VISVESVARAYA TECHNOLOGICAL UNIVERSITY,
BELAGAVI - 590018

Internship Seminar Report on

"THREAT MODELLING IN IT"

Submitted in partial fulfillment of the requirements as per VTU curriculum of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE & ENGINEERING

By

ABHISHEK P **4AL20CS003**

Under the Guidance of

Dr. Bramha Prakash H P
Associate Professor

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY
MOODBIDRI-574225, KARNATAKA

2023– 2024

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MIJAR, MOODBIDRI D.K. -574225

KARNATAKA

ALVA'S

Education Foundation®

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CERTIFICATE

This is to certify that the Internship report on **"THREAT MODELLING IN IT"** submitted by **ABHISHEK P (4AL20CS003)** is work done by him and submitted during the academic year 2023–24, in partial fulfilment of the requirements for the award of the degree of BACHELOR OF ENGINEERING in COMPUTER SCIENCE AND ENGINEERING

BP

Dr. Bramha Prakash H P
Mentor

BP 14/5/24.

Dr. Bramha Prakash H P
Internship Coordinator

Dr. Manjunath Kotari
Professor and Head of Department

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany a successful completion of any task would be incomplete without the mention of people who made it possible, success is the epitome of hard work and perseverance, but steadfast of all is encouraging guidance.

First I would like to thank **CySecK** for giving me the opportunity to do an internship within the organization.

I sincerely thank, **Dr. Bramha Prakash H P**, Associate Professor , Department of Computer Science & Engineering who has been the constant driving force behind the completion of the seminar.

The selection of Technical Seminar Topic as well as the timely completion is mainly due to the interest and persuasion of my Seminar Coordinator **Dr. Bramha Prakash H P ,** Associate Professor, Department of Computer Science & Engineering. He has been especially enthusiastic in giving his valuable guidance and critical reviews. I will remember his contribution for ever.

I sincerely thank, **Dr. Manjunath Kotari**, Professor and Head, Department of Computer Science & Engineering who has been the constant driving force behind the completion of the seminar.

I thank Principal **Dr. Peter Fernandes,** for his constant help and support throughout.

I am also indebted to **Management of Alva's Institute of Engineering and Technology, Mijar, Moodbidri** for providing an environment which helped me in completing the seminar.

Also, I thank all the teaching and non-teaching staff of Department of Computer Science & Engineering for the help rendered.

Finally I would like to thank my parents and friends whose encouragement and support was invaluable.

ABHISHEK P 4AL20CS003

K-tech

CySecK | K-Tech CoE for Cyber Security

Trisakha foundation

ALVA'S

CERTIFICATE

OF ACHIEVEMENT

This is to certify that

Abhishek P.

has successfully completed the training and the post-training assessment during the

Cyber Security Finishing School (CSFS) Programme

conducted at Alva's Institute of Engineering and Technology, Shobhavana campus, Mijar.

Date: 19-February-2024 to 22-March-2024

Promila Malik

Promila Malik
Managing Trustee, Trisakha Foundation

Karthik Rao Bappanad
Centre Head, CySecK

Prof. Peter Fernandes
Principal, Alva's Institute of Engineering and Technology

ABSTRACT

Insider threats, malicious or negligent actions by authorized users, pose a significant risk to cloud environments like AWS. Their trusted access makes them particularly dangerous. This abstract explores the challenges of detecting and responding to insider threats in AWS. The shared responsibility model in AWS places the onus of securing data and resources on the customer. The complexity of AWS environments, with its vast array of services and configurations, further hinders complete activity visibility. To address detection, the abstract highlights tools like CloudTrail for logging API calls, GuardDuty for threat intelligence analysis, Config for monitoring configuration changes, and Macie for sensitive data discovery. Additionally, robust IAM policies, user activity monitoring, and data encryption are emphasized. For response strategies, the abstract stresses the importance of a well-defined incident response plan encompassing containment, eradication, and recovery. It also advocates for proactive threat hunting and user education on security best practices. AWS's detection and response services like CloudTrail, GuardDuty, Config, and Macie, which, when combined, create a comprehensive security posture. By implementing these techniques, organizations can significantly reduce the risk of insider threats in their AWS environments. However, security is an ever-evolving battleground, necessitating continuous monitoring and adaptation of security practices.

DAILY LOGS

DAY	DATE	TOPICS COVERED
1-6	22/03/2024 – 27/03/20204	Information Security Basics & AWS Cloud Fundamentals
7-12	29/03/20204 – 03/04/2024	Network Security & Incident Management
13-18	05/04/2024 – 10/04/2024	Advanced Threat Detection in AWS
19-24	12/042024 – 17/04/2024	Cybersecurity Tools, Automation, and Compliance
25-31	18/04/2024 – 22/04/2024	Capstone Project and Case Studies

LIST OF FIGURES

Table of Content

CHAPTER I

INTRODUCTION

In today's rapidly evolving digital landscape, the importance of cybersecurity cannot be overstated. As technology advances, so do the threats that organizations face in safeguarding their sensitive information and critical systems. Threat modeling is a proactive approach to cybersecurity, providing a structured methodology for identifying, prioritizing, and mitigating potential threats to IT systems.

What is threat modelling in IT?

Threat modeling is a systematic process for identifying and prioritizing potential threats to IT systems, applications, or networks. It involves analyzing the security posture of an organization's assets and infrastructure to identify vulnerabilities and potential attack vectors. By understanding the various threats that may target an organization, security professionals can develop proactive measures to mitigate risks and enhance overall security.

The process of threat modeling typically involves several key steps:

Identifying Assets: The first step in threat modeling is to identify the assets that need protection. This includes sensitive data, critical systems, and infrastructure components that are vital to the organization's operations.

Identifying Threats: Once the assets are identified, the next step is to identify potential threats that may target these assets. Threats can come from various sources, including malicious actors, natural disasters, or inadvertent human error.

Assessing Vulnerabilities: With the threats identified, the next step is to assess the vulnerabilities that could be exploited by these threats. Vulnerabilities may exist in software, hardware, or human processes and can range from outdated software to weak authentication mechanisms.

Prioritizing Risks: Not all threats pose an equal risk to an organization. Threat modeling helps prioritize risks based on their likelihood and potential impact on the organization. This allows security professionals to focus their efforts on addressing the most significant threats first.

Mitigation Strategies: Once risks are prioritized, the final step is to develop mitigation strategies to address the identified threats and vulnerabilities. This may involve implementing security controls, conducting security awareness training, or updating policies and procedures to improve security posture.

