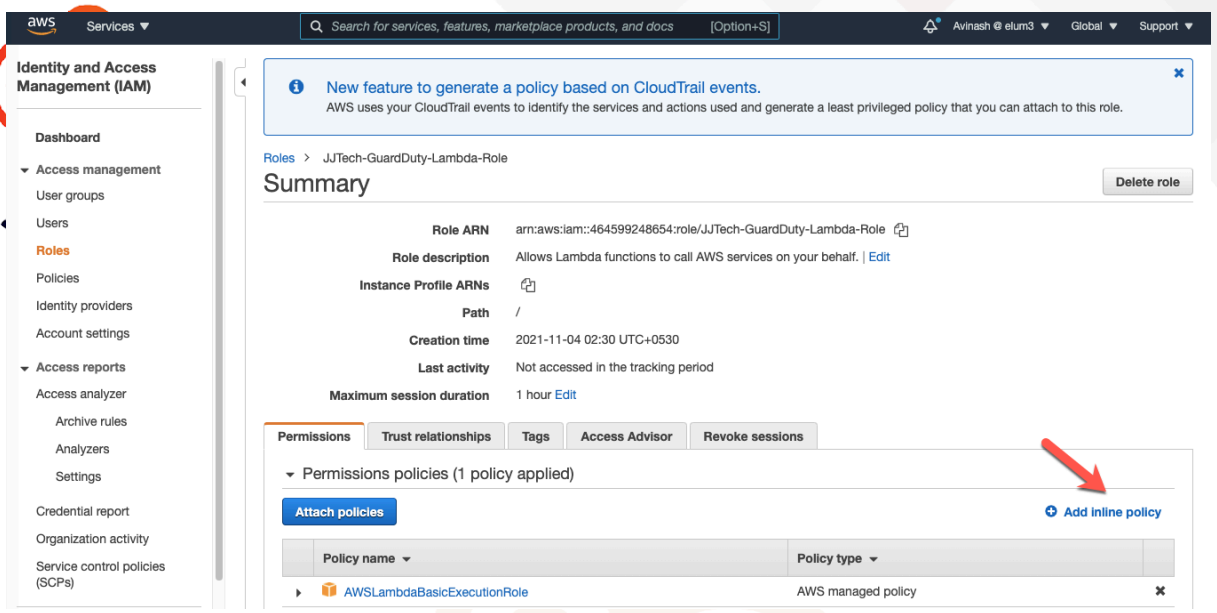
bas

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



- Navigate to the role you created

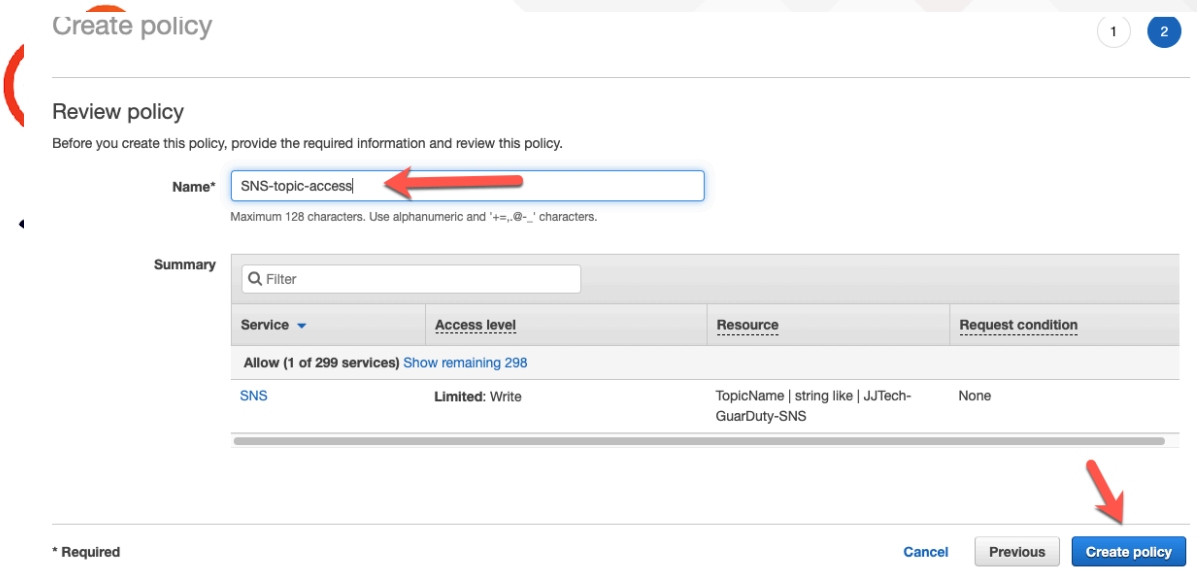
+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720



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

