

Faça as pazes com seu CISO

Mas não deixe a segurança te atrapalhar

Carolina Bozza

Sales LATAM @ Aqua Security

Carolina.Bozza@aquasec.com



“Até 2022, mais de 75% das organizações globais estarão rodando aplicações containerizadas em produção”

Gartner, Best Practices for Running Containers and Kubernetes in Production

Um pouco do mundo de cá...

Segurança



Lento e Criterioso



Averso a Risco



Políticas e Procedimentos



Poucas Pessoas



Mandatário e Formal



... comparado ao mundo de lá



DevOps



Rápido e Caótico



Falha Rápida e Constante



Automatizado

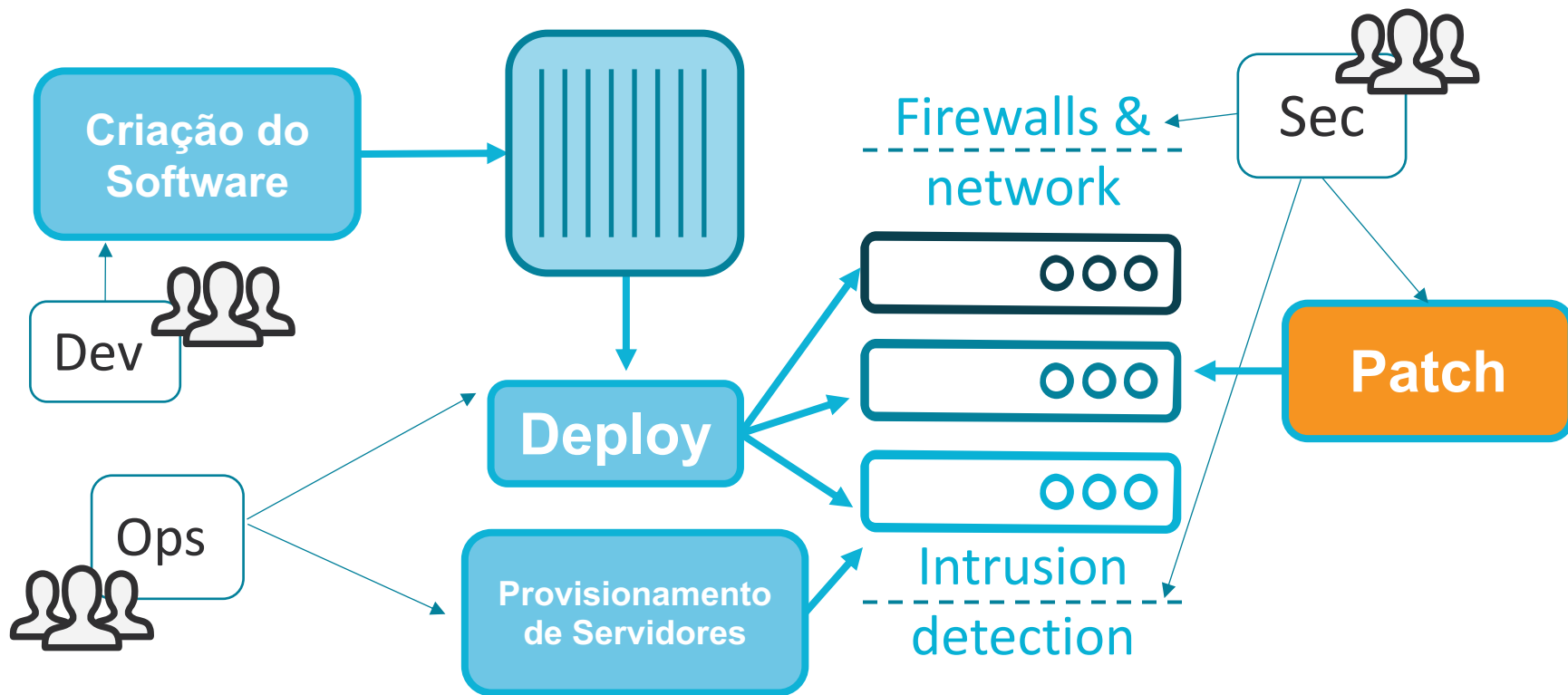


Muita Gente

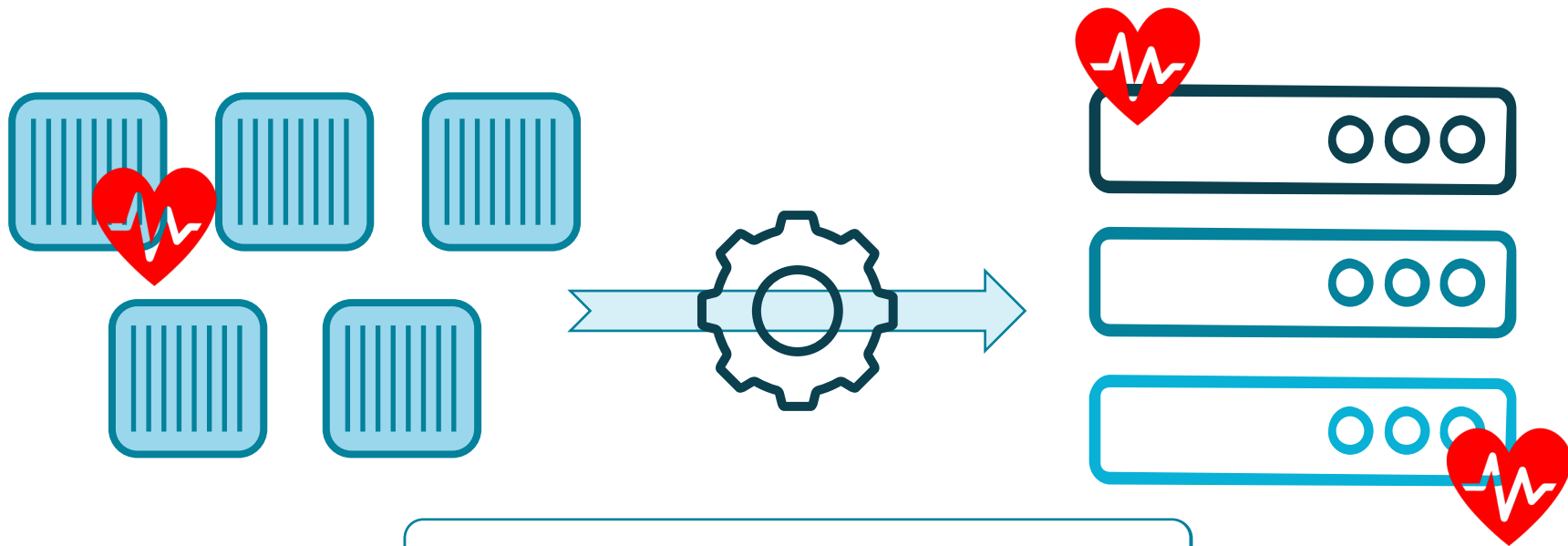


Livre, Informal e Aberto

Deployment Tradicional



O mundo ideal orquestrado e Seguro:



Tempo de vida: ~2,5 dias



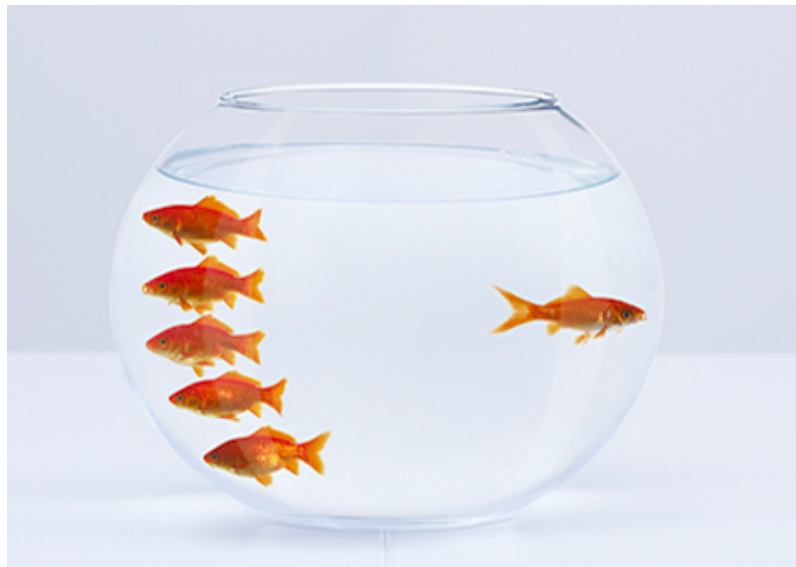


Container é seguro por que sim

- Micro-Serviço: Propósito ÚNICO
- Um container é imutável
- Curta janela de exposição
- Decomposição de Problemas



Shift-Left



- Desenvolvimento Seguro
- Análise de Código
- Scan de Vulnerabilidades
- Garantia de boas práticas
- Informações sensíveis
- Credencial Hard-Coded

Segredo – AUTOMAÇÃO!



