ENPM665: CLOUD SECURITY

MIDTERM PROJECT

Securing a Cloud-based Healthcare Application

GROUP 15

Members:

Rishabh Nama: rishabhn - 119548738

Manarth Bhavsar: mbhavsar - 120304804

Srinivasan Anandan: sanandan - 120412998

Under the Guidance of:

Prof. Kevin Shivers

Prof. Thomas Dineen

Table of Contents

Introduction 3

1.1. Scope 3

2. System Overview 3

2.1. Security Categorization 3

2.2. System Description 3

2.3. Purpose of System 3

Appendix A – Security Test Case ProceduRES 4

Appendix B – Vulnerability SCAN Results 5

Vulnerability Scans: Inventory of Items Scanned 5

Vulnerability Scans: Raw Scan Results 6

Appendix C – Access control Results 7

Access control Scan: Inventory of Items Scanned 7

Appendix D – Data security Results 8

Data security Scan: 8

Data security Scans: Manual Scan Results 8

Appendix E – virtual machine security Results 11

Virtual Machine scan: 11

Appendix F – network secuirty Results 12

network secuirty Scans: 12

network secuirty Scans: Results 12

Appendix G – Disaster recovery Results 12

Disaster recovery scan: Inventory of Items Scanned 13

Appendix H – conclusion: Report summary and recommendations 16

Appendix I – Acronyms and Glossary 22

Appendix J – REFERENCES 23

INTRODUCTION

This document consists of a *Security Assessment Report (SAR)* for **Medcircle Healthcare**. This report contains the results of the comprehensive security test and evaluation of the **Cloud infrastucture** system.

The group has been assigned a project to assess the security vulnerabilities in a healthcare company's cloud infrastructure. The application is designed to store and manage sensitive patient data, including medical records, personal information, and billing details. Your task is to ensure the confidentiality, integrity, and availability of the application and its data, as well as to identify and mitigate potential security risks. The project will involve various aspects of cloud security, including identity and access management, data encryption, network security, and vulnerability management.

The company relies on the cloud to store and manage sensitive patient data, conduct telemedicine consultations, and host critical healthcare applications. However, due to various security oversights and misconfigurations, the infrastructure is highly vulnerable to potential attacks. Your task is to identify and exploit these vulnerabilities to highlight the risks associated with the insecure cloud infrastructure and provide recommendations for remediation.

1.1. SCOPE

The scope of this assessment and report is limit to the access to the cloud infrastructure within the AWS account and its components which include:

Web servers: These serve the frontend of the website and handle user requests.
Application servers: These handle the business logic and process user requests.
Database servers: These store product information, user details, and medical history.

2. SYSTEM OVERVIEW

2.1. SECURITY CATEGORIZATION

The **Medcircle Healthcare** is categorized as a **Moderate to High** impact system. The **Cloud Infrastructure** categorization was determined in accordance with Amazon Web Services compliant laws and regulations and Standards.

2.2. SYSTEM DESCRIPTION

The application is designed to store and manage sensitive patient data, including medical records, personal information, and billing details.

2.3. PURPOSE OF SYSTEM

The company relies on the cloud to store and manage sensitive patient data, conduct telemedicine consultations, and host critical healthcare applications.

APPENDIX A – SECURITY TEST CASE PROCEDURES

1. A visual mapping of the overall architecture of the cloud infrastructure was done by deploying the templates to the AWS Cloud.

2. Identification of various components of the infrastructure was done.

3. A vulnerability scan using Snyk was performed, and the results were documented.

4. The IAM policies were studied and determined Access Controls

5. A Data Security scan was performed manually, and the results were documented.

6. A Virtual Machine scan was performed using Snyk and the results were documented.
7. A Network Security scan was performed manually on the AWS console and the results were documented.

8. An intensive study was conducted on the infrastructure to determine potential threats and disaster recovery options.

APPENDIX B – VULNERABILITY SCAN RESULTS

Operating systems, networks, routers, firewalls, DNS servers, domain servers, and other hardware that supports a network are all scanned as part of an infrastructure scan. Scans of infrastructures may include virtual and physical hosts and devices. The Cloud Infrastructure network and operating system components of Medcircle were scanned using the Snyk, v0.40 vulnerability scanner. This is manually reviewed configuration files for the remaining inventory in order to look for any vulnerabilities. All outcomes are included in the table.