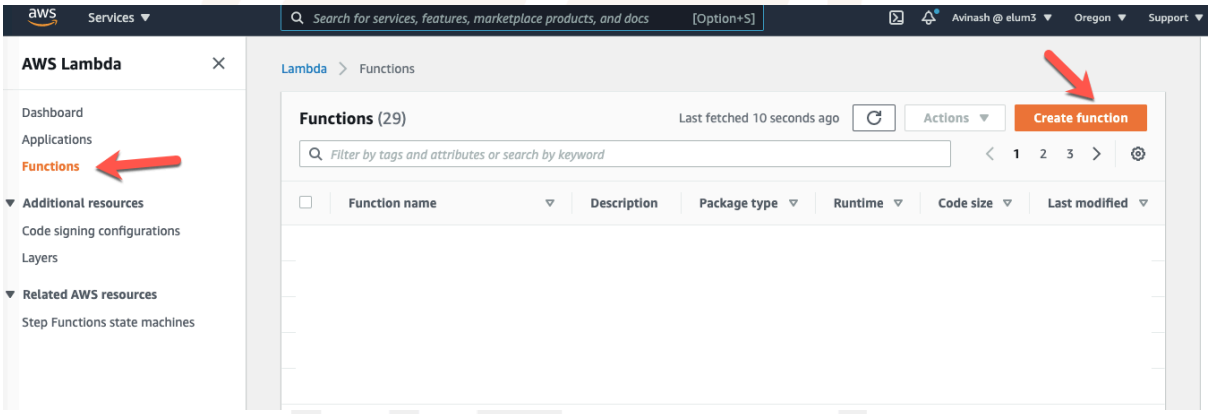
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "sns:Publish",
      "Resource": "<ARN-OF-YOUR-SNS-TOPIC>"
    }
  ]
}
```

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

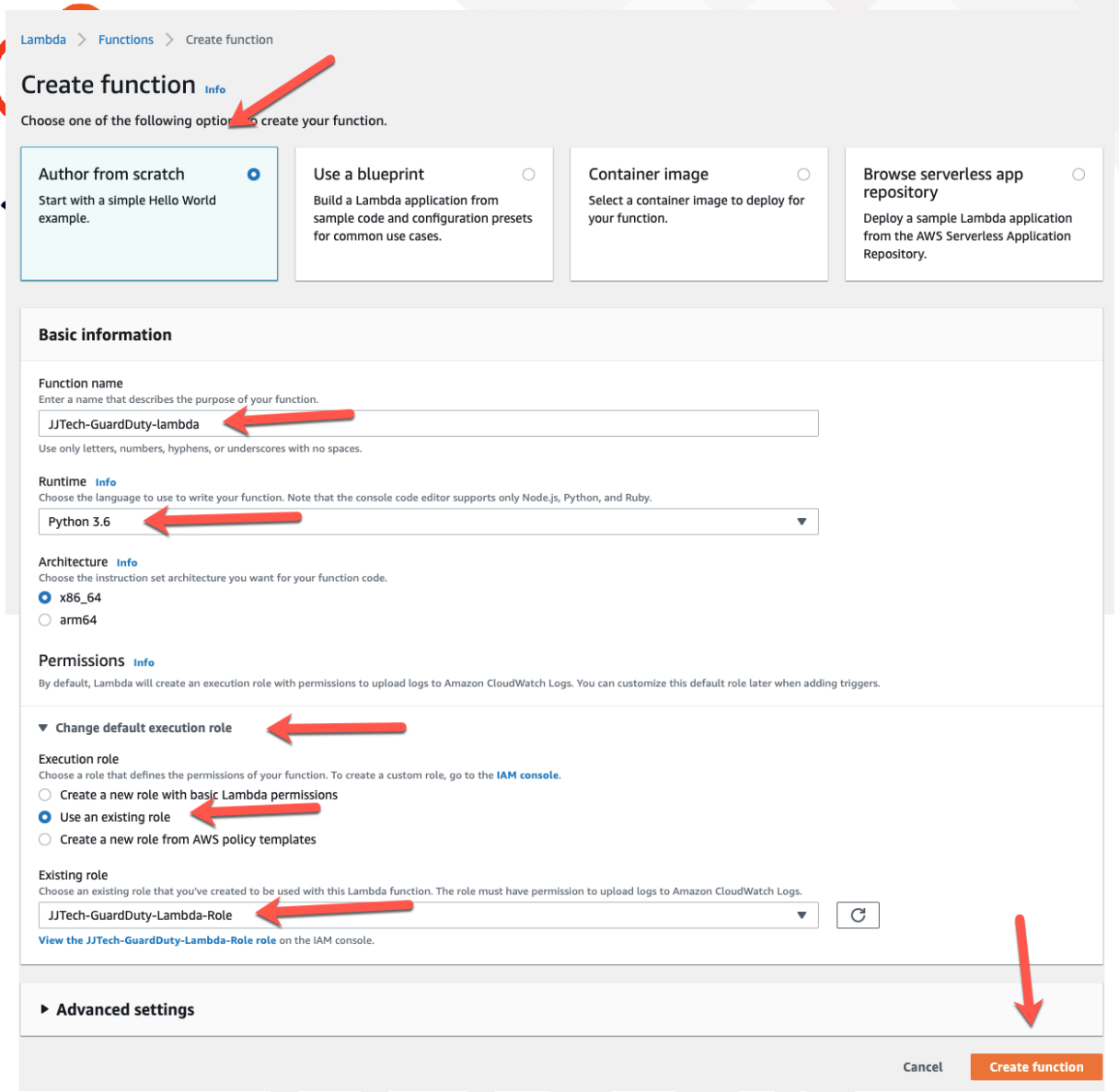


