Disclaimer:

The views and opinions expressed in this presentation are solely those of the presenter and do not necessarily reflect the official policy or position of any past or current employer or any other organization with which I have been associated. The information provided in this presentation is for educational purposes only and is based on personal research and experience.

Any references to specific organizations, companies, or their services or products are provided as examples only and should not be considered as an endorsement. Neither the companies I have worked with nor any other entity is responsible for the accuracy, completeness, or reliability of the content presented here.

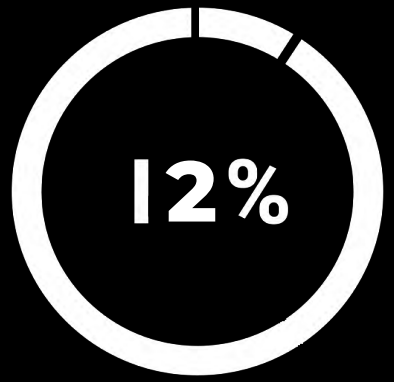
This presentation is not intended to provide, and should not be relied on for, professional advice. Attendees are encouraged to consult with professional advisors for advice concerning specific matters before making any decision.

Cracking the Code of Cloud Security

Protecting Containers Infrastructure and Workloads

Fouad Mulla

of Containers images are pulled of Public sources.



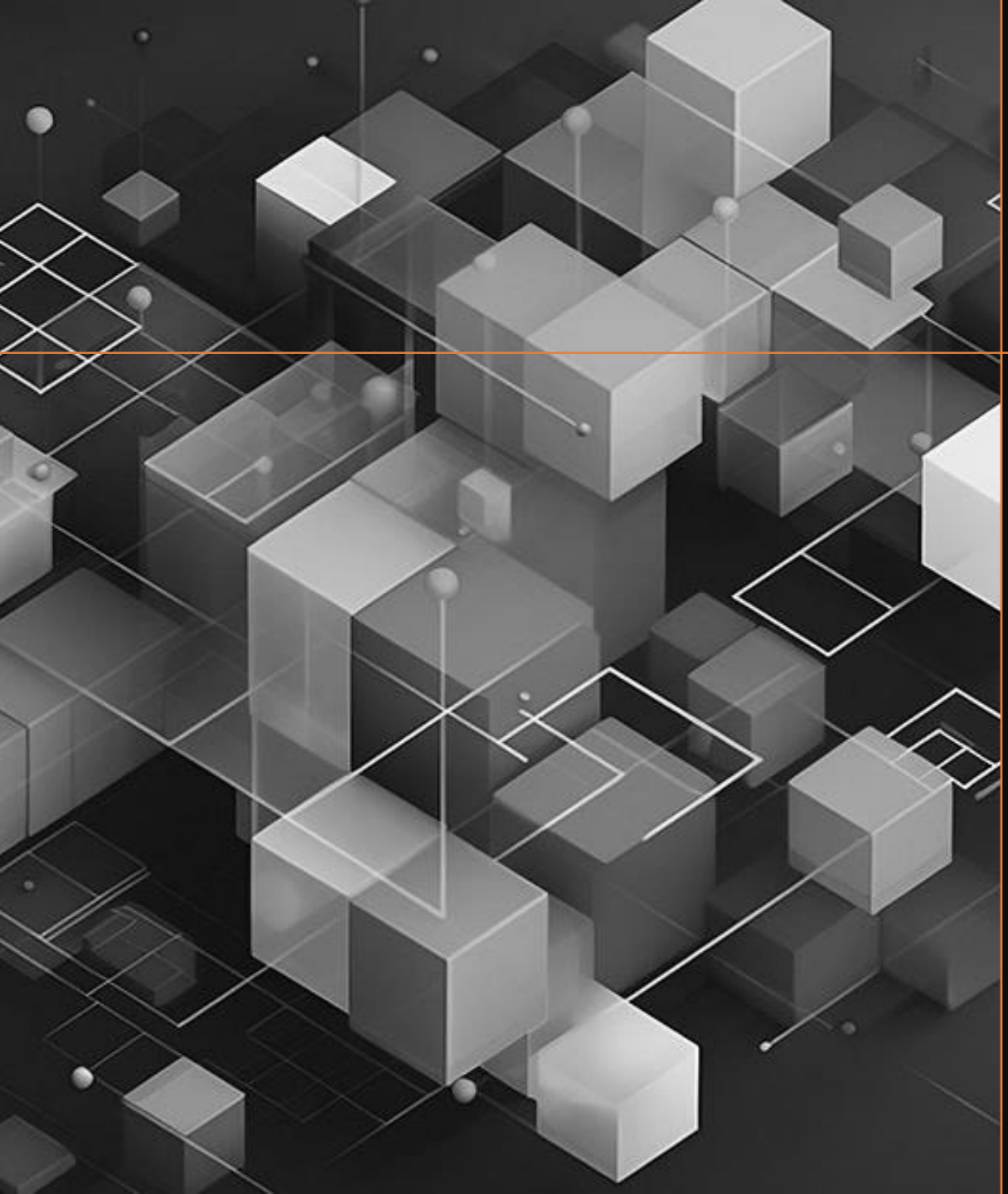
of containers were running as a non-root user, which is a best practice in container security.