VULNERABILITY SCANS: INVENTORY OF ITEMS SCANNED

Filename	AWS Component	Issue	Severity	Remediation
MedCircle-CreateInfrastructure.yml	EC2 Instance	EC2 API termination protection is not enabled. Instances may be terminated by accident.	Low	Set \`DisableApiTermination\` attribute with value \`true\`
MedCircle-CreateInfrastructure.yml	Public Subnet	Instances launched in this subnet will automatically have public IP assigned. Instances will be potentially accessible over public internet, which may lead to unauthorized access.	Low	Set \`Properties.MapPublicIpOnLaunch\` attribute with value \`false\`
MedCircle-CreateS3Bucket.yml	S3	S3 bucket versioning is disabled. Changes or deletion of objects will not be reversible.	Low	Set \`Properties.VersioningConfiguration.Status\` attribute to \`Enabled\`
MedCircle-CreateS3Bucket.yml	S3	The s3 access logs will not be collected. There will be no audit trail of access to s3 objects.	Low	Set \`Properties.LoggingConfiguration\` attribute
MedCircle-CreateInfrastructure.yml	RDS	Automatic backup of AWS Relational Database is disabled. No automatic backups will occur, availability risk if disaster occurs and manual backups have not been set.	Medium	Set \`Properties.BackupRetentionPeriod\` to \`1\` or more
MedCircle-CreateInfrastructure.yml	RDS and IAM	RDS IAM authentication is disabled and users will use paswords than tokens.	Medium	Set \`Properties.EnableIAMDatabaseAuthentication\` to \`true\`

Filename	AWS Component	Issue	Severity	Remediation
MedCircle-CreateInfrastructure.yml	Security Group	Security Group allows open ingress due to which inbound traffic is allowed to a resource from any source instead of a restricted range. That potentially everyone can access your resource	Medium	Set \`Properties.SecurityGroupIngress.CidrIp\` attribute with a more restrictive IP.
MedCircle-CreateInfrastructure.yml	RDS	Non-encrypted RDS instance at rest. Incase of unauthorized access the data would be readable.	Medium	Set \`Properties.StorageEncrypted\` attribute to \`true\`
MedCircle-CreateInfrastructure.yml	EC2	Non-Encrypted root block device. Incase of unauthorized access the data would be readable.	Medium	Set \`BlockDeviceMappings.Encrypted\` attribute of root device to \`true\`

Table 4-1 – Vulnerability Table

VULNERABILITY SCANS: RAW SCAN RESULTS

The following raw scan results files are included:
https://github.com/rishabhnama/medcircle/actions/runs/6817995593/job/18542685469

APPENDIX C – ACCESS CONTROL RESULTS

Access Control scans consist of scans of the IAM roles and policies. The policies were attached to the designated roles and users. The team did a manual review of configuration files to analyze for existing vulnerabilities. Any results are documented in the table.

ACCESS CONTROL SCAN: INVENTORY OF ITEMS SCANNED

Filename	AWS Component	Issue	Severity	Remediation
Admin Role-IAM_Policy.txt	IAM Policy	Allowed access to all resources	Medium	Allow access to only required resources. Use the “AdminstratorAccess” Role
Developer Role-IAM_Policy.txt	IAM Policy	Allowed access to all resources	Medium	Allow access to only required resources for the developer. Tailor the role, permission set and allow fine grain access control

APPENDIX D – DATA SECURITY RESULTS

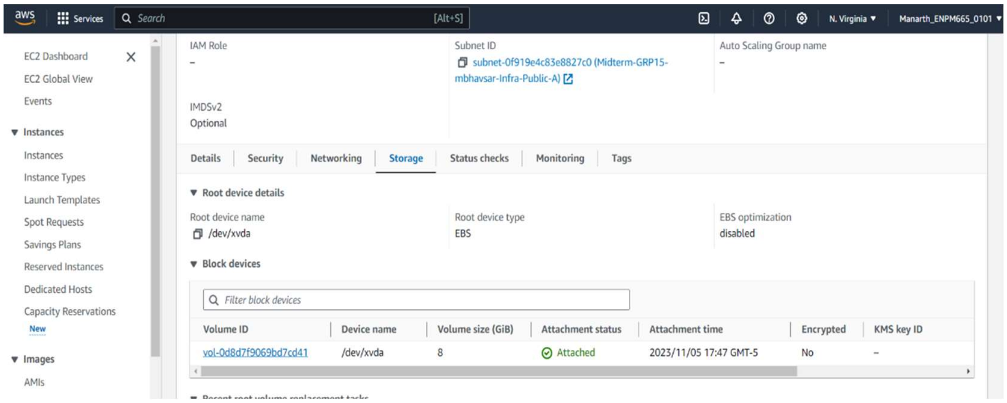
Data Security Scan included scanning S3, Relational Databases, EC2. Manual method was used to scan the **Medcircle's Cloud Infrastructure. 100**% percent of the inventory was scanned. Any results are documented in the table.