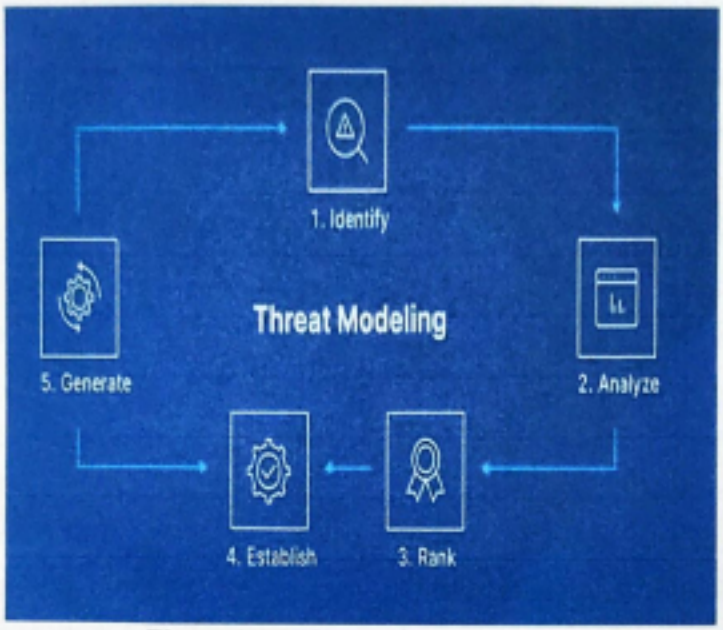

Figure 1.1 : Threats due to Insiders

CHAPTER 2

THREAT DETECTION TECHNIQUES

Threats lurk around every corner in the digital world, and cloud environments like AWS are no exception. Here's a comprehensive dive into threat detection in AWS, helping you secure your valuable data and resources.

1. **Amazon GuardDuty:**

Amazon GuardDuty is a security monitoring service that analyses and processes Foundational data sources, such as AWS CloudTrail management events, AWS CloudTrail event logs, VPC flow logs (from Amazon EC2 instances), and DNS logs. It also processes Features such as Kubernetes audit logs, RDS login activity, S3 logs, EBS volumes, Runtime monitoring, and Lambda network activity logs. It uses threat intelligence feeds, such as lists of malicious IP addresses and domains, and machine learning to identify unexpected, potentially unauthorized, and malicious activity within your AWS environment. This can include issues like escalation of privileges, use of exposed credentials, or communication with malicious IP addresses, domains, pre sence of malware on your Amazon EC2 instances and container workloads, or discovery of unusual patterns of login events on your database. For example, GuardDuty can detect compromised EC2 instances and container workloads serving malware, or mining bitcoin. It also monitors AWS account access behaviour for signs of compromise, such as unauthorized infrastructure deployments, like instances deployed in a Region that hasn't been used before, or unusual API calls like a password policy change to reduce password strength. GuardDuty informs you of the status of your AWS environment by producing security findings that you can view in the GuardDuty console or through Amazon Event Bridge. GuardDuty also provides support for you to export your findings to an Amazon Simple Storage Service (S3) bucket, and integrate with other services such as AWS Security Hub and Detective.

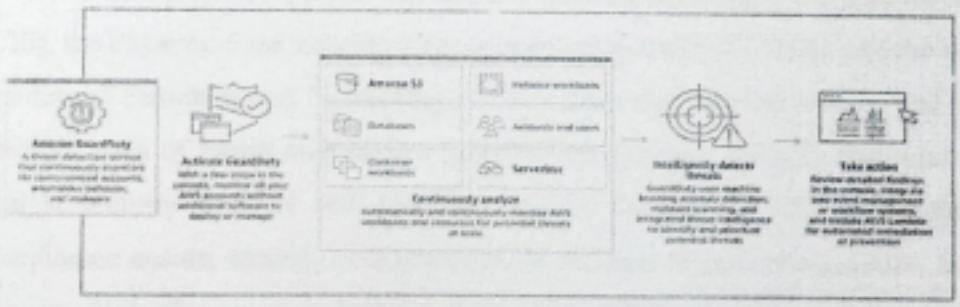

Figure 2.1: Guard Duty Working

2. **AWS Cloud Trail:**

AWS CloudTrail is an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs. CloudTrail is active in your AWS account when you create it and doesn't require any manual setup. When activity occurs in your AWS account, that activity is recorded in a CloudTrail event.

Figure 2.2: Cloud Trail

3. **AWS Security Hub:**

AWS Security Hub provides you with a comprehensive view of your security state in AWS and helps you assess your AWS environment against security industry standards and best practices. Security Hub collects security data across AWS accounts, AWS services, and supported third-party products and helps you analyse your security trends and identify the highest priority security issues. To help you manage the security state of your organization, Security Hub supports multiple security standards. These include the AWS Foundational Security Best Practices (FSBP) standard developed by AWS, and external compliance frameworks such as the Center for Internet Security (CIS), the Payment Card Industry Data Security Standard (PCI DSS), and the National Institute of Standards and Technology (NIST). Each standard includes several security controls, each of which represents a security best practice. Security Hub runs checks against security controls and generates control findings to help you assess your compliance against security best practices. In addition to generating control findings, Security Hub also receives findings from other AWS services—such as Amazon

GuardDuty, Amazon Inspector, and Amazon Macie— and supported third-party products. This gives you a single pane of glass into a variety of security-related issues. You can also send Security Hub findings to other AWS services and supported third-party products. Security Hub offers automation features that help you triage and remediate security issues. For example, you can use automation rules to automatically update critical findings when a security check fails. You can also leverage the integration with Amazon Event Bridge to trigger automatic responses to specific findings.

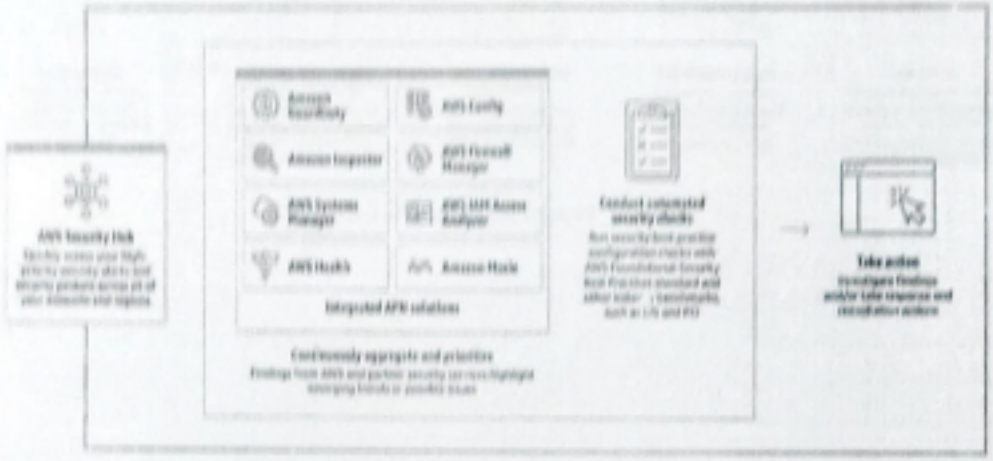

Figure 2.3: AWS Security Hub

4. Amazon Macie

Amazon Macie is a data security service that discovers sensitive data by using machine learning and pattern matching, provides visibility into data security risks, and enables automated protection against those risks. To help you manage the security posture of your organization's Amazon Simple Storage Service (Amazon S3) data estate, Macie provides you with an inventory of your S3 buckets, and automatically evaluates and monitors the buckets for security and access control. If Macie detects a potential issue with the security or privacy of your data, such as a bucket that becomes publicly accessible, Macie generates a finding for you to review and remediate as necessary. Macie also automates discovery and reporting of sensitive data to provide you with a better understanding of the data that your organization stores in Amazon S3. To detect sensitive data, you can use built-in criteria and techniques that Macie provides, custom criteria that you define, or a combination of the two. If Macie detects sensitive data in an S3 object, Macie generates a finding to notify you of the sensitive data that Macie found. In addition to findings, Macie provides statistics and other data that offer insight