Fouad Mulla

- A seasoned Cloud Security Architect and Lead Consultant.
- CISM,CISP,CASP+

Connect with me via LinkedIn

www.linkedin.com/in/mulla-fouad



Agenda

- Introduction
- Challenges in Container Security
- Cloud Container Vulnerabilities
- Containers Security : DevSecOps
- Enhancing Security: Beyond the Defaults
- Automated Vulnerability Management
- Configuration Management and Network Segmentation
- Best Practices in Container Security

Introduction

You don’t need containers to ensure application security...

But using containers wisely can enhance your application's security.

Introduction

You don’t need advanced security tools to start with containers...

But you do need to consider security to effectively use containers.

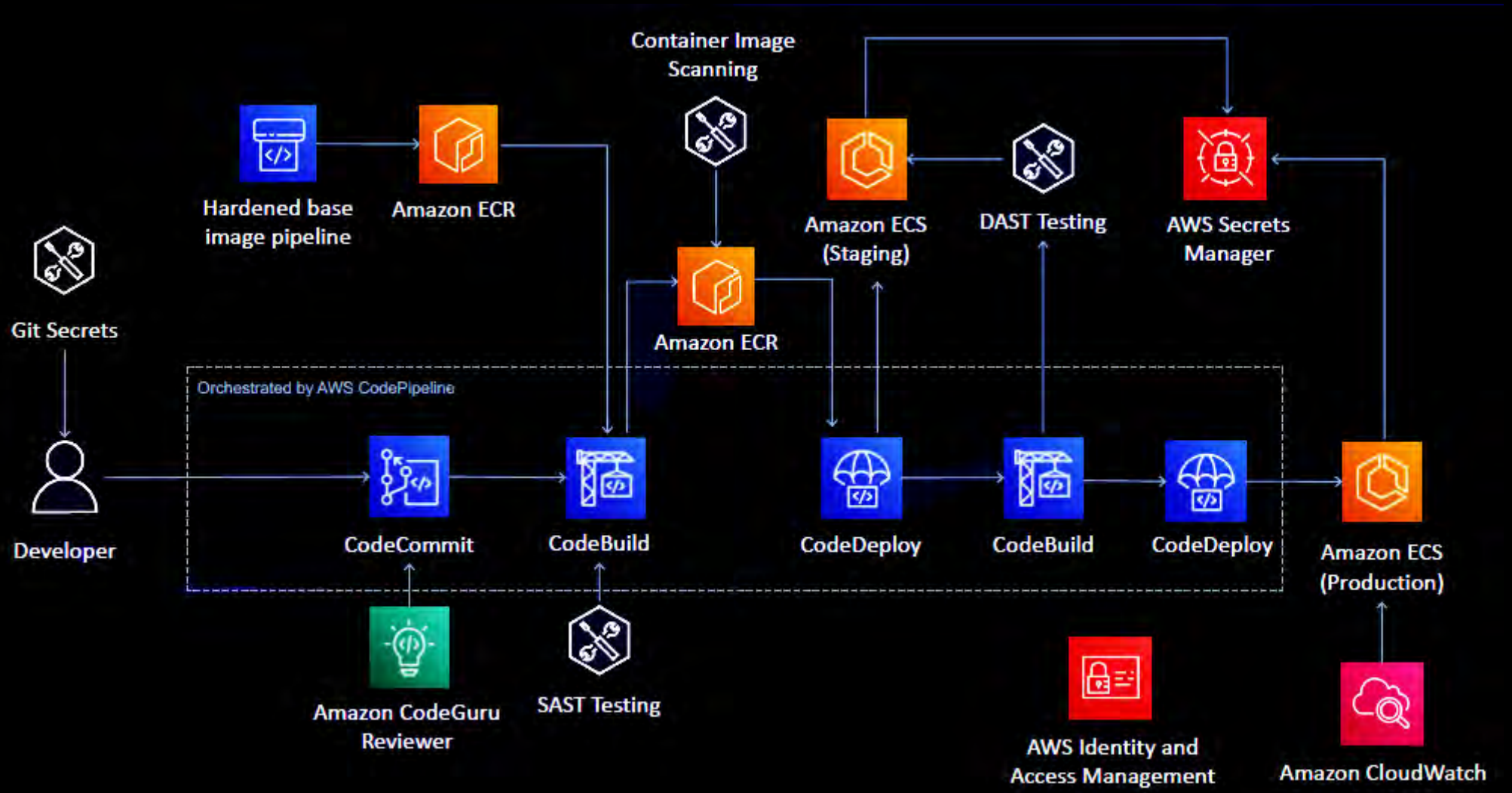
Challenges in Container Security

1. **Daemon Attack Surface**
   Potential vulnerabilities in containers own system
2. **Secrets Management**
3. **Untrusted Content Risks**
   Dangers of using compromised or vulnerable images
4. **Container Sprawl and Ephemeral Runtimes**
5. **Lightweight Isolation Risks**

