**Lab Steps**

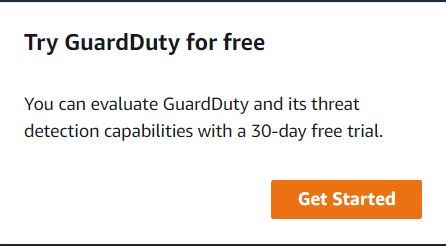
Task 1: Sign in to AWS Management Console

1. Click on the  button, and you will get redirected to AWS Console in a new browser tab.
2. On the AWS sign-in page,
   * Leave the Account ID as default. Never edit/remove the 12 digit Account ID present in the AWS Console. otherwise, you cannot proceed with the lab.
   * Now copy your **User Name** and **Password** in the Lab Console to the **IAM Username and Password** in AWS Console and click on the **Sign in** button.
3. Once Signed In to the AWS Management Console, Make the default AWS Region as **US East (N. Virginia) us-east-1.**

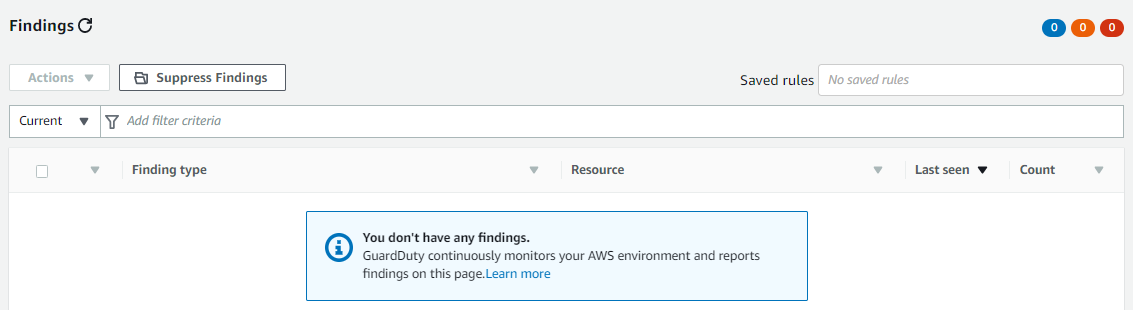
**Note: There is no Validation function for this lab.**

Task 2: Enabling Amazon GuardDuty

1. Make sure to choose the **US East (N. Virginia) us-east-1** region in the AWS Management console dashboard, which is present in the top right corner.
2. Navigate to the  menu at the top and click on **GuardDuty** in the **Security, Identity and Compliance** section.
3. Click on **Get started**.



1. Click on . With one click, the service will be enabled.



1. In the **Findings** page, you will see the warning **You don’t have any findings** because there is no malicious activity happening in your AWS Account. **Ignore** the warnings, wherever you find.

