# D Y Patil International University

## School of Computer Science, Engineering, and Applications

## Academic Year 2022-2023

## Practical Assignment No. 3

**Class: MCA-SEM III** **Subject: Computer Forensics**

**Date 26 / 10 /2023**

**Name: - Udayan Mukund Pawar**

**PRN No.: - 20220804032**

**Experiments:**

**Aim:** Find the Vulnerabilities on EC2 instance using amazon Inspector

**What is AWS?**

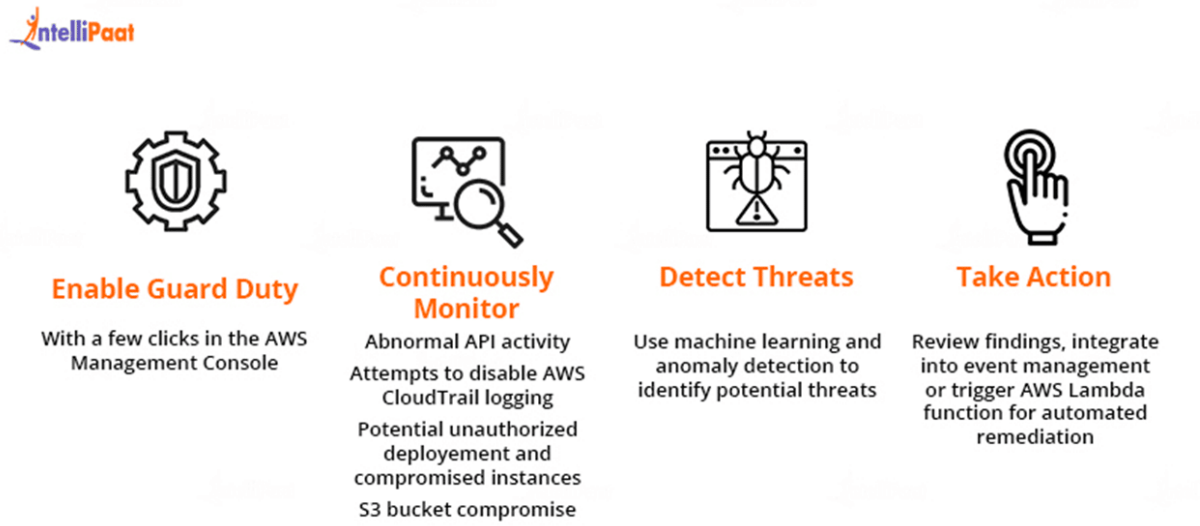
AWS (Amazon Web Services) is a comprehensive, evolving cloud computing platform provided by Amazon that includes a mixture of infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and packaged-software-as-a-service (SaaS) offerings. AWS services can offer an organization tools such as compute power, database storage and content delivery services.

Amazon.com Web Services launched its first web services in 2002 from the internal infrastructure that Amazon.com built to handle its online retail operations. In 2006, it began offering its defining IaaS services. AWS was one of the first companies to introduce a pay-as-you-go cloud computing model that scales to provide users with compute, storage or throughput as needed.

AWS offers many different tools and solutions for enterprises and software developers that can be used in data centers in up to 190 countries. Groups such as government agencies, education institutions, non-profits and private organizations can use AWS services.

**AWS Guard Duty**

This service allows customers to analyze AWS CloudTrail Event Logs, VPC Flow Logs, and DNS Logs to look for unusual or unexpected behavior in their AWS accounts. It then compares the log data to numerous security and threat detection feeds, searching for anomalies and known harmful sources such as IP addresses and URLs.




GuardDuty secures workloads and data on AWS by leveraging both AWS-developed and industry-leading third-party sources. It integrates machine learning, anomaly detection, network monitoring, and the detection of dangerous files.

Tens of billions of events per second can be analyzed by GuardDuty from a variety of AWS data sources, including DNS query logs, Amazon VPC flow logs, Amazon Elastic Kubernetes Service (Amazon EKS) audit logs, and AWS CloudTrail event logs.

In your accounts, Amazon GuardDuty notices unusual activity, assesses its security significance, and gives context. This makes it possible for a respondent to decide whether a follow-up query is necessary.

GuardDuty's results are ranked in terms of their seriousness, and by connecting with AWS Security Hub, Amazon EventBridge, AWS Lambda, and AWS Step Functions, actions can be automated.

