

Primeiro encontro CNCF Araraquara

Comunidade e Segurança

Código de Conduta da comunidade



Lembre-se sempre
de dar respeito o
código de conduta da
comunidade



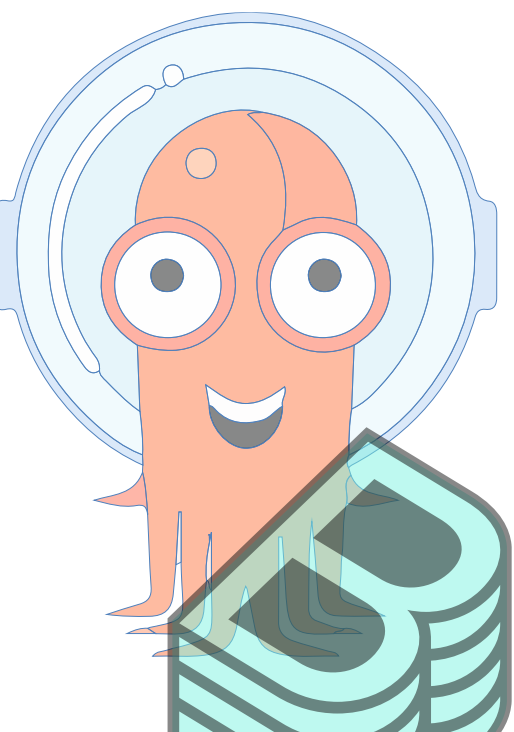
- **Abertura e Apresentação**
- **Quem somos nós?**
- **Como vai funcionar os encontros**
- **Como acompanhar o Ecossistema CNCF**
- **Segurança: CVE-2025-1974 no Ingress-NGINX**
- **Seu cluster está protegido pela cloud?**
- **Q&A**



ABERTURA E APRESENTAÇÃO



- **O que são os Community Groups**
- **Papéis dos CG da CNCF**
- **Porque criamos um CG em Araraquara**
- **Outros CG pelo Brasil e pelo Mundo**