into the security posture of your Amazon S3 data, and where sensitive data might reside in your data estate. The statistics and data can guide your decisions to perform deeper investigations of specific S3 buckets and objects. You can review and analyze findings, statistics, and other data by using the Amazon Macie console or the Amazon Macie API. You can also leverage Macie integration with Amazon EventBridge and AWS Security Hub to monitor, process, and remediate findings by using other services, applications, and systems.

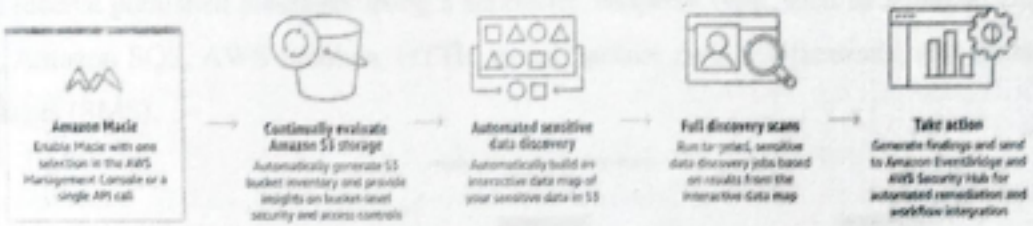

Figure 2.4: Amazon Macie

CHAPTER 3

THREAT RESPONSE TECHNIQUES

1. SIMPLE NOTIFICATION SERVICE

Amazon Simple Notification Service (Amazon SNS) is a managed service that provides message delivery from publishers to subscribers (also known as producers and consumers). Publishers communicate asynchronously with subscribers by sending messages to a topic, which is a logical access point and communication channel. Clients can subscribe to the SNS topic and receive published messages using a supported endpoint type, such as Amazon Data Firehose, Amazon SQS, AWS Lambda, HTTP, email, mobile push notifications, and mobile text messages (SMS).

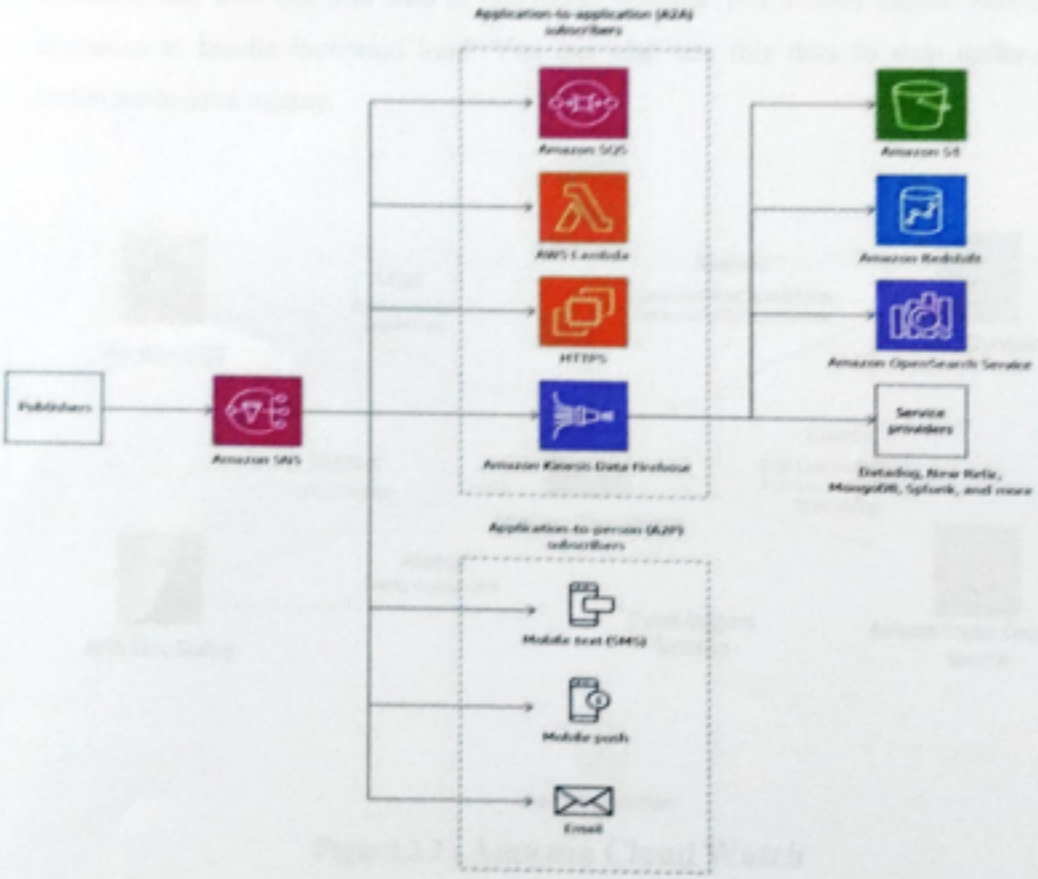

Figure 3.1: SNS

2. Amazon Cloud Watch:

Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real time. You can use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications. The CloudWatch home page automatically displays metrics about every AWS service you use. You can additionally create custom dashboards to display metrics about your custom applications, and display custom collections of metrics that you choose. You can create alarms that watch metrics and send notifications or automatically make changes to the resources you are monitoring when a threshold is breached. For example, you can monitor the CPU usage and disk reads and writes of your Amazon EC2 instances and then use that data to determine whether you should launch additional instances to handle increased load. You can also use this data to stop under-used instances to save money.

