AWS Well-Architected Framework - Security Pillar

www.thecyphere.com

info@thecyphere.com

Framework Pillars

- Operational Excellence
- Performance Efficiency
- **Security**
- Reliability
- Cost Optimization
- Sustainability

Security pillar:

- Helps with AWS recommendations and strategies to use when designing cloud architectures with security in mind
- Helps you meet your business and regulatory requirements.

01. Security foundations

www.thecyphere.com info@thecyphere.com

Refers to the fundamental principles and practices that provide a robust security base for your AWS environment.

Further broken into two approaches.

Shared responsibility

Refers to the division of security responsibilities between AWS (the cloud service provider) and the AWS customer (the organisation using AWS services).

Governance

All about establishing security policies, procedures, and controls to ensure compliance, and risk management across AWS environments.

Best practices

- Centrally manage accounts
- Organise workloads in separate accounts
- Set controls centrally for services and regions

- Perform threat modelling
- Isolate environments and set guardrails
- Limit root user access
- Implement organisational governance
- Stay current with security practices
- Automate continuous security testing

02. Identity management

Focuses on managing and controlling access to AWS resources.

www.thecyphere.com

info@thecyphere.com

Best practices

- Use strong authentication and temporary credentials.
- Utilise dedicated credential management services.
- Centralise workforce identity management.

- Regularly audit and rotate credentials.
- Group users and maintain accurate attributes.
- Apply for least privilege access.
- Establish emergency access with the least privilege.
- Continuously review and remove unnecessary permissions.

- Implement common access controls
- Monitor for public and cross-account access.
- Use just-in-time access and least privilege for third-party managed systems.

03. Detection

All about identifying and responding to security threats by implementing mechanisms to detect and analyse unusual or suspicious activities in your AWS environment.

Best practices

- Retain, access, and centralise security event logs.
- Integrate events into workflow systems.
- Embrace automation for investigations.
- Review and refine automation tools.

- Utilise Amazon EventBridge and GuardDuty in AWS.
- Create actionable alerts with relevant details.
- Develop investigation processes (runbooks/playbooks).

04.

Infrastructure protection

www.thecyphere.com info@thecyphere.com

Aim is to secure and maintain uninterrupted cloud operations.

This entails employing essential control methods like defense in depth to fulfill organisational and regulatory obligations.

Best practices

- Control traffic at all layers.
- Automate protection for a self-defending network with threat intelligence.
- Inspect and filter traffic at each layer.

- Scan source code and patch the environment.
- Integrate scanning into CI/CD pipelines.
- Harden OS and minimise components, libraries, and services.
- Utilise resource management services like Amazon RDS and AWS Lambda.

- Enforce secure configurations via tools.
- Limit interactive access to reduce human error.
- Implement code signing to verify software authenticity.

05. Data protection

www.thecyphere.com info@thecyphere.com

Best practices

- Categorise and protect data by criticality and sensitivity.
- Use resource tags, separate accounts, IAM policies, Organisations SCPs, KMS, and CloudHSM for data classification and encryption policies.

- Verify user origin and ensure decryption key access.
- Avoiding direct data access.
- Automate data identification and classification.
- Secure key management, and enforce encryption at rest.

- Securely store and rotate keys, and enforce encryption.
- Automate data protection and access control.
- Limit direct access to sensitive data and systems.

Catch up with us to discuss how you can build your AWS infrastructure securely

www.thecyphere.com

info@thecyphere.com

06. Incident response

www.thecyphere.com info@thecyphere.com

Best practices

- Educate staff on cloud technologies.
- Define roles and responsibilities.
- Engage external partners for incident response.
- Understand AWS response teams and support.

- Create a formal incident response plan.
- Pinpoint forensic investigation capabilities.
- Ensure pre-provisioned access for responders.
- Reduce reliance on long-lived credentials.

- Implement resource tagging.
- Regularly review and adapt incident response.
- Use simulations to assess and improve response.
- Automate incident containment and recovery.

07. Application Security

www.thecyphere.com info@thecyphere.com

Covers the entire software lifecycle.

Integrating AppSec into development and post-release processes proactively identifies and addresses security issues.

www.thecyphere.com **info@thecyphere.com**

Best practices

- Train developers in secure application development.
- Embrace security-oriented development practices.
- Automate security testing throughout development.

- Conduct routine penetration testing.
- Perform manual code reviews.
- Centralise software package assessments.
- Implement programmatic software deployments.

- Regularly assess pipeline security.
- Restrict builder access to pipeline tests.
- Configure pipelines for build environment validation.
- Establish a feedback mechanism for improvements.

Liked this?

Share with others

Need a chat? Get in touch:

thecyphere.com
info@thecyphere.com