AWS Cloud Configuration Review

For

CYRAAC Services Private Limited
(Third Floor, 22 | Gopalan Innovation Mall | Bannerghatta Main Road | JP Nagar Phase 3 | Bengaluru - 560076)

AWS Cloud Configuration Review

Report Created By
CYRAAC Services Private Limited

Report Created For
Ezetap Mobile Solutions Private Limited

Confidential Information

The following report contains company confidential information. Do not distribute, email, fax, or transfer via any electronic mechanism unless it has been approved by the recipient company's security policy. All copies and backups of this document should be saved on protected storage always. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. The specific IP addresses / Domain were identified by Client. Our subsequent test work, study of issues in detail and developing action plans are directed towards the issues identified. Consequently, this report may not necessarily comment on all the weaknesses perceived as important by the Client and / or Client management.

Table of Contents

1. AWS Configuration Review

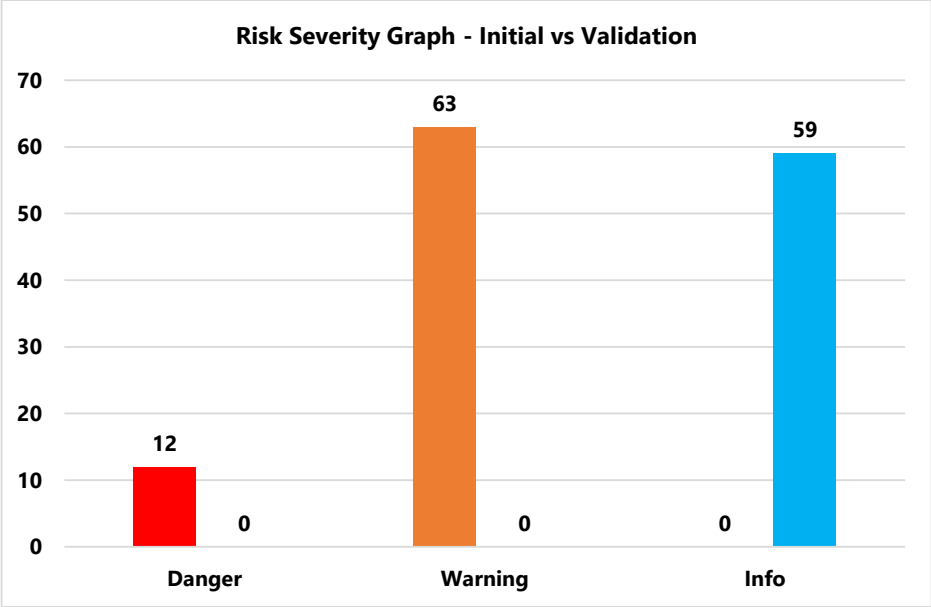
Configuration Assessment Initiated on:	11-Aug-23
Configuration Assessment Completed on:	14-Sept-23
Configuration Assessment Report Release Date:	15-Sept-23
AWS region for which the assessment was conducted:	ap-south-1
Assessment performed from location:	Bangalore

2. Summary of Configuration Issues

The project scope covered Cloud Configuration Review for 1 AWS **VPC-8769d1ee** account of **Ezetap Mobile Solutions Private Limited**.
Configuration deviation details after the validation review for **VPC-8769d1ee** component of **Ezetap Mobile Solutions Private Limited** is as shown below.

AWS Account ID: 192870797902				
VPC-8769d1ee				
Amazon Components	**Danger**	**Warning**	**INFO**	**Total**
CloudTrail	0	0	0	0
Config	0	0	1	1
EC2	0	0	42	42
ELB	0	0	2	2
ELBv2	0	0	0	0
VPC	0	0	14	14
Grand Total	**0**	**0**	**59**	**59**

Graphical Representation



3. Report Validity

The issues identified and proposed recommendations in this report are based on scans conducted by CyRAACS.

CyRAACS has made specific efforts to verify the accuracy and authenticity of the information gathered only in those cases where it was felt necessary.

The identification of the issues in the report is primarily based on the scans carried out during the limited time for conducting such an exercise.

Any changes to the configuration/issues which may have been discovered after the above-stated date, do not come under the purview of this report.

Any configuration changes or software/hardware updates made on hosts/machines on the IT Infrastructure covered in this test after the date mentioned herein may impact the security posture either positively or negatively and hence invalidates the claims & observations in this report. Whenever there is an update on the IT Infrastructure, we recommend that you conduct a penetration test to ensure that your security posture is compliant with your security policies.