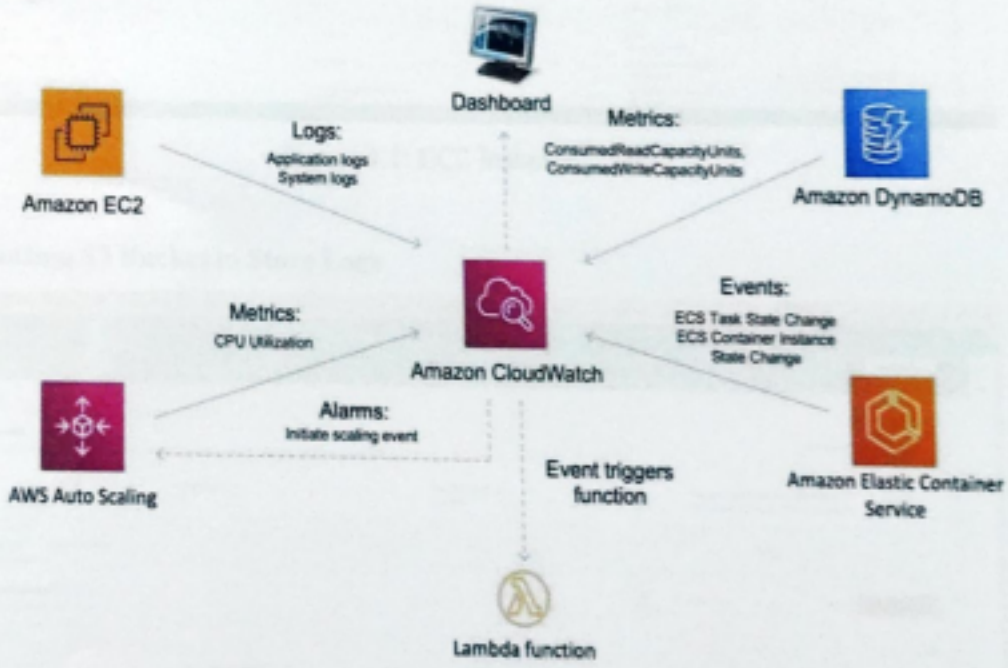

Figure 3.2 : Amazon Cloud Watch

CHAPTER 4

PROCEDURE AND SNAPSHOTS(RESULT)

Step 1: Creating EC2 for Windows Instance

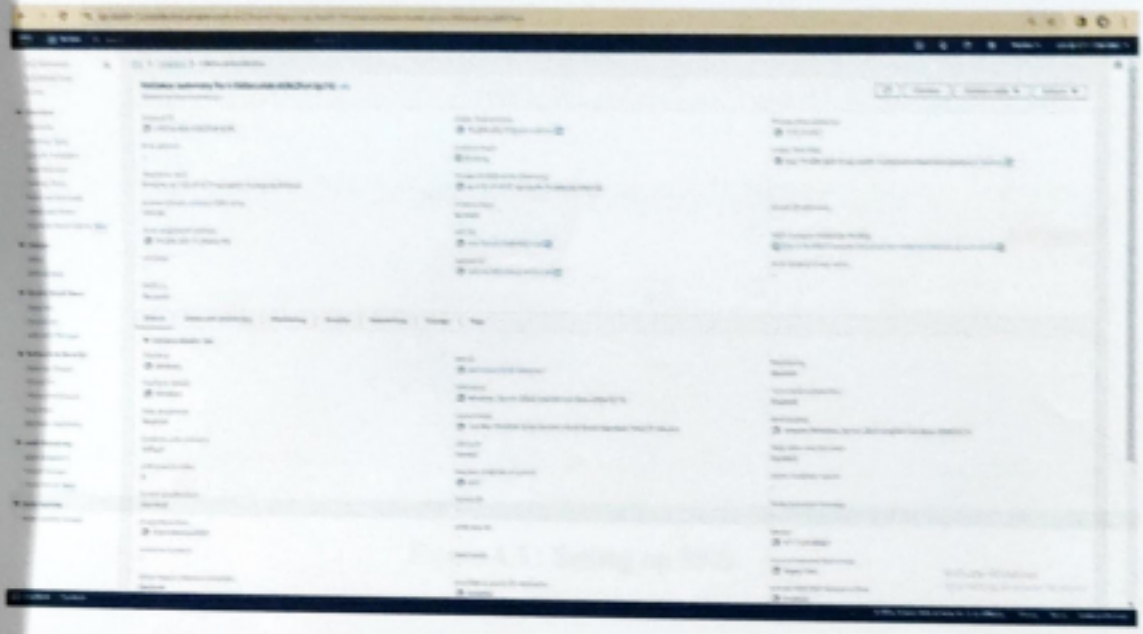

Figure 4.1: EC2 Instance

Step 2: Creating S3 Bucket to Store Logs

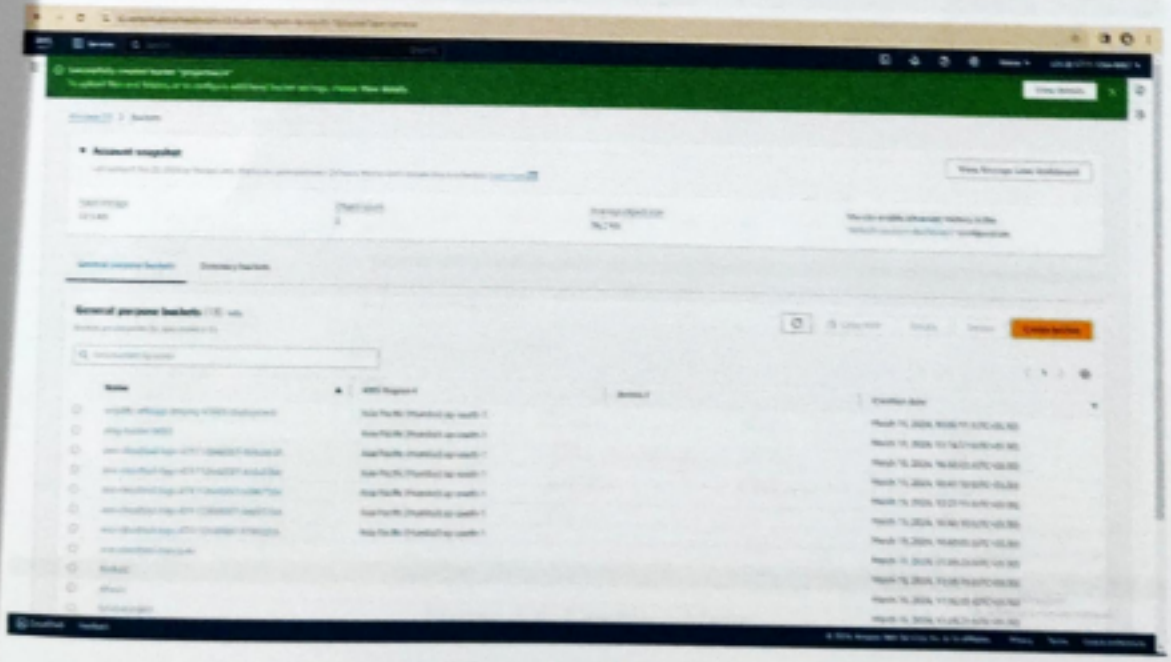

Figure 4.2: S3 Bucket

Step 3 : Creating Simple Notification Service(Topic and Subscription) to Receive threat Information