DATA SECURITY SCAN:

Filename	AWS Component	Issue	Severity	Remediation
MedCircle-CreateInfrastructure.yml	EC2	Non-Encrypted root block device. Incase of unauthorized access the data would be readable.	Medium	Enable Encryption: Set \`BlockDeviceMappings.Encrypted\` attribute of root device to \`true\`
MedCircle-CreateInfrastructure.yml	RDS	Non-encrypted RDS instance at rest. Incase of unauthorized access the data would be readable.	Medium	Enable Encryption: Set \`Properties.StorageEncrypted\` attribute to \`true\`
MedCircle-CreateInfrastructure.yml	RDS	Hardcoded Credential in plain text	High	Use AWS Secrets Manager to store, rotate and retrieve keys and passwords
MedCircle-CreateInfrastructure.yml	S3	Improper Access Control	Medium	Enforce Role Based Access control with least privilege.
MedCircle-CreateInfrastructure.yml	RDS	Poor Password Policy prone to brute force and enumeration	Low	Enforce strong password policies with at least 12 alphanumeric with symbols.

DATA SECURITY SCANS: MANUAL SCAN RESULTS

The following raw scan results files are included:



IAM Role
–

Subnet ID
subnet-0f919e4c83e8827c0 (Midterm-GRP15-mbhavsar-Infra-Public-A)

Auto Scaling Group name
–

IMDSv2
Optional

▼ Root device details

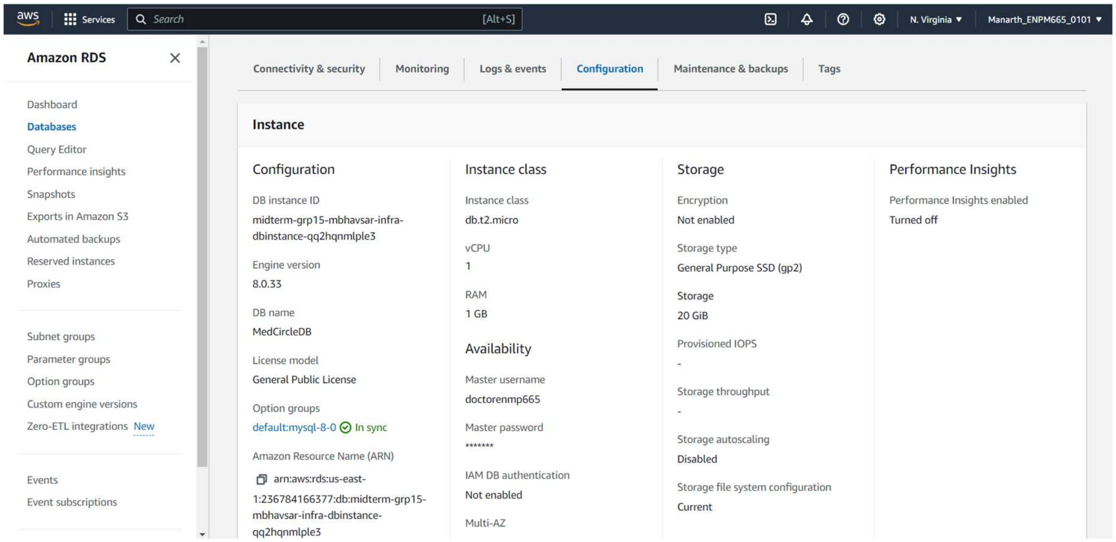
Root device name
/dev/xvda

Root device type
EBS

EBS optimization
disabled

▼ Block devices

Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID
vol-0d8d7f9069bd7cd41	/dev/xvda	8	Attached	2023/11/05 17:47 GMT-5	No	–



Instance

Configuration

DB instance ID
midterm-grp15-mbhavsar-infra-dbinstance-qq2hqnmlple3

Engine version
8.0.33

DB name
MedCircleDB

License model
General Public License

Option groups
default:mysql-8-0 ✓ In sync

Amazon Resource Name (ARN)
arn:aws:rds:us-east-1:236784166377:db:midterm-grp15-mbhavsar-infra-dbinstance-qq2hqnmlple3