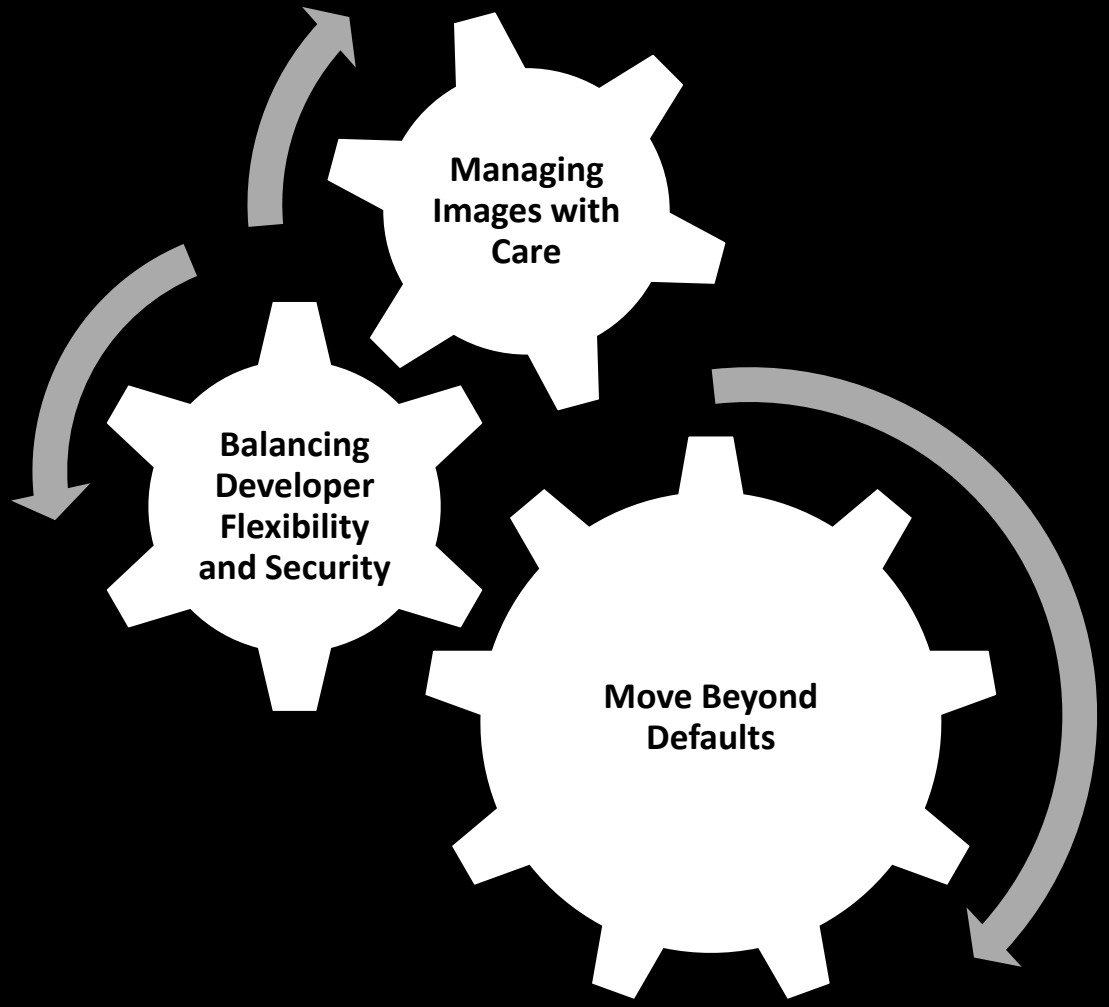
Cloud Container Vulnerabilities

- Image Vulnerabilities
- Insecure Container Runtime Configurations
- Inadequate Network Segmentation
- Container Escape Vulnerabilities
- Orchestrator Vulnerabilities
- Lack of Resource Limitations
- Dependence on Untrusted Container Registries
- Logging and Monitoring Gaps
- Immutable and Ephemeral Nature

Containers Security : DevSecOps

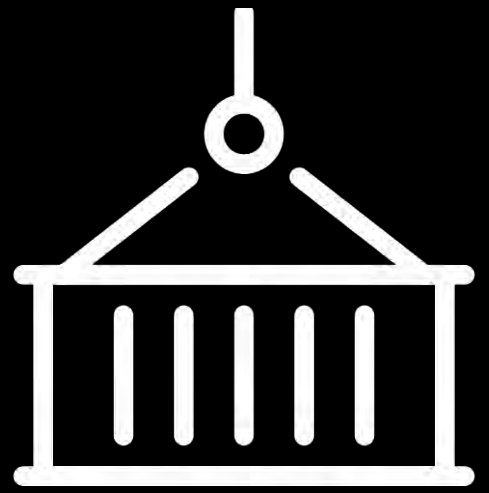