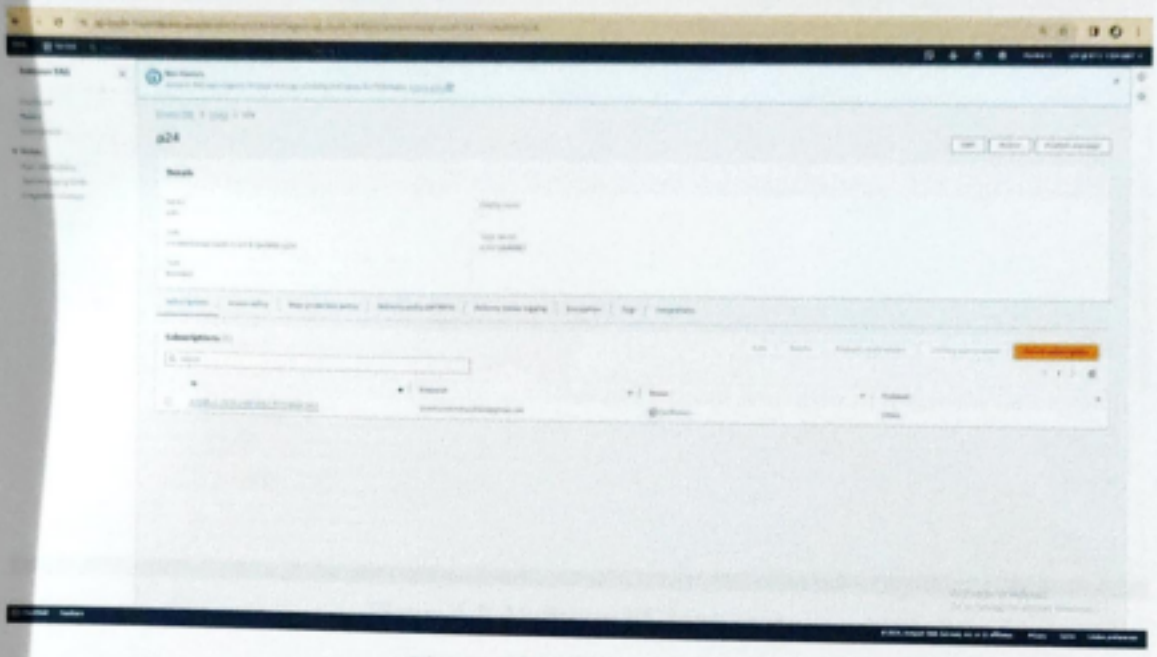

Figure 4.3 : Setting up SNS

Step 4 : Creating Inalarm And Updating it in EC2 Instance

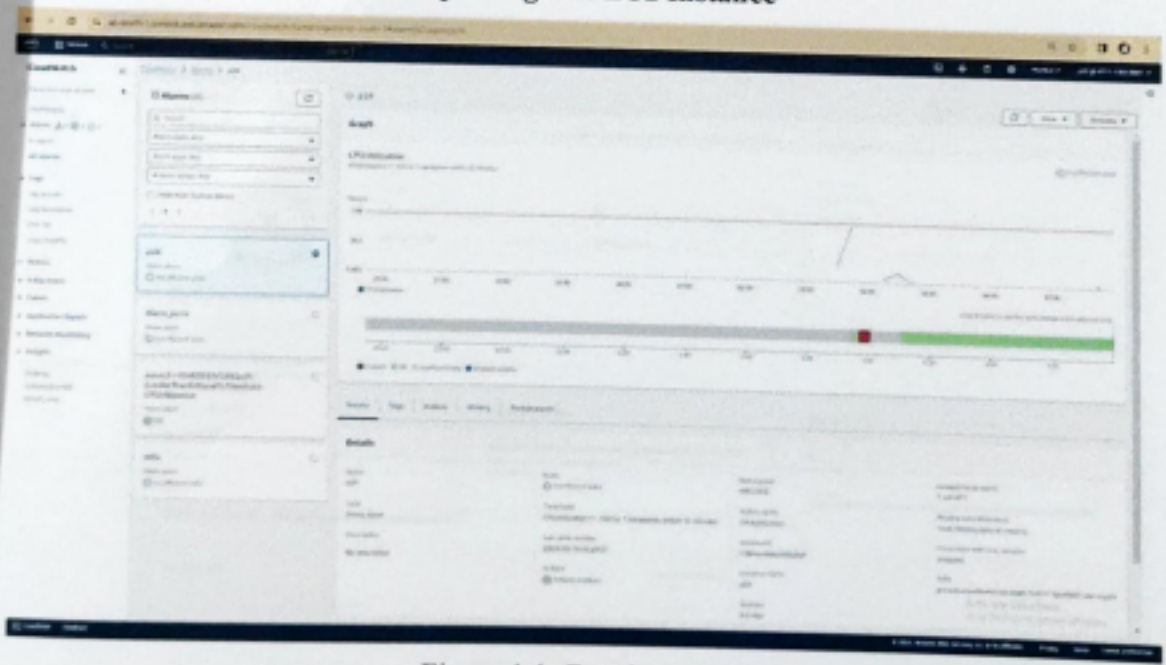

Figure 4.4: Creating Alarm

Updating EC2 Instance in order to trigger Alarm when CPUUTILIZATION Crosses 100units