Community Groups

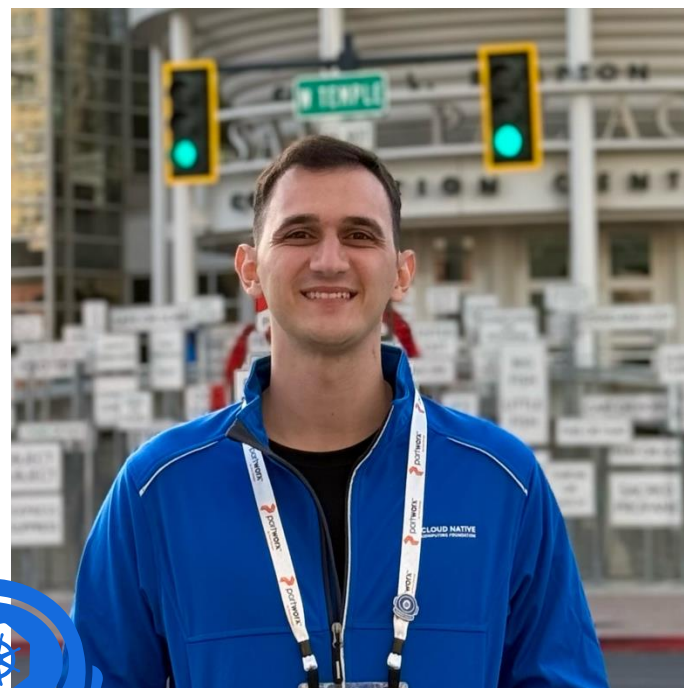


- <https://community.cncf.io/>

Technical Advisory Groups			
<div>North America</div> <div><u>Latin America</u></div> <div>Europe</div> <div>Africa</div> <div>Asia</div> <div>Oceania</div> <div>Virtual</div> <div>CNCF Hosted Projects</div> <div>Community Days</div>			
CLOUD NATIVE ARARAQUARA, SP Brazil 🇧🇷	CLOUD NATIVE AYACUCHO Peru 🇵🇪	CLOUD NATIVE BELO HORIZONTE, MG Brazil 🇧🇷	CLOUD NATIVE BRASÍLIA Brazil 🇧🇷
CLOUD NATIVE BUENOS AIRES Argentina 🇦🇷	CLOUD NATIVE COLOMBIA	CLOUD NATIVE COSTA RICA, HEREDIA PROVINCE Costa Rica 🇸🇨	CLOUD NATIVE CUENCA, AZUAY Ecuador 🇪🇨
CLOUD NATIVE CURITIBA, PR Brazil 🇧🇷	CLOUD NATIVE FORTALEZA, CE Brazil 🇧🇷	CLOUD NATIVE GOIÂNIA, GO Brazil 🇧🇷	CLOUD NATIVE GUADALAJARA, JAL. Mexico 🇲🇽
CLOUD NATIVE GUATEMALA GROUPS Guatemala 🇬🇹	CLOUD NATIVE JUIZ DE FORA, MG Brazil 🇧🇷	CLOUD NATIVE LATAM, CDMX	CLOUD NATIVE LIMA Peru 🇵🇪
CLOUD NATIVE MANAGUA, MN Nicaragua 🇳🇮	CLOUD NATIVE PEREIRA, RISARALDA Colombia 🇨🇴	CLOUD NATIVE QUERETARO, QRO. Mexico 🇲🇽	CLOUD NATIVE RIO GRANDE DO NORTE, RN Brazil 🇧🇷
CLOUD NATIVE RIO DE JANEIRO, RJ Brazil 🇧🇷	CLOUD NATIVE SALVADOR, BAHIA, BA Brazil 🇧🇷	CLOUD NATIVE SAN JUAN Puerto Rico 🇵🇷	CLOUD NATIVE SAN SALVADOR, SAN SALVADOR DEPARTMENT El Salvador 🇸🇻
CLOUD NATIVE SANTA CATARINA, SC Brazil 🇧🇷	CLOUD NATIVE SANTIAGO Chile 🇨🇱	CLOUD NATIVE SANTO DOMINGO, DISTRITO NACIONAL Dominican Republic 🇩🇴	CLOUD NATIVE SÃO PAULO CITY Brazil 🇧🇷
CLOUD NATIVE VALE DO PARAÍBA, SP Brazil 🇧🇷			



Quem somos nós?



Giovani Martins

5by5



Henrique Polsani

Nubank



Jean Carlos

5by5



Matheus Ulisses

Hapvida NotreDame Intermédica



Nossos Encontros



- **Meetups online mensais**
- **Eventos e palestras**
- **Talks técnicas, notícias da comunidade, apresentações de cases**
- **Sugestão de temas pela comunidade**

Como acompanhar a CNCF



- Entender níveis dos projetos: Sandbox, Incubating e Graduated
- Github dos projetos
- Projects Landscape (landscape.cncf.io)
- Newsletter e Blog dos projetos



**Kubernetes
Seguro na
Cloud? Só Se
Você Fizer Sua
Parte!**



CVE-2025-1974



- **Vulnerabilidade de segurança**
- **Redes**
- **Podiam ter acesso a toda a rede dentro de um cluster através do controller do Ingress**
- **Validating Admission Controller**