Enhancing Security: Beyond the Defaults



Enhancing Security: Beyond the Defaults

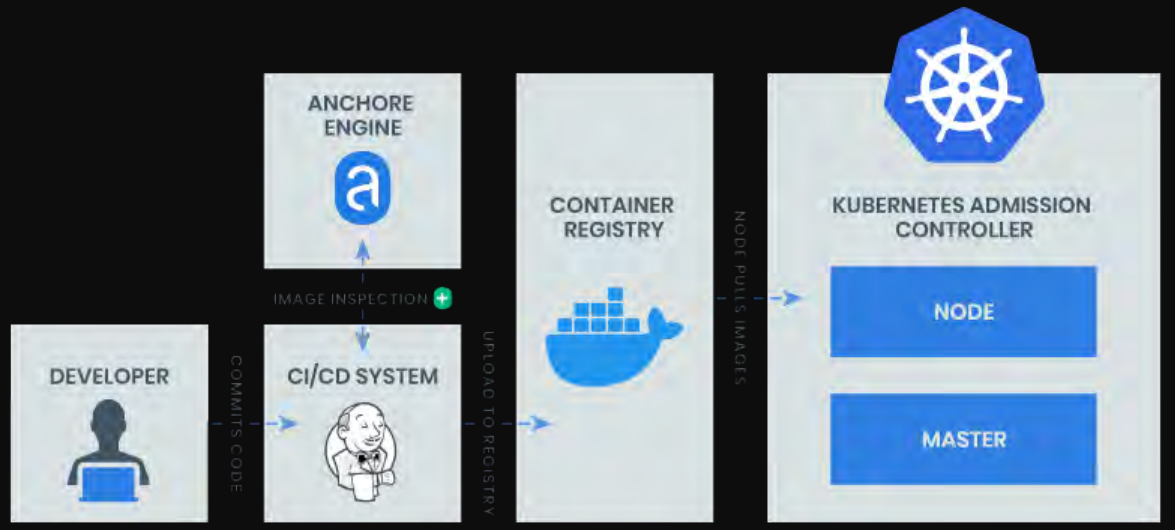
1. **Use Trusted Base Images with Regularly Scan for Vulnerabilities**
2. **Implement Least Privilege Access and Ensure Container Isolation**
3. **Maintain Immutable Containers and Read-Only Filesystems**
4. **Implement Robust policies Logging and Monitoring**
5. **Secure Configuration Management**
6. **Integrate Security in CI/CD Pipeline**