Cesar Gimenes

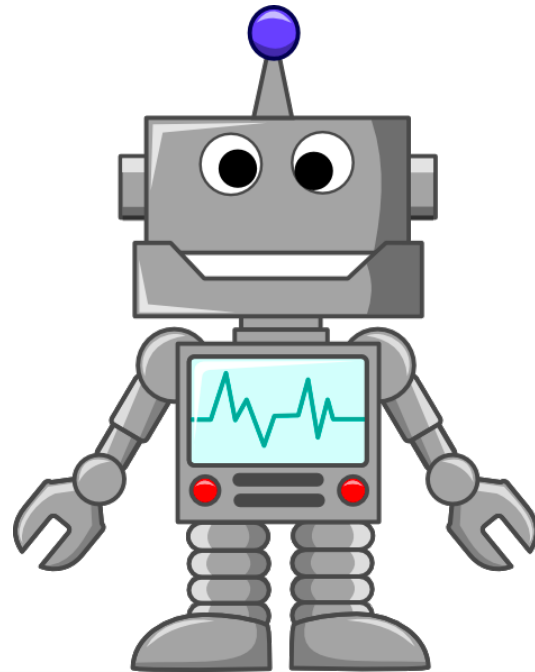
@crgimenes



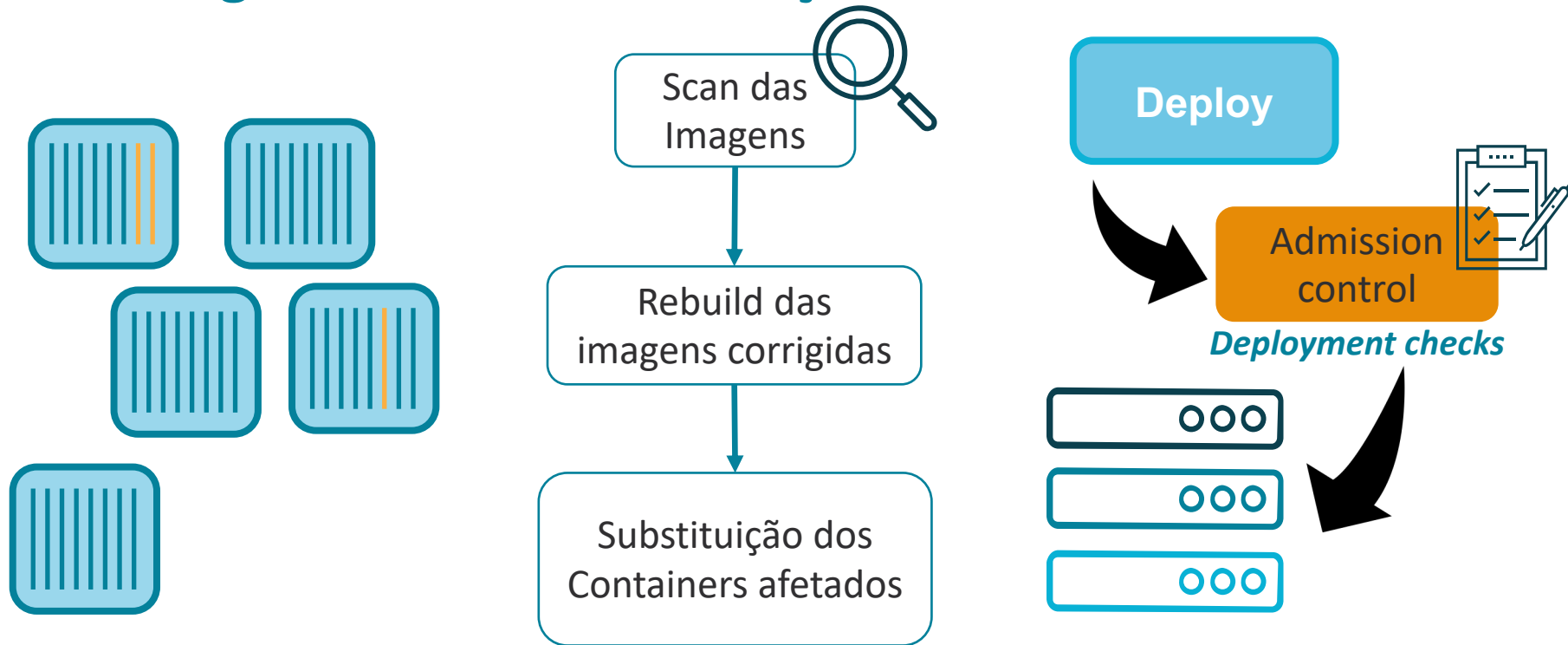
Errar é humano, propagar o erro por todos os servidores de forma automática é DevOps :D

5:22 PM · 27 set 16

23 RETWEETS 35 CURTIRAM



Patching Contínuo - AUTOMAÇÃO



Triste realidade,
no mundo de cá
e daí:



Free tools



Image vulnerability scanner

- Scan images for known vulnerabilities
- SO Packages and App Dependencies
- Works within CI tools
- github.com/aquasecurity/trivy



Image vulnerability scanner

- Allows developers to scan their Docker build for vulnerabilities
- Plug-in available for Jenkins
- <https://github.com/aquasecurity/microscanner>

Open Source Scanners



kube-bench

CIS benchmark for K8S

- Scans Kubernetes nodes against the CIS benchmark checks
- github.com/aquasecurity/kube-bench



kube-hunter

K8S penetration-testing

- Tests K8s clusters against known attack vectors, both remote and internal
- github.com/aquasecurity/kube-hunter



- **Gartner**

- ▶ Top 10 Security Projects for 2019
 - <https://www.gartner.com/en/conferences/emea/security-risk-management-uk/why-attend/gartner-insights/top-10-security-projects-2019>
- ▶ Best Practices for Running Containers and Kubernetes in Production
 - <https://info.aquasec.com/gartner-kubernetes-best-practices>

- **Securosis**

- ▶ The Complete Guide to Enterprise Container Security
 - <https://info.aquasec.com/securosis-assembling-container-security-program>

- **Aqua**

- ▶ GDPR Paper
 - <https://info.aquasec.com/gdpr-compliance-guide-for-containers>
- ▶ OnDemand Webinar - Why Developer Culture is Bypassing Traditional Security Methods
 - <https://info.aquasec.com/devsecops-agility-security>
- ▶ Liz Rice's Talk - Orchestration – Security Threat or Opportunity?
 - <https://www.youtube.com/watch?v=rc1sifwBVks&t=1016s>
- ▶ Aqua Open Source Projects – Kube-Hunter, Trivy & Kube-Bench
 - <https://www.aquasec.com/products/open-source-projects/>



Obrigada! (=

Carolina Bozza

Sales LATAM @ Aqua Security

@carolbozza // carolina.bozza@aquasec.com