Home / AWS / Guided Lab / Introduction to Amazon GuardDuty

Introduction to Amazon GuardDuty

Level: **Fundamental**

Amazon Web Services   Amazon GuardDuty

0h 20m 8s left

15 MIN

End Lab

Open Console

Validation

Lab Credentials

User Name

Whiz_User_80425.26221120

Password

4ded46a3-985f-4ef2-86f4-dd5328088e1a

Access Key

AKIAQ66O26BYOQF7TIQA

Secret Key

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

Lab Resources

No Lab Resources Found

Support Documents

ns

Need help?

- How to use Hands on Lab
- Troubleshooting Lab
- FAQs

Submit Feedback | Share

Lab Overview | Lab Steps | Lab Validation

Cloud Security Engineer

Security

Lab Details

1. This lab walks you through the steps to enable GuardDuty and create some sample

WHIZLABS 0 K

3. Duration: **30 minutes**

4. AWS Region: **US East (N. Virginia) us-east-1**

Introduction

What is AWS GuardDuty ?

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.

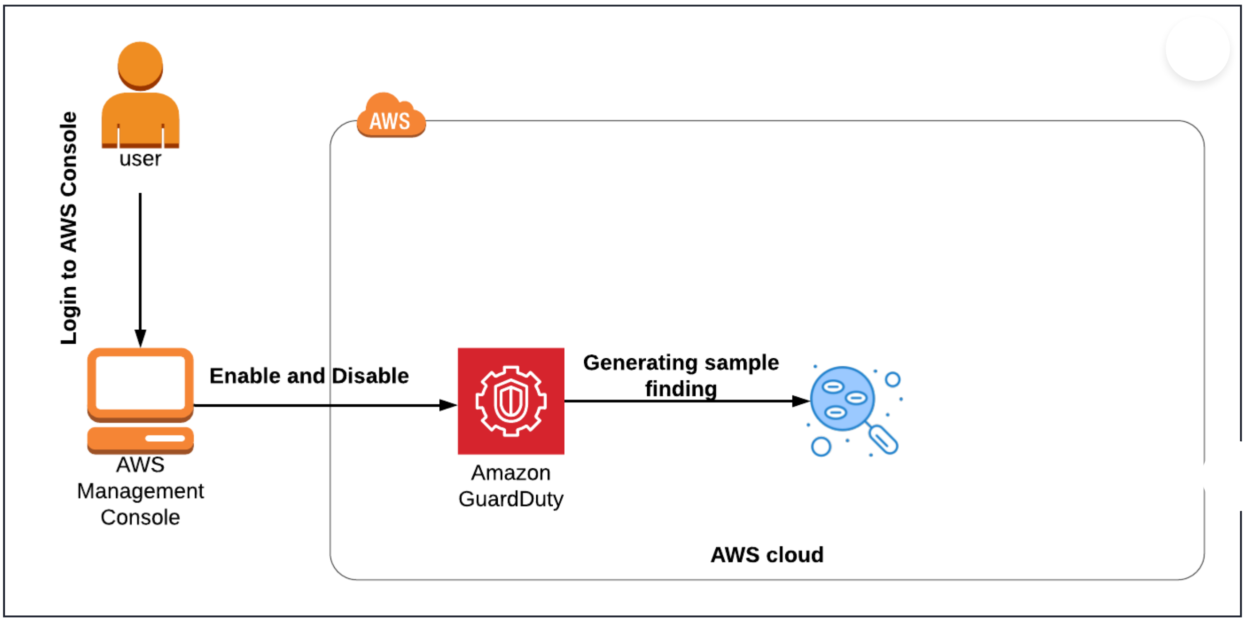
GuardDuty uses machine learning, anomaly detection, and threat intelligence to identify and prioritize potential threats. It can detect a wide range of threats, including:

- Unauthorized access to your AWS resources
- Suspicious network activity
- Malware infections
- Data exfiltration
- Account takeovers

Here are some of the benefits of using Amazon GuardDuty:

- Continuous monitoring: GuardDuty continuously monitors your AWS environment for malicious activity, 24/7. This helps you to identify threats early, before they can cause damage.
- Detailed security findings: GuardDuty provides detailed security findings that include information about the threat, the affected resources, and recommended actions. This makes it easy to investigate and remediate threats.
- Integration with other AWS services: GuardDuty integrates with other AWS services, such as AWS Security Hub and Amazon Detective, to help you investigate and respond to threats.
- Cost-effective: GuardDuty is a cost-effective way to protect your AWS environment from threats. There is no upfront cost, and you only pay for the resources that you use.

Architecture Diagram



Task Details

1. Sign into AWS Management Console.
2. Enable Amazon GuardDuty**.**
3. Explore the Amazon GuardDuty service.
4. Generate Sample findings and understand them.
5. Disable Amazon GuardDuty.

Launching Lab Environment

1. To launch the lab environment, Click on the **Start Lab** button.
2. Please wait until the cloud environment is provisioned. It will take less than a minute to provision.
3. Once the Lab is started, you will be provided with **IAM user name**, **Password**, **Access Key**, and **Secret Access Key**.

Note : You can only start one lab at any given time