Instance class

Instance class
db.t2.micro

vCPU
1

RAM
1 GB

Availability

Master username
doctorenmp665

Master password
****

IAM DB authentication
Not enabled

Multi-AZ

Storage

Encryption
Not enabled

Storage type
General Purpose SSD (gp2)

Storage
20 GiB

Provisioned IOPS
-

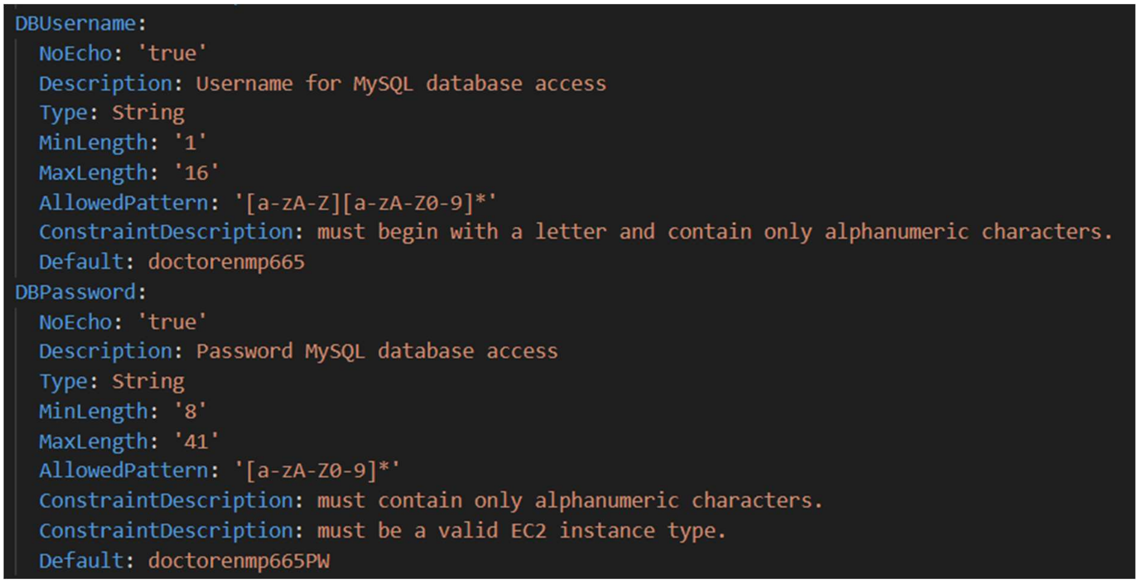
Storage throughput
-

Storage autoscaling
Disabled

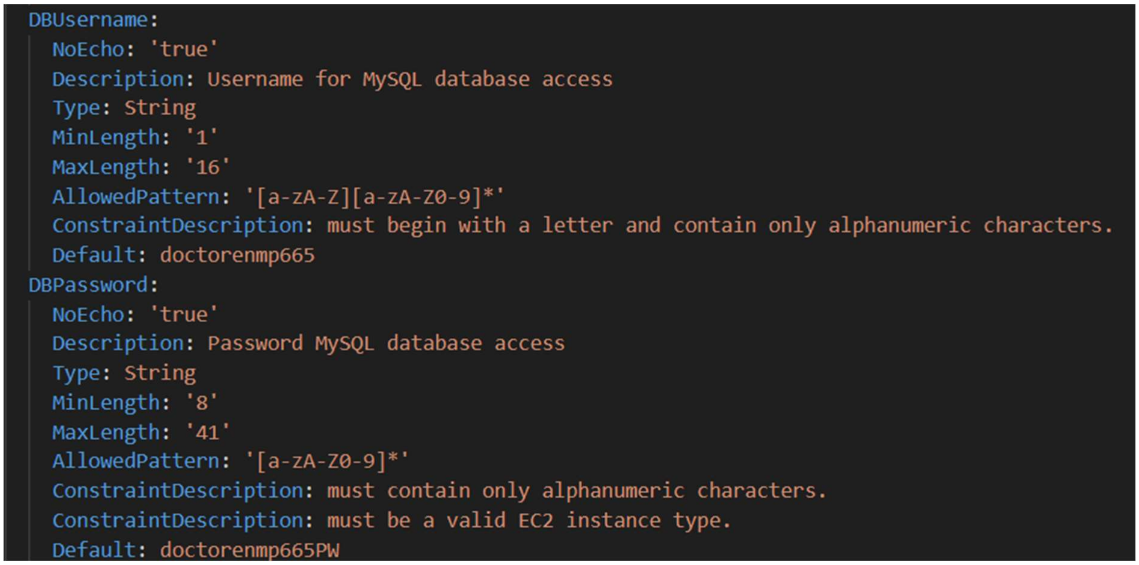
Storage file system configuration
Current