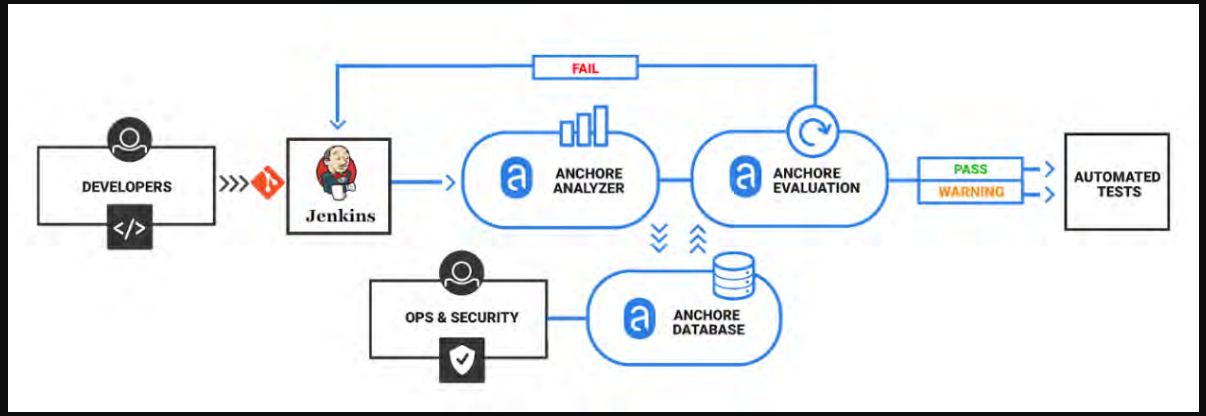


Automated Vulnerability Management

Anchore Engine is an open-source tool for deep image inspection and vulnerability scanning.