**Procedure:-**

**Step 1: Enable Amazon GuardDuty**

**Step 2: Generate sample findings and explore basic operations**

1. In the navigation pane, choose Settings.
2. On the Settings page, under Sample findings, choose Generate sample findings.
3. In the navigation pane, choose Summary to view the insights about the findings generated in your AWS environment. For more information about the components of the Summary dashboard, see Summary dashboard.
4. In the navigation pane, choose Findings. The sample findings are displayed on the Current findings page with the prefix [SAMPLE].

5. Select a finding from the list to display details for the finding.

**Step 3: Configure exporting GuardDuty findings to an Amazon S3 bucket**

1. To encrypt the findings, you'll need a KMS key with a policy that allows GuardDuty to use that key for encryption. The following steps will help you create a new KMS key. If you are using a KMS key from another account, you need to apply the key policy by logging in to the AWS account that owns the key. The Region of your KMS key and S3 bucket must be the same. However, you can use this same bucket and key pair for each Region from where you want to export findings.

a) Open the AWS KMS console at https://console.aws.amazon.com/kms.

b) To change the AWS Region, use the Region selector in the upper-right corner of the page.

c) In the navigation pane, choose **Customer managed keys**.

d) Choose **Create key**.

e) Choose **Symmetric** under **Key type**, and then choose **Next**.

f) Provide an Alias for your key, and then choose Next.

g) Choose Next, and then again choose Next to accept the default administration and usage permissions.

h) After you Review the configuration, choose Finish to create the key.

i) On the Customer managed keys page, choose your key alias.

j) In the Key policy tab, choose Switch to policy view.

k) Choose Edit and add the following key policy to your KMS key, granting GuardDuty access to your key. This statement allows GuardDuty to use only the key to which you add this policy. When editing the key policy, ensure that the JSON syntax is valid. If you add the statement before the final statement, you must add a comma after the closing bracket.

l) Choose Save.

2. Open the GuardDuty console at https://console.aws.amazon.com/guardduty/.
3. In the navigation pane, choose **Settings**.
4. Under **Findings export options**, choose **Configure now**.
5. Choose **New bucket**. Provide a unique name for your S3 bucket.
6. (Optional) you can test your new export settings by generating sample findings. In the navigation pane, choose **Settings**.
7. Under the **Sample findings** section, choose **Generate sample findings**. The new sample findings will appear as entries in the S3 bucket created by GuardDuty in up to five minutes.

**Step 4: Set up GuardDuty finding alerts through SNS**

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

1. Open the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
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.

11. To check for a subscription message, go to your email inbox, and in the subscription message, choose **Confirm subscription**.

**To create an EventBridge rule to capture GuardDuty findings and format them**

1. Open the EventBridge console at https://console.aws.amazon.com/events/.
2. In the navigation pane, choose **Rules**.
3. Choose **Create rule**.
4. 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.
5. For **Event bus**, choose **default**.
6. For **Rule type**, choose **Rule with an event pattern**.
7. Choose **Next**.
8. For **Event source**, choose **AWS events**.
9. For **Event pattern**, choose **Event pattern form**.
10. For **Event source**, choose **AWS services**.
11. For **AWS service**, choose **GuardDuty**.
12. For **Event Type**, choose **GuardDuty Finding**.
13. Choose **Next**.
14. For **Target types**, choose **AWS service**.
15. For **Select a target**, choose **SNS topic**, and for **Topic**, choose the name of the SNS topic you created earlier.

16. 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.
17. Choose **Configure input transformer**.
18. 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"
}
```

19. 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>. "

"For more details open the GuardDuty console at
https://console.aws.amazon.com/guardduty/home?region=<region>#/findings?search=id
%3D<Finding_ID>"
```

20. Choose **Confirm**.
21. Choose **Next**.
22. (Optional) Enter one or more tags for the rule. For more information, see Amazon EventBridge tags in the *Amazon EventBridge User Guide*.
23. Choose **Next**.
24. Review the details of the rule and choose **Create rule**.

25. (Optional) Test your new rule by generating sample findings with the process in Step 2. You will receive an email for each sample finding generated.

**Result: -**

AWS Guard Duty Launch Successfully.