Performance Insights

Performance Insights enabled
Turned off



```
DBUsername:
  NoEcho: 'true'
  Description: Username for MySQL database access
  Type: String
  MinLength: '1'
  MaxLength: '16'
  AllowedPattern: '[a-zA-Z][a-zA-Z0-9]*'
  ConstraintDescription: must begin with a letter and contain only alphanumeric characters.
  Default: doctorenmp665
DBPassword:
  NoEcho: 'true'
  Description: Password MySQL database access
  Type: String
  MinLength: '8'
  MaxLength: '41'
  AllowedPattern: '[a-zA-Z0-9]*'
  ConstraintDescription: must contain only alphanumeric characters.
  ConstraintDescription: must be a valid EC2 instance type.
  Default: doctorenmp665PW
```



```
  DBUsername:
    NoEcho: 'true'
    Description: Username for MySQL database access
    Type: String
    MinLength: '1'
    MaxLength: '16'
    AllowedPattern: '[a-zA-Z][a-zA-Z0-9]*'
    ConstraintDescription: must begin with a letter and contain only alphanumeric characters.
    Default: doctorenmp665
  DBPassword:
    NoEcho: 'true'
    Description: Password MySQL database access
    Type: String
    MinLength: '8'
    MaxLength: '41'
    AllowedPattern: '[a-zA-Z0-9]*'
    ConstraintDescription: must contain only alphanumeric characters.
    ConstraintDescription: must be a valid EC2 instance type.
    Default: doctorenmp665PW
```

APPENDIX E – VIRTUAL MACHINE SECURITY RESULTS

Virtual Machine Scan consists of scans of operating system. The **Snyk**, **v0.40**> vulnerability scanner was used to scan the **Medcircle's Cloud Infrastructure** network/OS components. Any results are documented in the table.

VIRTUAL MACHINE SCAN:

Filename	AWS Component	Issue	Severity	Remediation
MedCircle-CreateInfrastructure.yml	EC2	Missing Software security updates. In an event of a breach, critical software vulnerabilities could be exploited causing immense damage.	Medium	Enable AWS Patch Manager to automate patching and keep the system updated.
MedCircle-CreateInfrastructure.yml	EC2	Instance is placed in a public subnet	High	Place the subnet in a private subnet or place it in a VPC and establish VPC Peering
MedCircle-CreateInfrastructure.yml	EC2	Unencryted Root Block Device	Medium	Enable Encryption: Set `BlockDeviceMappings.Encrypted` attribute of root device to `true`

APPENDIX F – NETWORK SECUIRTY RESULTS

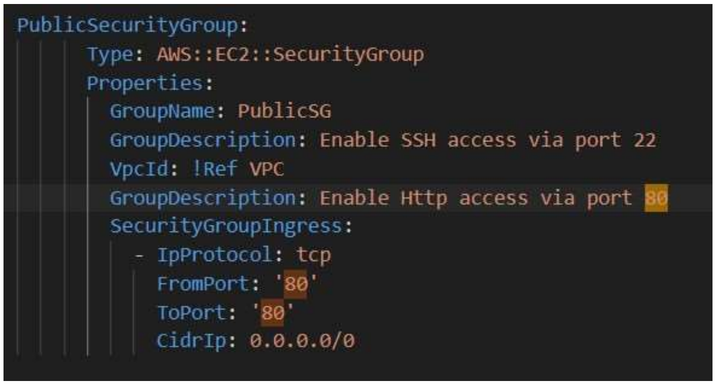
Network scans consist of scans of networks, routers, firewalls, DNS servers, domain servers, NIS masters, and other devices that keep the network running. **100**% percent of the inventory was scanned. Any results are documented in the table.

NETWORK SECUIRTY SCANS:

Filename	AWS Component	Issue	Severity	Info
MedCircle-CreateInfrastructure.yml	EC2	Unencrypted Communication (Web Communication through port 80)	Medium	Data Integrity is compromised on the web server as running on HTTP Protocol which is a clear text protocol
MedCircle-CreateInfrastructure.yml	WAF	Absence of Web Application Firewall	High	Firewall protects the web app from notorious requests and web attacks like DDoS, Command Injection, etc.
MedCircle-CreateInfrastructure.yml	VPC	Improper Access Control	High	Public Security group allows unrestricted access to the on port 80 and 22.
MedCircle-CreateInfrastructure.yml	Amazon Shield	Absence of DDoS protection	High	Amazon Shield can be enabled to protect the servers from potential DDoS attacks which are not enabled here.