https://github.com/quay/clair





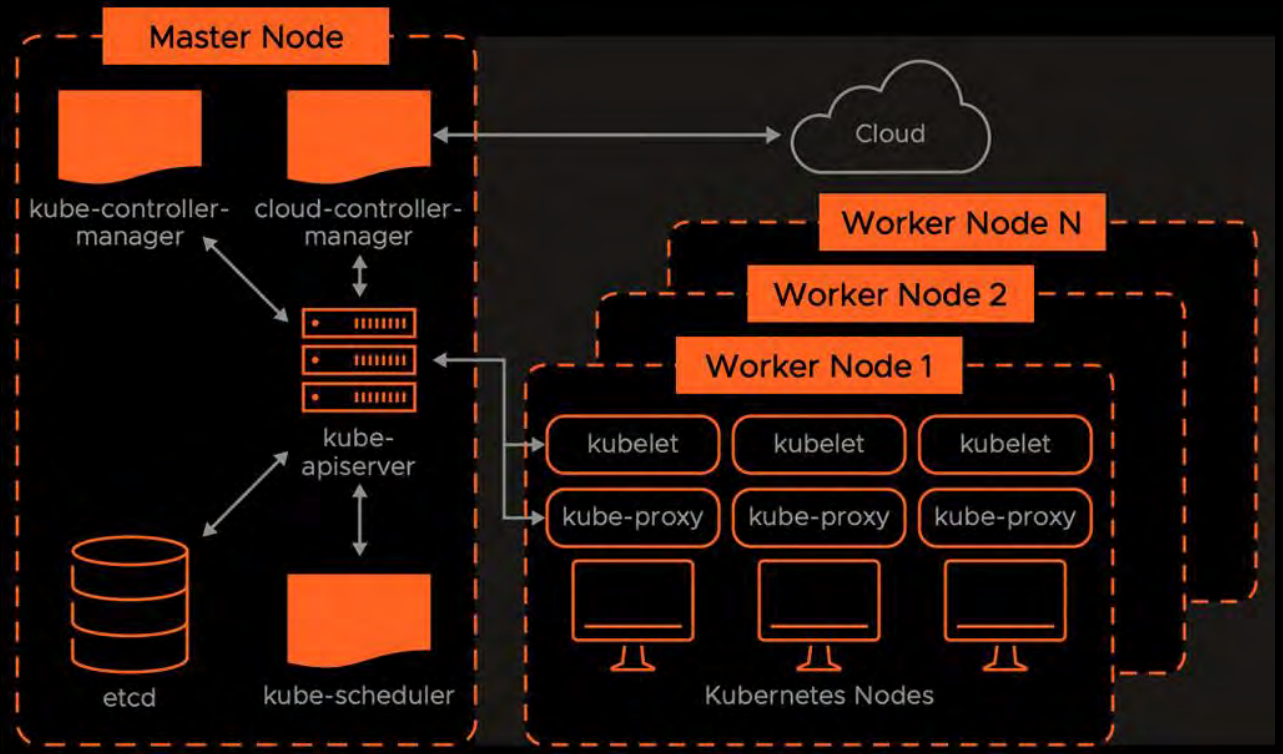
Automated Vulnerability Management

Clair is an open-source project for the static analysis of vulnerabilities in application containers (like Docker/OCI).

https://github.com/quay/clair

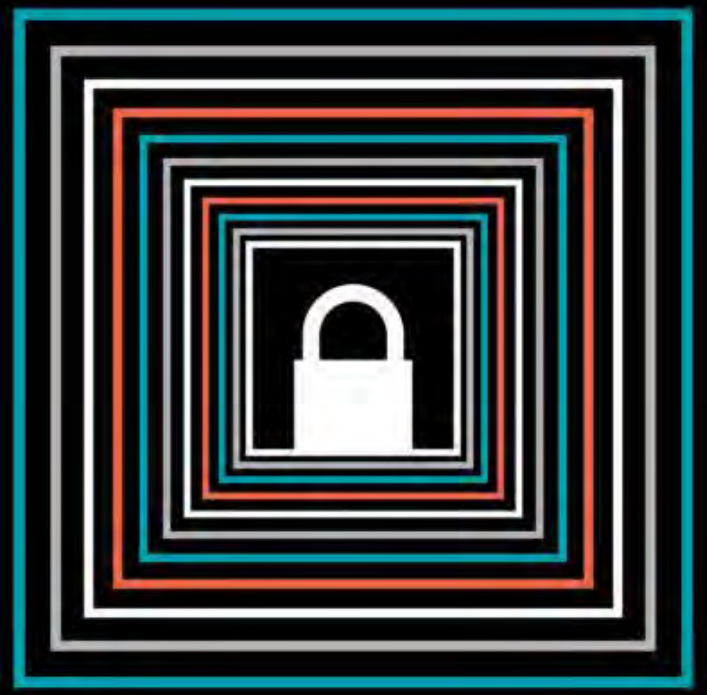
Configuration Management and Network Segmentation

- Implement Micro-segmentation and Leverage Namespaces for Segmentation
- Use Network Policies - Apply Default Deny Network Policies
- Isolate Sensitive Workloads
- Encrypt Container Traffic and monitor.
- Utilize Service Meshes

