# **How to setup AWS Guard duty:**

1. Open the GuardDuty in AWS console.
2. Choose **Get Started**.
3. Choose **Enable GuardDuty**.

## **GuardDuty findings:**

When GuardDuty discovers a security issue it generates a finding. A GuardDuty finding is a data set containing details relating to that unique security issue. The finding's details can be used to help you investigate the issue.

## **Store finding logs in s3 bucket:**

1. Go to guardduty console.
2. In the navigation pane, choose **Settings**.
3. Under **Findings export options**, choose **Configure now**.
4. Choose bucket in which you want to store your finding logs.
5. In the navigation pane, choose **Settings**.
6. Under the **Sample findings** section, choose **Generate sample findings**. The new sample findings will appear within five minutes as entries in the S3 bucket.

## **Encrypt the findings:**

To encrypt the findings, you'll need a KMS key with a policy that allows GuardDuty to use that key for encryption.

1. Log into the AWS KMS keys console.
2. In the navigation pane, choose **Customer managed keys**.
3. Choose **Create key**.
4. Choose **Symmetric** under **Key type**, and then choose **Next**.
5. Provide an **Alias** for your key, and then choose **Next**.
6. Choose **Next**, and then again choose **Next** to accept the default administration and usage permissions.
7. Choose **Finish** to create the key.
8. Choose your key alias.
9. In the **Key policy** tab, attach the policy for guardduty which allows GuardDuty to use that key for encryption.

## **Set up GuardDuty finding alerts through SNS:**

GuardDuty integrates with Amazon EventBridge which can be used to send findings data to other applications and services for processing. With EventBridge you can use GuardDuty findings to trigger automatic responses to your findings by connecting finding events to Amazon Simple Notification Service (SNS) and more. EventBridge create a rule that captures findings data from GuardDuty. The resulting rule forwards the finding details to an email address.

**To create an SNS topic for your findings alerts:**

1. Go to Amazon SNS console.
2. In the navigation pane, choose **Topics**.
3. Choose **Create Topic**.
4. For **Type**, select **Standard**.
5. For **Name**, enter guardduty.
6. Choose **Create Topic**. The topic details for your new topic will open.
7. In the **Subscriptions** section, choose **Create subscription**.
8. For **Protocol**, choose **Email**.
9. For **Endpoint**, enter the email address to send notifications to.
10. Choose **Create subscription**.

After you create your subscription, you must confirm the subscription through email.

**To create an EventBridge rule to capture GuardDuty findings:**

1. Go to EventBridge console, choose **Rules**.
2. Choose **Create rule**.
3. Enter a name and description for the rule.

A rule can't have the same name as another rule in the same Region and on the same event bus.

1. For **Event bus**, choose **default**.
2. For **Rule type**, choose **Rule with an event pattern** then choose **Next**.
3. For **Event source**, choose **AWS events**.
4. For **Event pattern**, choose **Event pattern form**.
5. For **Event source**, choose **AWS services**.
6. For **AWS service**, choose **GuardDuty**.
7. For **Event Type**, choose **GuardDuty Finding** and Choose **Next**.
8. For **Target types**, choose **AWS service**.
9. For **Select a target**, choose **SNS topic**, and for **Topic**, choose the name of the SNS topic you created earlier.
10. In the **Additional settings** section, for **Configure target input**, choose **Input transformer**.

Adding an input transformer formats the JSON finding data sent from GuardDuty into a human-readable message.

1. Choose **Configure input transformer**.
2. In the **Target input transformer** section, for **Input path**, paste the following code:

{

"severity": "$.detail.severity",

"Finding\_ID": "$.detail.id",

"Finding\_Type": "$.detail.type",

"region": "$.region",

"Finding\_description": "$.detail.description"

}

1. To format the email, for **Template**, paste the following code:

"You have a severity <severity> GuardDuty finding type <Finding\_Type> in the <region> region."

"Finding Description:"

"<Finding\_description>. "

1. Choose **Confirm** and create rule.

**Guard Duty with 4 findings.**