NETWORK SECUIRTY SCANS: RESULTS

The following scan results files/images are included:



```
PublicSecurityGroup:
      Type: AWS::EC2::SecurityGroup
      Properties:
        GroupName: PublicSG
        GroupDescription: Enable SSH access via port 22
        VpcId: !Ref VPC
        GroupDescription: Enable Http access via port 80
        SecurityGroupIngress:
          - IpProtocol: tcp
            FromPort: '80'
            ToPort: '80'
            CidrIp: 0.0.0.0/0
```

APPENDIX G – DISASTER RECOVERY RESULTS

A manual scan of the infrastructure was performed and any results are documented in the table.

DISASTER RECOVERY SCAN: INVENTORY OF ITEMS SCANNED

AWS Component Name	Location	Description	Impact	Severity
EC2	AWS Cloud	No Data Backups set up for EC2	AVAILABILITY No recovery of the data is possible incase of a disaster	Medium
EC2	AWS Cloud	No Snapshots set up for EC2	AVAILABILITY No recovery of the state of the instances is possible in case of a disaster or attack.	Medium
S3	AWS Cloud	No Archived Glacier storage has been setup	AVAILABILITY Incase of a disaster, restoration is difficult if it occurs in multiple locations.	Medium
RDS	AWS Cloud	No Encryption at rest is set up	CONFIDENTIALITY and INTEGRITY In case of theft during/after disaster, the data could be stolen and manipulated.	Medium
RDS	AWS Cloud	Automatic backup of AWS Relational Database is disabled.	AVAILABILITY No automatic backups will occur, availability risk if disaster occurs and manual backups have not been set.	Medium
Disaster Recovery Plan	Organization	No playbook for Disaster Recovery plan has been setup	AVAILABILITY In case of a disaster, no one in the organization knows what to do.	Medium
EC2, RDS, S3	AWS Cloud	Not Multi AZ	AVAILABILITY Single point of failure: If one geographical region is affected the entire infrastructure may collapse.	Low

DISASTER RECOVERY PLAN:

Here are the major goals of a disaster recovery plan:

1. To reduce disruptions to regular operations.
2. To reduce the degree of harm and disturbance.
3. To lessen the disruption's financial impact.
4. To plan ahead and establish alternate methods of operation.
5. To instruct staff members on emergency protocols.
6. To ensure a seamless and quick return of service.

For any disaster recovery plan, these three elements should be addressed.

1. Emergency response procedures

To document the appropriate emergency response to a fire, natural disaster, or any other activity in order to protect lives and limit damage.

2. Backup operations procedures

To ensure that essential data processing operational tasks can be conducted after the disruption.

3. Recovery actions procedures

To facilitate the rapid restoration of a data processing system following a disaster.

The management team must assess the damage and begin the reconstruction of a new data center.

If the original site must be restored or replaced, the following questions are some of the factors to consider:

1. When will all necessary computer equipment be available?

2. Will replacing the outdated computer systems with newer models be more economical and efficient?

3. What is the anticipated duration required for the data site's construction or repairs?

4. Is there another website that can be upgraded more easily for computer use?

Phase I: Evaluate and List down critical applications and infrastructure with all the associated components.

Eg:

Infrastructure	Application	Point of Contact	Company
EC2	Web Applications	Cloud Admin	Amazon
RDS	Data	Cloud Data Admin	Amazon
S3	Logs and Backups	Cloud Admin	Amazon

Ensure automatic backups are configured. Also, make sure for extra layer of protection an archived Glacier backup is always available for sensitive data. (See recommendations for more on that)

Phase II: Follow a Checklist

This checklist provides possible initial actions that you might take following a disaster.