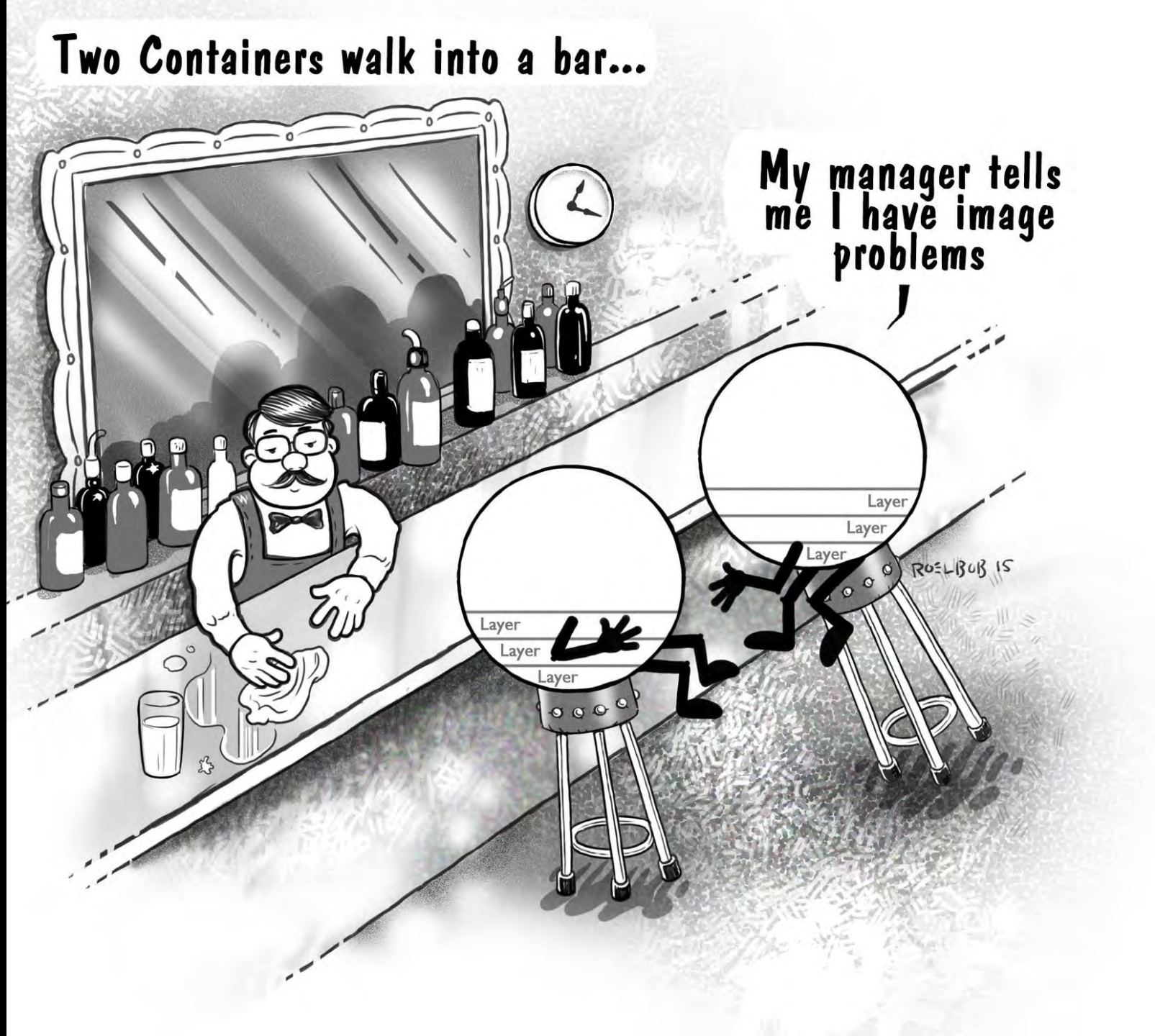


Key Takeaways

- Containers can improve security if used wisely.
- Docker is not secure by default. Never depend on the vanilla configuration.
- Treat images as sensitive data.
- Follow networking and configuration best practices.
- Use automated tools as much as possible and integrate Security into your DevOps pipeline.



Thank you



https://www.vmware.com/solutions/container-networking.html
https://www.trendmicro.com/pt_br/devops/22/b/container-security.html