Step 3: Create Lambda Function

- Navigate to Lambda console



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

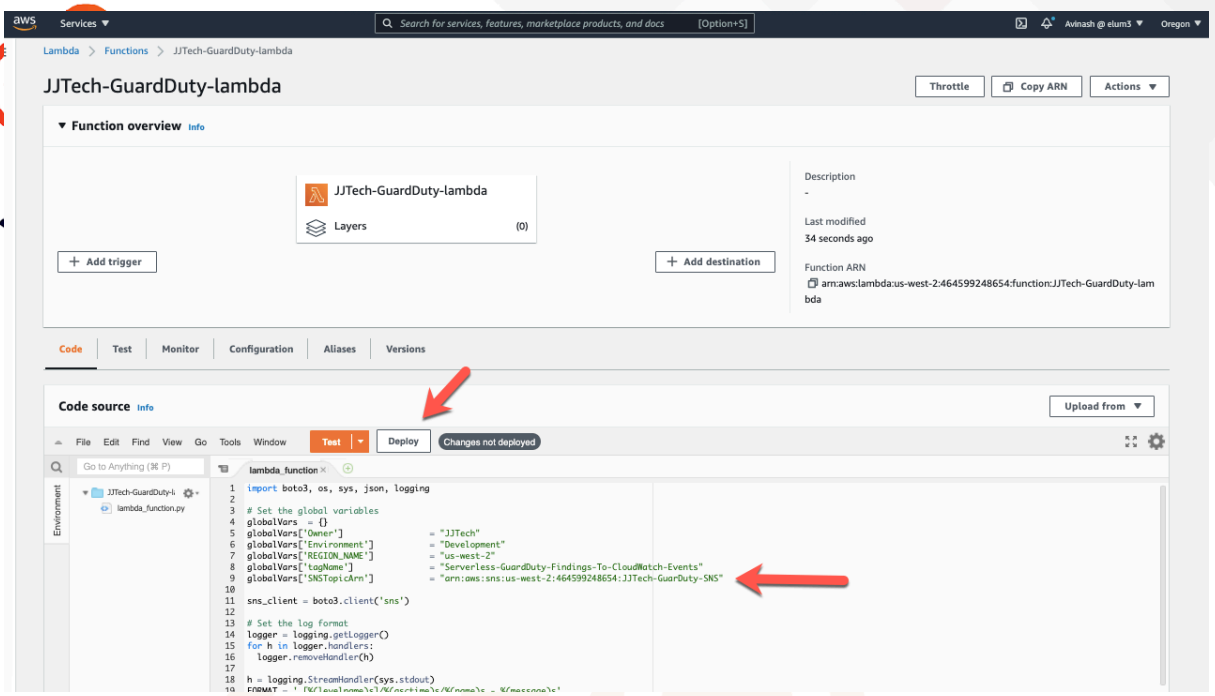


- Get the code from below link

https://raw.githubusercontent.com/JJTechInc/Serverless-GuardDuty-Findings-to-SNS/main/Serverless-GuardDuty-Findings-To-SNS.py