Initialitiaze the plan:

1. Advise upper management
2. Make arrangements and form a disaster recovery team.
3. Assess the catastrophe's severity
4. Implement an appropriate application recovery strategy based on the severity of the calamity.
5. Track developments.
6. Get in touch with the backup location and set up schedules.
7. Speak with all other required staff members, including data processing and users.
8. Get in touch with hardware and software suppliers.
9. Inform users of the service interruption.
10. Enumerate each team's duties
11. Inform insurance providers

Phase III: Recovery startup procedures for use after actual disaster

1. If rebuilding of the site is necessary, the costs and resources associated with it must be reviewed and the procedures must be scheduled to begin.
2. Any additional infrastructure components should be brought to light and begin setting up.
3. All the required workforce must be scheduled to begin working on restoring hardware and all the physical resources essential.
4. The management team must begin working on restoring the mechanisms essential for day-to-day activities.
5. Gather all the information about archives, backups and start verifying them.
6. The technical team can begin working on restoring as soon as all the requirements are met for restoration.

Phase IV:

1. Log and tag all activities performed by the team
2. Enforce best practices on all activities. (See recommendations for more information)
3. Document the processes to and iterate for improvisation.
4. Reconfigure any misconfigurations for future use cases

APPENDIX H – CONCLUSION: REPORT SUMMARY AND RECOMMENDATIONS

Sr.	Impact	Description	Recommendation
1	Low	The EC2 instance can be accidentally terminated, which is not preferred since the healthcare application is critical and should be up and running 24x7.	To prevent instance from being accidentally terminated using Amazon EC2, you can enable termination protection for the instance. Without this setting enabled the instances can be terminated by accident. This setting should only be used for instances with high availability requirements. Enabling this may prevent IaC workflows from updating the instance, for example terraform will not be able to terminate the instance to update instance type.
2	Low	Instances launched in this subnet will automatically have public IP assigned. Instances will be potentially accessible over public internet, which may lead to unauthorized access.	Always specify IP addresses on your own to minimize the surface area of attacks and reduce risk.
3	Low	S3 bucket versioning is disabled. Changes or deletion of objects will not be reversible.	S3 bucket versioning allows us to reverse accidental changes or deletion of objects in the storage which could be useful in some scenarios and should be turned on.
4	Low	S3 server access logging is disabled due to which S3 access logs will not be collected and there will be no audit trail of access to S3 objects.	Always enable S3 access logs which would be useful in most of the troubleshooting and auditing scenarios. Use CloudWatch logs to collect logs from OS. Analyze logs, findings, and metrics centrally. Use Object Lock to secure logs stored in S3.

Sr.	Impact	Description	Recommendation
	Medium	Automatic backup of AWS Relational Database is disabled. No automatic backups will occur, availability risk if disaster occurs and manual backups have not been set.	Always backup data and prepare for worst case scenarios. 1. Implement secure key management by defining an encryption approach that includes the storage, rotation, and access control of keys. 2. Use AWS KMS to manage encryption keys and create key-level policies. 3. Generate keys using secure HSMs which meet compliance requirements for data security. (FIPS 140-2). 4. Enforce encryption at rest using KMS 5. Enforce access control. 6. Audit the use of encryption keys using CloudTrail. 7. Use mechanisms to keep people away from data. 8. Automate data at rest protection
	Medium	RDS IAM database authentication is disabled, authentication tokens are not used to connect to DB instance. Users will connect to DB instance with password, which are less secure than temporary tokens which expire.	1. Rely on a centralized identity provider 2. Enforce least privilege practice 3. Use strong sign-in mechanisms (MFA), 4. Use temporary credentials by AWS SSO 5. Audit and rotate credentials periodically 6. Store and use secrets securely using Secrets Manager

Sr.	Impact	Description	Recommendation
	Medium	Security Group allows open ingress and inbound traffic is allowed to a resource from any source instead of a restricted range. That potentially everyone can access your resource.	1. Enforce Zero Trust model. 2. Place components which require no internet isolated in a subnet with no route to internet. 3. Control traffic at all layers using Transit Gateway. 4. Configure the network ACL to narrow the scope of traffic allowed between layers. 5. Use PrivateLink to allow customers to connect to the services from their VPCs over private IP addresses. 6. Inspect and filter your traffic at each layer 7. Inspect your VPC configurations for potential unintended access using VPC Network Access Analyzer. 8. Use AWS WAF to manage http(s) access to resources. 9. Use AWS Firewall Manager to centrally configure and manage firewall rules across your accounts and applications. 10. Automate network protection by using the AWS WAF Security Automations solution to implement web-based firewalls with IDS and IPS tools inbuilt.
	Medium	Non-encrypted RDS instance at rest. The DB instance storage is not encrypted by default. Should someone gain unauthorized access to the data they would be able to read the contents.	1. Implement secure key management by defining an encryption approach that includes the storage, rotation, and access control of keys. 2. Use AWS KMS to manage encryption keys and create key-level policies. 3. Generate keys using secure HSMs which meet compliance requirements for data security. (FIPS 140-2). 4. Enforce encryption at rest using KMS 5. Enforce access control. 6. Audit the use of encryption keys using CloudTrail. 7. Use mechanisms to keep people away from data. 8. Automate data at rest protection