4. Detailed Configuration Issues Identified

The assessment was conducted on AWS components mentioned below:

AWS Account ID: 192870797902			
VPC-8769d1ee			
Service	**Description**	**Affected resources**	**Risk level**
Config	AWS Config Not Enabled	1	**INFO**
EC2	Non-empty Rulesets for Default Security Groups	3	**INFO**
EC2	Security Group Opens UDP Port to All	2	**INFO**
EC2	Security Group Opens All Ports	16	**INFO**
EC2	Security Group Opens All Ports to All	2	**INFO**
EC2	Unrestricted Network Traffic within Security Group	7	**INFO**
EC2	Security Group Uses Port Range	6	**INFO**
EC2	Security Group Whitelists AWS CIDRs	6	**INFO**
ELB	Load Balancer Allowing Clear Text (HTTP) Communication	2	**INFO**
VPC	Subnet with "Allow All" egress NACLs	14	**INFO**

5. Checks Performed

Checks performed for the AWS
Enable CloudTrail logging across all AWS.
Turn on CloudTrail log file validation.
Enable CloudTrail multi-region logging.
Integrate CloudTrail with CloudWatch.
Enable access logging for CloudTrail S3 buckets.
Enable access logging for Elastic Load Balancer (ELB).
Enable Redshift audit logging.
Enable Virtual Private Cloud (VPC) flow logging.
Require multifactor authentication (MFA) to delete CloudTrail buckets.
Turn on multifactor authentication for the “root” account.
Turn on multi-factor authentication for IAM users.
Enable IAM users for multi-mode access.
Attach IAM policies to groups or roles.
Rotate IAM access keys regularly and standardize on the selected number of days.
Set up a strict password policy.
Set the password expiration period to 90 days and prevent reuseCustomer Visualforce pages with standard headers.
Don’t use expired SSL/TLS certificates.
User HTTPS for CloudFront distributions.
Restrict access to CloudTrail bucket.
Encrypt CloudTrail log files at rest.
Encrypt Elastic Block Store (EBS) database.
Provision access to resources using IAM roles.
Ensure EC2 security groups don’t have large ranges of ports open.
Configure EC2 security groups to restrict inbound access to EC2.
Avoid using root user accounts.
Use secure SSL ciphers when connecting between the client and ELB.
Use secure SSL versions when connecting between client and ELB.
Use a standard naming (tagging) convention for EC2.
Encrypt Amazon’s Relational Database Service (RDS).
Ensure access keys are not being used with root accounts.
Use secure CloudFront SSL versions.
Enable the requires parameter in all Redshift clusters.
Rotate SSH keys periodically.
Minimize the number of discrete security groups.
Reduce number of IAM groups.
Terminate unused access keys.
Disable access for inactive or unused IAM users.
Remove unused IAM access keys.
Delete unused SSH Public Keys.
Restrict access to Amazon Machine Images (AMIs).
Restrict access to EC2 security groups.
Restrict access to RDS instances.

Checks performed for the AWS
Restrict access to Redshift clusters.
Restrict access to outbound access.
Disallow unrestricted ingress access on uncommon ports.
Restrict access to well-known ports such as CIFS, FTP, ICMP, SMTP, SSH, Remote desktop.
Inventory and categorize all existing custom applications by the types of data stored compliance requirements and possible threats.
Involve IT security throughout the development process.
Grant the fewest privileges as possible for application users.
Enforce a single set of data loss prevention policies across custom applications and all other cloud services.
Encrypt highly sensitive data such as protected health information (PHI) or personally identifiable information (PII).

6. Key Observations

AWS Account ID: 192870797902			
VPC-8769d1ee			
Service	**Description**	**Risk level**	**Justification**
Config	AWS Config Not Enabled	INFO	Ezetap Team has confirmed AWS Config is not enabled due to business dependency and will be enabled on a later date.
EC2	Non-empty Rulesets for Default Security Groups	INFO	Ezetap Team has confirmed default AWS Security groups cannot be removed and has empty ruleset
EC2	Security Group Opens UDP Port to All	INFO	Business requirement
EC2	Security Group Opens All Ports	INFO	Ezetap team confirmed security groups have set rules to connect to restricted destination Ips. All port access is required.
EC2	Security Group Opens All Ports to All	INFO	Business requirement
EC2	Unrestricted Network Traffic within Security Group	INFO	Ezetap team has confirmed default AWS Security groups cannot be removed and has empty ruleset
EC2	Security Group Uses Port Range	INFO	Ezetap team has confirmed that the security groups are configured to use port range as part of internal security policy
EC2	Security Group Whitelists AWS CIDRs	INFO	Ezetap team Confirmed that the only internal CIDRs have been whitelisted and is done as part of internal security policy
ELB	Load Balancer Allowing Clear Text (HTTP) Communication	INFO	Ezetap team Confirmed that clear text communications is allowed for internal communication and is not exposed to external network
VPC	Subnet with "Allow All" egress NACLs	INFO	Ezetap team has confirmed that the changes can't be applied due to network dependency and will be remediated as per internal security policy.