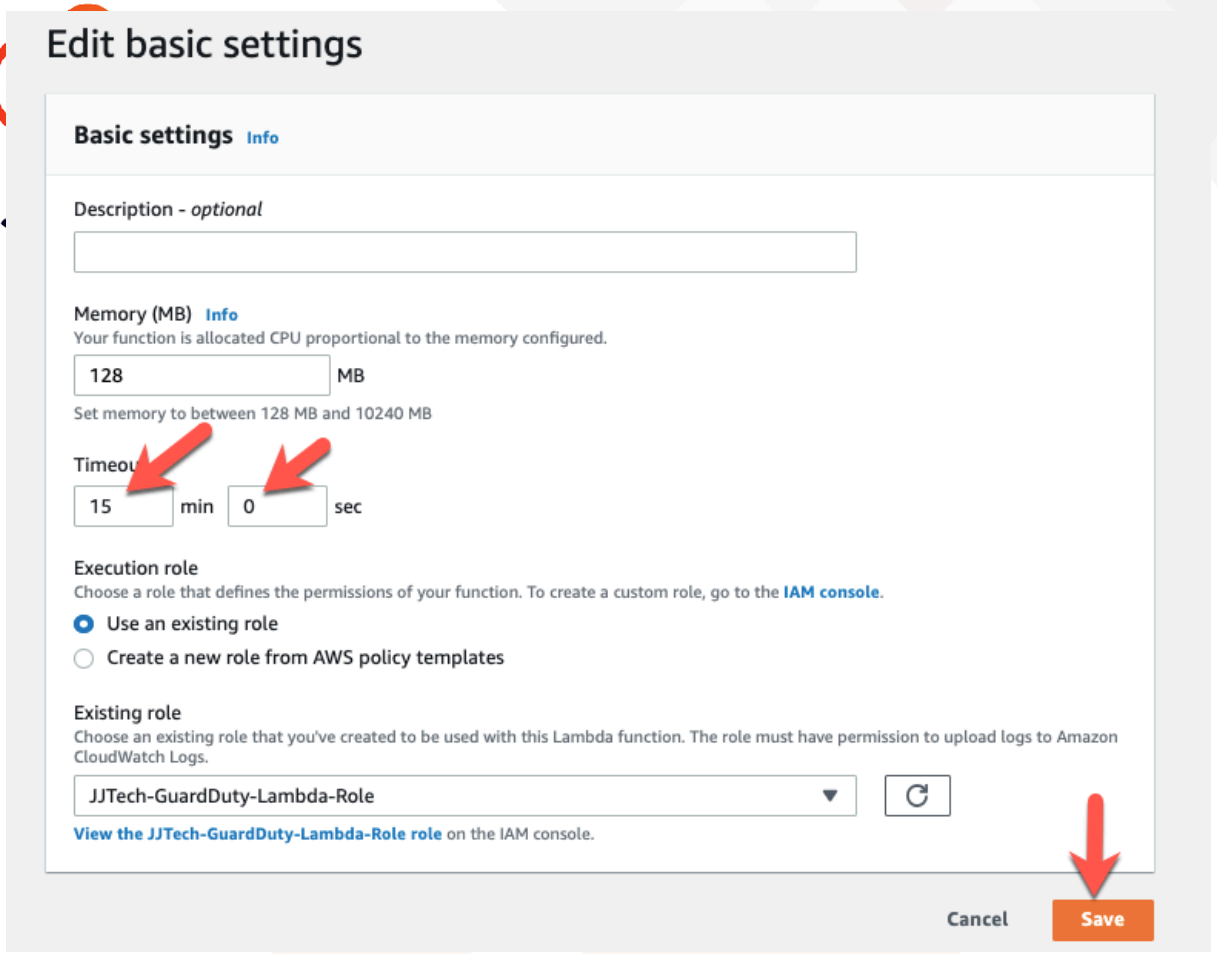
- Change line 9 with your SNS topic ARN you created at Step 1
- Then Deploy the new code to the lambda function

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



- Now we have to increase the lambda timeout