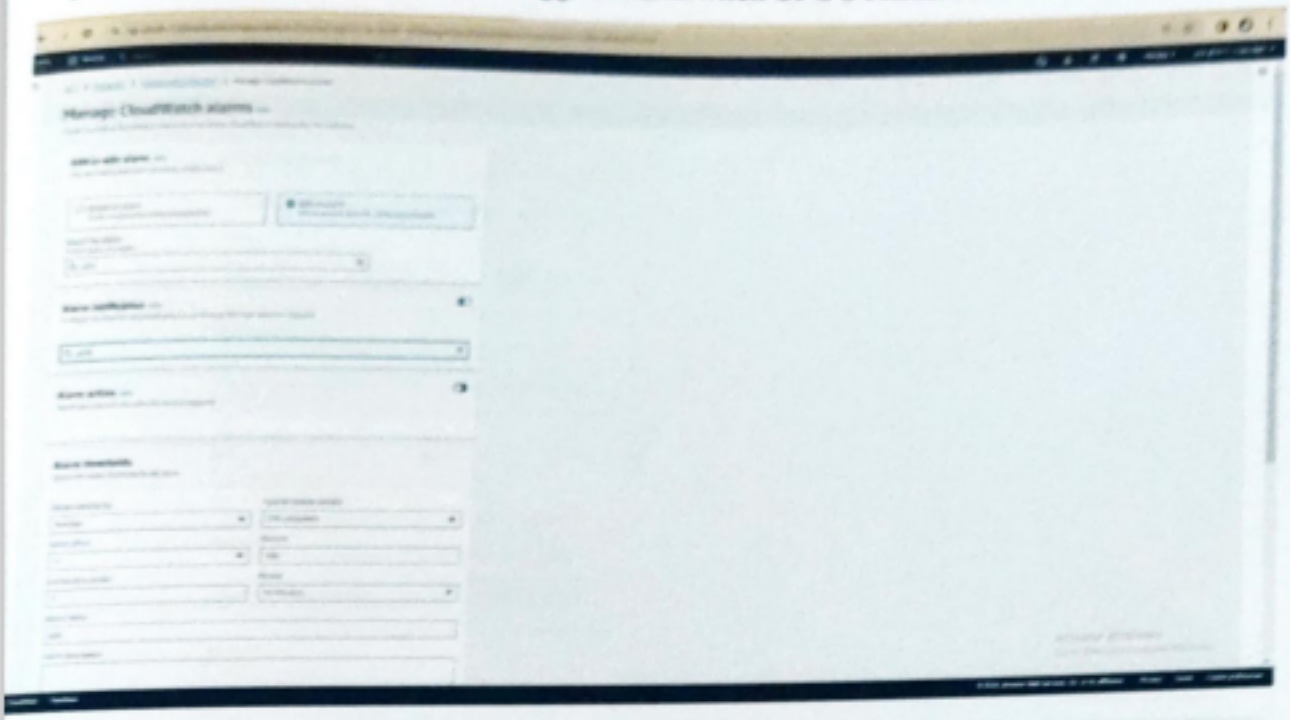

Figure 4.5: Updating EC2 instance

tep 5 : Enabling Amazon Macie in order to get the view of resources used and Threats side the cloud. Mainly S3 buckets to avoid data breaches.

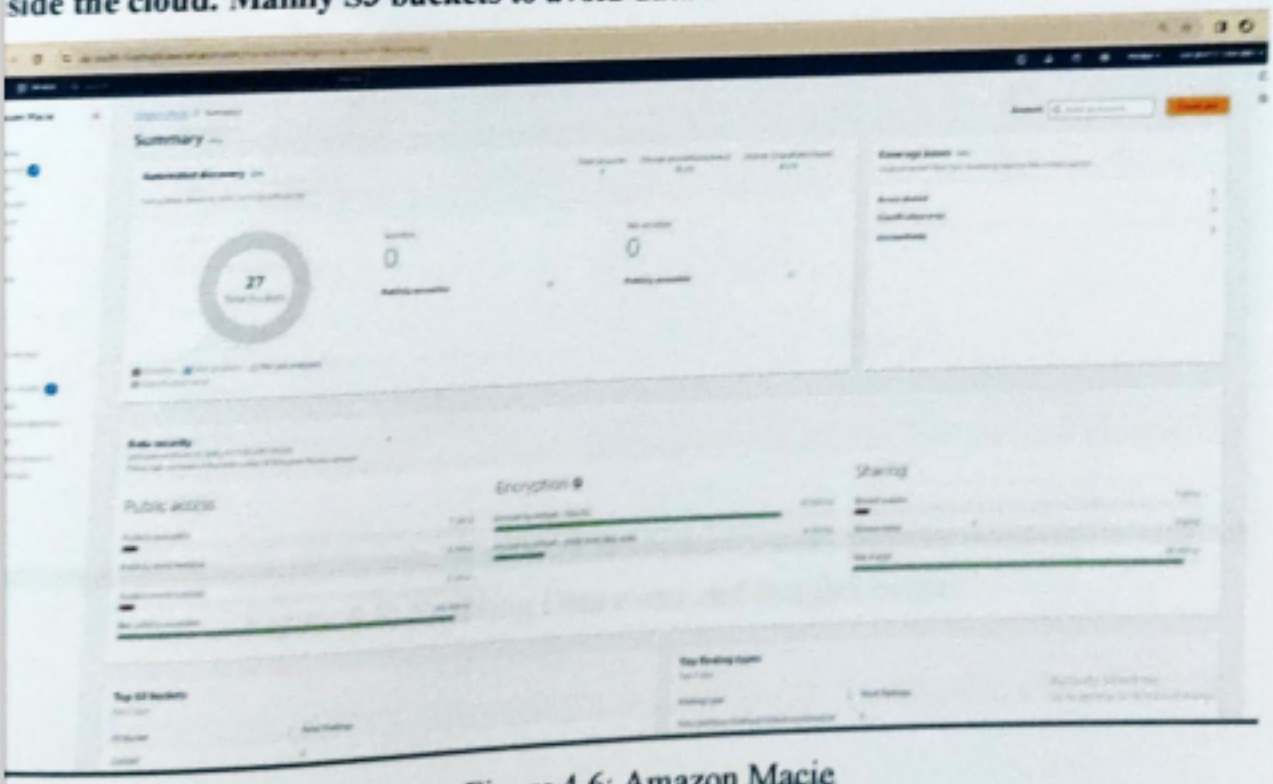

Figure 4.6: Amazon Macie

Step 6: Creating CloudTrail to collect log and Storing .json format file in S3 bucket. Also enabling Data events and Insights event identify unusual activity.