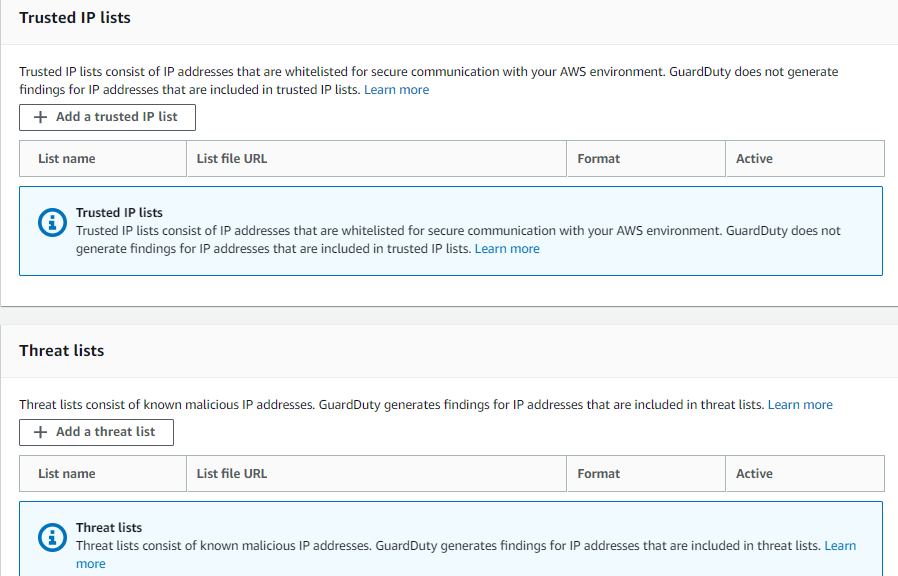
Task 3: Exploring Amazon GuardDuty

Settings

1. Click on **Settings** in the left panel.
2. You will see a **Detector ID**.  A detector is a resource that represents the GuardDuty service.
3. **Permissions**: GuardDuty uses a service role to monitor your data sources on your behalf.
4. Findings export options: Findings are automatically sent to CloudWatch Events. You can also export findings to an S3 bucket. New findings are exported within 5 minutes. No need to change anything.
5. Suspend GuardDuty:
   * **Suspend GuardDuty**: When you suspend GuardDuty, it stops monitoring your AWS environment and doesn't generate new findings. Your existing findings remain intact and aren't affected.
   * **Disable GuardDuty**: When you disable GuardDuty, you not only stop GuardDuty from monitoring your AWS environment and generating new findings, you also lose your existing findings and your GuardDuty configurations. You can’t recover the data later.

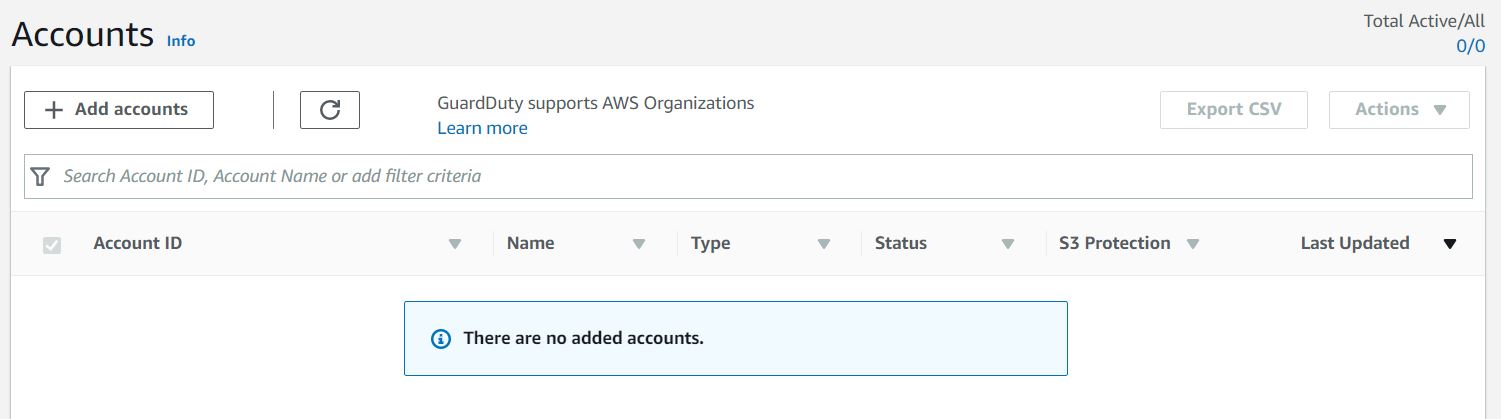
Lists

1. Click on **Lists** below **Settings**.
2. In the List Manager, you can add the Trusted IP Lists and Threat Lists.
3. **Trusted IP Lists**: Trusted IP lists consist of IP addresses that are whitelisted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists.
4. **Threat Lists**: Threat lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat lists.