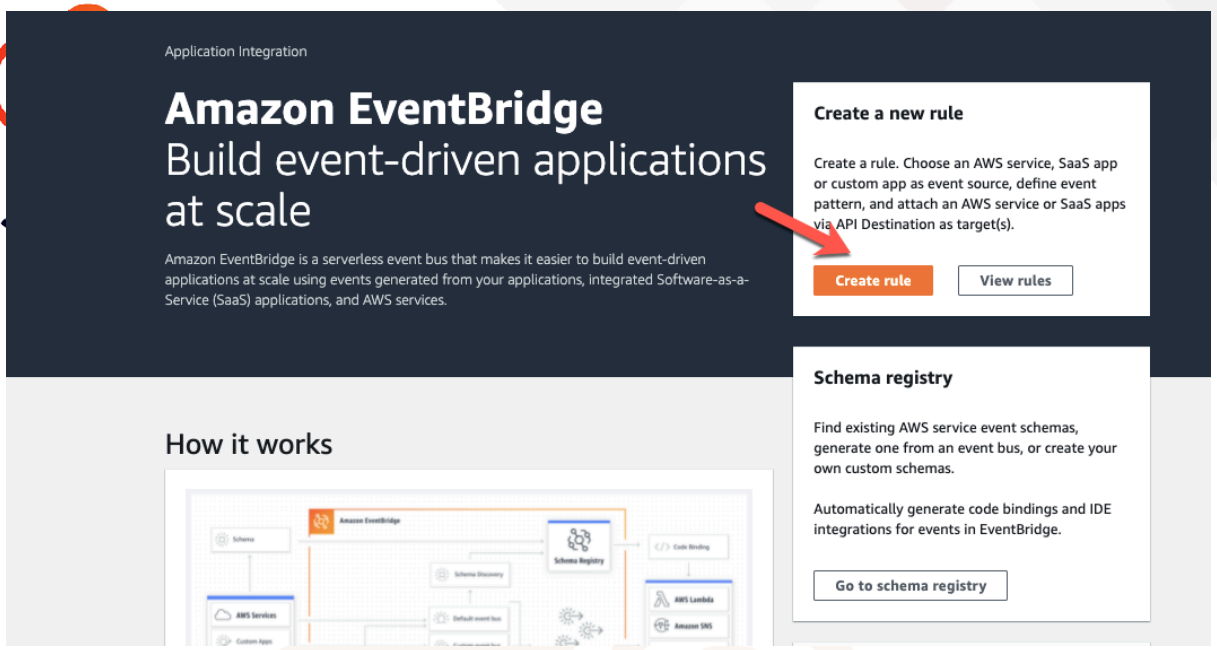
+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720



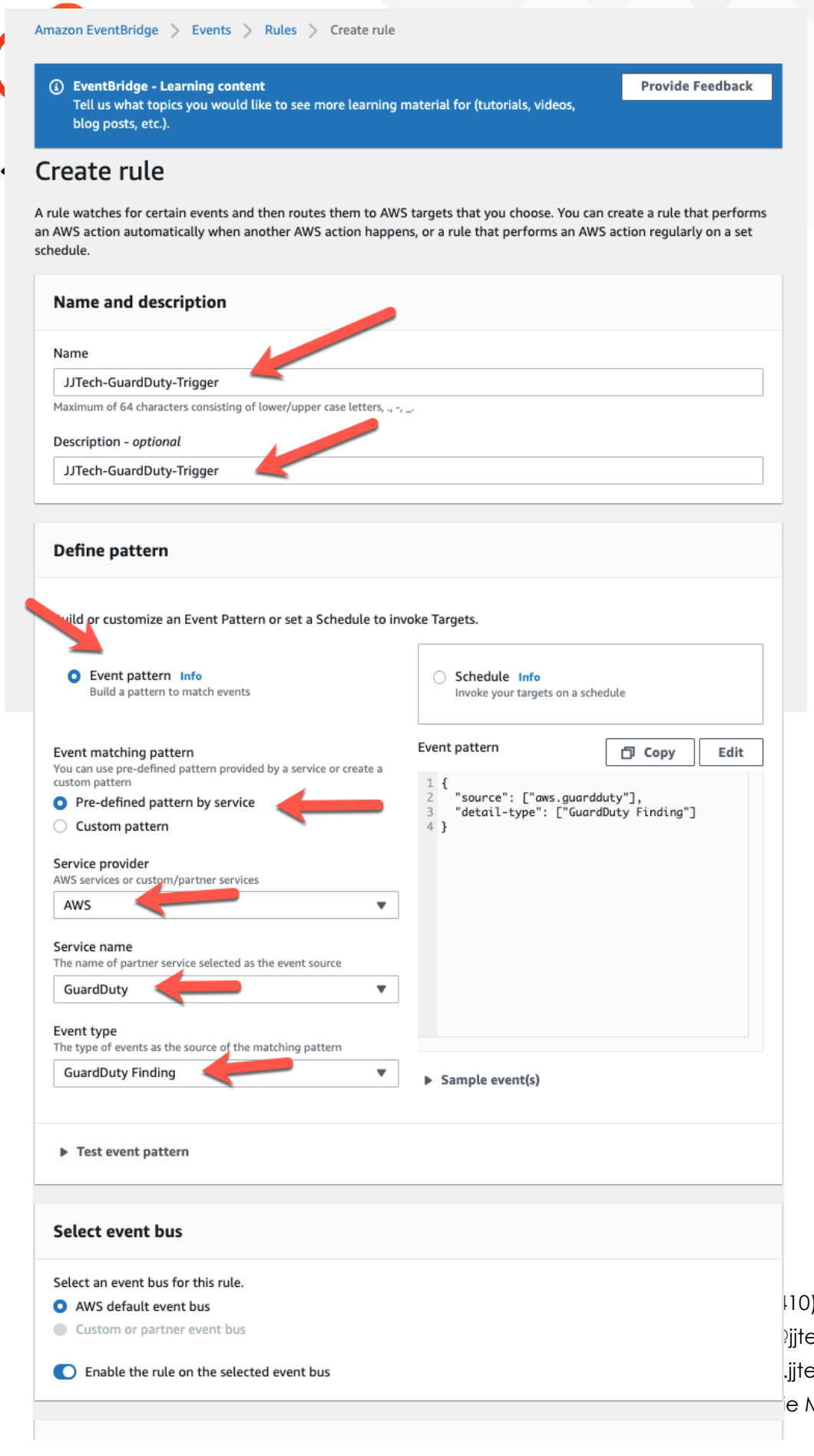
STEP 4: Create Cloudwatch rule to trigger the lambda

- 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

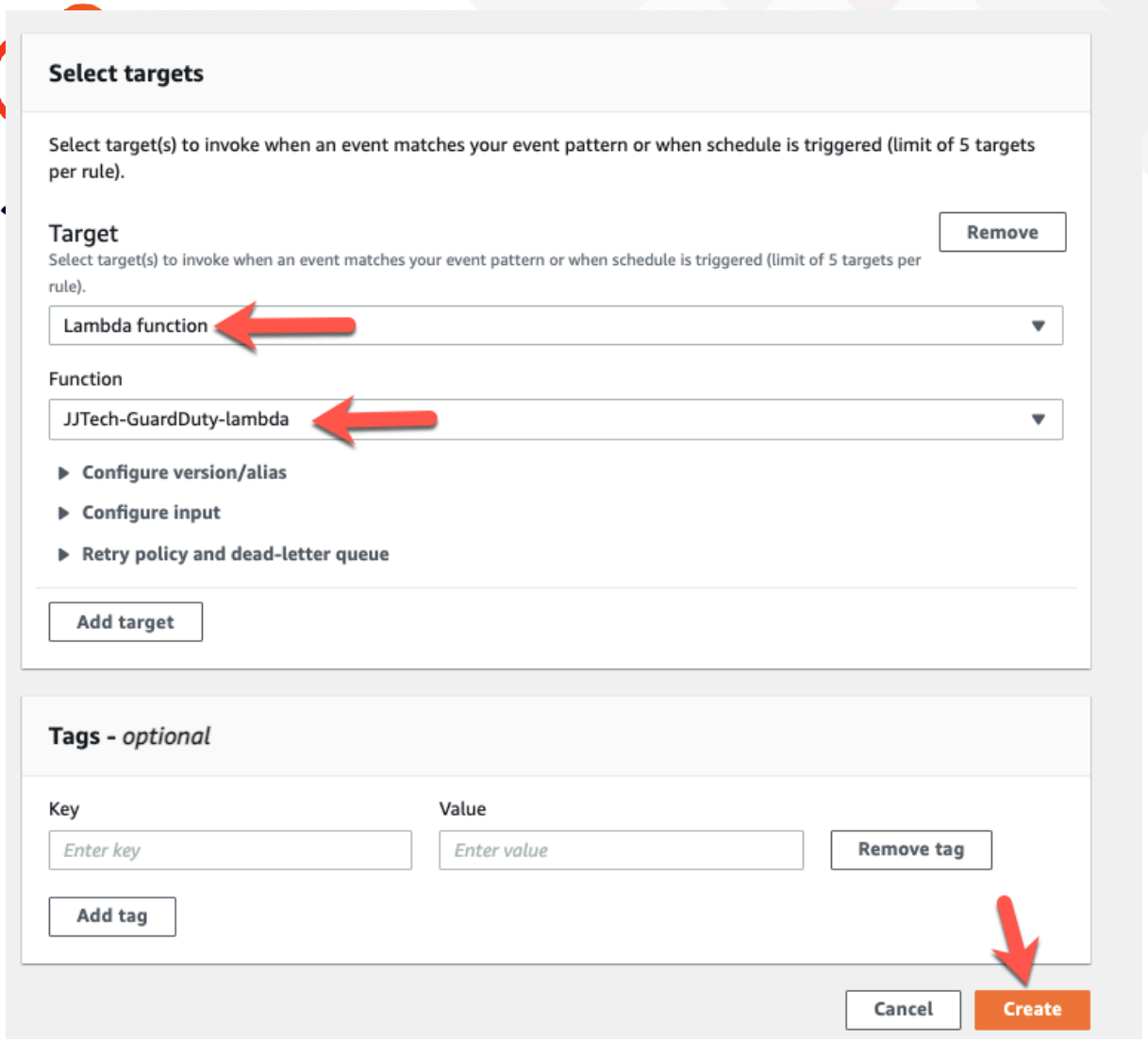