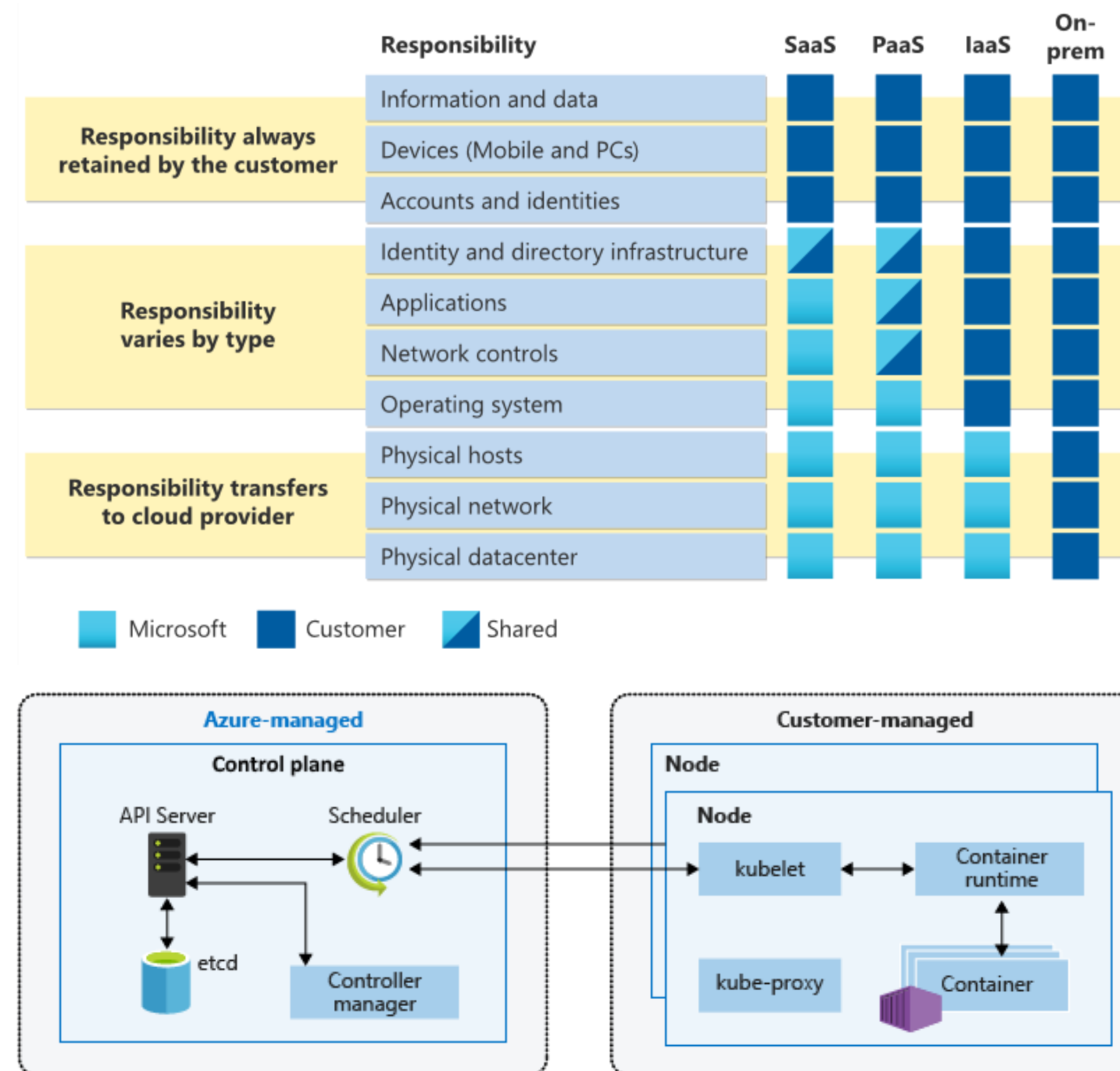
O problema



- **Alguém aqui já assumiu que seu cluster gerenciado estava 100% seguro?**
- **Se um atacante conseguisse acesso a um de seus pods agora, o que impediria ele de dominar seu cluster?**

O problema

- **PaaS:** O provedor gerencia toda a infraestrutura e o ambiente, permitindo que o cliente foque apenas no desenvolvimento da aplicação.
- **IaaS:** O provedor fornece a infraestrutura (VMs), mas a gestão, segurança e configurações são responsabilidade do cliente.