Accounts

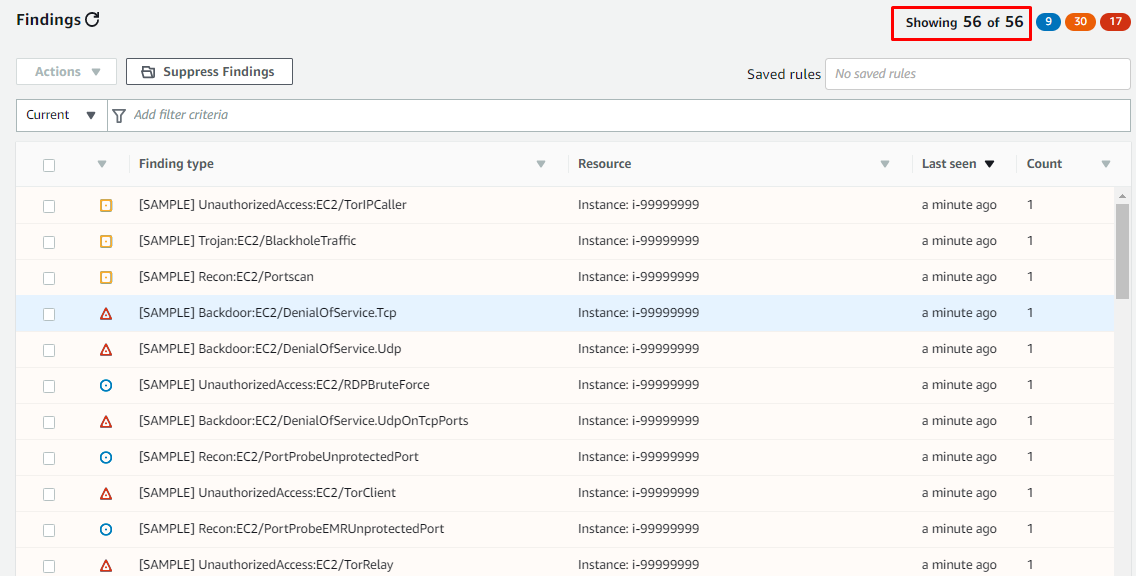
1. Click on **Accounts** below Lists.



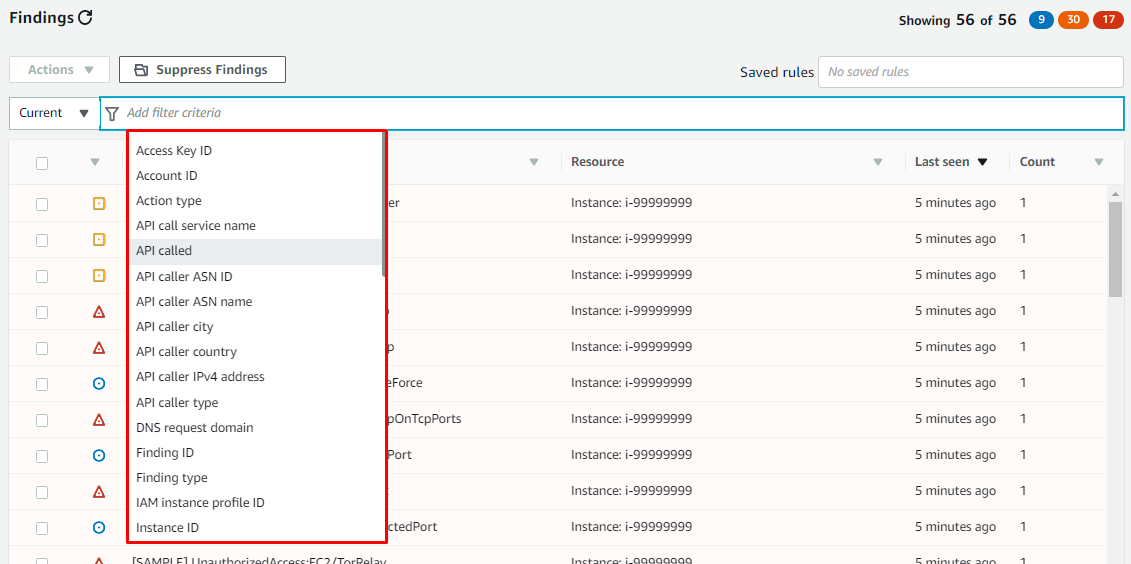
1. You can invite other accounts to enable GuardDuty and become associated with your AWS account.
2. When an invitation is accepted, your account is designated as the **master** GuardDuty account.
3. The account that accepts the invitation becomes a **member** account associated with your master account.
4. You can then view and manage the GuardDuty findings on behalf of the member account. In GuardDuty, a master account (per region) can have up to 1000 member accounts.