+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720



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

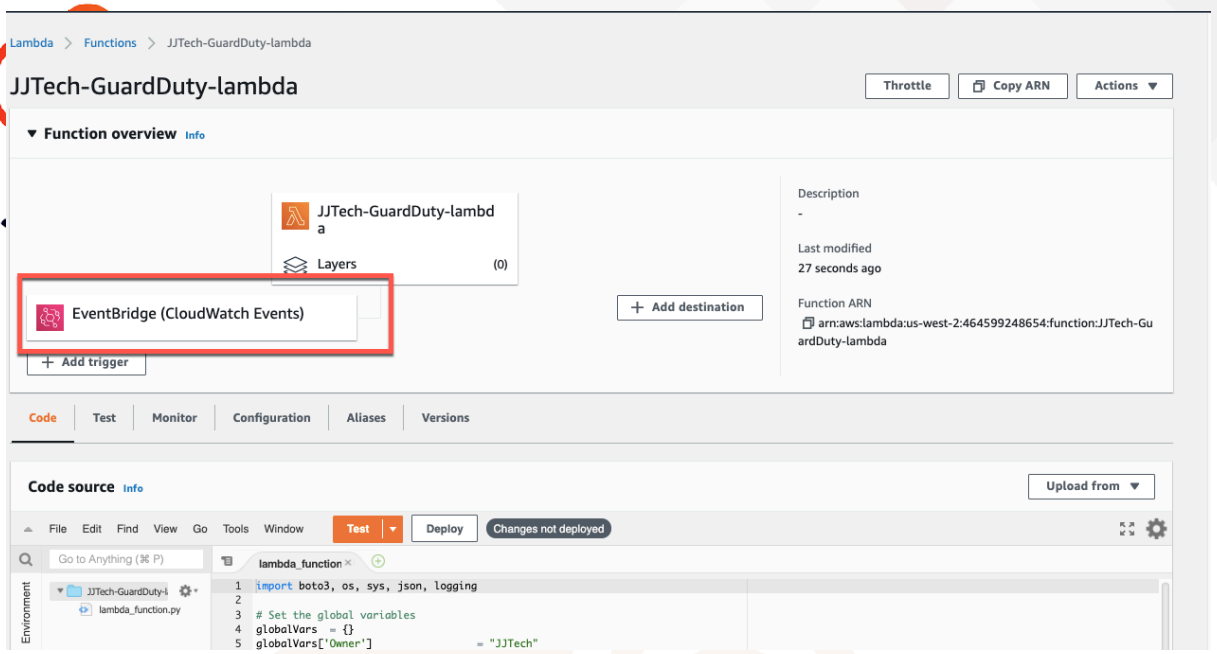


410) 8887049
jjtechinc.co
.jjtechinc.co
e MD 20720



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

