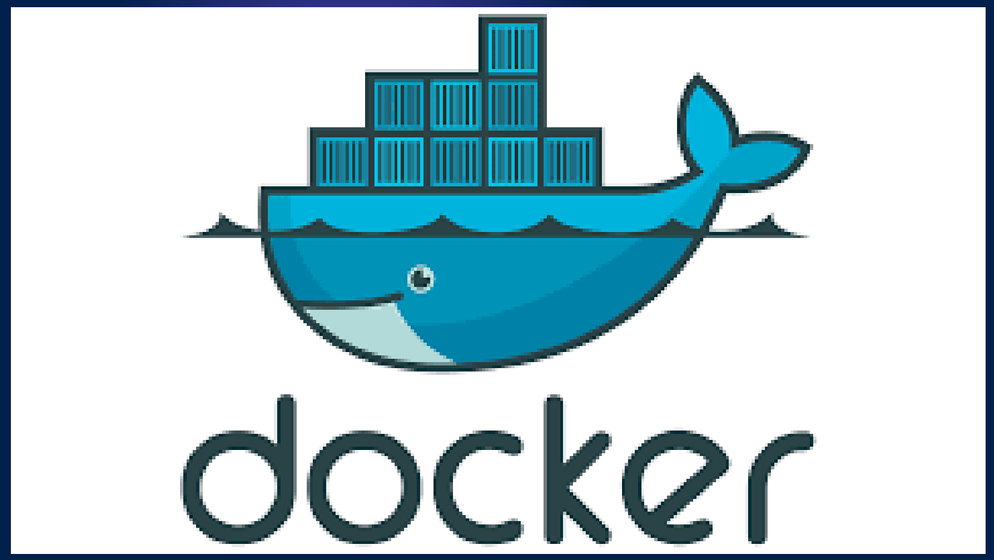
Introduction

Scan Docker Images using Amazon ECR: Identifying Vulnerabilities



ECR is a fully-managed container registry for storing, managing, and deploying Docker container images

Why Scan Docker Images?

- Identify Security Vulnerabilities
- Prevent Security Breaches
- Protect Against Malware and Malicious Code
- Ensure Compliance and Regulatory Requirements
- Maintain the Trust of Users and Customers
- Facilitate Secure DevOps Practices

How Image Scanning Works

- Docker images are automatically scanned for vulnerabilities upon pushing them to ECR
- Vulnerability data is obtained from trusted sources
- Results are categorized based on severity levels

Scan Results and Reports

- reports provide detailed information about vulnerabilities found in Docker images
- That reports include recommendations for remediation and improving the security posture

Best Practices for Image Scanning

- Effective Docker image scanning using Amazon ECR
- Regularly scan images to catch new vulnerabilities
- Monitor scan results and act promptly to remediate issues
- Implement image scanning as an automated step in the CI/CD process

Conclusion

The benefits of scanning Docker images using Amazon ECR. Emphasize the significance of identifying vulnerabilities for a secure container environment

Reference

https://docs.aws.amazon.com/AmazonECR/latest/userguide/image-scanning.html

Thank You