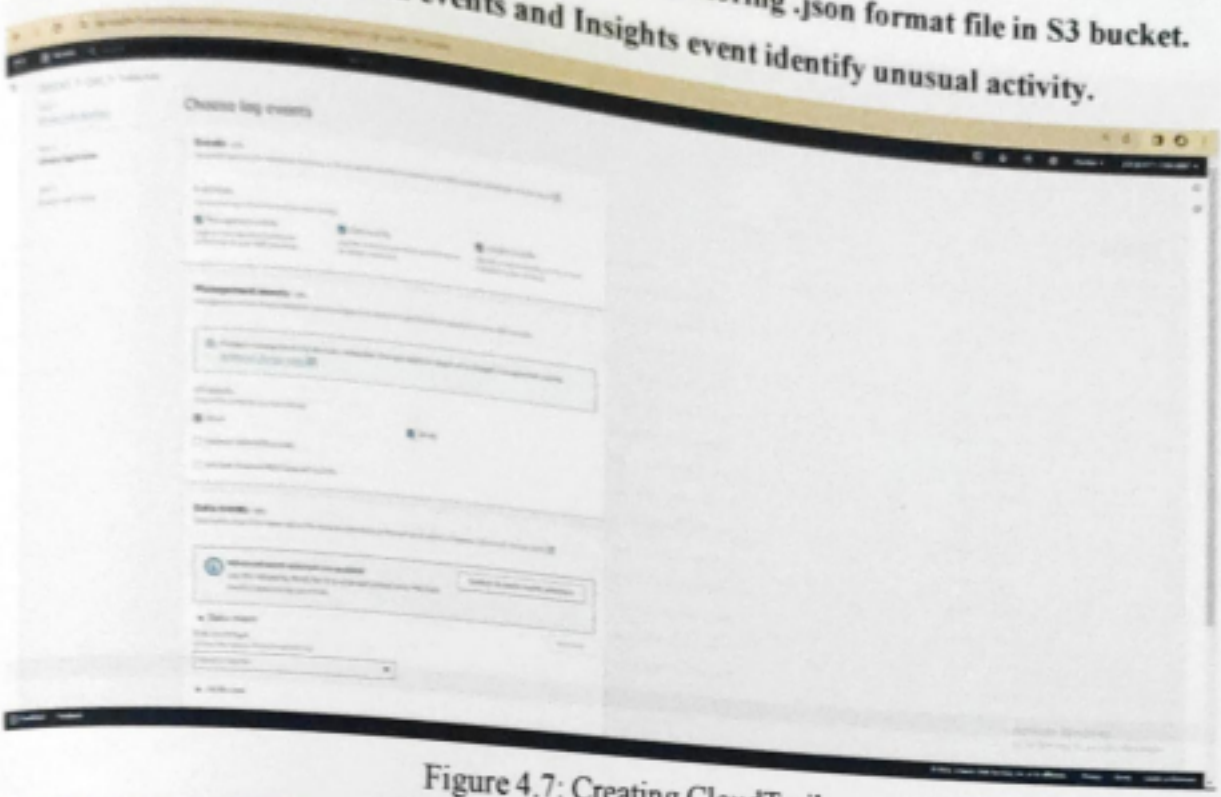

Figure 4.7: Creating CloudTrail

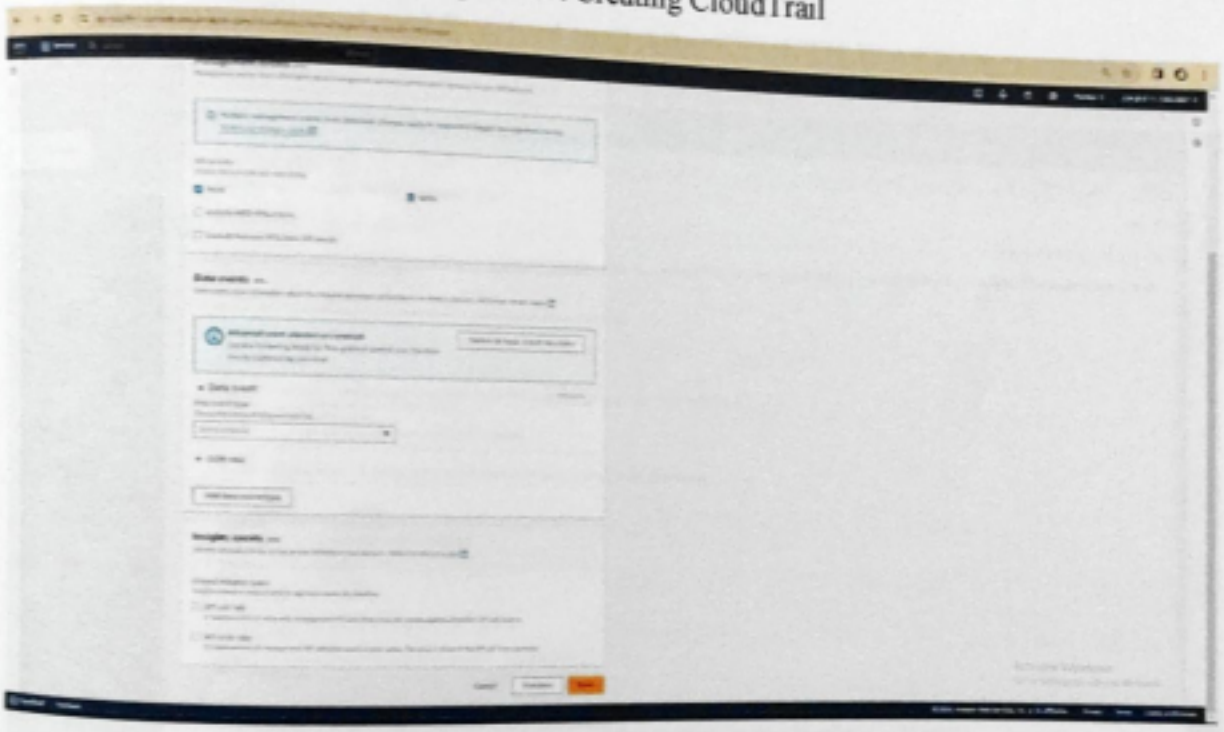

Figure 4.8: Enabling Data event and Insights events

Step 7: Logs recorded by CloudTrail And stored in S3 bucket

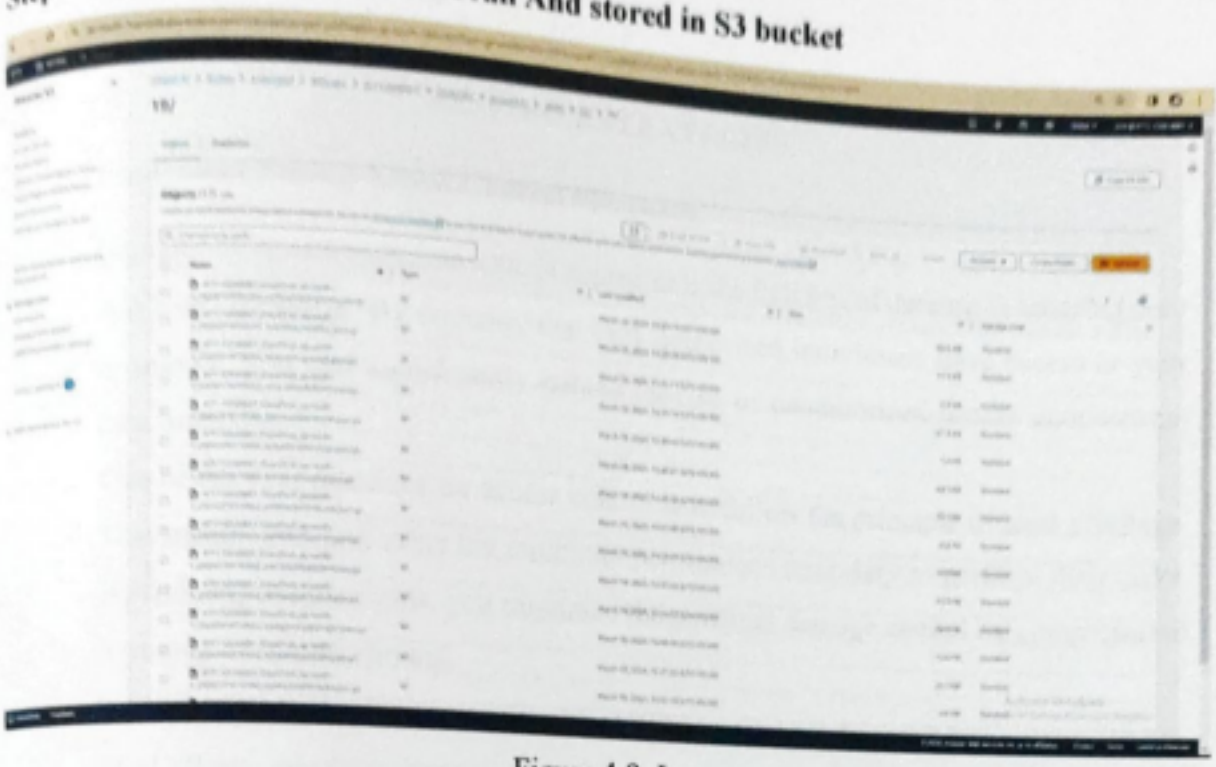

Figure 4.9: Logs

Step 8: Action performed and Received mail After CPUUTILIZATION crosses limit.