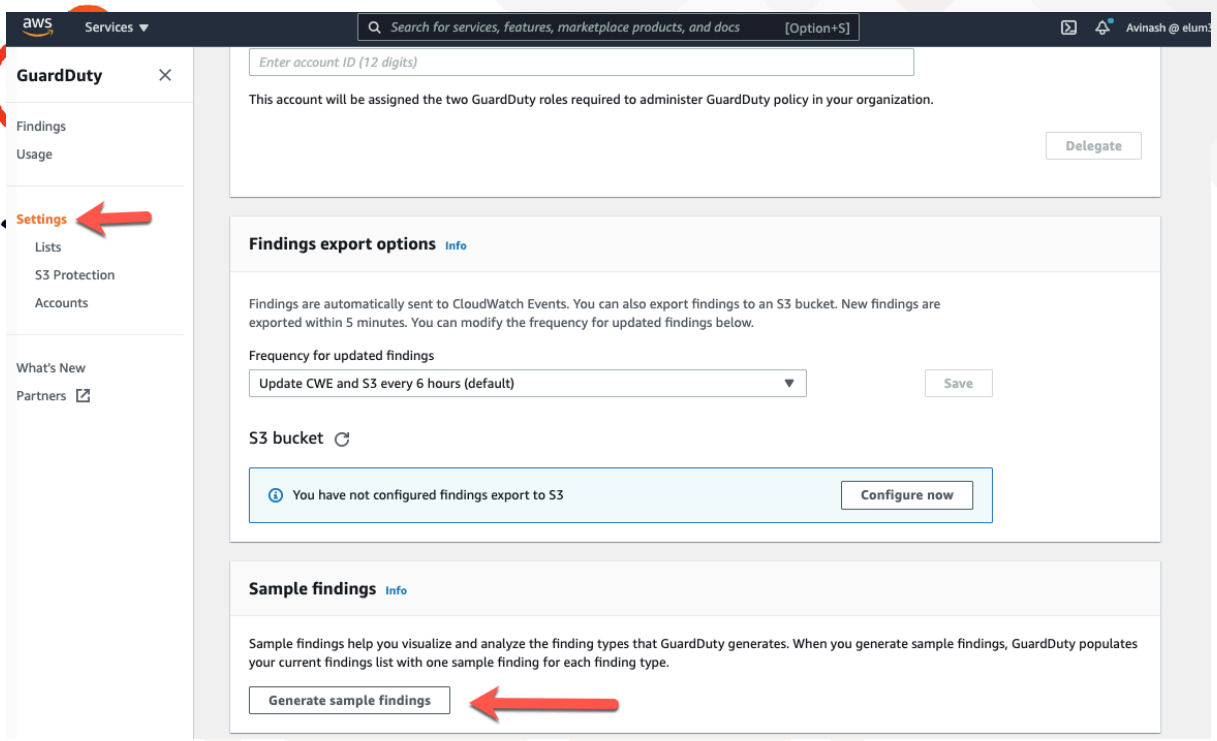
+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720

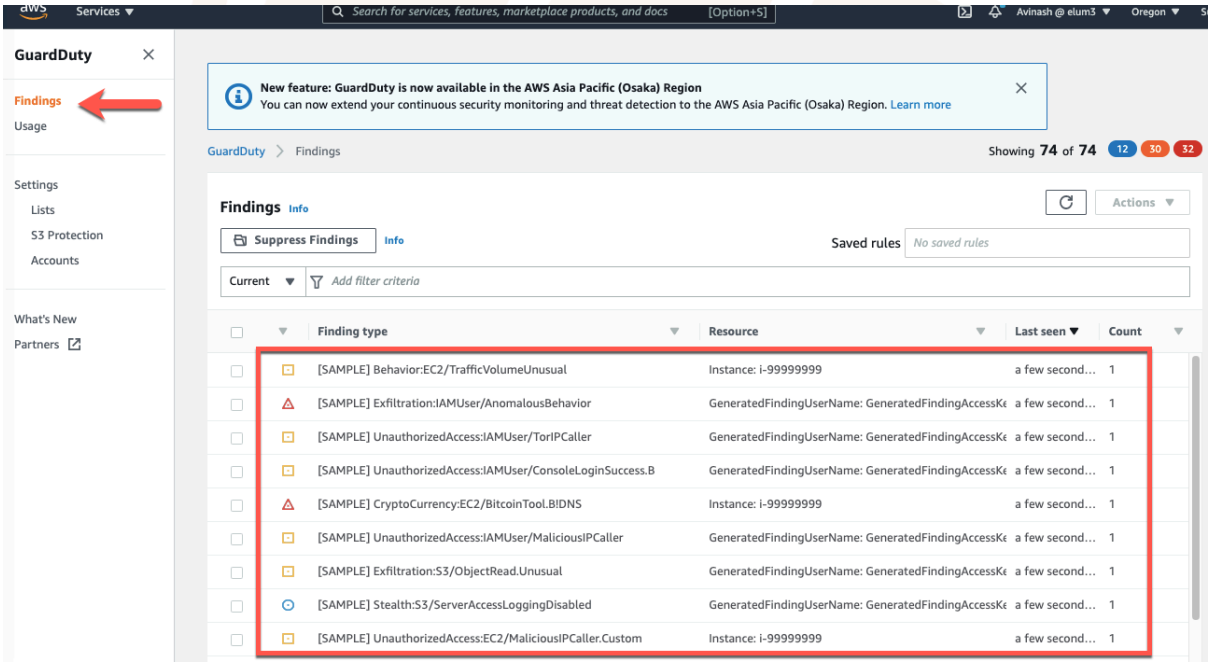


Step 5: Test the solution

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

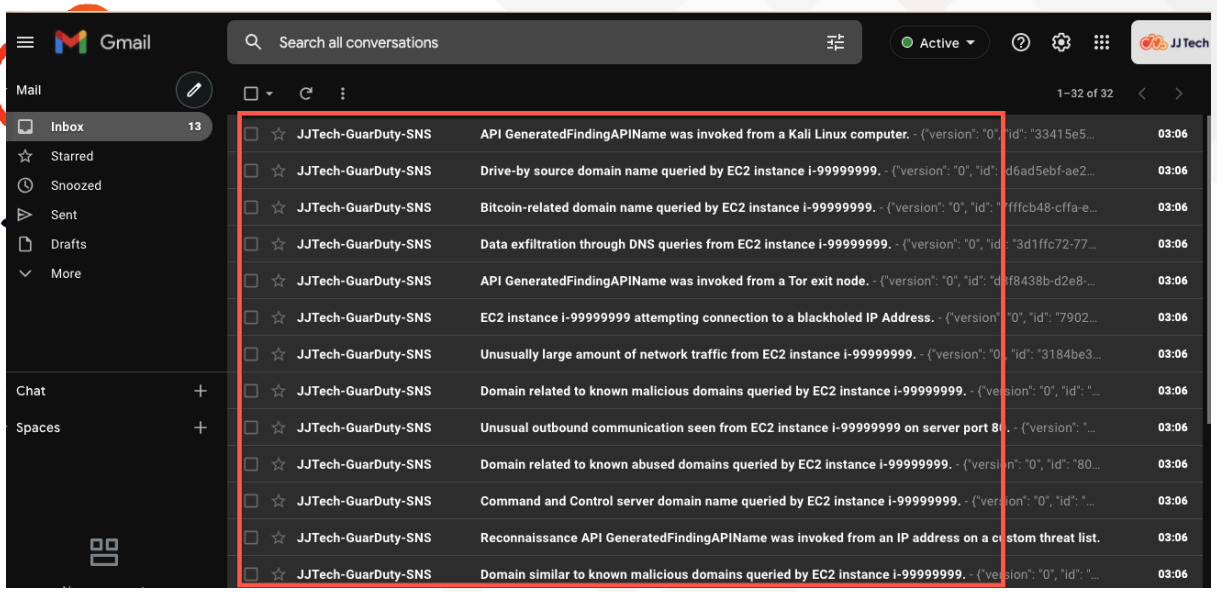
+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co
14103 Hammermil Field Dr Bowie MD 20720





- You will receive mails whenever new finding is available in GuardDuty
- Based on the issue you have to fix them

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



- 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