O problema



CLOUD SECURITY

Clusters Kubernetes em centenas de

Da Redação

09/08/2023

07

BOLETIMSEC

Últimas Notícias

ASSINE



Mercado de Cibersegurança

Vazamentos

Cibercriminosos

Vulnerabilidades

Patches e Correções

Tendências

Deep Web

Guerra Cibernética

Falhas de segurança no Kubernetes preocupam empresas globais

Google Kubernetes Clusters Suffer Widespread Exposure

BOLETIMSEC

Últimas Notícias



ASSINE



Mercado de Cibersegurança

Vazamentos

Cibercriminosos

Vulnerabilidades

Patches e Correções

Tendências

Deep Web

Guerra Cibernética

Ataque de Cryptojacking Visa Clusters Kubernetes Desprotegidos

engine (GKE) opens millions of

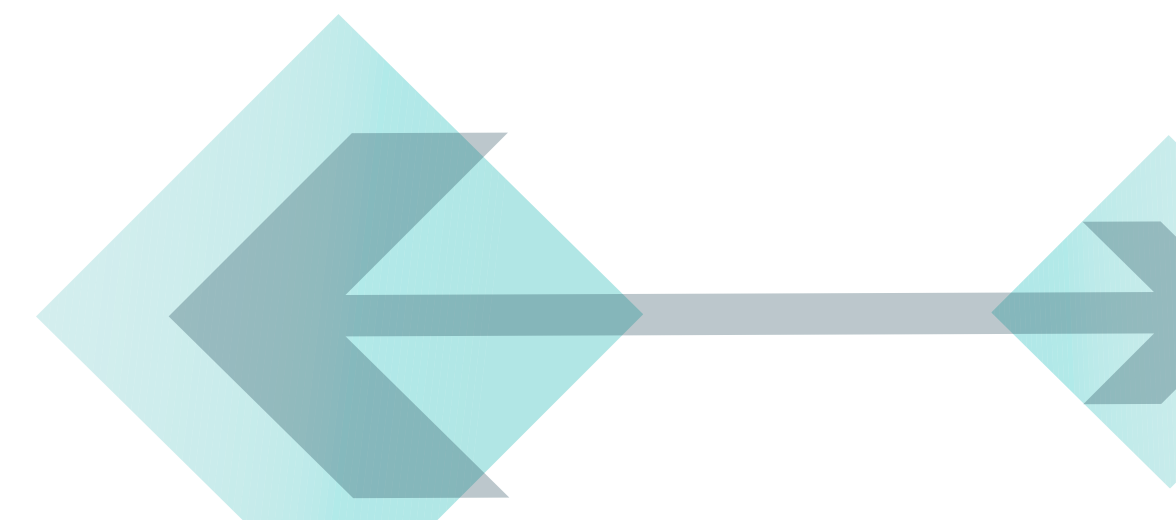
Related Content
Sponsored by



Os Principais Riscos que DevOps e Engenheiros Ignoram



- **Permissividade no RBAC:** Contas com privilégios excessivos podem se tornar portas de entrada para ataques internos.
- **Network Policies ausentes:** Muitas empresas simplesmente deixam o tráfego do cluster aberto.
- **Imagens vulneráveis:** Aplicações rodando com dependências desatualizadas ou mal escaneadas.
- **Configurações padrão perigosas:** Contêineres rodando como root, clusters sem proteção contra execução de código remoto, etc.



Boas Práticas para Blindar seu Kubernetes na Cloud

- **RBAC e Least Privilege** → Nunca dê mais permissão do que o necessário.
- **Network Policies** → Só permita comunicação essencial entre pods.
- **Escaneamento de Imagens** → Ferramentas como Trivy detectar CVEs antes do deploy.
- **Configurações Seguras** → Evite pods rodando como root, use PSP (ou Pod Security Admission no 1.25+), limitação de recursos, etc.
- **Monitoramento e Alertas** → Stack com Falco, Prometheus e Grafana para detectar comportamentos suspeitos.



Projetos CNCF - Segurança



Open Policy Agent



Segurança é uma Responsabilidade Compartilhada

- O **provedor** faz a parte **dele**, mas você precisa **fazer** a **sua**.
- Kubernetes **seguro não** é algo que “**vem na caixa**”.
- Checklist final para **levar** para casa:

⚠ Revisar **RBAC** regularmente.

🚧 Implementar **Network Policies**.

🛡 Escanear **imagens** continuamente.

📊 Monitorar **eventos suspeitos**.