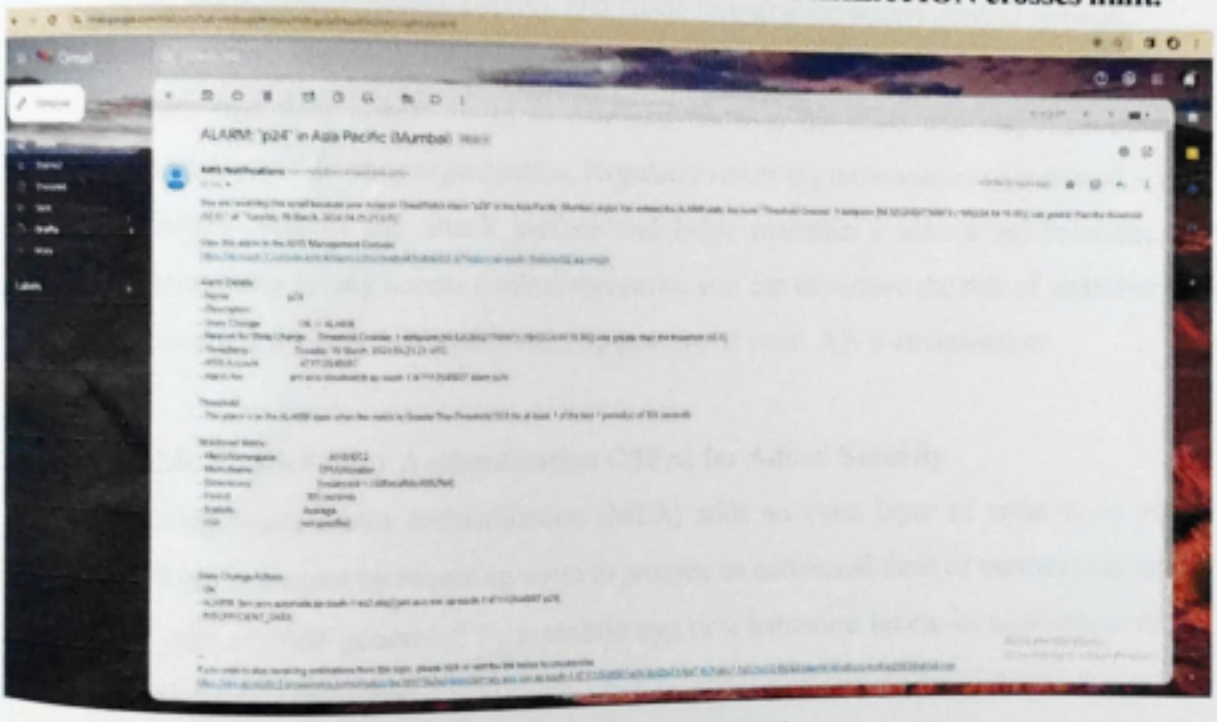

Figure 4.10: Alarm received

- CPU utilization crosses the limit when someone try to access instance for other purpose like mining Cryptocurrency.

CHAPTER 5

RESPONSE STRATEGIES

1. Implement Strong Access Control Measures

Implementing strong access control measures is the first line of defense in securing your AWS environment. By ensuring that only authorized individuals have access to your resources, you can significantly reduce the risk of unauthorized access andpotential data breaches.

One of the best practices for access control is to follow the principle of least privilege. This means granting users the minimum permissions necessary to perform their tasks. By limiting access rights, you minimize the potential damage caused by compromised accounts or insider threats.

Another essential measure is to enable AWS Identity and Access Management (IAM). IAM allows you to manage user access to AWS resources, create and manage groups, and assign permissions. With IAM, you can enforce strong password policies, enable multi-factor authentication (MFA), and create fine-grained access control policies.

Additionally, regularly reviewing and auditing user access privileges is crucial. This ensures that user access is up to date and matches the roles and responsibilities of individuals within your organization. Regularly removing unnecessary or outdated access privileges reduces the attack surface and helps maintain a secure environment. By implementing strong access control measures, you can minimize the risk of unauthorized access and increase the overall security posture of your AWS environment.

2. Enable Multi-Factor Authentication (MFA) for Added Security

Enabling multi-factor authentication (MFA) adds an extra layer of security to your AWS environment by requiring users to provide an additional form of verification, such as a unique code generated by a mobile app or a hardware token, in addition to their username and password.

MFA helps protect against unauthorized access, even if an attacker gains access to a user's password. By requiring an additional form of verification, MFA ensures that only authorized individuals with the correct device or token can access your AWS resources. AWS provides several MFA options, including virtual MFA devices and hardware [illegible] can be installed on mobile devices, while hardware

MFA devices are physical tokens that generate unique codes. Choose the option that best suits your organization's needs and ensure that all users with access to sensitive resources have MFA enabled.

It is important to note that enabling MFA should not replace strong password policies and access control measures. MFA should be used in conjunction with other security practices to provide a layered defense against unauthorized access.

By enabling MFA, you add an additional layer of security to your AWS environment and reduce the risk of unauthorized access.

CONCLUSION

Insider threats, malicious or negligent actions by authorized users, pose a significant challenge in AWS environments due to their trusted access. This report explored strategies for detection and response to insider threats, drawing insights from your simulations with enabled GuardDuty, CloudTrail, and CloudWatch.

CloudTrail logs user activity, allowing you to identify suspicious access patterns potentially indicative of insider activity. GuardDuty analyzes these logs with threat intelligence to detect anomalies and potential insider threats. CloudWatch helps visualize these findings and trigger alerts based on pre-defined thresholds.

The report recommends specific actions based on the simulations to further strengthen your AWS environment. This could involve optimizing detection techniques by refining CloudTrail and GuardDuty alerts or user activity monitoring methods. Additionally, reviewing and enforcing least privilege access principles with IAM policies and potentially implementing Multi-Factor Authentication (MFA) is crucial.

By implementing a layered approach that combines detection techniques, access controls, additional security measures, and ongoing user education, you can significantly mitigate the risk of insider threats in your AWS environment. Remember, security is an ongoing process. Regularly review security configurations, IAM policies, and detection techniques to ensure they remain effective against evolving threats. Utilize the valuable insights gained from your simulations to continuously improve your security posture and adapt your response strategies as needed.

ERENCES

1. https://docs.aws.amazon.com/pdfs/guardduty/latest/ug/guardduty-ug.pdf
2. https://aws.amazon.com/security-hub
3. https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html
4. https://docs.aws.amazon.com/macie/latest/user/what-is-macie.html
5. https://docs.aws.amazon.com/pdfs/AmazonCloudWatch/latest/monitoring/acw-ug.pdf# cloudwatch_architecture
6. https://aws.amazon.com/architecture/storage/?docs3_bp1&cards-all.sort-by=item.additionalFields.sortDate&cards-all.sort-order=desc&awsf.content-type= all&awsf.methodology=*all