Task 4: Generating Sample Findings

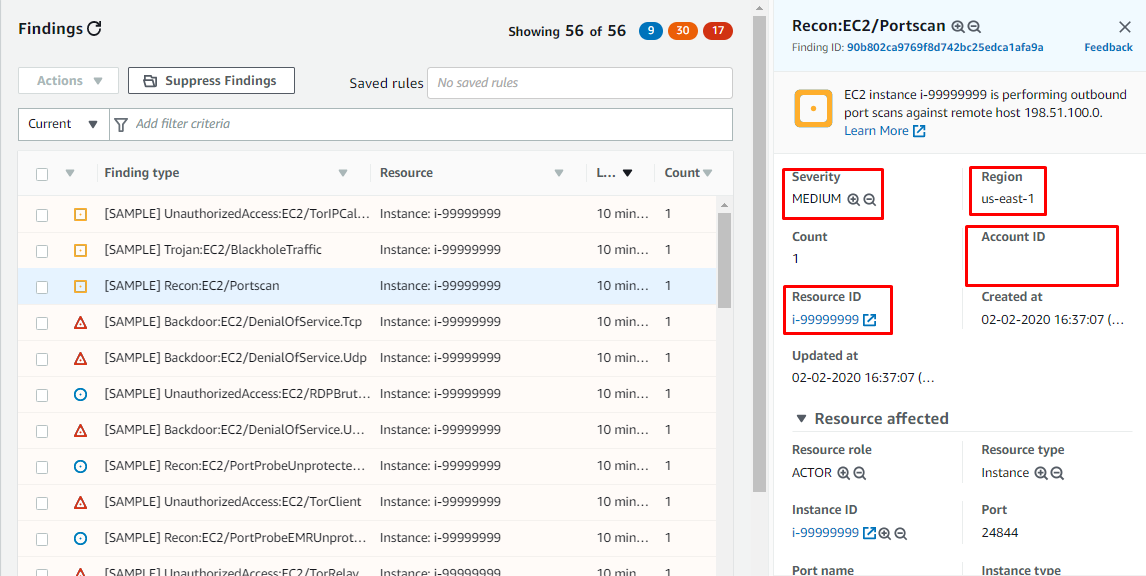
1. Since there are no potential threats in our AWS Account, let us generate some sample findings and learn about them.
2. Navigate to settings, scroll down and click on **Generate sample findings.**
3. To find your sample findings, go to **Findings**.
4. Wait until the loading is completed. On the top-right corner, you should see a number of findings.



1. On the Top-right corner, you can see numbers with colors .
2. Color Indications:
   * The **Blue** indicates **Low severity**
   * **Orange** indicates **Medium severity**
   * **Red** indicates **High severity**
3. You can use filter criteria to filter your findings.



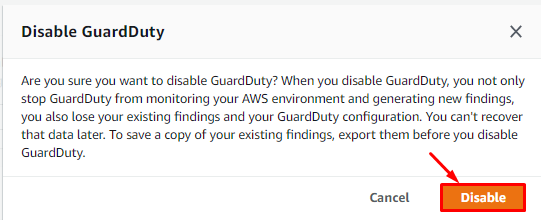
1. Click on one of the sample findings.
2. You can see various parameters like **severity, region, Account ID, Resource ID, Resource Affected, Target, etc**.



1. Go through the sample to learn more about the different severities.

Task 5: Disabling GuardDuty

1. Go to the settings and click on  under suspend GuardDuty to stop it.
2. Click on **Disable** to confirm.

****

1. You have successfully disabled GuardDuty.

**Completion and Conclusion**

* You have successfully used the AWS management console to enable Amazon GuardDuty.
* You have successfully explored the options of Amazon GuardDuty Service like  Settings, Lists, and Accounts.
* You have generated some sample findings and reviewed them.
* You have successfully disabled Amazon GuardDuty.

**End Lab**