Sr.	Impact	Description	Recommendation
	Medium	The root block device for EC2 instance is not encrypted. That should someone gain unauthorized access to the data they would be able to read the contents.	1. Enforce Zero Trust model. 2. Use AWS Systems Manager Patch Manager to automate the process of patching at scale. 3. Reduce attack surface by minimizing the use of dependency softwares, libraries, external services. 4. Reduce/Uninstall unused components. 5. Create your own AMIs, which you have patched and hardened meeting your own security standards. 5. Use EC2 Image builder to validate the functionality and security of your images before using them in production with AWS-provided tests and your own tests. 6. Use Amazon Inspector to perform configuration assessments against your instances for CVEs. 7. Use Fuzzing to test and find bugs using automation. 8. Enable people to perform actions at a distance using AWS Systems Manager instead of direct access or bastion host. 9. Implement managed services to reduce security burden. 10. Validate software integrity by code signing certificate of binaries and scripts to confirm the authenticity and use AWS signer to manage code-signing lifecycle. 11. Automate compute protection by reducing the risk of human error.
	Low	Vulnerable Operating System running in EC2	Patch all OS and DBs and applications regulary and train employees for awareness and follow best practices.

Sr.	Impact	Description	Recommendation
	Medium	No Logging and Monitoring Solutions Implemented	1.Check for unwanted configuration before a workload is deployed by implementing checks in the CI/CD pipelines or source control. 2. Use GuardDuty to setup alerts when unexpected and potentially unauthorized or malicious activity occurs within your AWS accounts. 3. Handle logs properly to avoid being analyzed for exploits. 4. Use CloudWatch logs to collect logs from OS. 5. Analyze logs, findings, and metrics centrally. 6. Use Object Lock to secure logs stored in S3.

Sr.	Impact	Description	Recommendation
		Lacks Automation: Automate, Simulate and Iterate attacks and Prepare for doomsday scenarios to create event driven responses.	1. Run game days to practice your incident management plans and procedures during realistic scenarios. 2. Create custom simulations tailored to your environment, team, and tools. 3. Gather evidence to review infrastructure and application logs to determine the source of the compromise. 4. Contain the incident after an incident is established and the source of the compromise is found. 5. Eradicate and focus towards mitigating any vulnerabilities in applications or infrastructure configurations that were susceptible to the compromise. 6. Recover from incident and ensure that all suspicious activity has ceased and continue to monitor to ensure a stable state. 7. Conduct Post-incident debrief to share learnings and increase the overall effectiveness of the organization's incident response plan and document lessons learned, update runbooks based on learnings, and determine if new risk assessments are required. 8. Automate containment and recovery capability. 9. Deconstruct the logic into a code-based solution, which can be used as a tool by many responders to automate the response. 10. Enable this code to be fully automated by being invoked by the alerts or events themselves, rather than by a human responder, to create an event-driven response.

Table G-1 – Report Summary and Recommendations

APPENDIX I – ACRONYMS AND GLOSSARY

Acronym	**Definition**
EC2	Elastic Compute Cloud
RDS	Relational Database System
API	Application Programming Interface
AWS	Amazon Web Services
IAM	Identity and Access Management
CD	Continuous Deployment
AO	Authorizing Official
MFA	Multi-factor Authentication
PaaS	Platform As A Service
IaaS	Infrastructure as a Service (Model)
S3	Simple Storage Service
ID	Identification
CI	Continuous Integration
IT	Information Technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OS	Operating System
POC	Point of Contact
RA	Risk Assessment
Rev.	Revision
SA	Security Assessment
SAR	Security Assessment
SDLC	System Development Life Cycle
AMI	Amazon Machine Image
SSP	System Security Plan

APPENDIX J – REFERENCES

1. Snyk: https://snyk.io/
2. Nessus: https://www.tenable.com/products/nessus
3. Github repo for infrastructure files: https://www.github.com/rishabhnama/medcirlce
4. Report structure references: https://www.fedramp.gov
5. AWS: https://aws.amazon.com/
6. For Recommendations: AWS Security Pillar: https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html
7. Google: https://google.com